ATM-based Cyber Attack on the Financial Sector of the United States

Research Paper by *Dachi Tarughishvili, Ronit Singh, and Jeongin Lee*

Abstract

This paper investigates the cyber security landscape of the financial sector of the United States and suggests an imaginative attack scenario where attackers exploit ATMs focusing on human and software vulnerabilities for the motivation of financial gain. We first discuss the reason for choosing the particular sector, analyze the landscape of the US financial sector and its vulnerabilities, and estimate the impact of a successful cyber-attack on the sector. In the next section, we analyze different vulnerabilities in terms of ease, impact, and stealthiness, and weaponize the vulnerabilities, mainly employing techniques such as social engineering and malware attacks. The specific target of our attack is ATMs (Automated Teller Machine) as they have a large range of vulnerabilities from the human, hardware, and software side. In addition, the report suggests that attacks on ATMs are likely to generate more financial gain than common credit card frauds. Through close examination of different vulnerabilities, we argue that the off-site attack, particularly a malware attack on a bank's main control server via phishing emails, is the most reasonable option, considering our primary motivation. To be specific, by sending phishing emails to the employees of the bank disguised as claimable benefits from partners, and baiting them into downloading malicious PDF files on their computers, we plan to get access to the main control server of the bank through privilege escalation of the self-spreading malware. Control server then can be used to send specific commands to ATMs to enable remote cash withdrawal by our hired henchmen. Moreover, we can transfer money to foreign accounts for later withdrawal. We consider our attack an Advanced Persistent Threat since it can cause meaningful damage and we have the ability to determine the launch of the attack. More specifically, we can keep gathering data and sensitive information and decide the timing for the main control server attack. We can further improve the attack by improving the stealthiness and carefully setting the timing of the malware instruction execution. Since we have backdoor access, we can further modify the procedure based on the developments and progress made. All this, in turn, helps us to devise a more persistent attack that has the potential to grow over time. All in all, by orchestrating a fake attack towards the financial sector of the US, this research aims to provide a better understanding of its security landscape and increase the security awareness of the chosen sector.

Milestone I: Introduction

After careful planning, we decided to orchestrate our cyber-attacks on one of the 16 critical infrastructure sectors in the United States from the Department of Homeland Security. It is important to describe critical infrastructure whose existence the country depends on. Thus, threatening one of them could result in potential damage across individuals' and industries' financial well-being, health, security, safety, and more. This project focuses on the Financial Services Sector in particular, as it is one of the most crucial components of any nation's infrastructure. We further narrow our path towards phishing-based ATM attacks with potential for modification.

1. Attacks on Financial Sector as Critical Infrastructure

The financial sector entails many banking systems, financial organizations, investment firms, and so on. These institutions widely vary in size and functions, but an important thing to consider would be the spillover effect. As financial institutions increasingly rely on each other for their operations, when planning an attack, one has to consider the damage it will bring not only to the institution at hand, but also to all those parties, entities, and individuals who are directly or indirectly affected by them. It would not be a far-fetched idea to say that the financial systems are building pillars of our world. The successful collapse of these institutions or hindrance to their operations for a certain period will result in huge detrimental effects similar or worse to the one people encountered in the financial crisis of 2008. Moreover, the financial sector contains around 24% of the world's GDP which is significant and relates to hacker activities who are profit-minded. Additionally, attacks can also be politically inspired (as in the case of Hacktivists). A broad real-life analysis by IBM Security X-Force further depicts just how frequent attacks are in the financial domain. Their data suggests that among the top targeted industries in 2020, the Finance and Insurance industry tops the list with 23% for the fifth year in a row. Furthermore, the annual cost of cybercrime study by Accenture in the year 2017, also puts the financial services industry in first place with an average annualized cost of 18.28 million. The cost has been increasing annually and will continue to rise with the gradual increased digitization of the sector. Moreover, those services are especially vulnerable when it comes to small businesses as they do not have enough resources and funds to protect themselves, thus giving an advantage to attackers.

We chose the United States in particular as it has been the victim of the most significant cyber-attacks ("156 between May 2006 and June 2020", Specops, 2020) in the past years and possesses one of the world's most advanced financial services sectors both in terms of sophistication and variability. We have a diverse representation of many institutions, from small businesses to huge conglomerates, such as JP Morgan Chase (3.19$ trillion in assets, Goldberg Matthew). The United States also suffers from a much higher average cost to business ratio from the data breaches of 8.64 million USD compared to the world average of 3.86 million USD. (Johnson, Joseph. 2020).

This sector has been subjected to several attacks over the years, particularly in the United States. As an instance, in the year 2008, Ukrainian immigrants stole more than $750,000 in cash by penetrating the network of Citibank-affiliated ATMs in New York city. Similar card heists have occurred on a larger scale in multiple locations. For instance, in February 2011, a criminal gang stole around $55 million through fraudulent ATM withdrawals over many countries. The gang leader, Ercan Findikoglu, was jailed for eight years in the U.S in 2017 with the three other suspects caught in 2014. One of the more recent attacks comes from a group of cybercriminals using GozNym malware to steal more than $100 million from thousands of victims, ranging from consumers and non-profits to huge corporations. Some of them are still on the loose but investigations across several countries, leading with the U.S Department of Justice and Europol have been effective in capturing the leaders and key team members (Carnegie Endowment for International Peace, 2021). All in all, we come to see how such attacks on this sector not only bear huge costs to governments and corporations but they extend to consumers as well, since their breached private data are often disclosed and monetized by cyber criminals on the darknet. Other than that, there are several instances where the criminals behind such lucrative attacks are not caught because of the ease of covering tracks in the cyber world.

2. Reconnaissance: Layout and Vulnerabilities

The financial sector in the US consists of both public and private entities which vary with their size and function. According to the 'Financial Services Sector-Specific Plan 2015' published by CISA, the organizations in the US financial sector can be categorized based on the services they offer: "(1) deposit, consumer credit, and payment systems products, (2) credit and liquidity products, (3) investment products, and (4) risk transfer products" (CISA). Deposit, consumer credit, and payment service providers manage the payment services such as "wire transfer, checking accounts, and credit and debit cards," as well as transaction processes such as "electronic large value transfer systems, automated clearinghouses (ACH), and automated teller machines (ATM)" (CISA). The involved entities can include private depository organizations like commercial banks to the public entities. For example, "National or State-chartered banks or credit unions" (CISA). The regulatory actions can be conducted by federal-level institutions like "Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC)" (CISA). Credit and liquidity product providers offer credits to individuals, corporations, and the government based on their needs. The involved organizations encompass both private and public sectors such as "depository institutions, finance and lending firms, securities firms, and government sponsored enterprises (GSEs)" (CISA). Investment product sellers include "securities firms, depository institutions, pension funds, and GSEs" (CISA). These organizations are governed by public entities such as "The Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), banking regulators, and insurance regulators" for regulations. Risk transfer product (including insurance) providers mainly involve private actors such as "insurance companies, futures firms, and financial derivatives, including futures and security derivatives".

Due to this sector's complexity regarding the landscape, different organizations involved are geographically distributed throughout the nation. However, there is a central bank called the Federal Reserve that supervises the overall economy. The Federal Reserve, so-called the Fed, is a federal agency of the United States, but operates independently from the federal government (Amadeo). The main function of the organization is to prevent inflation (Amadeo). The Fed is also distributed into 12 different districts that "operates individually but is equally supervised by the Federal Reserve Board of Governors" (Amadeo). Private firms are also largely distributed nationwide, while some of the large-scale financial organizations are located in the "Wall Street" in Manhattan, New York City. As mentioned earlier, private and state-level actors in some areas of the financial sector are supervised and regulated under the federal-level institutions.

