WHITE PAPER: SYMANTEC INTELLIGENCE Q4 2010 REPORT

# Symantec Intelligence Quarterly Report: October - December, 2010

## Targeted Attacks on Critical Infrastructures

Confidence in a connected world. Symantec.

White Paper: Symantec Intelligence Q4 2010 Report

# Symantec Intelligence Quarterly Report: October - December, 2010

## Targeted Attacks on Critical Infrastructures

**Contents**

## Introduction to Targeted Attacks

Targeted attacks occur when malicious code and threats are developed for and directed at specific individuals, organizations, corporations, or sectors. Attackers gather information on the target in order to focus attacks to their specifications prior to sending out the malicious code. The customization of targeted attacks can make them more dangerous than non-targeted attacks because they are tailored explicitly to affect a target group. For example, attackers could target senior employees at a financial institution who have access to confidential information. In the case of a data breach, attackers could take advantage of the leaked sensitive information to craft an attack that would lure victims to unwittingly download malicious code or to divulge even more information.

Commonly known as advanced persistent threats (APTs), targeted attacks can be as easy as using a spoofed email address to send email messages to addressees with the domain name of a company or customers of a specific institution. The email messages would have been written using social engineering techniques and, as such, typically have a sense of urgency or importance associated with them to coerce the recipient to open the malicious attachments. The email messages often contain legitimate details, such as references to real organizations or news events, to give them the appearance of authenticity. For example, attackers could use a spoofed email address of an IT security manager to send out email to employees about a potential security issue, or else masquerade as an HR manager requesting that employees verify payroll credentials included in an attachment. As with many targeted attacks, the attacker sends out only a limited number of emails in order to avoid attracting too much attention and therefore alerting security personnel to the potential threat.

Targeted attacks are also known to use phishing campaigns that direct the recipient to a malicious website, at which point the victim is exposed to malicious code, either from code embedded in the site itself or via a program or file they are encouraged to download.[1]An example of this type of attack is found with the cybercriminals peddling rogue security software, who rely on these phishing campaigns a great deal. Ironically, they exploit users' fear of being exposed to malicious code threats to expose them to malicious code, since the rogue antivirus programs that users are offered for free from these sites often contain malicious payloads.

Motivations for such customized attacks can range from stealing confidential information such as account credentials for profit, to interfering with day-to-day operations, to mischief. In many instances, attackers only need to compromise one vulnerable computer to gain access to an organization's network. They can then use the compromised system as a launching point for subsequent attacks.

Targeted attacks against critical infrastructure sectors are especially dangerous because the attacks are tailored to disrupt specific organizations that may be essential to the functioning of a country's society. Examples of critical infrastructure sectors include transportation, communication, and utilities. This section will discuss two prominent recent attacks: The Hydraq Trojan and the Stuxnet worm.

1-Also known as spear phishing or targeted phishing

## Trojan Hydraq – One Year Later

Trojan Hydraq,[2] also known as Aurora, was first discovered on January 11, 2010, when it was used as part of a targeted attack, likely in an attempt to gain access to a corporate network and steal confidential information.[3] Hydraq entered computers via email attachments or was downloaded by other threats, such as via malicious websites. It allowed attackers to compromise systems by exploiting a zero-day vulnerability in client-side software.[4] Once executed, the Trojan installed a backdoor that allowed an attacker to control the computer and perform a variety of compromising actions. These included modifying, executing, and deleting files; executing malicious files; and, most importantly, gaining access to the compromised corporation's network—which then opened up the target to additional attacks. As with other common Trojans, Hydraq would attempt to remotely contact its command and control (C&C) server via a number of URLs in order to receive updates and further instructions.[5]

The number of infections from Hydraq was limited due to the nature of the targeted attacks—only a small number of corporations were targeted (figure 1). Another factor limiting the number of infections is that attackers often prefer to avoid attracting attention by limiting their attacks and, thus, remain concealed on a small volume of computers as long as possible, rather than risk exposing themselves by compromising too many at once.[6] Finally, Trojan Hydraq thwarted antivirus sensors because it contained an obfuscation technique called "spaghetti code" in which blocks of code of the Trojan are rearranged to avoid detection.[7]

Once a targeted attack is discovered, it becomes less effective due to increased awareness and the adoption of increased security measures, such as updating patches and sanitizing infected machines. As such, the longevity of Hydraq was short-lived, peaking in January 2010 and subsequently tapering off after February 2010.

[2] Please see http://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99 and http://www.symantec.com/outbreak/index.jsp?id=trojan-hydraq
[3] http://www.symantec.com/connect/blogs/trojanhydraq-incident
[4] http://www.securityfocus.com/bid/35759
[5] http://www.symantec.com/connect/blogs/trojanhydraq-incident
[6] http://www.symantec.com/connect/blogs/hydraq-attack-mythical-proportions
[7] http://www.symantec.com/connect/blogs/seeing-past-trojanhydraq-s-obfuscation

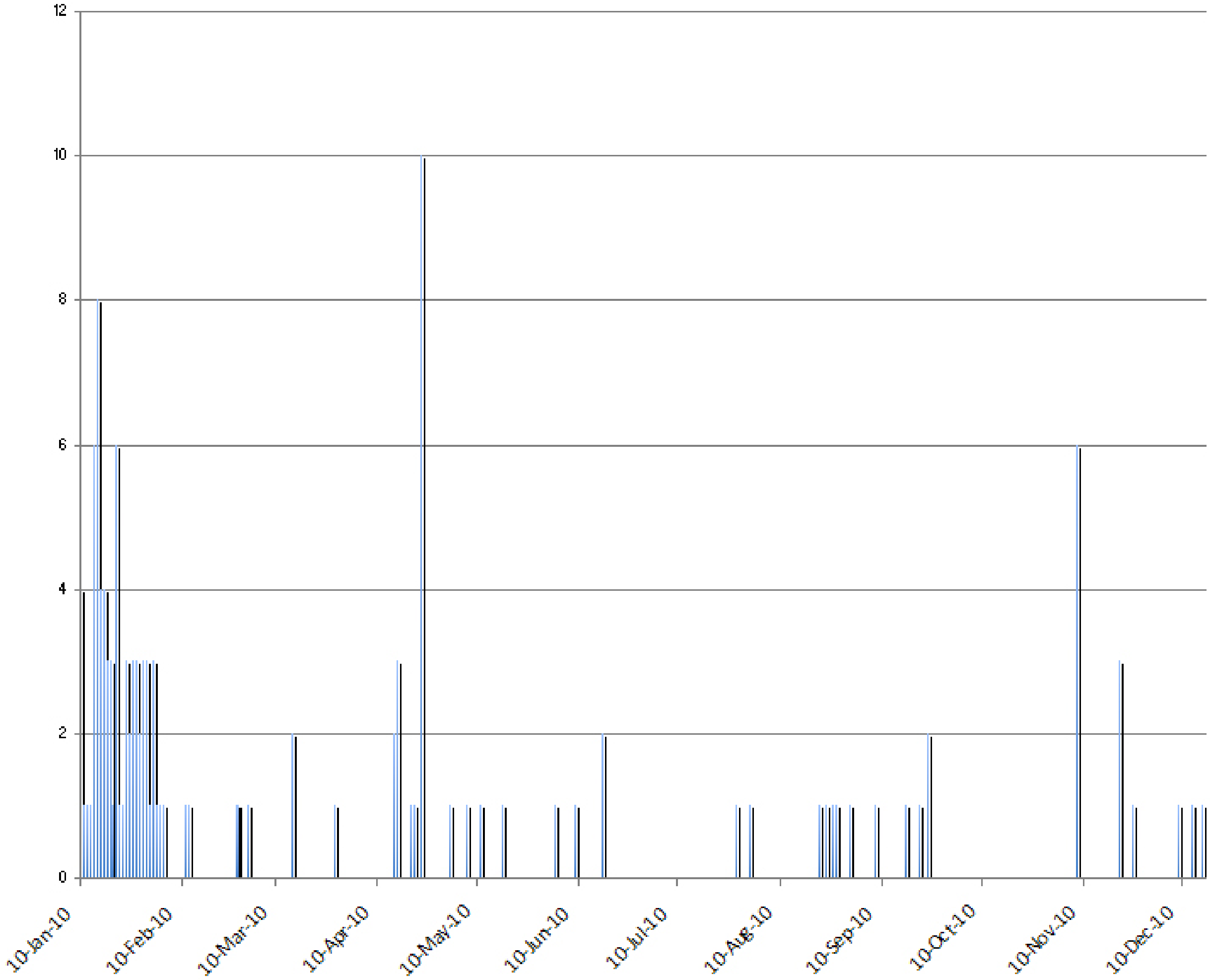

**Figure 1: Attempted Trojan Hydraq infections by month. (Source: Symantec Corporation)**

## The Stuxnet Worm

The Stuxnet worm first garnered international attention in July 2010 when it was linked with attacks that targeted industrial control systems such as power plants and gas pipelines (figure 2).[8] The worm infected at least 15 control systems in factories around the world, including in Germany and in a number of personal computers within Iran's Bushehr nuclear power plant.[9] It was also announced that the worm had affected the software used in centrifuges involved in Iran's uranium enrichment program.[10]

Stuxnet was designed to target its attack on particular industry control systems—specifically, programmable logic controllers (PLCs)—and to change the code to modify the frequency converter drives of the controller.[11] The worm was the first to simultaneously exploit four zero-day vulnerabilities in its attacks.[12] It also used stolen digital certificates to sign and legitimize the malicious files.[13] This type of attack demonstrated that the authors of Stuxnet had deep knowledge of their targets, and the control systems and processes of those targets.

8-http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99
9-Please see http://www.bbc.co.uk/news/technology-11388018, http://www.nytimes.com/2010/09/27/technology/27virus.html?_r=1, and http://www.wired.com/threatlevel/2010/11/stuxnet-sabotage-centrifuges/
10-http://af.reuters.com/article/energyOilNews/idAFLDE6AS1L120101129
11-http://www.symantec.com/connect/blogs/stuxnet-breakthrough
12-http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities
13-http://www.symantec.com/connect/blogs/hackers-behind-stuxnet

Stuxnet was especially dangerous because it was able to infect systems via removable flash drives—in other words, systems that were not normally connected to the Internet—and it was able to hide injected code located on a PLC. Elevating the threat was the fact it was able to update itself using a P2P component in its code. Using a P2P network makes it very difficult to take the threat offline, because there are no central control servers. Auto-propagation methods allowed the Stuxnet worm to thrive and operate for a longer period of time compared to, say, Trojan Hydraq. One method of propagation Stuxnet used was to copy itself onto network-shared drives that were protected by weak passwords.[14]

Since the worm did not collect personal information, such as financial information or account logins, nor did it herd infected systems into a botnet, possible motivations for Stuxnet may have been either sabotage or the extortion of a specific target. For more detailed information on Stuxnet, please see the latest version of Symantec's dossier on the subject.[15]

[14]-http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99
[15]-http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

