EXECUTIVE SUMMARY: SYMANTEC ENTERPRISE SECURITY

Symantec Report on Rogue Security Software

July 08 – June 09

Published October 2009

Confidence in a connected world.

symantec™

White Paper: Symantec Enterprise Security

Symantec Report on Rogue Security Software

Executive Summary

Contents

Introduction

The Symantec Report on Rogue Security Software is an in-depth analysis of rogue security software programs. A rogue security software program is a type of misleading application that pretends to be legitimate security software, such as an antivirus scanner or registry cleaner, but which actually provides a user with little or no protection and, in some cases, can actually facilitate the installation of malicious code that it purports to protect against.

The perpetrators of these rogue security software scams are well-equipped to prey on Internet users. Many of these scams are very lucrative and appear to be run by highly organized groups or individuals who maintain an effective distribution network bolstered by multi-level marketing efforts. These scams employ a full range of advertising and distribution techniques to ensnare potential victims, while offering substantial profit for scam distributors, given that advertised costs for these products range from $30 to $100.[1]

In total, Symantec has detected over 250 distinct rogue security software programs. During the period of this report, from July 1, 2008, to June 30, 2009,[2] Symantec received reports of 43 million rogue security software installation attempts from the over 250 distinct samples. Of the top 50 most reported rogue security software programs that were 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.

Overview of Rogue Security Software

Perpetrators of rogue security software scams use a wide variety of techniques to trick users into downloading and paying for these programs. Many of the methods use fear tactics and other social engineering methods that are distributed through spam, Web pop-up and banner advertisements, postings on forums and social networking sites, and sponsored or falsely promoted search engine results.[3] Scams have also been observed that exploit newer Internet phenomena such as tweeting and URL shortening services.[4]

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 botnet is used to do the work.[5] Web advertisements typically prey on users' fears of malicious code. Scam distributors also place these advertisements on major Internet advertising networks and with advertising brokers of legitimate sites in order to increase exposure and add an air of legitimacy to their scams.[6] Such exploits could 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, potentially restricting legitimate traffic. Attempts to falsely promote search engine results usually rely on exploiting popular news items, events, or celebrities.[7] Scam perpetrators use a range of black hat search engine optimization (SEO) techniques to effectively poison search engine results and increase the ranking of their scam websites whenever any topical news event is searched.[8]

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.

1-All currency in USD.
2-Except where otherwise noted.

There is also competition between scam distributors, with some scams advertising to remove rebranded versions of the same misleading application program or versions of others.[9] This often occurs once a rogue application becomes prevalent and other scam distributors advertise (misleading) applications that purport to remove the now widespread application.[10] Scam perpetrators seem unconcerned with creating the illusion of a trustworthy brand identity, but instead try to capitalize on the potential confusion resulting from the distribution of numerous rogue security products with similar names and interfaces.

Rogue security software typically gets onto a user's computer either by being downloaded and manually installed by the user (after being tricked into believing that the program is legitimate), or when the user unknowingly installs it, as occurs when the user opens an attachment or visits a malicious website designed to automatically download and install illegitimate applications. Once installed on a user's computer—and to induce payment—rogue security applications often misrepresent the computer's security status or performance, displaying fake or exaggerated claims of threats, even if the computer has not been compromised (figure 1).[11] 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

A major risk associated with installing a rogue security program 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 when, in reality, it is receiving little or no protection from threats. Some misleading applications may actually expose a computer to additional threats because they instruct users to lower existing security settings in order to advance the registration process. Some of these applications are also programmed to prevent a compromised computer from accessing legitimate security vendor websites, thus obstructing the victim's ability to research how to remove the misleading software. Another inherent risk is that, in addition to the immediate scam, the personal and credit card information that users provide if they register these fake products could be used in additional fraud or sold in the underground economy.[12]

To appear legitimate and fool potential victims, rogue security software programs are given valid-sounding names (e.g., Virus Remover 2008[13] or AntiVirus Gold[14]), or names that mimic existing legitimate security software (e.g., Nortel[15]). The websites, advertisements, pop-up windows, and notification icons used to market these scams are also designed to mimic

3-http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : pp 31 and 35
4-URL-shortening utilities provide a short alternative URL to users; the link will then redirect users to the actual site; users often do not know where the link will lead. See http://www.symantec.com/connect/blogs/tweeting-misleading-applications
5-Email addresses are inexpensive, costing as little as $0.33/MB on black market forums, with one MB containing as many as 40,000 email addresses. See http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf : p. 31, and http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 82
6-An advertising network is a distributor of advertisements to websites that want to host them; they typically have a large inventory of advertisements that are displayed each time a Web page is loaded or refreshed; the website will often not have control over the content of these advertisements.
7-http://www.symantec.com/connect/blogs/misleading-applications-show-me-money-part-2
8-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.
9-http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html
10-http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html
11-Ibid.
12-http://www.symantec.com/connect/blogs/misleading-applications-show-me-money

legitimate antivirus software programs (figures 1 and 2). The majority of these programs also have fully developed websites that include the ability to download and purchase the software.

Figure 2. AntiVirus 2009 Security Center (left) vs. legitimate Windows Security Center (right)

Courtesy: Symantec

Rogue security software programs are often rebranded or cloned versions of previously developed programs. Cloning is often done because the original version has been exposed by legitimate security vendors. Cloning is therefore fuelled by the hope that one or more of the clones will escape detection.[16] This process sometimes involves nothing more than changing out the name, logos, and images of a program while the program itself remains unchanged. Scam creators will also frequently change their domain registration information and company names to avoid being detected or profiled by security researchers or authorities.

Because of the often ill-defined legality of these scams, along with exploiting legitimate online advertising networks, perpetrators attempt to appear valid by using legitimate online payment services. The use of legitimate online payment services helps scam operators in multiple ways. First, these services facilitate gathering payments from victims who have been duped into purchasing a misleading application. Second, if victims see that the payment processor is legitimate, they may be slow to realize that they have been defrauded, allowing the scam perpetrator to operate undetected for longer. Because there is a constant threat that the payment service provider will discover that its service is being used for fraud, scam perpetrators want to avoid credit card chargebacks and payment reversals that may ultimately draw attention to the scam. This is another reason why rogue applications are often rebranded. Some scams actually return an email message to the victim with a receipt for purchase, complete with serial number and functioning customer service telephone number, which may further delay the victim becoming aware of the fraud.

There are also rogue payment processors that serve rogue security software affiliate networks.[17] Due to their illicit nature, these rogue payment processing services run a high risk of being shut down once their activities are discovered and are often short-lived, which may further explain why legitimate payment processors are attractive to scam operators.

13-http://www.symantec.com/security_response/writeup.jsp?docid=2008-072217-2258-99
14-http://www.symantec.com/security_response/writeup.jsp?docid=2006-032415-1558-99
15-http://www.symantec.com/connect/blogs/nort-what-av
16-http://www.symantec.com/connect/blogs/cloning-profit
17-http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

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 observed scams. Many of the samples discussed in this report are hosted on sites that website reputation services have flagged as having a reputation for malicious activity.[18] 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 security software and malicious code distribution operations. Exploits targeting client-side vulnerabilities are also present on some sites, which aid in drive-by downloads of malicious software and rogue security applications.

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.[19] 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 are an effective method of distributing rogue security software.

Although the reverse is not true, nearly all of the programs that used Web advertisements also used 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—used both a website and Web advertisements in addition to being distributed by malicious code 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.

A specific example of malicious code associated with rogue security software is the Zlob Trojan.[20] First identified in 2005, Zlob was the third most common staged downloader component observed by Symantec in 2008.[21] 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 trying to lure users into visiting specifically designed, malicious sites.[22] The top three rogue security applications observed by Symantec during this reporting period were all distributed in part by Zlob, as were a number of others. 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.[23] Vundo was the top-ranked malicious code sample observed by Symantec globally in 2007 and 2008.[24]

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. 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.

The creators of rogue security software scams often use an affiliate-based, pay-per-install model to distribute their misleading applications (figure 3). Those wanting to participate in these scams can register as an affiliate on a distribution site where they can then obtain the promotional and marketing materials to distribute and market the scams, including

18-http://safeweb.norton.com/

tools such as advertisements, malicious code executable files, and email templates, as well as obfuscation tools to help keep the scams from being exposed.

Figure 3. Traffic Converter website

Courtesy: Symantec

Making the rogue security software scam modular and comprised of re-usable components to perpetrate different variations of the same scam 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. Templates also allow for easy localization of scams for distribution in new markets.

Affiliate "master sites" such as TrafficConverter, Bakasoftware, 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.

While Symantec has observed localization of these scams into different languages to target different regions, the majority of scams observed target English-speaking users. For example, 61 percent of the rogue security software scams observed by Symantec during this period were attempted on users in the North America region, where English is the first language for the prominent majority of people (figure 4).

19-Many scams use a variety of methods for promotion, including websites and website advertisements.
20-http://www.symantec.com/security_response/writeup.jsp?docid=2005-042316-2917-99
21-http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 62
22-Ibid. : p. 31
23-http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99
24-http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf : p. 60

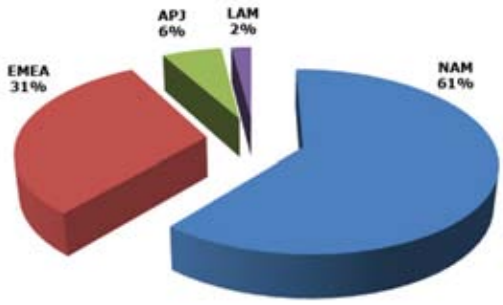

Figure 4. Percentage of rogue security software distribution, by region[25]

Source: Symantec

Affiliate distributors of these scams are paid a predetermined amount for every successful installation, ranging from $0.01 to $0.55 (table 1). Payouts vary based on the geographical location, the type of installation, and the distribution website. The observed payout rates also indicate that English-speaking regions are the overwhelming target of the scams, as indicated by English being the first language in the top four ranked countries in this measurement and that the payout rates for these four are significantly higher than for any other country. Affiliates are also offered incentives, 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.

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

Source: Symantec

While most domain names are linked to a single Web server, 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. Of the servers that were geographically located by Symantec during a two-month period in 2009, the United States accounted for 53 percent of the servers hosting rogue security software, far more than any other country (table 2).

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 2. Servers hosting rogue security software, by country

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 (figure 5). The 310 domain names (in blue) point to 13 IP addresses residing in 5 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. The registrants also make use of domain registration services that can either protect registrant privacy or ones that do not verify identities and email addresses.