Since the financial sector has been historically threatened by various cyber attackers due to its financial and political impacts, lots of organizations have implemented efficient security systems. Based on *X-Force Threat Intelligence Index 2021* by IBM Security, Figure 1 presents the types of attacks that are conducted in the financial sectors in 2020. As the graph shows, while the financial sector suffers from server access attacks, it has higher resilience against RAT, BEC, Spam, DDoS and Web Script attacks.

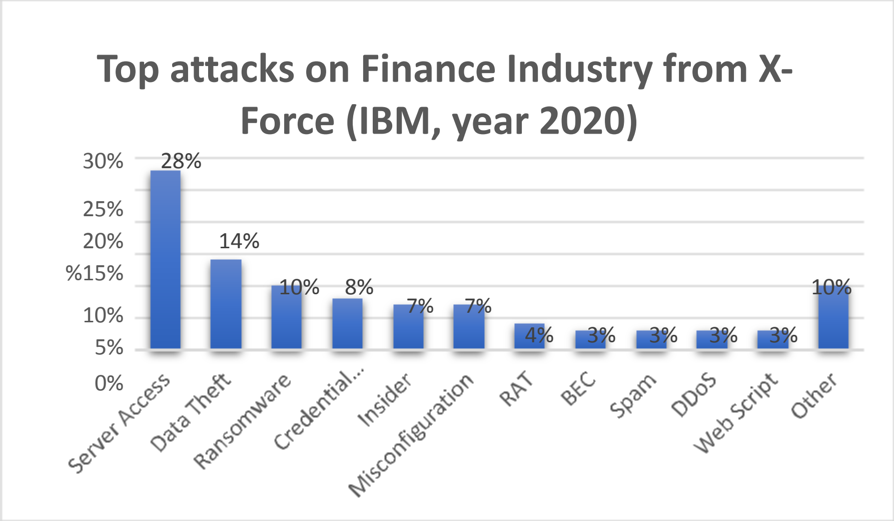


Figure 1. Top Attacks on Financial Sector in 2020

With digitalization, hackers are constantly in the process of figuring out new vulnerabilities with the main focus on financial systems. According to PTSecurity, vendors not customizing their systems for individual banks increases the risk since it leads to "flaws in protection mechanisms such as authentication and authorization" (PTSecurity 2018). The main attack targets include attacks against individual users as well as corporate users with a common goal of gaining sensitive personal data of users or attacks against bank web servers by exploiting web application flaws. Moreover, the personal data can include "compromised credit card numbers" that can be used by cybercriminals to make purchases. As we can see in Figure 1, server access attacks (28%) are one of the most commonly used resources followed by data theft (14%) and credential harvesting (10%). We could argue that these types of attacks were most effective in 2020, as hackers switch their approaches based on what's most profitable and feasible for that sector in that period. It's also interesting to note that Citrix vulnerability CVE-2019-19781 (allows directory traversal in Citrix Application Delivery Controller) represented 22% of server access attacks. (IBM Security, 2021)

Moreover, with mobile banking gaining trend these days, it has let hackers trick users into downloading fake malicious banking applications to capture the credentials. According to Intsights, a threat intelligence platform, "more than 1 in 3 consumers are fooled by fraudulent mobile apps". Some of the other common vulnerabilities that hackers have exploited in the past include:

- Direct Resource Access - lets users access other users' account information by traversing using URL or even transfer money from the account owner to the hacker's account using direct URL in the absence of server-side validation.

- Insufficient code protection leading to disclosure of crucial information in comments or source code analysis to help build an exploit.

- Using default usernames and password or Insufficient validation of user inputs leading to SQL Injection, Buffer Overflow, XSS (Cross-site Scripting) etc.

- Allowing users to enter negative amounts when transferring funds leading to a positive balance.

The possible attack vectors that hackers commonly use to exploit these kinds of vulnerabilities include DDoS (Distributed Denial of Service) attacks leading to interruption in bank operations, infiltration using USB sticks storing a malware (e.g., Trojan), Ransomwares, Credential Stuffing, exploiting comparatively less secure IoT devices like cameras, printers or routers.

Table 1. Resource Rankings

Efficiency Rank	Resource Title
1	Research Papers (IBM: X-Force Threat Intelligence, IBM: Cost of a Data Breach Report, Accenture: Cost of Cybercrime, Financial Services Sector-Specific Plan 2015…)
2	Website Data (Carnegie Endowment: Timeline of Cyber Incidents Involving Financial Institutions, CVE.mitre, Positive Technologies, Intsights by Rapid7…)
3	News Articles (Amadeo, Wiener Jeff, Goldberg…)

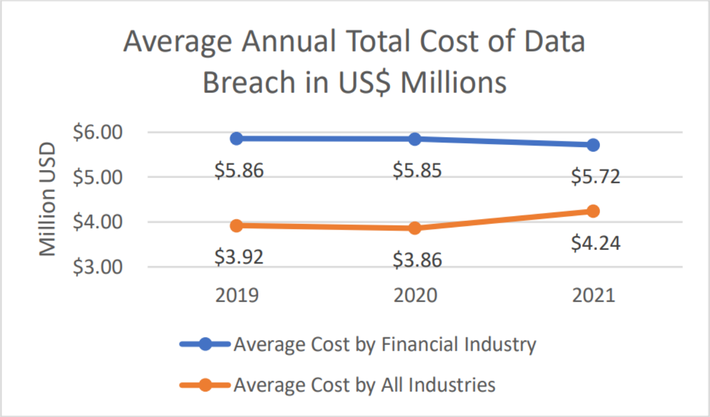


Figure 2. Annual Data Breach Cost in US$ Millions

Figure 2 from IBM's annual data breach cost analysis depicts the average total cost of a data breach per year in millions of USD for financial industries and all industries. Their research methodology allows them to calculate expenditures on a much wider scale including the initial detection costs, maintenance, or loss of business. We can see that costs associated with data breaches are upwards of millions of USD which is significant, especially since it does not involve huge data breach costs (per IBM). Moreover, it's significantly damaging for small to medium business administrations. For example, a small business with 100-499 employees has an average revenue of $40,775,000 (Wiener, Jeff, 2021). We can see how quickly those huge costs add up once we exclude other costs and calculate pure profit. Furthermore, smaller financial institutions rarely have the necessary means or resources to protect themselves from such attacks or pay the ransom, which is precisely why they have been the major target for hackers. (Beazley Breach Insight, 2017). You can also see that the cost across all industries has seen a significant rise in 2021. This is due to the increased digitalization, especially with the COVID-19 pandemic accelerating this process. Moreover, with new vulnerabilities to exploit, the cost substantially rises. It's also interesting to see how financial costs more or less remain the same, this is to be expected because we are talking about the average values of the financial sector in the study of specific organizations. One might argue that there is a slight decline which could be justified by the increase of concentration on healthcare industries by hackers due to higher profits following the COVID-19 pandemic (IBM, 2021). While there may be indirect costs to human lives from layoffs and reduction in salaries following cyber-attacks, there is not a significant direct relation between lethality and cyber-attacks in the financial sector unlike in the health and other sectors.

Milestone II: Preparing for ATM Attack

Weaponization

The Financial Sector is prone to a plethora of vulnerabilities as we described above. However, not all of them are always worth pursuing from the attacker's point of view. We have to consider several key factors when deciding the potential avenues: (1) the level of effort (how easy it is to exploit) (2) the intended impact (how effective it is at achieving the attacker's goal) and (3) stealthiness (how hard it is to detect the attack). In this case, our primary target is the Financial Sector, which we will later further narrow down to ATMs (Automated Teller Machines). It is also imperative to mention that some of the vulnerabilities are only useful and effective to attack against when combined together, and thus their complexity, impact, and such should be evaluated in conjunction.

In IBM's report "Top Attacks on Finance Industry," we observed that the majority of cyber-attacks came from server access (28%), data/credential theft (20%), and others (10%). Hackers usually pivot to areas that are more efficient or contain more vulnerabilities and exploits. Thus, we will be focusing on these three specific areas. After careful research, we chose our primary targets as ATMs, from which we plan to accomplish unauthorized transactions. An average ATM in the U.S can hold up to $200,000 which shows just how profitable such an attack can be, if successful, especially if executed at a mass scale (Kamerpower, 2021).

Beginning with 'network' side exploitations, an attack that would try to obtain server-side access to the targeted bank in the U.S would involve several steps varied in approaches and complexity. As attackers, we can use Shodan, a search engine for Internet-connected devices, to access some of the bank's IoT services to collect information about the employees. This would be the first step of data gathering i.e., reconnaissance phase. For instance, filtering by Port 3389 or other remote desktop ports that banks use could potentially reveal some of the user data. We could also use search engines like Google, Bing, or social media to gather information about staff members working in financial institutions. Using social engineering or more extreme forms of bribing or blackmailing, we could potentially recruit some of these people to act as an insider threat who would help us exploit the system. One of the scenarios might include inserting malware-loaded flash drives into the institution's system and obtaining some of the upper management credentials, or even gaining control of the whole ecosystem and more depending on the specific scenario. All in all, while we require several technical skills to move to later stages of the attack, the initial phase mainly targets the human vulnerability factor. The impact of human vulnerability will be fully assessed once we carry out all steps which are necessary for a successful attack. The stealthiness, however, depends on how careful and alert the attackers are. The data-gathering phase is relatively anonymous except the fact that direct contact with employees is more challenging. Any careless step could lead the attackers to getting exposed. Not to mention, employees could possibly warn the targeted authorities which could eventually delay or eliminate the chances of a successful attack.

Nevertheless, the human vulnerability factor does not end up with such direct interactions and is carried out through other forms of attack. While trying to execute server-side attacks to gain access to the bank's main Control Center, we could also immensely benefit from phishing. As an instance, we could send out a carefully crafted email with malicious attachments (e.g., we gained information about the recipient mail from our data gathering step). If planned carefully, our spear-phishing attack could be completely undetected, as an average user (something that we can also determine from the data gathering step) will likely not question the legitimacy of the mail. Moreover, the malicious software could potentially be a malware that creates a backdoor, which could remain idle in the system for a prolonged period of time. We could install keylogger and screen capture software as well. In such a manner not only are we able to execute any malicious code we want but also gather more information to strengthen our directed attack. Moreover, malwares (specifically, worms) could be designed to spread to other computers eventually leading to the Command-and-Control center. These kinds of attack scenarios rely not only on the technical factor (writing and employing use of malwares, building legitimate-looking phishing schemes, etc.) but also on the lack of competence from users. Through the bank's Control Server, we could then exploit ATMs to deposit the cash automatically at certain locations, steal credentials (to also be sold on the Dark web for money), and transfer the funds from legitimate user accounts to foreign fake accounts. Therefore, while such an attack is nothing close to easy to carry out in technical terms, the availability of outsourcing options and exploitation of lack of tech literacy among bank employees would be the desired avenue for achieving the greatest chance of impact and success. The ease of detection, in this case, would primarily be determined by the sophistication of the code present in the malware, that is to say, it should not reveal publicly identifiable information to trace back to us and careful conduction of data gathering steps and such.

Moreover, it’s also possible to pursue more physical or real-life approaches which involve being on-site where the ATM is situated. For example, we could install a Skimmer to steal credentials, connect an ATM to a crafted Control Server mimicking the real one or try to physically access the cash inside. While such an approach guarantees immediate impact upon successful completion, it might not align with our goal. In order to generate the maximum number of profits, one ATM would not be enough. Moreover, such physical attacks are hard to execute on a larger scale. This is mainly due to the amount of effort such an attack requires on a single ATM, and low stealthiness. A single-camera (CCTV), intervention from authorities, or a casual bystander might be able to identify the attacker. Also, if the ATM is situated in a populated area, the chances of being detected rises. Furthermore, even if the attacker uses henchmen to carry out the physical attack, they could be traced back to the “mastermind” in no time, as was the case with the Carbanak group. As such, while physical attacks are straightforward, they are not so favorable in terms of impact and stealthiness.

All in all, from the discussion above it is clear that those vulnerabilities are multifaceted and are sometimes built on each other. Conversely, as depicted in the aforementioned text, our actual goal would be to generate the maximum amount of profit with the least detectable mechanisms. While we also consider the ease of the attack, due to the outsourcing options and vulnerability of the human factor, we try to prioritize the other two factors. Apart from financial losses from the physical/virtual attacks (more on this in the next paragraph), we could also be responsible for the destruction of property, for instance, forking, or harming the ATMs. While human-life disruption may not be the primary goal, it is an immediate consequence. Not only will it impact the individuals in the financial institutions (especially in case of bribery/blackmail) but also the services, firms, or businesses (that depend on those institutions) along with the involvement of the Law Enforcement Agency in the eventual aftermath.

As mentioned in the previous paragraphs, there are multiple co-connected vulnerabilities in ATMs. Thus, the loss that can be caused by an attack may vary based on the detailed methodology of the attack as well as its scale. Indeed, according to the survey by ATM Industry Association (ATMIA) in 2016, one in five ATM attacks caused losses of under $1,000, while just two percent of the attacks cost more than $250,000 (ATMIA). Another point to consider is, as argued before, that the ideal attack methodology for us is to exploit human or software weaknesses for our goal is to earn the maximum financial gain while minimizing the risk of being revealed. According to the above statistics, software attacks like malware or blackbox resulted in an average cost of $104,000 per incident while human factor attacks like phishing cost an average of $10,000 per incident (ATMIA). While physical attacks turned out to be one of the most damaging attacks, with the average cost "ranging from $200,000 to $2,000,000 per year and average of $41,400 per incident (including collateral damage)," it does not guarantee the larger financial gain to the attackers as the number includes the collateral damage of physically destructed ATMs (ATMIA). In fact, it is relatively difficult to estimate the exact cost of the ATM attacks. The ATMIA report reveals that the costs of one in three attacks were unable to identify (ATMIA). However, another analysis by NCR suggests that every ATM deployed "faces the risk of the potential loss of $1,000 per machine," which means that we have some data to quantify at least the minimum cost of the attack based on the number of maliciously accessed devices (Wild). While the average cost for the malware attack is $104,000 per incident, since our attack targets the bank's Control Server, we could estimate our attack to encompass an even larger value, possibly within two top percent range of $250,000 or more.

