Common Cyber Attack Methodologies

Micah L Martinez

University of Maryland Global Campus

Networks are everywhere. Every day we are surrounded by computers and networks that compose the ever-growing Internet of Things (IoT). As the IoT grows in scale and complexity, it becomes more important to know how to protect yourself. With the increase of wireless technology, cloud systems, and interconnectedness, criminals have more opportunities to steal your personal, sensitive data. By learning about old and new methods hackers use to steal, you can protect yourself, your business, and your loved ones by reducing and vulnerabilities that the IoT creates. Criminals have used the following methods in the past, and present, to steal a tremendous amount of data.

When it comes to cybersecurity, there is a noticeable difference between the terms exploits and vulnerabilities. Vulnerabilities are simply a weakness in the system, while an exploit is an attack that purposefully targets the weakness created by the vulnerability (GizmoSphere, 2020). Vulnerabilities can be weak points of code that have not been discovered during updates, weaknesses in older software, or created by people when configuring settings, software, hardware, social media, or email accounts. Human behavior and mistakes can be a vulnerability since hackers can use them to access a system. Social engineering, various malware, viruses, and other attacks are all exploits used to steal or destroy information on vulnerable systems.

Social engineering is one of the oldest tricks that criminals use to access places that they should not and is the starting point for many cyberattacks. Social engineering uses manipulation tactics on other people to get someone to give up sensitive information (Webroot, 2020). When it comes to cybersecurity, using social engineering to gain access can be easier than using tools or other attacks to access computer systems.

Hackers often use human behavior to get people to trust them. By using a fake email from a friend or trusted source, a phone call as they pose as someone with access, or even baiting an employee with something they want, hackers can exploit trusting people to gain access. One popular method is "phishing," this technique uses email, social media, and instant messaging platforms to trick victims into providing sensitive information (Paganini, 2020). These messages capture the victim's attention; this is done by throwing much information to stimulate curiosity or use language to promote a sense of urgency. These messages often include a shortened hyperlink that leads to a malicious website that looks legitimate but has code that will install malware or attempt to steal your data. With the global pandemic caused by COVID-19, there has been an increase in using social engineering to gain profits (Tarun, 2020). Many of these attempts are scammers impersonating legitimate organizations such as the Center for Disease Control or the World Health Organization and then offering information or vaccines, but only if the target pays first.

One of the most dangerous types of vulnerabilities is the insider threat. An insider threat is a security risk that comes from within an organization. This person could be a current or former employee, a consultant, or a business partner. Jeff Petters (2020) describes two types of insider threats, the turncoat and the pawn. Turncoats are employees, current or former, who have gone rogue and have a motive to actively steal data from the organization. A pawn is an average employee who has mistakenly caused data loss or other security issues by being taken advantage of by turncoats, losing sensitive property like laptops, sending a document to the wrong person, or accidentally using a malicious file. Petters also describes two types of warning signs, digital and behavioral. Some of the digital warning signs include downloading excessive amounts

of data, accessing data that have no involvement with their job, using unauthorized storage devices like USB drives, and emailing sensitive data outside of the organization. Some of the behavioral warning signs include attempts to get through security and strange work hours. A more recent example of an insider threat is David Tinley (Townsend, 2020), who planted a logic bomb, described below, to secure future employment.

Logic bombs, like time bombs or bombs with tripwires, will not go off until a specific criterion or conditions are met. Logic bombs are made of malicious code that a hacker places into software or an operating system. Once specific conditions occur, the logic bomb runs its code and begins to exploit your computer. This can corrupt your hard drive, steal data, or take over your device completely. Hackers usually use logic bombs in conjunction with other attacks such as viruses, worms, and trojan horses. A recent instance involved Siemen's and one of their contractors, David Tinley, who had been trusted for about a decade (Townsend, 2020). Mr. Tinley planted a logic bomb in Siemen's offices in Monroeville, PA. The logic bomb that he planted was undetected for about two years. Every time something malfunctioned, Siemen's would have to call Mr. Tinley, who would then repair for a fee. It was not until Mr. Tinley was out of town when Siemen's IT staff discovered the logic bomb. Mr. Tinley pled guilty in 2019. To protect yourself from logic bombs, make sure to periodically scan all of your files, update your anti-virus/malware software, avoid pirated software, train your employees to spot phishing attempts, and never trust unsecured web links.

