REPORT: SYMANTEC ENTERPRISE SECURITY

Symantec Report on Rogue Security Software

July 08 – June 09

Published October 2009

Confidence in a connected world.

White Paper: Symantec Enterprise Security

Symantec Report on Rogue Security Software

July 08 – June 09

Contents

Introduction

The *Symantec Report on Rogue Security Software* is an in-depth analysis of rogue security software programs. This includes an overview of how these programs work and how they affect users, including their risk implications, various distribution methods, and innovative attack vectors. It includes a brief discussion of some of the more noteworthy scams, as well as an analysis of the prevalence of rogue security software globally. It also includes a discussion on a number of servers that Symantec observed hosting these misleading applications. Except where otherwise noted, the period of observation for this report was from July 1, 2008, to June 30, 2009.

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network. More than 240,000 sensors in over 200 countries monitor attack activity through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec Managed Security Services and Norton™ consumer products, as well as additional third-party data sources.

Symantec also gathers malicious code intelligence from more than 130 million client, server, and gateway systems that have deployed its antivirus products. Additionally, Symantec's distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks and providing valuable insight into attacker methods.

Spam and phishing data is captured through a variety of sources including the Symantec Probe Network, a system of more than 2.5 million decoy accounts; MessageLabs™ Intelligence, a respected source of data and analysis for messaging security issues, trends and statistics; and other Symantec technologies. Data is collected in more than 86 countries. Over 8 billion email messages and over 1 billion Web requests are processed per day across 16 major data centers. These resources give Symantec's analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam.

NOTE: Symantec advises against visiting the websites of the rogue security applications discussed in this report because these sites may be unsafe and could potentially harm your computer.

Also, rogue security applications are often marketed by different distributors under slightly different spellings. For example, AntiVirus XP 2008 may appear as AntiVirusXP 2008, AntivirusXP 2008, etc. Symantec uses what it considers to be a common variation for this report.

Overview of Rogue Security Software

A rogue security software program is a type of misleading application (also known as scareware) that pretends to be legitimate security software, such as an antivirus scanner or registry cleaner, but which actually provides the user with little or no protection whatsoever and, in some cases, can actually facilitate the installation of malicious code that it purports to protect against. There are two prevalent ways in which rogue security software can be installed on a user's computer: either it is downloaded and installed manually by a user after he or she has been tricked into believing that the software is legitimate; or it is unknowingly installed onto a user's computer, such as when a user visits a malicious website designed to automatically download and install illegitimate applications.

Profit is a primary motivation for creators and distributors of rogue security software scams. A common approach is to try to trick users into believing that these rogue security applications are valid and to get users to download and install the programs and to pay for them. Techniques used to entrap users often rely on fear tactics and other social engineering tricks that are distributed through means such as links in spam, pop-up and banner advertisements on websites and instant messaging programs, postings on forums and social networking sites, and sponsored or falsely promoted search engine results.[1] Attackers also market rogue security software with claims that the programs can remove unwanted applications such as spyware or adware. Not only do these scams cheat users out of money—advertised costs for these products range from $30 to $100 (all currency U.S.) and some even try to sell multi-year licenses—but the personal and credit card information that users provide to register these fake products could also be used in additional fraud.[2]

Once installed on a user's computer—and to induce payment—rogue security applications often deliberately misrepresent the computer's security status or performance, displaying fake or exaggerated claims of security threats even if the computer has not been compromised. These applications use continuous pop-up displays, taskbar notification icons, and other alerts to indicate that the user needs to purchase a full version or register for an annual subscription of the program in order to remove the reported threats and clean the computer (figure 1).[3] Some rogue security applications may even install additional threats onto the compromised computer while simultaneously producing reports that it is clean.

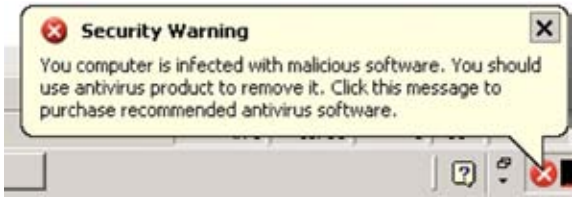

Figure 1. Rogue security software taskbar notification alert

Courtesy: Symantec Corporation

To fool potential victims, rogue security software programs are designed to appear as legitimate as possible. This includes using realistic-sounding names such as VirusRemover2008,[4] AntiVirusGold,[5] or SystemGuard2009,[6] or names that mimic existing legitimate security software, such as "Nortel."[7] Most rogue security programs also have fully developed websites that include the ability to download and purchase the software, with some actually using legitimate online payment services to process credit card transactions from successful scams. Some scams even return an email message to the victim with a receipt for purchase that includes a serial number and a valid, functioning customer service phone number. The advertisements, pop-up windows, and notification icons used to market these scams are also all designed to mimic

legitimate antivirus software programs, often using the same fonts, colors, and layouts as trusted security software vendors (figure 2).

Figure 2. Security warning mimicking a legitimate vendor

Courtesy: Symantec

Rogue security software programs are often rebranded or cloned versions of previously developed programs. Cloning is often done because the original version of the rogue security application has been discovered or detected by legitimate security vendors. Cloning is therefore fuelled by the hope that one or more of the clones will escape detection.[8] This process sometimes involves nothing more than changing out the name, logos, and images of a program in an attempt to give it a new identity while the program itself remains unchanged. One program may be rebranded multiples times.

Another reason for cloning programs is to minimize the impact of credit card chargebacks and payment reversals.[9] Major credit card companies fine issuing banks and credit card payment processors for retaining merchants with high chargebacks.[10] Usually, the payment processing company simply ceases conducting business with such merchants or else passes the cost of the fines onto them. By rebranding the applications and registering using a different name, rogue security software creators and distributors—the merchants in this case—can circumvent these issues. As well, many users might not recognize the rebranded application as false.

Examples of rebranded rogue security software programs include AntiVirus 2009,[11] which is a clone of Antivirus 2008,[12] and AntiVirus XP 2008,[13] which is a clone of Malware Protector 2008 (figure 3).[14] The latter program is also part of a family of rogue security software clones that includes AdvancedXPFixer[15] and WinIFixer.[16]

1-http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf: pp. 31, 35
2-http://www.symantec.com/connect/blogs/misleading-applications-show-me-money
3-Ibid.
4-http://www.symantec.com/security_response/writeup.jsp?docid=2008-072217-2258-99
5-http://www.symantec.com/security_response/writeup.jsp?docid=2006-032415-1558-99
6-http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-031311-4206-99
7-http://www.symantec.com/connect/blogs/nort-what-av (Please note that the spoofed site has no association at all with Nortel Networks™.)
8-http://www.symantec.com/connect/blogs/cloning-profit
9-A credit card chargeback is when the consumer's issuing bank returns the funds back to the consumer, and the payment to the merchant is reversed. This usually occurs when the consumer files a complaint regarding the charge with the issuing bank.
10-http://www.corporate.visa.com/pd/rules/pdf/visa-international-operating-regulations.pdf: Table 1-9
11-http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-082521-2037-99
12-http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-050906-3727-99
13-http://www.symantec.com/security_response/writeup.jsp?docid=2008-071613-4343-99
14-http://www.symantec.com/security_response/writeup.jsp?docid=2008-060420-4214-99
15-http://www.symantec.com/security_response/writeup.jsp?docid=2008-052212-0934-99
16-http://www.symantec.com/security_response/writeup.jsp?docid=2008-030406-0943-99

Figure 3. Malware Protector 2008 and its clone, AntiVirus XP 2008

Courtesy: Symantec

Risks

One major risk associated with installing rogue security software programs is that the user may be given a false sense of security with the belief that the application is genuine and that his or her computer is protected from malicious code threats. This is because rogue security applications frequently report that malicious threats have been removed and that the computer is clean and fully protected when, in reality, the opposite is often true and the misleading application is providing little or no protection from threats at all. These programs may actually increase the danger of the user's computer being compromised. This is because some rogue security software programs instruct the user to lower existing security settings in order to advance the registration process, such as switching off firewall settings and/or disabling existing (and legitimate) antivirus programs (figure 4). Also, once installed, the false application may prevent the computer from accessing legitimate security vendor websites, thus obstructing the user's ability to research how to remove the misleading software.

Figure 4. Registration pop-up display for AntiVirus 2009

Courtesy: Symantec

In other instances, a computer may have already been compromised with malicious code or may be at risk of attack from additional threats. This is because some rogue security applications are designed to install additional threats (even while continuing to report that the compromised computer is clean). For example, some applications will launch pop-up windows that, if any of the options presented are clicked, will download malicious code to the victim's computer.[17] This will occur even if the option chosen is the close window "X" or the negative response option.

Another potential risk involved with rogue security software is that the scam perpetrators will use the personal information gained from the victim to commit fraud and/or identity theft. Thus, not only can these programs cheat the user out of money, but the personal details and credit card information that are provided during the purchase (figure 5) can be used in additional fraud or else sold on black market forums, where credit card data is advertised for as much as $30 per card.[18]

17-http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : pp. 31, 35
18-Underground economy servers are black market forums for the promotion and trade of stolen information and services, such as credit card numbers and bank accounts. See the Symantec Report on the Underground Economy, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

Figure 5. AntiVirus 2009 payment page (with option for "Premium Support" and "upgrade to fileShredder")
Courtesy: Symantec

Some versions of rogue security software include keystroke loggers as well as backdoor functionality, allowing potential access to personal information and other stored information on the user's computer such as stored passwords and other sensitive information. For example, figure 6 shows the administrative interface to the Bakasoftware back-end management system. This administrative tool allows the Bakasoftware administrator to load new and additional software (for example, "cosma bot") on a computer already compromised with rogue security software.

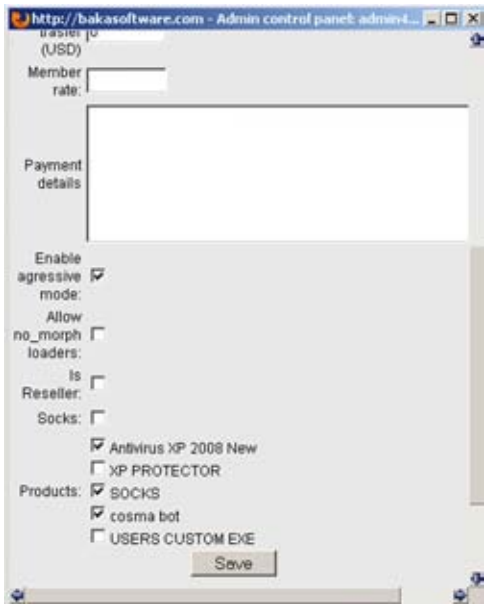

Figure 6. Bakasoftware administrative control panel

Courtesy: Symantec

Just as legitimate security software needs to contact a manufacturer's servers to obtain signature updates and other functions, the rogue security software may also contact the scam perpetrator's servers for updates and added functionality. In this case, though, the update results in the further compromise of the user's computer. In this way, rogue security software could represent a greater risk than expected if it is possible for a computer compromised with rogue security software to be used in a larger bot network that is maintained by structured updates from control servers.

Advertising methods

Attackers use many methods to tempt users into downloading and installing rogue security software programs. Along with employing a number of standard methods similar to legitimate Internet advertising campaigns, scam perpetrators also employ fear tactics and other social engineering techniques to sell their products. This section discusses some of the main advertising methods used to market rogue security software programs.

Spam

Spam is an easy way to advertise rogue security software programs because it is relatively quick and inexpensive to send a large number of email messages, especially if a spammer uses a botnet to do the work. For example, in 2008, spam for AntiVirus XP 2008 was sent out from botnets such as Peacomm,[19] Srizbi,[20] Rustock,[21] and Ozdok[22].[23] Email addresses suitable for spam are inexpensive, costing as little as $0.33/MB (with one MB containing as many as 40,000 email addresses).[24]

Some spam is sent with executable file attachments that, if opened, will install the rogue security software program. Because many security software programs and upstream providers now guard against this with spam filters that flag email containing suspicious attachments, spam distributors instead send email with messages that are worded to lure users into following a link to the associated website for the fraudulent program.

19-http://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99

Advertisements on websites

Rogue security software programs are advertised on a variety of both malicious and legitimate websites, including blogs, forums, social networking sites, and adult sites.[25] These advertisements typically prey on users' fears of malicious code, with claims such as, "If this ad is flashing, your computer may be at risk or infected," and will urge users to follow a link that will provide the software to remove the threats.

Link spamming packages (also known as auto-submitters) are also often used to place links pointing to rogue security application websites. One example is the Xrumer software package. Xrumer can bypass CATCHA protections, automatically register and confirm email activation requests, and is capable of quickly spamming large numbers of websites.[26] By using such tools, scam distributors can increase their search engine rankings and place links on thousands of websites to drive victims to a rogue security application website.

To increase exposure and add an air of legitimacy, scam distributors also place Web banner advertisements on major Internet advertising networks and with advertising brokers of legitimate sites.[27] This is possible because administrators of legitimate websites often link to feed services that control the dispersal of these advertisements and the administrators usually have no control what content is displayed in the advertisements.[28] Moreover, the feed service distributors may not be able to control content either, because they are often a middle ground between feed subscribers and the actual advertisers. If an advertiser pays the distributor to display advertisements, the distributor may have very little control over the data displayed in the advertisements. This makes mitigating deceptive or malicious advertisements very difficult. Tracking down the original source of the malicious or deceptive content can also be very challenging.

Search engine results seeding

Another method of advertising rogue security software programs is to seed search engine results by capitalizing on popular news items, events, or celebrities.[29] Scam creators use a range of black hat search engine optimization (SEO) techniques to effectively poison search engine results and increase the ranking of their scam sites whenever any topical news event is searched.[30] For example, the Downadup[31] worm (also known as Conficker) emerged and spread rapidly in the latter months of 2008, with well over a million individual computers affected by the end of that year.[32] To play on consumers' fears of the worm, scam perpetrators created website pages full of terms such as "remove virus" or "free anti-virus," etc. This increased the keyword count of the pages, thus making them seem more relevant to search engine relevancy algorithms.[33]

Browser helper objects

Another method recently observed by Symantec for advertising rogue security applications was used in the promotion of AntiVirus 2009, one of the most widely reported of these programs during this reporting period.[34] In this approach, once AntiVirus 2009 is installed on a computer, it creates a browser helper object (BHO) that modifies all pages from a search engine by adding a fake "security tip" that appears to originate from the search engine company, complete with legitimate logos (figure 7).[35] In reality, this tip service is non-existent. The purpose of the tip on the Web page is to entice the user of the compromised computer to click on the link to "activate" Antivirus 2009.

20-http://www.symantec.com/security_response/writeup.jsp?docid=2007-062007-0946-99
21-http://www.symantec.com/security_response/writeup.jsp?docid=2006-011309-5412-99
22-http://www.symantec.com/security_response/writeup.jsp?docid=2008-021215-0628-99
23-http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 31
24-http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 82

Figure 7. Fake tip page

Courtesy: Symantec

Installation techniques

Rogue security software programs can get onto a user's computer either by being manually installed by the user, who has been fooled into thinking that he or she is downloading a legitimate program; or it is unknowingly downloaded and installed by the user without his or her consent or knowledge. This section will discuss delivery methods and strategies used by scam distributors. (For best practices to safeguard against these threats, please see Appendix A of this report.)

Emailed executable files

One of the simplest ways to distribute rogue security software programs is through executable files attached to spam. The malicious attachments are typically disguised as executable files with false file extensions, such as music, media, or compressed (that is, .zip) files. If opened, these attachments will instead either install a rogue security software program directly, or else will load malicious code onto the computer that subsequently installs the rogue software. As mentioned, many security software programs and ISPs now have extensive safeguards to protect against potentially malicious attachments.

Malicious code

Rogue security software programs can be installed onto a user's computer by malicious code such as staged downloaders. Staged downloaders are threats that, once on a computer, will download and install other malicious code. This is typically done without the user's knowledge or consent. One of the more popular methods of getting malicious code onto a victim's computer is through drive-by download attacks. Drive-by downloads occur when a user visits a malicious website or a legitimate website that has been compromised and malicious code is downloaded onto the user's computer without the user's interaction or authorization. The attacks attempt to gain access to a user's system by exploiting vulnerabilities in browsers, browser plug-ins and applications, or desktop applications. The download is typically an executable file containing malicious code that then attempts to download additional threats, such as rogue security software programs. Because the user is usually oblivious to these occurrences, such attacks can be difficult to mitigate. Drive-by downloads

25-http://www.symantec.com/norton/theme.jsp?themeid=mislead
26-http://blog.washingtonpost.com/securityfix/2007/01/scary_blogspam_automation_tool_1.html
27-An advertising network is a distributor of advertisements to websites that want to host them; they typically have a large inventory of advertisements that get displayed each time a Web page is loaded or refreshed; the website often will not have control over the content of these advertisements.
28-See http://www.eweek.com/c/a/Security/DoubleClick-Serves-Up-Vast-Malware-Blitz/ and http://www.theregister.co.uk/2008/02/21/itv_scareware_peril/
29-http://www.symantec.com/connect/blogs/misleading-applications-show-me-money-part-2
30-SEO is a process for making websites more popular in search engine results; black hat SEO uses search optimization techniques that are considered unethical by the mainstream SEO community, which may include spamming and other questionable practices.
31-http://www.symantec.com/security_response/writeup.jsp?docid=2009-040823-4919-99
32-http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed2.pdf
33-http://www.symantec.com/connect/blogs/downadup-related-search-indexes-poisoned-fake-av-sites
34-http://www.symantec.com/security_response/writeup.jsp?docid=2008-082521-2037-99
35-http://www.symantec.com/connect/blogs/misleading-applications-start-tipping

are becoming an increasingly dominant vector of attack, as discussed in Volume 14 of the *Symantec Internet Security Threat Report,* especially since such attacks can be launched from both legitimate and malicious websites.[36]

A specific example of malicious code associated with rogue security software is the Zlob Trojan.[37]First identified in 2005, Zlob was the third most common staged downloader component observed by Symantec in 2008.[38] One of its primary attack vectors to get onto a user's computer is disguised as a video codec installer. A video codec is a type of software that supports the compression (or decompression) of digital video. Because additional codecs are often required to play a specific video format, depending on how the video in question was created, users may be more likely to trust such prompts and download the files. This type of Web-based attack follows a trend of attackers inserting malicious code into legitimate high-traffic websites where users are likely to be more trusting of the content, rather than attempting to lure users to visit specifically designed, malicious sites.[39]

Once embedded onto a compromised computer, one particular function of Zlob is to display fake security alerts and pop-ups claiming that the computer is infected with spyware. If a user clicks on the alert, Zlob will redirect the user's Web browser to a website containing malicious code, at which point the computer will be attacked further. The top three reported rogue security applications observed by Symantec during this reporting period (discussed below in "Top reported rogue security software") were all distributed in part by Zlob, as were a number of others, including PrivacyCenter,[40] Malware Defender 2009,[41] VirusProtectPro,[42] and IE Defender.[43]

IE Defender is worth noting further because, once installed on a computer, the program performs a scan that automatically detects the presence of malicious code, including Zlob. Thus, IE Defender prompts the user to pay for a full license of itself in order to remove Zlob, which is responsible for IE Defender being installed on the user's computer in the first place.

Another example of malicious code associated with rogue security software is the Vundo Trojan, which is a component of an adware program that exploits a browser vulnerability.[44] Vundo was the top-ranked malicious code sample observed by Symantec globally in both 2007 and 2008.[45] It typically infects computers through links to malicious websites from spam or email attachments that, in reality, also contain the malicious code. The compromise may also occur via a drive-by download, as described above.[46] As a staged downloader, once Vundo is installed on a computer, it attempts to contact certain IP addresses to download additional components, including the adware downloader component of the Trojan that, once executed, is used to display pop-up advertisements.

Rogue security software website downloads

Websites created to market rogue security software programs are designed to look as legitimate as possible so that users will be convinced that the products are authentic and will download them. As such, they often include the logos and formatting typical of the websites of legitimate security vendors, testimonials from satisfied customers, and other seemingly genuine techniques. One rogue security application site, for Green Antivirus 2009,[47] even claims to be the "world's first antivirus that cares about the environment," pledging that "$2 from every sale will be sent on saving green forests in Amazonia" [*sic*].[48] To trick users into downloading their products, some rogue security websites offer free trials or free system scans. In fact, MessageLabs Intelligence observed that, of the most frequent rogue security applications blocked through MessageLabs Web Security Service (WSS), 95 percent contained the generic "freescan.php" filename.

36-http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 52
37-http://www.symantec.com/security_response/writeup.jsp?docid=2005-042316-2917-99

Many rogue security software websites are associated with more than one domain name so that, if one server is taken offline to evade detection by authorities or shutdown by upstream ISPs, redundancies exist to keep the scam running. In Symantec's research on servers hosting rogue security software, discussed further below in this report, over 194,000 domain names were observed associated with these false applications over a two-month period.

Rogue security software distributors

The creators of rogue security software often use an affiliate-based, pay-per-install model to distribute their misleading applications. Users who wish to participate in a rogue security software scam can register as an affiliate on a distribution site, such as TrafficConverter.biz, where they can obtain the appropriate files and links to market the scam.[49] Typically, these websites offer free registration and the affiliates then carry out all of the marketing for the product. The main purpose of these distribution websites is to recruit affiliates to sell the rogue security software programs.

The creators of the distribution websites provide affiliates with the support and the tools required to distribute and market the scams, such as fake codec links, fake scanner links, and malicious code executable files. They may also provide affiliates with promotional and marketing materials, as well as obfuscation tools such as packers and binders (used to create versions of the code in order to evade detection by legitimate security software).

Another evasive maneuver is the use of polymorphic techniques. Polymorphic obfuscation modifies program code, as often as every five minutes, to alter the digital signatures of the code while keeping the underlying functionality intact. This makes polymorphic threats difficult to detect since they are constantly changing. These services and tools are usually provided to the scam distributors for free or for a nominal fee.

Affiliates are paid a predetermined amount for every successful installation, ranging from $0.01 to $0.55.[50] This per-installation payment is dependent on the type of installation and the distribution site, with malicious code installations returning the highest commission. The price is also dependent on the country of the computer on which the rogue security software program has been installed. For example, one distribution site paid $0.55 per installation on computers in the United States, but only $0.05 per installation on computers in Mexico (table 1).[51] The site also gave installation incentives to affiliates through additional bonuses, such as a 10 percent bonus for more than 500 installations per day and a 20 percent bonus for over 2,500 installations per day. The per-installation price variations from country to country may depend on the likelihood of a user in that country paying for either a subscription to, or a fully registered version of the rogue security software. Basically, the higher the percentage of users in a certain country that pays, the higher the per-installation payment.

38-http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 62
39-Ibid: p. 31
40-http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-050702-2910-99
41-http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-033012-2224-99
42-http://www.symantec.com/business/security_response/writeup.jsp?docid=2007-070323-1203-99
43-http://www.symantec.com/security_response/writeup.jsp?docid=2007-111420-0754-99
44-http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99
45-http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 60
46-http://www.securityfocus.com/bid/11515
47-http://safeweb.norton.com/report/show?name=green-av-pro.com
48-http://www.411-spyware.com/tag/green-anti-virus-2009
49-http://voices.washingtonpost.com/securityfix/2009/03/obscene_profits_fuel_rogue_ant.html
50-http://www.symantec.com/connect/blogs/misleading-applications-show-me-money-part-3
51-Ibid.

Country	Region	Per-installation Price
United States	NAM	$0.55
United Kingdom	EMEA	$0.52
Canada	NAM	$0.52
Australia	APJ	$0.50
Spain	EMEA	$0.16
Ireland	EMEA	$0.16
France	EMEA	$0.16
Italy	EMEA	$0.16
Germany	EMEA	$0.12
Belgium	EMEA	$0.12
Netherlands	EMEA	$0.12
Denmark	EMEA	$0.10
Norway	EMEA	$0.05
Mexico	LAM	$0.05
Other countries	N/A	$0.01

Table 1. Examples of per-installation prices for rogue security software, by country[52]

Source: Symantec

In the case of TrafficConverter.biz, the website was associated with the Downadup worm as a URL from which Downadup attempted to download its payload.[53] The site was shut down in November 2008 before the worm could download the unknown payload. TrafficConverter.biz and other reincarnations of the website paid affiliates $30 per sale of their rogue security software programs, such as XP Antivirus.[54] The site purported to have at least 500 active affiliates, with top affiliates earning as much as $332,000 in a month for installing and selling security risks—including rogue security software programs—onto users' computers.[55] The top 10 earning affiliates purportedly each earned $23,000 per week, on average. The website even kept statistics on their top sellers, including listing percentages on the conversion of installations-to-sales per day (figure 8). In addition, the website offered "VIP-points" contests to top-selling affiliates, complete with prizes such as electronics and a luxury car (figure 9).

The successful webmaster:

Date	Antispyware							Refs	Total
	U	I	U/I	I/S	U/S	S	Earn		
15.01.2008	36109	3794	10	53	502	72	$2304.00	$0.00	$2304.00
16.01.2008	34634	3972	9	46	398	87	$2784.00	$0.00	$2784.00
17.01.2008	47484	5543	9	55	475	100	$3200.00	$0.00	$3200.00
18.01.2008	54756	5748	10	55	527	104	$3328.00	$0.00	$3328.00
19.01.2008	70018	6630	11	55	583	120	$3840.00	$0.00	$3840.00
20.01.2008	71238	6744	11	77	810	88	$2816.00	$0.00	$2816.00
21.01.2008	77558	6562	12	49	575	135	$4320.00	$0.00	$4320.00
Total:	391797	38993	10	55	555	706	$22592.00	$0.00	$22592.00

Uniques - U
Sales - S
Installs - I

Figure 8. TrafficConverter.biz sample earnings per day

Courtesy: Symantec

52-NAM = North America, EMEA = Europe, the Middle East, and Africa, APJ = Asia-Pacific/Japan, LAM = Latin America
53-http://www.symantec.com/connect/blogs/downadup-motivations
54-http://www.symantec.com/security_response/writeup.jsp?docid=2007-101010-0713-99

Figure 9. TrafficConverter.biz website with contest announcement

Courtesy: Symantec

Dogma Software was yet another rogue affiliate program that offered incentives to install their scareware on victim computers. The Dogma affiliate program claims to be "cleaning software" and offers up to $30 per installation (figure 10).

55-http://voices.washingtonpost.com/securityfix/2009/03/obscene_profits_fuel_rogue_ant.html

Figure 10. Dogma Software website

Courtesy: Symantec

These affiliate "master sites" such as Bakasoftware, TrafficConverter and Dogma Software seem to be the drivers for the associated domain names, websites, and malicious advertising behind many rogue security software scams. Without the affiliate commission payouts and back-end billing systems in place, there would likely be fewer scams perpetuated. Many in the security community have realized this and have refocused their efforts on identifying and shutting down the scam creators instead of trying to track down and identify the myriad domain names used to offer rogue security software.

Legal actions and noteworthy scam convictions

Attackers who create and distribute rogue security software programs can make a significant amount of money through these scams. They can also use the credit card information obtained from the victims to commit further fraud or to sell the data on black market forums.[56] This section will discuss several notable scams and the actions that government organizations have taken to combat perpetrators of rogue software security scams.

Legal actions taken against this type of scam include charges of fraud, deceptive advertising, misrepresentation, and in some cases, spam distribution (in cases where the software itself may not be illegal). For example, in 2006, the Attorney General for Washington State obtained a $1 million settlement from a New York-based company through a combination of

56-http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 83

the state's 2005 Computer Spyware Act, federal and state spam laws, and the U.S. Consumer Protection Act.[57] The company fined was distributing the rogue security software program, Spyware Cleaner.[58] The state sued the company for marketing software that falsely made claims of threats on users' computers.

The Attorney General for Washington State has also filed lawsuits against a Texas-based company and its owner for misrepresentation of Registry Cleaner XP.[59] The lawsuit has asked for restitution for the victims of the scam, fines for the defendants, and recovery for damages for each violation.[60]

Under the Washington State Computer Spyware Act it is illegal to persuade a user to download software under the guise that it is necessary for the safe operation of his or her computer. In addition to requesting that the rogue security software creators and distributors cease all operations, the state also asks for monetary compensation to be provided for all victims of these scams.

In another case, in 2008 the head of a South Korean-based computer security company was charged with fraud by the Seoul Metropolitan Police Agency for the distribution of the rogue security software program Doctor Virus to over four million users.[61] The company is alleged to have made over $9.8 million over the course of three years in the scam.

In June 2009, a U.S.-based defendant and his company were required to pay more than $1.9 million to settle fraud charges with the Federal Trade Commission stemming from a rogue security software scam.[62] The defendants used deceptive advertising to mislead more than 1 million people into purchasing their rogue security applications, including such titles as WinFixer,[63] WinAntivirus, DriveCleaner,[64] XP Antivirus 2008 and ErrorSafe.[65]

The defendants placed advertisements for their rogue security software program on popular legitimate websites and on a major Internet advertising network and with brokers.[66] After receiving complaints that the banner ads contained code that would automatically install malicious software, the advertising network stopped placing advertisements for all security products. To bypass this, the operators created advertisements for legitimate companies, including a charity, and these advertisements were displayed for an IP address range associated with the advertising network company. For all other IP addresses outside of the range, it displayed the advertisement for the rogue security software program that contained code that automatically performed fake scans on the users' computers. The scan would report threats of spyware and illegal pornography, and then urge users to download and install the rogue security software program so that it could perform a more detailed scan. This second scan would also report that the computer was infected by the same threats as the first scan. Users were then directed to purchase a full copy for $39.95 to "fix" these false threats. In reality, no computer scans were conducted at any point and the threats that they detected were false and non-existent.

The settlement amount of $1.9 million represented the total gross revenue that the company realized from the scam. Moreover, the court order prohibited the defendants from engaging in deceptive advertising tactics and installing programs on consumers' computers.

In addition to government actions, some companies have also been effective in taking actions against rogue security software distributors and hosts. In August 2009, a Latvian ISP associated with rogue security software programs and the hosting of malicious activities (such as websites responsible for Web-based attacks and phishing sites) was taken offline after being disconnected by its upstream provider.[67] The ISP allowed customers to remain online even after they were

57-http://www.atg.wa.gov/pressrelease.aspx?&id=5926
58-http://www.symantec.com/security_response/writeup.jsp?docid=2006-041017-1914-99
59-http://news.bbc.co.uk/2/hi/technology/7645420.stm
60-http://www.pcworld.com/businesscenter/article/151640/washington_state_pursues_scareware_distributors.html

linked to malicious activities. As such, following complaints from Internet security researchers, the main provider informed the upstream provider to cease operations with the ISP or face sanctions.

61-http://www.theregister.co.uk/2008/03/04/south_korea_scareware_fraud_charges/
62-http://www.ftc.gov/opa/2009/06/winsoftware.shtm
63-http://www.symantec.com/business/security_response/writeup.jsp?docid=2005-120121-2151-99
64-http://www.symantec.com/business/security_response/writeup.jsp?docid=2006-062217-0726-99
65-http://www.symantec.com/business/security_response/writeup.jsp?docid=2006-012017-0346-99
66-http://www.ftc.gov/os/caselist/0723137/081202innovativemrktgcmplt.pdf
67-http://www.messagelabs.co.uk/download.get?filename=MLIReport_2009.08_Aug_FINAL.pdf

Prevalence of Rogue Security Software

To date, Symantec has detected over 250 distinct rogue security software programs. The following discussions are based on the top reported rogue security software programs that Symantec observed between July 1, 2008, and June 30, 2009. Of the top 50 most reported rogue security software programs that have been analyzed for this report, 38 of the programs were detected prior to July 1, 2008. The continued prevalence of these programs emphasizes the ongoing threat they pose to potential victims despite efforts to shut them down and raise public awareness. Each consumer report is considered to be an attempted and potentially successful scam. For example, during the period of this report, Symantec received reports of 43 million rogue security software installation attempts from the 250+ distinct samples. The results have been analyzed to provide insight into how certain aspects of the programs, such as advertising methods and regional distribution, may contribute to their prevalence.[67]

Top reported rogue security software

This section will discuss the top five of the most reported rogue security software programs observed by Symantec during this reporting period (table 2). The intention is to provide insight into methods of distribution of rogue security software for prevalence, examine related applications, discuss incidents related to the applications, and to highlight malicious activity originating from sites hosting the rogue security applications.

Rank	Name
1	Spyware Guard 2008
2	AntiVirus 2008
3	AntiVirus 2009
4	Spyware Secure
5	XPAntivirus
6	WinFixer
7	SafeStrip
8	Error Repair
9	Internet Antivirus
10	DriveCleaner

Table 2. Top reported rogue security software

Source: Symantec

Spyware Guard 2008

Spyware Guard 2008[68] was the most prevalent rogue security application that Symantec observed during this reporting period. First detected in October 2008, Spyware Guard 2008 uses deceptive Web advertisements that inform users that they have supposedly been exposed to malicious code threats. The advertisements advise users to "turn on protection," which will instead download and install the program if chosen. The downloaded program presents itself as a trial version that scans for and reports various threats (figure 11). After reporting false or exaggerated scan results, the software then asks the user to register and pay for a software license, purportedly enabling the removal of the reported threats. The website for Spyware Guard 2008 offers three different licenses, with costs marked at $49.95, $69.95, and $89.95.

Another distribution technique used by Spyware Guard 2008 is to inject links in innocuous search results for domains that redirect to websites for the rogue application.[69]

Figure 11. Spyware Guard 2008 fake scan results screen

Courtesy: Symantec

Spyware Guard 2008 was created by Pandora Software,[70] which has been identified as being responsible for a number of other rogue security applications, such as AntiVirus XP 2008, EasySpywareCleaner,[71] InfeStop,[72] Malware Protector 2008, SpyRid,[73] and WinIFixer. Pandora Software is believed to be associated with Bakasoftware, an affiliate network based in Russia.[74]Bakasoftware provides various services for its affiliates, including a range of installation methods to aid in scam distributions such as ActiveX controls, fake codecs, and fake online scanners. A list of earnings for Bakasoftware affiliates was published for a one-week period and the top earners purportedly made between $58,000 and $158,000.[75] Pandora is also reputed to act as a payment processor for purchases of misleading applications.[76]

Symantec also observed some unusual behavior on the part of Spyware Guard 2008 in that it was directing users to purchase legitimate software titles (figure 12).[77] This is also a scam, however, because the Web-based storefront is fraudulent and the software, if purchased, is never shipped to the victim. Symantec speculates that this may have been an attempt to gather credit card information. An additional possibility is that the scammers intended to sell pirated software, or did so for a short period, but subsequently stopped shipping the goods.

68-http://www.symantec.com/security_response/writeup.jsp?docid=2008-100114-4845-99
69-http://community.ca.com/blogs/securityadvisor/archive/2009/01/09/unabated-fraud-spyware-guard-2008.aspx
70-Note: The Pandora Software company mentioned in this report is solely affiliated with the distribution, publishing, and/or payment processing of misleading applications such rogue security software and is in no away affiliated with similarly named companies.
71-http://www.symantec.com/security_response/writeup.jsp?docid=2008-022916-2526-99
72-http://www.symantec.com/security_response/writeup.jsp?docid=2008-022916-3210-99
73-http://www.symantec.com/security_response/writeup.jsp?docid=2008-012117-0229-99
74-http://www.secureworks.com/research/threats/rogue-antivirus-part-2/
75-http://www.nytimes.com/2008/10/30/technology/internet/30virus.html?_r=1
76-http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html
77-http://www.symantec.com/connect/blogs/misleading-applications-supposedly-reselling-popular-software-titles

Figure 12. Spyware Guard 2008 advertising legitimate software

Courtesy: Symantec

Spyware Guard 2008 is not hosted on as many domains as has been observed with other samples (Symantec has observed four domains hosting Spyware Guard 2008 executables); however, other distribution methods have been noted. In particular, it was distributed by the Downadup.E worm (a variant of the original Downadup.C).[78] Additionally, Downadup.E was also observed to be distributing variants of Spyware Guard 2008.[79]

AntiVirus 2008 and AntiVirus 2009

AntiVirus 2008[80] was the second most reported rogue security application observed by Symantec during this reporting period, while AntiVirus 2009 was the third most reported. Because they are nearly identical variants from the same source, they will be addressed together here and referred to as AntiVirus 200X for the sake of discussion.

Antivirus 200X is designed to get installed on target computers a number of ways, including intentional downloads, misleading Web advertisements, drive-by downloads, and installation through malicious code. Once installed on a user's computer, AntiVirus 200X then performs a pseudo-scan of the system and falsely reports the discovery of numerous security threats (figure 13). The reported threats range from adware applications and spyware, to Trojans and viruses. AntiVirus 200X even reports the detection of rogue security software.

78-http://blogs.zdnet.com/hardware/?p=4131
79-Ibid.
80-http://www.symantec.com/security_response/writeup.jsp?docid=2008-050906-3727-99

Figure 13. Antivirus 2009 scan result page

Courtesy: Symantec

Upon completion of the mock scan, the user is presented with options to deal with these threats, including to "Remove all threats now" or to "Continue unprotected." Selecting the threat removal option will result in the user being presented with a prompt to purchase and to enter a registration key to fully activate and unlock the threat removal features; choosing not to pay will result in AntiVirus 200X continually bombarding the computer desktop with alarmist messages (figure 14).

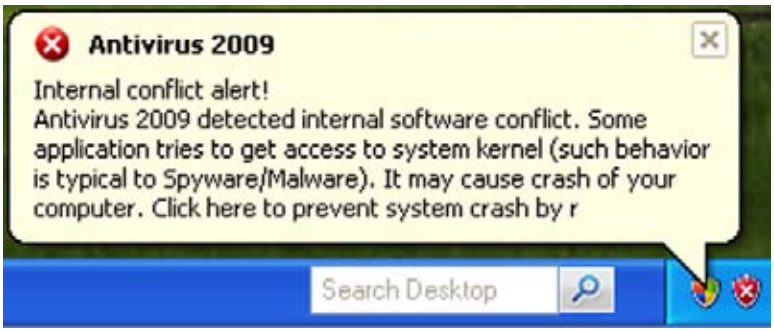

Figure 14. AntiVirus 2009 taskbar alert

Courtesy: Symantec

Furthermore, AntiVirus 200X incorporates a window that closely mimics the legitimate Microsoft®Windows® Security Center service (figure 15). When the software is unregistered, the false security center lists virus protection as "not found," even if there actually is a legitimate security application enabled, and explains that AntiVirus 200X is not fully enabled. It also presents a link for the user to click in order to purchase a license.

Figure 15. AntiVirus 200X Security Center (left) vs. Microsoft Windows Security Center (right)

Courtesy: Symantec

In addition to the described methods used by AntiVirus 200X to appear legitimate, the application will prompt unregistered users that a new database of threat signatures should be downloaded to update the software (figure 16). Choosing to update the program presents the previously described registration window.

Figure 16. AntiVirus 2009 software update alert

Courtesy: Symantec

AntiVirus 2008 was identified in May 2008, while Antivirus 2009 was detected just two months later, in July. Efforts by legitimate security firms to raise awareness and reduce the number of potential victims of the original program may have been cause for the scam authors to release a rebranded version. The rebranding may also have been an attempt to seem as though an upgraded version was available. This may suggest that the scam authors actively monitor the success of their scams and modify them accordingly. This level of involvement may be a contributing factor in the relative success of the scams as well.

Symantec has observed 218 unique domains hosting AntiVirus 2008 executables. Sites hosting AntiVirus 2008 were also observed to be hosting these other threats and rogue applications:

- AntiVirus 2009
- Bloodhound.Exploit.196[81]
- Downloader.Psyme[82]
- InternetAntivirus[83]
- SecureExpertCleaner[84]
- Trojan.Fakeavalert
- WinFixer[85]

A number of the threats detected on sites hosting AntiVirus 2008 are noteworthy because of their involvement in malicious activity. Bloodhound.Exploit.196 is a Symantec heuristic signature that detects exploits for a series of vulnerabilities in Adobe® Acrobat® and Adobe Reader®. The first series of vulnerabilities was discovered in February, 2008.[86] The second series of vulnerabilities was discovered in May, 2009.[87] (Both series have since been patched.) Downloader.Psyme is a downloader that attempts to transfer various malicious executables to the affected computer. InternetAntivirus, SecureExpertCleaner, and WinReanimator are other rogue security applications. The sites hosting AntiVirus 200X have also been observed to be distributing other forms of malicious code. Thus, in addition to the risk posed by the rogue security applications, visitors to these sites could be exposed to exploitation by client-side vulnerabilities or be the target of drive-by downloads.

One of the threats identified on sites hosting AntiVirus 2008 is the Trojan Fakeavalert.[88]FakeAvalert was discovered in October, 2007. Once on a victim's computer, it produces prompts with false alerts about the security status of the compromised computer and prompts the user to run a full scan. If the user authorizes the scan, Fakeavalert launches the user's browser and directs it to a site that tells the user that his or her computer is "infected," along with containing a "Fix now" button that, if clicked, will prompt a download of the rogue security software program, AVSystemCare.[89]

Some characteristics of AVSystemCare that make it appear legitimate are worth noting. This includes the presence of an installation wizard and an End-User License Agreement (EULA), to which the user actually must agree to in order to proceed with the installation. Symantec has observed over 100 clones of this program, with names such as Antispywaresuite, Antiworm2008, and so on. In addition to disabling access to websites of legitimate security vendors, AVSystemCare also disables access to adware sites, which may be an attempt by it to obstruct access to its competitors.

