Journal of Applied Digital Evidence

Volume 1 | Issue 1

Article 1

2018

Social Engineering in Non-Linear Warfare

Bill Gardner
Marshall University, bill.gardner@marshall.edu

Social Engineering in Non-Linear Warfare

In January 2017, the FBI, NSA, DIA, and CIA coordinated their efforts as the United States Intelligence Community (IC), under the authority of the Office of National Intelligence, and published *Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections*. This document is a declassified and redacted version of a highly classified assessment that was provided to President Obama, who subsequently approved it for public release. Although the IC rarely divulges such assessments, Obama administration officials deemed it highly important to provide the public with its contents to shed light on Russian interference in the 2016 United States presidential election (United States Intelligence Community, 2017).

The report came on the heels of allegations that Russia had taken down the Ukraine power grid with a spear-phishing attack that began in March 2015. "[…] emails to utility employees looked like they contained data about military mobilization. Workers who clicked MS Office files to 'enable macros' infected their workstations with remote access Trojans, the hackers moved laterally through the network and finally stole the credentials to access the utilities' operations systems" (Sjowerman, 2016, para. 11).

Russia has a lively history of non-linear warfare. In 2007, a disagreement between Estonia and Russia over the relocation of the "Bronze Soldier of Tallinn" statue and Russian war graves in Tallinn resulted in a series of massive coordinated cyber attacks on the Estonian public and private sectors, which put banks, parliament, ministries, newspapers, and TV stations offline (Rehman, 2013). Before a shot was fired in the Georgian conflict in 2008, Russian hackers began a cyber campaign that included the defacement of the Georgian parliament website and multiple denial of service attacks that took many other

Georgian sites offline (Hollis, 2011; Markoff, 2008). Hollis (2011) points out, "The Russian-Georgian war was quite historic and precedent setting for several reasons. This appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains (consisting of Land, Air, Sea, and Space)" (pp. 1-2). Russia has long been known for a combined arms approach to war. The domains have evolved to now consist of Land, Air, Sea, Space and Cyberspace. The combined arms approach to warfare reaches back to the days of the Soviet Union and the new focus on Cyberspace includes "The Russian Federation: Information Warfare Framework" (Carr, 2011).

A Brief History of Cyber Warfare, Information Warfare, and Non-Linear War

Cyberwar can be defined as a nation-state versus nation-state operation. In some cases, it appears that nation-states have used patriotic hackers and hacker gangs to further their national interest. We refer to these actions as cyberwar as well. Cyberwar has recently become a hot button issue, with most of the blame for intrusions being directed to the Chinese government. What we today call cyberwar, however, is not new. In 2003, an estimated three-year period of coordinated attacks on American computer systems began (Bodmer, Kilger, Carpenter, & Jones, 2012). The US government codenamed this series of attacks, which have been attributed to the Chinese government, as "Titan Rain" (Espiner, 2005).

Prior to this report, news headlines throughout the years have covered the use of new types of targeted weapons in what we now label as cyberwar. The most notable of these new "cyber weapons" is Stuxnet. The Stuxnet worm, a suspected US-Israel joint operation, targeted centrifuges at the Natanz uranium enrichment plant in Iran, which set

back the Iranian nuclear program for years and bypassed the need for conventional military intervention (Zetter, 2011, 2013).

A subset of cyberwar is cyber espionage. In September 2010, a number of Canadian-based law firms were reportedly breached by China-based hackers looking to derail the $40 billion acquisition of the world's largest potash producer by an Australian mining company (Riley & Pearson, 2012). On February 18, 2013, the Internet security firm Mandiant released a report, which claimed that it had hard evidence that the Chinese army was responsible for supplicated intrusions into US networks to steal sensitive data and trade secrets from both governmental and nongovernmental organizations (McWhorter, 2013).

While these tactics are not new, Russia has in recent years leveraged cyber and information warfare into a non-linear war against the West. The new strategy was identified by Pomerantsev (2014): The Kremlin's approach might be called "non-linear war," a term used in a short story written by one of Putin's closest political advisors, Vladislav Surkov, which was published under his pseudonym, Nathan Dubovitsky, just a few days before the annexation of Crimea. Surkov is credited with inventing the system of "managed democracy" that has dominated Russia in the 21st century, and his new portfolio focuses on foreign policy. This time, he sets his new story in a dystopian future, after the "fifth world war" (para. 2).

Surkov writes:

> It was the first non-linear war. In the primitive wars of the 19th and 20th centuries it was common for just two sides to fight. Two countries, two blocks of allies. Now four coalitions collided. Not two against two, or three against one. All against all (as cited in Pomerantsev, 2014, para. 3).

The Democratic National Committee Breach

In a breach of the Democratic National Committee, Russian hackers leveraged social engineering techniques to compromise the email of DNC official and Clinton campaign manager John Podesta, which is a key piece of the ongoing allegation that Russia used cyber and information warfare techniques to influence the 2016 U.S. elections (United States Intelligence Community, 2017).

