Global Security Review

Volume 1 Article 8

January 2017

Nation-State Hacking: Uniting Policy and Code to Limit the Threat

Mark M. Deen
Florida International University

Recommended Citation
Deen, Mark M. (2017) "Nation-State Hacking: Uniting Policy and Code to Limit the Threat," *Global Security Review*: Vol. 1 , Article 8.
DOI: 10.25148/GSR.1.009612
Available at: https://digitalcommons.fiu.edu/gsr/vol1/iss1/8

Nation-State Hacking: Uniting Policy and Code to Limit the Threat

Mark M. Deen, Florida International University

Abstract

This article examines nation-state hacking and analyzes some possible defenses against these attacks by combining policy and code level defense. The article examines some recent incidents of nation-state hacking and evaluates the actions taken by the attacker and the effected parties. This work focuses on a variety of nation-state hacking incidents and provides a critical perspective on how policy and code level controls could be combined to defend against these attacks. Nation-state hacking continues to be an important issue on the United States security agenda. Advanced nation-state hacking threats can adversely affect the day to day operations of a nation effectively crippling it with nearly complete anonymity. In 2013, the U.S. issued E.O. 13636, *Improving Critical Infrastructure Cybersecurity*. On December 1, 2016, President Obama unveiled the National Cybersecurity Plan to increase awareness of the threat that lack of appropriate cybersecurity controls presents.

Nation-state hacking is an important issue on the United States security agenda. Nation-state hacking is defined as an attack or series of attacks conducted by one nation-state against another nation-state to defend national sovereignty and project national power.[1] Nation-state hacking may provide access to information that may take years or decades to access with traditional methods such as the use of spies or surveillance techniques and in the twenty-first century has replaced the spy as the most effective and efficient method to access secure information with little risk and significant reward.

The organizations creating nation-state malware are typically well-funded, well-trained, and dedicated to achieving their hacking objectives. While these team members remain safe in a remote location their malicious code may travel deep within highly secured networks and systems thousands of miles away. Nation-state hacking represents a new arms race as countries rush to bolster defenses[2] and create newer, more effective attacks. Nation-states may hide attacks amongst a myriad of independent hacking organizations and may even mimic attacks used by independent hacking organizations. All of the preceding factors make it extremely difficult to forensically differentiate between an attack from a nation-state and an attack from an independent hacking organization.[3] To further complicate this, some nation-states may use independent hacking organizations to assist in attacks against other nations. The most predominant use of nation-state hacking is to resolve conflict and policy disputes in the cyber arena rather than the political arena. This article aims to examine the methods nations may use to defend against these threats.

Historical Context

In 2007, a piece of malicious computer code called Stuxnet was used to disrupt the Iranian nuclear program.[4] Stuxnet succeeded in slowing Iranian progress in their nuclear program by severely damaging the centrifuges by causing them to spin out of control while monitoring systems reported normal centrifuge operation.[5] Stuxnet was the first tangible evidence that nation-state level hacking was being used actively to alter international policies and politics.

In 2009, China allegedly attacked several US companies including Google[6] and RSA.[7] The Chinese attack escalated in 2014 when China allegedly hacked the United States Office of Personnel Management (OPM) network and obtained the OPM database, which contains information about more than 4 million current and former federal government employees.[8]

In 2014, North Korea purportedly attacked the computer systems of Sony Pictures Entertainment.[9] The North Korean attack significantly disrupted the network operations of Sony Pictures and affected customers around the globe. The North Korean attack was rumored to be a result of a Sony Pictures planned release of a movie concerning the North Korean President.

Later that year, Russia allegedly launched an attack that compromised the United States State Department and the White House. The attack permitted the attackers to access non-classified information including information concerning the President in the form of emails and the President's daily schedule.[10]

The outcome of these attacks was that for a period of time foreign nation-state sponsored organizations

had access to sensitive information within the United States government or U.S.-based companies. The policy response from the United States government was swift and decisive. In 2013, the administration issued E.O. 13636, *Improving Critical Infrastructure Cybersecurity* which defined the need for Information Security concerns to be addressed on a national level.[11] In February 2014, the United States government released a *Framework for Improving Critical Infrastructure Cybersecurity* which provided guidance focused on protecting critical infrastructure organizations from attacks.[12] The most recent iteration in U.S. policy concerning cybersecurity is the December 1, 2016 *Report on Securing and Growing the Digital Economy* issued by the Commission on Enhancing National Cybersecurity. The report calls for a greater investment in cybersecurity mechanisms[13] and provides some actionable steps for organizations seeking to protect themselves from cyber-attacks.

Policy And Why It Matters

All of the nation-state attacks involved the introduction of malicious code into trusted computer systems. In most cases the malicious code was introduced either by human interaction or previously unknown flaws in the configuration of effected systems. The absence of defined policy results in diversity within human processes and procedures. In turn, this leads to diversity in the configuration of computing systems which creates weaknesses that may be exploited to gain access to computing systems—often with increased levels of system permissions. The application of well-defined and sound policies minimizes the threat posed by inconsistent computing system configurations by employing general rules that should be applied to all computing systems. An excellent example of policy is the *National Institute of Standards and Technology (NIST) Cybersecurity Framework*. The *NIST Cybersecurity Framework* was developed in direct response to E.O. 13636, *Improving Critical Infrastructure Cybersecurity* and provides a framework to measure and enhance cybersecurity mechanisms in order to protect government and private sector organizations. The NIST framework provides a series of granular controls that address network configuration, connectivity, and Information Technology practices. However, the NIST framework provides very little guidance regarding code level security. NIST does however provide excellent guidance regarding human processes such as Information Technology change management practices. In the case of StuxNet simple human policy rules regarding system patching, system security monitoring, and the use of USB thumb drives could have been useful in limiting the threat StuxNet presented.

Another example of policy and its effect in guiding Information Security practices is the European Union's May 17th release of the *Network and Information Security (NIS) Directive*. The NIS Directive provides a uniform approach to securing information systems between European Union (EU) member states. The NIS Directive recognizes that cybercrime may cross national boundaries and facilitates cross border coordination between EU member states during the investigation of cybercrime. NIS requires that specific security controls are enabled where personal information concerning European Union citizens is being stored. The implementation of the NIS directive fundamentally affects the way that EU and non-EU organizations interact. The NIS requirement to add additional security layers around EU citizen's information requires many organizations to alter the way they address Information security practices for data stored both inside and outside the EU. The EU directives stresses the need for sound information security practices such as encryption, secure destruction, and accountability for data. However, it provides little information about programming code used to store and manipulate data.

Overall, neither the EU NIS Directives nor the *Report on Securing and Growing the Digital Economy* issued by the Commission on Enhancing National Cybersecurity address the concerns pertaining to code or strong coding standards for security. Nation-state hacking relies on poor code controls as well as a lack of policies that govern human behavior. Many of the policies are concentrated on the activities of humans and are not focused on activities performed in an automated manner by computer systems executing the commands stored in programming code.

Code And Why It Matters

At the most elemental level of computing systems, sequences of commands are contained in scripts referred to as code. The individual instructions contained within the code are then executed by the computer system. Because computers simply execute the instructions contained within code they cannot differentiate between malicious and benign instructions. Anti-virus and anti-malware tools are a means of restricting the execution of malicious code on computing systems. Anti-virus and anti-malware tools are based on known "signatures" of malicious

code and are therefore incapable of alerting system users concerning the possible threat presented by code for which signatures do not exist. Anti-virus and anti-malware software cannot defend computing systems completely due to the signature based nature of their operation.

The majority of nation-state hacking incidents required the execution of malicious code on effected systems in order to facilitate an effective attack. In the case of StuxNet the malicious code entered the Iranian nuclear facility on a USB thumb drive.[14] The code stored on the USB drive spread rapidly through the facility and around the world by exploiting a previously unknown flaw in the Microsoft Windows operating system.

Code level controls such as code whitelisting may limit the capabilities of malicious code.[15] Whitelisting is a process that permits computers to only execute code that is approved. Enacting policies requiring that only whitelist approved code may operate on computing systems decreases the probability that malicious code may be able to run on these computer systems.[16] Whitelisting is a supplementary control to existing anti-virus and anti-malware solutions and should be used in addition to these software countermeasures.

Furthermore, code is also contained in hardware components. The code in hardware components inform the computer how to communicate with the hardware component and is referred to as "firmware". Firmware code is stored in chips on the hardware component and is always present regardless of whether or not a computer system has been restarted or reset. Firmware code executes within the hardware device and may not be visible to malicious code scanning tools such as anti-virus and anti-malware software installed on the computer system. Currently, very few solutions exist to validate the code stored in firmware, but methods such as code signing, code validation, and independent code testing serve to validate the authenticity of firmware code. On September 6, 2016, the United States Computer Emergency Readiness Team (CERT) issued advisory TA16-250 which discusses the threat presented by firmware executing within "grey market" devices.[17] Grey market devices are devices such as network switches and routers that are resold on the secondary market by parties other than the original equipment manufacturer (OEM). Gray market devices may have been tampered with or have malicious firmware installed that may also be used to compromise sensitive information.

Conclusion: Combining Code And Policy

Current national cybersecurity policies focus on restricting electronic access to networked computer systems but do not address the need to protect computer systems at the code level despite the fact that this method is used by most nation-state attacks. Policies should also consider possible efficiencies by adding requirements for code level controls to limit the threat presented by nation-state level hacking. The combination of policy level guidance and code level controls would serve to decrease the opportunity for malicious code to enter into computer systems and adversely impact the operation of those systems. National cybersecurity policy should also clearly address the ability for code to communicate from within the network to outside parties. By blocking the ability for code to communicate outside of secured computer networks the ability to remotely control or send information from compromised computer systems is disabled.

Nation-state hacking will increase in the future as it is fundamentally a part of warfare. Protecting as many key infrastructure computer systems as possible is an effective method to limiting the threats presented by nation-state attacks. The human element may be controlled by effective policies and practices but ultimately the code and instructions executed by computing systems will define whether or not an attack is effective.

National policy should be expanded to address code level controls and provide some guidance on how to implement these controls to create a complete approach to securing national cybersecurity. Furthermore, national policy should provide simple guidance regarding technologies such as whitelisting as a method to limit the capability for malicious code to execute on computer systems and as a supplementary control for anti-virus and anti-malware software. Finally, the threat presented by malicious firmware stored on chips inside of computer systems and grey market devices should also be escalated as a risk in the national cybersecurity policy. There is a unique challenge to validate and verify the authenticity of firmware since it may not be removed without disabling the hardware device. This provides a perfect platform for nation-state attacks to hide and operate with little risk of detection.

Notes

1 Pierluigi Paganini, "FireEye World War C report–Nation-state driven cyber attacks," *FireEye*, October 3, 2013**,** http://securityaffairs.co/wordpress/18294/security/fireeye-nation-state-driven-cyber-attacks.html, accessed December 11, 2016

2 Ken Dilanian, "Obama issues order to bolster cyber-defenses," *Los Angeles Times*, February 12, 2013.

3 Kim Zetter, "We're at Cyberwar: A Global Guide to Nation-State Digital Attacks," *Wired*, September 1, 2015.

4 Chloe Albanesius, "Stuxnet Worm Crafted by U.S., Israel to Thwart Iran's Nuclear Program," *PC Magazine*, June 1, 2012.

5 Michael B. Kelley, "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," *Business Insider*, November 20, 2013.

6 Ellen Nakashima, "Chinese hackers who breached Google gained access to sensitive data, U.S. officials say," *The Washington Post*, May 20, 2013.

7 Gregg Keizer, "Researcher follows RSA hacking trail to China," *ComputerWorld*, August 4, 2011.

8 Ellen Nakashima, "Chinese breach data of 4 million federal workers," *The Washington Post*, June 4, 2015.

9 David E. Sanger and Nicole Perlroth, "U.S. Said to Find North Korea Ordered Cyberattack on Sony," *The New York Times*, December 14, 2014.

10 Polly Mosendz, "Report: Russians Hacked White House," *Newsweek*, April 7, 2015.

11 Federal Register, Vol. 78, No. 33, Executive Order 13636 of February 12, 2013 https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf, accessed December 11, 2016.

12 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Washington, D.C.: National Institute of Standards and Technology 2014) https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, accessed December 11, 2016.

13 Rob Freeman, "Commission on Enhancing Cybersecurity Report Calls for Greater Investment," *Cyber Law Monitor*, December 6, 2016.

14 Daniel Terdiman, "Stuxnet delivered to Iranian nuclear plant on thumb drive," *CNET*, April 12, 2012, https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/, accessed December 11, 2016

15 Homeland Security, Application Whitelisting (AWL): Strategic Planning Guide https://www.uscert.gov/sites/default/files/cdm_files/FNR_NIS_OTH_AWL_Strategic_Planning_Guide.pdf, accessed December 11, 2016.

16 Roger A. Grimes, "To detect 100 percent of malware, try whitelisting 'lite'," December 31, 2013, http://www.infoworld.com/article/2609643/security/to-detect-100-percent-of-malware--try-whitelisting--lite-.html, accessed December 11, 2016

17 United States Computer Emergency Readiness Team, September 6, 2016, https://www.us-cert.gov/ncas/alerts/TA16-250A, accessed December 11, 2016.