Case Study: THE RISE OF CYBER-ESPIONAGE
At a Hopkinton, Massachusetts, office, an executive received an email that appeared to be from a coworker on March 1, 2011. Attached to the email was an Excel spreadsheet titled “2011 Recruitment Plan.” The man opened the spreadsheet. The email was not from a coworker, it was a carefully crafted attack known as “spearfishing” in which a fraudulent email is sent to a specific person.

The spearfishing email contained an Excel spreadsheet with a zero-day exploit and a version of the Poison Ivy RAT (remote administration tool) payload embedded. The RAT enabled a hacker to gain privileged access to the network of RSA Security (an American computer and network security company). The company had been founded by Ron Rivest, Adi Shamir, and Leonard Adleman, the inventors of the RSA public key cryptographic algorithm. This single event initiated an attack that would result in the compromise of one of the largest and most respected data security companies in the world.

Within weeks, hackers had penetrated RSA’s defenses and stolen the source code to the vaunted two-factor authentication system, SecurID. SecurID is used by an estimated 250 million people worldwide. The attack was believed to have been initiated using a zero-day exploit created by a Chinese hacker. Evidence suggests the possibility of Chinese-sponsored cyber-espionage. RSA’s CEO, Art Coviello, stated the stolen SecurID information “could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack” (italics added). This proved to be an ominous prediction.

On May 27, 2011, an employee at L-3 Communications, a major supplier of communication, intelligence, surveillance, and reconnaissance technology to the Department of Defense, noticed suspicious activity in the network. An in-
vestigation showed a hacker had accessed the network using cloned RSA SecurID tokens and potentially accessed critical intellectual property related to defense projects. This is only one of several reported attacks that seem to have originated from the RSA breach months before. It is believed that Northrup Grumman Corporation (a designer, systems integrator, and manufacturer of military aircraft) may have been targeted, and Lockheed Martin (an American aerospace, defense, security, and advanced technology company) announced that it too was the target of a “significant and tenacious” attack, which also apparently originated from the compromised RSA tokens.

By February 2012 security analysts began to acknowledge what many have known for a long time. The US government and US companies are losing the battle to protect sensitive data. At RSA’s
annual security convention, Robert Mueller, head of the Federal Bureau of Investigation, told the audience, “There are only two types of companies. Those that have been hacked, and those that will be.” Echoing his sentiments, RSA’s Coviello took the stage and ominously informed the crowd, “Our networks will be penetrated. We should no longer be surprised by this.” He added, “The reality today is that we are in an arms race with our adversaries, and right now, more often than not, they are winning.”

The comments at RSA accurately depict the state of cybersecurity today. Organizations are spending billions of dollars per year and are being literally and figuratively eviscerated by people intent on stealing data. There are growing numbers of reasons why data is stolen but, in general, the motivations can be fit into three broad categories: political or social activism, cyber-espionage, and financial crimes. Regardless of the basic motivations, the methods of attack are similar and the same techniques used to perpetrate politically motivated attacks are used to steal financial data.

During a London speech in 2007 on credit card security and compliance, a French participant stated unequivocally that the recommendations provided did not apply to companies accepting credit cards in France because, “In France we do things differently.” My response was to ask a series of simple questions. “Is the Internet in France based on the Internet protocol? Does the OSI model apply in France? Is structured query language used in France?” He sheepishly answered “yes” to all the questions. Whether the motivation is stealing credit card data, intellectual property, or state secrets, the attack principles are the same because the underlying protocols and technologies are the same.

To understand the difficulty of protecting systems from today’s attacks, it is useful to look at the concepts of unrestricted warfare and guerilla tactics. As stated in

“One man’s freedom fighter is another man’s terrorist. So let them call us terrorists. I’ll still bomb their buildings.”

—Jeremy Hammond, Anonymous hacker
ther of two who lives on public assistance in a housing project in New York's Lower East Side. With a dilapidated computer he allegedly wreaked havoc on numerous companies, including Fox, Sony, and PBS. He does not require sophisticated equipment. All he needs is knowledge, patience, time, and motivation to attack a company.

As mentioned previously, there are several motivations that drive hacking behavior. Although these motivations often intersect and may overlap, generally, they tend to be either financial or ideological. Financially driven crimes are, arguably, easier to anticipate and counter. Volumes have been written on the exploits of the Russian Business Network, BOA Factory, Mazafaka, and other alleged financially motivated criminal groups. Today, companies are also facing increasingly dangerous adversaries driven by ideology. People driven by ideology are often more dangerous and difficult to deter. Their willingness to accept greater risk and focus greater resources for less-perceived return makes them particularly challenging. There are primarily two types of ideologically motivated adversaries threatening companies today: social or politically motivated hacktavists, and “patriotic hackers” involved in cyber-espionage.

Hacktavism refers to cyberattacks or data thefts that are conducted primarily to make a political, social, or other statement. It should be noted that although the primary objective may be politically or socially motivated, these attacks often result in stolen financial and other data that may be used for financial gain. Two of the most prominent groups active today appear to be LulzSec and Anonymous.

In 2004 a relatively anonymous hacker named Jeremy Hammond presented the LulzSec manifesto at the hacker convention known as DefCon. To a chorus of boos and hisses, and with a bandana cov-
ering his face, the hacker, political activist, and self-styled anarchist known online as “anarchaos” and “crediblethreat” stated defiantly, “One man’s freedom fighter is another man’s terrorist. So let them call us terrorists.” He added moments later, “I’ll still bomb their buildings.” He served two years in prison in 2006 for cyberattacks. In 2011 Hammond was arrested again for a hack against the US intelligence company Stratfor.

