Prepared Testimony and
Statement for the Record of

Dean Turner
Director, Global Intelligence Network,
Symantec Security Response
Symantec Corporation

Hearing on

Securing Critical Infrastructure in the Age of Stuxnet

Before the

United States Senate
Committee on Homeland Security
And Governmental Affairs

November 17, 2010
342 Dirksen Senate Office Building

INTRODUCTION

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, thank you for the opportunity to appear here before you today to discuss the Stuxnet worm and the important topic of securing the industrial control systems that underpin our nation's critical infrastructure.

My name is Dean Turner and I am the Director of Symantec's Global Intelligence Network which is part of Symantec Technology and Security Response[1]. My primary responsibilities include managing Symantec's DeepSight[2] Analyst teams and security intelligence. I also co-author and manage Symantec's *Internet Security Threat Report* which is a trusted source of global research and analysis of cyber attack data gathered from our DeepSight Threat Management System, Managed Security Services, Business Intelligence Services and Antivirus Research Automation.

As the global information security leader, Symantec protects more people and businesses from more online threats than anyone in the world. Our best-in-class Global Intelligence Network[3] allows us to capture worldwide security intelligence data that gives our analysts an unparalleled view of the entire Internet threat landscape including emerging cyber attack trends, malicious code activity, phishing and spam. We maintain eleven Security Response Centers globally and utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year. In short, if there is a class of threat on the Internet, Symantec knows about it.

Critical infrastructure protection is a top priority at Symantec as we are committed to assuring the security, availability and integrity of our customers' information. We believe that critical infrastructure protection is an essential element of a resilient and secure nation. From water systems to computer networks, power grids to cellular phone towers, risks to critical infrastructure can result from a complex combination of threats and hazards, including terrorist attacks, accidents, and natural disasters.

Symantec welcomes the opportunity to provide comments as the Committee continues its important efforts to ensure that adequate policies and procedures are in place, both in the private sector and in the federal government, to monitor and secure these critical systems from cyber attack. In my testimony today, I will provide the Committee with:

- Symantec's latest assessment of the Stuxnet worm including an analysis of the threat that this malware poses to Industrial Control Systems;

---

[1] 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. More information is available at www.symantec.com.

[2] Symantec™ DeepSight™ Threat Management System provides actionable intelligence covering the complete threat lifecycle, from initial vulnerability to active attack. With personalized notification triggers and expert analysis, the system enables enterprises to prioritize IT resources in order to better protect critical information assets against a potential attack. Powered by the Symantec Global Intelligence Network, the service is an authoritative source of tailored information about known and emerging vulnerabilities, threats, risks and global attack activity.

[3] Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec Global Intelligence Network. This network captures worldwide security intelligence data that gives Symantec analysts unparalleled sources of data to identify, analyze, deliver protection and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. More than 240,000 sensors in 200+ countries monitor attack activity through a combination of Symantec products and services as well as additional third-party data sources.

- Our Insights into the major challenges and vulnerabilities associated with better securing the critical infrastructure from cyber attacks in the future;
- Observations on how the public and private sector can better secure these systems; and
- Several policy recommendations for the Committee's consideration to enhance the nation's critical infrastructure preparedness and resilience.

THE STUXNET WORM

I begin my testimony today by providing Symantec's observations of the Stuxnet worm as well as offering some insights on the implications that this threat poses to the nation's industrial control systems. As the Committee is aware, Stuxnet is a Windows-specific computer threat first discovered in June 2010. It is the first threat that Symantec has identified that spies on and reprograms industrial control systems, and is also the first to include a programmable logic controller (PLC) rootkit and, the first to target critical industrial infrastructure. It was written specifically to attack Industrial Control Systems used to control and monitor industrial processes, and not only can it reprogram PLCs, but also it can hide the changes.

Stuxnet is an incredibly large and complex threat. In fact, it is one of the most complex threats that we have analyzed to date at Symantec. I would like to draw the Committee's attention to a recent Symantec research paper entitled, *W32.Stuxnet Dossier*[4], in which we provide a detailed examination of Stuxnet and its various components with a particular focus on analyzing the final goal of Stuxnet, which we believe is to reprogram industrial control systems.

Symantec examined each of the different components of Stuxnet in an effort to better understand how the threat works in detail while keeping in mind that the ultimate goal of the threat is the most interesting and relevant part of the threat. Stuxnet is a threat targeting a specific industrial control system, such as a gas pipeline or power plant. To date, the majority of infected systems appear to be in Iran. We speculate that the ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries, and to hide those changes from the operator of the equipment.

