

Fraud Tools and the Malware Economy

Addressing the explosive growth and dissemination patterns of fraud security tools, and illuminating the economic impact of these applications in order to pinpoint countermeasures.

Pekka Andelin and Albin Bodahl
Malware Analysts, Lavasoft AB

Fraud Tools and the Malware Economy

Introduction

The Internet has been beneficial to consumers by generating a vast amount of new opportunities. However, continuously extending users' lives into the virtual arena has resulted in other, detrimental, repercussions. In recent years, we have seen an explosion-like increase in malicious applications – a trend that seems to be continuous, year after year.

Internet users face a plethora of threats. The limits for what is possible are set solely by the inventiveness of cyber criminals. New phenomena, activities and functionalities generate new conditions that can be exploited by criminals; these criminals constantly seek new ways of translating the credulity of computer users into their own financial gain. This has also cornered users, forcing them into a situation where they constantly have to take precautions in order to protect their privacy and their system's integrity. The security necessities of users has been extended to require increased levels of both awareness and caution, protective software, and an increased level of knowledge about possible threats. The dynamic nature of threats further complicates users' digital lives.

While it's a given that there were fewer threats in 2005 – and that these threats were of another kind all-together – something else happened in that year that came to change the virtual scene for years to come. A new phenomenon emerged: fraud applications.

The result of this analysis shows that a dramatic increase in fraud applications, also known as rogues, took place between 2007 and 2008. This increase was partly initiated in 2006 when Zlob downloaders established their foothold. In 2005, the total amount of rogues discovered by Lavasoft totaled at 11. In 2008, the frequency of newly detected rogues averaged at 16 per month. This significant swell can be attributed, in part, to improved methods of dissemination that increased the public's exposure to rogues. In this way, new dissemination techniques also increased the potential illegal profits for this type of cyber crime.

This report's objective is to illuminate rogues as a phenomenon – their anatomy, their dissemination and their dissemination patterns. The other objective is to illuminate the economic impact of rogues on different levels and to discuss possible countermeasures that could offset further dissemination of rogues.

Defining Fraud Applications and Rogues

In this article, fraud applications are defined as a means by which defrauders can commit fraudulent actions in order to generate monetary gain for themselves. The fraudulent actions are committed at the expense of victims – individuals that are misled and/or deceived. In this context, the term fraud application, or rogue, encompasses applications such as false anti-spyware-/anti-virus applications that are constructed in order to mislead and deceive users. The usability of fraud applications is exaggerated and false security warnings – or other scare tactics like phony detection data – may be used in order to make users believe that their computers are infected by malicious elements. The objective for this type of fraudulent activity is to mislead and/or deceive users into buying the fraud application; registration or purchase of the application is stated to activate its “removal” or “cleaning” capabilities. Such stated capabilities are usually inactivated until the user registers or purchases the program.

In this article, the term “rogue” is used instead of the term “fraud applications”, as the former is more in tune with the common conception of the behavior exhibited by these applications.

Methods of Analysis

Research material and data from Lavasoft Malware Labs forms the basis of this analysis. We have also used some Internet-based sources in order to show possible similarities and/or differences between the results of our research and deductions and other previously published data from sources with an adequate level of credibility. Some data, especially that which relates to cyber criminality, is included as subjective references that have a lower level of credibility; such information is used in our analysis if it, together with our research data, could be shown to have sufficient weight in order to be included as reference material.

Analysis

Paradigm Shift: A New Wave of Applications

SpyAxe is commonly regarded as the first rogue in the new genre that emerged in the latter half of 2005. SpyAxe was the first representative in the family of fake anti-spyware/anti-virus applications presenting false detection data for users. The fraud consisted of making users believe that their system was heavily infected and then urging them to register the phony scanner in order to “disinfect” their system. The “disinfection” functionality was disabled until the user paid a fee to register SpyAxe. The SpyAxe rogue also frequently generated warnings in order to increase the anxiety of users until they caved in and bought the rogue. The method of installation was relatively aggressive; SpyAxe usually piggybacked on Trojan horses or other malicious applications

that were downloaded automatically when users browsed to certain websites. The automatic downloads, or drive-by downloads, were possible due to the exploitation of vulnerabilities either in the Operating Systems or in the users' web browser.

SpyAxe was quickly followed by new types, or clones, of the same family. SpyFalcon, SpywareStrike and Winfixer were some of the early rogue representatives that followed in SpyAxe's footprints. The fact that several of the rogue applications are clones means that they have similar functionality, along with possessing similarities in their Graphical User Interfaces (GUIs). Cloning applications is a way to generate or derive "new" versions rapidly while minimizing expenses and resources.

The entrance of these rogues on the virtual scene in the latter half of 2005 was a paradigm shift as the rogues represented a new wave of applications that utilized social engineering in order to deceive users into buying fake or phony applications. The social engineering tactics used have also come to encompass using lures of a sexual nature in order to address the elementary human needs of users, making the lures increasingly effective. The early rogues (SpyAxe and its clones) were associated with the Smitfraud Trojan that, in turn, was associated with the Cool Web Search (CWS) Trojans. CWS Trojans were programmed to download rogues when they were initiated or executed by users. The Trojans were able to install and hide on users systems by exploiting security vulnerabilities in Windows and in the Java Real-time Environment (JRE). CWS Trojans existed in several varieties in 2005 and CWS was a common infection during that period of time, infecting large numbers of PCs all over the world. The fact that certain variants of CWS could "re-route" traffic and thereby redirect users to specific web locations – most often pornography-related sites – made them widely used as dissemination tools that could help spread rogues to vast amounts of computer users.

Downloaders and Redirectors

The usage of different "helper programs," usually consisting of Trojans of different types, are commonly used to redirect users to malicious sites. When the user has been directed to the malicious site, the actual installation of the rogue application may be performed in different ways; it can occur automatically by exploiting existing vulnerabilities in the user's system and browser, or by manipulating the user into downloading and installing the rogue application. Several types of lures are used to induce users into downloading malicious helper programs. Lures of a sexual nature are often associated with movie codecs that are a stated "must-have" for the decoding and playback of certain movies or for the playback of certain "free" music files. The blooming of digital video technology has created a need for different codecs, such as DivX, Xvid, and MPEG. This need is exploited by the makers of rogues and Zlob Trojans.

Downloader Trojans, such as variants of Zlob Trojans, are commonly used to perform automatic downloads of rogue applications when executed by gullible users. Zlob Trojans with downloading capabilities emanated in late 2005 but their actual breakthrough was during 2007. That was the year that they also came to consolidate their leading position among downloader Trojans.

