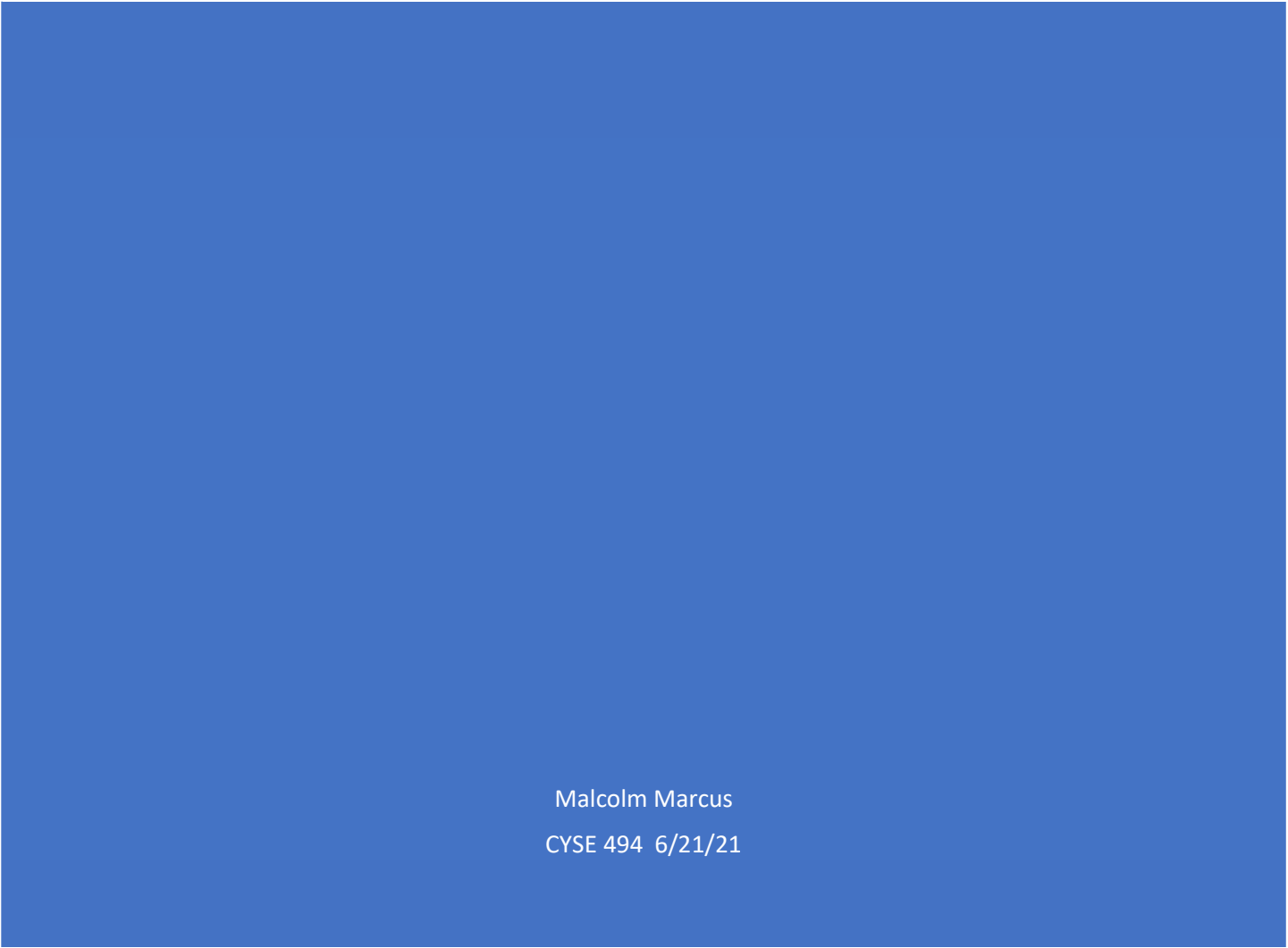




BANKING MALWARE PREVENTION



Malcolm Marcus
CYSE 494 6/21/21

Table of Contents

BANK MALWARE PREVENTION	2
Introduction	2
LITERATURE REVIEW	3
Banker Trojans: An Overview.....	7
Examples of banking malware;	8
Cerberus is a new Android banking malware that targets renters.....	Error! Bookmark not defined.
Gustuff: The Android Banking Trojan Targeting 100 Banking Apps.....	Error! Bookmark not defined.
Highlights Vulnerabilities in Mobile Banking Applications	8
Fake Apps Have Been Found in Official App Stores.....	8
The Main Vulnerabilities of Android.....	9
Repackaging an application	9
Fake Installer	9
Attacks such as Cold Boot and Others	9
Vulnerabilities in Dalvik and ART	9
Attack Man-in-the-Middle	10
1. Use SCA-compliant two-factor authentication for online banking.....	10
2. Use RASP to Strengthen Your Mobile Apps	10
System for Behavioural Authentication and Fraud Detection.....	10
4. Collaborate with Anti-Virus Vendors to Detect and Remove Known Malware.....	11

5. Educate Your Client	11
6. Self-Reflection.....	15
References.....	17

BANK MALWARE PREVENTION

Introduction

Banking malware is a type of malicious software that steals data from financial institutions. New variants of banking malware are being produced by the original developers or others utilizing disclosed source code. Every day, banks around the world are entrusted with trillions of dollars of people's money, and any amount of that can be gone in the blink of an eye at the hands of a hacker. This could be accomplished in various ways, but in today's world, malware is the most general approach used by hackers to get access to the financial system.

Malware is a sort of software designed and distributed to inflicting harm to a computer or a network as a whole. The issue is that banks and other financial institutions around the world lack the necessary security to prevent an attack effectively. The problem is exacerbated by the fact that, with the rise of mobile banking, it is becoming easier for attackers to get malware onto your mobile device and computer, allowing them to gain access to banking information and other sensitive information. After gaining access to the account, the attacker can carry out an unlimited number of transactions on the victim's behalf.

In the last few years, the number of malware infections has steadily increased, from around 12 million people affected in 2009 to around 813 million users in 2018. The rise will continue as technological advances accelerate, and people's lives become increasingly reliant on IoT devices. As a result, a newer method of protecting users and institutions from the malware that has been plaguing the internet world is required, as the current methods allow hackers to bypass them quickly and have their way. With the various banking malware that is out there, such as Zeus (Zbot), which has been around since 2007 and is constantly evolving, Gozi, which has also been around since 2007 and has multiple different variants of the original malware, GozNym, which is one of the variants of the Gozi malware and many others, their goals are all the same: to disguise themselves as something they are not.