Symantec has observed 179 unique domains hosting AntiVirus 2009 executables. Sites hosting AntiVirus 2009 have also been observed to host the following threats and rogue applications:

- AntiVirus 2008
- Bloodhound.Exploit.196
- Bloodhound.Exploit.213[90]
- IEDefender
- Trojan.Blusod[91]
- Trojan.Fakeavalert
- Trojan.Virantix[92]
- Trojan.Virantix.C[93]

81-http://www.symantec.com/security_response/writeup.jsp?docid=2008-080702-2357-99

In many cases, other misleading applications and threats may be hosted together. This may indicate that the website has been used to launch various attacks and scams. In some cases, malicious software and exploits are hosted on the same website for the purpose of distributing scams. Some of the threats and rogue applications that have been hosted on the same sites as AntiVirus 2009 are worth noting further: Bloodhound.Exploit.213 is a Symantec heuristic signature that detects exploits for a vulnerability in Adobe Acrobat;[94] Trojan.Blusod displays a "blue screen of death" screensaver and false warnings about security threats on the computer and also attempts to download a variant of Zlob from malicious sites; the Trojans Virantix and Virantix.C display false security warnings and also attempt to download additional software to affected computers; Virantix.C also attempts to install the WinReanimator rogue security application on computers.

Spyware Secure

Spyware Secure[95] was the fourth most prevalent rogue security application that Symantec observed during this reporting period. Spyware Secure has been distributed mainly through a single domain that hosts installation executables. Symantec first discovered Spyware Secure in September, 2007. The length of time that the scam has been distributed, in addition to the fact that the main site hosting the executables is still operational, may be contributing factors to the prevalence of this sample.

Spyware Secure is a good example of a scam that tries to socially engineer users into downloading a rogue security application by convincing them that their computers are not protected from, as the ad reads, "spywares" (figure 17). The interface cites statistics from a legitimate security software company in an attempt to scare users into installing the program. It also list common occurrences that many computer or Internet users are likely to encounter such as occasional crashes, slow navigation, and unwanted pop-ups.

Figure 17. SpywareSecure registration screen

Courtesy: Symantec

82-http://www.symantec.com/security_response/writeup.jsp?docid=2004-040112-5204-99
83-http://www.symantec.com/security_response/writeup.jsp?docid=2008-081212-1113-99
84-http://www.symantec.com/security_response/writeup.jsp?docid=2008-072807-2626-99
85-http://www.symantec.com/security_response/writeup.jsp?docid=2005-120121-2151-99
86-http://www.securityfocus.com/bid/27641
87-http://www.securityfocus.com/bid/34169
88-http://www.symantec.com/security_response/writeup.jsp?docid=2007-101013-3606-99
89-http://www.symantec.com/security_response/writeup.jsp?docid=2007-061509-3222-99
90-http://www.symantec.com/security_response/writeup.jsp?docid=2008-110718-2219-99
91-http://www.symantec.com/security_response/writeup.jsp?docid=2008-062711-5534-99
92-http://www.symantec.com/security_response/writeup.jsp?docid=2007-073011-3204-99
93-http://www.symantec.com/security_response/writeup.jsp?docid=2008-050916-1055-99
94-http://www.securityfocus.com/bid/30035
95-http://www.symantec.com/security_response/writeup.jsp?docid=2007-091719-0351-99

Once a rogue application becomes prevalent, there is also a risk that scam distributors may capitalize on its popularity to advertise other scams that purport to remove the now widespread application. For example, searches for Spyware Secure return a sponsored link that advertises applications that claim to remove the threat (figure 18).

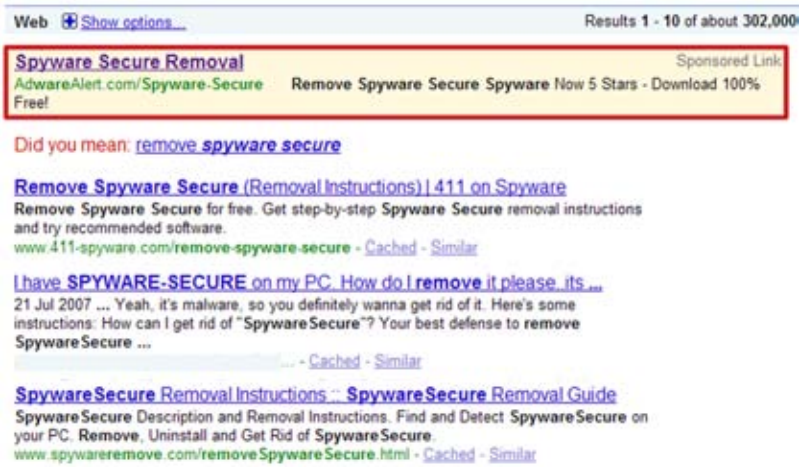

Figure 18. SpywareSecure search results

Courtesy: Symantec

Similar cases have been reported where scam distributors have advertised software that purports to remove rogue security software offered by competitors.[96] Some scams even purport to remove rebranded versions of the same program.[97] This demonstrates competition between scam authors and that they may not be concerned with creating the illusion of a trustworthy brand identity, but instead are attempting to capitalize on the confusion resulting from the distribution of multiple rogue products with similar names and interfaces.

As individual rogue applications are deemed untrustworthy, new versions are often cloned by the same developers and distributed with the promise of removing the old versions. By disassociating themselves from other rogue applications, the scam authors can create confusion and make it difficult to discern which security software programs are authentic. Furthermore, cautious users may be led to distrust advertisements for security applications in general due to the prevalence of false and malicious advertising. This could adversely affect the ability of new, legitimate security software products to establish a trustworthy brand in the marketplace.

XP Antivirus

XP AntiVirus was the fifth most observed rogue security application by Symantec during this reporting period. XP AntiVirus was, at one point, distributed by the Russian Business Network (RBN),[98] and was also one of the rogue security applications targeted by the FTC complaint against Innovative Marketing, Inc. and ByteHosting Internet Services, LLC.[99] These companies were also responsible for distributing other rogue applications including WinAntivirus, DriveCleaner, ErrorSafe, and WinFixer. WinFixer and ErrorSafe are noteworthy because of an incident where they were distributed through banner advertisements in Windows Live™ Messenger.[100]

96-http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html
97-http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html
98-http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html
99-http://ftc.gov/opa/2008/12/winsoftware.shtm
100-http://msmvps.com/blogs/spywaresucks/archive/2007/02/18/591493.aspx

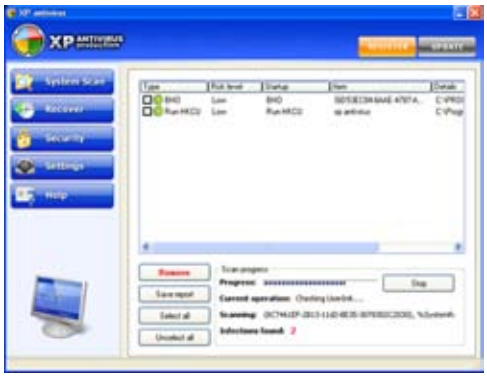

Figure 19. XP AntiVirus interface

Courtesy: Symantec

XP AntiVirus was observed by Symantec to be hosted on 73 unique domains. Sites hosting XP Antivirus have also been observed to host the following threats and rogue applications:

- AntiVirus 2008
- AntiVirus XP 2008
- Trojan.Fakeavalert
- Trojan.Galapoper.A[101]
- Trojan.Zlob

A few of the rogue applications and threats listed above are worthy of discussion. AntiVirus XP 2008 was implicated in an incident where search engine advertisements were poisoned with a number of client-side exploits to install AntiVirus XP 2008.[102] Trojan.Zlob was also found on sites that were hosting XP AntiVirus.

Many of the samples discussed here are hosted on sites that website reputation services have flagged as having a reputation for malicious activity.[103] While this malicious activity is not necessarily directly associated with rogue security applications, it is likely that scam distributors are reusing these domains for various rogue software and malicious code distribution operations. This may be to extract the maximum value from the domains under their control. Exploits targeting client-side vulnerabilities are also present on some sites, which aid in drive-by downloads of malicious software and rogue security applications. In particular, browser plug-in vulnerabilities are often exploited in such attacks. These vulnerabilities are a potent means of distributing rogue security software due to the large number of users affected. Symantec discusses the prevalence of browser plug-in vulnerabilities in Volume 14 of the *Symantec Internet Security Threat Report*.[104]

Additional noteworthy rogue security software samples

As well as the discussion above on the most widely reported rogue security samples observed by Symantec, there are two other examples worth additional mention that Symantec observed during this reporting period.

101-http://www.symantec.com/security_response/writeup.jsp?docid=2006-042013-1813-99
102-http://sunbeltblog.blogspot.com/2008/08/xp-antivirus-2008-now-with-sploits.html
103-http://safeweb.norton.com/
104-http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 40

FileFix Professional

FileFix Professional[105] is a rogue security application that is installed by the Trojan Xrupter.[106]Xrupter is a malicious executable that is installed by Vundo Trojan variants.[107] The rogue security application works in tandem with Xrupter. When Xrupter is installed on a victim's computer, it encrypts personal documents. The Trojan then displays warnings to the user about corrupt documents with a button to repair them (figure 20).

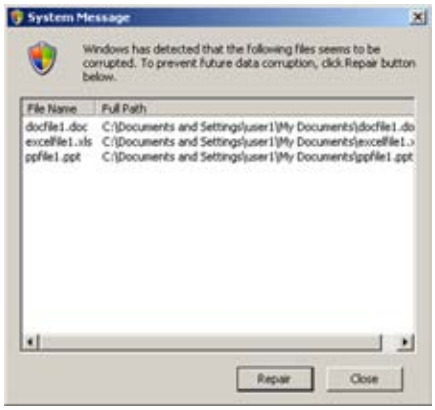

Figure 20. Trojan.Xrupter results detecting corrupted files

Courtesy: Symantec

When the "Repair" button is clicked, the user is directed to obtain FileFix Professional (figure 21). However, if the user opts to obtain FileFix Professional, a demo version is instead presented and the user must pay to register for a full version in order to recover the files. Instead of attempting to sway the user with false security alerts, this variation of the rogue security software business model attempts to extort money from affected users in return for decrypting their documents, which were initially encrypted when Xrupter was installed.

Figure 21. FileFix Professional

Courtesy: Symantec

The connection to the Vundo Trojan is noteworthy. Once computers are affected by Vundo, a number of misleading applications and threats may be installed. Vundo itself has been distributed by other malicious code samples. In February

105-http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-032209-4419-99

2009, Symantec observed a spike of Vundo infections as a result of the W32.Ackantta.B@mm mass-mailing worm.[108] These multiple layers of misdirection help Vundo variants, related threats, and misleading applications evade detection. Vundo variants have also been detected exploiting vulnerabilities as a means of propagating, such as a vulnerability in Microsoft Internet Explorer®.[109]

Malicious software such as the Vundo and Zlob Trojans that are used to distribute rogue security software are effectively acting as affiliates. This implies that their revenue generation model is similar to other affiliate programs, whereby commissions are generated on a per-install basis. As noted earlier, Vundo was listed as the most prevalent malicious code sample for 2007 and 2008 in Volume 14 of the *Symantec Internet Security Threat Report*.[110] One of the reasons Zlob and Vundo were originally created was to download and install adware onto users' computers, likely earning money for the creators through adware affiliate programs. Legislative measures have reduced the profitability of adware scams and may have led to the modification of these Trojans for rogue security software scams instead. This may have contributed to the success of numerous misleading applications that have been associated with Zlob and Vundo. Through these methods, it is possible for malicious code authors to monetize their creations.

Mac OS X rogue security applications

Rogue security applications have not been limited to Microsoft Windows operating systems. In January, 2008, a rogue security application targeting Mac OS® X users named MacSweeper[111] was discovered (figure 22). Symantec believes that MacSweeper is a Mac OS X clone of the MalwareAlarm Scanner rogue security application that runs on Microsoft Windows.[112]

Figure 22. MacSweeper "scan" results page

Courtesy: Symantec

A further variant was released for Mac OS X entitled iMunizator.[113] When run, iMunizator flags a number of safe system binaries as problematic and prompts the user to pay a licensing fee to fix the problems on the computer. iMunizator is a fairly simple rogue security application that uses UNIX command-line utilities to find random files on the computer that it

106-http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-032207-0838-99
107-http://www.symantec.com/connect/blogs/offer-too-good-refuse-courtesy-vundo

will flag as problematic. This is in contrast to many rogue security software applications that purport to remove specific well-known security risks and malicious code.

These Mac OS X samples lack the degree of social engineering and functionality demonstrated in other prevalent samples targeting Microsoft Windows users. It is apparent that scam developers are experimenting with the Mac OS X platform, but that the observed samples lack the sophistication of those targeting Microsoft Windows users, which have generated far more success and revenue.

Innovations such as encrypting the user's data in exchange for a ransom payment and targeting Mac OS X users have not resulted in rogue security applications that are highly prevalent. Neither FileFix Professional nor MacSweeper/iMunizator rank among the top reported samples observed by Symantec. While this may be a matter of distribution, it is also likely that conventional tactics are profitable enough that novel techniques are not required to increase the revenue of scammers.

Top rogue security software by region

For this measurement, Symantec analyzed the regional distribution of the consumer reports between July 1, 2008, and June 30, 2009 of the top 50 rogue security software programs (figure 23). During this period, 61 percent of rogue security software scams observed by Symantec were attempted on users in the North America (NAM) region, 31 percent occurred in the Europe, the Middle East, and Africa (EMEA) region, six percent occurred in the Asia-Pacific/Japan (APJ) region, and two percent occurred in the Latin America (LAM) region.

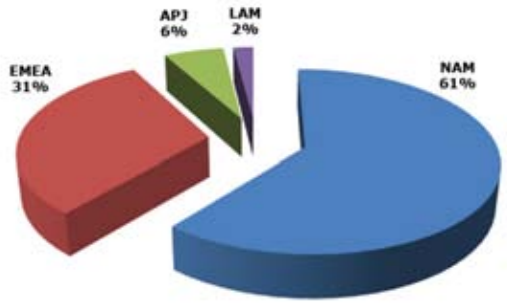

Figure 23. Percentage of rogue security software distribution, by region

Courtesy: Symantec

The variance in the percentages of reported scams between each region suggests that regional boundaries affect the distribution of rogue security software. This may be related to the amount of malicious activity in general that affects these regions. As discussed in Volume 14 the *Symantec Internet Security Threat Report,* the majority of malicious activity globally is detected in the NAM and EMEA regions.[114] Considering that rogue security software is often installed on computers by malicious code or through drive-by download attacks, the prevalence of malicious activity in NAM and EMEA may be a contributing factor in the distribution of rogue security software programs.

108-http://www.symantec.com/security_response/writeup.jsp?docid=2009-022520-1425-99
109-http://www.securityfocus.com/bid/11515
110-http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 60
111-http://www.symantec.com/security_response/writeup.jsp?docid=2008-011613-5206-99
112-http://www.symantec.com/connect/blogs/attack-clones-ii
113-http://www.symantec.com/connect/blogs/cloning-shop-mac-users-now-open
114-http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 17 and 31

An additional factor contributing to the prominence of NAM and EMEA in this measurement may be the regional difference in per-installation prices paid for affiliate distribution, as discussed earlier in this report. For example, the price-per-install for North America is as much as 10 times that of the price-per-install for Latin America, which would likely incline scam distributors toward distributing these programs where the returns will be greater.

The overwhelming number of attempted rogue security software scams reported in North America may also be due to the majority of programs being created in English, the primary language for the majority of people in the region. Although some programs target other languages—such as CodeClean,[115] which targets Korean users (figure 24)—the majority of the programs that Symantec observed during this reporting period have been developed and distributed in English.

Figure 24. CodeClean rogue security application that targets Korean language users

Courtesy: Symantec

Top rogue security software installation methods

There are two main ways that rogue security software programs can get onto a user's computer, as described earlier in this report. This is either through an intentional download, where the user is persuaded to download and install the program, or via an unintentional download, where the download occurs without the user's permission or knowledge. This section will examine the prevalence of the distribution methods used by the top 50 rogue security software programs observed by Symantec during the period of this report. It is worth noting that distribution methods are not mutually exclusive and that, in nearly 70 percent of reports for the top 50 programs, both distribution methods were employed.

The most common distribution method observed by Symantec during this reporting period was intentional downloads, which were employed in 93 percent of the attempts of the top 50 rogue security software scams. One reason that this method of distribution is popular may be because many users are suspicious of unauthorized installation procedures or programs that appear on their computers without their interaction.

Legal implications could also be a factor that makes intentional downloads a popular distribution method. Downloading and installing a program onto a computer without the user's consent is illegal in some countries. However, if a program is

115-http://www.symantec.com/security_response/writeup.jsp?docid=2007-013111-5717-99

downloaded and installed intentionally, the onus could fall on the user and not the scam distributor. Scam perpetrators operating where such restrictions exist may opt to reduce legal liability as much as possible and rely on intentional downloads. Some rogue security software programs implement EULAs that must be accepted during installation; by accepting a EULA, the consumer may potentially be releasing the scam distributor from legal implications.

Unintentional downloads were employed in 76 percent of the attempts in the top 50 rogue security software scams observed by Symantec during this reporting period. As noted earlier, an unintentional download occurs when malicious code is downloaded onto a computer without the interaction or knowledge of the victims, such as via drive-by download attacks, or when users have been duped into downloading and installing what they think are legitimate applications, such as missing video codecs. These downloads often contain staged downloaders that, once the user's computer is compromised, download and install additional programs such as rogue security applications.

The lower percentages for unintentional downloads compared to intentional downloads as a distribution method may also be a reflection of the relative skill levels of some scam authors or distributors. The development of the code required for intrusive distribution might require a deeper technical ability than some of these people are able to learn or care to use. Although scam distributors may pay malicious code developers per install to distribute rogue security software, some of them might not have the desire or necessary contacts to do so. Additionally, some scammers may be effective at using other means to lure in users, such as social engineering skills, and thus do not require the technical demands of programming code.

Additionally, some malicious code authors may have been slow to realize the revenue generating potential of rogue security software scams. With Trojans such as Zlob and Vundo being successful and effective affiliates for rogue security software, there may be an increase in malicious code as a distribution method in the future as other authors realize the earning potential from these scams.

Top rogue security software advertising methods

Scam distributors use many methods to tempt users into downloading and installing rogue security software. This section examines the prevalence of certain advertising methods used in the top 50 rogue security software programs that Symantec observed during this reporting period.

The most common advertising method used by the top 50 rogue security software programs that Symantec observed during this reporting period was through dedicated websites, which were used in 93 percent of scams. It should be noted that although the percentage of advertising using scam websites is the same as the percentage of distribution by intentional downloading, discussed in "Top rogue security software installation methods," above (with both being 93 percent), the results are coincidental. While this method of advertising is closely related to distribution by intentional downloads (that is, if a website exists, the program can most likely be downloaded there), the ability to also download programs from third-party hosts means that a particular scam does not necessarily require a website in order to be intentionally downloaded. Also, some websites dedicated to rogue security software act solely as a launching point for drive-by download attacks, forgoing the use of distribution by intentional download altogether.

The second most common advertising method for rogue security software observed by Symantec during this reporting period was Web advertising, which was used in 52 percent of the attempted rogue security software scams. While this may

suggest that Web advertisements are not as effective as dedicated websites for promoting rogue security software, more Web advertisements were observed for the top 10 programs than in the remaining 40 of the top 50 programs combined. This may indicate that well-deployed Web advertisements can be a very effective method of distributing rogue security software.

Although the reverse is not true, nearly all of the programs that use Web advertisements also use malicious code and drive-by downloads (or both) as a distribution method. For example, the WinFixer scam—the sixth most reported scam observed by Symantec during this reporting period—uses both a website and Web advertisements in addition to being distributed by malicious code, including by the Vundo Trojan, and by both intentional and drive-by downloads. This may indicate that Web advertisements are more effective as launch points for intrusive distribution tactics than they are for luring intentional downloads. This may also explain why the percentage of rogue security software programs that use Web advertisements is similar to the distribution method percentages of malicious code and drive-by downloads.

Analysis of Rogue Security Software Distribution

This section of the *Symantec Report on Rogue Security Software* will expand on the overview of this topic earlier in this report. It will discuss specific examples of how rogue security software applications are distributed, presenting more information about specific incidents and insight into the infrastructure of rogue security software distribution.

Given that profit is a motive behind most rogue security software scams, the success of these scams depends on convincing consumers to purchase the fake software. To do so, scam creators try to convince users of exaggerated or non-existent threats on their computers and that the fake security software is a valid solution. As such, scam software often mimics the appearance of legitimate security software. A common tactic is to present an interface that is similar to the Microsoft Windows Security Center, as is shown in the discussion on AntiVirus 2008 and AntiVirus 2009, above (figure 15).[116] The Security Center has been a feature of Windows since the release of XP Service Pack 2, with minor changes to the interface in Windows Vista®; users are likely to be familiar with this interface and might consider the false applications that mimic its appearance to be the real thing.

As noted, other scam software may mimic the appearance of well-known, genuine security software. To facilitate this, scam authors create user-interface templates that can be reused and modified to create new variations of the scam. The templates enable the customization of various aspects of the scam, such as the title of the rogue application, the text to display, and the appearance of the interface. This helps scam creators to easily re-brand rogue applications once they are identified and exposed as scams. Templates also often incorporate social engineering tactics to scare users. In one example, a fake "blue screen of death" interface is presented that urges the user to solve this critical issue by installing a rogue security application named SystemSecurity.[117] Templates also allow for easy localization of scams for distribution in new markets. For example, the fake "blue screen of death" template has also been observed localized into Arabic.[118]

Making the rogue software modular and comprised of re-usable components to perpetrate different variations of scams reduces the time required to develop and deploy new scams. Additionally, it allows different skills to be outsourced, such as the design of templates and social engineering angles. Symantec observed similar behavior with phishing scams in its study of the underground economy.[119] It was observed that different individuals and groups may develop modular components of phishing methods such as scam letters and phishing website templates, which may then be sold as part of a customized package to scam distributors. This tactic is also used by websites designed to deliver malicious code.[120] The same principle can be applied not only to the applications themselves, but also to the websites that distribute the applications.

Scam distributors also attempt to have the websites for their rogue security applications appear at the top of search engine results to increase the chances of being noticed—and considered genuine—by users. If these websites can appear among legitimate websites in search results for malicious code and security-related search queries, it may be more difficult for users to distinguish legitimate sites from those that are malicious. For example, in March 2009, distributors of rogue security applications employed this tactic by injecting links to their software in Downadup-related search results.[121] In the same month, scam distributors also manipulated search results for a number of keywords related to antivirus and desktop applications.[122]

116-http://www.microsoft.com/windowsxp/using/security/internet/sp2_wscintro.mspx
117-http://blogs.zdnet.com/security/?p=3912
118-http://ddanchev.blogspot.com/2009/08/scareware-template-localized-to-arabic.html
119-http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf : p. 30
120-http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

Scam distributors also capitalize upon interest in current events to lure users into visiting websites that host rogue security software. For example, in May, 2009, one scam attempted to exploit public interest in the H1N1 virus outbreak as a means to distribute rogue security software.[123] Symantec also observed malicious code authors exploiting interest in the H1N1 virus by developing and distributing a PDF with FAQs on the flu that also included a payload of malicious code.[124] Spam distributors were also observed exploiting the headlines about H1N1.[125] This demonstrates that rogue security software scam perpetrators are willing to use the similar social engineering tactics employed by spammers and malicious code authors.

Search engines are a common means of distributing rogue security software. Black hat SEO operations are conducted to push sites that host rogue security applications to the top of search engine indexes.[126] A common black hat SEO tactic involves planting links to rogue security software websites on legitimate websites, such as blogging services, wikis, forums, and social networking sites. This tactic exploits search engine indexing algorithms that determine the relevancy of a website by the number of links that point to it. This process is typically automated by software that can visit these various Internet locations and add content. Because this activity is considered a form of spam, many websites implement measures such as CAPTCHA schemes to prevent content from being added automatically.[127] CAPTCHA schemes are used to ensure that human users, and not automated systems, are adding the content. This in turn has resulted in a number of efforts to bypass CAPTCHA that range from exploiting weaknesses in CAPTCHA algorithms to outsourcing the task of manually solving CAPTCHA challenges.[128]

Other black hat SEO tactics include link farming, keyword stuffing, and cloaking: link farming is an SEO tactic used to increase search rankings by having a large group of websites include reciprocal links to each other; keyword stuffing involves placing long lists of often irrelevant keywords into Web page content; cloaking involves creating website content specifically for search engine website crawlers and which is different than the content accessible to users, which may cause search engines to index the site based on misleading content and potentially improve search rankings. Black hat SEO campaigns have also been known to exploit vulnerabilities in websites such as cross-site scripting.[129] In one reported example, vulnerabilities in a popular blogging platform were exploited to promote rogue security software.[130] Scam distributors also purchase keywords from search engines in order to boost the ranking of their scam websites and so that the websites will appear as valid, "sponsored" results.[131]

Rogue security software distributors use these black hat SEO tactics in combination with other techniques such as typo-squatting. Typo-squatting involves hosting sites with domain names that are similar to sites the scan authors are trying to spoof. Mistyping a URL may lead a user to the spoofed site instead of the legitimate website the user is trying to reach.

Malicious or false search engines have also been employed. To get users to use the illegitimate search engine, they are enticed to search for a special file, usually a topical video or the like. When the user searches with one of these fake search engines, the results instead mislead the user to websites that host malicious code and rogue security software.[132]

Affiliate networks can provide the scam developers with the talent and resources necessary to distribute their software using the tactics discussed above. In turn they may rely on resources in the underground economy to launch spam and black hat SEO campaigns. This may include purchasing lists of email addresses in bulk, spam proxies, credit cards to register domains in bulk, etc. When activities such as the development and distribution of rogue security software are

121-http://www.symantec.com/connect/blogs/downadup-related-search-indexes-poisoned-fake-av-sites
122-http://www.symantec.com/connect/blogs/yahoo-sponsored-search-results-leads-misleading-websites
123-http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html
124-http://www.symantec.com/connect/blogs/malicious-code-authors-jump-swine-flu-bandwagon

monetized and begin to generate revenue, the demand for other products and services in the underground economy increases as well.

Internet advertising networks have been used as a means to distribute scams. The legitimate appearance of rogue security applications may allow scam distributors to penetrate Internet advertising networks. The advertisements are likely to remain on the networks until the software being advertised is exposed as fraudulent. Additionally, scam distributors have also employed "malvertising" tactics.[133] In one observed attack, malicious advertisements were found to be exploiting a client-side vulnerability.[134] The advertisement redirected users to a site that exploited a vulnerability in Adobe Reader (since patched) via a malicious PDF document. Upon exploitation, the rogue security application Anti Virus 1 was installed. The attack also changed the system "hosts" file to redirect users to a site advertising further rogue applications.[135] In another attack, a malicious Flash advertisement that exploited a client-side vulnerability was distributed through an advertising network to a number of high-profile websites.[136] In one additional example, the advertising network for a news site was serving advertisements that prompted users to install rogue applications.[137]

Such attacks damage the reputation of not only the advertising networks, but potentially of the websites that circulate the malicious advertisements. In addition to the negative press surrounding such incidents, website reputation services may flag these sites as disreputable or suspect. Some browsers and security software will check website reputation databases before letting users browse to a website, thus potentially affecting legitimate traffic to flagged sites. Additionally, advertising revenue could be lost as users begin to distrust the advertising networks and implement security measures to block their advertisements.

In order to collect registration and/or subscription fees from consumers who have purchased rogue security software, scam perpetrators need online payment processing services. Since the payment services used are often legitimate, there is a constant threat that the payment service provider will discover that its service is being used for fraud. This is one reason why rogue applications are often re-branded, to avoid credit card chargebacks and payment reversals that may ultimately draw attention to the scam. However, rogue payment processors have also been established to serve affiliate networks who distribute rogue security software.[138] Due to their illicit nature, these rogue payment processing services run the risk of being shut down once their activities are discovered and are often short-lived.

In order to further evade discovery, scam payment processing often occurs through a number of gateway websites registered under different domain names that will redirect to the actual payment processor for the scam.[139] The domains are registered under a variety of email addresses to make it appear as though multiple individuals own the domains. Scammers can acquire email addresses by means such as purchasing them in bulk in the underground economy or by the automated generation of email accounts through popular Web-based email services. Similar approaches are used to register domain names for hosting the scam software, as is discussed next in "Analysis of rogue security software servers." Distributors of rogue security software may register domains with domain registrars in places where enforcement is perceived to be weak or where anonymous registration services are offered.[140] Rogue ISPs such as the RBN have also been

125-http://www.symantec.com/connect/blogs/swine-flu-outbreak-headlines-used-spammer-s-gain
126-SEO (Search Engine Optimization) is a process for making websites more popular in search engine results. Black hat SEO uses search optimization techniques that are considered unethical by the mainstream SEO community, which may include spamming and other questionable practices. For an overview of SEO techniques and guidelines, please see: http://www.google.com/support/webmasters/bin/answer.py?hl=en&answer=35291
127-CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart". CAPTCHA schemes often take the form of an image containing characters that must be entered before the user can perform an action such as creating an account or submitting content on a website.
128-http://ddanchev.blogspot.com/2008/08/exposing-indias-captcha-solving-economy.html
129-http://ha.ckers.org/blog/20060608/xss-redirects-and-seo/
130-http://pandalabs.pandasecurity.com/archive/New-Blackhat-SEO-attack-exploits-vulnerabilities-in-Wordpress-to-distribute-rogue-antivirus-software.aspx
131-http://blogs.zdnet.com/security/?p=1995
132-http://www.computerweekly.com/Articles/2009/05/07/235935/cybercrooks-develop-own-search-engines-to-burgle-users.htm
133-Malvertising is a term to describe the practice of malicious advertising which includes tactics such as obfuscating malicious content in Flash advertisements or embedded exploit code into advertising content
134-http://www.eweek.com/c/a/Security/Attackers-Infect-Ads-With-Old-Adobe-Vulnerability-Exploit/

involved in various aspects of scam development and distribution. This includes hosting domains that distribute rogue security applications.[141]

Scammers also benefit by phishing personal information from users who register rogue applications. Information such as email addresses, credit card details, and payment processing credentials can be used for further fraudulent activities or sold in the underground economy. In this manner, a single scam can be used to generate revenue in different ways. Furthermore, fraudulent activities such as credit card and payment processing fraud can help to finance the startup costs of additional scams.

135-The system hosts file maps IP addresses to hostnames. The system hosts file is often consulted before domain name server lookups to resolve a hostname. This means that mappings in the hosts file often take precedence over DNS lookups; malicious code often employs the tactic of changing hostname to IP address mappings so that users are redirected to malicious sites or blocked from visiting sites where security updates and security software are available.
136-http://blogs.zdnet.com/security/?p=1815
137-http://blogs.zdnet.com/security/?p=3140
138-http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html
139-http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html
140-http://voices.washingtonpost.com/securityfix/2008/09/estdomains.html
141-http://rbnexploit.blogspot.com/2007/10/rbn-top-20-fake-anti-spyware-and-anti.html

Analysis of Rogue Security Software Servers

In this section, Symantec conducted a geographic analysis of servers hosting rogue security software. This analysis is not meant to represent all rogue security software servers; instead the goal was to identify any emerging patterns in the way these servers are created, managed, and interconnected with each other. The data was collected in a two-month period over July and August 2009.

For this measurement, Symantec analyzed 6,500 DNS entries pointing to 4,305 distinct IP addresses hosting rogue security software servers.[142] At least 45 percent of these domains were registered through just 29 out of several hundred existing domain registrars. This may indicate that rogue security software distributors are choosing specific registrars, possibly because of perceived lax security or oversight of the registration of names.

The DNS entries resolving to these IP addresses were first identified by monitoring DNS activity across the servers. From this, an additional 187,514 DNS entries associated with rogue security applications were observed, for a total of 194,014 domain names. In total, 2,677 Web servers hosting domains (as identified by their unique IP addresses) were identified as dedicated to serving only rogue security software, an additional 118 Web servers hosted rogue security software along with domains that served malicious code, and the remaining 1,510 IP addresses served malicious code along with innocuous domains.

Of the servers hosting rogue security software that Symantec geographically located, 53 percent were in the United States, far more than any other country (table 3 and figure 25). The high ranking of the United States may be due to the methods for identifying rogue security software sites, which more easily identified English-language sites than sites marketing scams in other languages. Germany ranked second in this survey, accounting for 11 percent of the total servers hosting rogue security software identified by Symantec. This ranking may be due to Germany being the top country in EMEA for broadband subscribers and a major broadband connection hub.

Rank	Country	Percentage
1	United States	53%
2	Germany	11%
3	Ukraine	5%
4	Canada	5%
5	United Kingdom	3%
6	China	3%
7	Turkey	3%
8	Netherlands	2%
9	Italy	2%
10	Russia	1%

Table 3. Servers hosting rogue security software, by country

Source: Symantec

142-The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network.

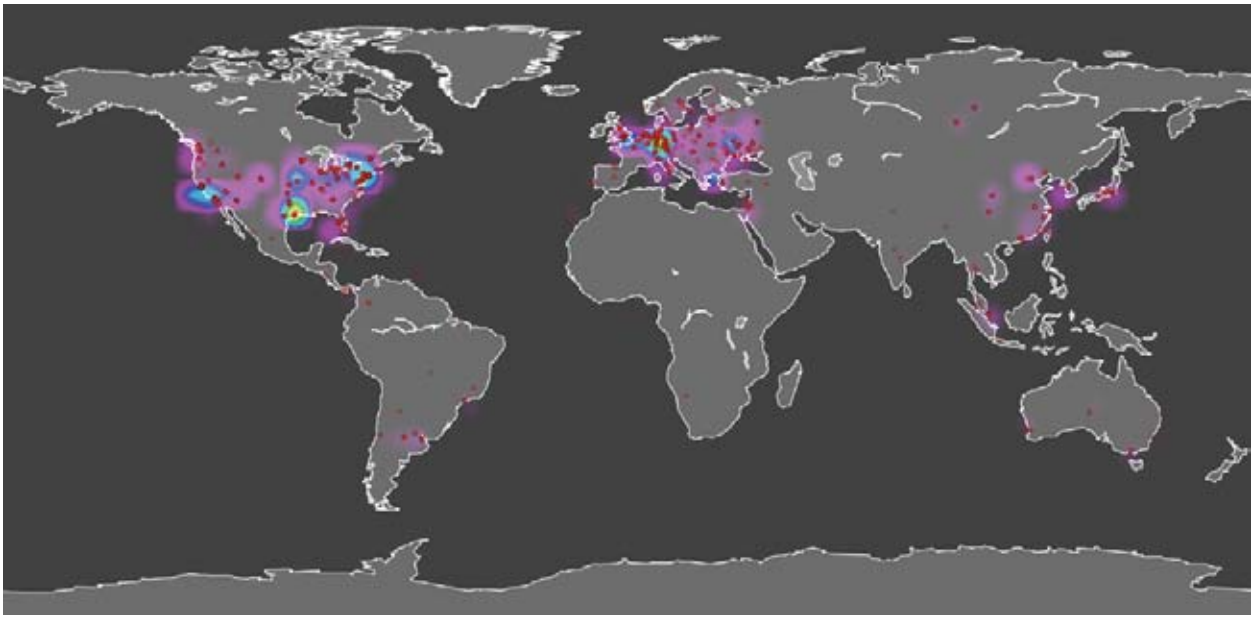

Figure 25. Global distribution of rogue security software servers[143]

Source: Symantec

After analyzing the distribution of the servers hosting rogue security software and their corresponding DNS servers, there appears to be a high degree of correlation between the two (figure 26). As such, it is likely that distributors of rogue security software are not using botnets as part of their hosting infrastructure, although some malicious code, such as Downadup, attempts to download rogue security software onto compromised computers.[144] Since botnets can be easily operated from home computers, the use of botnets as rogue security software servers would likely have resulted in a more even distribution of server IP addresses across the entire address space, instead of the concentration that was observed. This correlation of servers indicates that many rogue security software distributors are likely just using commercial Web server hosting providers.

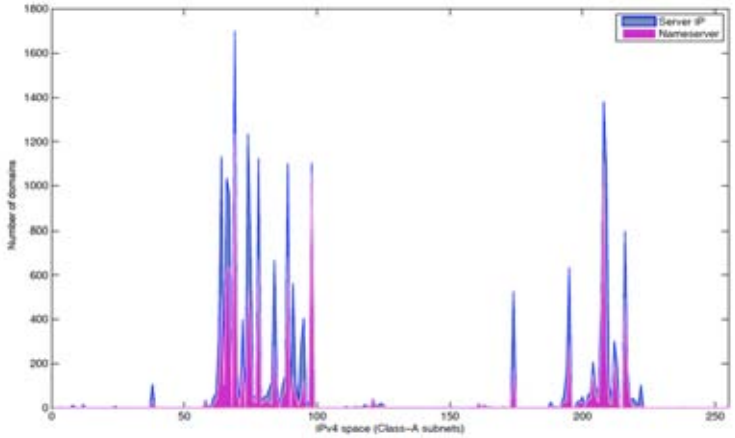

Figure 26. Distribution of rogue security software server IP addresses and their DNS servers

Source: Symantec

143-Each red dot represents a distinct server, while the different gradients on the background underline the areas with highest density of deployed servers.
144-Downadup is associated with rogue security distribution scams such as TrafficConverter.biz, as discussed above.

To determine the relationship between servers (IP addresses) and domain names for rogue security software, a subset of the total analyzed domains has been graphically represented as clusters (figure 27). This subset represents 174 servers that were hosting a total of 30,632 distinct domain names.[145] The relationship between domains (dots in the figure) that were associated with servers is represented by the connecting lines. Clusters are formed when one server has multiple domains associated with it.

Of this observed domain set, those that hosted rogue security software accounted for 15 percent of the total (shown as red in the figure). Nine percent of the total domains were observed to host malware such as malicious executables, scripts, and documents, but may not be hosting rogue security software (shown as orange), and domains that are not malicious accounted for 76 percent of the total observed servers (shown as green).

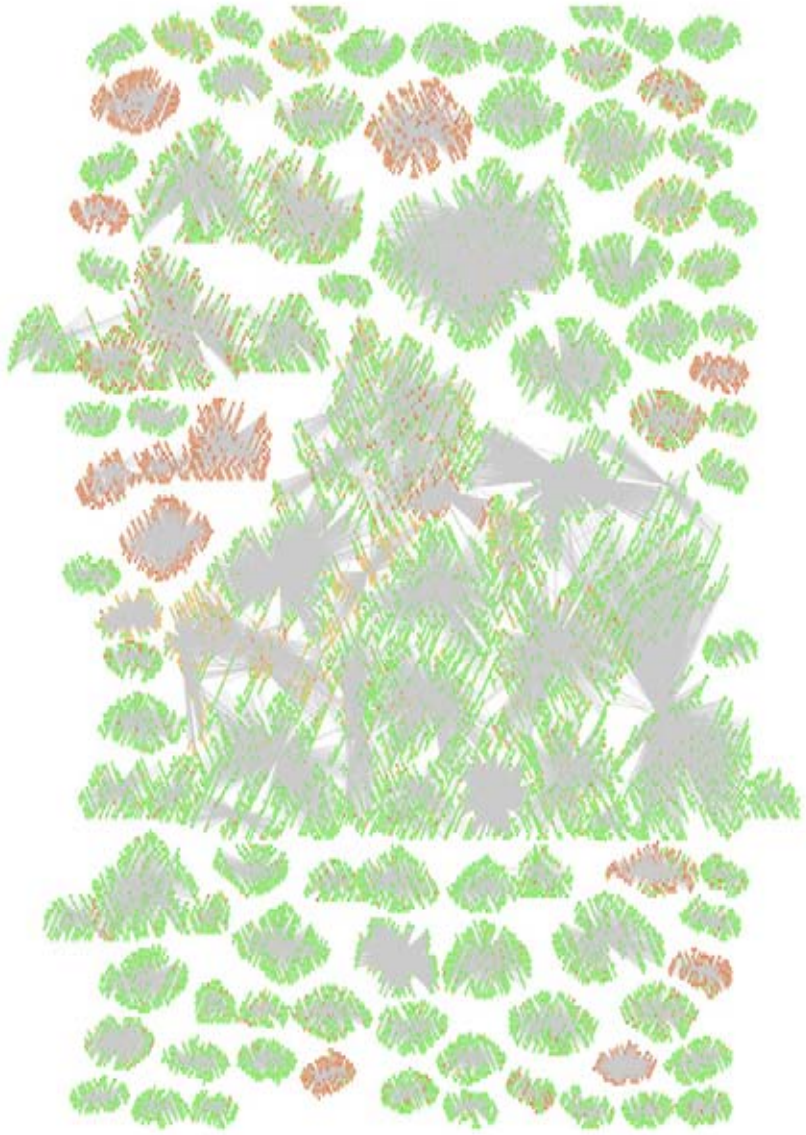

Figure 27. Observed servers and domain name cluster relationships

Source: Symantec

145-For representation purposes, only servers that were observed hosting at least 100 distinct domains are shown in the figure; although the figure does not show all domains, all were used in the analysis.