Zlob Trojans come in several varieties, similar to CWS Trojans. Small frequent changes of the code are used in order to make them bypass detection. The Zlob Trojan exists in two main variants, one that deploys a rootkit that runs in user mode and another that comes without a rootkit. Rootkits are, to put into simple terms, programs that can hide processes, files and registry keys from the user.

A common infection scenario is that a user visiting a pornographic site clicks on a porn video in order to initiate a download or to start the playback. The user is then presented with a message stating that a specific codec needed for the playback of the file is missing and must be downloaded to the user's system. The message is often accompanied with a download window, making it easier for the user to download the malicious helper program. The message – and the opened download-window – may be hard to close down as doing that often initiates new windows to appear. The functionality of presented control buttons in the window, such as “close” or “quit” options, may also be reversed, making it especially hard for the user to avoid the download. The deployment of Zlob Trojans on porn sites is a particularly devious strategy as users falling for the temptation to download the deployed lures often feel shame and therefore avoid reporting their discovery to anti-spyware/anti-virus companies. When the user has swallowed the bait and activated the downloaded “codec”, he or she is often presented with an End User License Agreement (EULA) similar to those presented during installs of legitimate applications. The Zlob Trojan variant that deploys a rootkit is the exception, as it does not present a EULA during the install. The install is, instead, started in the background automatically.

The non-rootkit variant of the Zlob Trojan installs a folder in “%SystemRoot%\ProgramFiles%”, in the program or program files folder depending on the version of the Operating System. The installed folder usually contains between 6 and 10 additional malicious files that are run as background processes on the infected system. The installed folder usually shares the name of the fake codec. The box, below, shows examples of folder names that the malware analysts at Lavasoft Malware Labs have discovered during analysis of non-rootkit Zlob Trojans.

pornmagpass, hqvideo, hq codec, zipcodec, winmediacodec, videocodec, videokeycodec, videocompressioncodec, videoaccess, video activex object, vidcodecs, truecodec, super codec, strcodec, softcodec, silver codec, qaltiy codec, perfect codec, pcodec, my pass generator, mpvideocodec, mpcodec, mmediacodec, media-codec, jpeg encoder, ivideocodec, intcodec, imcodec, icodepack, hqvideocodec, hqvideo, hq codec, gold codec, freevideo, elitecodec, brain codec, videobox, video access activex object, moviecommander, video ax object, moviebox, video activex access, private video, image activex access, pornoplayer, videoaccesscodec, XXXPlugin, Video ActiveXAccess, Online Video Add-on, VideoHeaven, Online Image Add-on, Image Add on, Video Add-on, Image Add-on, SmartVideoCodec, XXXSoft, NetProject, Web Technologies, SunPorn, Applications, RichVideoCodec, FreeCodec.

The name of the folder is altered frequently in order to complicate and avoid detection. Another common tactic is that a dynamic-link library (DLL) file is changed in the different versions of the Trojan. DLL files provide shared functions for applications installed on Microsoft Windows. The DLL file in question is also installed as a Browser Helper Object (BHO) that could be described as plug-in modules for Microsoft's Internet Explorer web browser. The DLL file that is executed with Internet Explorer generates phony pop-up messages that are characteristic of the non-rootkit Zlob Trojan. The messages urge the user to download the rogue application in question in order to protect the system against the stated "infections". The "nagging" pop-up messages are frequent and deliberately disturbing. These types of nagging pop-up messages do not occur only when surfing the Internet with Internet Explorer; they can also occur when the user is offline. The installed DLL file may also cause a redirection of network traffic, steering the user to a specific Web location where the user can be exposed to the rogue. The processes of the Zlob Trojan are run in the background, without the user's knowledge, and it is not uncommon that the processes support or guard each other, making them hard to close down. Due to these parameters, the Zlob Trojan has a multi-headed approach of attack.

The rootkit version of the Zlob Trojan is also called "DNS Changer" as it has the capability to change the settings for the "DNS NameServer" on infected machines. DNS stands for Domain Name System, and is a system for associating domain names with IP numbers. Changing the DNS NameServer may result in a redirection of network traffic so that traffic from the infected machine is redirected to locations hosting malicious content. The aim of this is to channel users to Web locations where they can be exposed to misleading marketing strategies, striving towards luring the users into installing rogue applications. Another possible aim for this action is to steer users to phishing sites where exploitation of possible vulnerabilities can take place.

The Zlob type of user-mode rootkit operates in the user or application layer of the operating system. The rootkit is run as a thread of csrss.exe, the Client Server Runtime Process. The fact that csrss.exe is a legitimate process on Microsoft Windows operating systems makes the Zlob Trojan harder to detect, at least for common users. The Zlob rootkit Trojan ensures that it will start up with Windows by altering a registry key in the Windows registry, HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon "System", to point to the executable rootkit file.

Several variants of fake codecs have emerged between 2007 and 2008. Their characteristics may differ somewhat from those of the Zlob Trojans. The core strategy is, however, to deceive users into licensing or purchasing specific rogue applications. Analysis and research work at the Lavasoft Malware Labs has discerned that Zlob Trojans block Internet Explorer from accessing other malicious domains that host competing versions of rogues. This could indicate that a certain level of competition between the different creators of rogue applications exists.

Informal Naming Convention

Lavasoft Malware Labs has discovered an existing standard, or informal naming convention, among rogue applications. The most popular naming alternatives are combinations of the words "Spy" and "Spyware" (15%) with the addition of a suitable phrase, for example "Crush" or "Secure." This results in names such as SpyCrush and SpywareSecure. Combinations of the word "Win" have a relatively high prevalence. Winantispysware and WinProtector are examples of resulting names.

Malware Labs' analysis also shows that names hinting to security and threats have a high prevalence, possibly due to their capacity to catch the attention of users. The mimicking of the names of legitimate security applications is also very common; this is done in order to attract and mislead users. Rogue applications like SpywareBot (its legitimate counterpart is Spybot Search & Destroy) and AdwareBot (its legitimate counterpart is Lavasoft's Ad-Aware) serve as examples of such variants.