LITERATURE REVIEW

Hackers target internet banking as one of the most common activities on computers and cellphones. Although security has improved substantially in recent years to reduce consumer

risks, users remain the weakest link in the system. According to Bijmans et al. (2019), hackers only need to inadvertently install a malicious program to launch attacks on your digital assets, whether it's personal data or money.

The malware uses no advanced low-level system compromises. People are encouraged to open attachments or click links via spam. They unwittingly install harmful malware on their PCs as a result of this. This software allows fraudsters to acquire unauthorized access to and control over their victims' internet financial accounts. Web injects (fake displays that look like the online banking environment) are used by the malware to collect victims' login information. The quantities and details of the recipients are modified behind the screens. It simply took use of the Android platform's "Accessibility" permissions (Kumar et al., 2014). The APIs are important because of developing applications to those with restricted smartphone capabilities (blind users, limited hands) but in the wrong hands they may be dangerous. Once the rights have been given, the virus may read the contents of any windows shown on the screen. It may recognize the beginning of a mobile banking app and provide a wrong login user interface at the right moment. According to Bettany et al. (2017), the virus may even mimic activities and prevent a user from erasing them by automatically closing the Settings app. The target evolution process basically modifies the behaviour of malware in both targeted and untargeted environments/hosts. Each host's environment is described here as a collection of resources, such as files, the system registry, system objects, configuration, language, keyboard layout, IP/MAC addresses, and user-specific data, such as user profile and credentials. Such environment data is increasingly being utilized to direct malware's activity. Stuxnet[95], for example, is a well-known example of malware that has been detected targeting Iran's nuclear facilities. Stuxnet infects a host when it detects that the host environment is similar to that found in devices that operate nuclear power

plants. One significant conclusion from the example is that targeted malware often incorporates environment-sensing logic to aid in target identification. Existing dynamic malware methods are incapable of cracking this logic because they do not pre-provide the captured malware with the required environment for examination.