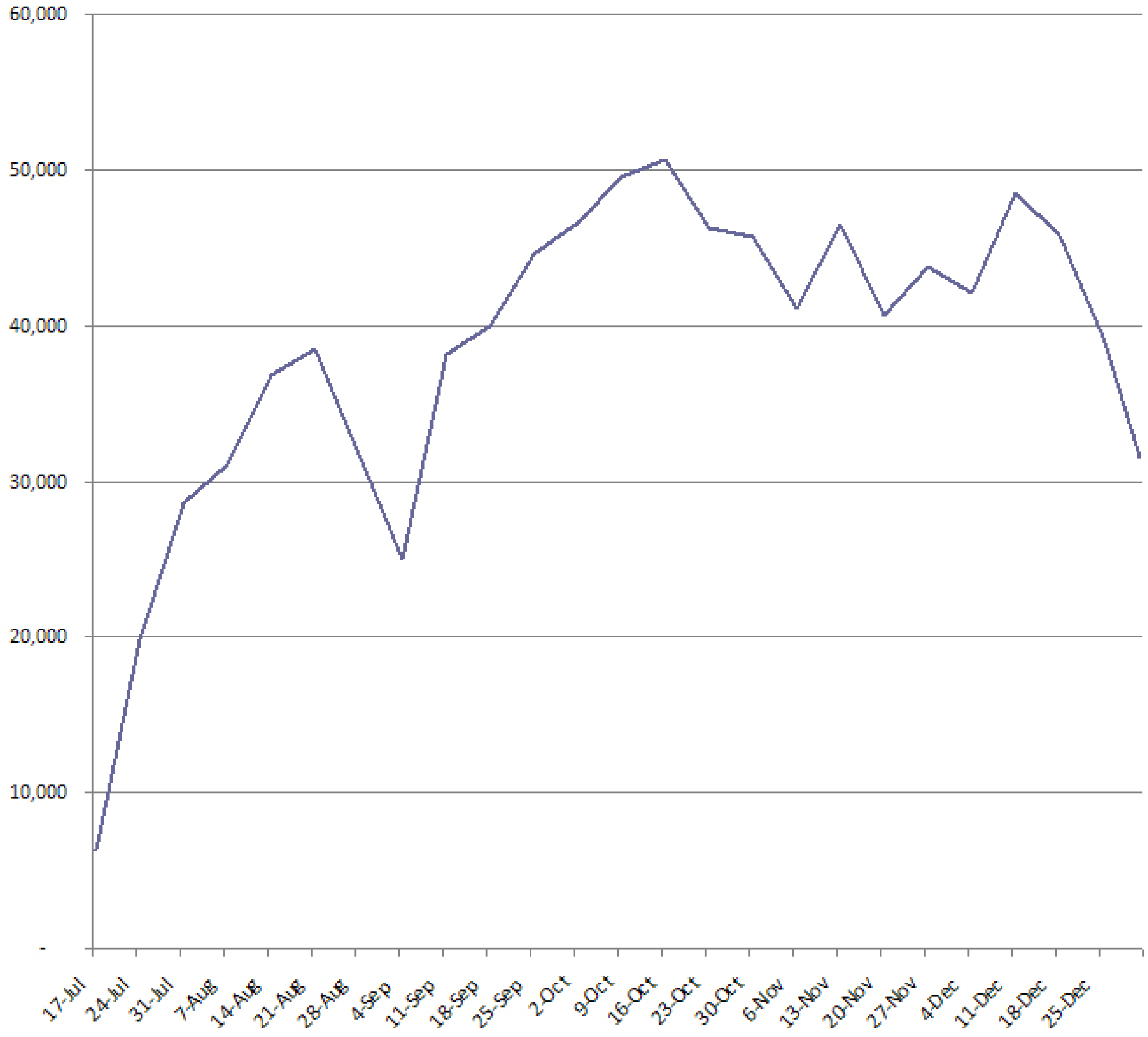

**Figure 2: Attempted Stuxnet worm infections by month. (Source: Symantec)**

## Vulnerabilities in SCADA Systems

SCADA (Supervisory Control and Data Acquisition) represents a wide range of protocols and technologies for monitoring and managing equipment and machinery in various sectors of critical infrastructure and industry, such as those used for power generation and distribution. Therefore, the security of SCADA technologies and protocols is a particular concern of governments because the disruption of related services can result in the failure of infrastructure and the potential loss of life, among other consequences.

This discussion is based on data surrounding publicly known vulnerabilities affecting SCADA technologies. The purpose of this section is to provide insight into the state of security research in relation to SCADA systems. To a lesser degree, this may also provide insight into the overall state of SCADA security. Vulnerabilities affecting SCADA systems may present a threat to critical infrastructure that relies on these systems. Due to the potential for disruption of critical services, these vulnerabilities may be associated with politically motivated or state-sponsored attacks. This is a concern for governments and enterprises that are involved in the critical infrastructure sector. While this discussion provides insight into public SCADA vulnerability disclosures, due to the sensitive nature of vulnerabilities affecting critical infrastructure, there is likely private security research conducted by SCADA technology and security vendors. Symantec does not have insight into any private research because the results of such research are not publicly disclosed.

In the fourth quarter of 2010, Symantec documented 10 public SCADA vulnerabilities; a total of 15 SCADA vulnerabilities were documented for all of 2010. The number of vulnerabilities reported in SCADA technologies is typically very small because SCADA is currently a very niche area of security research. Only a small proportion of the security community is involved in researching SCADA security vulnerabilities; the resources and access to technologies remain a challenge for lab testing by security researchers. However, attackers with malicious intent are able to target live systems and apply their existing knowledge of security vulnerabilities and exploits to these systems. Examples of such vulnerabilities include:

- A total of three Web application vulnerabilities were discovered in the Intellicom Netbiter webSCADA WS100 and WS200 products.[16] The vulnerabilities can allow attackers to upload and execute arbitrary script code and may also allow access to potentially sensitive information.
- An SQL-injection vulnerability affecting the login page of the Industrial Technology System (ITS) SCADA system was discovered and may allow attackers to compromise the application by making unauthorized changes to the underlying database.[17]
- There were three remote buffer-overflow vulnerabilities discovered in the DATAC RealWin SCADA server.[18]Attackers can exploit these vulnerabilities to execute code on the servers.
- Three vulnerabilities were discovered in Ecava IntegraXor, including two remote code-execution vulnerabilities and a directory-traversal vulnerability.[19]These issues can be exploited by attackers to execute arbitrary code or to access potentially sensitive information that may aid in further attacks.

Web application vulnerabilities (such as the first four vulnerabilities above) are often easy for attackers to discover and exploit. Additionally, many SCADA implementations, such as the DATAC RealWin SCADA server, run on Microsoft Windows or other widely deployed operating systems and employ Web applications and browser plug-ins for their functionality. This can make it is easier for attackers to generalize their existing skills to target these technologies.

While security researchers have pinpointed vulnerabilities specific to SCADA technologies, there is also a potential threat from vulnerabilities in components connected to SCADA systems. This can include operating systems hosting the SCADA technologies or other components such as database software. Network-accessible devices may use either common or specialized networking protocols that are prone to attacks, which may compromise the availability and integrity of affected devices. Therefore, malicious or otherwise malformed network traffic may affect these devices in a manner similar to other network-accessible services within the enterprise. Additionally, many SCADA environments employ legacy technologies that are not equipped with mechanisms for authentication or measures to ensure the availability, integrity, and confidentiality of data. These systems may be particularly at risk, especially if they are not fault-tolerant or designed to handle exceptional conditions such as malformed input.

16-http://www.securityfocus.com/bid/43636
17-http://www.securityfocus.com/bid/43680
18-http://www.securityfocus.com/bid/44150
19-Please see http://www.securityfocus.com/bid/45487, http://www.securityfocus.com/bid/45535, and http://www.securityfocus.com/bid/45549

Testing these technologies in a lab environment is a challenge for security researchers due to limited resources and access to the necessary equipment. As a result, this can hinder the preemptive discovery of potential vulnerabilities. However, attackers with malicious intent can target live systems in the wild and apply their existing security knowledge to the systems with little regard for any unintended repercussions.

## Real-World Implications of Targeted Attacks on Critical Infrastructure

Industrial control systems (ICS), such as SCADA, are used by the critical infrastructure sector to control the processes for daily operations. They are essential for gathering and processing information sent by sensors and sending out the appropriate commands that control local operations. In addition, ICS are crucial for monitoring plant and station environments to ensure they are working under safe conditions. If required, the control systems send out commands to protect the local environment and prevent any emergency situations, such as the overheating of machinery, increased levels of toxic gases, fire, or potential power grid overloads. The commands can be sent to shut down systems, isolate zones, open pressure valves, or take other safety measures. When ICS fails to function as intended, these problems can go unnoticed.

In July 2010, for example, a SCADA system used to monitor water pumps failed to report that water storage levels for a residential water supply were extremely low.[20] This resulted in city residents being unable to access water from their faucets. Although the problem was identified quickly and the supply was replenished after just a few hours, this illustrates how an attacker could hamper basic essential services by attacking these systems.

There are many different causes of ICS-related incidents, such as inadvertent administrative mistakes or errors during system updates, insider attacks, and mischief. The risks of industrial sabotage or state-sponsored attacks aimed at disrupting critical infrastructure are the most concerning. These types of threats could have potentially devastating outcomes if successfully executed.