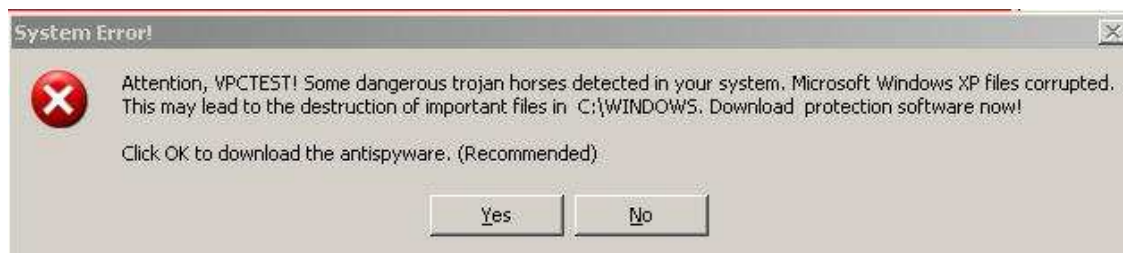
In 2008, the makers of rogue applications started to reorder the words in their application names, increasing the confusion of both the public and anti-spyware/anti-virus companies. A new clone of a rogue application is usually given a new name before it is released. Reordering the words in the name of a rogue application generates a new, unique name while making it possible to release "new" versions without any extensive alterations of its interface. The names of clones such as "Antivirus XP 2008" and "Antivirus 2008 XP" are examples of such reordering. The following image shows a statistical compilation of the distribution of different variants of prefixes that are used in the names of rogues.



This chain of events takes place in order to install a BHO in the background without the users' knowledge. A successful install and initiation of the BHO object depends on an execution of Internet Explorer which is done in order to start the DLL file, or BHO, that has been installed to %SYSTEMROOT%\system32. The image below shows the activated BHO.



When the system has been infected in this manner, users are presented with fake security warnings each time they open folders via Windows Explorer or when they click links within Internet Explorer. The falsified security warnings are intended to make the user believe that their system is heavily infected, scaring them to download the rogue application. The following image shows an example of this type of fake security warning.



If the user takes the bait and chooses to click "Yes", a new window (see image below) allowing for the rogue to be downloaded is presented.



IE Antivirus has copied its ways of deception from the Zlob Trojan. Users are drawn to pornographic sites and the need for a specific Video ActiveX Object is aroused. Small and frequent changes in "c-setup.exe" along with the DLL file (BHO), in order to avoid detection by anti-spyware/anti-virus applications, increases the power of this rogue-application. The updated files are downloaded and deployed in the background without the user's knowledge. The rogue is thereby designed to be hard to detect. When a system is fully infected, users are exposed to frequent and annoying pop-ups, urging them to purchase the rogue to clean their system. The image, below, shows the

interface of IE Antivirus, including the text link “Unregistered version! Click here to register your copy...”



XP Antivirus 2008

XP Antivirus 2008 uses another form of strategy than IE Antivirus. There are, however, many similarities between these two types of rogues. The main similarities exist in the methods of installation and dissemination. Both rogues use nagging pop-ups in order to mislead and deceive users. XP Antivirus 2008 generates message windows in order to make users believe that their system is infected. Users are then frequently urged to install the rogue in order to “clean” their system. However, the fake security warnings do not appear to descend from webpages. The fake pop-up warning messages seem to originate from the operating system but they actually do not. If users try clicking the “Cancel” button in the message interface, a new window is generated, stating that their system is to be scanned by XP Antivirus 2008.

Prior to the install, users are directed to a webpage where they are exposed to several graphical interfaces giving the impression that their system is being scanned. The “scan” is a fake, but a “scanning sequence” is still presented for users visiting the webpage. The

result of the scan is a pre-defined list of fake threats that do not exist on the user's system. As a final touch, users are presented with another interface where one click within the presented window results in an install of the rogue.

XP Antivirus 2008 gives the impression of being a professionally developed application. A logotype stating "Windows Compatibility" is used in order to further enhance the professional appearance. As a part of the installation process, users are directed to a relatively legitimate-looking webpage where the makers behind the rogue expose the user to marketing stating that registered users can utilize support services, and that credit card and payment data is safeguarded in a proper manner. The truth is, however, a tragic one as users swallowing the bait give their credit card number, along with their money, to cybercriminals. Registering XP Antivirus 2008 costs \$49.95 but additional offerings may be presented to gullible users. Users that decide to purchase the rogue are directed to a secure shell (SSH) webpage, such as <https://secure.software-payment.com>. The host of such webpages may be localized at Bridgetown, Barbados; this is a common localization for such webpages associated with rogue applications and fraudulent money transactions.

When the installation finishes, users are presented with a window that is almost identical to the one used by the legitimate version of Windows Security Center. The differences are that the XP Antivirus version of "Security Center" detects itself as a legitimate anti-virus application and that the link presented to users via the interface is part of the scam. Users that click the link presented are, once again, directed to the homepage of the rogue. The link presented by the legitimate Windows Security Center provides – in contrast to the one presented by the rogue – users with help documentation regarding installs of anti-spyware/anti-virus software. Users that have installed XP Antivirus will be presented with two different Security Center applications within the Windows Control Panel. The legitimate one is called "Security Center" while the rogue version is named "Windows Security Center". The names are similar and that can cause confusion among common users that may think that "Windows Security Center" sounds more legitimate than "Security Center."

Users that leave their computers for a few minutes without performing any operations on them will usually find that XP Antivirus 2008 presents them with fake scan reports, stating that a number of malicious items have been found during the "scan." If users then press the "Remove" button in the rogue interface – in order to remove the listed "infections" – the sequence is repeated and the users are once again directed to the rogue site. Clicking "Cancel" within the rogue interface generates new pop-ups, which may state that "...Program is transferring unreliable data to the user...", urging users to block the transfer. The actual content of the presented messages may vary and contain spelling errors.

The common factor is that all presented links and executed commands, such as pressing “Cancel” or other buttons in the rogue interface, directs users to the XP Antivirus 2008 webpage. The makers of the rogue utilize social engineering tactics to mislead and deceive users. While the loss of the \$49.95 registration fee may be possible to live with, the effects of a stolen credit-card number (possibly accompanied by the victim’s name and social security number) may be disastrous for any affected individuals.

BraveSentry

BraveSentry is a rogue that uses a peer-to-peer botnet of infected nodes in order to disseminate. BraveSentry is installed forcefully when a user executes a Win32.TrojanDownloader.Tibs/Nuwar/Win32.Worm.Zhelatin type of malicious file. BraveSentry is one of the rogues with the longest lifespan. It was discovered by Lavasoft in mid 2006 and is still active.

