5

Phishing, Watering Holes, and Scareware

ABSTRACT

As victim organizations and users have become more cautious and aware of certain cyber attacks, cyber threat actors have developed new, creative methods to circumvent technical countermeasures and user vigilance. This chapter explores how attackers use deception strategies and techniques to skillfully circumvent human defenses. The chapter first looks at spear phishing, particularly through the lens of conjuring methods of misdirection and attention control. Later in the chapter the discussion turns to a burgeoning attack method—watering hole attacks, or strategic web compromises—which shifts the attack vector away from targeting victim communication platforms, particularly email, to compromising web servers. This section introduces the watering hole attack deception chain and examines attackers' implementation of passive misdirection techniques and persuasive technology principles to deceive victims. The final section revisits and summarizes how certain deception techniques are used to initiate and perpetuate psychologically vectored cyber attacks.

Keywords: *Phishing; Psychology of hacking; Social engineering; Spear phishing; Strategic web compromises; Watering hole attacks.*

CHAPTER OUTLINE

Almost everyone enjoys when a magician pulls off a great magic trick or illusion. Getting duped by the trickery and wondering "how did they do that" is the positive reaction desired by the magician and audience members alike. However, falling for the deception of a hacker, phisher, or scammer is never appreciated. No one wants to be tricked by the techniques used by digital con artists who want people to fall prey to their sleight of hand.

Deception in the Digital Age. http://dx.doi.org/10.1016/B978-0-12-411630-6.00005-0

Social engineering is a practice used in magic and Shulman (2015) states, "social engineering is one of the most powerful tools in the hacker's arsenal." A Smithsonian Magazine interview with the renowned magician Teller (of Penn and Teller) revealed seven of his secrets of how he deceives his audiences and uses to psychology to manipulate their minds. Of these seven secrets, several relate directly to the social engineering and hacking techniques used by phishers, scammers, and other online con artists. Four key points from Teller (2013) include:

- exploit pattern recognition;
- keep the trickery outside the frame;
- nothing fools you better than the lie you tell yourself; and
- if you are given a choice, you believe you have acted freely.

This chapter focuses on social engineering and how the digital sleight of hand is used in a variety of cyber attacks including (1) phishing, (2) watering hole attacks, and (3) scareware.

Phishing

Over the years, there have been many definitions of phishing. According to the InfoSec Institute (2016), "Phishing is an attempt by Internet fraudsters to access and obtain personal and sensitive information, such as usernames, passwords, and financial information, by utilizing social engineering techniques." This type of fraud is actually quite old, dating back to the 1990s when Internet Service Providers (ISP) billed users by the hour for access. Skilled hackers would try to capture the usernames and passwords of unsuspecting victims by posing as an ISP, especially America Online due to its scope and penetration in the market. Fraudsters would harvest known AOL email addresses and send messages claiming to need account updates or validation of user profiles. The mass mailing strategy was like fishing, in that they were hoping to hook victims through deceptive bait. The term "phishing" emerged as a corruption of the term akin to that of phreaking within the general argot of the hacker community. Unsuspecting victims who thought these messages to be legitimate would forward their information to the sender in the hopes of correcting their account. The fraudsters, however, would keep the accounts for their own use or trade the information with others for pirated software or other information.

When looking at phishing through the lens and "secrets" told by Teller (2013), the phisher attempts to bait the user by hoping that their emails would:

- be recognized by having the right look and feel of legitimate communications previously received (*exploit pattern recognition*);
- use tricks outside the frame such as spoofing the email address so that a valid looking sender address is viewed on the "sent line" while the real deception can be seen in the email header (*keep trickery outside the frame*);

- rely on the theory that most humans will want to do the right thing and fix their account data even if they suspect that their account data is fine or that they do not even have an account with the company allegedly sending the email (*nothing fools you better than the lie you tell yourself*); and
- rely on the theory that most humans will "choose" to act and provide the requested information, particularly if there is a negative consequence attached if action is not taken (if you are given a choice, you believe you have acted freely).

Phishing messages often mimic legitimate communications from financial institutions and service providers, such as PayPal or eBay. The message usually contains some of the branding and language commonly used by that institution in an attempt to convince the recipient that the message is legitimate. The message usually suggests that a person's account has been compromised, needs to be updated, or has some problem that must be corrected as soon as possible. The time-sensitive nature of the problem is commonly stressed to confuse or worry the prospective victim in order to ensure a rapid response.

To that end, the email will also include web links that appear to connect to the appropriate website so that the victim can immediately enter their login information for the affected account. Generally, however, the link redirects the user to a different site controlled by the scammer that utilizes collection tools to capture user data. More sophisticated fraudulent sites will also feature branding or logos from the institution to help further promote the legitimacy of the phishing email. Upon arriving at the site, individuals are prompted to enter sensitive information, such as their bank account number, username, password, or even in some cases, personal identification numbers to validate their account. Upon entering the data, it is captured by the scammer for later use and may either redirect the victim back to the original website for the company or provide a page thanking them for their information.

The success of phishing techniques led some to begin to target e-commerce and online banking sites as they became popular with larger segments of the population in the early 2000s. Hackers began to recognize the value in targeting these institutions, and some began to create sophisticated phishing kits that came preloaded with the images and branding of the most prominent global banks. These kits, combined with spam email lists, enabled hackers to readily steal financial data from thousands of unsuspecting users around the world. In fact, the problem of phishing has become so commonplace that over 38,000 unique phishing websites were identified in June of 2013 alone (Anti-Phishing Working Group, 2013). These sites were hosted primarily in the United States due in part to the substantive proportion of hosting resources available to hackers, along with Germany, Canada, France, and the United Kingdom (Anti-Phishing Working Group, 2013). Thus phishing is a global problem that cannot be understated, though the prevalence of phishing victimization in the general population is largely unknown.

Since 2006, phishing has evolved into several variants including Voice over Internet Protocol (VoIP)/Voice phishing (vishing), short messaging service (SMS) phishing (smishing), spear phishing, and whale phishing. When phishing started in the 1990's, there were no smartphones, tablets, or apps. No one had text messaging, social media, or Wi-Fi yet. Thus as these new technologies and devices emerged, phishing evolved and proliferated to take advantage of the vast expanding digital environment. All of these phishing variations are based on the same premise as traditional email phishing; the scammers are just using different attack vectors. Smishing is defined as phishing via text message, and vishing is when victims are persuaded to disclose personal details or transfer money over the telephone, cellphone, or VoIP (Keyworth, 2016).