Although Anonymous is believed to be a loosely knit, decentralized group of hackers whose members may overlap with those of LulzSec, its motivations can be seen in its published manifesto. Like LulzSec, Anonymous has political interests. Its manifesto states:

“The intention of Anonymous is to protect free flow of information of all types from the control of any individual, corporation, or government entity. We will do this until our proverbial, dying breath. We do this not only for ourselves, but for the citizens of the world. We are people campaigning at this very moment for your freedom of information exchange, freedom of expression, and free use of the Internet. Please remember this as you watch the news, read posts on Twitter, comment on YouTube or Facebook, or send email to a friend or loved one: Anonymous is making every effort to defend free speech and free information on the Internet.”

Anonymous concedes that it does not control, or try to control its own members’ actions.

“May we remind you that Anonymous is a dynamic entity. Furthermore, anything attributed, credited, or tagged to Anonymous is not always based on the consensus of us as a whole. Even the document you read now was written by at
least ten people simultaneously.'

State-sponsored cyber-espionage includes hacks perpetrated directly by foreign governments, or by foreign organizations and individuals associated with foreign governments. Although numerous countries engage in cyber-espionage, the largest perpetrator of cyber-espionage appears to be the People's Republic of China. Although the motivations are often ultimately financial, we see a glimpse into how China reportedly motivates attackers to perpetrate the crimes. China calls those who steal for the benefit of China, “patriot hackers”.\(^{11}\) By appealing to the patriotism of the hacker, it applies moral relativism to the act. In short, the hacker, in their eyes, is not committing a wrong, he or she is patriotically supporting China.

On April 15, 2011, the US Congressional Subcommittee on Oversight and Investigations conducted a hearing on Chinese cyber-espionage. The hearing revealed the US government's awareness of Chinese cyberattacks. In describing the situation in her opening remarks, subcommittee chairperson Dana Rohrabacher astutely stated:

“[The] United States is under attack.”\(^{12}\)

“The Communist Chinese Government has defined us as the enemy. It is buying, building and stealing whatever it takes to contain and destroy us. Again, the Chinese Government has defined us as the enemy.”

The RSA compromise, as well as the theft of data from DuPont, and the theft of intellectual property from American Superconductor, Microsoft, Cisco, and Motorola to name but a few, demonstrate the motivation and sophistication of the efforts to steal data from US companies.\(^{13}\) It should be noted that the United States is not the only victim. The United Kingdom reportedly loses $45 billion per year due to cyber-theft.

The economics of cyber-theft is simple: Stealing technology is far easier and cheaper than doing original research and development.
year from cybercrime with $28 billion in losses directly attributable to cyber-espionage.\textsuperscript{14} As detailed in the congressional report:

“The PRC utilizes a large well-organized network of enterprises, defense factories and affiliated research institutes and computer network operations to facilitate the collection of sensitive information and export-controlled technology.”

“The economics of cyber-theft is simple: Stealing technology is far easier and cheaper than doing original research and development. It is also far less risky to the spy than historic cloak and dagger economic espionage.”\textsuperscript{15}

Cybercrime has been an issue for companies since the Internet boom of the late 1990s. Early criminal efforts focused on stealing financial data such as credit and debit card information, and website defacements. Throughout the 2000s companies have been plagued with data thieves stealing financial data. Today, companies and governments are increasingly facing more dangerous hacktivist and cyberespionage attacks. Companies that have focused on protecting financial data are now faced with the daunting task of protecting intellectual property and systems from a motivated, sophisticated adversary often driven by ideology.

ABOUT THE AUTHOR

Mr. Mark is the founder of Mark Consulting Group, Inc. He is a data security and risk professional. He has consulted for numerous Fortune 500 companies and publishes the blog: www.GlobalRiskInfo.com.

END NOTES

\textsuperscript{1}http://jeffreycarr.blogspot.com/2011/06/18-days-from-0day-to-8k-rsa-attack.html (accessed 3/18/12)
\textsuperscript{5}http://www.eweek.com/c/a/Security/Northrop-Grumman-L3-Communications-Hacked-via-Cloned-RSA-SecurID-Tokens-841662/ (accessed 3/18/12)


Get your FREE EXPO PASS for limitless information sharing and networking with over 2,500 professionals in two days of exhibit time at the LARGEST stand alone military vehicles event in the world!

Benefit from 15+ free educational sessions in the Presentation Theater and evaluate the latest products from over 200 exhibitors.

REGISTER TODAY!

Quote Promo Code: CT12

Go online for complete speaker and agenda details! www.MilitaryVehiclesExpo.com/CT12

NEW EXPO PASSORS!

FREE EXPO PASS for limitless information sharing and networking with over 2,500 professionals in two days of exhibit time at the LARGEST stand alone military vehicles event in the world!

Benefit from 15+ free educational sessions in the Presentation Theater and evaluate the latest products from over 200 exhibitors.

REGISTER TODAY!

Quote Promo Code: CT12

Go online for complete speaker and agenda details! www.MilitaryVehiclesExpo.com/CT12


\textsuperscript{7}21st Century U.S. Military Manuals: Mao Tse-tung on Guerrilla Warfare (Yu Chi Chan) U.S. Marine Corps Reference Publication FMFRP 12-18 (accessed 3/12/12)


\textsuperscript{10}http://www.indybay.org/news-articles/2010/12/09/18666107.php (accessed 3/12/12)


\textsuperscript{14}http://cyberpointllc.com/news_09.html (accessed 3/13/12)