While most domain names are linked to a single Web server (shown as an isolated cluster), some rogue security software networks span multiple Web servers. Also, some domains were observed as being hosted on more than one server, which may be an attempt to reduce the effectiveness of mitigation measures such as IP blocking or blacklisting servers.

Figure 28, below, highlights the domain clusters that hosted rogue security software. In other words, non-malicious servers (the green in figure 27, above) and servers hosting malicious code (orange, above) have been removed to show just the rogue security software domain clusters.[146] The figure represents 416 servers (IP addresses) hosting 9,964 rogue security software domains (shown in red). Their relationship is shown by a connecting line.

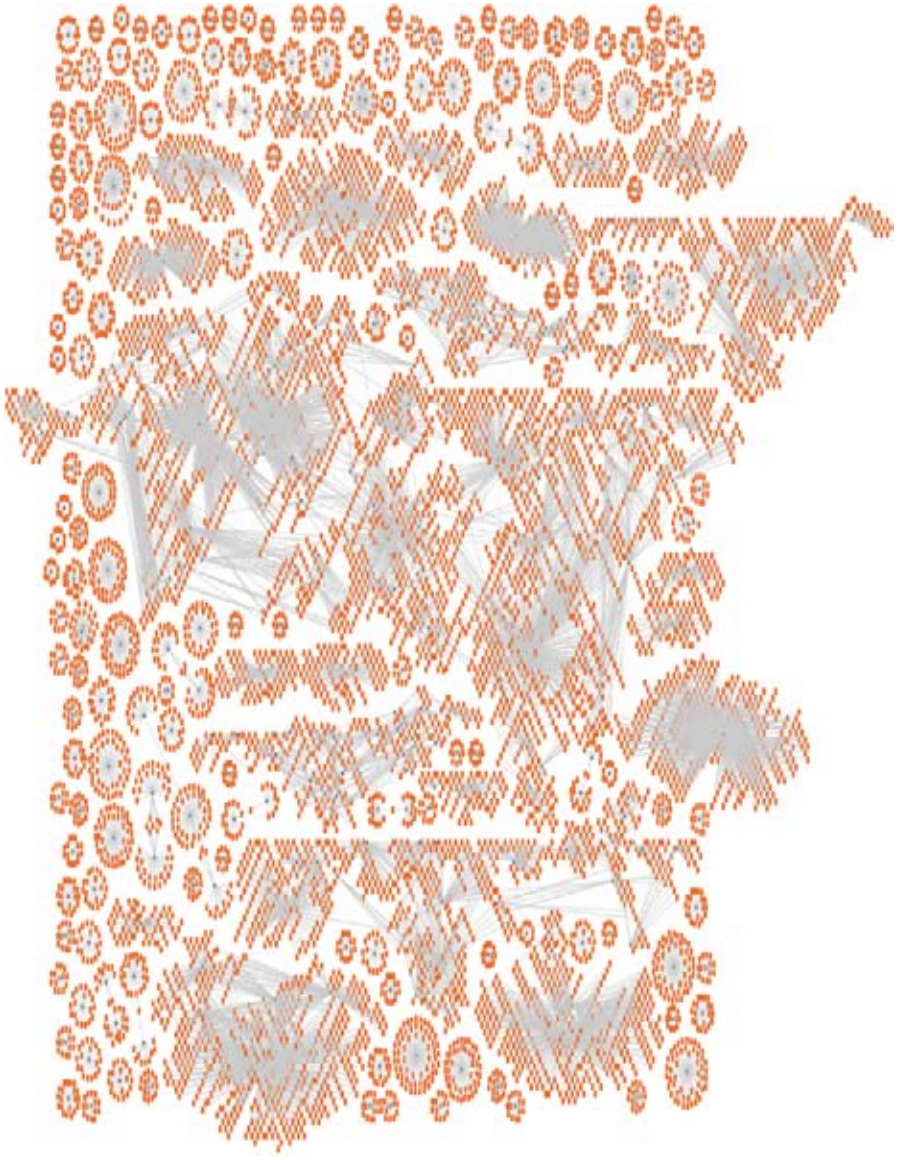

Figure 28. Observed servers and domain name clusters hosting only rogue security software

Source: Symantec

Although a majority of the servers are not malicious, Symantec did observe a number of highly malicious servers. Of the observed rogue security software domains, 26 percent of the total served malicious content of various types (table 4). In

addition, 13 percent of the domains attempted to use browser exploits, one percent attempted to perform drive-by downloads, which seek to infect client computers by forcing them to download and execute malware, without requiring further action (such as a confirmation prompt) by the user, and less than one percent led to the installation of spyware on the user's computer. (Note that a given Web server could belong to several of these categories.)

Rank	Type of Activity	Percentage
1	Infected system with malicious code	26%
2	Attempted to exploit browser vulnerability	13%
3	Attempted a drive-by download	1%
4	Installed spyware	< 1%

Table 4. Percentage of rogue security software domains serving malicious activity, by type
Source: Symantec

Two specific clusters of rogue security software servers from figure 28 were analyzed in detail (figures 29 and 30). Although the two clusters initially appear to be distinct, they have a number of similarities:

- Both clusters use the exact same domain naming scheme (except that one uses “spyware” while the other uses “virus”)
- All of the domains in each cluster use the same registrar and are serviced by the same two ISPs
- All domains within each cluster were registered in a single day and became active (serving software) at nearly the same time
- The email addresses of all domain registrants are in “.ru” domains;
- The servers were on consecutive IP addresses
- The content of these sites was identical, with the exception of one differing image

These similarities strongly suggest that the task of registering, creating, and hosting these rogue security software domains was automated and that the same entity may be responsible for both clusters. Also worth noting is that both clusters are split between two different ISPs, suggesting an attempt to provide some level of redundancy in case a cluster is taken offline by the ISP.

146-As with figure 27, for graphical clarity in figure 28, only rogue security software domain clusters containing at least 10 observed domains are shown.

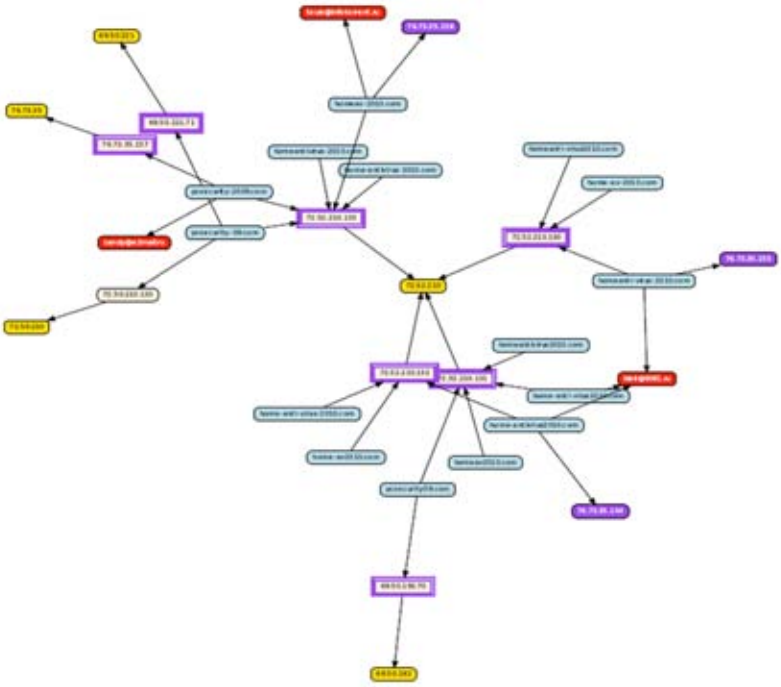

Figure 29. Example cluster 1[147]*Source: Symantec*

147-DNS domains are shown in light blue, DNS servers in purple, the Web server /24 subnets in yellow, and the email address of the registrant in red. Double-edged purple boxes indicate servers with co-located DNS and Web servers.

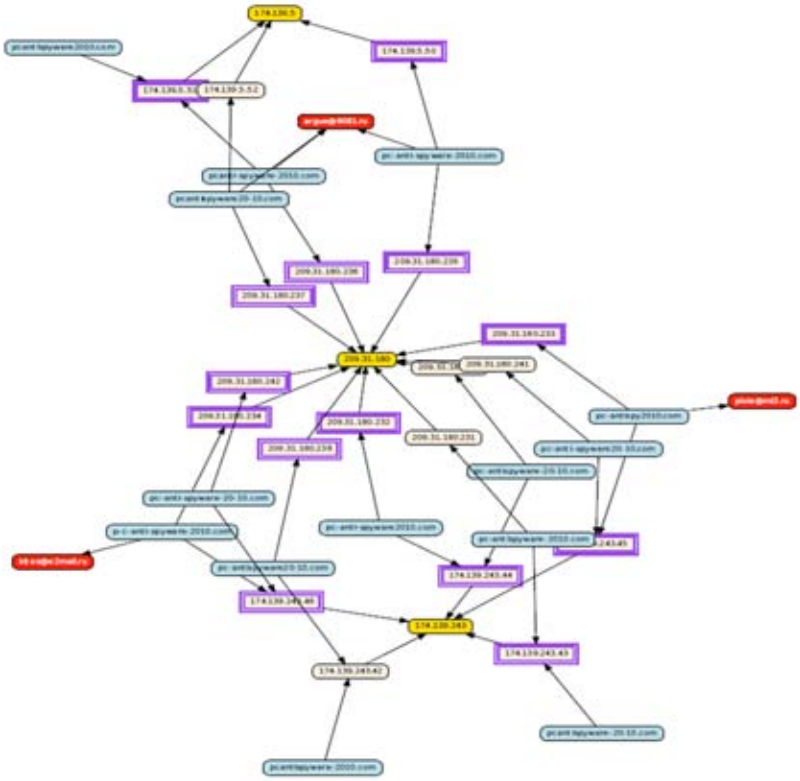

Figure 30. Example cluster 2[148]*Source: Symantec*

A commonly observed characteristic of rogue security software operations was that domain names are registered in large groups within a span of a few days. Symantec observed one site that registered 310 .cn top-level domain names in three days (represented in Figure 31), The 310 domain names (in blue) point to 13 IP addresses residing in five subnets (yellow) and were registered by a number of Web-based email addresses (red) in three days (purple). The prevalent use of popular Web-based email accounts to register these domains is assumed to be because these email services are easily anonymized. These registrants also make use of domain registration services that can either protect registrant privacy or ones that do not verify identities and email addresses.

148-DNS domains are shown in light blue, DNS servers in purple, the Web server /24 subnets in yellow, and the email address of the registrant in red. Double-edged purple boxes indicate servers with co-located DNS and Web servers.

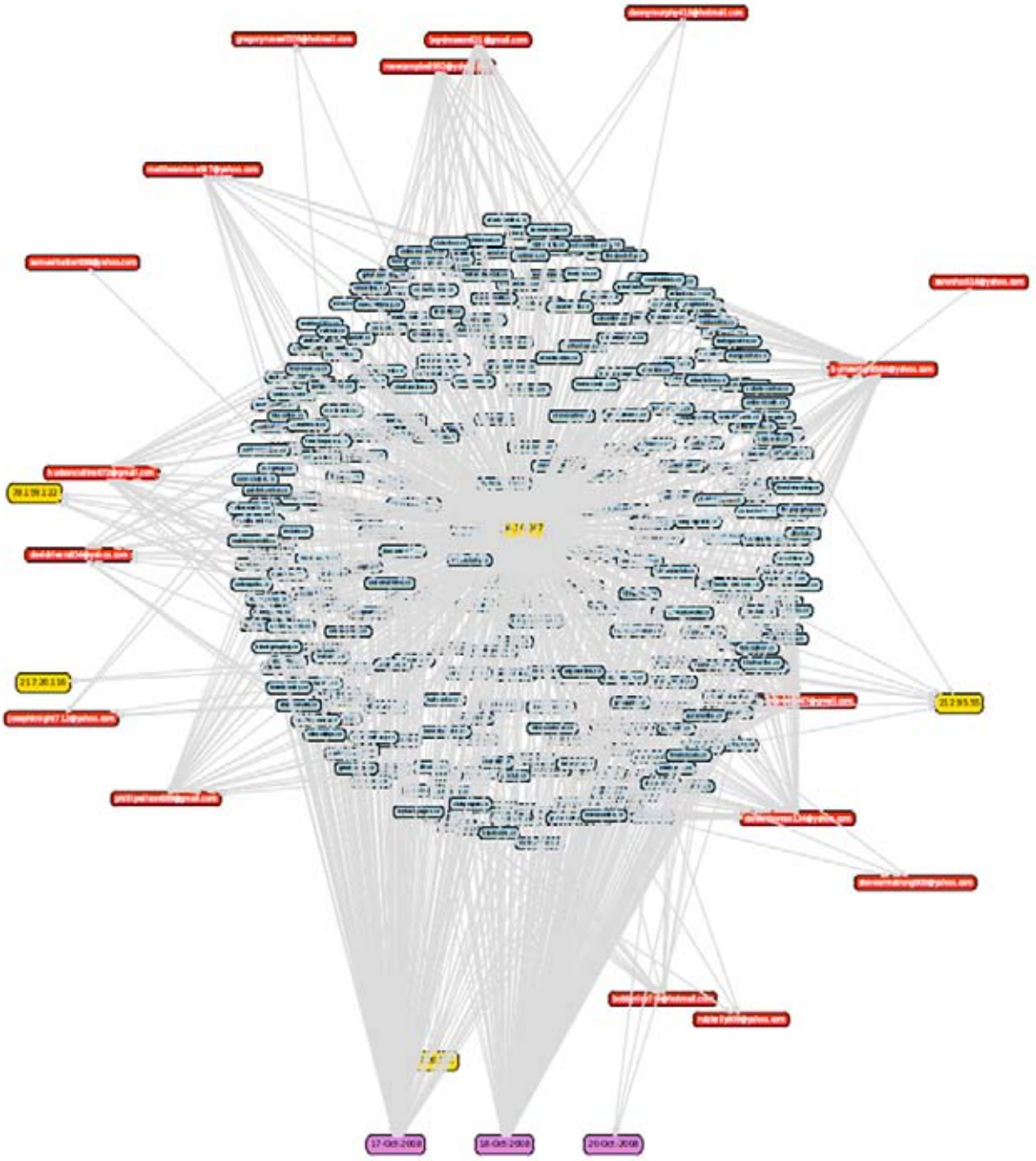

Figure 31. Cluster of 310 domain names registered within three days

Source: Symantec

In another example, 750 .cn top-level domain names (resolving to 135 IP addresses in 14 subnets) were registered on eight specific dates over a span of eight months (figure 32). It should be noted that the .cn top-level domain has no registration restrictions and non-Chinese based operators can register a domain name. For example, of the 750 domains registered in the second example, the majority of the IP addresses of the hosting servers (pointed to by these domains)

were hosted in the United States, Germany, and Belarus. No servers could be identified as being located in China (.cn is the domain designation for China).

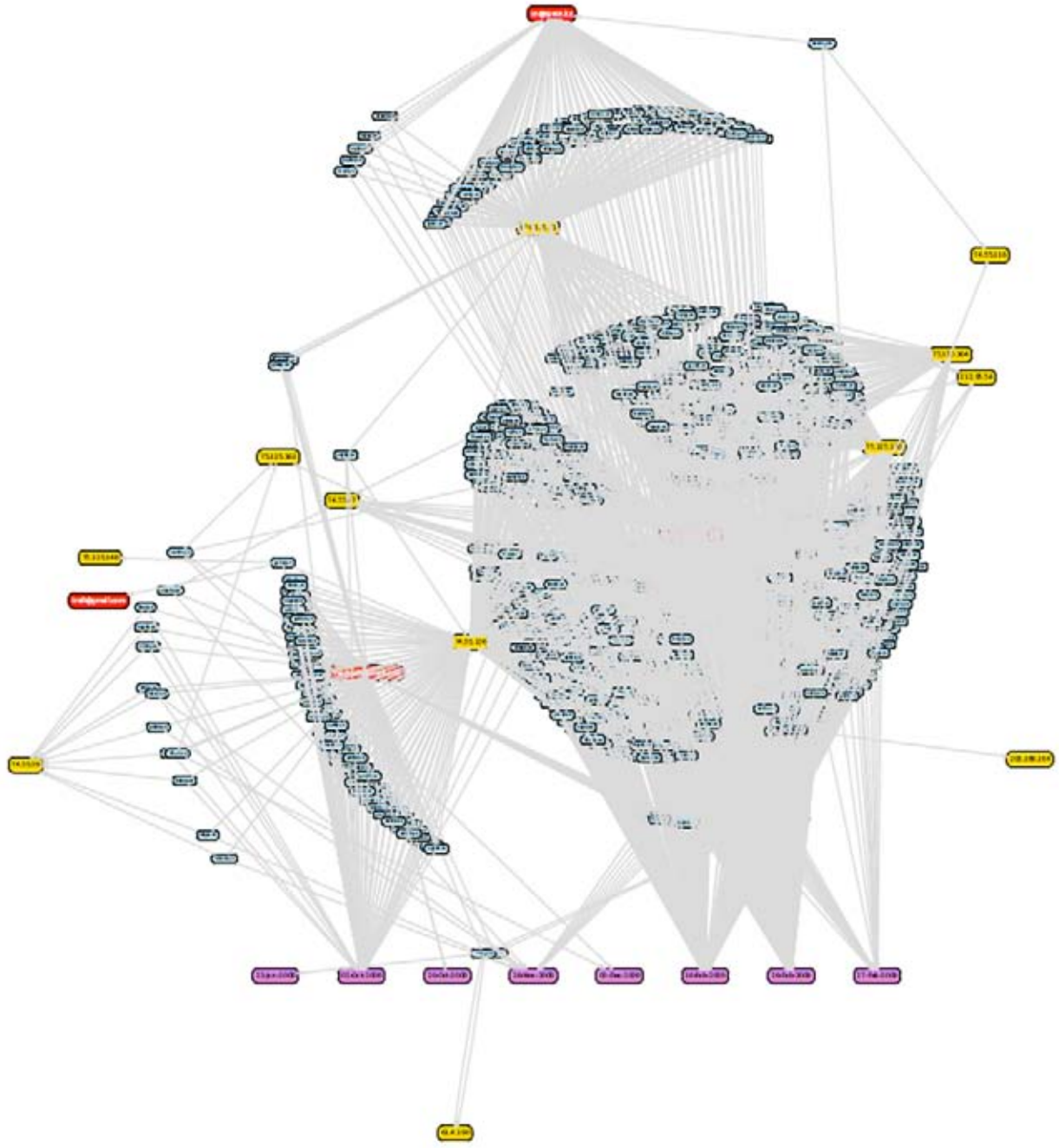

Figure 32. Cluster of 750 domain names

Source: Symantec

Appendix A: Protection and Mitigation

There are a number of general measures that enterprises, administrators, and end users can employ to protect against fraud-related activities such as rogue security software scams.

Enterprise

Administrators should update antivirus definitions regularly and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. Also, computers should use the latest protection from spyware and other security risks, such as Norton Internet Security. As compromised computers can be a threat to other systems, Symantec also recommends that enterprises notify their ISPs of any potentially malicious activity, such as bots. Symantec recommends that organizations perform both ingress and egress filtering on all network traffic to ensure that malicious activity and unauthorized communications are not taking place. Organizations should also filter out potentially malicious email attachments to reduce exposure to enterprises and end users.

Organizations should monitor all network-connected computers for signs of malicious activity including bot activity and potential security breaches, ensuring that any infected computers are removed from the network and disinfected as soon as possible. Organizations should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall.[149]

To protect against potential rogue security software scam activity, organizations should educate their end users about these scams. They should keep their employees notified of the latest scams and how to avoid falling victim to them, as well as provide a means to report suspected malicious rogue security software websites. By creating and enforcing policies that identify and restrict applications that can access the network, organizations can minimize the effect of malicious activity, and hence, minimize the effect on day-to-day operations.

Administrators can use a number of measures to protect against the effects of vulnerabilities. They should employ a good asset management system to track what assets are deployed on the network and to determine which ones may be affected by the discovery of new vulnerabilities. Vulnerability management technologies should also be used to detect known vulnerabilities in deployed assets. Administrators should monitor vulnerability mailing lists and security websites to keep abreast of new vulnerabilities in Web applications.

Website maintainers can reduce their exposure to site-specific vulnerabilities by conducting a security audit for common vulnerabilities affecting their sites. Web application code should be audited prior to being released to production systems. When developing Web applications, organizations should investigate the availability and applicability of secure libraries to perform validation of user-supplied input. Secure development practices and threat modeling should also be employed when developing Web-based applications. Web-application firewalls may also detect and prevent exploitation of Web-based vulnerabilities on production sites.

To protect against successful exploitation of Web browser vulnerabilities, Symantec advises users and administrators to upgrade all browsers to the latest, patched versions. Symantec recommends that organizations educate users to be extremely cautious about visiting unknown or untrusted websites and viewing or following links in unsolicited emails. Administrators should also deploy Web proxies in order to block potentially malicious script code. While attacks are likely

to originate from websites that are trusted as well as those that are not, Web browser security features can help reduce exposure to browser plug-in exploits, as can whitelisting. Specifically, administrators and end users should actively maintain a whitelist of trusted websites, and should disable individual plug-ins and scripting capabilities for all other sites. This will not prevent exploitation attempts from whitelisted sites, but may aid in preventing exploits from all other sites. Only plug-ins that have been audited and certified should be installed on workstations throughout the organization.

Symantec recommends that certain best security practices always be followed to protect against malicious code infection. Administrators should keep patch levels up to date, especially on computers that host public services and applications-such as HTTP, FTP, SMTP, and DNS servers-and that are accessible through a firewall or placed in a DMZ. Email servers should be configured to only allow file attachment types that are required for business needs and to block email that appears to come from within the company, but that actually originates from external sources. Additionally, Symantec recommends that ingress and egress filtering be put in place on perimeter devices to prevent unwanted activity.

Administrators should ensure that all email attachments are scanned at the gateway to limit the propagation of email-borne threats. Additionally, all executable files originating from external sources, such as email attachments or downloaded from websites should be treated as suspicious. All executable files should be checked by antivirus scanners using the most current definitions.

Enterprises should take measures to prevent P2P clients from being installed on any computers on the network. They should also block any ports used by these applications at the network boundary. End users who download files from P2P networks should scan all such files with a regularly updated antivirus product.

End user

In addition to the protection and mitigation measures recommended for enterprises, end users could also take more security precautions when conducting Internet activities to ensure that their computer will not be compromised and their information will not be compromised and used for identity fraud. Users should also avoid following links from emails, as these may be links to spoofed or malicious websites. Instead, they should manually type in the URL of the website. Symantec also advises that users never view, open, or execute any email attachment unless the attachment is expected and comes from a known and trusted source, and unless the purpose of the attachment is known. Also, users should be suspicious by an email that is not directly addressed to their email address.

Users should be cautious of pop-up displays and banner advertisements that mimic legitimate displays or try to promote security products. Also, users should not accept or open suspicious error displays from within their Web browser as these are often methods rogue security software scams use to lure users into downloading and installing their fake product. In addition, users should only purchase security software from reputable and trusted sources and only download applications directly from the vendor's website or legitimate partners.

Individual Web users should also exercise caution when browsing the Web. Since malicious attacks can result in hijacking of open sessions, users should make sure to log out of websites when their session is complete. Users should also be wary of visiting untrusted or unfamiliar sites. Scripting and active content can also be disabled when casually browsing the Web.

Users should regularly review credit card and other financial information as this can provide information on any irregular activities. For further information, the Internet Fraud Complaint Center (IFCC) has also released a set of guidelines on how to avoid Internet-related scams.[149] Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

149-Defense-in-depth emphasizes multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology. Defense-in-depth should include the deployment of antivirus, firewalls, and intrusion detection systems, among other security measures.

Appendix B: Methodologies

Top reported rogue security software

This metric will determine the most prevalent rogue security software programs based on the number of consumer reports for each rogue security software program observed during the reporting period. The top five applications will be discussed, including analysis of their affects and features. This will provide insight into which rogue security software scams have been the most successful and may indicate prevailing attributes that will continue to be employed or enhanced in future scams.

Top rogue security software by region

Using the top 50 rogue security software programs, as determined by the number of consumer reports per program, this metric will discuss the geographic location of rogue security software reports. The percentage of reports in each of the regions (NAM, LAM, EMEA, and APJ) will be examined to determine whether or not geographic boundaries affect the distribution of software and to provide insight about whether or not these scams are tailored for specific regions or languages.

Rogue security software distribution methods

Using the top 50 rogue security software programs, as determined by the number of consumer reports per program, this metric will discuss how rogue security software gets onto a user's system. Information about each of the top 50 programs will be analyzed to determine which distribution methods each program uses. The resulting data will be combined with the number of consumer reports to determine the prevalence of each distribution method during the reporting period. Distribution methods will include intentional downloads and unintentional downloads.

Rogue security software advertising methods

Using the top 50 rogue security software programs, as determined by the number of consumer reports per program, this metric will discuss how attackers lure users into downloading the rogue security software. Information about each of the top 50 programs will be analyzed to determine which advertising methods each program uses. The resulting data will be combined with the number of consumer reports to determine the prevalence of each advertising method during the reporting period. Advertising methods will include dedicated websites and advertisements on websites (either legitimate or illegitimate) such as social networking sites or blogs.

Rogue security software servers

The data collection and analysis for this section occurred over a period of two months in July and August, 2009. For the servers, data was collected and analyzed on "network observables" including IP addresses, DNS domain names, other DNS entries pointing to the same IP, geolocation information on IP addresses, server identification string and version number, ISP identity, DNS Registrar, DNS registrant information, uptime, and DNS-to-IP resolution changes and the speed with which such changes occurred. In total, 6,500 DNS entries pointing to 4,305 distinct IP addresses hosting rogue security software servers were analyzed.

Using a novel attack attribution method based on a multi-criteria fusion algorithm developed by Symantec and six other academic and industrial external partners as part of a research project, known as the Worldwide Observatory of Malicious Behaviors and Attack Threats (WOMBAT),[150] rogue security software domains were automatically grouped together based upon common elements likely due to the same root cause.[151] This method was used to identify patterns of various types of relationships among rogue security domains and the manner in which they operate, resulting in the creation of domain clusters.

150-WOMBAT is a three-year European Commission-funded project, which aims at providing new means to understand the existing and emerging threats that are targeting the Internet economy and its users. See http://www.wombat-project.eu/

151-For further details on this attack attribution method, please see "Addressing the attack attribution problem using knowledge discovery and multi-criteria fuzzy decision-making", http://www.eurecom.fr/util/publidownload.en.htm?id=2806

Credits

Marc Fossi

Executive Editor

Manager, Development

Security Technology and Response

Dean Turner

Director,

Global Intelligence Network

Security Technology and Response

Eric Johnson

Editor

Security Technology and Response

Trevor Mack

Editor

Security Technology and Response

Téo Adams

Threat Analyst

Security Technology and Response

Joseph Blackbird

Threat Analyst

Security Technology and Response

Mo King Low

Threat Analyst

Security Technology and Response

David McKinney

Threat Analyst

Security Technology and Response

Marc Dacier

Senior Director

Symantec Research Labs Europe

Angelos D. Keromytis

Senior Principal Software Engineer

Symantec Research Labs Europe

Corrado Leita

Senior Research Engineer

Symantec Research Labs Europe

Marco Cova

Ph.D. candidate

University of California Santa Barbara

Jon Orbeton

Independent analyst

Olivier Thonnard

Royal Military Academy, Belgium

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

10/2009 20100385