Spear phishing and whale phishing differ a bit from traditional phishing because the victims of these scams are specifically targeted and not part of a mass emailing. There are numerous reasons why a phisher would want to target a specific person. According to the InfoSec Institute (2016), spear phishing is a method used by hackers to gain personal or valuable information and ultimately to gain access to a network by targeting particular individuals within an organization; the first notable cases of spear phishing attacks were recognized around the year 2010.

Spear phishing attacks have targeted government agencies, corporations, banking clients, and universities. The techniques are all very similar, luring the selected group to click a link, download a file, or open an attachment. In the example in Fig. 5.1

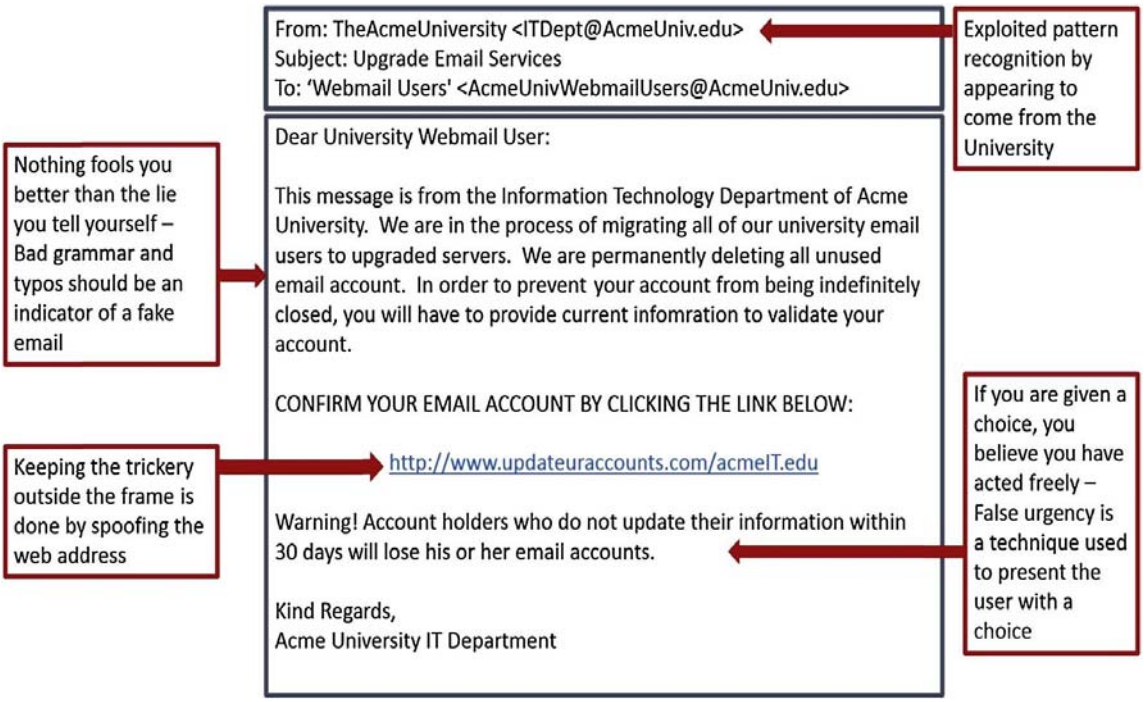

FIGURE 5.1 Spear phishing example.

below, a typical spear phishing email includes the core elements of deception as the scammers try to coerce university webmail users into giving up personal identifiable information.

Instead of targeting a population that belongs to a certain organization, spear phishers also send out large volumes of scam emails, which have a high probability of reaching real users of a particular service. Over the years, services like PayPal have been used as phishing lures to collect account data and passwords from legitimate PayPal users. In the example below, the spear phish actually uses the account holder's correct name and email address. Other elements of the phishing email appear to be real, as the scammers use the company's logo and do not make some of the spelling and grammatical errors commonly seen in spam. One of the tricks presented is to hide the actual URL where the user would put in username, password, and account information. But if the user hovers the mouse/cursor over the link, the real URL will appear; in this example case, the actual URL goes to a site in Russia. The example in Fig. 5.2 uses a fictitious company (ElectroPay Service); however, the elements of deception are typical.

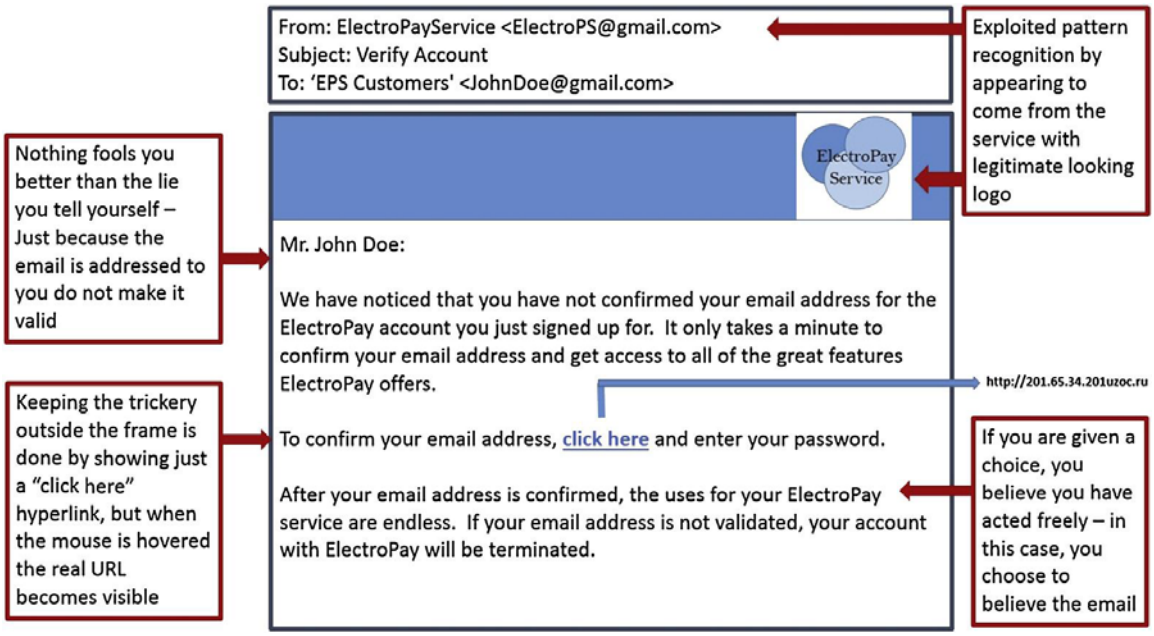

FIGURE 5.2 Example of a mass mailed spear phishing attack.