Hackers do not break in through firewalls anymore; they now bypass them by targeting the user directly. Organizations have spent billions of dollars developing layered defenses against online attackers. Such protections include antivirus programs, intrusion detection systems, intrusion prevention systems, and other technical solutions to safeguard information. With these sophisticated solutions in place, attackers are now turning to more targeted methods focused on tricking users into clicking links or opening attachments Such tactics are referred to as social engineering, which is defined by the Social Engineering Framework (2017) as "any act that influences a person to take an action that may or may not be in their best interest" (para. 1). More specifically, this process entails deceiving people to gain access to restricted areas or systems and confidential information. In information security, humans are the weakest link. Employees generally wish to be helpful and provide good service to clients, vendors, and coworkers. People are also curious. Social engineers seek to exploit these characteristics in humans.

Russia has adopted social engineering as a key component of non-linear warfare. One recent example includes the events leading up to the DNC breach in March of last year. "Hillary Clinton's campaign chairman John Podesta received an alarming email that appeared to come from Google. The email, however, was actually an attempt to hack into his

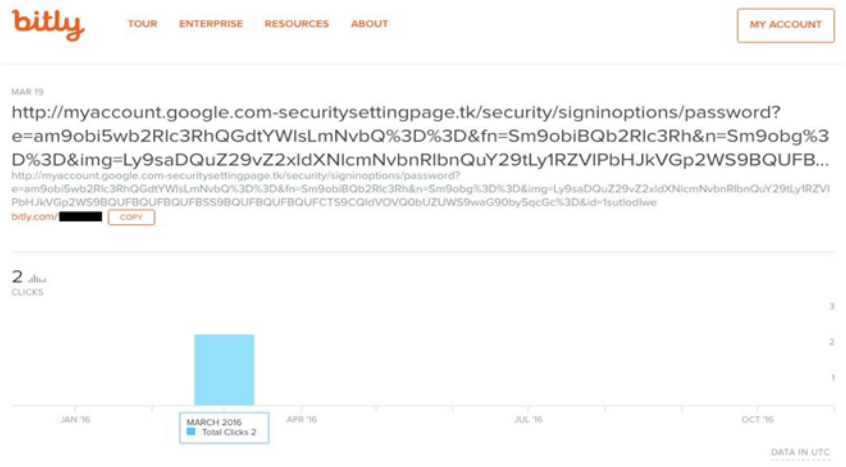
personal account. The message came from a group of hackers that security researchers, as well as the US government, believe are working for the Russian government. At the time, however, Podesta was unaware of the attack and clicked on the malicious link contained in the email, ultimately giving hackers access to his account" ("How Hackers Broke into," 2016). In October of 2016, one month before the general election, WikiLeaks began publishing thousands of Podesta's hacked emails. ("How Hackers Broke into," 2016)

After the Podesta email leak, investigators discovered evidence that pointed to the hack being backed by Russia. The malware used in the attack was dubbed Fancy Bear, APT28, or Sofacy, when they found a common thread of malware used in other DNC related leaks. These leaks appeared on a website named "DC Leaks" and included the hacked emails of Colin Powell. "All these hacks were done using the same tool: malicious short URLs hidden in fake Gmail messages. And those URLs, according to a security firm that has tracked them for a year, were created with Bitly accounts linked to a domain under the control of Fancy Bear. The phishing email that Podesta received on March 19 contained a URL, created with the popular Bitly shortening service, pointing to a longer URL that, to an untrained eye, looked like a Google link." ("How Hackers Broke into," 2016)

Below is an image[1] of the Bitly link used to compromise Podesta's Gmail account. While it is not particularly well crafted, the link redirecting to the Bitly link was sufficient

[1] "A screenshot of the Bitly link used against John Podesta." (2016). *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/mg7xjb/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts

enough to deceive Podesta into clicking and downloading the malware.



In 2009, Google, Adobe, and a number of other high-profile companies were targeted in an attack that came to be known as Operation Aurora. The attack, which originated from China, was aimed at the intellectual property of targeted companies. This intellectual property included source code that controlled major systems, including Google's Gmail service. The attackers then used the information gained through the breach to access the Gmail accounts of human rights activists (Zetter, 2010). Dmitri Alperovitch, McAfee's vice president of threat research commented, "We have never ever, outside of the defense industry, seen commercial industrial companies come under that level of sophisticated attack. It's totally changing the threat model" (as cited in Zetter, 2010, para. 2).

How Social Engineering Works

Not all social engineering attacks are designed to yield pieces of sensitive information, such as passwords. Some are meant to obtain a piece of information that seems insignificant to the target, such as the name of their cleaning company. The attacker

uses these smaller pieces of information to create a cover story, or pretext, to perform an attack (Gardner & Thomas, 2014).

Social engineers examine the target's website closely for some obvious reasons, such as identifying their industry and products/services. This can also be classified as open source intelligence gathering, as the attackers are using public sources to gather information. These sources include websites, annual reports, news stories, as well as publicly available government documents. Attackers will use an organization's web site to gather the following information:

- Number of employees—It is more difficult to social engineer an organization where everyone is on a first-name basis. Difficult but not impossible.
- Locations—Understanding where the target's offices are located is crucial. If the attacker is going to impersonate an employee from engineering, they want to be sure that their target is not sitting in the next cubicle.
- Job openings—Detailed postings provide insight into specific technologies that the target may be using, such as antivirus and intrusion detection systems (IDS). Job postings also provide high-level detail on where company departments are located. For example, three accounting jobs are posted with a location of Dallas.
- Names of executives and managers—This information can be used to draft an organizational chart.

- E-mail address format—Once an attacker knows the target's e-mail scheme, such as john.smith@abc.com, they can create e-mail lists with names discovered from other sources. The user's naming scheme in their e-mail address can sometimes be the same format for their login username.
- Current events—Has the target company merged with another company recently? Posing as an employee from the newly acquired company could be a possible attack vector. Are they having any events that are open to the public? These events can be an opportunity to learn company lingo and observe their level of security awareness.

Ultimately, attackers need a granular understanding of the target to pose as an employee or trusted insider. The company website is a valuable intelligence source, but it is not the only one. Social media websites are great for staying connected with friends and colleagues, and they are also fertile hunting ground for attackers. Facebook and Twitter often provide an in-depth look into the personal lives of potential targets. In addition to a near real-time update of an individual's activities, other pieces of useful information can also be gleaned. Examples include

- names of family members;
- high school attended;
- birthday;
- names of pets;
- favorite color;
- hobbies or interests;

The aforementioned items provide potential answers to password resets or other security-related questions. These pieces of personal information also provide an attacker with potential attack vectors for infecting the victim's computer.

In addition to sites such as Facebook and Twitter, LinkedIn yields an even greater amount of particularly useful information. To a social engineer, the site is a shopping list for targets. The granular search options allow for filters such as current employer, previous employer, physical location, industry, and more. Want to know who works in the engineering department of the target company? With a premium LinkedIn account and a few tailored searches, a list is available in a matter of minutes. Better yet, most profiles include a partial resume detailing job duties and technical skills, which provide an overview of defensive technologies in place at the target organization.

Using any search engine of choice, it may be possible to obtain "juicy" documents. These may contain internal information such as common acronyms, financial details, network diagrams, and other items of interest. Some refer to this process as "Google hacking" (Gardner & Thomas, 2014).

Types of Social Engineering Attacks

The RSA Advanced Threat Intelligence Team first defined Watering Hole attacks in 2012.

According to Gragido (2012), Watering Hole attacks have three phases:

1. The victim visits a compromised "watering hole" website.
2. This website, through an injected JavaScript element, redirects the visiting browser to an exploit site.

3. This exploit site checks that the visiting machine is running a Windows operating system and a version of Internet Explorer, and then exploits the Java client on the visiting host, installing a 'gh0st RAT' (Remote Access Trojan) variant.

A recent example of a water hole, or watering hole, attack is the use of a compromised website containing the menu for a Chinese restaurant to serve exploits to a targeted oil company. As a result, the attackers circumvented numerous sophisticated defensive measures that the company had paid a hefty sum to implement.

> "Unable to breach the computer network at a big oil company, hackers infected with malware the online menu of a Chinese restaurant that was popular with employees. When the workers browsed the menu, they inadvertently downloaded code that gave the attackers a foothold in the business's vast computer network" (Perlroth, 2014).

Watering hole attacks, while not as common as phishing attacks, have increased in number over the past few years as users improve in spotting phishing attacks. Due to the requirement of compromising a site that the target regularly uses, which increases the complexity of carrying out the attack, watering hole attacks will likely never surpass spear phishing attacks in popularity. Phishing campaigns, such as the DNC Gmail are much less complex to execute. In the case of the DNC breach, the attackers targeted Gmail.

Remote Access Trojans

The common attack vectors in Operation Aurora, Operating Shady RAT (Remote Access Trojan), and the targeted attacks against RSA and defense contractors were all highly targeted spear phishing campaigns. This previously unknown malware siphoned

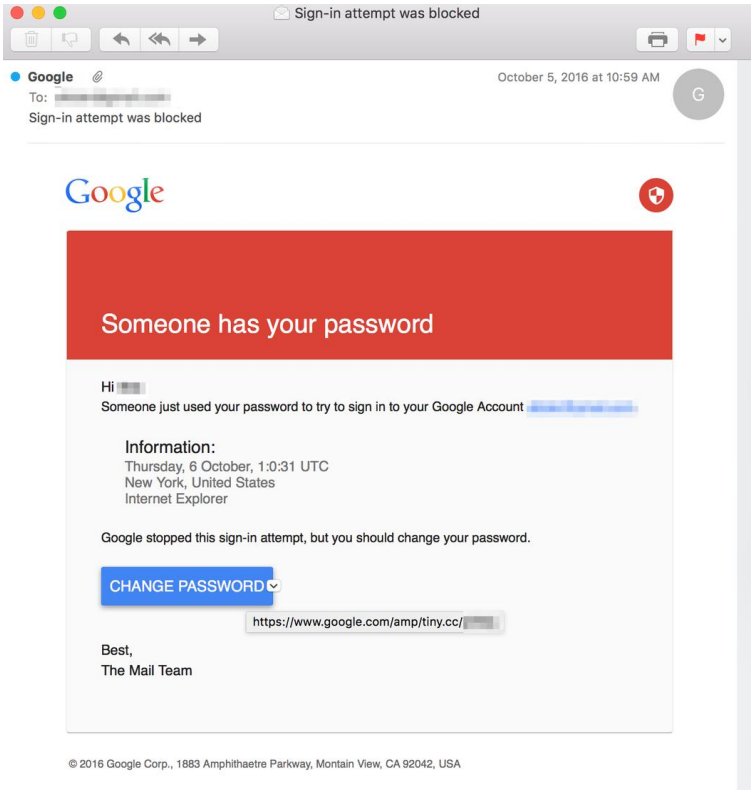
confidential information and intellectual property out of each organization. The other commonality is that these organizations have spent millions, if not tens of millions, of dollars on antivirus, intrusion detection systems, intrusion prevention systems, and other information security defenses only to have such measures internally circumvented. Someone inside of the organization simply opened a link or an attachment contained in an e-mail, which led to the compromise of their entire enterprise networks.

All organizations, regardless of size, contain information that is of interest to attackers– and they will use any means possible to gain access to it. Smaller breaches often go unreported because an organization is unaware of an intrusion or is reluctant to admit a data compromise to business partners and customers. While most social engineering attacks are nontechnical, the results can be disastrous for the target when these attacks are combined with technical methods.

Spear Phishing

A similar approach was taken using spear phishing that lead to the compromise of Colin Powell's Gmail account. An example screenshot[2] of the fake email used in this campaign is below. It has been reported that other journalists and key current and former US government employees have been targeted by the same malware. Security researchers also say that this malware points directly back at Moscow and an attempt to influence the US election cycle because of the type of malware used in the attacks.

[2] "A screenshot of a phishing email received by a Bellingcat journalist." (2016). *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/mg7xjb/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts



In general, a spear phishing message:

- addresses the recipient by name
- appears to be sent by a person or vendor that the recipient is familiar with
- includes a proper signature block with logo and contact information
- often includes an infected attachment
- can contain a link to a website similar to the sender's (abcbank.com instead of abc-bank.com)

While other phishing e-mails are sent in large quantities, spear phishing e-mails are sent to very few employees—usually less than five. However, the additional time spent researching usually pays off, as spear phishing messages have the highest rate of success. Phishing messages are normally crafted to include the following key elements:

- An attention-grabbing subject
- A sense of urgency in the message body that will motivate the recipient to take action
- Logos and other applicable images
- Sender's name and email address match the theme of the email
- A complete signature block, if the email appears to originate from a person
- A privacy statement at the end of the e-mail, if it appears to be automatically generated

Unless attackers are performing an attack with an attachment, the email will include a link for the target to click. The appearance of the link, or uniform resource locator (URL), plays an important role. If the URL looks suspicious or misspelled, employees are less likely to click. Graphic editing tools allow users to easily modify the display text of a URL so it deceptively appears as http://abc.com, but once clicked goes to http://cba.com. Using this technique will educate your employees on URL modification and how to verify a link's true destination before clicking. These tools and techniques are used by both attackers to attack networks and by defenders to test their networks before they experience a breach (Gardner & Thomas, 2014).

What Went Wrong at the Democratic National Committee

It appears the DNC did not have any sort of information security program in place at the time of the breach. It is also interesting to note the attackers went after private email accounts hosted by Google. The attackers used open source intelligence to find these Gmail addresses and then constructed attention-grabbing phishing email causing the targets to become compromised.

According to the US Intelligence Community (2017), the release of the hacked email was part of a much larger campaign being used by the Russians to attempt to influence the 2016 U.S. presidential campaign. More specifically, the assessment states:

> Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations (p. ii).

In further detail, the US Intelligence Community (2017) reports:

> We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments (p.ii).

Hactivism

The Russians also began adopting tactics long used by hacktivist groups such as Anonymous. Hacktivists act with political motivations. Hacktivism is defined as "the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft (Samuel, 2004).

There are many different examples of hacktivism, but the largest, most successful, and most well-known was Operation Sony, also known as Op Sony. The operation involved a denial of service attack and compromise of Sony's online services. At the center of the case was a hacker by the name of George Hotz, also known as GeoHot. Hotz was the first hacker to "jailbreak" the iPhone, which allows users to play and share homemade games (Brad, 2011).

On December 29th, 2010, Hotz and the rest of hacker collective known as fail0verflow announced they had retrieved the root key of Sony's PlayStation 3 gaming console and subsequently published the findings on a personal website. On January 11th, 2011, Sony filed a lawsuit against Hotz and other members of fail0verflow for releasing the PlayStation 3's root key (Brad, 2011).

In April 2011, Anonymous fired the first salvo in what came to be known as Op Sony, by taking the PlayStation Network (PSN) and several PlayStation-related domains, including the PlayStation Store, offline. It was later learned that the attacks not only resulted in an outage of the PSN service but also turned out to be one of the largest data breaches in history involving over 70 million records including personally identifiable information (PII) and credit card information (Ragan, 2011).

This period of time also saw the rise of a subgroup of Anonymous known as LulzSec. This brash subgroup of Anonymous ultimately took credit for stealing 24.6 million records in the PlayStation Network (Arthur, 2013). The group then went on an extensive hacking spree that involved a number of high-profile targets, including Fox.com, PBS, and the game company Bethesda Game Studios. The group saw themselves as modern-day Robin Hoods that were exposing the insecurities of the websites they breached. As their hacking spree continued, and became more brazen and outlandish, they garnered increasing public and law enforcement attention throughout the summer of 2011.

Russian Hackers and the Alt-Right

The same Russian hackers who compromised the DNC were later linked to the spread of "fake news" (Winter, 2017). The goal of this information warfare campaign according to U.S. intelligence agencies was to further exploit the virtual beachhead of the

DNC hacks and subsequent leaks of the confidential information related to the Clinton campaign and the DNC which put both organizations in a negative light.

At the same time, the Alt-Right ("Alternative Right," n.d.; Bokhari & Yiannopoulos, 2016) began to use the well-known hacktivist tactic of using memes and internet rumors to further spread negative stories about Clinton and the DNC. Most famously, Pepe the Frog, which for years had been a harmless meme spread across 4Chan and other Internet message boards, became a weaponized, racist symbol in the hands of the Alt-Right (Roy, 2016).

With the introduction of memes, the attackers also began to engage in acts of trolling related to the memes. Trolling is defined as the deliberate spreading of false and inflammatory information to cause upset to people (Coleman, 2015). Trolling for political means has been used by hacktivist groups in the past to attempt to equalize the political power differential for those who feel political oppression or for the victims of social and political injustice. To paraphrase Peter Ludlow in *The Hacker Wars* (2014): The purpose of trolling is to embarrass the power elite. Some trolls argue trolling is in the Socratic tradition.

Groups such as Anonymous to push an anarchist/social justice agenda have used Hacktivist tactics, mainly trolling and memes, in the past. According to the US Intelligence Community (2017), Russian hackers, both those employed by the Russian military and their surrogates, have utilized these "weapons of the geek" in combination with spreading propaganda to influence the election in favor of Donald J. Trump.

Attribution

The US Intelligence Community (2017) also describes Russia's use of trolls and trolling as a part of its propaganda efforts. It was assessed that such campaigns likely financed professional trolls who are affiliated with the Internet Research Agency, an organization based in Saint Petersburg.

Beyond the Russian trolling connection there are trolling communities, such as 4chan (Beran, 2017), and a particularly famous Internet troll known as Weev, whose real name is Andrew Auernheimer. Weev is a hacker folk hero due to his legal battles with AT&T (O'Neill, 2014). The AT&T case resulted in a prison sentence for Weev, but he was later released on a legal technicality (Zetter, 2014). After his release, Weev left the US and spent time living in Lebanon and Serbia before taking up residence in eastern Ukraine where he found financiers who shared his white nationalist views (Hacker "weev" has left, 2014). From there, Weev– who is now known as the "King of the Internet Trolls" (Coleman, 2015) – became an unofficial part of the Russian propaganda machine through the use of the online publication *Daily Stormer* as his message platform. By using proxy hackers such as Guccifer 2.0, who claimed responsibility for the DNC breach (Guccifer2, 2016) and subsequent information leak to WikiLeaks, Russia's contact and influence in the criminal hacker underground and organized crime is well documented (Nakashima, 2017). The use of these assets allows Russia to create plausible deniability and distance from targets.

Russia has also managed to exploit the hacker ethic of "All information should be free" (Levy, 1984, p. 458) as an avenue to leak stolen information to WikiLeaks, incorporating the organization as another part of the Russian propaganda machine (Boot, 2017). This new adoption of tools and techniques formerly used by hacktivists have

allowed Russian influence to spread beyond its own network of underground hackers to the hacker mainstream and has managed to unwittingly enlist anti-establishment hacker groups and organizations, such as WikiLeaks and 4chan, as mouthpieces for Russian propaganda– and to affect the outcome of US elections.

In December of 2016, U.S. cybersecurity firm CrowdStrike reported that Russia hacked into a Ukrainian artillery Android application using the Fancy Bear malware– the same malware used in the DNC breach–and resulted in heavy losses of D-30 Howitzers in Ukraine's war with Russian-backed separatists (ClowdStrike Global Intelligence Team, 2016).

