CO325 – Computer Network Security

Assignment 2

K.A.D. Nadeeshan – (E/13/234)

1. ***Social media scams and email threats***

People’s lives are becoming more intertwined due to online interactions over time. While the Internet provides several options for users to create and maintain relationships, social media sites make it even easier to do so. Unfortunately, time spent on social media sites opens windows of opportunity for cybercriminals and online threats.

Cybercriminals can initiate contact with users, it is not surprising that social media sites are constant targets for spam, scams and other attacks. Furthermore, there are now several options for creating and sharing content.

These attacks primarily proliferate on social media websites such as Facebook and Twitter, both of which currently have millions of active users. Their popularity makes them perfect venues for executing cybercriminal activities.

However, social media threats are not contained within the social networking sites’ walls. Public interest in social media is in itself a powerful tool that cybercriminals have repeatedly used to their advantage. Sending spammed messages purportedly from a legitimate social media site is a common social engineering tactic.

Virus writers and other cybercriminals go where the numbers are -- and that includes popular social media sites.

There are four social media scams are listed below.

1. Hidden URLs

*Beware of blindly clicking on shortened URLs. You'll see them everywhere on Twitter, but you never know where you're going to go since the URL ("Uniform Resource Locator," the Web address) hides the full location. Clicking on such a link could direct you to your intended site, or one that installs all sorts of malware on your computer.*

*URL shorteners can be quite useful. Just be aware of their potential pitfalls and make sure you have real-time protection against spyware and viruses.*

3. Hidden Charges

*"Find out who is the Hollywood character who want to marry you!" Hmm, this sounds interesting, so you enter your info and cell number, as instructed. After a few minutes, a text turns up. Well, that’s interesting… but not as much as your next month’s cell bill will be. You’ve also just unwittingly subscribed to some dubious service that charges Rs.30/= every month*.

4. Cash Grabs

*By their very nature, social media sites make it easy for us to stay in touch with friends, while reaching out to meet new ones. But how well do you really know these new acquaintances? That person with the attractive profile picture who just friended you -- and suddenly needs money -- is probably some cybercriminal looking for easy cash. Think twice before acting. In fact, the same advice applies even if you know the person.*

5. Chain Letters

*You’ve likely seen this one before -- the dreaded chain letter has returned. It may appear in the form of, "Resend this massage to 10 friends and see the miracle happens and if you don’t do it Huge black snake will bite you!"*

*So why would someone post this? Good question. It could be some prankster looking for a laugh, or a spammer needing "friends" to hit up later. Many well-meaning people pass these fake claims onto others. Break the chain and inform them of the likely ruse.*

1. ***Targeted attacks, spear phishing and intellectual property theft***

What is Phishing Requests? Let’s take some example. "Somebody just put up these pictures of you drunk at this wild party! Check 'em out here!" Immediately, you click on the enclosed link, which takes you to your Twitter or Facebook login page. There, you enter your account info -- and a cybercriminal now has your password, along with total control of your account.

How did this happen? Both the email and landing page were fake. That link you clicked took you to a page that only looked like your intended social site. It's called phishing.

Intellectual property is any innovation, commercial or artistic; any new method or formula with economic value; or any unique name, symbol, or logo that is used commercially. Intellectual property is protected by patents on inventions; trademarks on branded devices; copyrights on music, videos, patterns, and other forms of expression; and state and federal laws.

Stealing intellectual property is cheap and easy. All a thief has to do is copy someone else’s ideas or product. It is a growing threat—especially with the rise of digital technologies and Internet file sharing networks. And much of the theft takes place overseas, where laws are often lax and enforcement is more difficult. All told, intellectual property theft costs U.S. businesses billions of dollars a year and robs the nation of jobs and tax revenues.

The two forms of IP most frequently involved in cybercrime are copyrighted material and trade secrets. Piracy is a term used to describe IP theft—piracy of software, piracy of music, etc. Theft of IP affects the entire U.S. economy. Billions of dollars are lost every year to IP pirates. For example, thieves sell pirated computer software for games or programs to millions of Internet users. The company that actually produced the real product loses these sales and royalties rightfully due to the original creator.

1. ***Data breaches & privacy***

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak and also data spill. Incidents range from concerted attack by black hats associated with organized crime, political activist or national governments to careless disposal of used computer equipment or data storage media.

Most such incidents publicized in the media involve private information on individuals, i.e. social security numbers, etc.. Loss of corporate information such as trade secrets, sensitive corporate information, details of contracts, etc. or of government information is frequently unreported, as there is no compelling reason to do so in the absence of potential damage to private citizens, and the publicity around such an event may be more damaging than the loss of the data itself.

In the last two years, Fortune 500 companies from Sony to Target to Anthem have experienced major data breaches. Executives have lost their jobs, tens of millions of consumers have had their credit card and other personal data compromised, and corporations have frantically tried to contain the damage. Just last week, Target agreed to pay $10 million in a proposed settlement of a class-action lawsuit related to a huge 2013 data breach.

