ASA

Annie Searle & Associates LLC

Research Note

Trends in Data Breaches

By Andrew H. R. Hansen

Keywords: hacktivism, Anonymous, LulzSec, cyber warfare, cyber security, targeted attacks, Stuxnet

Abstract – As society becomes increasingly dependent upon technology, the need for information security rises. New trends in data breaches include various types of targeted attacks. Recent hacktivist and cyber warfare events illustrate challenges facing individuals, businesses and governments. Organizations should inventory their current security policy and protocol to ensure they are sufficiently protected.

Introduction

Over the past half century Western culture has evolved from an industrial economy to a knowledge economy. We are now in the early stages of what some are referring to as the "creative economy."[1] Throughout these societal changes, our dependence upon technology – from both a business and personal perspective – has risen dramatically. With this increased reliance on technology, individuals, businesses and governments are gradually realizing the critical responsibility of protecting information. This article will reference recent security breaches to bring to attention trending information assurance concerns from a local and global perspective, as well as discuss possible ways to prepare for and mitigate these threats.

Hacktivism

One increasingly prevalent concern in information security is "hacktivism" – the "act of hacking, or breaking into a computer system, for a politically or socially motivated purpose."[2] Those who engage in hacktivism often belong to hacking groups or communities. Anonymous and Lulz Security (usually abbreviated LulzSec), are arguably the most prominent of these hacking communities. Although the motives of these two hacking groups may differ, they have successfully exploited a diverse selection of targets, including: major

corporations, religious groups, social networks, and governments. In October, 2011, hackers from Anonymous claimed responsibility for removing forty secret child pornography websites.[3]

Stratfor

With the aim of better understanding international events and reducing risk,[4] Stratfor is an Austin, Texas, based security think tank and consulting firm that claims to provide "an audience of decision-makers and sophisticated news consumers in the U.S. and around the world with unique insights into political, economic, and military developments."[5] They are also amongst the latest targets of an Anonymous hack.

On December 24, 2011, members of Anonymous claimed responsibility for "crashing the Web site of the (Stratfor) group… pilfering its client list, e-mails and credit card information in an operation they say is intended to steal $1 million for donations to charity."[6] The hacking group allegedly posted a list online that they claim contains "Stratfor's confidential client list as well as credit card details, passwords and home addresses for some 4,000 Stratfor clients."[7] Anonymous also claimed the portion of client information already posted online represented a fraction of the 200 gigabytes they stole from Stratfor.[8] The 200 gigabytes of data is reportedly mostly

email, with the hacking group claiming to have obtained over 3 million emails.[9] Stratfor later denied the allegation that their private client list was compromised,[10] but surprisingly, the credit card details appeared to be unencrypted, "an easy-to-avoid blunder which, if true, would be a major embarrassment for any security-related company."[11]

Although there has been some speculation that this was not in fact the work of Anonymous,[12] it appears that whoever carried out this hack is sticking to the original plan, as shortly after the breach donations to charities like the Red Cross, Save the Children and Care started to show up on the credit cards of Stratfor clients.[13] In addition, false emails are being sent out claiming to originate from George Friedman, the political scientist, author and CEO of Stratfor, an action that required releasing a video warning message to Stratfor customers by Vice President Fred Burton on the company's YouTube page.[14] As of the writing of this article, the company's website has not returned to its normal functionality. A simple message explaining the situation currently occupies their website homepage.[15]

Cyber Warfare

Cyber warfare "involves units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means."[16]

Many nations, including the United States, have established formal cyber security teams. In 2011, the United States deployed a new cyber unit specifically geared towards "combating the millions of low-grade attacks targeting the nation's 15,000 networks and 7 million computers on a daily basis."[17]

The United States is not the only nation concerned about malicious cyber activities. China also recently organized a thirty member "Cyber Blue Team," tasked with defending against cyber-attacks.[18] In a similarly manner, Japan has partnered with Fujitsu Ltd., "one of its major technology giants, in developing a virus for tracking down the source of cyber attacks and for nullifying their effect."[19]

Stuxnet

Originally deployed in 2009, the computer worm known as Stuxnet has since rapidly launched to the forefront of the cyber warfare dialogue, and "may be the most sophisticated cyberweapon ever deployed."[20] Stuxnet started appearing in industrial programs around the globe, but as experts started dissecting it, they "soon determined that it had been precisely calibrated in a way that would send nuclear centrifuges wildly out of control, adding suspicion that it was meant to sabotage Iran's nuclear program."[21] The basic functionalities of the worm have been described thusly:

> "The worm itself now appears to have included two major components. One was designed to send Iran's nuclear centrifuges spinning wildly out of control. Another seems right out of the movies: The computer program also secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart."