While this is the only publicly reported use of this Russian-based malware on the battlefield, it does not rule out the potential for the current and future use of such malware to gain a strategic edge on the kinetic battlefield. As such, military personnel– particularly in the Baltic states and Ukraine– should be aware of this threat and take preventative measures to avoid being infected with this type of malware.

Defending Against Social Engineering

While most people think of the traditional sites for social networking, such as Twitter and Facebook, there are hundreds of additional sites that are potentially being used (Mehra, 2011, 2015). Beyond data leakage, these sites can house malware. Because anyone can typically upload any code they wish to these sites, social media sites have been the points of infections for zero days in the past (Mimoso, 2014). With the prevalent use of social media in originations at all levels, informing users of the threats that exist on social media platforms and how to detect and avoid them is especially important.

It is critical to emphasize to employees the extent of their personal information that is collected for payroll and insurance purposes by the organization. When the risk is made personal, employees become more aware of the importance of securing the organization's data because a breach may affect them as well. People check their bank accounts from work, shop from work, and have pictures of their loved ones stored on their computer. How would they feel if the flight reservations of their college-aged daughter ended up in the wrong hands? When risks and the consequences of a breach are personalized, compliance with policies that keeps information safe will increase. No matter what our position in our respective organizations, we are all network defenders.

The only real defense against social engineering is awareness training. However, most training takes the form of lectures and, sadly, the lecture is no longer an effective teaching tool. Few enjoy a lecture, except for perhaps the individual giving it. For the lecturer, the act of giving a lecture is an active exercise. For attendees, the lecture is a passive exercise. Passive learning has been demonstrated to be less effective than active learning when conveying information. In fact, many in higher education claim that the lecture, a centuries-old teaching technique, is dead (Gunderman, 2013).

For a more effective training approach, research demonstrates that we should do something that universities have been moving toward in the past few years: replacing passive learning with active learning. Active learning, depending on how it is implemented, has become known as "peer instruction" or "interactive learning." These techniques make students responsible for their own learning and fosters interaction between students as they engage the material to be learned (Lambert, 2012).

"Peer instruction" and "interactive learning" take the form of giving students reading assignments, and then splitting the students into groups to interact with the material. These interactions involve writing assignments, group discussion, completing assigned tasks as a team, and sometimes a group grade. S ometimes, students play question and answer games based in popular game show formats to engage the material. Points can be awarded in candy or toward a group grade (Jaramilla, n.d.).

It is clear the current training administered to employees is ineffective, as examples of breaches that involve exploiting humans to gain access to data occur on a nearly daily basis. Users are also exhibiting signs of message malaise; most think they will never be tricked into clicking on a link or opening an attachment because they view themselves as savvy Internet users.

Schneier (2013) asserts that funds spent on user awareness training would be better spent on better system design. This argument caused a firestorm in information security circles, and while some agree with the notion, many do not (Kennedy, 2013; Poniatowski, 2013). Everyone, however, agrees that something must be done. Even Schneier (2000) states, "Security is a process, not a product" (para. 3). If we never inform end users of threats, they will never know about them.

Security awareness has a lot in common with other awareness campaigns. Other awareness campaigns use memorable spokesmen like Smokey the Bear and McGruff the Crime Dog. They also involved memorable slogans like "Only you can prevent forest fires," and "Take a bite out of crime." In the field of information security awareness, we fail at these two simple goals because we continue to have debates about the effectiveness of security awareness programs.

The process of security is a long hard road that begins with getting management buy-in, drafting and enforcing policies that give the user expectations of what they can and cannot do with the organization's technological resources, building an effective security awareness program, and then measuring the effectiveness of that program using meaningful metrics. Once metrics are gathered and processed, the cycle begins again with a review of policies, awareness program, and metrics, and changes are made based on the organization's needs.

While there is value in making sure your organization has the latest security products and that your IT staff has proper security training, it is a waste of time and money if you ignore the human factor. Next-generation firewalls, antivirus, intrusion detection systems, intrusion prevention systems, and web application firewalls are all great productions, but these products do not provide protection against an employee making a poor decision about clicking links, opening attachments, and other nontechnical attacks employed by social engineers (Gardner & Thomas, 2014).

People have different learning styles based upon generational and educational background. The current generation entering the workforce learns much differently than those entering the workforce thirty years ago. Some individuals learn better from reading, others are visual learners, and some learn best from listening (Pashler, Mcdaniel, Rohrer, & Bjork, 2008).

The best strategy is to teach is a mixture of learning (Kramer-Koehler, Tooney, & Beke,1995; Korwin & Jones,1990) or example, instead of lecturing users on what a good password policy is, ask them if they can explain the best practices for passwords and discuss what constitutes a good password. Another example entails trainees discussing the

types of malware they have encountered in the past, how they think the infection(s) occurred, and what they think the attacker was after. Such exercises will aid in demonstrating to users that malware is not just an inconvenience that slows down their computer, but is an attempt by online criminals to steal data from their computers and/or to use their computer as part of a botnet, to hide child pornography and other contraband, or to gain a foothold in organization's network. Another possible exercise comes in the form of instructing trainees to read one or more of the organization's security policies, reflect on why the policy is in place, and question why such a policy is needed.