Around the same time period, other industrious hackers went after persons of notoriety or high net worth, otherwise known as "whales." The idea was that targeting those with power, influence, and money would reap better rewards for the attackers. Whale phishing has more recently morphed into "whaling," in which the scammers are using legitimate executive names and email addresses to persuade unsuspecting employees to wire money, sensitive business documents, tax forms, or human resource information to

their accounts (Boulton, 2016). Whether the attack vector is email, phone, or text message, the underlying deceptive techniques are basically the same, using deceptive techniques to take advantage of our emotions, cognitive biases, and human physiology (i.e., fatigue, illness, injury).

One well-publicized whaling attack targeted the toy company, Mattel. In 2015, an account executive appeared to receive an email from the CEO of Mattel requesting that a payment be made to a new vendor in China. While nothing appeared to violate policy, procedure, or protocol (and the account executive wanted to impress the new CEO), a payment was made to the "new vendor" (Ragan, 2016). Of course, there was no new vendor. Mattel lost three million dollars because of an orchestrated social engineering attack. Remember Teller's "secret sauce of deception":

- *exploit pattern recognition*: the email appeared to come from the CEO and looked legitimate;
- *keep the trickery outside the frame*: the IP address associated with the sent email did not originate from within the company, and the money was not wired to a named vendor's account but to an unnamed bank account number;
- *nothing fools you better than the lie you tell yourself*: the account executive was convinced that sending the money was the right thing to do (even though it was a banking holiday in China and their new vendor would also most likely be on holiday); and
- *if you are given a choice, you believe you have acted freely*: the account executive wanted to please the new CEO and not wiring money to the new vendor would have certainly been insubordination (although the account executive never initiated a verbal confirmation with the real CEO).

Audience members attending a magic show typically do not shout out or ask, "hey, what is in your other hand?"…but when it comes to digital deception, it becomes necessary to ask. If a certain communication is asking for too much information or highly sensitive information, it is worth the while to ask and to do the asking via a different communications mode. If the communication comes in through email, call the would-be sender. If the communication comes in through text message, use email. While in some circumstances it may be unusual or uncomfortable to double-check, no one wants to be duped, and certainly not out of millions of dollars.

Watering Hole Attacks (Strategic Web Compromises)

As victim organizations and users have become more cautious and aware of spear phishing attacks, cyber attackers have developed new, creative methods to circumvent technical countermeasures and user vigilance. One of these burgeoning attack methods, *watering hole attacks*, or *strategic web compromises*, shifts the attack vector away from targeting victim communication platforms, particularly email, to compromising

web servers, and in turn, the target victim group(s) that are known or likely to navigate to the website.[1]

Gaining salience in 2009, and sophisticatedly evolving over time, watering hole attacks pose a challenging threat to defend against. While the attack name is certainly curious on first impression, it is thematically accurate, since it is based off of the observed process in nature where concealed predators wait near small bodies of water used by their prey to drink and cool off, striking while prey are otherwise distracted (Fig. 5.3).

FIGURE 5.3 The inspiration behind the like-named cyber attack.

One of the most prominent examples of a watering hole attack is the security incident dubbed *Operation Aurora* by the security vendor McAfee. In 2009, as many as three groups of very sophisticated Chinese hackers compromised multiple high-level targets including Google, Adobe, Juniper Networks, Yahoo, Symantec, Northrop Grumman, and Dow Chemical (Shmugar, 2010; Zetter, 2010). The attackers utilized various methods to gain access to these institutions, though one of the most prevalent attack techniques was a watering hole strategy employed by a group referred to as the Elderwood Gang (Clayton, 2012).[2] The group would spear phish employees to click on links to a website hosting malware that would exploit a specific zero-day vulnerability in the Internet Explorer web browser. From there, the attackers appeared to use these infected systems as launch points to identify and compromise source code repositories within these companies (Markoff & Barboza, 2010; Zetter, 2010).

In 2013, the sophistication of strategic web compromises escalated, leading to high-profile breaches. In particular, a watering hole attack was used in 2013 that targeted a page regarding Site Exposure Matrices (SEM) on the US Department of Labor's

[1] Brandan, B. (January 24, 2014). *Spear phishing still popular, but more watering hole attacks coming.* http://searchsecurity.techtarget.com/news/2240213164/Spear-phishing-still-popular-but-more-watering-hole-attacks-coming.

[2] See also, Kambic, et al. (2013). *Crude Faux: An analysis of cyber conflict within the oil and gas industries,* CERIAS Tech Report 2013-9, Center for Education and Research, Information Assurance and Security, Purdue University.

website (Kaplan, 2013).[3] The page contained a malicious script that directed victims to a separate page hosting the Poison Ivy remote access Trojan and used an exploit for a common vulnerability in the Microsoft Internet Explorer browser that had been patched a few months prior to this incident. The content of the page that was compromised gives some potential insights into the target of the attack, as the SEM page details toxic substances commonly present at nuclear sites and the potential health concerns stemming from exposure to those materials (Kaplan, 2013). Further, sophisticated watering hole attacks such as those attributed to the "Hidden Lynx" hacking group, who were responsible for the VOHO Campaign and the attacks against security Bit9, demonstrated how potent these attacks could be, even against technically sophisticated victims.[4]

With the success of these attacks, cyber adversaries continued this momentum into 2014 and 2015. With new web browsers such as Internet Explorer 10 emerging, attackers quickly developed zero-day exploits to insidiously compromise these programs, stealthily placing these tools in secretly compromised websites trusted by the victims who visited them[5] The aerospace and automotive industries were heavily targeted, revealing the attacker's victim selection, motivations, and willingness to craft, refine, and patiently execute strategic web compromises against these highly desired victims.[6] Understanding the watering hole attack deception chain and the deception principles implemented by the attackers helps elucidate why these pernicious attacks are successful and will continue to be a threat in the cyber landscape.

