ASA

Risk Consultants

Research Note

The Cyber Intelligence Sharing and Protection Act and Online Privacy

By: Travis Warren

Keywords: CISPA, Cybersecurity, China, Cyber Weapons

Abstract – This research note discusses the arguments for the passage of the Cyber Intelligence Sharing and Protection Act (CISPA) and elaborates the criticisms made by privacy advocates with regards to the more controversial aspects of the bill. New markets in cyber weapons are also discussed and put forward as an alternative area for potential regulation.

Introduction

Online privacy was, is and will continue to be a hotly debated topic. This debate continues despite the fact that many CEOs of large tech sector companies have derided the idea of online privacy and gone so far as to declare "the age of privacy to be over."[i] However, public outcry over recent changes to Instagram and Facebook's privacy terms,[ii] seem to indicate that privacy and the contractual language supporting privacy protection, do still matter to a large portion of the online community. This is particularly in evidence during the backlashes that inevitably occur in reaction to attempts by the United States government to control, regulate and gain access to personal information of Internet users.

On April 26, 2012 the United States House of Representatives passed H.R. 3523 also known as the Cyber Intelligence Sharing and Protection Act (CISPA).[iii] CISPA was broadly criticized across the political spectrum with groups as diverse as the American Civil Liberties Union (ACLU)[iv] and Freedom Works[v] publicly advocating against its passage. Ultimately, although the bill passed the House, it failed to make its way out of the Senate.[vi] Even had the Senate approved the bill, President Obama had threatened a veto based on the grounds that CISPA lacked

"privacy, confidentiality, and civil liberties safeguards."[vii] Despite this, the original sponsors of CISPA are reported to be reintroducing a very similar bill in the 2013 legislative session.[viii]

Why CISPA?

At the beginning of its previous stint through the House of Representatives, CISPA was introduced on the House floor by Intelligence Committee Chairman Mike Rogers and was defended as necessary owing to the myriad of threats to American infrastructure and business interests that exist in cyberspace. During the speech, Representative Rogers made three references to China, specifically pointing to the Chinese role in stealing American intellectual property and as a result costing American jobs.[ix] Charged language and specific countries are referenced in the speech, beginning with this initial statement "In just the last few years, nation states like China have stolen enough intellectual property from just defense contractors, that would be equivalent to 50 times the print collection of the US Library of Congress" (ibid). No specific incidents or data thefts are referenced to defend this assertion and CISPA is put forward as reasonable counteragent against the specter of these foreign enemies without examples as to why this is the case.

Specifics aside, where China is concerned the security community and numerous American journalists share a common or sympathetic view with Representative Rogers. Recently, three prominent newspapers, The New York Times, The Washington Post and The Wall Street Journal, have gone public with claims and evidence that they were victims of attacks, which likely originated in China.[x] The New York Times stated "Chinese hackers had persistently attacked its computers over the past four months since the paper published a story on Premier Wen Jiabao, but sensitive material related to the report was not accessed." (ibid) These highly publicized attacks are not the first accusations of illegal behavior by Chinese sponsored cyber criminals. In June of 2012, Google publicly claimed that "Suspected Chinese hackers tried to steal the passwords of hundreds of Google email account holders, including those of senior U.S. government officials, Chinese activists and journalists…"[xi]

Additionally, a recent intelligence assessment appears to contextualize these apparently isolated incidents as examples of a widespread issue.[xii] The Washington Post reported that, "The National Intelligence Estimate identifies China as the country most aggressively seeking to penetrate the computer systems of American businesses and

institutions to gain access to data that could be used for economic gain" (ibid). Additionally, the assessment, "…describes a wide range of sectors that have been the focus of hacking over the past five years, including energy, finance, information technology, aerospace and automotive…" (ibid). These examples indicate that the hyperbole and advocacy for new cybersecurity laws and policy are warranted however; they do not make an equally compelling case as to why CISPA would improve this otherwise bleak security landscape.

Privacy Concerns

Opponents of CISPA argue that while certain threats are real, security policy, law and privacy should not be mutually exclusive concepts. As an example an open letter to Congress that was drafted by security experts, engineers and various other industry experts stated, "We take security very seriously, but we fervently believe that strong computer and network security does not require Internet users to sacrifice their privacy and civil liberties."[xiii] The argument then, is not whether Internet security should be improved or better policed but instead, that the original CISPA bill lacks protections for those users that it is intended to protect.

Specifically, opponents of CISPA cited the fact that the bill was

prefaced with the statement "Notwithstanding any other provision of law."[xiv] This verbiage allows the provisions of CISPA to supersede any previously drafted legislation that may provide for privacy protections or limitations on government access to private or personal information. Additionally, another section at issue grants immunity to private entities for sharing information that would have previously required warrant, with agencies of the federal government (ibid). This section would prevent the possibility of legal ramifications for the sharing of network data, similar to what was seen during the AT&T wiretapping scandal in 2006.[xv] While the legislation does not explicitly legalize warrantless wire tapping of the variety seen in the AT&T scandal, it does allow private companies such as AT&T to share that same color of data with the government without risk of liability.

Oversight is also addressed and limited within the language of the bill. Specifically it states, that any information shared with a federal agency, does not have to conform to the regulations specified in the Freedom of Information Act (FOIA).[xvi] Essentially, this provision prevents members of the public from evaluating the scope and details of the information that would be shared by private entities without first filing a lawsuit against the government (ibid). This is particularly

concerning owing to the vagueness of the language, which defines the initiating reasons and class of information can be shared. H.R. 3523 defines cyber threat information as information pertaining to vulnerabilities, threats and efforts to deny or gain access to any system or network of a government or private entity.[xvii] According to the EFF this broad definition could include "things like port scans, DDoS traffic, and the like. Indeed, merely using a proxy or anonymization service to let you browse the web privately could be construed to be a cybersecurity threat indicator. Using cryptography to protect one's communications or access systems securely could similarly be taken as a way to defeat an operational control" (ibid).

Existing Private Sector Solutions

Based on the fact that the security threats to U.S. networks and related infrastructure are real and documented and that previous attempts at legislating a solution (like CISPA) have failed to provide privacy protections ample enough to inspire passage; the question becomes what is the private sector currently doing to protect its own vulnerable networks? What best practices, guidelines and markets are filling the void left by the Senate's failure to pass CISPA?

A recent series on National Public Radio (NPR) outlined the major

approaches currently being recommended and adopted by the private sector in response to consistent and ongoing cyber threats. This report indicates that the consensus among cybersecurity firms is that the private sector should shift focus from network defenses to a more offense-based strategy.[xviii] Honeypots are the specific offensive option used to exemplify the potential efficacy of this methodology. A honeypot is a scheme wherein a company plants inaccurate and misleading documentation on its network with the hopes that an attacker would illegally obtain that documentation and the sponsoring agency of that attacker would then act on the false information, ultimately leaving the attacking organization worse off than they were previously. While no other offensive strategies are specified it is noted that there "is nevertheless a vigorous debate over the legal issues in offensive cyber-operations by private companies" (ibid). Whatever ethical concerns are raised by the practice of offense as a from of defense, it seems, absent clear legal definition around what is and is not permissible, private companies are likely to start trending in the direction recommended by security experts.

Another extralegal private sector solution discussed in multiple separate reports on NPR[xix] and the MIT Technology Review[xx] is the role

that exploit markets currently play in economy of network and information security. According to the report, "There is no regulation of the vulnerability market in the U.S." (ibid). However, the industry exists, and while industry participants prefer to remain somewhat anonymous, the report did state, "In the U.S., the National Security Agency and other branches of the U.S. military, law enforcement and intelligence agencies are among the biggest buyers of vulnerabilities" (ibid). As the reality of the US government's interest in this market is not accompanied by a large number of reported incidents of federal involvement in the patching of vulnerabilities, it can be assumed that the various agencies involved in these purchases are involved for the offensive capabilities associated with the information.