Another typical attack hackers use to disrupt a system is called a Denial of Service Attack (DoS). There are many types of DoS attacks; two of the most common methods are Distributed Denial of Service and Amplified Denial of Service (ADoS) attacks. A

DDoS attack attempts to disrupt the traffic on a server, service, or network by flooding it with traffic. By using compromised computers or other hosts on the Internet of Things (IoT), CloudFare (CloudFare Inc., 2020) describes this kind of attack as a traffic jam on a highway; it prevents the data from reaching the intended destination by clogging up the roadway. When malware controls a device remotely, they become a "bot;" when many bots are connected, they become a botnet. Once an attacker has established a botnet, each bot sends requests to the targeted IP address to overwhelm the server or network. This results in familiar non-bot devices to be denied service by the server or network. The most obvious symptom of a DDoS attack is if the service suddenly becomes much slower or unresponsive. However, this is also a symptom of legitimate traffic spikes, so it is not the best way to diagnose the issue as a DDoS attack. A recent instance of a DDoS attack happened in February of 2020 when Amazon Web Services (AWS) customer was attacked (SecurityExpert, 2020). The attack involved a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) Reflection, which relies on third-party CDLAP Servers to redirect traffic and amplify incoming data about 50 to 70 times the average volume. This attack lasted for three days and had lasting implications for AWS customers and brand damage.

One method of attack that is difficult to notice is called War-driving. War-driving is when someone goes around and looks for wireless access points that are unsecured and open to the public. It gained this name because it was common to drive around while looking for access points, hence the name "war-driving." TechSlang (2020) describes four easy methods to help protect yourself from this method of attack. The first is to create or change the password and enable encryption on your router. It is best to avoid the Wired Equivalent Privacy (WEP) encryption because it is easily cracked by

current software. The better encryption choice would be Wi-Fi Protected Access (WPA) or WPA2. The third option is to install a firewall to prevent access from unapproved sources. The last option is to shut down your wireless access point when you are not using it.

The rogue access point and the evil twin attack methods are similar; users are usually lured onto rogue access points or evil twins because they have the same name as legitimate organizations. A rogue access point occurs when a wireless access point has been installed onto a wired network without the authorization or knowledge of the network administer or owner (Technopedia, 2020). In general, this type of vulnerability occurs when an employee wants access to Wi-Fi when there are no wireless access points available. Without permission, the employee installs an access point that is not configured with the organization's policies in mind. An evil twin attack is when someone sets up a Wi-Fi network that looks legitimate but is used to steal your data. This network usually comes from a rogue access point or an access point made to look like it is on your network. NordVPN (2020) describes how this type of attack is commonly a "man in the middle" attack. The fake network eavesdrops on users and steals login information and any other sensitive information. Since the hacker is the one that owns the equipment, the victim is unlikely to know that this information is stolen until it is too late. Using phishing with an evil twin is another standard method. Victims connect to the network only to be led to a site that asks for login information or other details, after the user sends this information, the evil twin disconnects and shows that the server is temporarily unavailable.

In 2018, a Russian hacker group named "GRU" was charged with implementing an evil-twin attack using war-driving methods (Orsi, 2018). The members of the group

would park a car near target buildings, as if they were war-driving, which included anti-doping agencies in Colorado, Brazil, Canada, and others, as well as the Westinghouse Electric Company's nuclear power operations building, the Spiez chemical testing laboratory in Switzerland, and the Organization for the Prohibition of Chemical Weapons in the Netherlands. In their car, they had batteries for their gear, a Wi-Fi pineapple, a high-gain directional antenna, a 4G modem, and a small computer to store all the stolen data. Once they were parked, they would create their access point using the same, or similar, name as the access points around the building instead of searching for an open access point. They would then wait for employees to log onto their evil-twin access point.

Ransomware is a type of malware that, after infecting your computer, steals and encrypt your files. It then holds your files hostage until you pay a fee to get access to your data (Fruhlinger, 2020). Generally, this ransom is paid in Bitcoin since it is more difficult to track and has high anonymity built-in. Like most malware types, there are many ransomware styles; one variation of ransomware is called "leakware," in which the attacker threatens to release your sensitive information or files onto the internet or social media to get you to pay the ransom. On February 17, 2020, a ransomware attack caused ISS World, a Denmark facilities management firm, to turn off their networks and left hundreds of thousands of employees without access to their systems or email (Novinson, 2020). It was not until March 20 that ISS World was in full control of most of their systems. ISS expects to finish repairing and gaining control of 100% of their system by the end of 2020 but not before spending between 75 and 112 million dollars.

One type of attack that may soon make a comeback is Domain Name Server (DNS) cache poisoning or DNS spoofing. Imperva (2020), a cybersecurity software and

services company, describes DNS spoofing as an attack in which DNS records are altered to redirect traffic to a false website that seems legitimate. Once users are at the false website, they are asked to provide their login information and other sensitive data. In addition to stealing data, this false website could install worms or viruses on the victim's computer to give the attacker long-term access to the victim. In 2018, Amazon Web Services suffered from a DNS spoofing attack (Nation, 2018). An unknown attacker hijacked Amazon's Route 53 service, which provides cloud services to other organizations, and redirected traffic to a phishing site. The organization that was affected most was MyEtherWallet.com, a cryptocurrency website. Affected users likely lost the entire sum of their cryptocurrencies by entering their credentials on the website and unknowingly giving those credentials to the scammers.