It is believed that in its prime, Stuxnet was responsible for destroying "1,000 centrifuges at the Natanz fuel enrichment facility by sabotaging their motors."[22] Experts estimate Stuxnet potentially set Iran's nuclear development program back several years.[23] Not surprisingly, Iran has responded by embarking on an "ambitious plan to boost its offensive and defensive cyber-warfare capabilities and is investing $1 billion in developing new technology and hiring new computer experts."[24]

Chief amongst the mysteries that still surround Stuxnet is who developed it. Ed Byres, Chief Technology Officer for Byres Security, estimated it would take months, if not years, of coding to make Stuxnet operate like it did.[25] Combining the complexity of the code with the fact that nearly sixty percent of infected machines were located in Iran[26] and most experts will agree that this is most certainly the work of a

nation state.[27] The most prominent theory points to the mounting evidence that suggests Stuxnet is the product of collaboration primarily between the United States and Israel.[28] Both countries formerly deny these allegations, however, "Israeli officials grin widely when asked about its (Stuxnet's) effects."[29] In a 2011 conference concerning Iran, Gary Samore, chief strategist for combating weapons of mass destruction for the United States sidestepped a question about Stuxnet, but then said with a smile, "I'm glad to hear they are having problems with their centrifuge machines, and the U.S. and its allies are doing everything we can to make it more complicated."[30]

Handling Hacktivism

These trends may appear unrelated, but they share the common threads of both being manifestations of targeted attacks and products of political discord. Targeted attacks, like the one illustrated in the Stratfor case, are expected to rise in 2012.[31] By leaving their sensitive customer data unencrypted, Stratfor is a prime example of a high profile, sophisticated organization, failing to comply with basic security practices. "Mitigating exposure of your accounts and systems to hacktivism (or hacking in general) should always be a part of a comprehensive security strategy."[32] Some additional precautions organizations can take include:

- Limiting access to your corporate social media accounts to specific personnel and govern them with policy and password enforcement
- Use a web content filtering system to limit downloading of malware
- Ensure that web servers and public-facing portals are protected behind an active intrusion-prevention system or firewall that actively scans uploaded and downloaded content.[33]

Organizations should regularly review their security practices and policies to ensure there are no gaps in security and that the organization is keeping pace with advancing trends.

Dealing With Disruption

Although the thought of cyber warfare may seem distant and unlikely, the probability that businesses will face some form of disruption in normal operations increases with the constant unrest in the global political climate. It may be wise to pause and consider alternative ways of implementing business practices should a major disruption of systems occur. Researchers at New York University identified three primary ways communications are disrupted in a disaster, they include:

- Physical destruction of network components

- Disruption in supporting network infrastructure
- Network congestion.[34]

Dedicating the resources to research each of these three forms of disruption and building remediation protocols that deal specifically with the unique consequences of each type, will better prepare the organization for recovery should a major catastrophe or act of cyber warfare occur.

Conclusion

As society becomes increasingly dependent on technology, the need for individuals, businesses and governments to implement information security practices is no longer an optional decision. With political unrest becoming a constant factor, targeted attacks like hacktivism and cyber warfare will become more common occurrences. Fortunately, these threats are often manageable if appropriate policy, controls and remediation protocols are put in place. Organizations need to research the specific challenges they may face and prepare alternative courses of action in preparation for major disruptions in normal operations.

References

[1] Plooy, Peter du. "Narrowing the Gap Within Different Generations in the Workplace." *Management Exchange*. 31 Oct. 2011. Web. 5 Jan. 2012. <http://www.managementexchange.com/hack/narrowing-gap-within-different-generation-workplace>

[2] "Hacktivism." *SearchSecurity.* Web. 5 Jan. 2012 <http://searchsecurity.techtarget.com/definition/hacktivism>

[3] Liebowitz, Matt. "Anonymous Hackers Take Down Child Porn Websites, Leak Users' Names." *Security News Daily.* 20 Oct. 2011. Web. 5 Jan. 2012. <http://www.securitynewsdaily.com/anonymous-hackers-child-porn-sites-1260/>

[4] Stratfor Global Intelligence. "Beware of False Communications." *YouTube.com.* 6 Jan. 2012. Web. 6 Jan 2012. <http://www.youtube.com/user/STRATFORvideo?feature=watch>

[5] Beware of False Communications, *YouTube.com*.

[6] Perlroth, Nicole. "Hackers Breach the Web Site of Stratfor Global Intelligence." *The New York Times.* 25 Dec. 2011. Web. 5 Jan. 2012. <http://www.nytimes.com/2011/12/26/technology/hackers-breach-the-web-site-of-stratfor-global-intelligence.html?scp=1&sq=stratfor&st=cse>

[7] Perlroth, n.pag.

[8] Vinograd, Cassandra and Ramit Plushnick-Masti. "'Anonymous' Hackers Target US Security Think Tank." *Yahoo! News.* 25 Dec. 2011. Web. 5 Jan. 2012 <http://news.yahoo.com/anonymous-hackers-target-us-security-think-tank-190846242.html>

[9] Perlroth, Nicole. "Questions About Motives Behind Stratfor Hack." *The New York Times.* 27 Dec. 2011. Web. Jan 5. 2012. <http://bits.blogs.nytimes.com/2011/12/27/questions-about-motives-behind-stratfor-hack/>

[10] Albanesius, Chloe. "Stratfor Denies Hack Included Access to 'Private Client' List." *Pcmag.com.* 27 Dec. 2011. Web. 5 Jan. 2012. <http://www.pcmag.com/article2/0,2817,2398060,00.asp>

[11] Albanesius, n. pag.

[12] Perlroth, "Questions," n. pag.

[13] Perlroth, "Hackers," n. pag.

[14] Stratfor, YouTube.

[15] Stratfor Global Intelligence. *Stratfor.com.* <http://www.stratfor.com/>

[16] Billo, Charles G. and Welton Chang. "Cyber Warefare: An Analysis of the Means and Motivations of Selected Nation States." *Institute for Security Technology Studies at Dartmouth College.* Dec. 2004. Web. 5 Jan. p. 3. 2012. <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>

[17] Pentland, William. "Still Recovering From Largest Cyber Attack on Record, U.S. Military Creates 'Cyber Unit.'" *Forbes.com.* 24 July. 2011. Web. 6 Jan. 2012. <http://www.forbes.com/sites/williampentland/2011/07/24/still-recovering-from-largest-cyber-attack-on-record-u-s-military-creates-cyber-unit/>

[18] Agence France-Presse. "China Sets up Military Cyberwarfare Team: Report." *DefenseNews.com.* 27 May. 2011. Web. 6 Jan. 2012 <http://www.defensenews.com/story.php?i=6644608>

[19] Kardare, Ankita. "Fujitsu Developing Virus to Combat Cyber Threats – Japan Government Funded Project." *Crazyengineers.com.* 2 Jan. 2012. Web. 6 Jan. 2012. <http://www.crazyengineers.com/fujitsu-developing-virus-to-combat-cyber-threats-japan-government-funded-project-1540/>

[20] "Stuxnet." *The New York Times.* 15 Jan. 2011. Web. 6 Jan. 2012. <http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html?inline=nyt-classifier>

[21] "Stuxnet," n. pag.

[22] Katz, Yaakov. "Iran Embarks on $1 b. Cyber-warfare Program." *The Jerusalem Post.* 18 Dec. 2011. Web. 6 Jan. 2012. <http://www.jpost.com/Defense/Article.aspx?id=249864>

[23] "Stuxnet," n. pag.

[24] Katz, n. pag.

[25] Zetter, Kim. "Blockbuster Worm Aimed for Infrastructure, But no Proof Iran Nukes Were Hit." *Wired.com.* 23 Sept. 2010. Web. 6 Jan. 2012. <http://www.wired.com/threatlevel/2010/09/stuxnet/>

[26] Halliday, Josh. "Stuxnet Worm is the 'Work of a National Government Agency." *Theguardian.com.* 24 Sept. 2010. Web. 6 Jan. 2012. <http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency>

[27] Allen, Ian. "Experts See Nation-State Behind Sophisticated Computer Virus Attack." *Intelnews.org.* 29 Sept. 2010. Web. 6 Jan. 2012. <http://intelnews.org/2010/09/29/01-571/>

[28] Broad, William J., John Markoff and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *The New York Times.* 15 Jan. 2011. Web. 6 Jan. 2012. <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all>

[29] Broad et al., n. pag.

[30] Broad et al., n. pag.

[31] Gonslaves, Antone. "10 Security Predictions for 2012." *Crn.com.* 26 Dec. 2011. Web. 6 Jan. 2012. <http://m.crn.com/69730/show/c8379739b3dec244f54a38ab1167382a&t=g6jgm2amio26v3801438oo6sn0>

[32] Byers, Cameron. "Hacktivism: How to Stay one Step Ahead of the Trend." *Astaro.com.* 14 Nov. 2011. Web. 6 Jan. 2012. <http://www.astaro.com/blog/perspectives/hacktivism-how-to-stay-one-step-ahead>

[33] Byers, n. pag.

[34] Moss, Mitchell L. and Anthony M. Townsend. "Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications." *New York University.* April. 2005. Web. 6 Jan. 2012. p. 4. <http://www.nyu.edu/ccpr/pubs/NYU-DisasterCommunications1-Final.pdf>