Malware is regarded as one of the most severe risks to system security, causing complicated system problems. Numerous kinds of malware may gain access to and infiltrate networks and systems through coordinated assaults. Anti-forensic methods are often used by malware to evade detection and investigation. Additionally, the findings of such studies are often useless and may cause impediments to collect clear evidence owing to a lack of adequate instruments and an immature forensics approach. Malicious software, such as Internet worms, computer viruses, and Trojan horses, poses a significant danger to networked systems' security. Classic signature-based detection is significantly hampered by the diversity and quantity of its variants. Nonetheless, malware families have common behavioral patterns that reveal their origin and intent. We want to use these common characteristics to classify malware and provide a method for learning and distinguishing malicious behaviour.

A malware detector is software for detecting a malicious application. Malware authors often use obscure detection software. Malware detectors that match patterns (like commercial virus scanners) are hackable. The pattern correlation method for virus detection is a major defect: it is purely syntactical and ignores the semantics of instructions. Approximately 3,000 online banking clients were affected by a computer virus that empties their accounts and shows false information that enable the fraud to go undetected. Experts say that the assault using a Trojan virus was known as the most sophisticated and deadly malware ever conceived. Experts warn that between July 5 and August 4, cybercrooks stole £675,000 and the assault is still continuing.

Once hackers have made money with banking malware, they will want to launder the money to hide the illicit origins and avoid being prosecuted. Malware can hook directly into a user's browser because it is an executable on the user's PC. After receiving bank-specific malware, the operator parameters it, specifying which accounts will be targeted, how much money will be stolen, and where the money will be transmitted afterward. To authorize transactions, some institutions employ a second channel.

Following authorization methods are useless, and malware can overcome them because malware can modify transaction data "on-the-fly" and change server answers. Hardware token generators, TAN codes Security overview of script-based malware detection in online banking, SMS without transaction data. Malicious software is comprised of viruses, worms, spyware, and Trojans (CyberSecurity Products and Services). Cyber risk assessment is a process that many companies use to determine how vulnerable their systems are to cyber-attack. The standard cybersecurity risk assessment process begins with identifying the different companies' assets that may be compromised, which may include procedures, databases, and other hardware that contains critical data. Following the identification of possible hazards, the following stage is to choose the control mechanisms that will prevent the assault.

A Trojan banker is a harmful program for accessing information stored or processed by online banking systems that are sensitive or material. A backdoor in a computer like this allows other parties to access a computer or copy credentials of banking clients by copying a financial institution's login page. It is a kind of Trojan horse that may be hidden on the computer as legitimate software. Once installed, the Banker Trojan may access data and systems from a computer that enables attackers to conduct fraudulent activities, steal customers' identities and take money from customers' accounts.

The new Trojan virus, Zeus v3, is a variant of the Zeus Trojan banking virus that originated three years ago and could empty bank accounts without owners' knowledge of theft because of false statements (Vijayalakshmi et al.,2017). 'We have never seen such an intelligent and severe attack,' said M86 Security. Keep an eye on your balance and be conscious of what it is. After M86 had access to an Eastern European criminal command and control server, fraud was discovered. It gathers information like passwords and even transfers funds automatically from accounts, but only after the verification is at least £800 available. "The virus that the usual security software cannot identify is a brilliant kind," said Bradley Anstis, M86 Vice President of technological strategy.

The organization claimed it was the most sophisticated and dangerous malware it has ever encountered and recommended online banking users to constantly check their balances and have a good notion of what it should be.

Banker Trojans: An Overview

The Banker Trojan is an online banking and financial horse, which redirects the traffic to another site, allegedly controlled by the assailant. Every time the system starts, the program replicates to the host, creates folders, and sets registry entries. You are looking for specific personal financing cookie files which financial websites have saved on the computer during an internet visit. The Trojan horse has the ability to run files, download and remotely send files, steal information, and log keystrokes from the clipboard, among other things. It collects cookies and passwords and can delete from a computer if instructed.

Patel et al. (2010) say that consumers and organizations should be cautious about downloading programs, but errors occur, and systems may get infected. Criminals have improved their confidential financial information methods. Although computer viruses, spyware, and Trojan horses can still steal usernames and passwords, many of them go on to collect in real-time and ingeniously transfer money into other accounts. Financial organizations' authentication processes for fighting the efficiency of Trojan horse malware have increased their safety. That is particularly critical when banks expand the number of banking transactions that are inherently less safe than transactions per person, either via the Internet or mobile devices.

Examples of banking malware;

Vulnerabilities in Mobile Banking Applications

PSD2 permits third-party applications and, potentially, social media sites to be used with mobile banking(Valcke et al., 2015). As a result, developers may be forced to use potentially insecure remote APIs, thus exposing them to new dangers. Hackers could, for example, reverse-engineer and attack the API that connects the mobile phone app to the third-party server. Criminals might abuse the API's cryptographic key, which could be found in the mobile app code. In such circumstances, additional app-specific defense measures can assist in safeguarding the applications.

Fake Apps Have Been Found in Official App Stores

Large companies like Google and Apple seem unable to completely block the distribution of telephone applications through their secure webshops, Google Play and Apple Store. Fake apps can control a telephone, steal the data and interfere on the same phone or tablet with other

financial apps (Clapsadi et al., 2012). Although malware-infected programs can sometimes be released to official app stores, unknown sideloading software is still a much more risky option. If the device has not been broken in prison, there is little chance of sideloading apps.

The Main Vulnerabilities of Android

Here are some of the commonly found vulnerabilities of the Android Operating System:

Repackaging an application

If the source code is not well-obfuscated, the hacker decompiles it to gain access to the source code. The application is then repackaged and disseminated through legitimate channels with malicious malware installed in it.

Fake Installer

The hacker delivers a setup file that appears to be legal, but it actually installs a trojan. It also takes advantage of the permissions it asks for from the user. The phoney setup employs a foreign language to conceal the app's genuine "intentions." After being kindly requested, the user will generally grant the installer permissions.

Attacks such as Cold Boot and Others

The device is forced into recovery mode by a variety of attacks. This is the location where a customized operating system is downloaded.

Vulnerabilities in Dalvik and ART

Dalvik is a process that runs on a virtual machine (now known as Android Runtime - ART). In the Android environment, this runtime runs bytecode. It has several flaws that could allow an attacker to gain administrative rights or cause a denial of service.

Attack Man-in-the-Middle

Man-in-the-Middle Assaults are the brutalist preventative attacks. In Android, malware that claims to be banking apps works as a middle man between users and simple banking apps. It then records second-factor authentication and utilizes this with various amounts and recipients in the actual application. How to Get Rid of Malware

1. Use SCA-compliant two-factor authentication for online banking.

Bank customers are safe with robust 2FA authentication, even if malware steals their username and password. It's because if malware tries to use the credentials to make a payment, the consumer will be notified and will be able to reject it right away. One example of a security method is a mobile token app.

2. Use RASP to Strengthen Your Mobile Apps

The current mobile malware uses accessibility or monitoring features to detect a mobile banking application and to provide a fake login user interface at the appropriate time.

Modern RASP systems, including Wultra's Promon-powered App Shielding, provide various mitigators to address issues with security issues. You can disable untrusted screen readers and, among other things, hide the process name of the running mobile banking app. As a result, mobile malware cannot view the mobile banking app and cannot perform its disastrous activities.

System for Behavioural Authentication and Fraud Detection

Saevanee et al. (2012) explain that even when an attacker gathers customer credentials, he must be able, if the relevant counteractions are in place, to successfully put these credentials in the financial systems to steal the money. In other words, the attacker needs to persuade the system that the correct user entered the credentials and paid for the right channel.

The behavioral authentication and fraud detection system of Threat Mark can both identify a correct person based on the in-depth behavior evaluation of a fraudster. It can score the operation on its own, using various inputs, like user location or payment attributes.

4. Collaborate with Anti-Virus Vendors to Detect and Remove Known Malware

Although some malware bypass current security measures, specific malware signatures, such as the package name, can be blocked. Antivirus software providers maintain massive databases of known safety hazards and viruses. Their technologies can detect a possible threat on your users' gadgets. When a malicious program is detected on the device, your mobile banking application can cry out 'Help' to the banking system, alert the bank's security staff and immediately block the client account to prevent further harm. You can use the native SafetyNet APIs of Android to check for potentially dangerous applications.

5. Educate Your Client

No security mechanism is complete without the active involvement of the system's weakest link: the end consumer. Banks should provide simple-to-understand instructions for customers on how to remain secure online.

To prevent the success of these various schemes, some kind of software or security program must be linked to online banking websites or applications. Thus, this proposal is to introduce an application that would be linked to online banking and, rather than attempting to prevent malware from infecting the computer and gaining access to sensitive information through some type of dual encryption, one performed by the bank, the encrypted data would then be encrypted in such a way that it would believe that the information had been compromised if a hacker gained access. Additionally, we would work with the financial institution to ensure that the encryption key is updated on a regular basis and that recycled keys are used wherever feasible. Knowing how hackers operate and how they are constantly changing the programs they use, the app would be able to learn from that encounter and send information about that variant back to headquarters, which could then determine what type of malware it is and configure a code to prevent that malware and similar ones from having an effect. Then, this information would be sent to the financial institutions who have collaborated with us and integrated into the applications and websites, ensuring that all users can rest confident that their money is secured correctly both internally and externally.

This software would already have an edge in that we could include information about the banking malware that we currently have in order to establish a solid baseline of protection since many types of malware just vary from one another. Similar methods have been used in the past to combat the dangers posed by hackers, but not to this degree, which would need our business to remain on guard 24 hours a day, seven days a week, since attacks may occur at any time and from anywhere. It would also require a significant amount of workforce, not only for the programming necessary to keep the app current and to maintain the confidentiality of the

individual's financial account while still being present to protect it, but also for lawyers to assist us in writing contracts with the banks. This may be why others have refrained from doing anything as ambitious as this, owing to the effort needed to get it started and maintain it. Still, once it is up and running, I think it would be a game-changer in terms of financial stability.

This software would already have an edge since we could include information about the banking malware that we currently have in order to establish a solid baseline of protection, as many types of malware just vary from one another. Similar methods have been used in the past to combat the dangers posed by hackers, but not to this degree since it would need our business to remain on guard 24 hours a day, seven days a week, because attacks may occur at any time and from any location. It would also need a significant amount of personnel to maintain the app's functionality and preserve the secrecy of each user's financial account while yet being there to safeguard it and assist us in writing contracts with the banks. This may be why others have refrained from doing anything as ambitious as this, owing to the effort needed to get it started and maintain it. Still, once it does, I think it would be a game-changer in terms of financial stability.

Some potential roadblocks include convincing significant banks to support and believe in the concept that there is a way to reduce the number of financial breaches drastically. To do so, we would simply need to start small and test the product with smaller banks to establish a foundation and tested experience before approaching the big. Another possibility is that an employee with access to the encryption key decides to leak it as a result of a disagreement within the company or perhaps after being fired and to assist with this, only a select few high-ranking individuals within the bank are to have access to both encryption keys, with access to both being immediately revoked upon termination. Given that the system may not be completely secure at first, some new malware may end up bypassing the degree of protection associated with online

banking and the software. Still, with continuous monitoring, this would combat any new malware, thereby keeping an eye on everything that is happening.

Due to the rise in bank malware-related crimes, the issue must be addressed. To make my idea a reality, the following steps must be taken: obtaining funding from potential investors; convincing significant banks to support and believe in the concept of my innovation; starting small and testing the product with smaller banks initially to establish a foundation and the tested experience we require; approaching larger companies such as navy federal, Wells Fargo, and SunTrust; and finally, being able to scale.

Efficiency and efficacy are critical characteristics of malware analysis and must be maintained throughout the investigation. Effectiveness contributes to the identification of significant elements of the evidence, resulting in meaningful studies. Digital forensics efficiency is directly linked to the resources utilized to collect evidence. These characteristics are functionally distinct and serve distinct functions in digital forensic investigations. With malware authors using a variety of methods to evade detection and conceal themselves from analytical instruments, the necessity to use the right approach is critical.

Marketing is a critical component in ensuring that ideas succeed. Marketing is crucial since it is the only way to inform people that you are offering a product or service. Marketing increases product recognition, establishes brand reputation, fosters consumer trust, and provides value to your audience in the form of information, entertainment, and inspiration. It enables companies to keep long-lasting and constant contact with their audience. It is not a one-time solution; it is a long-term strategy that allows companies to thrive. To successfully commercialize this invention,

many large organizations will need to join together. Making these organizations partners would be a significant step.

6. Self Reflection

Banking malware is a type of malicious software that steals data from financial institutions. New variants of banking malware are being produced by the original developers or others utilizing disclosed source code. Every day, banks worldwide are entrusted with trillions of dollars of people's money, and any amount of that can be gone in the blink of an eye at the hands of a hacker.

In the last few years, the number of malware infections has steadily increased, from around 12 million people affected in 2009 to approximately 813 million users in 2018. The rise will continue as technological advances accelerate, and people's lives become increasingly reliant on IoT devices. To stop these different programs from being successful, there must be some app or security program attached to online banking websites or apps. So, this proposal is to introduce an application that would be linked to online banking and instead of just trying to prevent the malware from getting to the computer and gaining access to sensitive information by some dual encryption one that the bank does and then the encrypted data would then be encrypted in such a way that it would believe that the information that if a hacker were to be able to get passed the apps second layer of encryption, they would think that the information that they are looking at is accurate. Then it would be able to detect the presence of any malware without having any precise information. To see that the program works would mean that financial breaches would begin to see a substantial decrease in the number of violations in their system, and the breaches would be at an all-time low. At first beginning this assignment I was not sure what I would do for an innovation, but once I was able to decide and do some research, I was able to learn a lot of

information about not only malware but the entrepreneur process as well. Being in a group and brainstorming our ideas for pitches was a little difficult at first until we were able to gain a foundation on what exactly we would be discussing and then it was only up from there.

References

- Bettany, A., & Halsey, M. (2017). *Windows virus and malware troubleshooting*. Apress.
- Bijmans, H. L., Booij, T. M., & Doerr, C. (2019). Inadvertently making cyber criminals rich: A comprehensive study of cryptojacking campaigns at internet scale. In 28th {USENIX} Security Symposium ({USENIX} Security 19) (pp. 1627-1644).
- Clapsadl, M. (2012). *Standardizing the security of mobile app store platforms* (Doctoral dissertation, Utica College).
- Kumar, G., & Kumar, K. (2014). Network security—an updated perspective. *Systems Science & Control Engineering: An Open Access Journal*, 2(1), 325-334.
- Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management & Computer Security*.
- Saevanee, H., Clarke, N. L., & Furnell, S. M. (2012, June). Multi-modal behavioural biometric authentication for mobile devices. In *IFIP International Information Security Conference* (pp. 465-474). Springer, Berlin, Heidelberg.
- Valcke, P., Vandezande, N., & Van De Velde, N. (2015). The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4.
- Vijayalakshmi, Y., Natarajan, N., Manimegalai, P., & Babu, S. S. (2017). Study on emerging trends in malware variants. *International Journal of Pure and Applied Mathematics*, 116(22), 479-489.

