Proceedings of the 13th Colloquium for Information Systems Security Education
University of Alaska, Fairbanks
Seattle, WA June 1 - 3, 2009

Case Study: Using Security Awareness to Combat the Advanced Persistent Threat

Allen M. Smith, Nancy Y. Toppel, *Northrop Grumman Corporation*

Abstract – United States (U.S.) government agencies and defense contractors are the target of extremely complex foreign state-sponsored cyber attacks referred to as the "advanced persistent threat." These attacks are intended to steal sensitive information, such as national defense, research and development, and personal information. While the techniques for information gathering to determine targets (both information assets and people) may be complex, a common method used for infiltrating networks is simple social engineering. Technical controls may be used to tighten access controls but are not the total solution. Changing employee behavior through security awareness is required. This paper describes the project implemented by a U.S. defense contractor to communicate to its large employee population the risks associated with the advanced persistent threat, awareness of situations that should alarm, and the actions that employees should take to minimize this risk.

Index terms – advanced persistent threat, espionage, information security awareness

I. Introduction

Over the past few years, the United States (U.S.) government and U.S. defense contractors have detected an increasing number of attempted cyber attacks on their networks [1] [2]. In the 2007-2008 fiscal year, government agencies reported almost 13,000 cyber security incidents to the U.S. Homeland Security Department, three times the number reported two years prior [1]. This rise in cyber attacks has been attributed to cyber espionage - foreign countries' desire to obtain U.S. information or technology. These cyber espionage attacks, now referred to as the "advanced persistent threat," are extremely complex, foreign state-sponsored attacks that attempt to obtain financial, strategic, technology, national defense, and personal information [1] [3]. As discussed in the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* [4], targeted technologies include aeronautics, information technologies, lasers, sensors, and optics. Unique manufacturing processes and trade secrets are targeted as well [4].

The adversaries involved in the advanced persistent threat are not amateur hackers seeking "bragging rights" from a simple penetration of a company's network defenses. Their efforts are well-funded, and their goals are to gain detailed knowledge of company networks and obtain deep and long-term access to those networks. Their methodology includes obtaining valid employee credentials in order to conduct their operations. In this way, they are able to navigate around a company network as any allowed user would, with the same accesses of the user whose credentials they have stolen.

The adversaries determine their targets by complex, time-consuming investigation and information gathering. Government agencies, companies, projects, programs, and employees of interest may be found by researching the Internet, the media, and other public information sources. More information on targeted individuals may be gathered from social networking sites (such as MySpace) blogs, or chat rooms. Lost or stolen computers, cell phones, and portable storage devices may hold company or employee information, or further clues on how to access the company network. Requests for information may also be made directly to employees about the work they do or their personal lives, via e-mail or in person. Direct contact with employees at industry conferences or other events may allow the adversaries to gather even more information from seemingly innocent, friendly conversation.

Once target employees are identified, the adversaries frequently use social engineering principles to obtain valid user credentials. From their information gathering, they will target specific employee groups or organizations with "spear phishing" e-mail. Using information that makes the spear phishing e-mail appear legitimate, they trick the user into divulging personal or sensitive information or click on a link or attachment that contains malicious software. Once the user clicks on the link or attachment, malicious software is installed that allows the adversary to gain control of the system and access to the network with valid employee credentials [1].

Because the adversaries use valid user credentials and are able to log on to a network as any trusted employee

would, relying on network perimeter defenses is no longer effective. To traditional perimeter defenses, this activity appears perfectly legitimate and access is unquestioned. Therefore, in addition to implementing strong technical controls at the perimeter and within the company network to detect and respond to attacks, attention must also be focused on the human factor, on security awareness.

To increase awareness of the advanced persistent threat to its employees, and to educate them on their responsibility, Northrop Grumman has implemented an internal information security awareness campaign focused on identifying specific threats related to the advanced persistent threat, and reinforcing desired employee behaviors that help to minimize the risks. This paper describes the techniques used and challenges faced in executing this targeted security awareness program.

II. Background

Northrop Grumman Corporation is a leading global security company that provides systems, products, and solutions in aerospace, electronics, information systems, shipbuilding, and technical services to government and commercial customers worldwide [5]. A $34 billion company (2008 fiscal year) with 120,000 employees worldwide, Northrop Grumman is one of the top providers of information technology to the federal government and the nation's second largest defense contractor, and therefore has a key role in protecting the information generated and used on those sensitive projects from unauthorized access. Safeguarding this information, in addition to company and employee information, is essential to maintaining Northrop Grumman's competitive advantage, customer trust, and the security of the nation.

Northrop Grumman has taken a very proactive approach to the challenge of protecting its data in the face of the ever-changing threat by hackers, criminal elements, and now, nation states, and maintains 24 x 7 monitoring and response against potential threats. Northrop Grumman has been very successful in mitigating threats to its network through implementation of information security best practices, including rapid security patching of major operating systems and applications, e-mail protections to guard against malicious spam, use of multi-factor authentication for remote access to the company network, and blocking access to known malicious Web sites.

In addition to technical controls, Northrop Grumman's executive management understands the role that the non-technical "human factor" plays in the protection of company information assets [6], [7]. Northrop Grumman has had an ongoing company-wide information security awareness campaign in place for several years, which includes monthly awareness communications and mandatory annual information security awareness courses.

Northrop Grumman has again pursued both technical and non-technical means to further protect its network and information assets to combat the advanced persistent threat. Because adversaries are targeting individuals as the keys into corporate and government systems, Northrop Grumman wanted to arm its employees with awareness of good information security practices in response to the new and complex dangers posed by the advanced persistent threat.

A separate team within the company was charged with designing and implementing a communications campaign specifically designed to increase awareness of the advanced persistent threat among Northrop Grumman employees. Although there are many sources of information on general security awareness campaigns, including those released by the National Institute of Standards and Technology (NIST) [9] [11], there has been little information available on the successes or failures of security awareness methods employed specifically to manage the advanced persistent threat. Subject matter experts within the company, who have relationships with peers in industry with similar concerns, were relied upon to provide guidance on topics and behaviors to be reinforced through the communications campaign.

III. Attack Methods and Targets

With the advanced persistent threat, the adversaries attempt to gain long-term access to a company network by using valid user credentials so they have less chance of being detected. To do this, the adversaries frequently employ teams of people to gather information about employees from various sources, such as publicly available information on the Internet [3], [8]. Sophisticated programs combine these multiple pieces of innocuous information together to create a profile of a "person of interest" to the adversaries. Those who appear to have access to the most sensitive information (such as executives and program management) or have elevated privileges on systems (such as system administrators) are key targets. The adversaries then launch a targeted attack on the person of interest to attempt to obtain his or her employee credentials and other sensitive information.

Employees must understand the methods used by the adversaries to gather information about a company and its employees. Understanding the tactics used allows them to recognize those situations where they are at risk so that they can change their behavior and also know when and how to report suspected incidents.

Information Acquisition: The first phase of the attack consists of gathering information about potential "persons of interest." Two of the simplest methods used are gathering information from public sources and venues, and social engineering. These methods cannot be thwarted through technical controls, but require employees to understand and apply good information security practices to better control the information that they disclose to others who may be potential adversaries.

1. *Information collected from public sources and venues:* Company e-mail addresses, affiliations, and project information can be obtained easily from various sources on the Internet, including industry networking sites, publicly available research papers, directories from academic institutions, and industry conference proceedings. Conferences almost always provide a list of attendees, including contact information. Personal information is also of interest to the adversaries, and is much more accessible as individuals freely post information about themselves, their interests, and their families on the Internet on social networking sites.

2. *Social engineering*: The adversaries may obtain information by manipulating a victim into divulging sensitive or personal information via phone calls, e-mail, or personal contact. The adversary may attempt to rush the victim with a sense of urgency (e.g., pretend to be an executive with an "urgent" request), or prey on the victim's empathy (e.g., pretend to have a demanding boss with an urgent request). Adversaries may also attempt to gain information through "friendly" conversation or eavesdropping at industry conferences, employer-sponsored classes, or other public places.

Credential Acquisition: Based on the information acquired, targets and associated e-mail addresses are identified. The most common attack method used by the adversaries to obtain employee credentials is spear phishing.

Spear phishing is a form of social engineering in which a targeted e-mail appears to be sent from a familiar source (such as a fellow employee or a manager) or company organization and includes language that implies the sender is familiar with the company or a particular project. The e-mail usually contains malicious software embedded in an attachment (such as a PDF file or PowerPoint presentation) or a link to a Web site. Once the employee clicks on the link or attachment, the malicious software is installed, potentially giving the adversary access to the employee's system and his employee credentials.

Once valid credentials are obtained, the adversary has access to all of the data, systems, and applications that the employee can access. The adversary may also use this entry point to gather information on other persons of interest, continuing the cycle in order to steal additional employee credentials and find sensitive project, company, and employee data.

IV. Security Awareness Campaign Development

At Northrop Grumman, the Information Security organization is charged with conducting the information security awareness campaign, which includes the communication and training mentioned earlier. For the advanced persistent threat awareness campaign, Information Security employees have teamed with individuals in the communications department to develop and execute the campaign. Executive buy-in was essential to providing resources and "legitimacy" to the campaign, and understanding the communication processes and vehicles was essential to distribute the message effectively in a company as large as Northrop Grumman [12]. The following steps were completed to develop the campaign:

Leadership sponsorship [12]: Management buy-in was necessary in order to obtain the resources and funding to plan and launch a security awareness program. The advanced persistent threat awareness campaign was sponsored by the vice president and corporate information security officer (CISO), whose participation in the executive security and policy councils ensured executive leadership support.

Policy, strategy, and implementation model [9]: The existing organizational roles and responsibilities were considered in creating security policy, developing the strategy for the security awareness program, and implementing the strategy. The size and geographical dispersion of the organization were determining factors as well.

Campaign team members: A team was assembled to develop, approve, and disseminate the information, with the communications organization taking the lead on overall campaign planning. The team included the advanced persistent threat program execution manager as the subject matter expert, and resources from the information security awareness and communications groups. Three information security directors were included in the approval team for all communications.

Needs assessment [9]: A needs assessment provided justification for the resources required to implement the program. Target audiences for specialized awareness training were also identified. At Northrop Grumman, employees who have e-mail addresses and/or network accounts were identified as the primary target audience. System administrators were also identified as a target audience because of their elevated privileges on company systems.

Survey of communication vehicles: Existing processes were studied to determine if they could be adapted to the new campaign, and new communication vehicles were considered. Northrop Grumman's existing information security awareness campaign provided a good model for a monthly communications format and the internal Web site design. Existing Web-based training modules were considered a possible vehicle in which to add advanced persistent threat awareness as a topic. Higher visibility for advanced persistent threat messages was obtained by releasing them through corporate communications.

Branding [10]: For this campaign, a one-line tagline and a short boilerplate paragraph describing the advanced persistent threat were used to provide recognition of advanced persistent threat campaign-related material.

Information sources [9]: Subject matter experts used information from threat monitoring and situational awareness to alert the team to awareness of events, potential exploits or threats that need to be communicated.

V. Awareness vehicles

The communication campaign used a number of communication vehicles and techniques to reach and engage Northrop Grumman's large employee base [12]. The cornerstones of the program were the company's internal advanced persistent threat Web site and monthly communications.

Intranet Web site: An internal Web site was developed to provide a central location for employees to obtain information about the advanced persistent threat. The site includes links to the archives of all released communications, links to Internet articles, terms and Frequently Asked Questions (FAQs). A link to the site is part of the boilerplate text included at the end of all communications.

Monthly communications [9] [11]: A one-page awareness communication is developed each month, explaining a potential risk related to the advanced persistent threat and describing the desired employee behavior in response to the problem or issue [11]. Current potential threats and news stories to illustrate the threat and consequences are used when possible. The information is presented in a question and answer format. Applicable company policies and procedures are referenced for reinforcement. Each communication includes the tagline and boilerplate text.

Topics have included:

1. Introduction to the advanced persistent threat and what it means to Northrop Grumman
2. Travel advisory – keeping company data safe while traveling abroad
3. The difference between spam e-mail and spear phishing e-mail
4. General tips on what to look for in an e-mail to determine whether it is a spear phishing attempt

The monthly communications are released by the corporate communications organization to each business sector's communication organization for release to their population via their preferred distribution method. Distribution methods may include direct e-mail, a regularly scheduled e-mail newsletter, or posting the communication on an internal business sector Web site.

Audio vignette [9] [11]: A five minute audio message with graphics was created as a general introduction to the advanced persistent threat. A link to the vignette is part of the boilerplate text included at the end of all communications, and is also accessible from the advanced persistent threat internal Web site.

Audio message from the vice president and CISO [12]: An e-mail directly from an executive catches employees' attention. This e-mail includes a three-minute audio interview with the CISO, giving his perspective on the advanced persistent threat, its potential negative effect on the company, and the employee's responsibilities in combating the threat.

Management briefing [9]: In a large company, important company messages need to be flowed down from management. This shows buy-in and support from the employee's management, and identifies the subject as a priority. A PowerPoint presentation with extensive notes describing the advanced persistent threat has been distributed to all managers to flow down to their employees.

Incorporation into existing communication and training vehicles: In order to capitalize on the work being done in the existing information security awareness campaign, efforts were made to incorporate the advanced persistent threat message into those projects as well:

1. *Mandatory employee awareness training [9] [11]:* As directed by company policy and procedure, employees are required to complete an internal information security awareness course on a yearly basis, to reinforce knowledge of company information security policies and procedures. Web-based training and text-copy are available. Information on the advanced persistent threat was incorporated into the training course that is being offered in 2009.

2. *Mandatory security awareness training for system administrators [9] [11]:* System administrators are required to take additional yearly security awareness

training to reinforce awareness of company security policies and procedures that are applicable to those with elevated privileges on company systems. System administrators have been determined to be a prime target for the adversaries because of their elevated access privileges. Information on the advanced persistent threat and best practices is included in the 2009 system administrator security awareness training.

3. *Messages on awareness giveaways [9] [11]:* Giveaways have been distributed at various company sites during company security awareness month events. The giveaways feature the advanced persistent threat campaign tagline and a URL to the internal Web site.

4. *Contest [9]*: The general campaign includes a yearly contest to engage employees in testing their security awareness knowledge, and to give the advanced persistent threat communications team feedback as to whether its messages are reaching the employees. The 2008 contest featured a 10-question security quiz, and advanced persistent threat awareness was the topic of one of the questions.

5. *Feedback and questions [12]:* A central internal e-mail address for general information security questions is advertised on all communication and training vehicles. Employees with questions regarding the advanced persistent threat are also referred to the same e-mail address.

6. *Security awareness events [9]*: November is traditionally the month that security, including information security, is emphasized with in-person/booth events. These events are advertised within the company and held around lunch time near cafeterias at larger sites to attract the most employees. Posters are displayed, branded giveaways provided and information security professionals available to answer any questions.

VI. Challenges

There were several challenges that were encountered when planning and implementing this awareness campaign.

Lack of public information on attacks: Citing "real world" examples of threats and consequences is an effective tool in conveying the importance of security awareness. But, because of the sensitive nature of cyber-espionage and the concern over losing customer trust, companies and government agencies do not divulge much information on the details of advanced persistent threat attacks to the media. Because of the nature of the threat, the campaign team only wanted to cite publicly available articles and sources.

Difficulty explaining desired employee behavior: With spear phishing attempts, e-mail parameters are spoofed (faked) to look like legitimate e-mail from a familiar source. Employees can only be cautioned to be suspicious of unexpected e-mails– they don't have the technical expertise and specialized tools to determine with certainty whether an e-mail is spoofed. Using digital signatures and encrypting e-mail are recommended practices, but are not yet widely deployed. Employees are asked to rely on intuition in these cases and report anything that seems suspicious. Also, since there are two separate special e-mail addresses for reporting spam and suspected incidents, employees must also be educated on the difference between spam and what may be a potential security incident.

Preventing over-saturation or overlap of information security messages: Employees are receiving communications regularly, from their business sector, the enterprise, and other operating units within the company. Communications sent more frequently than once a month have been determined in other campaigns to cause over-saturation, in which employees start ignoring messages. Also, the general information security campaign has its own monthly communication vehicle. Care is taken to ensure topics and distribution dates do not conflict.

Large, widely distributed employee base: Northrop Grumman has a large, geographically dispersed employee base in which some employees work at customer sites without access to the company network or are based primarily at their homes. Communicating effectively to such a diverse population is a challenge and requires multiple modes of communication in which to disseminate the messages.

Lack of more obvious branding: Attention-grabbing branding such as a logo is recommended to build recognition for the awareness program [10]. The communications team leading the communications effort recommended that a tagline and short boilerplate paragraph be used instead of a logo or slogan.

Decentralized distribution of messages: Corporate communication is selective about the types of messages sent corporate-wide via e-mail. Therefore, advanced persistent threat messages have been sent out in a more decentralized way. The corporate office releases the monthly messages as syndicated stories to the five business sectors' communications groups. Each business sector communications group distributes the information based on its standard process – via direct e-mail to the employee, inclusion in a weekly e-mail newsletter, or posted on the business unit intranet Web site.

VII. Metrics [9]

Metrics play an important role in determining if an awareness campaign is effective [10], and justifying

budget and resources for the campaign. The following metrics have been developed for the advanced persistent threat awareness campaign:

Web site hits: The number of hits to the internal advanced persistent threat Web site is tracked on a weekly and monthly basis. Increases in Web site hits have been observed immediately after communications are released. An exponential increase in Web site hits was tracked after an e-mail and audio message from to the vice president and CISO was released, demonstrating that employees are responsive to direct e-mail from executive management.

Training course completions: The completions for both the employee awareness training and the system administrator training are tracked to ensure compliance with policy and procedure regarding mandatory training. Adding the advanced persistent threat topic to both courses in 2009 will ensure that employees are exposed to the basic awareness information.

Web Survey [9]: To establish a "baseline of awareness" at the beginning of the campaign, a Web survey was sent to 5,000 randomly chosen employees. The twofold purpose of the survey was to determine whether the employees were aware of the advanced persistent threat and to engage their feedback on how to more effectively distribute the messages. The baseline survey revealed 57 percent awareness of advanced persistent threat prior to a full-fledged campaign.

Although many employees understood what advanced persistent threat meant and what their role is in combating it, a fair portion of the employees had not received information on the advanced persistent threat efforts consistently. The advanced persistent threat team was able to use survey feedback to fine tune the campaign to reach more employees. A follow-up survey will be conducted so that improvements can be measured and more feedback can be collected to ensure continuous process improvement.

VIII. Conclusion

Ongoing and malicious cyber attacks toward governments and defense companies have escalated over the recent years, making it imperative that employees in these environments understand how to recognize and thwart cyber spies.

Employees serve an important role in the frontline defense against cyber spies, as employees are often the first targeted as a means to gain access to corporate networks.

Northrop Grumman has demonstrated a viable approach in combating the advanced persistent threat through engaging its employees in a multi-faceted and sequential communications approach.

This approach also underscores the strategic value of effective internal communications, and the ability of those from within the Information Security, Internal Communications, and other corporate areas to join together to build, refine, execute and measure results of the awareness campaign and plan.

References

[1] Grow, Brian, Epstein, Keith, Tschang, Chi-Chu. *The New E-spionage Threat.* April 10, 2008. Business Week. Retrieved February 4, 2009 from http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

[2] Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, February 27, 2008. Retrieved February 11, 2009 from http://www.dni.gov/testimonies/20080227_testimony.pdf

[3] Greenberg, Andy. *Cyberspies Target Silent Victims.* September 11, 2007. Forbes.com. Retrieved February 4, 2009 from http://www.forbes.com/2007/09/11/cyberspies-raytheon-lockheed-tech-cx_ag_0911cyberspies.html

[4] Office of the National Counterintelligence Executive. Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07. September 10, 2008. Retrieved February 5, 2009 from http://www.ncix.gov/publications/reports/fecie_all/fecie_2007/FECIE_2007.pdf

[5] Northrop Grumman Web site. Retrieved February 9, 2009 from http://www.ngc.com.

[6] Hayes, Heather B. *On Their Toes.* Fed Tech Magazine. January 2008. Retrieved February 9, 2009 from http://fedtechmagazine.com/article.asp?item_id=353

[7] Walsh, Katherine. *Northrop Grumman's Timothy McKnight on Security and Identity Management.* CSOonline.com. February, 12, 2008. Retrieved February 9, 2009, from http://www.csoonline.com/article/217032/Northrop_Grumman_s_Timothy_McKnight_on_Security_and_Identity_Management?page=1

[8] Acohido, Bryan. *Internet Thieves Make Big Money Stealing Corporate Info.* USA Today. November 14, 2008. Retrieved February 4, 2009 from

http://www.usatoday.com/tech/news/surveillance/2008-11-11-thieves-cyber-corporate-data_N.htm

[9] Wilson, Mark and Hash, Joan. National Institute of Standards and Technology (NIST) Special Publication 800-50: "Building an Information Security Awareness and Training Program," October, 2003. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[10] Information Risk Executive Council. *Inflecting End-User Awareness: High-ROI Tactics for Sustainable Behavior Change. 200*6. Retrieved February 5, 2009 from http://irec.executiveboard.com

[11] Wilson, Mark, Editor. National Institute of Standards and Technology (NIST) Special Publication 800-16: "Information Technology Security Training Requirements: A Role- and Performance-Based Model," April 1998. Retrieved April 3, 2009 from http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

[12] Hansen, E. Kelly. "Success Strategies for Security Awareness." May 6, 2004. Techrepublic.com. Retrieved April 3, 2009 from http://articles.techrepublic.com.com/5100-10878_11-5193710.html