In the case of Russia's ongoing campaign to influence policy in not just in the United States, but in the also the policies of US allies, information security awareness training is more important than ever. This ongoing campaign is clear and present danger and could be the greatest national security threat facing the NATO and the West ("GCHQ warns politicians", 2017; Kagan, 2017; US Intelligence Community, 2017).

Conclusion

The nation-state of Russia has adopted non-nation-state hacktivist tactics, such as trolling, hacking, leaking, and spreading false news, to influence elections in other countries. While information warfare and cyber warfare are not new, the use of the aforementioned techniques by nation-state actors is. This new form of non-linear warfare has been perfected by Russia and was used to influence the 2016 US presidential election. It is likely Russia and other countries will continue to adopt and adapt these hacktivist tactics in the future.

Because the malware used in the DNC hack was also found on the battlefield of the Ukraine it is likely that this sort of theatre specific malware attacks will become more

common by Russia and other nation-states. As a result, nation-state defenders need to implement nontechnical defenses such as security awareness training as well as technical defenses.

References

Alternative right. (n.d.). *Southern Poverty Law Center*. Retrieved from https://www.splcenter.org/fighting-hate/extremist-files/ideology/alternative-right

Arthur, C. (2013). LulzSec: What they did, who they were and how they were caught. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail

Beran, D. (2017). 4chan: The skeleton key to the rise of Trump. *Medium*. Retrieved from https://medium.com/@DaleBeran/4chan-the-skeleton-key-to-the-rise-of-trump-624e7cb798cb#.4dhilziuu

Bodmer, S., Kilger, M., Carpenter, G., & Jones, J. (2012). *Reverse deception: Organized cyber threat counter-exploitation*. New York: McGraw-Hill Osborne Media.

Bokhari, A. & Yiannopoulos, M. (2016). An establishment conservative's guide to the alt-right. *Breitbart*. Retrieved from http://www.breitbart.com/tech/2016/03/29/an-establishment-conservatives-guide-to-the-alt-right/

Boot, M. (2017). WikiLeaks has joined the Trump administration. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2017/03/08/wikileaks-has-joined-the-trump-administration/?utm_content=buffer18814&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer

Brad. (2011). Operation Sony. *Know Your Meme*. Retrieved from http://knowyourmeme.com/memes/events/operation-sony

Carr, J. (2011). *Inside cyber warfare*. (2nd Ed.). O'Reilly Media.

ClowdStrike Global Intelligence Team (2016). Use of Fancy Bear Android malware in tracking of Ukrainian field artillery unit. Clowdstrike. Retrieved from

https://www.crowdstrike.com/wpcontent/brochures/FancyBearTracksUkrainianArtillery.pdf

Coleman, G. E. (2015). *Hacker, Hoaxer, Whistleblower, Spy: The many faces of Anonymous.* London: Verso.

Espiner, T. (2005). Security experts lift lid on Chinese hack attacks. *ZDNet News*. Retrieved from http://web.archive.org/web/20061211145201/http://news.zdnet.com/2100-1009_22-5969516.html

Gardner, B., & Thomas, V. (2014). *Building An Information Security Awareness Program: Defending Against Social Engineering and Technical Threats*. Waltham, MA: Elsevier.

GCHQ warns politicians about Russian hacking threat. (2017). *BBC News*. Retrieved from http://www.bbc.com/news/uk-39248879

Gragido, W. (2012). Lions at the watering hole - the "voho" affair. *RSA*. Retrieved from http://blogs.rsa.com/lions-at-the- watering-hole-the-voho-affair/

Guccifer2. (2016, October 4). Guccifer 2.0 hacked Clinton foundation. [Web log comment]. Retrieved from https://guccifer2.wordpress.com/2016/10/04/clinton-foundation/

Gunderman, R. (2013). Is the lecture dead? *The Atlantic*. Retrieved from https://www.theatlantic.com/health/archive/2013/01/is-the-lecture-dead/272578/

Hacker "weev" has left the United States. (2014). *Errata Security*. Retrieved from http://blog.erratasec.com/2014/09/hacker-weev-has-left-united-states.html#.WNKYUhIrKV4

Hollis, D. M. (2011). Cyberwar case study: Georgia 2008. *Small Wars Journal*. Retrieved from http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

How hackers broke into John Podesta and Colin Powell's gmail accounts. (2016). *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts

Jaramilla, M. (n.d.). How to ignite peer to peer learning with games. *Quora*. Retrieved from https://www.quora.com/profile/Michelle-Jaramilla/Posts/How-to-Ignite-Peer-to-Peer-Learning-with-Games-by-wheeldo-admin

Kagan, R. (2017). Russia's ability to manipulate U.S. elections is a national security issue, not a political one. *Brookings*. Retrieved from https://www.brookings.edu/opinions/russias-ability-to-manipulate-u-s-elections-is-a-national-security-issue-not-a-political-one/

Kennedy, D. (2013). The debate on security education and awareness. *TrustedSec*. Retrieved from https://www.trustedsec.com/2013/03/the-debate-on-security-education-and-awareness/

Korwin, A. R., & Jones, R. E. (1990). Do Hands-On, Technology-Based Activities Enhance Learning by Reinforcing Cognitive Knowledge and Retention?. *Journal of Technology Education*, *1*(2), 26-33.