Conclusion

In reaction to the deteriorating security situation this cyber weapons market and resulting arms race is likely fueling, President Obama drafted an Executive Order on February 12th, 2013 titled Improving Critical Infrastructure Cybersecurity.[xxi] The order defines what may be considered critical infrastructure and mandates the creation of a framework for improving security and reducing risks to those structures that meet that definition. Additionally, it outlines a

series of policy goals, including the creation of regular threat reports, which will be made available to the private sector and the process by which classified threat information can be released to private companies (ibid). The fact that at least some of this classified information is likely to include vulnerabilities purchased on the open market and available to the highest bidder will raise interesting questions regarding the efficacy of the information sharing framework. Should the bar for access to this threat information exceed the expense of purchasing the information on the open market, will private entities choose the exploits market over the framework offered by the government?

Regardless, the Obama administrations effort to protect critical infrastructure has the potential to be a limited test case in regards to the efficacy of information sharing in combating cyber threats, whereas the reintroduction of CISPA refocuses the cybersecurity discussion on issues that now have legal remedies. With the introduction of the Executive Order on Improving Critical Infrastructure Cybersecurity, at least a portion of the information sharing intended through CISPA, can now be realized and acted upon. Additionally, it is already illegal to access government or private networks without permission. While

reporting these crimes might create negative PR for the company that has been victimized, it would create the opposite direction information-sharing situation that is not defined in the Executive Order. If the government seeks information in an ongoing investigation it has the legal ability to request a warrant or a national security letter.[xxii] The merits of speeding up this process or eliminating it all together can be debated but even a completely open information-sharing framework will not help to solve the current escalation of cyber attacks and online criminality.

The threats to US networks and private businesses are very real and the federal government has not taken steps to regulate the industry that creates, sells and improves the weapons that are being used to perpetrate these attacks. Quite the contrary, the US government is a known innovator of cyber weaponry[xxiii] and widely recognized as a major customer of the cyber exploit and malware industry.[xxiv] The fact that US agencies are such willing participants in a marketplace that facilitates the very thing being decried in the 2013 State of the Union address[xxv] makes legislation like CISPA, which require further sacrifices to civil liberties (privacy), seem disingenuous. A more logical first step would be to strengthen the laws combatting the

creation and sale of the very weapons the US is attempting to protect its critical infrastructure from; instead of further weakening the legal protections that exist for the population it is the government's job to defend. Further, standing idly by and allowing the exploit industry to flourish, likely emboldens and increases the capabilities of nations like China, who's activities are held up as the reason CISPA is required in the first place.

ASA

Risk Consultants

References

[i] Schneier, B. (2010, April 6). Google And Facebook's Privacy Illusion. Forbes.com. Retrieved February 15, 2013, from http://www.forbes.com/2010/04/05/google-facebook-twitter-technology-security-10-privacy.html

[ii] Timberg, C. (2012, December 18). Instagram, Facebook stir online protests with privacy policy change. Washington Post. Retrieved from http://articles.washingtonpost.com/2012-12-18/business/35908189_1_kevin-systrom-instagram-consumer-privacy

[iii] Rogers, M. Cyber Intelligence Sharing and Protection Act. , Pub. L. No. H.R. 3523 (2012). Retrieved from http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523rfs/pdf/BILLS-112hr3523rfs.pdf

[iv] ACLU Opposition to H.R. 3523, the Cyber Intelligence Sharing and Protection Act of 2011. (2011, December 1). American Civil Liberties Union. Retrieved February 15, 2013, from http://www.aclu.org/technology-and-liberty/aclu-opposition-hr-3523-cyber-intelligence-sharing-and-protection-act-2011

[v] Borowski, J. (2012, April 27). House Passes Online Privacy Invasive CISPA. FreedomWorks. Retrieved February 15, 2013, from http://www.freedomworks.org/blog/jborowski/house-passes-online-privacy-invasive-cispa

[vi] Martinez, J. (2012, August 2). Cybersecurity Act fails Senate vote. The Hill's Hillicon Valley. Retrieved February 15, 2013, from http://thehill.com/blogs/hillicon-valley/technology/241851-cybersecurity-act-fails-to-advance-in-senate

[vii] Statement of Administration Policy - H.R. 3523 - Cyber Intelligence Sharing and Protection Act. (2012, April 25). The White House. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saphr3523r_20120425.pdf

[viii] Protecting the American Economy from Cyber Attacks: Introducing the "Cyber Intelligence Sharing and Protection Act of 2013". (2013, February 13). The Permanent Select Committee on Intelligence Democratic Office. Retrieved February 15, 2013, from http://democrats.intelligence.house.gov/event/protecting-american-economy-cyber-attacks

[ix] Rogers, M. (2013, April 26). Chairman Mike Rogers Statement. The Permanent Select Committee on Intelligence. Retrieved February 15, 2013, from http://intelligence.house.gov/press-release/chairman-mike-rogers-statement

[x] Blanchard, B. (2013, January 31). New York Times says targeted by China hackers after Wen report. Reuters. Retrieved February 15, 2013, from http://www.reuters.com/article/2013/01/31/us-china-newyorktimes-idUSBRE90U05620130131

[xi] Wee, S.-L. (2011, June 2). Google reveals Gmail hacking, says likely from China. Reute. Retrieved February 15, 2013, from http://www.reuters.com/article/2011/06/02/us-google-hacking-idUSTRE7506U320110602

[xii] Nakashima, E. (2013, February 10). U.S. said to be target of massive cyber-espionage campaign. The Washington Post. Retrieved February 15, 2013, from http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html

[xiii] An Open Letter From Security Experts, Academics and Engineers to the U.S. Congress: Stop Bad Cybersecurity Bills. (2012, April 23). Electronic Frontier Foundation. Retrieved February 15, 2013, from https://www.eff.org/deeplinks/2012/04/open-letter-academics-and-engineers-us-congress

[xiv] McCullagh, D. (2012, April 27). How CISPA would affect you (faq) | Privacy Inc. CNET News. Retrieved February 15, 2013, from http://news.cnet.com/8301-31921_3-57422693-281/how-cispa-would-affect-you-faq/

[xv] Singel, R. (2006, January 31). AT&T Sued Over NSA Eavesdropping. Wired. Retrieved February 15, 2013, from http://www.wired.com/science/discoveries/news/2006/01/70126

[xvi] Jaycox, M. M. (2013, February 13). CISPA, the Privacy-Invading Cybersecurity Spying Bill, is Back in Congress. Electronic Frontier Foundation. Retrieved February 15, 2013, from https://www.eff.org/deeplinks/2013/02/cispa-privacy-invading-cybersecurity-spying-bill-back-congress

[xvii] McCullagh, D. (2012, April 27). How CISPA would affect you (faq) | Privacy Inc. CNET News. Retrieved February 15, 2013, from http://news.cnet.com/8301-31921_3-57422693-281/how-cispa-would-affect-you-faq/

[xviii] Gjelten, T. (2013, February 13). Victims Of Cyberattacks Get Proactive Against Intruders. NPR. Retrieved February 15, 2013, from http://www.npr.org/2013/02/13/171843046/victims-of-cyberattacks-now-going-on-offense-against-intruders

[xix] Gjelten, T. (2013, February 12). In Cyberwar, Software Flaws Are A Hot Commodity. NPR. Retrieved February 15, 2013, from http://www.npr.org/2013/02/12/171737191/in-cyberwar-software-flaws-are-a-hot-commodity

[xx] Simonite, T. (2013, February 13). Welcome to the Malware-Industrial Complex. MIT Technology Review. Retrieved February 15, 2013, from http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex/

[xxi] Executive Order -- Improving Critical Infrastructure Cybersecurity. (2013, February 12). The White House. Retrieved February 16, 2013, from http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[xxii] National Security Letters. (n.d.). American Civil Liberties Union. Retrieved February 16, 2013, from http://www.aclu.org/national-security-technology-and-liberty/national-security-letters

[xxiii] Williams, C. (2011, May 27). Stuxnet virus: US refuses to deny involvement. Telegraph. Retrieved February 16, 2013, from http://www.telegraph.co.uk/technology/news/8541587/Stuxnet-virus-US-refuses-to-deny-involvement.html

[xxiv] Simonite, T. (2013, February 13). Welcome to the Malware-Industrial Complex. MIT Technology Review. Retrieved February 15, 2013, from http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex/

[xxv] Transcript of President Obama's 2013 State of the Union -. (2013, February 12). San Jose Mercury News. Retrieved February 15, 2013, from http://www.mercurynews.com/politics-government/ci_22575732/transcript-president-obamas-2013-state-union