The Watering Hole Attack Deception Chain

In a cyber context, cyber threat actors in watering hole attacks use victim profiling, reconnaissance, stealth, and deception techniques to tailor their attack process. The following are the steps in a typical *watering hole attack deception chain* (Fig. 5.2):

1) **Victim Selection.** The cyber attacker selects a target organization for compromise. Since 2009, watering hole attacks have targeted government agencies, financial

[3] *See also*, Blasco, J. (May 1, 2013). *U.S. Department of Labor website hacked and redirecting to malicious code*. Retrieved from https://www.alienvault.com/blogs/labs-research/us-department-of-labor-website-hacked-and-redirecting-to-malicious-code.

[4] Gragido, W. (July 2012). *Lions at the Watering Hole: The VOHO Affair*. The RSA Blog, EMC Corporation; Doherty, S., Gegeny, J., Spasojevic, B., Baltazar J. (September 17, 2013). *Hidden Lynx- Professional Hackers for Hire*. Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf.

[5] Lin, Y. (February 13, 2014). *New IE Zero-Day Found in Watering Hole Attack*. Retrieved from https://www.fireeye.com/blog/threat-research/2014/02/new-ie-zero-day-found-in-watering-hole-attack-2.html; *New Internet Explorer 10 Zero-Day Discovered in Watering Hole*. Retrieved from http://www.symantec.com/connect/blogs/new-internet-explorer-10-zero-day-discovered-watering-hole-attack.*Attack,* Symantec Security Response Symantec Employee, February 2014.

[6] Donohue, B. (September 2014). *Watering Hole Attack Targets Automotive*. Aerospace Industries, Retrieved from https://threatpost.com/watering-hole-attack-targets-automotive-aerospace-industries/107998/.

institutions, news organizations,[7] defense contractors,[8] energy sector companies,[9] dissident groups, human rights groups,[10] and civil society groups,[11] among other organizations.

2) **Web Profiling.** The cyber attacker(s) profile victim website visitation patterns, selecting legitimate web sites that the target set likely frequent.
3) **Server Reconnaissance.** Once the attacker(s) identify websites that are well-suited for a watering hole attack against their target victim set, they conduct reconnaissance, analyzing and probing the web servers for vulnerabilities that can be exploited, providing request access and resources to successfully facilitate the watering hole campaign.
4) **Server Compromise.** The attacker(s) will compromise these sites in advance of the watering hole campaign using a web injection and other attacks to breach and establish redirection elements (such as iframe) so that visitors are transparently directed to separate sites controlled by the attacker where an exploit is waiting to compromise a vulnerability in the victims' web browsers.
5) **Victim Compromise.** The resulting attack trajectory enables the attacker to successfully infect the victims' computers through what appears to be a normal, innocuous visit to a website. This provides backdoor access to systems inside sensitive networks, creating a foothold to facilitate wider compromises. It is during this pivotal stage that the attacker's effective use of *passive misdirection to disguise* the server compromise deceives the ultimate targeted victims in the larger attack trajectory.
6) **Continued Attack Trajectory.** From there, the attacker can perform secondary injection attacks to install keylogging malware and remote access trojans in order to help conceal their actions within the network (Fig. 5.4).

Passive Misdirection

Recall from Chapter 1, The Psychology of Deception that magicians use certain *misdirection* techniques to shape the spectator's *perceptions* (processing and interpreting of sensory

[7] See Rashid, F.Y. (February 11, 2015). *Chinese Attackers Hacked Forbes Website in Watering Hole Attack: Security Firms*. Retrieved from http://www.securityweek.com/chinese-attackers-hacked-forbes-website-watering-hole-attack-security-firms.

[8] Lee, B., Grunzweig, J. (July 20, 2015). *Watering Hole Attack on Aerospace Firm Exploits CVE-2015-5122 to Install Is Space Backdoor*. Retrieved from http://researchcenter.paloaltonetworks.com/2015/07/watering-hole-attack-on-aerospace-firm-exploits-cve-2015-5122-to-install-isspace-backdoor/.

[9] See Feinberg, A. (April 8, 2014). *Intrepid Hackers Use Chinese Takeout Menu to Access a Major Oil Company*. Retrieved from http://gizmodo.com/hackers-are-being-forced-to-target-chinese-takeout-menu-1560755886; Symantec Security Response, (June 30, 2014). *Dragonfly: Western Energy Companies Under Sabotage Threat Cyberespionage campaign stole information from targets and had the capability to launch sabotage operations*. Retrieved from http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat; Walker, D. (June 25, 2014). *Havex' malware strikes industrial sector via watering hole attacks*. Retrieved from http://www.scmagazine.com/havex-malware-strikes-industrial-sector-via-watering-hole-attacks/article/357875/.

[10] Leyden, J. (January 24, 2013). *RAT-flingers target human right activists in watering hole attack*. Retrieved from http://www.theregister.co.uk/2013/01/24/watering_hole_attack/.

[11] See Villenueve, N. (October, 2009). *0 day: Civil Society and Cyber Security*. Retrieved from http://www.nartv.org/2009/10/28/0day-civil-society-and-cyber-security/.