Targeting

Upon consideration, we decided to set our motivation for the attack as a financial gain since it is one of the biggest motivations behind the attacks against financial institutions as in their functional nature. According to the Boston Consulting Group, financial corporations experience 300 times more attacks than other institutions. There are multiple past incidents where financial institutions were targeted for financial gain. One example is the Citibank ATMs attack in 2008 where Ukrainian immigrants stole more than $750,000 in cash by the successful attack on the Citibank ATM network which linked 2,200 kiosks inside 7-Eleven stores. (Marzulli). The technical difficulty may depend on the vulnerability that the attack is conducted on as well as the size and security level of the targeted institution. As mentioned in the previous section, while the initial stage of the attack, targeting human factors, might require minimum technical skills with some social engineering and phishing techniques, the later stage with malware development and deployment may need some technical and professional knowledge. In terms of the economical aspect, the attack for financial gain will earn money to the attackers but will cause significant financial and business losses to the attacked entity. Not to mention the stolen money, when the attack goes public, the attacked institution may lose social reputation and credibility from their customers that will lead to greater financial losses in the future. These possible side effects on the business side are closely related to the social impact of the attack. A successful attack on one financial institution may affect the landscape of the industry, which can lead to the political gains and losses of parties which rely on those industries. This may introduce further imbalance and increased inequality in the socio-political landscape.

Based on our research, we decided on ATMs as our primary target of attack to accomplish our financial objectives by the means of unauthorized transactions. Our attack tree contains two primary pathways to reach our main goal i.e., on-site attacks and off-site attacks. Each of these has various interconnected sub-paths leading to them. We carefully considered each of the methods outlined in the attack tree and chose the off-site attack method specifically. We gave importance to the factor of scalability to gain maximum profit (by attacking many machines at the same time) as well as the stealthiness it provides thus making it harder to trace back to the attacker in the digital world due to access to anonymity. While on the other hand, physical attacks have much higher chances of getting caught. Moreover, the investment needed for physical on-site attacks is comparatively higher due to the need for a variety of equipment to carry out the attack unlike the completely off-site attack methods where the only big investments required are in the case of hiring henchmen or buying malwares. Hence, our attack method will begin from a phishing scheme targeting bank officials to deliver the malware payload and then on pivot to the bank's main control server to command the ATMs to transact cash at specific locations for the henchmen to collect on our behalf. According to Business Insider, bank account information can make revenue of "$1,000 or more depending on how much money is in the account" (Business Insider, Thompson). Since our main motive is to gain money, we could sell the breached data gained from the attack on the dark web instead, as it turns out to be lucrative as well.

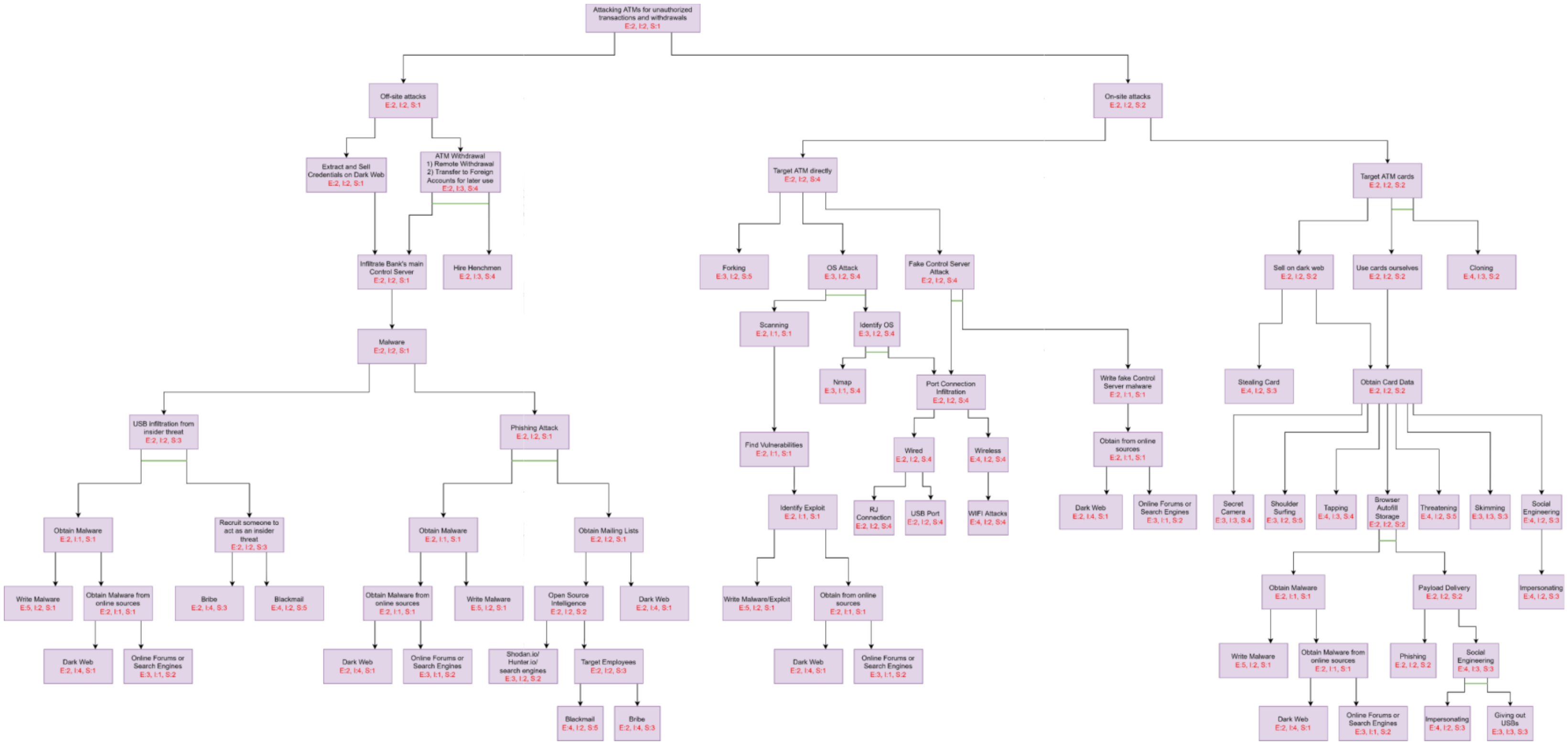

Attacking ATMs for unauthorized transactions and withdrawals E:2, I:2, S:1
Off-site attacks E:2, I:2, S:1
On-site attacks E:2, I:2, S:2
Extract and Sell Credentials on Dark Web E:2, I:2, S:1
ATM Withdrawal 1) Remote Withdrawal 2) Transfer to Foreign Accounts for later use E:2, I:3, S:4
Infiltrate Bank's main Control Server E:2, I:2, S:1
Hire Henchmen E:2, I:3, S:4
Malware E:2, I:2, S:1
USB infiltration from insider threat E:2, I:2, S:3
Phishing Attack E:2, I:2, S:1
Obtain Malware E:2, I:1, S:1
Recruit someone to act as an insider threat E:2, I:2, S:3
Write Malware E:5, I:2, S:1
Obtain Malware from online sources E:2, I:1, S:1
Bribe E:2, I:4, S:3
Blackmail E:4, I:2, S:5
Dark Web E:2, I:4, S:1
Online Forums or Search Engines E:3, I:1, S:2
Obtain Malware E:2, I:1, S:1
Obtain Mailing Lists E:2, I:2, S:1
Obtain Malware from online sources E:2, I:1, S:1
Write Malware E:5, I:2, S:1
Open Source Intelligence E:2, I:2, S:2
Dark Web E:2, I:4, S:1
Dark Web E:2, I:4, S:1
Online Forums or Search Engines E:3, I:1, S:2
Shodan.io/ Hunter.io/ search engines E:3, I:2, S:2
Target Employees E:2, I:2, S:3
Blackmail E:4, I:2, S:5
Bribe E:2, I:4, S:3
Target ATM directly E:2, I:2, S:4
Forking E:3, I:2, S:5
OS Attack E:3, I:2, S:4
Fake Control Server Attack E:2, I:2, S:4
Scanning E:2, I:1, S:1
Identify OS E:3, I:2, S:4
Nmap E:3, I:1, S:4
Port Connection Infiltration E:2, I:2, S:4
Write fake Control Server malware E:2, I:1, S:1
Find Vulnerabilities E:2, I:1, S:1
Wired E:2, I:2, S:4
Wireless E:4, I:2, S:4
Obtain from online sources E:2, I:1, S:1
Identify Exploit E:2, I:1, S:1
RJ Connection E:2, I:2, S:4
USB Port E:2, I:2, S:4
WIFI Attacks E:4, I:2, S:4
Dark Web E:2, I:4, S:1
Online Forums or Search Engines E:3, I:1, S:2
Write Malware/Exploit E:5, I:2, S:1
Obtain from online sources E:2, I:1, S:1
Dark Web E:2, I:4, S:1
Online Forums or Search Engines E:3, I:1, S:2
Target ATM cards E:2, I:2, S:2
Sell on dark web E:2, I:2, S:2
Use cards ourselves E:2, I:2, S:2
Cloning E:4, I:3, S:2
Stealing Card E:4, I:2, S:3
Obtain Card Data E:2, I:2, S:2
Secret Camera E:3, I:3, S:4
Shoulder Surfing E:3, I:2, S:5
Tapping E:4, I:3, S:4
Browser Autofill Storage E:2, I:2, S:2
Threatening E:4, I:2, S:5
Skimming E:3, I:3, S:3
Social Engineering E:4, I:2, S:3
Obtain Malware E:2, I:1, S:1
Payload Delivery E:2, I:2, S:2
Impersonating E:4, I:2, S:3
Write Malware E:5, I:2, S:1
Obtain Malware from online sources E:2, I:1, S:1
Phishing E:2, I:2, S:2
Social Engineering E:4, I:3, S:3
Dark Web E:2, I:4, S:1
Online Forums or Search Engines E:3, I:1, S:2
Impersonating E:4, I:2, S:3
Giving out USBs E:3, I:3, S:3

Figure 3.0 Attack Tree: Attacking ATMs for unauthorized transactions and withdrawals

Milestone III: Execution

Delivery

As presented in the Attack Tree above, there can be multiple delivery methods to distribute malware for ATM attacks in both off-site and on-site attacks, including (1) USB infiltration, (2) phishing attacks, and (3) fake control server attack with port infiltration. For off-site attacks, we can distribute the malware on the bank server by using either USB infiltration or phishing attacks. By bribing or blackmailing, we can recruit insiders from the targeted financial institution and force them to distribute the malware by physically inserting a malware-containing USB into one of the internal computers. Or if we obtain the mailing list either by using open-source intelligence, bribing, or the dark web, we can conduct phishing attacks on the employees, encouraging them to download the malware by clicking malicious website links or downloading attachments malicious in nature using clever disguises. On the other hand, when considering on-site attacks, the connection to the ATM is established by wired port infiltration, RJ connection or USB port, or wireless port infiltration. The malware can exploit the Operating System (OS) of the ATM or act as a fake processing server that will give us access to ATMs functions including money withdrawal. The aforementioned attacks include different levels of complexity, stealthiness and cost. The ATM on-site attack (fake control server USB infiltration) is the least desirable, thereby least feasible in terms of stealthiness and easiness since it requires direct physical contact and is also not scalable for larger attacks with multiple ATMs due to the exponential rise in risk and complexity. While the level complexity and cost for USB and phishing attacks are similar, the phishing attack is stealthier as there are multiple tools (Tor, VPNs, Proxies, botnets, etc.) to cover our presence online and does not require direct on-site presence. USB attack is less feasible than phishing attack in terms of stealthiness as the acquired human asset needs to insert the USB drive physically, where it could be costly and detectable, especially if the company has prohibited their employees from using external drives.

Due to the difference in feasibility as mentioned above, we decided to deliver our malware using a phishing attack. Though the level of ease and investment is similar to the other options, the stealthiness is much higher for phishing. Delivering the malware through a phishing attack is a network delivery as we need to enforce insiders to download the malware which we will send via the network, for example, email attachments. To achieve this, we plan to disguise our emails as advertisements to delude the receivers, as we will further expand in the next section where we will discuss our action steps. It could be argued that hiring henchmen is part of a physical attack, however, we are not required to directly interact with them. We could order them to leave the cash from ATMs at predetermined times and predetermined locations, requiring no point of contact from us.

The possible assets that we can utilize to deliver the malware through a phishing attack are data and human assets. Data assets include the mailing list of the possible targets that we can perform phishing attacks on and deceive to download the malware on the bank computers. Data assets additionally include information about Bank's partner companies which we will use as our disguise for our fake advertisement. Data assets can further encompass pre-installed browsers, software and operating system versions and their potential vulnerabilities, for our malware to exploit. The ease of obtaining the mailing list ranks 2 out of 5, referring to the above Attack Tree, as we can either use several open-source intelligence sources such as social media, search engines, Shodan, Hunter.io, and more to get the publicly available information such as emails, in our case, relatively easily (more on this later). Additionally, if we succeed in obtaining the data asset, then we have a high chance of securing human assets to actually deliver the malware on the target server. Gathering human assets differs by stages. For instance, bribing someone for credential extraction or using social engineering to extract the information may not be as challenging as securing their clicks on malicious phishing mail attachments.

Exploit and Install

To fulfill the goals mentioned above, we will go with the option that generates the maximum amount of profit for our attack. In case of a successful attack, we could extract and sell the obtained data on the dark web, however, there arise two main issues. First, we will not be able to sell the data for the original amounts the corresponding financial accounts hold, as buyers would only have an incentive to purchase such data only for a reduced price. Hence, we would have to sell it at lower profit margins. Moreover, there is a possibility that our platform might be compromised (similar to the Silk Road marketplace on Dark Web) which will further delay our plans, and will require us to stay longer in contact with each other to find alternative platforms and pathways. This would, in turn, increase our chance of getting caught. In this case, the best approach would be to obtain the cash directly. Not only, will this method be instantaneous, but also generate the same amount of profit as the ATMs or accounts themselves contain. Moreover, we can transfer some of the money to foreign fake accounts abroad for later withdrawal, thereby including some of the benefits (e.g., selling data) of the previous approach.

In such a scenario, our target is the bank's main control server through which we can manipulate not only the financial accounts of the users but also certain vulnerable ATMs. To infiltrate the main control server, we would have to gain access to a computer with enough administrative privileges to obtain either credentials to the server or log into the server directly. We could use certain hacking techniques to escalate our privileges as well once inside the infected computer. However, we do not know which specific computers to target in advance. Hence, our whole plan relies on infiltration: infecting at least one computer which would then try to spread the malware to other computers over the same network. If the attack remains undiscovered, sooner or later we will have access to a computer with enough privileges to exploit its properties and obtain access to the main control server. Moreover, we could install a backdoor upon successful infiltration, enabling us to stay persistent, continue data gathering and perhaps rediscover further exploits to gain access to the main control server if the original plan does not work.

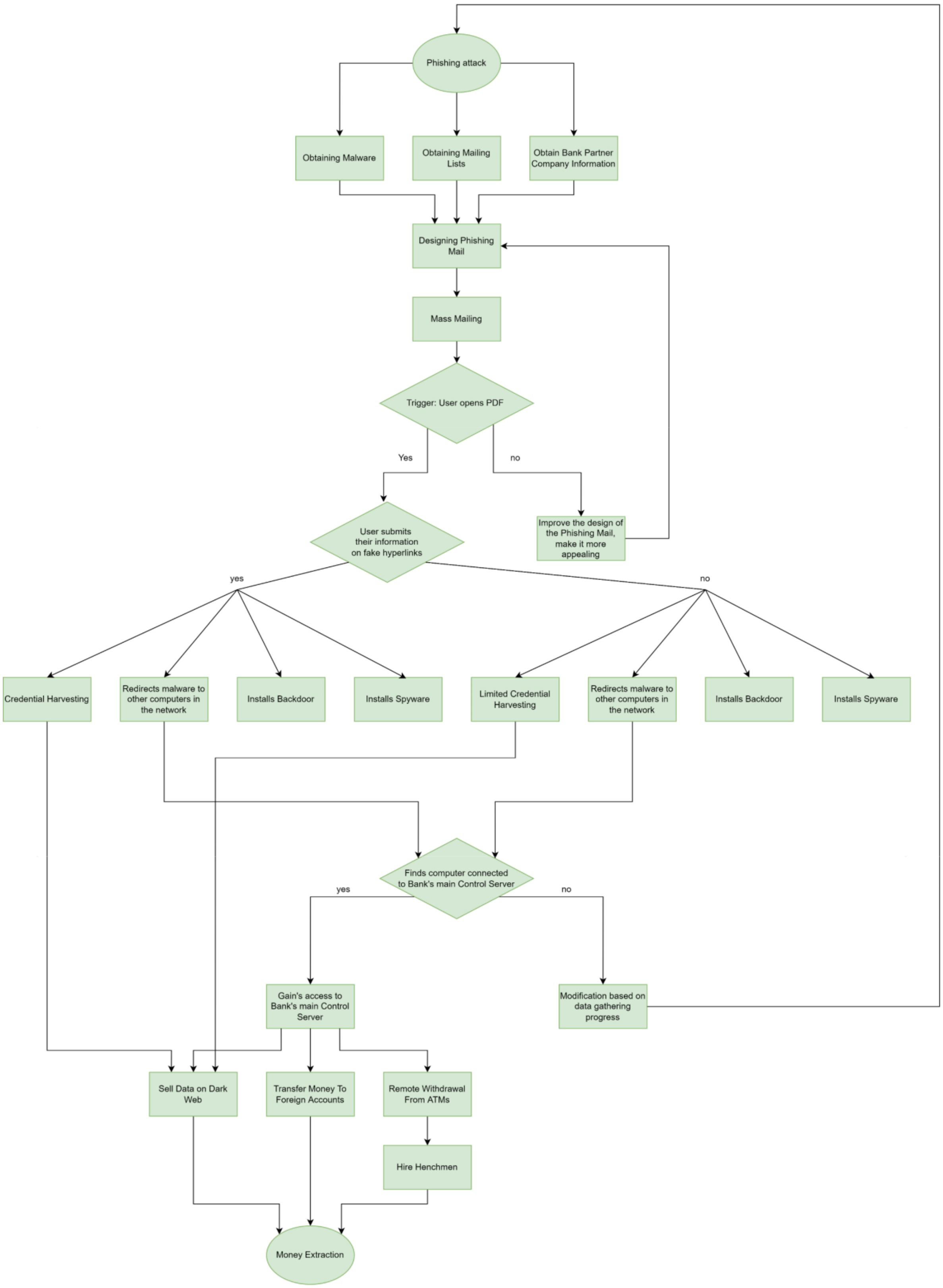
This kind of phishing attack requires two subgoals: obtaining the malware and mailing lists. The malware will come in the form of a PDF attachment (more on this later). The malware can include many built-in exploits in the forms of spyware, backdoor, and worm. The underlying obfuscated code should guarantee that malware 1) can spread through the system 2) collect information 3) install a backdoor for later access 4) allow modification via backdoor and 5) take complete control over the user's computer. In our data gathering step, we should find more information about the bank's partner companies, or companies from which a targeted phishing mail would not be suspicious. This can be done by online research or bribing a certain employee for seemingly "harmless" information. Additionally, we need to find out the bank's PDF reader software which it preinstalls on employees' devices. There is a high chance that our targeted bank might not be using the latest up-to-date version, thereby, leaving room for vulnerabilities. We could perhaps extract this information from the aforementioned bribed employee. We could also use open-source intelligence to achieve this step. In such a scenario, we could hire people from the dark web or other hacking forums who will write malware for us. We could pay a certain sum upfront and the rest after the successful completion of the attack. This could potentially save us on some of the high costs associated with this sub-node.

We would also need mailing lists to spread malware through the mail. Using open-source intelligence, we could employ different search engines to find the emails or other contact information of the employees. This could be done by visiting their website, finding the address to their groups or pages on social media. For instance, we could also use shodan.io to look for remote desktops which would reveal certain account user credentials and so on. If these methods do not work, we could target employees directly. Unlike directly asking them to plug in an infected USB drive which would be suspicious, we could use social engineering to ask for credentials of their superiors and co-workers. Alternatively, we could bribe them since they will be more likely to give out information, they have easy access too without much hustle or risk for exchange of reasonable sum. The aforementioned could also be useful when researching banks' partner companies. These methods vary in cost and stealthiness, hence some adaptation might be needed based on the initial data gathering described above.

Once we have both the malware and mailing list, we will send out mass phishing emails also known as the shotgun method. However, if we were to obtain the credentials of someone with a high likelihood of having access to the bank's main control server, then we might pursue a spear-phishing attack instead which targets specific groups or individuals. We could use commonly used malicious HTML attachments and disguise phishing attacks as a request from IT to employees to update their passwords, however, this would quickly get the attention of the higher-ups and sabotage our attack. Instead, we decided to obtain information about the bank's partner companies to plan a more reliable phishing attack. The distributed emails would mimic the language of previously used emails from partner companies offering employees certain "benefits" for accessing their programs. This advertisement would contain believable carefully crafted heading along with a PDF attachment where users could find out more information about their received benefits. Once the user interacts with PDF documents by opening it with preinstalled PDF software, a certain malicious code will be executed which will utilize vulnerabilities in the software and deliver the payload either via buffer overflow attack or obfuscated malicious JavaScript code. Nevertheless, this attack might need modification based on the vulnerabilities revealed in the data gathering step. In such a scenario, a PDF document executes a malicious code enabling us to take over the computer, gather more information, spread itself, and stay dormant through the backdoor – waiting for our future commands. Furthermore, the PDF document in itself will contain carefully crafted text to seem as authentic as possible about the aforementioned benefits. Since the employees have seen similar offers before, they might be tempted to engage with the hyperlinks present in the document. Those hyperlinks could further redirect them to fake log-in pages where they have to enter their credentials to claim the fake benefits. Not only are we able to infect the computer, but we are also able to gather further credentials, which could be used for achieving other goals or perhaps selling them to generate profit. Furthermore, if the phishing emails are distributed randomly with significant time intervals, an average advertisement will not raise much attention among users and will allow us to maintain our attack in the longer term.

Once we obtain access to the main control server, we can send out commands to ATMs in a network to withdraw money at a predetermined location. We will hire henchmen who will take money for us, and as such our physical presence won't be required, reducing the risk of getting caught. We will transfer some of the sums to foreign accounts in different countries, from which we can withdraw money, provided that the targeted bank does not have enough time to react. If there are additional credentials or private information harvested during the process of the attack, we could sell them on the dark web for further profit.

In this manner, we would have two main triggers: 1) users clicking on the phishing mail and 2) users downloading PDF documents (or even clicking existing hyperlinks). While we cannot directly automate when users will click our phishing email or download the malicious files, we can automate the timing of infection after the user downloads the malware to a certain extent. For example, once we infect certain computers, we might want to schedule the infection throughout a specific period. This would decrease the likelihood of it being noticed or talked about, increasing our stealthiness. We could also schedule the malware to execute when the user is away (e.g., at lunchtime). In such a fashion, the user will not be able to notice a potential increase in CPU usage, slowdowns, pop-ups, or such, thus increasing our stealthiness. However, if we find that their mailing services or browsers are outdated in our data gathering step, we could perhaps modify our malware for drive-by downloads, which does not require user intervention and as such would be an example of full automation. Additionally, our final point of attack is accessing the bank's control server. If we gain access to it, we can decide the timing of our final point of the attack. All in all, the aforementioned steps will increase the likelihood of a successful attack by increasing stealthiness without adding too much complexion and cost in the forms of basic scheduling.


Phishing attack
Obtaining Malware
Obtaining Mailing Lists
Obtain Bank Partner Company Information
Designing Phishing Mail
Mass Mailing
Trigger: User opens PDF
Yes
no
Improve the design of the Phishing Mail, make it more appealing
User submits their information on fake hyperlinks
yes
no
Credential Harvesting
Redirects malware to other computers in the network
Installs Backdoor
Installs Spyware
Limited Credential Harvesting
Redirects malware to other computers in the network
Installs Backdoor
Installs Spyware
Finds computer connected to Bank's main Control Server
yes
no
Gain's access to Bank's main Control Server
Modification based on data gathering progress
Sell Data on Dark Web
Transfer Money To Foreign Accounts
Remote Withdrawal From ATMs
Hire Henchmen
Money Extraction

Flow Chart 1.0 of the Phishing Attack

Modify and evolve

It is always important to have complete control of an attack all the way until its job is done. In our case, we will design malware in such a way that once it's delivered successfully, it takes control over the main control server of the targeted bank. Thereafter, our intention will be to install multiple other malicious programs or applications such as keyloggers, spywares, Remote Access Trojans (RATs), create backdoors, etc. on other machines in the office including that of the executives. Attacking and taking control of the bank's main control server will be the most essential stage as once it's successful, we will have the ability to accomplish pretty much anything malicious because we have obtained full control of the bank's network at this stage. Our motive to infect computers with other malicious programs (as mentioned above) while staying idle for a certain period of time is to remotely monitor (using spyware) the employees' behaviors and usage on the computer which could turn out to be crucial knowledge for us in initiating our final attack or even capture credentials (using spyware or keyloggers) and there on escalate our privileges, as mentioned in earlier paragraphs. Additionally, we can capture credentials and steal the bank's sensitive financial data or documents to be either used by ourselves or sold on the dark web for huge amounts of money. However, our primary goal is to attack the ATMs.

Staying persistent should be one of the primary goals of a successful attack. We plan to have our attack stay undetected from anti-virus software and other detection systems through the combination of some of the ways described here. Infecting or attacking the main control server might not be a straightforward attack to carry out with stealthiness and we may want to stay idle for a certain period of time to figure out and think of different ways based on server configurations to accomplish the attack and prevent time-based recognition. Additionally, we will use the concept of 'polymorphism' which refers to changing the malware code every time it replicates to another system. Since we will be trying to infect other machines on the network, it will turn out to be very helpful in evading detection. In order to ensure more stealthiness, we will combine 'polymorphism' with 'encryption' to prevent signature-based matches in anti-virus software. Additionally, the communication channels between the control center and machines can be concealed using an encrypted network. This will decrease the probability of useful data (that malware authors don't want to be noticed) being captured in alerts or log files of monitoring systems.

The information gained from the first milestone was not enough to carry out an attack successfully, but it was a crucial and important step in planning out an effective and directed attack plan by narrowing down our primary target and gaining a clear picture of our motives to attack the financial sector. For example, in the first milestone, we lacked the specific steps of attack and information such as the detailed action steps - malware delivery and initiation, phishing using a mailing list, and finally, server infiltration - and required assets and ways to obtain them. A targeted and directed attack is more successful and damaging as compared to an untargeted one because "it has been specifically tailored to attack your systems, processes or personnel, in the office." (National Cyber Security Centre). The knowledge of the absence of proper security measures in ATMs that are using legacy systems and the larger scale of impact that a similar attack method can have, compared to other sectors, helped us get convinced to dive deep and plan out. Hence, based on the knowledge gained from the first milestone, it helped us have a broader view of the attack landscape while considering several attack scenarios and methods.

Milestone IV

As investigated in Milestone 1, the most common cyber-attacks towards the financial sector are server access (28%), followed by data or credential theft (20%) (IBM). Thus, our attack can be considered as using one of the most popular methods in the literature. As our attack uses malware to harvest user credentials, it can be compared to the aforementioned 2019 GozNym malware attack, where a criminal gang stole more than $100 million with stolen user credentials from thousands of victims. Both have another similarity as they also use phishing emails as the delivery method of their attacks. However, while the GozNym attack directly targeted victims to steal their critical information, our attack mainly targets the main control server of a bank to distribute commands to ATMs to withdraw money in ordered locations.

Our attack can be considered an advanced persistent threat based on the attack scenarios. More specifically, our attack can cause meaningful damage and we are in control of when we can execute the infection or the final stages (gain access to the main control server) of the attack. As we have mentioned, we are trying to spread through the bank's network for admin privilege escalation from where we can gain access to the bank's main control server. For example, upon the first infection (executing malware through malicious PDF which spreads itself to other computers in the network), we can monitor the user's activities, while keylogging their sensitive information. We can then use this information to plan out our attack. We might choose a more suitable time or a period where most profit can be generated. Furthermore, staying for a prolonged period in a system will allow us to understand banking mechanisms to see what would be the most undetectable manner for our final attack or if it needs to be modified. Additionally, during the data gathering process, we will be able to capture sensitive information and credentials of bank employees or any other bank files they operate on. Not only does this count as a threat that rises exponentially with the time we stay in the system but also could potentially enable us to generate additional profit from selling captured data on the dark web. In such instances, we are not only posing a financial threat but also a threat to the bank's whole structure, its dependencies, employees, their lives, and assets. The cascading effect such an attack might bring about is hard to measure but the impact will be felt throughout the country.

Being stealthy is one of our major priorities while carrying out the attack. An attack is truly successful only if it also has the mechanism to stay hidden before, during, and after the final attack is performed. Our initial steps include phishing – delivering malware through emails, or social engineering the email such that the user or bank employee visits the malicious website through the PDF hyperlinks and enters his banking credentials. So, in this case, phishing is carried out through the web, and web-based attacks have significant advantages for attackers with respect to stealthiness. According to the research paper "Guarding Against Network Intrusions," web servers "serve up an attack only once per IP address, and otherwise serve up legitimate content" (Chen & Walsh). In simpler terms, the infected server recognizes and saves the IP addresses of the visitors. Hence, visitors may only be targeted once, effectively making the attack detection more complex.

We plan to use multiple ways in combination to evade detection by network monitoring systems. To increase our stealthiness, our main operations will prioritize stealthiness over speed and resilience, and will use a delay-tolerant methodology, which is “transmitting information through circuitous channels to avoid detection by defenders” (Center for Security and Emerging Technology). It is because hard-coded communication channels offer no flexibility and are easier to detect and block once discovered. As an instance, in the Moonlight Maze case, in the late 1990s, Russian government hackers “used two common networking protocols as their C2 channels”, making it easier for the defenders to detect and block the communication (Center for Security and Emerging Technology). Moreover, we could use automated techniques to obscure control server’s malicious activities by including a mechanism in our malware such that the control server activities are camouflaged to blend in among the targeted bank’s normal network traffic. Performing this during the working hours (active network traffic) of the targeted bank will improve the stealthiness overall as well.

An important part of this process would be to employ the use of machine learning in our attack, without which it would be infeasible to “blend into the background traffic without triggering alarms” (Center for Security and Emerging Technology). The attackers with the intention to “blend into the background noise of the victim’s network” can keep track of and analyze the “types of network traffic, volume, and usage patterns” (Center for Security and Emerging Technology). This will be critical because “armed with this data, attackers can modify command and control and exfiltration systems if stealth is a priority” (Center for Security and Emerging Technology). Once the bank’s main control server is compromised, the malware will use the techniques of ‘polymorphism’ and ‘encryption’ in combination (as explained in Milestone 3) to prevent signature-based matches by anti-virus software. Additionally, as a final step once the attack is executed successfully, the malware will perform the “destruction of system log files” in order to “evade network defenders and baffle incident responders” as well as prevent the defenders from tracing back the attack to us (Center for Security and Emerging Technology).

Additionally, in order to be certain to have access to the network anytime in the future, we will create administrator accounts that would “run scripts that are automatically executed at boot or logon to establish persistence”, disable firewall rules, and even activate remote desktop access on servers and other systems on the network (Huntress).

Conclusion

On a final note, through careful examination of all four milestones we have identified various mechanisms through which we can infiltrate financial systems in the U.S for maximized profit generation. Based on all possible attack avenues with evaluations in regards to their stealthiness, ease of deployment and cost, we narrowed our choice down to phishing-based ATM attack where our primary target is bank's main control server, through which we are able to remotely access ATMs for cash withdrawal, transfer of money to foreign accounts and sell the data (e.g., credentials). The attack contains a carefully crafted exploit which allows full control via control server, later modifications, along with possibilities of trigger automation which in turn enables our attack to persist for a long time, increasing the likelihood of a successful outcome. Moreover, the use of today's modern and secure encryption technology and polymorphism will play a significant role in evading detection throughout the infection lifecycle. Our attack in order to succeed relies heavily on stealthiness and persistence as we use the delay-tolerant methodology once the control server is infected or compromised. Hence, we can consider this as an APT threat. All in all, each milestone enabled us to advance our attack with a more detailed plan in mind, which ultimately enabled us to come up with a methodology that would guarantee a successful attack based on necessary steps, feasibility considerations, and opportunities for modifications by enabling complete control.

References

"Financial Services Sector." Cybersecurity and Infrastructure Security Agency CISA, https://www.cisa.gov/financial-services-sector.

2017 Cost of Cyber Crime Study | Accenture. https://www.accenture.com/_acnmedia/pdf-62/accenture-2017costcybercrime-us-final.pdf.

Singleton, Camille. X-Force Threat Intelligence Index. IBM Corporation, 2021, https://www.ibm.com/downloads/cas/M1X3B7QG.

Johnson, Joseph. "Data Breach: Average U.S. Organizational Cost 2020." Statista, 25 Jan. 2021, https://www.statista.com/statistics/273575/average-organizational-cost-incurred-by-a-data-breach/.

Goldberg, Matthew. "These Are the 15 Largest Banks in the US." Bankrate, https://www.bankrate.com/banking/biggest-banks-in-america/.

"The Countries Experiencing the Most 'Significant' Cyber-Attacks." Specops Software, 13 July 2020, https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/.

"Timeline of Cyber Incidents Involving Financial Institutions." Carnegie Endowment for International Peace, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide.

Cost of a Data Breach Report 2021. IBM Corporation, 2021, https://www.ibm.com/downloads/cas/OJDVQGRY.

Cost of a Data Breach Report 2019. IBM Corporation, 2019, https://www.ibm.com/downloads/cas/RDEQK07R.

Wiener, Jeff, et al. "How Much Profit Does the Average Small Business Owner Make a Year in 2021?" Entrepreneur.com, 13 Aug. 2021, https://www.thekickassentrepreneur.com/profit-average-small-business

CVE, https://cve.mitre.org/index.html.

Amadeo, Kimberly. “Who Really Owns the Federal Reserve?” The Balance, April 29, 2021, https://www.thebalance.com/who-owns-the-federal-reserve-3305974.

CISA. “Financial Services Sector-Specific Plan 2015” CISA, 2015, https://www.cisa.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf.

Positive Technologies. “Financial Application Vulnerabilities.” PTSecurity, 13 Sept. 2019, www.ptsecurity.com/ww-en/analytics/financial-application-vulnerabilities.

Intsights. “The 3 Most Common Vulnerabilities for Banking and Financial Services Organizations.”,

29 May 2019, https://intsights.com/blog/the-3-most-common-vulnerabilities-for-banking-and-financial-services-organizations

KamerpowerKamerpower est un hub pour les étudiants. “How Much Money Is in an ATM : Money ATM Machine Holds.” Kamerpower, 20 Sept. 2021, https://kamerpower.com/how-much-money-is-in-an-atm-money-atm-machine-holds.

Boston Consulting Group. “Global Wealth 2019: Reigniting Radical Growth.” Accessed November 16, 2021, https://www.bcg.com/publications/2019/global-wealth-reigniting-radical-growth.

Marzulli, John. “Two Brooklyn men ripped off $5M from ATMs around globe, feds charge.” New York Daily News. March 6, 2008, https://www.nydailynews.com/new-york/brooklyn/brooklyn-men-ripped-5m-atms-globe-feds-charge-article-1.285511.

Wild, Owen. “How much does ATM crime cost?” NCR Corporation. January 6, 2016, https://www.ncr.com/company/blogs/financial/how-much-does-atm-crime-cost.

Cyber Attacks Work.” National Cyber Security Centre, 14 Oct. 2015, www.ncsc.gov.uk/information/how-cyber-attacks-work.

“Here’s How Much Thieves Make by Selling Your Personal Data Online.” Business Insider, 26 Nov. 2018, www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5?international=true&r=US&IR=T.

Thomas M. Chen, Patrick J. Walsh. "Guarding Against Network Intrusions", 2014, https://doi.org/10.1016/B978-0-12-416689-9.00003-4.

“Automating Cyber Attacks.” Center for Security and Emerging Technology, 22 June 2021, cset.georgetown.edu/publication/automating-cyber-attacks.

Fortinet. “Understanding the Security Challenges of ATMs Why Banks Should Be Concerned.” 2019, https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-understanding-the-security-challenges-of-atms.pdf