The Tibs/Nuwar infection has proven to be a highly diversified infection that performs frequent updates in order to avoid detection by anti-spyware/anti-virus companies. The fact that each node computer in a peer-to-peer botnet has both client and server functionality, thereby forming a decentralized ad-hoc network, makes it harder to find the source of the botnet. That also makes them difficult to close down. Nuwar/Tibs has contact with its infected pairs and it can harvest e-mail addresses from different accounts. The Tibs Trojan uses a built-in Simple Mail Transfer Protocol (SMTP) engine to send unsolicited spam e-mail to the harvested e-mail addresses, increasing its dissemination capabilities. In a way, the Nuwar worm serves as a “carrier” of rogues. The usage of botnets for the dissemination of rogues presents as an existing interaction between disseminators/carriers and rogue applications – aimed at an increased economic gain.

Rogue Applications on Mac Platforms

Innovagest – besides being the name of a rogue application – is also the name of the development group behind rogues such as XP Antivirus 2008 and Winiguard. Some signs may point to the fact that the same developer(s) lies behind the MacGuard rogue which has been promoted via the macguard.net domain. The domain has the IP address of 78.157.142.165 and is localized in Latvia via the host, VdHost Ltd. That IP address, along with the host, is shared with the winiguard.com domain. It could be argued that this points towards an existing relationship between the creators of these rogues. The fact that the naming convention, along with the look of the websites, shows clear similarities strengthens this argument. Therefore, this could indicate that developers behind Windows rogues have extended their activities to also encompass development of

rogues for the Mac platform. MacSweeper and iMunizator are examples of other rogues aimed at Mac users.¹²

The Botnet Threat

During the latter part of 2005, botnets were regarded as the biggest threat with couplings to cyber criminality and the malware economy. Botnets were predicted to play an important role as a profit-generator in the cyber criminal world. Botnets can be described as networks of infected computers that are controlled by a central node computer. The infected puppet computers are given different types of tasks via the central node computer, such as to disseminate spam. The first botnets were created manually but automation, via e-mail worms such as MyTob, increased the botnets' dissemination possibilities along with increasing the possibilities for monetary gain. The fact that botnets were relatively easy to control and that it was possible to "rent" them out increased their profit potential even further.

In its "Fortinet Reviews Malicious Code Activity During 2005" report, Fortinet illuminates that virtual self-protection should be a trinity consisting of anti-virus, system updates and education.³ Despite the adoption of these protective measures, it is still difficult to stay protected against zero-day attacks – the first wave of attack by a new type of threat phenomenon. In order to stay protected from such attacks, users must avoid high-risk activities such as opening certain types of e-mail attachments and downloading and executing unknown files. Users also have to avoid falling for advertisements and offerings, presented in different virtual environments, that sound too good to be true. The fact that botnets are rentable for different criminal purposes enable them to be used for the dissemination of advertising campaigns that can reach a large number of people in a very short period of time. Mass e-mail messages that include links to malicious sites or links pointing to fake codecs associated with rogue software are becoming increasingly prevalent. This is – and has been – a phenomenon that can be verified by the malware analysts at Lavasoft Malware Labs.

¹ Alex Eckelberry (Sunbelt), "New Mac rogue?". <http://sunbeltblog.blogspot.com/2008/10/new-mac-rogue.html>. Retrieved on 2009-03-26.

² Peter (Intego), "Beware Bogus Security Software". <http://blog.intego.com/index.php?s=beware+bogus>. Retrieved on 2009-03-26.

³ Fortinet, "Fortinet Reviews Malicious Code Activity During 2005". http://www.fortiguardcenter.com/report/roundup_2005.html. Retrieved on 2009-03-29.

The utilization of botnets is significant for the dissemination of rogue software. The mass-mailing of lures is highly prevalent. For example, the user is urged to click on links in order to access erotic movies; if the user falls for the lure and clicks the presented links, he or she is urged to install a codec in order to be able to watch the movie. In reality, the codec is mostly a Zlob Trojan that can download rogue applications from predestined IP addresses. In this way, the botnets – along with other types of dissemination tools or strategies – interact in order to increase the profit potential of this form of cyber criminality. This has much in common with marketing strategies where increased exposure correlates with higher profits. Even if the majority of people have learned to be vigilant against mass-mailed advertisements, some will always take the bait, hook, line, and sinker.

The rental income from botnets, along with profits originating from the sales of rogue software, may ultimately yield large sums for criminal networks. Such interaction makes it difficult to illuminate rogue software from an isolated economical perspective; this approach would generate misleading results. The economical impact of dissemination tools must, therefore, be considered as various components making up a whole sum.

The Russian Business Network (RBN) is a criminal organization that reportedly originates in St. Petersburg, Russia. Beginning as a concrete and tangible entity in the world of cyber criminals, RBN has increasingly become an international grouping of parties engaged in twinning and market interactions in order to reach the masses and to maximize profits. RBN is stated to be the leading force behind the notorious Storm botnet which was named for the worm – Storm – that was used to link zombie computers to a botnet that encompassed between 250,000 and 50 million (depending on the data source) infected computers. In the case of RBN and their eventual couplings to the Storm botnet, there is great reason to take a critical view of the data that flourishes. Obtaining unbiased data and information about RBN and other criminal networks is difficult as there are little to no trustworthy sources; this is something that also increases the breeding ground for rumor spreading.

The Storm botnet, and other botnets such as Nugache, that emerged between 2006 and 2008 have been followed by a marked rise in spam levels. The Nugache botnet was also named for the worm that was used to link zombie computers. Storm and Nugache reportedly originate in Russia, but links to RBN have not been fully established.

According to Trend Micro, the extensive block of IPs formerly associated with RBN were closed down in late 2007, which could point to the fact that RBN dissolved.⁴

⁴ Trend Micro, "RBN goes *Poof*". <http://blog.trendmicro.com/rbn-goes-poof/>. Retrieved on 2009-03-26.

Another explanation is that RBN has spread its activities across the world in order to complicate detection. Asia, particularly China, and the Pacific are areas that may become the next foci for centralized cyber criminal activities. The reason is that these regions allow for the mass registration of domains and large blocks of IP addresses. The ability to make extensive profits with a relatively small work effort is a propulsive force behind the development of botnets. The broad use of botnets as dissemination tools for many types of threats, including rogues, make them an interesting and important phenomenon to follow-up and investigate.⁵

Dissemination Patterns

Since the end of 2005, Lavasoft Malware Labs has collected data on different types of rogues in order to follow their dissemination and development. We have collected data such as design changes and attack/infection approaches, and we have monitored their geographical starting points by tracking IP addresses. The aim is to investigate existing patterns of dissemination in order to find out how and why the criminals behind rogue applications utilize the network architecture at specific locations globally. Our hope is that, with the help of the collected data, we will be able to find new and more efficient ways to combat rogues.

The collected data shows patterns in the localization of servers hosting rogues between 2006 and 2009. The collections of red dots presented in the maps, below, show patterns with clear foci.

⁵ The Washington Post, "Shadowy Russian Firm Seen as Conduit for Cybercrime".
<http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html>.
Retrieved on 2009-03-26.



A relatively low amount of new rogues emerged during 2006. USA and Ukraine are clear foci.



The image above shows that a major increase in rogue applications took place in 2007. The US west and east coast, along with Canada, Ukraine and Hong Kong, are clear foci.



The map above shows the situation in 2008 when the number of new rogues literally exploded. USA and Russia suffered a major increase in rogues, with Middle Europe and Ukraine close behind with a high prevalence of new rogues.

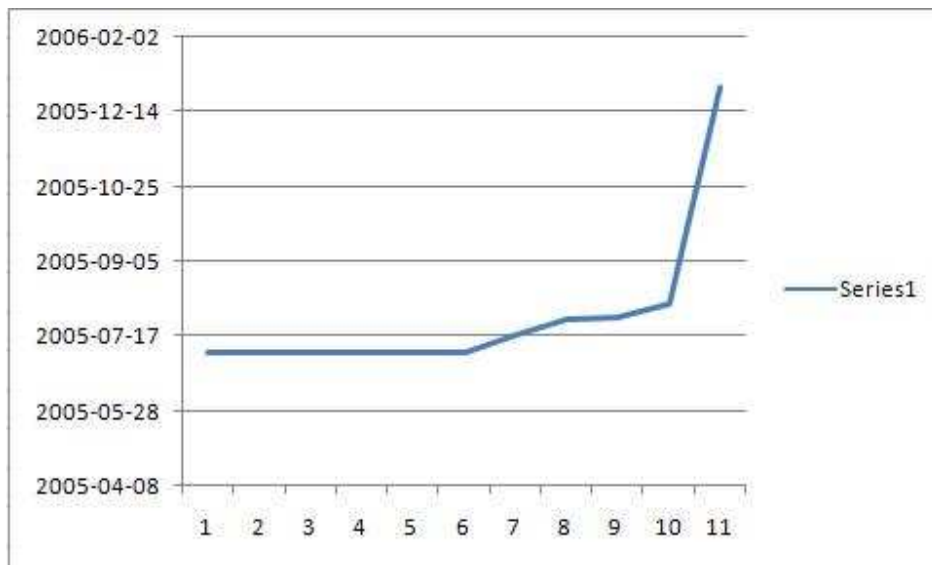


The beginning of 2009 – January to March – is showing clear foci on Latvia and USA.

Since 2007, we have noticed a clear increase in the dissemination of rogue applications from the U.S., especially from California and the surrounding area. From late 2007 to March 2009, Lavasoft Malware Labs' analysis shows that more than 30% of the "mother-domains" associated with rogues are located on the west coast of the U.S. The analysis shows that up to 30 rogue applications were distributed from that geographical location during that period of time. It may be argued that the increase is caused by the fact that past Russian activity – with couplings to the dissolved Russian Business Network – has taken a new impetus in the western U.S.

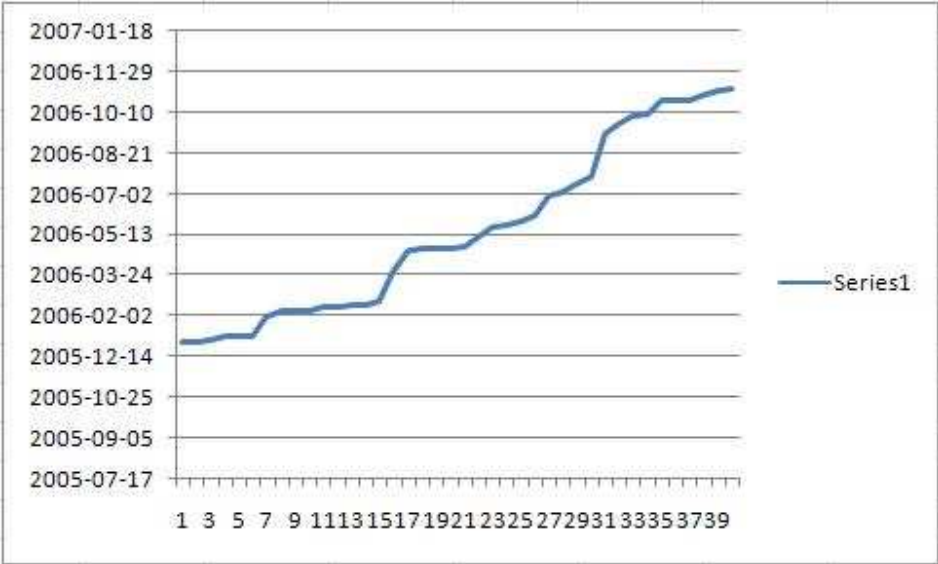
The following charts show the general growth rate of rogue applications between 2005 and 2008, based on data collected by Lavasoft Malware Labs.

2005



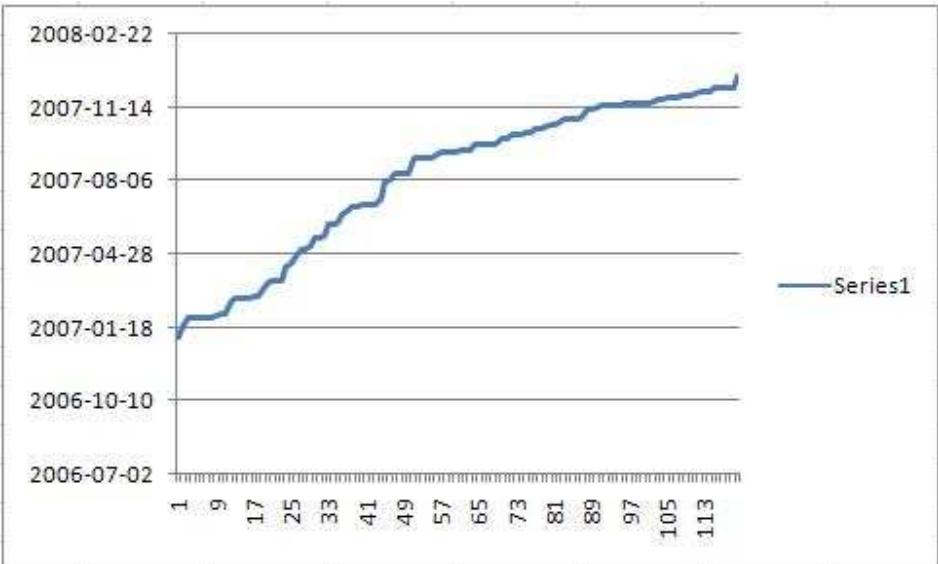
11 new rogue applications were found in 2005.

2006



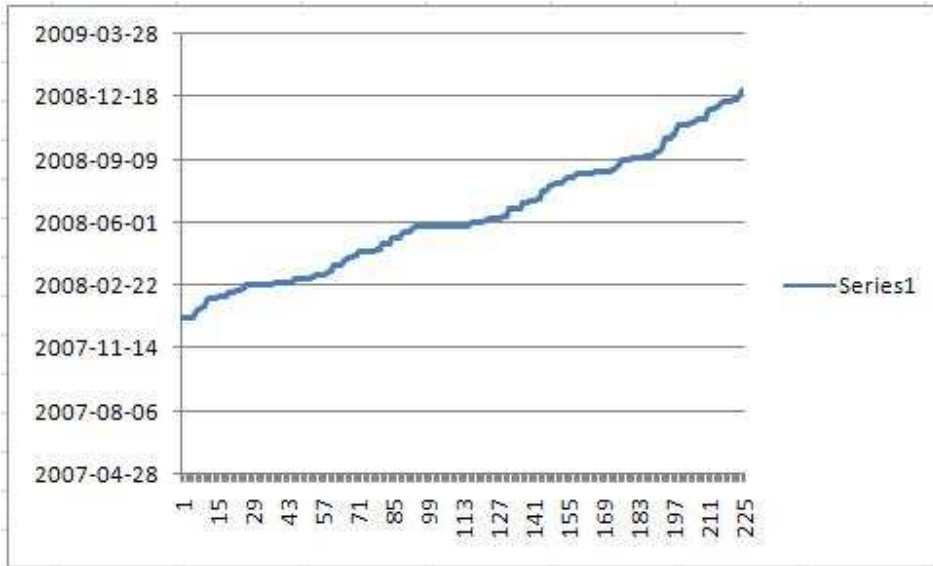
39 new rogue applications were found in 2006.

2007



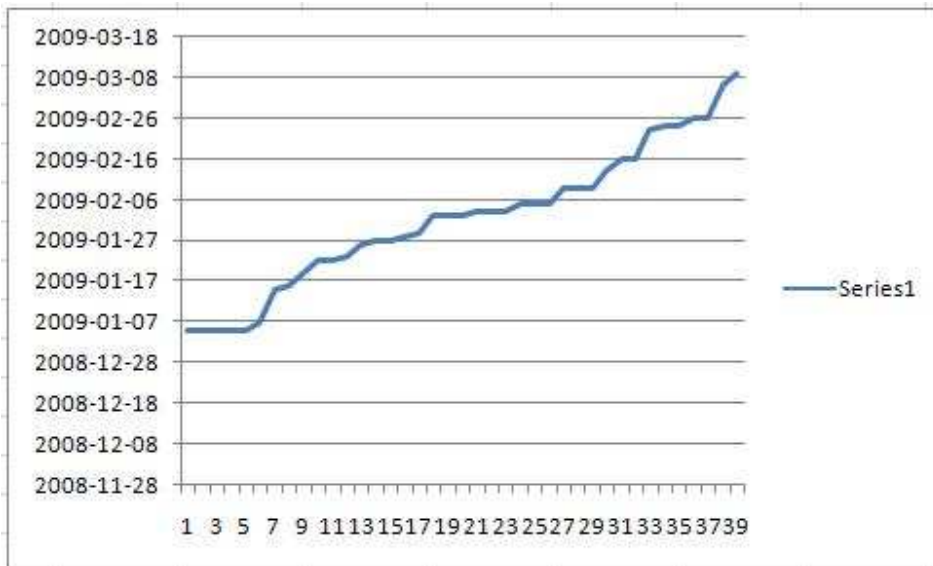
119 new rogue applications were found in 2007.

2008



225 new rogue applications were found in 2008.

2009



39 new rogue applications have been found in 2009 (January to March).

The tendency shown above indicates that the increase in rogues will continue in 2009. From 2005 and 2008, rogue applications increased by 2,045%.

Varying Degrees of Countermeasures

The main responsibility for protection against rogue applications is laid upon the shoulders of individuals. However, efforts to combat rogues are taken at a higher level; one example is the worldwide Domain Name Registrars. Domain Name Registrars may refuse registration of large blocks of IP addresses or close down misused IPs. These kinds of measures are effective in order to prevent dissemination from an early stage. The Internet Corporation for Assigned Names and Numbers (ICANN) is the authority that has overall responsibility for Internet Protocol address space allocation and the top level domain name system. ICANN, however, does not conduct checks in order to pinpoint how different IPs are used. The Domain Name Registrars act as agents in the registration of domains and must, in turn, be accredited or approved by ICANN in order to be able to register domains. Still, accreditation does not guarantee total protection against mistakes and misdirected activities.⁶ For example, Computersweden has stated that ICANN recently was stripped of its own domains “iana.com” and “icann.com” by a Domain Name Registrar that was deceived into transferring the domains to another party.⁷

According to Domainnews.com, EstDomains is a Domain Name Registrar that “tried” to take up the fight against the distribution of rogues from the blocks of IPs that are/were in their possession. Domain Name Registrars may always get some customers that use their services and domains with malicious intent, making total protection hard to achieve. EstDomains stated to have included protection against domain misuse in their corporate structure; this was carried out by way of ongoing control of registered domains and by websites acting as hosts for malicious applications being closed down on short notice. The U.S.-based EstDomains also stated to cooperate with the Net provider, Intercage, in order to spot domain misuse at an early stage. According to EstDomains, it has developed a system, aside from these measures, that makes it possible to reveal malicious sources and malicious websites in an efficient manner. The utilization of information sources such as malwaredomainlist.com, malwaredomains.com

⁶ ICANN, "About". <http://www.icann.org/en/about/>. Retrieved on 2009-03-26.