Kramer-Koehler, P., Tooney, N. M., & Beke, D. P. (1995). The use of learning style innovations to improve retention. *Frontiers in Education Conference, 1995. Proceedings., 1995*, *2*, 4a2-5.

Lambert, C. (2012). Twilight of the lecture. *Harvard Magazine*. Retrieved from http://harvardmagazine.com/2012/03/twilight-of-the-lecture

Levy, S. (1984). *Hackers: Heroes of the computer revolution*. Garden City, NY: Anchor Press/Doubleday.

Markoff, J. (2008). Before the gunfire, cyberattacks. *The New York Times*. Retrieved from http://www.nytimes.com/2008/08/13/technology/13cyber.html

McAfee Foundstone Professional Services and McAfee Labs. (2011). *Global energy cyberattacks: "Night dragon"*. Retrieved from https://www.mcafee.com/fr/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

McWhorter, D. (2013). APT1 three months later – significantly impacted, through active & rebuilding. *FireEye*. Retrieved from https://www.fireeye.com/blog/threat-research/2013/05/apt1-months-significantly-impacted-active-rebuilding.html

Mehra, G. (2011). Beyond Facebook: 74 popular social networks worldwide. *Practical Ecommerce.* Retrieved from http://www.practicalecommerce.com/articles/2701-Beyond-Facebook-74-Popular-Social-Networks-Worldwide

Mehra, G. (2015). 91 Leading social networks worldwide. *Practical Ecommerce*. Retrieved from http://www.practicalecommerce.com/91-Leading-Social-Networks-Worldwide

Mimoso, M. (2014). Details emerge on latest Adobe flash zero-day exploit. *The Threat Post*. Retrieved from http://threatpost.com/details-emerge- on-latest-adobe-flash-zero-day-exploit/104068

Nakashima, E. (2017). Justice Department charges Russian spies and criminal hackers in Yahoo intrusion. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/justice-department-

charging-russian-spies-and-criminal-hackers-for-yahoo-intrusion/2017/03/15/64b98e32-0911-11e7-93dc-00f9bdd74ed1_story.html?utm_term=.741f65b61ce5

O'Neill, P.H. (2014). The fall of hacker-troll Andrew 'weev' Auernheimer. *The Daily Dot*. Retrieved from https://www.dailydot.com/layer8/weev-hates-jewish-people/

Pashler, H., McDaniel, M., Rohrer, D., & Bjork, R. (2008). Learning styles: Concepts and evidence. *Psychological science in the public interest*, *9*(3), 105-119.

Perlroth, N. (2014). Hackers lurking in vents and soda machines. *New York Times*. Retrieved from https://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html

Pomerantsev, P. (2014). How Putin is reinventing warfare. *Foreign Policy*. Retrieved from http://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/

Poniatowski, K. (2013). Does security awareness training actually improve enterprise security? *Security Innovation*. Retrieved from https://blog.securityinnovation.com/blog/2013/03/does-security-awareness-training-actually-improve-enterprise-security-1.html

Samuel, A. W. (2004). *Hackivism and the future of political participation* (Doctoral dissertation). Harvard University, Cambridge, Massachusetts.

Ragan, S. (2011). Anonymous' operation: Sony is a double-edged sword. *The Tech Herald*. Retrieved from http://www.thetechherald.com/articles/Anonymous-Operation-Sony-is-a-double-edged-sword/13239/

Rehman, S. (2013). Estonia's lessons in cyberwarfare. *U.S. News.* Retrieved from http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare

Riley, M. A. & Pearson, S. (2012). China-based hackers target law firms to get secret deal data. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html

Roy, J. (2016). How 'Pepe the Frog' went from harmless to hate symbol. *Los Angeles Times*. Retrieved from http://www.latimes.com/politics/la-na-pol-pepe-the-frog-hate-symbol-20161011-snap-htmlstory.html

Schneier, B. (2000). The process of security. Schneier on Security. Retrieved from https://www.schneier.com/essay-062.html

Schneier, B. (2013). On security awareness training. *Dark Reading*. Retrieved from http://www.darkreading.com/risk/on-security-awareness-training/d/d-id/1139381?

Sjouwerman, S. (2016). Russian breach US grid? nah, someone fell for social engineering and enabled macros. *KnowBe4*. Retrieved from https://blog.knowbe4.com/russian-breach-us-grid-nah-someone-got-social-engineered-and-enabled-macros

The Social Engineering Framework. (2017). *Social engineering defined*. Retrieved from https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/