In order to achieve this goal, the creators of Stuxnet amassed a vast array of components to increase their chances of success. This includes zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface.

Industrial control systems are automated through special code contained in the PLCs—for instance, to operate and control machinery in a plant or a factory. Stuxnet can steal code and design projects and also hide itself using a classic Windows rootkit, but unfortunately it can also do much more. Stuxnet has the ability to take advantage of the programming software to also upload its own code to the PLC in an industrial control system that is typically monitored by SCADA systems. Stuxnet effectively hides certain programming code, so when a programmer using an infected machine tries to view all the code on a PLC, they will not see the code injected by Stuxnet. Thus, Stuxnet isn't just a rootkit that hides itself on Windows, but is the first publicly known rootkit that is able to hide injected code located on a PLC.

---

[4] Nicolas Falliere, Liam O Murchu, and Eric Chien, "*W32.Stuxnet Dossier*," September 20, 2010, version 1.0, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf .

In particular, Stuxnet hooks the programming software, which means that when someone uses the software to view code blocks on the PLC, the injected blocks are nowhere to be found. This is done by hooking enumeration, read, and write functions so that you cannot accidentally overwrite the hidden blocks as well. Stuxnet contains 70 encrypted code blocks that appear to replace some "foundation routines" that take care of simple yet very common tasks, such as comparing file times and others that are custom code and data blocks. Before some of these blocks are uploaded to the PLC, they are customized depending on the PLC.

By writing code to the PLC, Stuxnet can potentially control or alter how the system operates. A previous historic example[5] includes a reported case of stolen code that impacted a pipeline. In this case, code was secretly "Trojanized" to function properly and only some time after installation it instructed the host system to increase the pipeline's pressure beyond its capacity. This resulted in a three kiloton explosion, about one-fifth the size of the Hiroshima bomb.

STUXNET'S THREAT TO ICS SYSTEM SECURITY

Stuxnet demonstrates the vulnerability of critical national infrastructure industrial control systems to attack through widely used computer programs and technology. Stuxnet is a wake-up call to critical infrastructure systems around the world. This is the first publicly known threat to target industrial control systems and grants hackers vital control of critical infrastructures such as power plants, dams and chemical facilities. Stuxnet also represents the first of many milestones in malicious code history – it is the first to: exploit four zero-day vulnerabilities, compromise two digital certificates, and inject code into industrial control systems and hide the code from the operator – all in one threat.

Whether Stuxnet will usher in a new generation of malicious code attacks towards real-world infrastructure—overshadowing the vast majority of current attacks affecting more virtual or individual assets—or if it is a once-in-a-decade occurrence remains to be seen. Stuxnet is of such great complexity—requiring significant resources to develop—that a select few attackers would be capable of producing a similar threat, to such an extent that we would not expect masses of threats of similar sophistication to suddenly appear. However, Stuxnet has highlighted that direct-attacks to control critical infrastructure are possible and not necessarily spy novel fictions. The real-world implications of Stuxnet are beyond any threat we have seen in the past. Symantec was able to reverse engineer Stuxnet in order to better understand its purpose.

The intended target of Stuxnet is not known. Short of finding out the exact hardware configuration of every ICS system in the world we cannot be sure of the true extent of Stuxnet's victims. Speculation pointing to Iran as the likely target is just that–speculation. The large number of Stuxnet infections in that country may merely be a consequence of other factors. It is unknown who exactly is behind the Stuxnet attack. We know even less about who could have written Stuxnet than the target itself. Portions of Stuxnet's code that suggest authorship are vague at best; there is nothing in the code that could be taken to be a definitive link to anyone. What we *do* know is that whoever was behind it had good knowledge of ICS systems, particularly those they targeted. In addition, using so many un-patched vulnerabilities in just one malware family is unheard of outside of Stuxnet, again suggesting that these authors are more sophisticated than the typical cybercriminal gangs or attackers.

Without better knowledge of the persons behind these attacks, it is nearly impossible to say with any certainty who was responsible and possible motives behind the attack. The combination of sophisticated attacker and

[5] Nicolas Falliere, "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems," August 10, 2010, http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices.

target means that any guesses of who was behind this is nothing more than speculation. However, the implications of Stuxnet's ability to modify commands sent to SCADA systems are significant. Industrial control systems under SCADA control that were targeted by Stuxnet could be damaged or outright destroyed, depending on the modified commands sent.