Disabling system safeguards and triggering actions outside of intended operation can result in permanent physical damage to machinery and other equipment as well as the facilities that house them. Should extensive damage affect a system such as the water storage supply discussed above, residents of a city could be forced to go without accessible potable water for extended periods of time. Despite being an electronic attack, this would put a burden on emergency services and other aid organizations. This would also cause significant financial setbacks while equipment is repaired or replaced. Other scenarios could result in blackouts of power grids and communication networks. In more extreme examples, machinery failure could cause fire, explosions, or release harmful toxins that could damage the environment or cause the loss of life. The implication of these attacks is very important because they effectively represent a much larger target than the vulnerable system itself.

Although the ICS security community has been actively growing, there may be a significant amount of catching up to do across the numerous industries that use the technology. Awareness and proactive research and development by security communities can only culminate in real success through the adoption of effective mitigation and prevention measures in environments outside the lab.

Past targeted attacks, such as Trojan Hydraq and the Stuxnet worm, are important because they demonstrate that there are vulnerabilities in critical infrastructure sectors—specifically, in the power and energy sectors. The Stuxnet attacks

[20]-http://www.isssource.com/incident-report-scada-water-system-fails/

were the first ones that specifically targeted ICS.[21]This is significant because it is an actual event of what was formerly just a plausible scenario.

Despite being isolated from external networks, the affected systems became infected with malicious code, which caused damage to the systems.[22]To repair the damage, systems were taken off-line and shut down, resulting in production and revenue loss, and increased manpower to fix the issues.[23]In addition, the malicious code could be indiscriminate in its attacks, causing widespread collateral damage to other non-targeted systems. In the case of Stuxnet, the worm infected over six million computers in China.[24]

An important implication of targeted attacks on ICS, specifically Stuxnet, is that the attackers who crafted the malicious code were able to exploit and take advantage of a wide variety of vulnerabilities affecting these systems. The Stuxnet worm developers may have helped to pave the way for others to cultivate more sophisticated attacks or inspire copycat targeted attacks. Other attackers could reverse engineer the Stuxnet worm and use it as a template for future attacks. Or, they could use variations of the worm to launch attacks that disrupt other critical infrastructures, such as utilities, power grids, or oil and gas refineries. Targeting the latter could leave cities and communities in emergency situations.

21-http://www.symantec.com/connect/blogs/stuxnet-breakthrough
22-http://www.businessweek.com/ap/financialnews/D9JLF8F03.htm
23-http://www.nytimes.com/2010/11/30/world/middleeast/30tehran.html?_r=2&hp
24-http://news.xinhuanet.com/english2010/china/2010-10/01/c_13538835.htm

## Mitigation & Protection

To limit exposure to attacks, networks running SCADA protocols and devices should be isolated from other networks. These assets should not be connected to the Internet or other networks unless strictly required. If this is not possible, to completely limit access by external networks, network access should be strictly regulated by limiting incoming/outgoing traffic to required protocols only. IPSec and VPNs can also be deployed to limit access to authorized networks and individuals. A defense-in-depth strategy should be deployed so that security risks elsewhere in the organization cannot affect the control network. Additional layers of defense should be deployed to protect key assets. Endpoint security products may provide an additional level of protection for hosts within the SCADA environment that run commonly available commercial operating systems.

Securing a SCADA environment may present different challenges than those faced when securing an enterprise. In many cases, it may not be possible to create a test environment for auditing purposes. Furthermore, any disruption of services may be costly or damaging. Therefore, both passive asset discovery as well as vulnerability scanning technologies are best applied to limit the potential for side effects. Antivirus and patch management measures should be undertaken with care and organizations should consult security and control system vendors for support in applying these solutions in a manner that minimizes risk and downtime. Policy compliance and auditing should ensure that configuration benchmarks and security baselines are enforced through the organization and especially on critical control systems. Intrusion detection and prevention systems should be deployed to monitor and prevent attacks on critical systems and networks.

## Credits

**Marc Fossi**

Executive Editor

Manager, Development

Security Technology and Response

**Gerry Egan**

Director, Product Management

Security Technology and Response

**Eric Johnson**

Editor

Security Technology and Response

**Trevor Mack**

Associate 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

## 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. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

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

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security**, and **application security** solutions.

1/2011 21169903