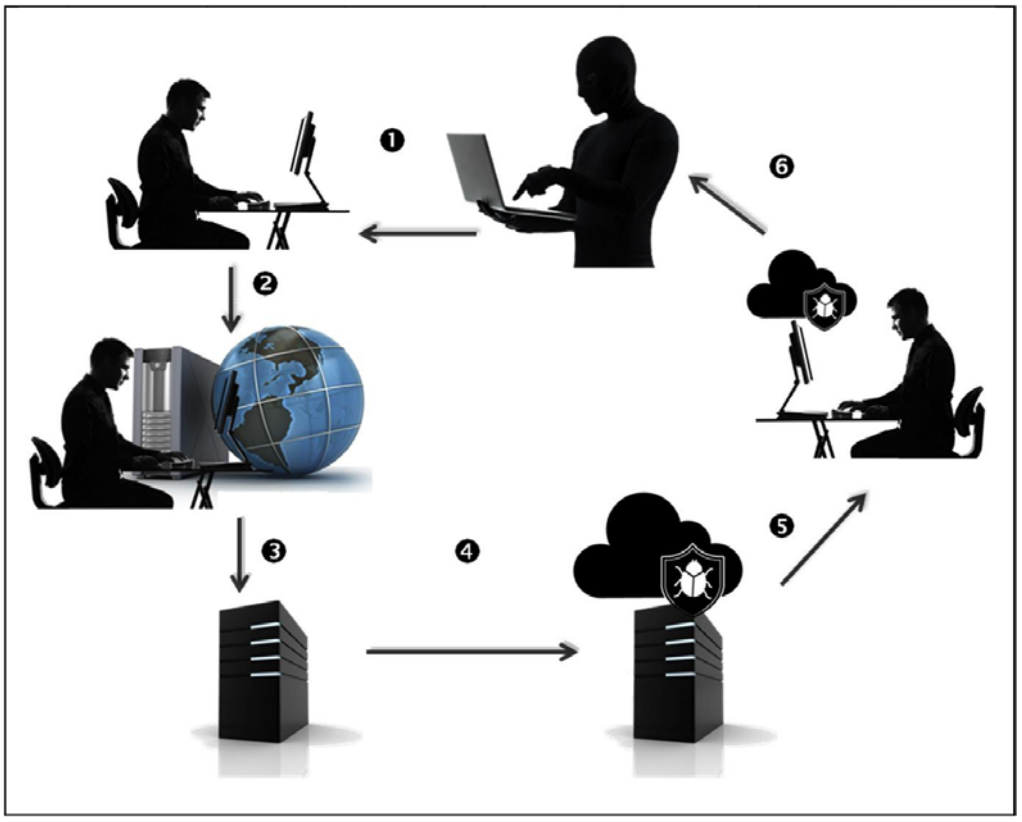

FIGURE 5.4 The watering hole attack deception chain.

information) and *beliefs* (confidence that the sensory information perceived is reality). This is often achieved by attracting the spectator's gaze and attention to an *unsuspicious* and interesting point, while a surreptitious action is taking place elsewhere, undetected and unsuspected (Ascanio & Etcheverry, 2005). Attackers utilizing watering hole attacks rely upon *passive misdirection* to ensure that victims navigating to the compromised server are not alerted to the impending secondary malware attacks on their systems. *Passive misdirection* within the context of a cyber attack is used to alleviate or dispel suspicion surrounding a nefarious online resource (such as a website) by ensuring that the web presence or "digital experience" resonates with victims as natural, familiar, and innocuous (Fig. 5.5).

Factors such as expected visual appearance, content, and user experience impact the attacker's ability to properly misdirect and deceive. When digital content is viewed and experienced by victims visiting the watering hole site as innocuous, nonsalient, and familiar, their *perception vigilance* is lowered and *inattention*, or diluted concentration, is induced (Sharpe, 1988). Factors that impact this type of misdirection include:

- familiarity, lack of unusual features, appearing nondescript;
- camouflage;
- disposition (placing content in a manner that confuses visitor's perception of position, etc.);

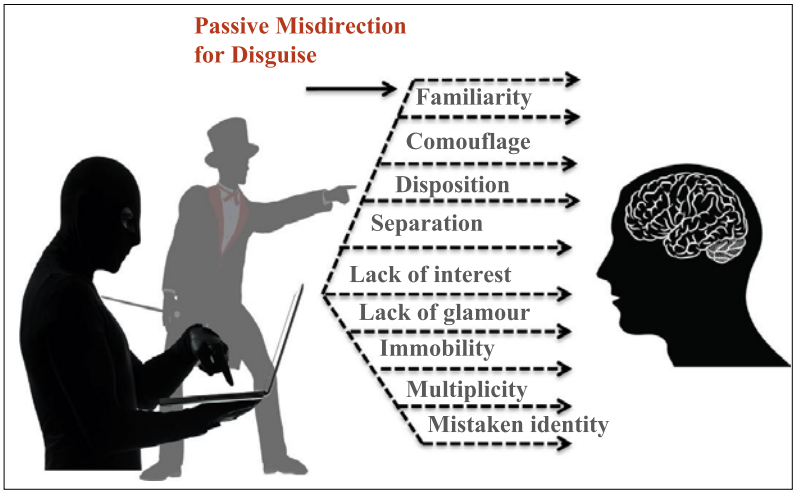

FIGURE 5.5 Attackers use of passive misdirection for disguise in watering hole attacks.

- separation;
- lack of interest; and
- lack of glamour;

Technical Persuasion

To effectively misdirect and deceive unsuspecting victims visiting the watering hole server, attackers must ensure that the misdirection narrative is supported and amplified by *technical persuasion elements* to properly convey a normal, expected, and credible web experience. Thus the digital user experience on the online resource—typically a web site—must convey *credibility* to the ensnared, surreptitiously infected visitors. Conversely, a substantial alternation of content, domain names (or infrastructure), or user experience detracts credibility, likely alerting victims to "a problem," causing them to further investigate and/or alert information technology/security professionals to do so—and potentially stymieing the watering hole attack platform and attack trajectory.

Website credibility, although studied for over a decade, is still in many ways a nascent area of research. Researchers found that there are four types of web credibility (Fogg, 2003) (Fig. 5.6):

- ***Presumed***: Credibility that is based upon general assumptions in the user's mind.
- ***Reputed***: This is derived or "earned" based upon third-party endorsements, reports, or referrals.
- ***Surface***: This is an aesthetic and limited interaction level; it is based upon simple inspection and first impressions.
- ***Earned***: Derived from the user's first-hand experience with the website over an extended period of time.

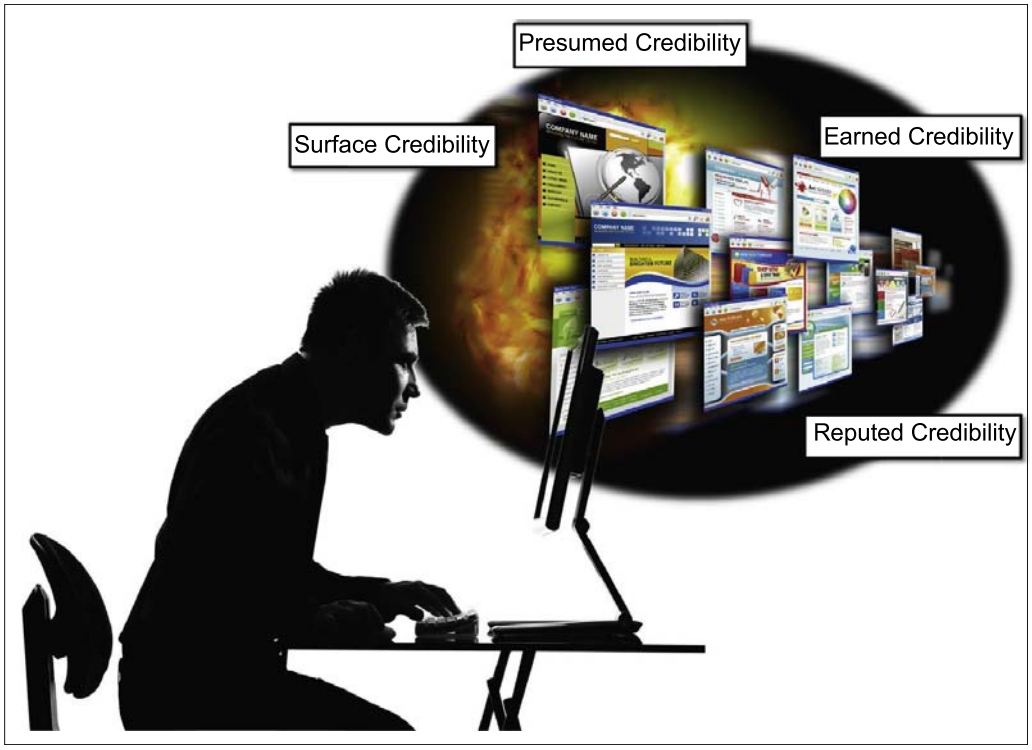

FIGURE 5.6 The four types of web credibility.

Similar to the importance of perceived source credibility when a communicator is trying to convey a persuasive message to a receiver of the communication, web credibility is based upon two factors: *trustworthiness* and *expertise* (Fogg, 2003; Flanagin & Metzger, 2007; Rains & Karmikel, 2009). Elements that bolster a website's credibility through conveying trustworthiness and expertise include:

- design features;
- depth of content;
- site complexity;
- contact details that correlate to physical address, email addresses, etc.;
- content that contains references that can be verified; and
- links to credible outside materials and sources.

Conversely, web credibility can be negatively impacted if the website has:

- confusing content (e.g., ads that are indistinguishable from true content);
- lack of contact data;
- unexpected content, such as pop-up windows and problematic links; and
- lack of updated content

(Fogg, 2003; Kąkol & Nielek, 2015).

Attackers staging and conducting watering hole attacks need to carefully modify and weaponize the watering hole server so as preserve all facets of the victim website's

credibility, while ensuring the attack trajectory of exploiting a vulnerability in the victims' web browsers. This critical balance often causes cyber attackers in these strategic web compromises to use zero-day malware or less common exploits in order to compromise their target browsers.[12] Such a step increases the likelihood of a successful machine compromise as the users' software may not be fully patched. Additionally, the security tools on the target systems may not recognize the attack method and allow the compromise to take place unabated, ensuring that the infection trajectory remains undetected by both system security and user observation.

While watering hole attacks are not as common as spear phishing attacks, they are becoming more prevalent, resulting in successful, problematic compromises into sensitive victim networks.

Historically, attack methods such as spear phishing to compromise the human actors behind systems in a network focused on psychological vulnerabilities, particularly since these are a much more effective vector than hardware or software. There are no patches for mental vulnerabilities, such as *conformation biases*, causing at least a small number of targeted victims to click through any web links provided via email. Watering hole attacks use clever deception techniques to take advantage of targeted user's existing perceptions of web credibility, and through passive misdirection, leverage these trusted web resources to compromise the unsuspecting victims.

Scareware

Ayala (2016) states that scareware is a "form of malicious software that uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software." Scareware is also called fraudware, fakeware, or very generically malware and may come in the form of pop-ups. The pop-up messages, claiming to be from legitimate antivirus companies, typically provide a stern warning indicating that there are infected files or malware on the user's computer, such as "*Your computer may be infected with harmful spyware programs.*" The scareware message also includes the solution, which is to pay for the software fix that will eliminate the infected files. Users who believe the deceptive message and download the antivirus software will end up introducing malware onto their systems, usually malware that is looking to steal personal identifiable information, passwords, and banking data (Kaspersky Lab, 2016).

The pop-up messages are crafted in a way to make them appear legitimate. In some cases people click on the scareware because the messages masquerade as the actual antivirus company that the user has installed on their machine. It seems reasonable, and in a lot of cases the user probably has not kept up with their antivirus updates. Unlike some of the phishing emails from years ago that contained misspellings, incorrect grammar, and the name of everyone's uncle (the Nigerian Prince whose inheritance is waiting to be distributed), these scareware ads and warning messages are well crafted.

[12] Symantec Internet Threat Security Report 2014, Vol. 19. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

In addition to pop-ups, scareware can be delivered by spam. A number of fraudulent companies, pretending to be cyber security firms or claiming they are working with legitimate firms, have launched massive email campaigns, which tricked users into purchasing worthless software and services. Once the user purchases the fake services, the fraudsters possess credit card numbers, and in some cases banking information and/or personal information. A recent action by the Federal Trade Commission, with the states of Connecticut and Pennsylvania, engaged in legal action to stop operations at Innovazion Research Private Limited, which has allegedly engaged in a major scareware operation. According to the lawsuit, Innovazion Research Private Limited defrauded consumers out of more than $17 million by pretending to represent Microsoft, Apple, and other major tech companies. The company supposedly used several attack vectors including pop-ups, phone calls, and online advertisements (Griffin, 2016).

The Pokémon GO craze in the summer of 2016 has also resulted in app-based scareware. Fraudsters have tempted Pokémon GO players with user's guides and cheat books, such as "Guide & Cheats for Pokemon Go" and "Install Pokemongo" on Google Play (Stefanko, 2016). At the same time, Google had to remove over 150 Android apps that were collecting personal data from users and serving up fake ads for services and software (Liam, 2016). While Android apps have received the most attention for security flaws, researchers at SANS Technology Institute discovered a fake Adobe Flash update targeting OS X. According to Ullrich (2016), "the attackers used a simple and effective trick to deceive victims, the attack starts with a popup window alerting users that their Flash Player software is outdated and providing them the instruction to update it."

Ransomware

It is one type of problem to get infected by malware via phishing, smishing, or scareware, but another thing all together for a user to have all of their data just "disappear." While technically not categorized as "scareware," ransomware can definitely be defined as a deceptive scheme that scares. According to the FBI, ransomware is a type of malware that prevents or limits people from accessing their systems, data, or devices by either locking the system's screen or by encrypting files unless a ransom is paid. It will be very obvious that ransomware malware has infected a device, as a large message will cover the screen, indicating that your data is being held hostage (see sample message below).

Sample Ransomware Message

Your documents, photos, databases, and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Ransomware is installed when a user opens an attachment sent from an attacker, visits a compromised or fake website, or clicks on malicious ads or bad links in social media or instant messenger chats. Thus the attack begins with the same type of deceptive tactics and social engineering techniques used in most other cybercrimes. Hackers may also take advantage of known vulnerabilities in systems and networks to launch their ransomware attacks (Siwicki, 2016).

Ransomware is the digital form of data hostage taking. In most cases, taking data hostage is not a "life and death" situation, as is a physical kidnapping for ransom. However, the relative importance or sensitivity of the data being held hostage can result in a crisis situation. The digital hostage takers do use some of the same tactics as kidnappers. They rely on the fact that people need their data, their personal lives depend on their data, their businesses depend on their data, and most importantly, they want their data back, safely, soundly, and in one piece. The emotional and psychological reactions of most people who have their data kidnapped and held hostage include shock, panic, fear, frustration, and anger. Victims are not only impacted by their stolen data, but many are confused and unsure about how to interact with the hostage takers…or wonder if they even should engage them. However, most people are willing to pay the ransom to get their data returned, thus the scam continues and nets millions of dollars. Ransomware is just the next iteration of digital attack, and it is extremely profitable (Federal Bureau of Investigation, 2016).

Ransomware originated in Russia by the same hackers who have been active for years launching virus attacks, phishing attacks, and distributing malware (Vargas & Vargas, 2016). Generally speaking, ransomware can be divided into two types: (1) lock-out ransomware and (2) crypto ransomware. Lock-out ransomware denies access to systems, networks, or devices and typically locks up the device interface. However, the device remains active enough to allow the victim(s) to interact with hackers to pay the ransom. Crypto ransomware is a bit more sophisticated and prevents the user(s) access to data files on a targeted device by encrypting those files. Thus the hackers hold the decryption key, and the ransom payment will provide the decryption. In some cases very specific file types are targeted. For example, some ransomware will focus on files or file extensions that they believe are more important to people such as Excel, QuickBooks, or tax forms (Vargas & Vargas, 2016).

The attackers are usually very helpful to their victims, providing instructions on the pop-up message which involves how to make the payment, and Bitcoin is typically the payment method of choice (Vargas & Vargas, 2016). In some cases, the digital hostage takers will provide the victim with a clock-timer contained in the ransom note that indicates that the user's files have been encrypted and that the victim has some amount of hours, minutes, and seconds left to pay the ransom. This additional use of the "ticking clock" is just part of the attacker's layered psychological strategy. If the disappearance of the user's data combined with the sinister looking ransom note does not coerce the user into paying, the timer (like the ticking bomb in many action movies that has to be deactivated) is there to strike another emotional chord.

Many users are unaware that ransomware also can just as easily seize control over files stored on cloud services. According to Krebs (2016), an employee working at Children in Film opened Outlook, clicked on a voicemail message attachment, and received the infamous ransom note. All of the company's data (i.e., email, data files, accounting) is hosted by a managed cloud service, and they felt secure because their data was allegedly safe "in the cloud." These criminals can target any computer, laptop, smartphone, or tablet user, whether it's a home computer, endpoints in an enterprise network, storage in the cloud, or servers used by a government agency. In other words, no one is safe from a potential ransomware attack. It can be argued that the ransomware fraudsters are the masters of social engineering. In order to pull off a full-on data ransom attack, the hackers must lure and persuade the would-be victims through multiple stages including the initial deception, the belief that their data is really not recoverable without the assistance of the attacker, the belief that their "time is limited" and the clock is ticking, the belief that otherwise nontech savvy people will in a time crunch learn to use Bitcoin, and in the end, send the money. That is a lot of persuasion and manipulation wrapped into one attack. But perhaps the real deception is that in some cases, the user's data can be recovered without the help of the attackers and without having to pay the ransom. Krebs (2016) provides instructions and a web link to a computer help forum called BleepingComputer.com, creator of TeslaDecoder, which allows victims to decrypt files locked by a form of ransomware called TeslaCrypt.

Social Engineering

So why do people still fall for phishing emails and fake ads? Why, even after training and education do employees get duped by SMS scams and fake phone calls requesting passwords, banking data, and other personal information? It seems as though people intellectually understand the dangers and the risks, but their behaviors do not follow suit. Unfortunately, it is because we are human, and we all have certain weaknesses, flaws, and predispositions. Social engineers rely on cognitive biases, which are patterns of judgment that deviate from the norm or rationality about people and situations, all of which provide a venue for effective attacks (Raman, 2008). Effective engineers will utilize biases to increase the likelihood of responses from potential victims. For instance, choice-supportive bias focuses on an individual's likelihood to identify only the positives of any past decision they have made rather than any negatives (Mather, Shafir, & Johnson, 2000). That person may be inclined to provide information through a fraudulent e-commerce site or financial service provider because they assume it was in response to actual past behaviors. Conformation bias recognizes that individuals will interpret new information or events through a lens of personal views and beliefs in order to support their decisions (Nickerson, 1998). For instance, individuals may become accustomed to certain uniforms, identification badges, and other behaviors that are symbolic of belonging within a working environment. Engineers can use this to their advantage and dress and act in a way that blends into the environment and would keep potential targets from questioning their

behavior. The exposure effect identifies the notion that people are more willing to recognize and respond to familiar items and behaviors (Zajonc, 1968) and may be more inclined to act in response to messages and requests from services they use or are familiar with. Finally, anchoring involves individuals who base decisions on simple pieces of information that may be immediately acquired, as when an engineer uses bank logos and branding in order to increase the likelihood that a victim will reply to a phish request.

Each type of bias presents an opening for an attacker to present their deception scheme. Digital deception will only get more creative as additional technologies, devices, and products enter the market. Fraudsters, scammers, and other adversaries have already taken advantage of the new technologies available through the use of digital photography, video, drones, and satellite imagery.

References

Anti-Phishing Working Group. (2013). *Phishing activity. Trends report.* 2nd Quarter 2013. http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf.

Ascanio, A., & Etcheverry, J. (2005). The magic of Ascanio. *The structural conception of magic* (Vol. 1). Paginas.

Ayala, L. (2016). *Cybersecurity Lexicon.* New York: Apress Media.

Boulton, C. (April 21, 2016). *Whaling emerges as major cybersecurity threat.* CIO Magazine. Online Source: http://www.cio.com/article/3059621/security/whaling-emerges-as-major-cybersecurity-threat.html.

Clayton, M. (September 14, 2012). *Stealing US business secrets: Experts ID two huge cyber "Gangs" in China.* Christian Science Monitor. Online Source: http://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China.

Federal Bureau of Investigation. (April 29, 2016). *Incidents of Ransomware on the rise: Protect yourself and your organization.* Online Source https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise.

Flanagin, A. J., & Metzger, M. J. (2007). The role of site features, user attributes, and information verification behaviors on the perceived credibility of web-based information. *New Media & Society, 9*(2), 319–342.

Fogg, B. J. (2003). *Persuasive technology: Using computers to change what we think and do.* Amsterdam: Morgan Kaufmann Publishers.

Griffin, K. (May 19, 2016). *FTC expands tech support fraud lawsuit.* Online Source http://www.hartford-business.com/article/20160519/NEWS01/160519909/ftc-expands-tech-support-fraud-lawsuit.

InfoSec Institute. (2016). *A brief history of spear-phishing.* Online Source http://resources.infosecinstitute.com/a-brief-history-of-spear-phishing/.

Kaplan, D. (May 2, 2013). *US department of labor web page serves watering hole attack.* SC Magazine. Online Source http://www.scmagazine.com/us-department-of-labor-web-page-serves-watering-hole-attack/article/291779/.

Kaspersky Lab. (2016). *Definitions – Scareware.* Internet Security Center. Online Source http://www.kaspersky.com/internet-security-center/definitions/scareware.

Keyworth, M. (January 1, 2016). *Vishing and smishing: The rise of social engineering fraud.* BBC World Service. Online Source http://www.bbc.com/news/business-35201188.

Krebs, B. (January 16, 2016). *Ransomware a threat to cloud services, too.* Online Source http://krebsonsecurity.com/2016/01/ransomware-a-threat-to-cloud-services-too/.

Kąkol, M., & Nielek, R. (2015). What affects web credibility perception? An analysis of textual justifications. *Computer Science, 16*(3), 295–310.

Liam, T. (August 2, 2016). *Scareware trojan infects 2.8 million android devices.* CSO Online. Retrieved from http://www.cso.com.au/article/604406/scareware-trojan-infects-2-8-million-android-devices/.

Markoff, J., & Barboza, D. (February 19, 2010). *2 China schools said to be linked to online attacks.* The New York Times. Online Source http://www.nytimes.com/2010/02/19/technology/19china.html.

Mather, M., Shafir, E., & Johnson, M. K. (2000). Misremembrance of options past: Source monitoring and choice. *Psychological Science, 11*(2), 132–138.

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology, 2*(2), 175.

Ragan, S. (March 29, 2016). *Chinese scammers take Mattel to the bank, phishing them for $3 million.* CSO Magazine. Online Source http://www.csoonline.com/article/3049392/security/chinese-scammers-take-mattel-to-the-bank-phishing-them-for-3-million.html.

Rains, S. A., & Karmikel, C. D. (2009). Health information-seeking and perceptions of website credibility: Examining web-use orientation, message characteristics, and structural features of websites. *Computers in Human Behavior, 25*(2), 544–553.

Raman, K. (2008). Ask and you will receive. *McAfee Security Journal,* 1–12.

Sharpe, S. (1988). *Conjurers' psychological secrets.* Calgary: Hades Publications.

Shmugar, C. (2010). *More details on operation aurora.* https://securingtomorrow.mcafee.com/mcafee-labs/more-details-on-operation-aurora/.

Shulman, A. (November 27, 2015). *Social engineering: Hacker tricks that make recipients click.* SC Magazine UK. Online Source http://www.scmagazineuk.com/social-engineering-hacker-tricks-that-make-recipients-click/article/455134/.

Siwicki, B. (May 17, 2016). *Cybersecurity special report: Ransomware will get worse, hackers targeting whales, medical devices and IoT trigger new vulnerabilities.* Health Care IT News. Online Source http://www.healthcareitnews.com/news/cybersecurity-special-report-ransomware-will-get-worse-hackers-targeting-whales-medical-devices.

Stefanko, L. (July 15, 2016). *Pokémon GO hype: First lockscreen tries to catch the trend.* Online Source http://www.welivesecurity.com/2016/07/15/pokemon-go-hype-first-lockscreen-tries-catch-trend/.

Teller, R. J. (March 2013). *Teller reveals his secrets.* Smithsonian Magazine. Online Source http://www.smithsonianmag.com/arts-culture/teller-reveals-his-secrets-100744801/.

Ullrich, J. B. (February 2016). *Fake adobe flash update OS X malware.* SANS Technology Institute. Online Source https://isc.sans.edu/forums/diary/Fake+Adobe+Flash+Update+OS+X+Malware/20693/.

Vargas, D., & Vargas, S. (June 2016). Ransomware: Is it really give up and pay up? In *Presentation presented at the techno security conference, Myrtle Beach, SC.*

Zajonc, R. B. (1968). Attitudinal effects of mere exposure. *Journal of Personality and Social Psychology, 9*(2p2), 1.

Zetter, K. (2010). *Google' hackers had ability to alter source code.* Wired. Online Source http://www.wired.com/threatlevel/2010/03/source-code-hacks/.