PROTECTING ICS NETWORKS AGAINST STUXNET AND FROM SIMILAR THREATS

The first obvious measure to protecting ICS networks from Stuxnet and similar threats is to deploy an anti-malware solution, and assure it is kept up to date. Of course, many SCADA systems today need to be modernized in order to even be capable of receiving anti-malware solutions. A good place to start in modernizing an SCADA system is with incorporation of Web-based capabilities. The functionality standard in web-enabled HMI workstations today significantly surpasses those of only a few years ago. Newer units can be configured to perform sophisticated notification of incidents and to respond automatically with cellular text messages, email or autodial phone calls. Such can simplify remote location monitoring and allow operators to respond to threats in a quicker fashion.

However, anti-malware alone does not provision the entire security landscape. The second most important element is to watch out for vendor security notifications and alerts, and to apply patches or workarounds as soon as possible. Next, ensure that users are kept up to date through a security education and awareness program. Last, but not least, know your assets, identify your perimeter of secure operations, and maintain a high level of situational awareness to ensure you are aware of, and can respond to, incidents in a timely manner for the sake of operational survival.

ENSURING RESILIENCY AGAINST CRITICAL INFRASTRUCTURE CYBER ATTACKS

Yes, Stuxnet is very sophisticated; and yes, it has the potential to cause damage. But it also has several weaknesses. First, it was found; second, it was highly specific; and third, that level of sophistication does not come cheap and may be difficult to replicate. But these weaknesses are not reasons for complacency. There is much we can learn from this attack and much we can do to lessen the impact of a similar attack. Symantec recommends the following steps be taken in order to better protect critical systems from cyber attack:

- **Develop and enforce IT policies** and automate compliance processes. By prioritizing risks and defining policies that span across all locations, organizations can enforce policies through built-in automation and workflow and not only identify threats but remediate incidents as they occur or anticipate them before they happen.
- **Protect information** proactively by taking an information-centric approach. Taking a content-aware approach to protecting information is key in knowing who owns the information, where sensitive information resides, who has access, and how to protect it as it is coming in or leaving your organization. Utilize encryption to secure sensitive information and prohibit access by unauthorized individuals.
- **Authenticate identities** by leveraging solutions that allow businesses to ensure only authorized personnel have access to systems. Authentication also enables organizations to protect public facing assets by ensuring the true identity of a device, system, or application is authentic. This prevents individuals from accidentally disclosing credentials to an attack site and from attaching unauthorized devices to the infrastructure.
- **Manage systems** by implementing secure operating environments, distributing and enforcing patch levels, automating processes to streamline efficiency, and monitoring and reporting on system status.

- **Protect the infrastructure** by securing endpoints, messaging and Web environments. In addition, defending critical internal servers and implementing the ability to back up and recover data should be priorities. Organizations also need the visibility and security intelligence to respond to threats rapidly.
- **Ensure 24x7 availability.** Organizations should implement testing methods that are non-disruptive and they can reduce complexity by automating failover. Virtual environments should be treated the same as a physical environment, showing the need for organizations to adopt more cross-platform and cross-environment tools, or standardize on fewer platforms.
- **Develop an information management strategy** that includes an information retention plan and policies. Organizations need to stop using backup for archiving, implement de-duplication everywhere to free up resources, use a full-featured archive system and deploy data loss prevention technologies.

EDUCATION IS A KEY COMPONENT TO SECURING CRITICAL SYSTEMS FROM CYBER ATTACK

But technology alone does not solve all the ICS vulnerability problems. After all, if that were the case, there would be far fewer breaches now with all the technological advances. People, processes, organization and technology must all be addressed. The question being asked of security professionals associated with U.S. critical national infrastructure is what should they be doing in response to the recent discovery of Stuxnet? We believe that the answer in part is related to education and awareness and Symantec sees this topic being broken down into a number of areas:

- Education in the classroom, where tomorrow's software developers and network architects can be found. We need them to think security from the outset.
- Education in colleges and the commercial education aftermarket, where people learn how to write software and learn how to design and manage networks. Security needs to be a byword.
- Education at the board level to convey the message that security should be primarily business-led and that support is required to ensure security is part of an organization's ethos - so security is led from the top. Understanding (from a business perspective) the threats and risks to an organization and how these interact with the cyber world is key to this understanding.
- Education at the management level to ensure the message that good security requires secure software and well-designed and maintained networks. In other words, security must be baked in from the outset and part of this is ensuring that staff skillsets are maintained appropriately and continuously. It is key to understand the risks and threats to an organization and be able to translate and/or augment the board's view of risk and threat into action plans.
- Finally, the security professional needs to be just that. Skillset maintenance is not an option, belonging to professional organizations is not an option, interfacing and carrying the security message to the board, management and staff level is not an option. That professional must be comfortable with assessing the risks to an organization based on what is on the ground and input from the board, management and industry. Being able to translate a risk assessment into a security get-well program and/or continuous security improvement programs is a key part of the security professional's job.

SYMANTEC 2010 CRITICAL INFRASTRUCTURE PROTECTION SURVEY

Our nation's critical information infrastructure is characterized as businesses and industries whose importance is such that if their cyber networks were successfully breached and disabled, it could result in a threat to national security. In the U.S., upwards of eighty-five percent of the nation's critical infrastructure is owned by the private sector. Symantec commissioned a recent study about critical infrastructure protection. The goal of Symantec's *2010 Critical Infrastructure Protection (CIP) Survey* was to find out how aware critical infrastructure companies

were of government efforts in this area and how engaged and enthusiastic private enterprise was about working with government.

Symantec conducted the survey in August 2010 that included 1,580 enterprises in 15 countries worldwide, with companies ranging from 10 employees to more than 10,000. The median company had between 1,000 and 2,499 employees. We focused on six key critical infrastructure segments: Energy, Banking and Finance, Communications, Information Technology, Healthcare, and Emergency services. Symantec's *2010 Critical Infrastructure Protection (CIP) Survey* included the following highlights:

- **Critical infrastructure providers are being attacked.** Fifty-three percent of companies suspected experiencing an attack waged with a specific goal in mind. Of those hit, the typical company reported being attacked 10 times in the past five years. Forty-eight percent expect attacks in the next year and 80 percent believe the frequency of such attacks is increasing.
- **Attacks are effective and costly.** Respondents estimated that three in five attacks were somewhat to extremely effective. The average cost of these attacks was $850,000.
- **Industry is willing to partner with government on CIP).** Nearly all of the companies (90 percent) said they have engaged with their government's CIP program, with 56 percent being significantly or completely engaged. In addition, two-thirds have positive attitudes about programs and are somewhat to completely willing to cooperate with their government on CIP.
- **Room for readiness improvement.** Only one-third of critical infrastructure providers feel extremely prepared against all types of attacks and 31 percent felt less than somewhat prepared. Respondents cited security training, awareness and comprehension of threats by executive management, endpoint security measures, security response, and security audits as the safeguards that needed the most improvement. Finally, small companies reported being the most unprepared.

HOW GOVERNMENTS CAN ENHANCE CRITICAL INFRASTRUCTURE PROTECTION

Symantec would like to offer the following recommendations as the Committee considers how the U.S. government can further enhance its efforts to promote critical infrastructure protection including:

- Governments should continue to make resources available and partner with industry to establish critical infrastructure protection programs.
  - The majority of critical infrastructure providers confirm that they are aware of critical infrastructure programs.
  - Furthermore, a majority of critical infrastructure providers support efforts by the government to develop protection programs.
- Governments should partner with industries and industry organizations to develop and disseminate information to raise awareness of CIP organizations and plans. Specific information should include how a response would work in the face of a national cyber attack, what the roles of government and industry would be, who the specific contacts are for various industries at a regional and national level, and how government and private business would share information in the event of an emergency.
- Since most of the nation's cyber infrastructure is not government owned, a public-private partnership of government, corporate and private stakeholders is required to secure the Internet. Symantec commends the Department of Homeland Security for their engagement with the private sector. Under the National Infrastructure Protection Plan construct, DHS is the lead federal department for engaging

with the IT Sector. DHS has been a valuable partner to Symantec and the private sector, through the Sector Coordinating Councils (SCC) as well as the IT Information Sharing and Analysis Center (IT-ISAC)[6].