⁷ Computersweden, "Icann lurades på sina domännamn". <http://computersweden.idg.se/2.2683/1.171173>. Retrieved on 2009-03-26.

and malwarebytes.org, along with incoming tips from the public worldwide, are mentioned as additional weapons in their stated fight against the dissemination and distribution of rogue applications.⁸

EstDomains' cooperation with InterCage, with the stated aim at curbing the spread of rogues, was perceived as unlikely due to InterCage's previous reputation of being "malware-friendly". In the past, InterCage has been associated with transferring (utilizing their network structure) great parts of the malicious network traffic flowing from the US west coast. The news source, *The Register*, touched on the subject of InterCage being a carrier of malicious content in September 2008. InterCage had, for example, strong ties to Esthost, a notorious ISP in East Europe. InterCage's stated shift towards more benign activities may be an effect of their closed cooperation with Esthost, according to *The Register*. While InterCage's cooperation with Esthost was closed, Esthost accounted for up to 50% of InterCage's total profits. As an Internet service provider, InterCage has exclusive control over its network traffic flowing in its infrastructure in the San Francisco area. That gives them a unique opportunity to counter misuse and/or the dissemination of malicious software. In light of this, it would be easier to comprehend the cooperation between Estdomains and InterCage. By cooperative efforts, they may have been able to achieve a synergistic effect where the efforts of one party may have been enhanced by the others. ICANN, however, took away Estdomains' rights to register domains on November 24, 2008, due to Estdomains' criminal behavior. ICANN referred to a clause in the rules that apply to Domain Name Registrars, claiming that the Domain Name Registrars cannot undertake criminal activities. Estdomains' alleged criminal activities made ICANN terminate the contract with Estdomains before it expired. Estdomains had, according to ICANN, approximately 281,000 domains at their disposal. The future will tell if InterCage, in fact, has cleaned up its act or not.^{9 10}

As previously mentioned, the analysis of the latter months of 2007 up till today shows that more than 30% of the "mother-domains" associated with the dissemination of rogues are localized on the U.S. west coast; up to 30 different rogue applications have

⁸ Domainnews.com, "EstDomains Denies Links to Malware Distribution; Fails to Deny Washington Post Allegations". <http://www.domainnews.com/en/general/estdomains-denies-links-to-malware-distribution.html>. Retrieved on 2009-03-26.

⁹ The Register, "'Malware-friendly' InterCage back among the living". http://www.theregister.co.uk/2008/09/24/intercage_back_online/. Retrieved on 2009-03-26.

¹⁰ Tech World, "ICANNs beslut att stänga av Estdomains står fast". <http://techworld.idg.se/2.2524/1.192748/icanns-beslut-att-stanga-av-estdomains-star-fast>. Retrieved on 2009-03-29.

been distributed from that location during that period of time. Cooperation's between ISPs and Domain Name Registrars could form a possible approach in the development of an efficient high-level defense strategy in the fight against the dissemination and distribution of rogues, especially in the U.S. west coast area and other dissemination foci. We wish, however, to sound a note of caution: increased surveillance of domain-based activities, and Internet traffic, may result in restrictions on user privacy. All such surveillance activities should be balanced and carefully considered. The registration of large blocks of IP addresses must be accompanied by great caution, extended control and follow-up. ICANN's accreditation process, which an applicant must submit to in order to become a Domain Name Registrar¹¹, does not automatically mean that deficient applicants are rejected. ICANN may also have to take greater responsibility for the control and follow-up of accredited registrars. The fact that accredited registrars may, by many parties, be considered secure and reviewed makes it even more important to achieve efficient filtering of deficient actors among the registrars.

Conclusion

Revisiting Rogues: Anatomy, Dissemination, and Dissemination Patterns

One of this report's objectives was to illuminate rogues as a phenomenon – their anatomy, their dissemination and their dissemination patterns. Our research at Lavasoft Malware Labs shows that the arrival of rogue applications in the latter part of 2005 was a paradigm shift as the rogues represented a new wave of applications that utilized social engineering in order to deceive users into buying fake, or phony, applications. We have also visualized the chain of infection, link by link, by showing three different examples encompassing both similarities and differences between the different types of rogues.

We have illuminated the utilization of downloaders, such as Zlob Trojans, which are used to facilitate the depositing of rogues. These downloaders are frequently masked as applications, like codecs, that attract large groups of users. The authors play on the needs of users, supplying what appears to be applications that are a so-called "must have" for the playback of digital movies or music files. We also pointed to the fact that the usage of other "helper programs," usually various Trojans, in order to redirect users to malicious sites is very common. When users reach rogue sites, a forced drive-by installation of the rogue may be possible by utilizing exploits (for example, browser

¹¹ ICANN, "Accreditation Overview". <http://www.icann.org/en/registrars/accreditation.htm>. Retrieved on 2009-01-21.

exploits). The users may also be exposed to different types of social engineering tactics in order to make them download and install the rogue on their own.

The goal of the perpetrators behind rogues is to mislead and deceive users into paying good money for useless applications. Rogues rely heavily on the usage of social engineering and scare tactics in order to make users believe that their system is severely compromised by different types of threats that are stated to be dangerous. With the help of frequent pop-ups, users are nagged into taking action, either into (re)visiting the rogue homepage or into purchasing the rogue by providing confidential credit card information, possibly through phishing. Leaking personally identifiable or financial data to cyber criminals is often disastrous for the affected individuals.

Mimicking the names and look of legitimate security applications is another approach used by rogues to mislead and deceive users. Small alterations of the graphic user interfaces of rogue applications, and/or their names, are techniques that are used in order to mislead users. That strategy also makes it possible to easily create clones of rogues without the need for extensive resources. Such alterations are used by the analysts at Lavasoft Malware Labs in order to categorize rogues into families and to prove parentage.

The usage of peer-to-peer botnets, where the users' computers are nodes in the network, is an efficient way to increase the dissemination of rogues. The fact that rogue applications may be force-installed on the nodes reduces the originator's need of relying on social engineering in order to make users install the rogues themselves. The decentralized structure of botnets makes it more difficult to track the originator.

The analysis shows that there may be evidence pointing to the fact that developers or development groups, which have previously focused on the creation of rogues for the Microsoft Windows platform, are now expanding their operations to create rogues for the Mac platform. The future will tell if the increasing trend of newly developed rogue applications will include the Mac platform. This development will certainly be followed by most anti-spyware/anti-virus vendors.

The analysis of collected data between 2006 and 2009 points to the existence of a pattern in the localization of the hosts of rogue applications. The U.S., Russia and Ukraine – and later Latvia – show the highest concentrations. The concentration increase in the US west coast area is striking. The North American west coast can thus be said to constitute a growing seat in this context. The fact that previous Russian operations may have taken a new impetus in the western U.S. may explain the increase of rogue hosts in that area. Both Estdomains and Intercage have had clear links to Eastern Europe, for example via the notorious ISP EstHost. Clear links between the striking increase of rogue hosts on the North American west coast and the Russian

Business Network are difficult to prove and need to be explored further. However, we suspect that former Russian operations have been relocated, possibly to the US west coast area.

Revisiting Rogues: The Economic Impact and Possible Countermeasures

The other objective of this report was to illuminate the economic impact of rogues on different levels and to discuss possible countermeasures that could counter further dissemination of rogues.

In our daily work as malware analysts at Lavasoft Malware Labs, we are constantly reminded of the impact of rogue applications on the individual level. We receive e-mail messages and read blog posts from users that wonder why Lavasoft's Ad-Aware is detecting their newly purchased anti-spyware/anti-virus application. It is always discouraging to have to announce that what the person believed to be a legitimate anti-spyware/anti-virus application is, in fact, a rogue application that exposed the user to fraud. If the registration of a rogue application cost about \$45 U.S., that amount on its own, is a relatively small amount of money. However, that initial loss may escalate into a much higher amount if credit card details and/or banking details that were intercepted during the online payment session get in the hands of cyber criminals specializing in phishing. Such details may also be sold to others; the danger that a cyber criminal will drain the account of the affected user is imminent. Such stolen information could also be used for identity theft, for the ordering of goods, for blackmailing purposes, etc. Therefore, the registration of a single rogue application may generate negative repercussions for a long period to come.

An analysis of the high level economic impact of rogue applications raises the need to highlight several parameters; otherwise the result would not be fair or credible. In order to produce a fair holistic perspective, elements such as fees paid to the developers of helper Trojans (the rental of botnets, and the cost of other dissemination tools or services has to be taken into account. The fact that half of the profits of North American ISP, InterCage, descended from their cooperation with the notorious Esthost, an Eastern European webhost, also points to the fact that the economic impact of rogue applications spans over several stakeholders. The striking increase in newly developed rogue applications, along with the expansion to the Mac platform, points to the fact that the development of rogues – together with other ancillary activities – is generating significant amounts of money. Exact amounts are hard to produce and estimates would only feed the existing large wave of rumors of an estimated total.

High- Level Countermeasures

The high-level measures for mitigating, or eliminating, the continued spread of rogue applications may include a review of ICANN's accreditation of Domain Name Registrars. The purpose of this would be to strengthen the filtering of deficient applicants. ICANN may also have to take greater responsibility for the control and follow-up of accredited registrars. The Domain Name Registrars could strive towards increasing the transparency of what is hosted on controlled IP ranges; the registration of large blocks of IP addresses should be accompanied by great caution and an increased follow-up. The suspension of Estdomains' rights serves as an example of the fact that ICANN has a possibility of managing their follow-up responsibilities in an efficient manner.

At the same time, it cannot be stressed enough that all forms of control of domain content and domain activities must be done in a balanced way, minimizing the impact on user privacy. The problem with allowing the registration of large blocks of IP addresses, without increased control and follow-up of what is served on the domains, may be exemplified by looking at the situation in China. China moved from having to apply for IPs from one of the five Regional Internet Registries to creating their own "IP Allocation Alliance" in late 2004. China's Internet Network Information Center (CNNIC) is currently the only national distributor of IPs in China that has the possibility to apply for large numbers of IP addresses. Small operators in China may apply for IPs directly from CNNIC without a risk of being rejected by APNIC. The ability to register IPs easily and with less control from former distributors of IPs, is exploited by spammers. The future will tell if this fact will be extensively exploited by the originators of rogue applications as well.

We welcome initiatives where Domain Name Registrars and Internet service providers join forces in order to curb further dissemination of rogue applications and, of course, other types of malicious software. ISPs could also, independently, provide filtering of malicious code to their customers. The possibilities of doing this are further discussed in the whitepaper "ISP Level Malware Filtering - An Extended Clean Feed?"¹² The control and blacklisting of domains/IPs known for hosting malicious content, which is performed by anti-spyware/anti-virus vendors, could be made more streamlined and efficient in order to minimize false positives. The dynamic nature of domains and hosted content, along with the possibility of hosting malicious content on large blocks of IPs, makes efficient blacklisting of malware-hosting domains a harder task. A balanced "self-

¹² Pekka Andelin (Lavasoft), "ISP Level Malware Filtering - An Extended Clean Feed?".

http://www.lavasoft.com/support/spywareeducationcenter/wp_ispmalwarefiltering.php. Retrieved on 2009-01-21.

regulation” performed by Domain Name Registrars and ISPs could prove to be helpful in the filtering of rogue hosting entities. The synergic effect of such cooperative efforts may be significant. Efficient high-level protection is a far more powerful means in the fight against rogue applications than the unilateral reliance on low- or individual-level protective measures.

Consumer Level Countermeasures

The protective measures that could be taken at a lower, individual level include having updated anti-spyware protection installed on consumer systems. Users should also keep their systems – including their browsers – updated with the latest security patches in order to strengthen their protection against the exploitation of security holes that could result in drive-by downloads of rogue applications. Security-conscious Windows users could use Microsoft’s Baseline Security Analyzer, in order to check if their system is patched with the latest security updates.¹³

However, having knowledge about and insight into the strategies used by the perpetrators behind rogue applications is even more important. Keeping the rogues off the system is, of course, far better than having to clean them from the system after an infection. The real-time protection offered by many anti-spyware products, including Lavasoft’s Ad-Aware, can block many rogues. Still, not all rogues can be blocked by this means as new clones are created constantly and the newest ones may not yet have been added to the anti-spyware product’s detection databases. Therefore, the ability to see through the most common fraudulent strategies, along with knowledge of the most common social engineering tactics, is essential for all computer users.

Due to the diversity of threats and the steep learning curve, keeping up with the latest information can be relatively hard and time-consuming for non-computer savvy users. Still, the time invested in information retrieval could prove to be extremely valuable in the end. The responsibility of providing relevant and up-to-date security information is shared by vendors in the anti-spyware/anti-virus industry along with security conscious members of the media. There is still much that could – and should – be improved in order to provide vital and easily comprehensible information to the public, in a fast and efficient manner.

¹³ Microsoft TechNet, "Microsoft Baseline Security Analyzer". <http://technet.microsoft.com/en-us/security/cc184924.aspx>. Retrieved on 2009-03-26.