Some celebrities have found themselves to be the victims of inappropriate medical record access breaches, albeit more so on an individual basis, not part of a typically much larger breach. Given the series of medical data breaches and the lack of public trust, some countries have enacted laws requiring safeguards to be put in place to protect the security and confidentiality of medical information as it is shared electronically and to give patients some important rights to monitor their medical records and receive notification for loss and unauthorized acquisition of health information. The United States and the EU have imposed mandatory medical data breach notifications.

1. ***Security in Cloud and IT Infrastructure***

Cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security.

Cloud computing and storage provides users with capabilities to store and process their data in third-party data centers. Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the sixth biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

An efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls such as Deterrent controls, Preventive controls, Detective controls and Corrective controls.

Infrastructure security is the security provided to protect infrastructure, especially critical infrastructure, such as airports, highways rail transport, hospitals, bridges, transport hubs, network communications, media, the electricity grid, dams, power plants, seaports, oil refineries, and water systems. Infrastructure security seeks to limit vulnerability of these structures and systems to sabotage, terrorism, and contamination.

1. ***Ransomware and Businesses***

A new strain of ransomware has spread quickly all over the world, causing crises in National Health Service hospitals and facilities around England, and gaining particular traction in Spain, where it has hobbled the large telecom company Telefonica, the natural gas company Gas Natural, and the electrical company Iberdrola. You know how people always talk about the Big One? As far as ransomware attacks go, this looks a whole lot like it.

For latest example for ransomware is wannaCRY ransomeware. Software security companies said a ransomware worm called "WannaCry" infected about 200,000 computer systems in 150 countries on Friday, with Russia, Ukraine, and Taiwan being the top targets.

The hack forced British hospitals to turn away patients, affected Spanish companies such as Telefonica, and threw other government agencies and businesses into chaos.

WannaCry is a form of ransomware that locks up files on your computer and encrypts them in a way that you cannot access them anymore.

It targets Microsoft's widely used Windows operating system.

When a system is infected, a pop-up window appears with instructions on how to pay a ransom amount of $300.

The pop-up also features two countdown clocks; one showing a three-day deadline before the ransom amount doubles to $600; another showing a deadline of when the target will lose its data forever.

Payment is only accepted in bitcoin.

The ransomware's name is WCry, but analysts are also using variants such as WannaCry.

A hacking group called Shadow Brokers released the malware in April claiming to have discovered the flaw from the US' National Security Agency (NSA), according cyber-security providers.

1. ***Zero-Day vulnerabilities***

A zero-day vulnerability is an undisclosed computer-software vulnerability that hackers can exploit to adversely affect computer programs, data, additional computers or a network.

It is known as a "zero-day" because it is not publicly reported or announced before becoming active, leaving the software's author with zero days in which to create patches or advise workarounds to mitigate its actions. In effect, zero time has passed since the exploitable bug's existence was disclosed. Similarly, an exploitable bug that has been known for thirty days is sometimes called a 30-day exploit.

Malware writers can exploit zero-day vulnerabilities through several different attack vectors. Sometimes, when users visit rogue websites, malicious code on the site can exploit vulnerabilities in Web browsers. Web browsers are a particular target for criminals because of their widespread distribution and usage. Cybercriminals can also send malicious e-mail attachments via SMTP, which exploit vulnerabilities in the application opening the attachment. Exploits that take advantage of common file types are numerous and frequent, as evidenced by their increasing appearances in databases like US-CERT. Criminals can engineer malware to take advantage of these file type exploits to compromise attacked systems or steal confidential data.

Zero day vulnerabilities can be serious security risks. When searching for an appropriate antivirus solution, look for security software that protects against both known and unknown threats.

Browsers are similarly vulnerable; it’s a good idea to update your browser often, for updated security as well as features.

It’s extremely difficult to detect zero-day attacks, especially with traditional cyber defenses. Traditional security measures focus on malware signatures and URL reputation. However, with zero-day attacks, this information is, by definition, unknown. Cyber attackers are extraordinarily skilled, and their malware can go undetected on systems for months, and even years, giving them plenty of time to cause irreparable harm.

Zero-day attacks are cyber attacks against software flaws that are unknown and have no patch or fix.

***References:***

* <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/75/spam-scams-and-other-social-media-threats>
* <https://us.norton.com/yoursecurityresource/detail.jsp?aid=social_media_scams>
* <http://www.ncpc.org/topics/intellectual-property-theft>
* <https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft>
* <http://law.jrank.org/pages/11992/Cyber-Crime-Intellectual-property-theft.html>
* <https://en.wikipedia.org/wiki/Data_breach>
* <http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/>
* <https://en.wikipedia.org/wiki/Zero-day_(computing)>
* <https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/>
* <http://www.aljazeera.com/news/2017/05/ransomware-attack-hit-200000-150-countries-170514104555370.html>
* <https://www.fireeye.com/current-threats/recent-zero-day-attacks.html>