- Symantec has provided input to DHS on a number of "Comprehensive National Cyber Initiative" projects and we've also been engaged with the Department on several other cyber policy initiatives around the development of the National Cyber Incident Response Plan (NCIRP) including: resiliency, incentives, metrics, risk assessments, information sharing, and cyber exercises. In addition, we recently participated in the National Cyber Exercise, Cyber Storm III, which demonstrated the value of operational incident collaboration across the public and private sectors. Further, we've held several briefings with DHS to share expertise on Stuxnet and how critical infrastructures can better secure their systems against such threats. We look forward to continuing to partner with DHS and other agencies on the many issues and preparedness activities related to the nation's critical infrastructure protection.
- Governments should emphasize that security alone is not enough to stay resilient in the face of today's cyber attacks. In addition, critical infrastructure providers and enterprises in general should also ensure that their information is stored, backed up, organized, prioritized, and that proper identity and access control processes are in place.

CONCLUSION

Critical infrastructure industrial control systems face increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks as demonstrated by reported incidents. Threats can be intentional or unintentional, targeted or nontargeted, and can come from a variety of sources. Stuxnet demonstrates that industrial control systems are more vulnerable to cyber attacks than in the past for several reasons, including their increased connectivity to other systems and the Internet. Further, as demonstrated by past attacks and incidents involving industrial control systems, the impact on a critical infrastructure could be substantial.

Critical infrastructure control systems are more vulnerable today than in the past due to the increased standardization of technologies, the increased connectivity of control systems to other computer networks and the Internet, insecure connections, and the widespread availability of technical information about control systems. Further, it is not uncommon for control systems to be configured with remote access through either a dial-up modem or over the Internet to allow remote maintenance or around-the-clock monitoring. If control systems are not properly secured, individuals and organizations may eavesdrop on or interfere with these operations from remote locations. Such pre-cautions would certainly prevent, limit or contain the threats posed by Stuxnet and similar malware.

Multiple private sector entities such as critical infrastructure industry organizations, trade associations, and standards setting organizations specific to the electric, chemical, oil and gas, and water sectors are working to enhance industrial control system security. These entities are developing standards, providing guidance to members, and hosting workshops on control systems security. Over the past few years, federal agencies—including the Department of Homeland Security (DHS), the Department of Energy, the National Institute of Standards and Technology (NIST), and others—have initiated efforts to improve the security of critical infrastructure industrial control systems.

[6] Symantec currently serves in the role of chairing the Information Technology Sector Coordinating Council and sits on the Board of the IT-Information Sharing and Analysis Center. As one of the critical sector organizations identified under the US National Infrastructure Protection Plan, the IT SCC is recognized by DHS as the representative IT industry body for coordinating strategic activities and communicating the sector's views on infrastructure protection, response and recovery issues. The IT-ISAC is a non-profit organization of leading IT companies focused on providing a mechanism for the trusted exchange of information on cyber incidents, vulnerabilities, attacks, solutions and countermeasures.

.

Stuxnet certainly has demonstrated the importance of public private information sharing partnerships across the critical infrastructure community. While DHS has made strides to partner with control systems vendors through its ICS-CERT, it should build on its October 2009 "Strategy for Securing Control Systems" and enhance its control systems partnership by including the IT and IT security community, who have traditionally worked with the DHS US-CERT. Cross collaboration within DHS is the key to improved situational awareness and operational response, and DHS should continue its efforts to integrate these functions. Until there is greater coordination between IT and IT security vendors and the industrial control systems owners and operators, there is an increased risk that multiple organizations will conduct duplicative work and miss opportunities to learn from and collectively respond to threats. Given the importance of these issues, we recommend that DHS (1) further enhance information sharing on control systems vulnerabilities with the IT and IT security communities; and (2) continue to work on integrating its information sharing capabilities to improve situational awareness and operational response partnerships with industry.

In closing, I'd like to take this opportunity to convey Symantec's strong support of S. 3480, the Protecting Cyberspace as a National Asset Act. We believe that this important legislation will enhance and modernize our nation's overall cybersecurity posture in order to safeguard our critical infrastructure from attack. The bill also importantly recognizes cybersecurity as a shared government and private sector responsibility which requires a coordinated strategy to detect, report, and mitigate cyber incidents. We look forward to continuing to work with the Committee to help advance this important legislation.

Symantec would like to thank the Committee for the opportunity to testify today. We remain committed to continuing to work in coordination with Congress, the Administration and our private sector partners to secure our nation's critical infrastructure from cyber attack. Thank you.