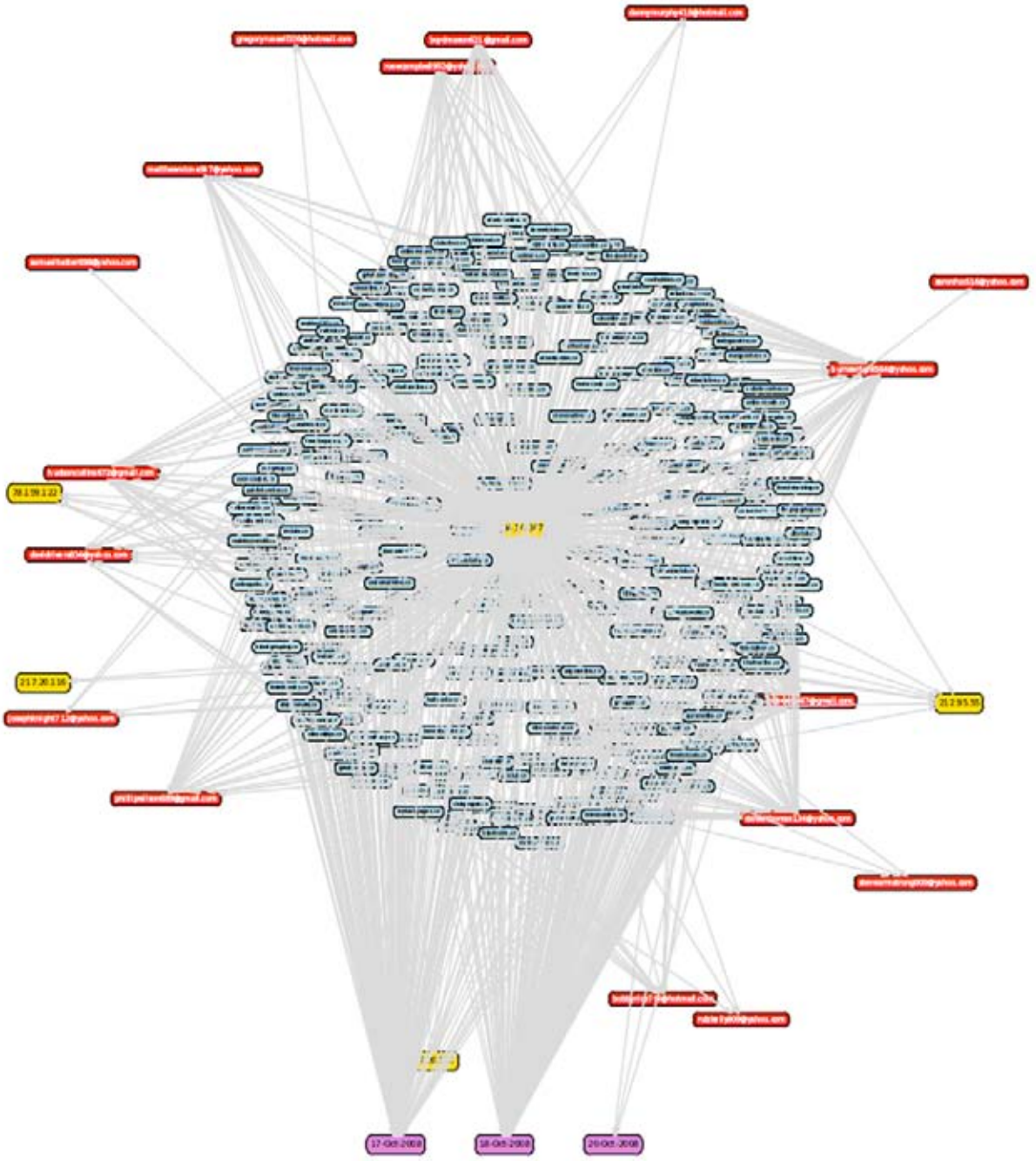

Figure 5: Cluster of 310 domain names registered within three days

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. It should be noted that the .cn top-level domain has no registration restrictions and non-Chinese based operators can register a .cn domain name. In the case 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.

Conclusion

As with the increasing danger posed by many of the security threats on the Internet today, given the sophistication of many of these scams and the challenges of mitigation, Symantec believes that a hybrid approach to protecting against rogue security software scams is necessary. While actions such as whitelisting and blacklisting can improve protection, they are just one measure against the profusion of URLs that have been detected hosting rogue security applications. Symantec is working towards creating an online environment that will enable users to supplement protection with reputation-based security techniques whenever possible. This would see applications earning a reputation value through the collective consensus of the online community, improving the ability of users to gauge the validity and safety of any application and, thus, significantly improving the capability of users to defend against scams such as rogue security applications.

To continue to protect against rogue security software, Symantec recommends that users always follow best practices for protection and mitigation. These are outlined in Appendix B of the Symantec *Report on Rogue Security Software*. Specifically, users should invest in and install only proven, trusted security software from reputable security vendors whose products are sold in legitimate retail and online stores.

Highlights

- During this reporting period, Symantec received reports of 43 million rogue security software installation attempts from the over 250 distinct such programs identified
- Rogue security applications are often distributed on websites that appear legitimate
- Black hat search engine optimization operations are conducted to push sites that host rogue security applications to the top of search engine indexes. Scam operators capitalize on interest in current events to lure users to websites that host rogue security software
- Symantec estimates that the initial monetary loss to consumers who downloaded and purchased these misleading applications during this reporting period ranged from $30 to $100.
- Among the distribution sites Symantec observed for this report, the highest payouts to affiliates for installations by users were in the United States, where payouts averaged $0.55 per installation; next highest were the United Kingdom and Canada, where payouts averaged $0.52 per installation in each; Australia ranked fourth, where payouts averaged $0.50 per installation.
- One distribution site observed by Symantec, TrafficConverter.biz, purported to have its 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.
- The top five reported rogue security applications observed by Symantec during this reporting period were, in order, SpywareGuard 2008, AntiVirus 2008, AntiVirus 2009, Spyware Secure, and XP AntiVirus.
- Of the top 50 reported rogue security applications during this reporting period, 61 percent of the scams observed by Symantec were attempted on users in the North America region, 31 percent occurred in the Europe, the Middle East, and Africa region, six percent occurred in the Asia-Pacific/Japan region, and two percent occurred in the Latin America region.
- The most common distribution method observed by Symantec during this reporting period was intentional downloads, which were employed by 93 percent of the attempts of the top 50 rogue security software scams; unintentional downloads were employed in 76 percent of the observed attempts. (Note: many scams employed both methods.)
- The most common advertising method used by the top 50 rogue security software programs that Symantec observed during this reporting period was dedicated websites, which were used in 93 percent of scams; the second most common advertising method was Web banner advertisements, which were used in 52 percent of the attempted rogue security software scams. (Note: many scams employed multiple methods.)
- Of the servers hosting rogue security applications that were observed by Symantec during a two-month reporting period (July to August, 2009), 53 percent were located in the United States; Germany ranked second in this measurement, with 11 percent. Symantec identified 194,014 domain names associated with rogue security applications during the same two-month observation period.
- Of the observed rogue security software domains in that two-month period, 26 percent of the total served malicious content of various types, 13 percent attempted to use browser exploits, one percent attempted to perform drive-by downloads, and less than one percent led to the installation of spyware on a user's computer. (Note: a given Web server could belong to several categories.)

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
Universite 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 20326021