A typical attack method is the brute force attack. Force Point (2020) describes a brute force attack as a password cracking method that relies on continuously guessing the password until the correct password is found. The biggest flaw in this method is that as passwords become longer and more complex and data obfuscation becomes commonly used, brute-forcing a password takes much longer and could essentially become impossible. However, simple passwords can easily be cracked in a matter of seconds. The most straightforward methods to prevent a brute force attack from succeeding are using a complex password, limiting the number of incorrect login attempts, and using two-factor authentication. In an opinion piece, Rakesh Soni believes that stay at home restrictions caused by Covid-19 and a sharp increase of brute force attacks are related (Soni, 2020). Since mid-March, as people began to work from home, organizations worldwide began to implement remote desktop protocols on many of their systems. With this increase in remote desktops, hackers believed that

many systems would be poorly configured and vulnerable to exploits. It turns out they were right. In Italy, over 900,000 brute force attacks were recorded in March, while in China, over 700,000 attacks were recorded in April. Despite being one of the easier attack methods to thwart, it remains one of the easiest and reliable methods to hack into a system.

Criminals have been developing techniques to steal data for as long as computers and the internet have been around. The IoT is beginning to incorporate itself into our daily life through smartwatches, phones, smart refrigerators, and other devices. This growing connection between us and technology is providing an unprecedented amount of data regarding our daily lives. From bank accounts, work, and daily routines, if criminals gain access to your devices, they could have everything they need to make a profit at your expense and possibly cause an extreme amount of damage. It is crucial to understand the possible vulnerabilities in your networks so that you can take proper measures to defend yourself and others from cyberattacks.

References

CloudFare Inc. (2020, November 2). *What is a DDoS Attack?* Retrieved from CloudFare: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/?utm_referrer=https://www.google.com/

Force Point. (2020, November 22). *What is the Brute Force Attack?* Retrieved from Force Point: https://www.forcepoint.com/cyber-edu/brute-force-attack

Fruhlinger, J. (2020, June 19). *Ransomware explained: How it works and how to remove it*. Retrieved from CSO: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

GizmoSphere. (2020, November 2). *Network Security: Exploits vs. Vulnerabilities*. Retrieved from GismoSphere: https://www.gizmosphere.org/network-security-vulnerabilities-vs-exploits/#:~:text=Put%20simply%2C%20vulnerabilities%20are%20a,vulnerabilities%20could%20exist%20without%20exploits.

Green, E. (2020, March 3). *How to identify and prevent evil twin attacks*. Retrieved from NordVPN: https://nordvpn.com/blog/evil-twin-attack/

Imperva. (2020, November 2). *DNS Spoofing*. Retrieved from Imperva: https://www.imperva.com/learn/application-security/dns-spoofing/#:~:text=Domain%20Name%20Server%20(DNS)%20spoofing,that%20resembles%20its%20intended%20destination.

Nation, J. (2018, April 24). *Major DNS Spoofing Hack Affects Amazon Web Services*. Retrieved from Metacert: https://medium.com/metacert/major-dns-spoofing-hack-affects-amazon-web-services-157e3565c844

Novinson, M. (2020, June 30). *The 11 Biggest Ransomware Attacks of 2020 (So Far)*. Retrieved from CRN: https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-/12

Orsi, R. (2018, October 7). *Russian Wi-Fi Hacking – Evil Twin attacks EXPLAINED*. Retrieved from Secplicity: https://www.secplicity.org/2018/10/07/russian-wi-fi-hacking-evil-twin-attacks-explained/

Paganini, P. (2020, August 6). *The Most Common Social Engineering Attacks [Updated 2020]*. Retrieved from InfoSec: https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/

Petters, J. (2020, September 22). *What is an Insider Threat? Definition and Examples*. Retrieved from Varonis: https://www.varonis.com/blog/insider-threats/

SecurityExpert. (2020, September 2). *Top Five Most Infamous DDoS Attacks*. Retrieved from Security Boulevard: https://securityboulevard.com/2020/09/top-five-most-infamous-ddos-

attacks/#:~:text=Amazon%20Web%20Services%2C%20the%20800,Access%20Protocol%20(CLDAP)%20Reflection.

Soni, R. (2020, October 9). *Onslaught of Login (Brute Force) Attacks Shakes Enterprise IT Security*. Retrieved from Info Security: https://www.infosecurity-magazine.com/opinions/ogin-brute-force-attacks/

Tarun, R. (2020, March 23). *COVID-19 Social Engineering Attacks*. Retrieved from CSO: https://www.csoonline.com/article/3533339/covid-19-social-engineering-attacks.html

Technopedia. (2020, November 17). *Rogue Access Point (Rogue AP)*. Retrieved from Technopedia: https://www.techopedia.com/definition/4082/rogue-access-point-rogue-ap

TechSlang. (2020, November 2). *What is war-driving?* Retrieved from TechSlang: https://www.techslang.com/definition/what-is-wardriving/

Townsend, C. (2020, November 2). *Logic Bombs: How to Prevent Them*. Retrieved from United States Cybersecurity Magazine: https://www.uscybersecurity.net/logic-bombs/

Webroot. (2020, November 22). *What is Social Engineering?* Retrieved from Webroot: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering