Cybercrime Investigations
INSE 6610 – Summer 2022

Course Instructor: Dr. Ivan Pustogarov

Group Project Report

For

Comprehensive review of Cyber-attacks using specific case studies

Team Contributors:

1. Ajayi Samson (40202929)
2. Damilola Sanni (40199391)
3. Eunice Msheliza (40160778)
4. Jasmeen Kaur (40184380)
5. Olivia Okechukwu (40189600)
6. Varnesh Gawde (40159406)
7. Perehrat Sambo-Daju (40184186)
8. Mabir Singh (40191664)
9. Rowan Singh Sandhu (40196883)

A COMPREHENSIVE REVIEW OF CYBER-ATTACKS USING SPECIFIC CASES

Varnesh Gawde
Information Systems Security
Concordia University,
Montreal, Canada
varnesh.gawde@mail.concordia.com

Olivia Okechukwu
Information Systems Security
Concordia University,
Montreal, Canada
olivia.okechukwu@mail.concordia.ca

Damilola Sanni
Information Systems Security
Concordia University,
Montreal, Canada
damilola.sanni@mail.concordia.ca

Ajayi Samson
Information Systems Security
Concordia University,
Montreal, Canada
samson.ajayi@mail.concordia.ca

Eunice Msheliza
Information Systems Security
Concordia University,
Montreal, Canada
mshelizaeunice@gmail.com

Perehrat Sambo-Daju
Information Systems Security
Concordia University,
Montreal, Canada
perehrat.sambo-daju@mail.concordia.ca

Jasmeen Kaur
Information Systems Security)
Concordia University,
Montreal, Canada
k_smeen@live.concordia.ca

Rowan Singh Sandhu
Information Systems Security
Concordia University,
Montreal, Canada
rowansingh.sandhu@mail.concordia.ca

Manbir Singh
Information Systems Security
Concordia University,
Montreal, Canada
manbir.singh@mail.concordia.ca

***Abstract* — The world has become more advanced in communication, especially since the invention of the internet. Using computers for our day-to-day transactions is quite common nowadays. The key issue facing today's society is the increase in cybercrime or e-crimes (electronic crimes), another term for cybercrime. Thus, e-crimes pose threats to nations, organizations, and individuals across the globe. Every day, many fall victim to multiple cyber crimes - most of which stay unreported, boosting the confidence of cybercriminals. In this case study, we review three of some of the biggest cyber attacks ever conducted, which changed the world's point of view towards cyber-attacks. We analyze the process of attack, conduction of investigation and the charges pressed accordingly.**

Keywords—Cybercrime, Investigation, Security, Zero-Day, Melissa, Target Attack.

I. Introduction

The Internet is a system of international computer networks that are linked together using the internet protocol family [1]. Every day, the value of the internet is evident. People all over the world use it every day in one way or another, whether it be on their smartphones, tablets, laptops, smart watches, etc. People feel connected, and as usage rises, the distance between the virtual and physical worlds is closing. However, despite all these improvements, internet users still have to deal with a lot of negative side effects. The phrase "cybercrime" is associated with all the benefits of the internet [1]. At some point, everyone who uses the internet has encountered phishing, dangerous websites, phony emails (designed to trick the user), or at the very least submitted their information to a website that then sold their information to attackers [2]. Aside from such small-scale operations, attackers have attacked businesses on a massive scale on numerous occasions, causing damages in the billions of dollars. Such attacks never have a single purpose; they could be motivated by everything from avarice to retaliation, corporate rivalry, social activism, or even just a desire for vengeance. We have examined three of these major cyberattacks in-depth in our paper.

1) J.P. Morgan Chase Data Breach

2) Melissa Attack

3) Target Attack.

The impact of each of these incidents was significant in altering public perceptions of cyber security. Each of these attacks was unique in some manner, which helps to spread knowledge about cybercrimes and their security.

The investigation methods used to catch the attackers' perpetrators and the accusations that were brought against them are also covered in the report.

II. Case study - 1 (J.P.Morgan)

A. Literature Review

Over 83 million of JP Morgan's customers had their customer details stolen during the JP Morgan hack, which occurred between June and August 2014 [3]. It continues to rank among the greatest data breaches in history. Following this incident, the perception of the significance of cyber security among all financial institutions worldwide underwent a significant transformation. Eventually, it was found that the JP Morgan data breach was a part of larger computer crimes committed against American financial institutions, financial service providers, and financial news publishers. These crimes included "the U.S. Financial Sector Cyberattacks," the biggest ever customer data theft from a banking firm in the

United States. They took place between about 2012 and mid-2015 [4].

Challenges

- Loss of Data
- Loss of Trust
- Identify and patch the Loophole.

The Attack made the news like a wildfire as a huge company like JP Morgan was breached. The news created a shock across the world, especially in the United States. Not just JPMorgan many financial sector based companies were targeted by the attackers, As per the reports, the attacks were done in consideration of Stock Market manipulation, Money Laundering, Wire fraud and Illegal gamblings.

B. Attack Implementation

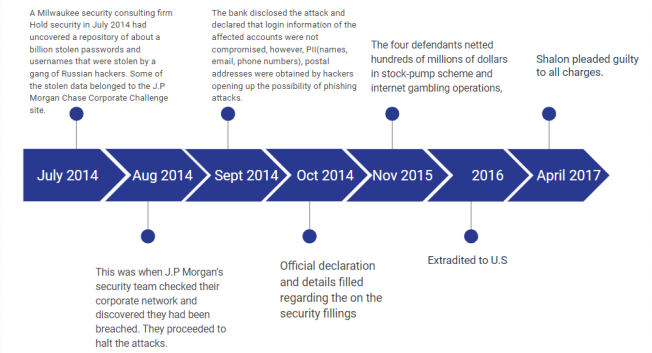


Fig. 1. Timeline of JP Morgan Data Breach

a. Overall

The business experienced a cyber event over a period of four months that coincidentally fit into all three of the "CIA trinity" categories. Data confidentiality, integrity, and availability make up the CIA trinity, which is well-known to those working in the field of information security [5]. In the case study, the business experienced attacks that had an effect on all three information security goals:

• **Confidentiality**: Private data was unavoidably made public.

• **Integrity**: Malicious software put information that was at rest in danger.

• **Availability**: Systems were looked at during the attack, which had an impact on the resources' availability.

Talking about the attack, When JPMorgan Chase's computer systems were compromised in October, full names, residences, contact information (phone and email), and URLs of the owners of about 83 million accounts were made public. This was one of the worst data breaches in history. The previously disclosed cyberattack on_For the sake of its customers, JPMorgan Chase & Co. was updated on October 2 on the webpages Chase.com and JPMorganOnline along with the mobile applications for Chase and J.P. Morgan... The Company revealed: [6]

- [7] *full names, residences, contact information (phone and email), and URLs, as well as their personal internal JPMorgan Chase data, have all been hacked. The compromised data affects 76 million people and 7 million small businesses. There is no evidence, however, that any account information, such as account numbers, credentials, login Details, birth dates, or Security Numbers, for the affected consumers was exposed as a result of the attack.*
- *As of the date given, the company has not yet experienced any expected customer fraud in relation with this occurrence.*
- *JPMorgan Chase customers who immediately report any unauthorized activity on their accounts to the business are not held liable.*

The people with knowledge of the investigation said that hackers gained access to the JP morgan complex computer network and reached more than Ninety servers. Since there is no proof that the attackers stole any money from users accounts, law enforcement investigators are still baffled as they look into the details of the breach.

Law enforcement authorities and security specialists have made the assumption that the hackers, who some assume to be from Russia, may have received backing from the Russian government due to the absence of any obvious financial motivation. From this vantage point, the data leak appeared to be more than just a sloppy cyber-attack.

Others involved with assessment, hackers had already entered the bank's network by the time security personnel noticed the breach in late July. accessed dozens of the bank's computer servers with the highest degree of administrative authority. How the hackers were able to get such broad access was still unknown at the time.

b. Investigation

Attackers

The attackers' team continued to have an effect on the American financial sectors after the strike by carrying out more attacks and engaging in online fraud. In November 2015, the government charged Gery Shalon, Ziv Orenstein, and Joshua Samuel Aaron along with twenty three charges.. Unknown is the identity of the fourth hacker who helped them access the networks [8].

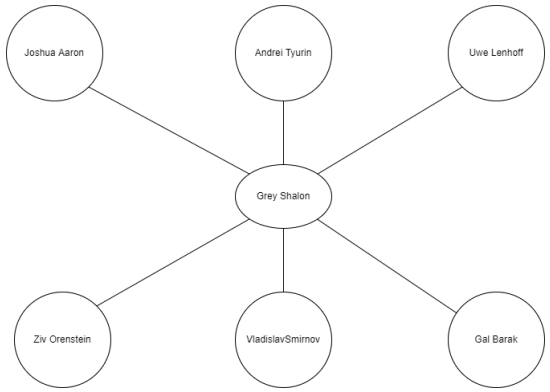


Fig. 2. The Shalon Network

The network of attackers responsible for the US financial cyberattacks, including the JP Morgan Chase data leak, was depicted in the above graphic.The US District Council in Atlanta, Georgia has filed new accusations against Shalon, Aaron, and an unidentified hacker. Ten charges are included in the Georgia indictment, including wire fraud and improper computer access. Orenstein is only being held accountable in New York. They are alleged of breaking into six additional financial institutions, including JP Morgan Chase, as well as online stock brokers, financial news websites, and even software companies. The parent firm of The Wall Street Journal, Dow Jones, along with Scottrade and ETrade were all hacked.
[8]
The alleged masterminds planned and boasted to one another in emails as they carried out what Federal agents refer to their operations as a "*sprawling criminal operation*" that stretched across the world with schemes buried inside schemes..

Shalon boasted about the extent and reach of his stock-price manipulation techniques and explained how he made use of stolen data. He sold stakes in one business at a profit. "*a small step towards a large empire. ... We buy them very cheap, perform machinations, then play with them.*"

In July, Anthony Murgio was detained in the US, while Shalon and Orenstein were detained in Israel. at about the same time on suspicion of running an illegal money-transfer business utilizing the virtual currency bitcoin that assisted in the laundering of the scheme's proceeds. Murgio was charged with running the Coin.mx service, which the hackers used to hide their profits, in a second indictment.
Officials claim that Aaron, who is known to have connections to Russia, is still at large. While an extradition process is underway, Shalon and Orenstein are still being held in Israeli prison. Although the origin of this cyberattack is now unknown, Russia and Brazil were reportedly under suspicion, according to Goldstein, Perlroth, and Corkery (2014). Brazil was not explicitly stated as the country where this crime originated, and there was no supporting documentation. Due to economic sanctions and US meddling in the disputes between Russia and Ukraine, Russia was still likely to remain a rival. The FBI eventually asserted that it was not the culprit.

.

A total of 30 criminal offenses with sentences ranging from five to twenty years are included in the indictments.
The following table gives a summary of the sentences and the penalties accordingly.
[9]

TABLE 1 - Criminal Offenses and Sentences charged against Defendants

Count	Defendants	Charge (United States Code)	Maximum Prison Term (years)
1.	Gery Shalon, Joshua Samuel Aaron, and Ziv Orenstein	Conspiracy to commit securities fraud	5
2.	Gery Shalon, Joshua Samuel Aaron, and Ziv Orenstein	Conspiracy to commit wire fraud	20
3.	Gery Shalon, Joshua Samuel Aaron, and Ziv Orenstein	Securities fraud	20
4.	Gery Shalonand Joshua Samuel Aaron	Securities fraud	20
5.	Gery Shalonand Joshua Samuel Aaron	Securities fraud	20
6.	Gery Shalonand Joshua Samuel Aaron	Securities fraud	20
7.	Gery Shalon, Joshua Samuel Aaron, and Ziv Orenstein	Securities fraud	10
9.	Gery Shalon, Joshua Samuel Aaron, and Ziv Orenstein	Wire fraud	20
9.	Gery Shalon, Joshua Samuel Aaron, and Ziv Orenstein	Conspiracy to commit identification document fraud	15
10.	Gery Shalon and Joshua Samuel Aaron	Aggravated Identity Theft	2
11.	Gery Shalon and Joshua Samuel Aaron	Conspiracy to commit money laundering	20

Table no: 1 Charges issued on the attacker

Robert J. Sica, Agent in Charge, said: "*This case highlights the Secret Service's investigative skills and our commitment to collaborate with our partners in detecting and dismantling highly sophisticated transnational criminal enterprises targeting the United States. These crimes can have a detrimental impact on our nation's critical financial infrastructure. The Secret Service, in conjunction with its many law enforcement partners across the United States and around the world, is committed to deploying cutting-edge investigative practices and technology in order to bring these offenders to justice.*"

c. Security Analysis

The majority of large banks employ a two-factor authentication method. The security staff at JPMorgan, however, apparently neglected to equip one of its network servers with the two step password method, according to persons who were informed of the incident. The bank was therefore vulnerable to an invasion.. Such basic security loopholes make it easy for attackers to infiltrate and seek what they were looking for. The loopholes are usually left because of multiple reasons from carelessness or not enough resources to carry security analysis on all the existing systems that play a key role in the infrastructure of the online base of the company.

It is evident that JPMorgan's hack did not deploy a "zero-day attack," a sophisticated, entirely new software flaw that may Sell for high bids on the illicit market.. Additionally, hackers did not employ the damaging malware that North Korean hackers allegedly used to corrupt Sony Pictures' data, according to government authorities. Many such attacks can lead to serious implications to big companies like JP Morgan as they possess huge amounts of user data and private information which need not be breached out of the wrong hands. A security team should always be updated with all the zero-day attacks present in the cyber world, as they can be the next target with those attacks.

Hackers did, however, succeed in gaining high-level access to more than Ninety servers once they were inside JPMorgan.., according to the sources informed on the investigations, but they were stopped before they could steal the financial information of individual customers. This shows the importance of privilege management. Having a proper hierarchy based system and not giving out privileges to any random user is crucial. It is not always the case that the attacker is going to be someone outside the company, many times there can be attacks from an internal circle.

Vulnerabilities

- Lack a two-factor authentication server[11]
    - 2FA is essential to web security because it instantly reduces the vulnerabilities associated with password breach. A password alone is meaningless without authorization at the second factor, thus if one is stolen, guessed, or even phished, it is no longer enough to allow access. [12].

- Unpatched software vulnerabilities
    - In particular, patch management is crucial for the reasons listed below: Security: Patch management repairs holes in your software and apps that can be exploited by hackers, lowering the security risk for your company[13].

- Lack of good host-based Intrusion Detection Software
    - Efficiency boost for other security controls: An IPS decreases the workload for other security devices and controls by filtering out harmful traffic before it reaches them, enabling those measures to operate more effectively[14].

- Heartbleed bug
    - The Heartbleed vulnerability allows anybody with Internet access to read the memory of machines secured by weak OpenSSL software. As a result, the user's identities, passwords, content, and secret keys used to identify service providers and encrypt communications could be stolen.[15].

Prevention

- Host-based intrusion prevention would have provided traces of malware.
- System patching on a regular basis to keep them updated would have reduced the chances of vulnerability in other parts of the software infrastructure.
- Employee training Would have educated employees to prevent malicious injection or accidentally providing attackers with higher access.
- Application whitelisting ensures that only authorized software is installed on the network. This would have stopped the network from getting the zero-day infection.
- Implementing access with the least privilege. The hackers wouldn't have been able to get the highest degree of admin privileges.

Costs

- An estimated cost of 1.782 billion USD was suffered by JP Morgan during the attack.
- One of the most important costs suffered by the company is the cost of the potential exposure of victims to phishing attacks leading to more personal loss of the client base.

- After the attack, The company compiled a cost of improving and upgrading their security systems at an estimated 250million dollars per year.

C. *Court Proceedings*

Preet Bharara, the U.S. Attorney for the Southern District of New York, Diego Rodriguez, the Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation (the "FBI"), and Robert J. Sica, the Special Agent in Charge of the U.S. Secret Service New York Field Office (the "USSS"), announced today the unsealing of an indictment accusing GERY SHALON, JOSHUA.SAMUEL and AARON. The Israel Police detained SHALON and ORENSTEIN today in Israel. The US Attorney's Office will ask for their extradition so they can face justice in the US. AARON remains at large.

Preet Bharara (Manhattan U.S. Attorney) said: "*As alleged, the defendants manipulated trading in U.S. securities from overseas, using fake identities to funnel millions of dollars in unlawful proceeds through a web of international shell companies. Using false and misleading spam e-mails sent to millions of people, these defendants allegedly directed their pump-and-dump scheme from their computers halfway around the world.*"

Diego Rodriguez (FBI) said: "*Crimes, such as the ones alleged herein, are multinational and complex in nature. The defendants are alleged to have profited in the millions of dollars and defrauded innocent investors for their own gain. The FBI is committed to working with our partners, both foreign and domestic, to ensure the integrity of our markets and protect our communities from fraud and deception, regardless of the scheme, means, or medium.*"
[10]

Violations

- With conspiracy to commit computer hacking, in violation of Title 18, United States Code, Section 371 (Count One)
- Computer hacking, in violation of Title 18, United States Code, Sections 1030(a)(2)(A), 1030(c)(2)(B) and 2 (Count Two);
- Computer hacking, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B), and 2 (Count Three);
- Conspiracy to commit securities fraud, in violation of Title 18, United States Code, Section 371 (Count Four);
- Conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349 (Count Five);
- Securities fraud, in violation of Title 15, United States Code, Sections 78j(b) and 78ff, Title 17, Code of Federal Regulations, Section 240.10b-5, and Title 18, United States Code, Section 2 (Counts Six through Twelve);
- Wire fraud, in violation of Title 18, United States Code, Sections 1343 and 2 (Count Thirteen);
- Identification document fraud conspiracy, in violation of Title 18, United States Code, Sections 1028(f) and 2 (Count Fourteen);
- Aggravated identity theft, in violation of Title 18, United States Code, Sections 1028A and 2 (Count Fifteen);
- Unlawful Internet Case 1:15-cr-00333-LTS Document 178 Filed 03/25/21 Page 1 of 21 2 Gambling Enforcement Act conspiracy, in violation of Title 18, United States Code, Section 371 (Count Sixteen);
- Unlawful Internet Gambling Enforcement Act, in violation of Title 31, United States Code, Sections 5363 and 5366, and Title 18, United States Code, Section 2 (Count Seventeen);
- Operation of an illegal gambling business, in violation of Title 18, United States Code, Sections 1955 and 2 (Count Eighteen);

With these, the attackers were heavily fined and penalized by the court. The Attorneys, and the cooperation between US and Israel to properly extradite to the United States. Stil many more are considered to be part of this series of attacks and they still remain unidentified.
[16]
[17]

III. Case study - 2 (Melissa virus)

A. *Literature Review*

On March 26, 1996, on the alt.sex discussion group, a virus was uploaded. The Melissa virus, purportedly named after a nearly naked dancer in Florida, was the result of the union of famous, computer, and sexual cultures. It included a nod to Bart Simpson, a list of pornographic websites, and an unquenchable need for identity. The industry went into overdrive very fast, with a lot of computer users shutting email servers to get rid of the malware and many taking advantage to develop and extensively distributed system-saving security software.[18]. This virus, which damaged network infrastructure in late March at an astounding rate, sent shivers down the spine of the computing industry. Concerns were raised when Melissa quickly spread through malicious email links which, once opened, sent the malware to contacts in unwitting recipients' contact lists. As a result, before it could be halted, Melissa spread quickly over the world and clogged up email servers [9]. According to this macro virus investigation, the need for human interaction (a user viewing a Word document that is infected) is necessary for the virus to propagate. [20].

A self-replicating piece of code in the macro language of an application is known as a macro virus.

Numerous programs include macro functionality, such as the automated replay of keystrokes seen in earlier iterations of Lotus 1-2-3. Less complex versions of programming languages like Visual Basic may be found in more powerful macro languages [10]. Microsoft Word 97 or Word 2000 users may become infected with the macro virus known as Melissa. Additionally, Word 98 for Macintosh documents and the malware are both susceptible. But the virus won't spread itself instantly and disseminate the infected document to others in the Macintosh environment. Computer viruses known as macro viruses replicate by using the application's built-in macro programming language. Macro viruses can potentially harm the document and other computer applications [21]. But maybe the most concerning aspect of this virus is what it might imply for the future. The virus, Melissa targeted flaws in significant and widely used technology that may be re-exploited with much more detrimental effects. Melissa was rather simple to develop [19]. A potential security flaw presented by macro languages was also used by the virus. In this instance, Microsoft's VBA allowed clients to include executable functionality in documents. In this situation, a file that was received as an email attachment included malicious capabilities. Thus, according to Peter Tippett, who was the Head Technologist of "The International Computer Security Association (ICSA)" and also a consultant in security, the Melissa virus marks a significant new advance in viral technology [19].

B. Attack Implementation

The Melissa virus was created by a man from New Jersey by name of David Lee Smith, who chose the name of a Florida exotic dancer he fancied. Smith said in court that he only planned to cause trouble and had no idea that his actions would result in such severe denial-of-service or damage at a time when financially driven malware was uncommon[22].

The virus was a creation of Smith, based on a macro from Word 97. On the morning of March 26, 1999, shortly after 7:00 a.m. [20], he uploaded it to Alt.sex (physical), an erotica-focused website, by inserting it in a Word document titled "Passcodes 3-26-99". Newsgroups on Usenet. This was the first instance of a virus spreading via an email that contained a Word document. The Melissa virus looked to be a list of passwords for pornographic websites in the document. It was published using the email skyroket@aol.com, which belonged to Scott Steinmetz of Lynnwood, Washington. [22].

A macro virus that was propagating through email links and attacking MS Word 97 and MS Word 2000 was reported to CERT-CC, located at Pittsburgh's Carnegie Mellon University Pennsylvania, on Friday, March 26, 1999, at around 2:00 PM Eastern Time. The quantity and diversity of reports that were submitted suggested that there was a broad outbreak that affected a wide range of places. This macro infection was known as the Melissa macro or W97M Melissa virus by antivirus software providers [20]. The subject header for the message is frequently reported to be as follows:[23].

"Subject: Important Message From <name>"[23]

"Where <name> is the complete name of the sender of the message"[23].

The main content of the message is of two sections with multiple components. The written text below may be found in the message's first portion (Content Type: text or plain).

"Here is that document you asked for ... don't show anyone else ;-)" [13]

It was previously said that the next part (Content Type: application or MSword) was a file named "list.doc." We can come across papers with different names as the macro infection spreads. The Melissa virus may occasionally create attachments that contain files which the victim created. [23]. Whenever a client accesses an infected document or file in MS Word 97 or 2000 with macros enabled, the virus is instantly activated. [23]. When a document is accessed in the future, the first thing the virus does is to reduce the security settings for macros to allow all of them to be executed. As a result, the user will not be informed the next time the virus is run [23].

Next, the macro verifies whether the key of the registry: -

"HKEY_Current_User\Software\Microsoft\Office\Melissa?"

has its value set as **"... by Kwyjibo"** If the key does not contain the value or is non-existent, the virus spreads itself. **"... by Kwyjibo"**, in such an instance, with the above-described message structure, it emails the first 50 addresses from each Outlook address book that the user running the macro may access. The message or text will be sent to everyone on their mailing lists. Microsoft Outlook must be installed on the afflicted PC for the virus to spread properly, although Outlook need not be the mail client used to view the message [23]. Melissa would infect the Normal.dot template in both Word97 and Word2000, therefore infecting every document written by the victim, which would then send itself to 50 email addresses, putting sensitive or confidential information at risk [23]. Word97 versions that haven't been fixed may trust macros in template files, which might permit the virus to run without being detected [23].

If an infected document was opened when the hour's minute matched the day of the month after Melissa had infected the Normal.dot template, the macro would insert a passage from an episode of The Simpsons: "*Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here*." in this document [22]. All allusions to "The Simpsons," a well-known animated television series, may be found in this text as well as the virus's creator's pseudonym name, **"... by Kwyjibo"[24]**.

Note that Word97 and Word2000 do not display the macro when you open a document which is already infected with macros disabled and the document's macros list is also

checked. The code is VBA code that is connected to the "document.open" approach. Open the Visual Basic editor to view the code. [24].

Email propagation posed a danger to organizational security and the sensitive data of many businesses since it could seriously jeopardize that [20]. Many organizations experienced denial of service issues because of the widespread email duplication's high bandwidth usage during delivery. However, you will be protected against email-based propagation but remain vulnerable to file transfers of corrupt Word documents if you didn't use Microsoft Outlook as your email client [20]. Melissa was known to several sites on March 26 which was a Friday and to others throughout the weekend and to yet some more on 29 March 1999, which was a Monday. They found Monday to be a difficult day for them. But on the 26th of March, CERT-CC already wrote and published a superb study of the virus, including steps for identifying and containing it at the host level. Many large corporations, including Microsoft and Intel, reported intrusions on Friday, according to anti-virus provider Data Fellows. Microsoft had to shut down its email system to stop the virus from propagating internally and globally. Thousands of systems located across hundreds of sites were reportedly impacted, according to reports. Even though the virus received a lot of media attention, it did not deliberately harm systems or data [20].

Implication of the attack

The Melissa virus has shown the huge challenge the government faces in protecting its sensitive data and information technology resources, despite claims that critical government data was not compromised or system impaired [21].

The first thing Melissa did was demonstrate how rapidly viruses may spread owing to the complex and vast interconnection of today's networks; within a few days after the release of the virus, this brought about several reports of infection all around the nation. Even worse, when the virus spread throughout the Internet, versions emerged that could evade security programs built to catch Melissa. Launching countermeasures against the virus was quite challenging just because of these two variables[21].

Second, this virus may indirectly cause mail servers to experience a denial of service. The spread of this malware has caused performance issues with mail servers at several big websites [23].

Thirdly, Melissa showed how challenging it can be to determine a virus's point of origin. The writer known as "VicodinES" was first believed to have created Melissa and was spreading it from an America Online account under the username "Sky Roket." Investigators eventually learned, that the account was taken by the suspect who was detained for generating the malware after getting a tip from America Online. Without this amount of collaboration, it's possible that the culprit wouldn't have ever been found [21].

Fourth, Melissa showed that there are no efficient agency- or government-wide procedures for documenting and evaluating the results of computer intrusions. The Department of Defense and DOE only have incomplete information and there isn't a comprehensive list of the agencies that were affected. Furthermore, there are currently no statistics that can be used to estimate the impact of the attack, such as productivity losses or the cost of lost data

Finally, Melissa demonstrated that when people are made aware of threats and the hazards involved with using computers, they can effectively secure their systems. According to media reports, businesses that informed and prepared their staff for the attacks performed significantly better compared to the others that didn't. [21].

Recommendation

To deactivate Microsoft Word macros, advise users at your website. All your users should be made aware of the problem and urged to disable word macros. This is because this type of vulnerability is not restricted to only Microsoft Word, clients need to be instructed to deactivate macros in any product that supports macro languages [23].

Computer associates like Sophos, McAfee/Network Associates, Symantec, and Trend Micro can be used [23].

At the mail transfer agents that are being used or another central point of control, filter communications that have the virus' signature. This can be achieved with the use of: -

With Sendmail - Information about setting send mail to screen out communications that could contain the Melissa virus was contributed by Nick Christenson of sendmail.com. The following URL will take you to the relevant information:http://www.sendmail.com/blockmelissa.html [23].

Also putting virus scanners to use. Most virus-scanning programs can identify and remove macro viruses. For identifying and getting rid of current malware, you must keep your vulnerability scanners updated with the most recent configuration files. [23].

a. Case analysis and investigation

The Email connection

An international manhunt began to identify Melissa Virus's developer.

The original List.doc newsgroup message was uploaded using the email address "skyroket@aol.com.". After obtaining a court order, the FBI asked America Online for information about the person who uses the email address "skyroket@aol.com". They were able to learn that the owner of this email address was a man with grayish brown hair

named Scott Steinmetz. His email account, "skyroket@aol.com," was hacked to post the virus. The same email account was associated with a website where virus writers posted their harmful code, according to the FBI's investigators. Everyone believed Scott Steinmetz was the one who had written the virus, this is because the origin of the contaminated mail was first posted by his email: skyroket@aol.com. Scott Steinmetz was able to convince AOL that he is innocent, which initiated a search or investigation to find the author of the message. The investigators were able to trace the website back to a web host at Access Orlando, a small ISP in Florida. The web server hosted "Source of Kaos," a group of dubious websites loaded with harmful code[25].

The web server is not owned by Access Orlando; rather, its owner, Roger Sibert, rents space from the company for $150 a month [26].

To preserve any evidence of Melissa's origin that Roger's server logs might provide, the FBI approached Access Orlando to take down Roger Sibert's server, and then went on to seize his computer or server for a thorough examination of its logs [25].

The owner of the Source of Kaos sites, Sibert, claimed that he did not know who created the Melissa Virus, that he permits individuals with unconventional viewpoints to host websites on his Web server, and that many of the about 80 sites belonged to the virus writers or virus collectors. The FBI refused to comment on Access Orlando [26].

Melissa's Mystery

There were speculations that Mr. Smith was VicodinES, the Internet moniker of a hacker who had written similar viruses in the past after numerous independent security experts conducted their private investigations.

Fredrik Bjorck, a Swedish Ph.D. researcher at the Computer Science Department of Stockholm University, and Richard Smith, who is the CEO of application tools producers Phar Lap Software Incorporated on the 29th of March 1999 found the person they thought was Melissa's author on a website run by a virus writer. They were able to discover that the MS Global User Identification (GUID) of the file uploaded to the newsgroup and with the Melissa virus contained in the document was identical to the GUID present in a different virus, called PSD2000.doc. This virus PSD2000.doc was discovered on the website of a virus creator known as VicodinES at "http://www.sourceofkaos.com/homes/vic/start.html".

VicodinES has acknowledged in writing that the virus PSD2000.doc was written based on the "Shiver" virus, created by ALT-F11, another virus creator. A comparison of the "Shiver" virus's GUID with other malware revealed that it also matched Melissa's encoded GUID. A "Groovie2", another virus produced by ALT-F11, was also discovered to have identical GUIDs. Analyzing the additional MS Word macros the author VicodinES showed that PSD2000.doc has a distinctive GUID, every other document that VicodinES claims to have created had different GUID. However, this GUID is said not to be a foolproof way to identify a document's creator. The first time a Microsoft Office document is produced, the GUID is stored in that document. Whether a document is copied or moved to a different device and saved with a different name, the initial GUID number remains constant. Many programmers base their initial development of new programs on portions of existing programs' core code rather than starting from scratch. The same is true of viruses. Additionally, the MAC address of the network card utilized in creating the GUID was not taken from the hardware of the network card directly. It is retrieved via the operating system's software driver. Most of the time, it is derived from the hardware's MAC address, although it can also be modified in the registry of the system, allowing you to set up numerous computer systems to create files or documents with identical GUID. As a result, despite being good and helping with identification, the GUID matching effort was not "the nail in the coffin" as different people claimed [20].

Additionally, on that day Richard Smith gave the FBI the identities of those who had altered the virus, this included the suspect, David L. Smith. State officials, however, asserted that Smith is not VicodinES, despite their vague suggestion that he might have benefited from the hacker's expertise or knowledge [27].

The Monmouth ISP Connection

Richard Smith's suspicion that skyroket@aol.com had been hacked was then validated by AOL. On its servers, AOL "tags" newsgroup postings, including messages uploaded on alt.sex with details on the account that this post originated as well as details or information about the message itself and the application utilized to publish the message. AOL backtracking to a listserver and IP address 209.191.60.64 that related to Monmouth Internet, a New Jersey-based Internet Service Provider, which had been used to publish the original message. This was possible using the original infected file which contained information about the email server and the tag on the post. [20].

A communications warrant was delivered by state police to Monmouth Internet about the IP address 209.191.60.64. When a user connects, Monmouth Internet is one of those internet service providers that gives them a fresh, randomly assigned IP address, granting them a certain amount of anonymity [25].

The names of 12 of its clients who used that IP address on March 26, when the Melissa virus was originally released, to send and receive data to the Internet were made available to the New Jersey investigators. David L. Smith was one of the clients [28].

Within 72 hours, the high-tech computer crime unit of the State Police of New Jersey and the FBI's technology experts were able to link the evidence to a phone number and home address [29].

The Arrest

Detectives from the New Jersey Prosecutor's Office, FBI agents, and the Technology Crime Division of the State Police showed up at the house of David L. Smith in Aberdeen Township on the 1st of April with a search warrant but couldn't find anyone there. Officers examining his flat discovered that the CPUs from two computers were missing. The remainder of the computer parts which includes floppy discs, power cables, different monitor, monitor cables, and

writeable CD-ROMs were seized by police. The fact that the equipment was in the apartment and on a table suggested that it was utilized alongside the processing units [30]. They questioned residents in the area, who characterized him as a typical computer fanatic and a quiet neighbor who rarely left his flat. They added that he had a brother who lived nearby.

Three hours later, authorities in nearby Eatontown found David Smith at his brother's house and detained him. Following this, David Smith was accused of interfering with official communications, conspiring to commit the crime, attempting to do so, and third-degree computer service theft. At the time of his arrest, David L. Smith was working as a software developer for an organization that developed applications for a company named AT&T. The company's identity was not made public [28].
During the time David Smith was arrested, he relinquished his Miranda rights, which are a suspect's right to remain silent when being questioned. He also confessed to creating and disseminating the Melissa virus, using the hacked email address skyroket@aol.com, without authorization to upload it to the Internet, and erasing the laptop he used to create and upload the virus [20].

Evidence

- The email address of *Scott Steinmetz,* which was initially used to upload the virus, skyrocket@aol.com
- The web server owned by Roger Sibert was seized by the FBI.
- The IP address (209.191.60.64) was given to the FBI by AOL.
- Seized items from *David L. Smith's* apartment which included, floppy discs, writeable CD-ROMs, monitors, and power connections.

The Aftermath

On December 9th, 1999, David L. Smith pleaded guilty to a federal charge of disseminating the virus and a second-degree offense of computer theft. After which, he was granted bail. David Smith assumed a phony persona and started assisting the FBI in locating and contacting more targets of investigations into computer crimes. He assisted the FBI in gathering further data that allowed for the capture of Simon Vallor, the inventor of three viruses, and Jan de Wit, the Dutchman who created the Anna Kournikova virus [25].

Court Proceedings

United States of America v. David L. Smith

EDWARD F. BORDEN, JR. defended the defendant, DAVID SMITH.

On 12-9-99, the defendant entered a plea of guilty to count (1) of the information. In light of this, this court has determined that the accused has committed the following crime(s):

Title 18: US Code Section 1030(a)(5)(A) and 2

Nature of Crime committed: Fraud and related activity in connection to computers.

Date Crime was Committed: 26th March 1999.

According to the Conviction Reform Act of 1984, the sentence was given as of 1st May 2002.

The defendant is required to immediately pay the US a special assessment of $100 for count (1) of the complaint. This special assessment must be paid by the District Court Clerk of the United States.

It is further stipulated that up until all penalties, compensations, costs, and special assessments given by this judge are paid in full, the accused must give notice to the United States Attorney for this district within 30 days of any change in name and place of residence. Any significant change in the defendant's financial situation, if they are required to make restitution, must be communicated to the court and the US Attorney.

This agreement was signed on May 3, 2002, by Joseph A. Greenaway Jr. (Judge of the United States) [31].

Imprisonment

The offender is hereby convicted to serve a 20-month term in the Federal Bureau of Prisons [31].

The offender must present themselves for sentence serving in the facility specified by the Federal Bureau of Prisons of the United States.

Supervised Release

The defendant will spend three years under supervision after being released from prison [31]. The following standard requirements must be followed when the defendant is under supervision:

- Following the start of supervised release, the offender must perform a drug test within the period of 15 days after release and at least two more tests which will be decided by the probation supervisor.
- In 72 hours of being released from the Federal Bureau of Prisons, the prisoner must appear in person at the probation office in the district where they were released.
- It is a requirement during supervision after release that the offender pays any fines, special assessments, expenses, or restitution obligations that are still owed after the term of supervised release has started [31].
- From the time probation is granted, the offender must complete 100 hours of community service

over 36 months or less. The exact work placement must receive the U.S. Probation Officer's approval before performing such service, which shall be performed without payment. The Court will advise that the community service be carried out in the field of technology.

- Unless specifically permitted by the Probation Officer or supervisor, the defendant is not permitted to own, obtain, buy, or gain access to any type of computer network, bulletin board, Internet service, or exchange that will involve computers. The Court will decide whether this condition is applicable in any disputed situations[31].
- Upon request by the Probation supervisor, the offender shall submit complete disclosure of his financial data, including annual income tax returns. The offender is required to cooperate with the probation officer in their inquiry of the defendant's financial activities and to give accurate monthly income statements.
- If the U.S. Probation Office so requests, the defendant must take part in a mental health evaluation and treatment program. The criminal must stay in treatment up until he or she is successfully released and with the U.S. Probation Officer's approval [31].

Standard condition of supervision

If the defendant is under supervised release as a result of this judgment:

- During the period of supervision, the offender shall not commit any more crimes at the federal, state, or municipal levels.
- It is forbidden for the defendant to illegally possess any controlled substances.
- The offender shall not possess a firearm or other harmful device if found guilty of a felony offense [31].
- The defendant is not permitted to leave the court's jurisdiction district without the judge's or the probation officer's approval.
- In the first five days of every month, the offender must make a true and comprehensive written report to their probation supervisor which will be instructed by the court or probation supervisor or officer.
- The offender must respond truthfully to all the questions or inquiries made by the probation officer and adhere to his/her directives.
- The offender is responsible for providing for their dependents and taking care of other family obligations [31].
- The offender must routinely perform a legal job unless the probation officer grants an exception for schooling, training, or another justifiable cause.
- If there is a change in residence or employment, the defendant must report to the probation supervisor in 72 hours.
- The offender must abstain from much use of alcohol and must not acquire, consume or distribute any narcotics or other restricted substances, or any of the accessories associated with them.
- The defendant must avoid going to locations where illegally obtained controlled substances are sold, consumed, distributed, or administered [31].
- Without the probation officer's consent, the offender is not allowed to identify with any individuals involved in any criminal activity or those who have been convicted of a felony.
- The offender must consent to visits from a probation officer whenever, whether at home or abroad, and must allow the probation supervisor to seize contrabands they see in plain sight.
- Within 72 hours after being detained or questioned by the police or law enforcement, the offender must inform the probation officer.
- Without the judge's approval, the defendant is not permitted to sign a contract to serve as an informant of a law enforcement organization.
- The defendant must notify third parties of risks as instructed by the probation supervisor or officer, and they must allow the officer to notify them and verify that the defendant complied with the requirement to notify them. These risks may be brought on by the defendant's criminal history, personal history, or other characteristics [31].

Fine

The offender must pay a $5,000 fine. The penalty is due immediately. It is advised that the defendant should take part in the Inmate Financial Responsibility Program of the Federal Bureau of Prisons. If the entire fine is not paid before the start of monitoring or supervision, the offender must pay the balance throughout the supervised release in at least equal monthly payments[31].

If the payment is not paid, the defendant could get any possible punishment that was initially given by the court. Title 18: US Code Section 3614 is cited as “Resentencing upon failure to pay a fine or restitution”.

The following payments must be made in that order: assessments, restitution principal, restitution interest, fine principal, community restitution principal, fine interest, penalties, and costs, which include attorney fees and court costs [31].

IV. Case study - 3

A. Literature Review

From November 27th to December 18th, 2013, a US retail company ‘Target Corporation’ had its network

infiltrated. The attackers gained access to 40 million credit and debit card information as well as 70 million personal identifiable information (PII) records after which they transferred all the data to servers in Eastern Europe and proceeded to erase it from Target's network. Following the attacks on Heartland Payment Systems (2009), and TJX (2007), this was the third largest credit and debit card compromise in history [32] [33]. Reissuing of cards alone after this event cost credit card unions more than $200 million by February 2014; due to other "bank reimbursement demands, regulatory fines, and direct customer service costs", the cost was driven up to $291 million [34].

Cost of the Attack

The attack against Target had huge cost implications for the organization. We classify the costs into two main categories; direct and indirect.

a. Direct Costs

1. System investment: Target invested heavily in and implemented chip-enabled technology in stores and on Target REDcards by 2015, which was half a year earlier than planned [43].
2. Replacement of its branded credit and debit Redcards as well as setting up new payment terminals. These costs along with the roll-out of chip technology cost Target $100 million.
3. Employee security awareness training: Target hired a security specialist from Verizon a few days after the hack was announced.

b. Indirect Costs

1. Loss of partnerships/suppliers [44]
   - The attack extended the turnaround time because of the volume of requests for card reissuance. Due to the enormous volume of cards they had to make, card vendors reportedly fell behind for weeks. One bank faced delays of up to three months for cards to be replaced, and about two months for normally expiring cards unrelated to the attack.
   - Impact on bank customers [44]: Customers reported that the Target attack caused cardholders significant inconveniences throughout the hectic holiday shopping season. It was a major nuisance for many bank clients who no longer use checks and only had debit cards [44].
   - Impact on bank revenue [44]: Several employees reported losses in spend and revenue from reissued portfolios and accounts lost due to inactive cards. There was also a loss of revenue attributed to legitimate declines in point-of-sale transactions due to heightened fraud strategies [44].
   - Impact on bank operations: The intrusion significantly interfered with the daily tasks performed by bank staff [44].
   - Additional costs to the bank: The survey participants also mentioned costs associated with inbound and outbound phone calls, fraud monitoring, claims processing, and responding to customer inquiries in addition to reissuing cards [44].
2. Legal penalties
   - Target paid $67 million to Visa and $39.4 million to Mastercard and affiliated banks and credit unions.
3. Loss of customers
   - In 2013, Target was ranked 7th best-perceived brand among consumers, but by 2014 it had dropped out of the top 10 to being ranked as 21st.
   - Many customers either halted use of or canceled their credit cards.

4. Damage to corporate reputation and stock value declination [44]
   - Target's Corporate Social Responsibility score, fell sharply from 2011 and had the greatest decline of any U.S. retail company within that period [42].
   - As of February 1st 2014, Target had already spent more than $61 million defending against the attack and was facing over 90 lawsuits relating to the significant data breach [45].
   - Following the security breach, Target's stock price dropped by 10%.

Collateral damage that impacted Target's subsequent prospects.

B. Attack Implementation

Detection of the Attack

In May 2013, some months prior to the incident, Target installed 'FireEye', a recognised and reliable anti-malware and intrusion detection system. However, the security administrators were unfamiliar with the FireEye technology, and so left some preventative features disabled. Hence, the early detection of the hack was overlooked by Target and numerous virus warnings were unfortunately disregarded [35].
Target's first breach occurred with a third party, Fazio Mechanical Services, an AC, and heating company. An employee who clicked on an attachment in a phishing email downloaded the Trojan horse called Citadel that established itself on Fazio's machines. Due to Fazio's poor security, the Trojan gave the attackers full control over their network which allowed access to Target's network [35].

Target's network was poorly segmented, hence by accessing Target's business segment, the attackers gained access to Target's complete network. They then conducted a probe of the network to identify vulnerabilities which were taken advantage of to access confidential data. Other vulnerabilities were used as the conduit for data exfiltration from Target. As soon as they escalated their access to Target's entire network, they installed BlackPOS malware on point-of-sale (PoS) machines.

First, BlackPOS went unnoticed, and it started gathering millions of records during busy business hours. The hackers' base of operations in Eastern Europe was waiting to receive this material. FireEye quickly identified the malware, though, and sent out an alert. The Minneapolis security center was contacted by the Target security team in

Bangalore after they took note of the alarm. However, Target's security ignored the red light.

Up to five distinct variants of the malware were detected by FireEye. Due to a mistake made by the infiltrators, the malware program comprised the login credentials as well as the addresses for the "staging ground" servers, which would have allowed Target security to log in and view the stolen data for themselves. The warnings made by FireEye were all ignored. The identical server that FireEye had identified as conducting malicious activity was also identified by Symantec - Target's antivirus software around November 28. Furthermore, FireEye's automated malware deletion function might have put a halt to the attack without the need for human intervention given that many notifications were sent out before any data was deleted from Target's systems. However, Target's security team disabled the function, in favour of manually reviewing all security-related verdicts. [36].

On December 2, 2013, as FireEye's alerts were triggered, the hackers started relocating the stolen data. For approximately two weeks, the malware freely exfiltrated data. In addition to complaints of unauthorized credit card purchases, Target was notified about the breach on December 12 after the Department of Justice recovered the stolen data from the servers they were sent to, which the attackers had not erased [34].

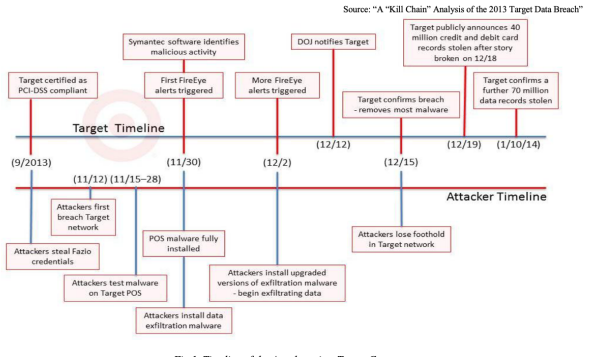


Fig. 3. The timeline of the attack.

Technical details of the attack

The attack had 5 main phases namely.

1. *Initial Infection:* Target's first breach occurred with a third party, Fazio Mechanical Services, an AC and heating company. An employee who clicked on an attachment in a phishing email downloaded the Trojan horse called Citadel that established itself on Fazio's machines. Due to Fazio's poor security, the Trojan horse granted the hackers full control of their network which allowed access to Target's network [35]. To process electronic billing, submit contracts, and manage projects, Fazio Mechanical relied on Ariba - Target's network [6]. Target's network was poorly segmented, hence, just by gaining access to that business segment, the intruders acquired access to Target's complete network. The intruders obtained access to Target's internal network for the first time on November 12 [38].
2. *PoS Infection:* Upon accessing Target's business segment, the intruders gained access to Target's complete network. They then conducted a probe of the network to identify vulnerabilities which were taken advantage of to access confidential data. Other vulnerabilities were used as the conduit for data exfiltration from Target. They installed a point-of-sale malware called BlackPOS onto the PoS machines once they acquired access to Target's network. Unnamed investigators claim that between November 15 and November 28, the attackers compromised a limited number of POS terminals with malware before spreading to the remainder of the Target-owned POS systems by November 30 [39].

Workings of BlackPOS

BlackPOS is a malware commonly termed "memory scraper" that grabs some of the memory from a system and scans it for credit card data.
POS machines at Target were infected with a customized version of the "BlackPOS" malware, which can be purchased for between $1,800 and $2,300 on underground cybercrime forums [40].
BlackPOS is made to infect POS devices running on Windows operating systems. Fig. 2. presents the BlacksPOS's components and functionalities.
The malware that infects POS terminals registers as the "POSWDS" Windows service. After the service has been launched, it scans the list of programs that might interface with the card reader and uploads the credit card information it has retrieved to a compromised server (internal network depository). Credit card numbers are compared against sensitive procedures and verified according to predefined criteria before being sent. The depository aggregation function is only activated, and card data submitted to the internal network depository during the busiest business hours of the day.

The target processes' memory is read and examined in 10,000,000-byte chunks. BlackPOS searches credit card numbers stored in memory trunks using proprietary logic. This approach is thought to be more cost-effective and efficient than regular expressions in general [41]. Credit card numbers that have been obtained will be encrypted, saved in the file "C:nWINDOWSnsystem 32nwinxml.dll,". SMB and NetBIOS protocols are then used to upload the files to the internal depository intermittently.

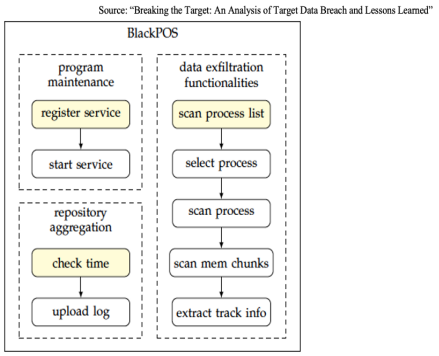


Fig. 4.Detection Evasion Mechanisms of BlackPOS

The following design features of BlackPOS increased the difficulty of its detection once it was active in Target's network.

a. Multi-phase extraction: Sensitive information is not directly sent to the external network by infected POS terminals. Rather, information is sent to a compromised internal server depository that is utilized as a relay between the target and external network [42]. This system reduces abnormal data flow across networks.
b. String obfuscation [35]: To avoid signature-based antivirus detection, crucial strings in malware executables are obfuscated. There are strings that contain important information about scanning and NetBIOS commands for transferring records to the internal depository.
c. Self-destructive code [35]: To reduce its exposure, the malware avoids infections that are not essential. In the case where the contaminated environment is not an intended target, it destroys or deletes itself. This decreases the likelihood of detection in unknown environments.
d. Data encryption [35]: Before being submitted to the internal depository, the received credit card data is encrypted in the "Winxml.dll" file at every POS terminal. Conventional data loss prevention (DLP) systems are unable to detect the breach since encryption ensures that credit card numbers are not delivered in cleartext.
e. Constrained communication: Internal network's communications are scheduled to occur during business hours [41]. It is possible to conceal unusual exchanges between the exploited internal depository and infected POS terminals by using heavy office hour traffic terminals and compromising the internal depository.
f. Customized attack mechanism: The malware includes hardcoded internal IP addresses and login information for infected servers. It suggests that the creator of the infection understands the internal network. The creator intentionally developed the countermeasures against detections alongside the data exfiltration process.

3. *Data collection* [35]: Upon the setup, testing, and update of BlackPOS, it began to scan the PoS's memory for card numbers and other track information from cards scanned by PoS card readers.

4. *Data exfiltration* [35]*:* The debit & credit card numbers were concealed using encryption, then sent from the PoS devices to the compromised internal depositories. Attackers deliberately chose the backdoor usernames "Best1 user" & "BackupU$r," which are generated typically by IT management program "*Performance Assurance for Microsoft Servers"*, to access 3 of Target's internal FTP servers at the time of intrusion. The malware on the PoS devices would send large amounts of card data to the nearby FTP Server at busy hours of the day. The infected machines subsequently passed along the stolen card information to collection sites in Miami and Brazil.

5. *Monetization* [34]*:* According to numerous reports, the stolen credit card data which amounted to 11Gb, was collected at a server in Russia between November to December 2013. This credit card data was found for sale on black-market scenes.

Fig. 3. Below shows an illustration of the attack phases.

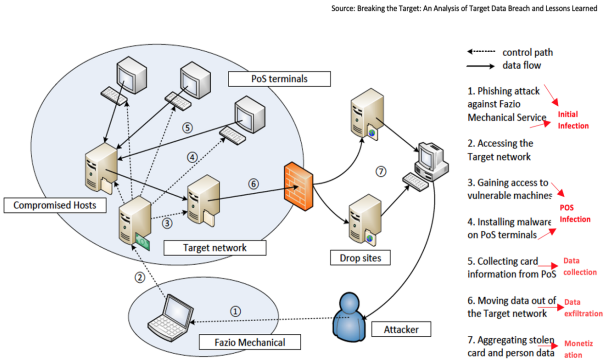


Fig. 5. Analysis of Target Data Breach

Investigation

When the breach happened, Target hired some cybercrime investigators at Verizon so that they could help identify the factors that were responsible for this breach. A security inspection was executed thoroughly from Dec 21. 2013 to Mar 1, 2014. The main goals of this were first to figure out what was the main reason behind this breach and second that what ways could be there so that the Target's security is enhanced for no further attacks. The report from Verizon is restricted but there had been several reports from some media that they got some data from the actual report itself. These reports are not confirmed but they are presented by reliable security investigators and media. The foremost entry that happened was from hijacked credentials snuck out of Fazio Mechanical Services which is an intermediary service supplier. The owner of that company tied a partnership with Target to expand his business across the United States. Thus, he had access to target's services such as e-billing system, Submit a contract and project management. A cyber-attack operation was performed on his company in 2013 fall since he didn't perform any remote monitoring on his refrigeration systems for target. The infection emerged from an infection of Citadel malware that is useful in sneaking out of the login details from the computer devices. Although Fazio claimed industrial best practices were considered, it's suspected that Fazio was relying on zero cost and non-commercial version of an anti-virus software called Malwarebytes which has zero protection in real time. It is assumed that Target did not comply with best security measures while doing business with its vendors. Since there was no sudden effect on Fazio Company, it is assumed that data was stolen to gain access to Target's systems while the breach was happening at Fazio. But this access did not allow the attackers to get all customers' data. There must be other vulnerabilities inside the target's systems which led to stealing of 40 million credit information. One of the problems was there was no barrier to retrieve point of sales (pos) areas once it is inside the network. This way it is easier for an attacker to pass through a network and retrieve devices from pos areas to the backend of the system. To show how it was done, the Verizon team accessed some cash registers when they played a little with the deli counter scale present in other stores. Investigation found some issues with password guidelines being enforced by the company. This guideline had some industry standard appeals.

There was some login information stored on its servers. During the inspection, it was found out that misconfigured services were being utilized like MS SQL servers having weak admin pass, Apache Tomcat servers using default pass. This way the team was successful in retrieving corporate n/w access and thus gaining admin access at the end. Target was using weak passwords on a large basis such that investigators gained 500k passwords that belong to 86 percent of accounts and some of the target systems. There were problems with maintenance and repairing parts of systems. Just for Instance, MS patches were nowhere to be found, out of date software like Apache, IBM WebSphere and PHP. All of these were running on the web servers, DB and its setup frame. Since these were outdated, it was easier to crack the systems without even knowing the credentials. The Verizon and Target Red Team exploited the vulnerabilities, and the result was gaining access to the n/w and all the important information via domain admin account [5].

Category of Crime/ Associated Laws

1. The federal Computer Fraud and Abuse Act (CFAA): With this, the computers that come under federal concern like bank computers, computers exploited for regional or overseas trade are safeguarded. This means there should be no invasion, extortions, destruction or even spying on such devices. It has come into effect after the remake, reform, and alteration in many other ways by Congress to strengthen the act made for above reasons. It has constructed more rigid rules so that the following is prohibited:

- Intentionally, gaining access to a device with no authorization, to gather constrained govt. information.
- Accessing government devices and misusing the same.
- Harming the bills and thus exchanging the information purposely.
- Retrieving some valued data to cause fraud.
- Forming traffic in the guarded device.
- Blackmailing or threatening to harm the device.
- Doing the same as above just for more other authorities like:
    - Banks
    - Federal govt
    - Safeguarded device

In the Target breach, some of the laws relating to theft and misuse of wires are also included. Additionally, there are some laws which forbid the transactions of credit cards and identity theft.
Moreover, this breach is coming under the CFAA, gaining unauthorized access to a computer involved in overseas trade producing a loss of more than $5000. Thus, the person could get up to 5 to 10 years of prison adding up with up to $250k damages per crime. It criticizes any overseas information exchange that could lead up to a fraudulent act. [46]

Characters

1. **Ruslan Bondars** who is a citizen of Latvia held responsible for building a code (called Scan4You) which was proven to be helpful for the hackers to improve malware- which was utilized in this data breach. [47]
2. **Andrey Hodirevski:** He is another suspect from Ukraine. He is known to authorities because of prior card stings. He is a part of at least one of the sites called “Rescator” that sells stolen card information. Although police had already identified this site and tons of similar other sites, the criminals built another protection program such that they can know any undercover law enforcement trying to purchase data. There is no public record found for this person held responsible for the large malware attack.[48]
3. **Daniel Dominguez Guardiola and Mary Carmen Vaquera:** They are a couple from Mexico, aged about 28 and 27 years old respectively. They were traveling to the US when they were taken into custody by the customs and border police. The authorities found out that they were traveling with about 90 fraudulent cards. They accepted the fact that they spent around 35k+ shopping in McAllen with those cards which they thought would sell in Mexico to earn more profit.[49]

C. Court Proceedings

The Trial and the Sentence

There were so many things involved in the trial for the target breach 2013. We would be discussing them as we move on this report. The government was not able to pinpoint the hackers involved exactly and there are still so many investigations going on today with the help of many private investigation companies and the Federal Bureau Investigation **(FBI)** [51]. To track down cybercriminals is not easy at all as there are a lot of technical things involved and there are not so many trained people for investigations.
The below trials would be discussed according to reports made to the public. [52]

The Hacker Linked to the Target Breach 2013

- There was a case between the hacker linked to the Target breach in 2013 and the government because there was evidence that proved that he was guilty.
- The hacker in question was a **37-year-old Latvian citizen**. He was found guilty by a federal court named Alexandria court and there was proof that he worked with the Latvian government [53].

- The hacker Ruslan Bonders was a famous computer programmer who designed the "Scan 4You program to discover if intelligent anti-virus software designed by companies would identify their malicious software. There was proof that he also packaged the software as malware kits to be sold out to other cybercriminals.
- In the federal court, Bonders bluntly argued that this "Scan4You" program waw used for only legal purposes and he was not to be blamed if it was used illegally by cybercriminals.
- The defense attorney, Jessica Carmichael argued as part of her claims that anything invented or innovated today are both used illegally and legally. Therefore, the defendant should not be blamed and found guilty of certain use cases of the "scan4You" program.
- Interestingly, the judge of the case, Judge Liam O'Grady replied to the attorney Jessica and told Bonders that it is almost impossible that he was not aware the perpetrators were using his software to break into the defenses of companies, especially Target in question [53].
- Several prosecutors came together and commented that for someone to invent a software, he knows the ins and outs. This includes the technical products of the software. Therefore, the law permits that they are charged because they know when it's been used for good and to commit crimes. There was no case that Bonders reported the incident, so we could conclude that he was involved in the breach.
- The Assistant U.S attorney at the time, Kellen Dwyer also came out to give a statement that Ruslan Bonders should not think this is the first time someone is charged for creating a software that was used to breach the defenses of an organization.
- Ruslan Bonders' co-conspirator, Taylor Huddleston was one of the witnesses who testified against Bonders and claimed that he was part of the crime. Also, Taylor was prosecuted for creating a software that was used illegally and he made the same arguments as Bonders.
- Bonders in conclusion made a statement that he is very ashamed that his software was used for the illegal things he was charged.
- Bonders as the defendant argued that his software was not used in the Target breach to steal credentials of 110 million users. He also argued that he should not be blamed because target's intrusion prevention system saw the malware in their system, and they clearly ignored it.[53]
- An Investigation expert from Verizon concluded that a file of "Scan4You" assisted in determining where the payment information was stored in Target.
- At the time, Target demanded restitution from Bonders for an amount not decided because they spent a lot in trying to regain customer trust.
- The trial was a Judge only trial and did not involve the Jury in Alexandria Federal court

- After hearing all concluding statements from the prosecutor and defendant in a 5-day trial, Judge O'Brian found Ruslan Bonders guilty and sentenced him to **14 years in prison.** [53]

People of the State of California against Target Corporation

For this case, the below are taking into considerations for the parties and Jurisdictions

- The case was tried in the Superior court of California for the people of San Francisco
- The People of the state of California would be the Plaintiff.
- Xavier Becerra being the Attorney General of the State of California and he has Yen P. Nguyen as the Deputy Attorney General of the state of California [60]
- Target Co-corporation would be the defendant
- The defense Attorney for this case is Nathan D. Taylor of Morrison & Foerster LLP.
- The Judgment for this case against Target would be subject to California Code section 17200 eq
- The Supreme court would have jurisdiction over all parties involved and can come to a decision not limited to San Francisco [60]

The Supreme court of California through the Judge, **Harold Khan** passed the following to Target

I. Target in connection with its collection and maintenance must comply with the unfair competition Law.

II. Target must be honest on how customer information is protected

III. Target must comply going forward with the Data Breach Law

IV. Target must come up with an Information security program to protect customers within the 180 days after the effective date of judgment.

V. Target must not only come up with the information security program, but it must be written to include technical, physical, and administrative controls

VI. Target must ensure that these controls include proper segmentation, whitelisting, complying with PCIDSS, risk-based penetration testing methods, file integrity monitoring, proper logging and monitoring, proper change management [61].

VII. Target must hire an expert responsible to implement the Information security program and to advice the Chief Information officer very critically

VIII. Target shall ensure that the Information security program meets the standards of the judgment.

IX. Target must ensure that all third-party companies are accessed by a professional who is a certified information systems security professional or a certified Information systems auditor.

X. Target must ensure that the accessed third-party report is provided to the Connecticut Attorney General's office within 180 days of completing the report [60]

XI. Upon request, the Connecticut Attorney general may provide to the California Attorney General upon request and this must never be disclosed according to public records laws

The Fine

According to the Assurances of Voluntary Compliance **(AVC),** with the Attorneys General of other states also involving identical allegations, Target must pay a total sum of $18,500,000 to the states. Target must pay a portion of it to the California Attorney general within 30 days.

II. The payment must be used by the states to fund the investigation and the enforcement of the California General consumer protection laws. [63]

The Release Statement

I**.** Target shall be released and discharged by the attorney general from all civil claims that the California Attorney General did not bring under the Competition law, the data breach law, the security law related to the intrusion

II. All obligations made to TARGET shall expire 5 years after the judgment was made. However, this does not exclude TARGET from complying with federal and state laws. [64]

The Trial Conclusions

i. After the Judgment, the California Attorney General has the right to demand a written notice if TARGET fails to comply with all obligations
ii. The California Attorney General must protect the interests of the California people
iii. TARGET must comply to all federal laws, regulations, and rules.[61]
iv. TARGET shall deliver a copy of the judgements to the new Chief Information officer, Chief Executive officer, Chief Information security officer and all board of directors within 90 days.
v. TARGET must not leave out any costs associated with the filing of the judgment [60]
vi. TARGET must not form a corporation or merge with another with sole purpose of engaging in activities to escape the judgment
vii. If TARGET does not comply with all laws in this judgment, the California Attorney General advises that a notice is satisfied by Yen P. (TiTi) Nguyen, Deputy Attorney General, Office of the Attorney General, 455 Golden Gate Avenue, Suite 11000, San Francisco, CA 94102-7004
viii. The court retained jurisdiction to ensure that any party at any time can make further orders and directions necessary to carry out the judgment
ix. The Judge, Harold Khan ordered the clerk to enter the Judgment Forthwith. [63]

The Mexican Pair Linked to the Target Breach 2013

- The trial was a judge only case. The Judge was **Ricardo H. Hinojosa**
- The Mexican pair made up of 27-year-old Mary Carmen Vaquera-Garcia and 28-year-old Daniel Dominguez- Guardiola admitted in the U.S District court as advised by the defendant U.S Attorney Kenneth Magidson for possession of 96 TARGET credentials.
- The Mexican pair further admitted that this stolen Target credentials were used to shop online on various websites, so they are not traced [54]
- As part of the plea by the defendant's attorney, the defendants would pay a restitution amount of $35,422.21 and the defendants would also forfeit all properties in their possession.
- The investigations were done by the McAllen Police Department and was prosecuted by U.S attorney Christopher Sally after a proper investigation report was written.
- The U.S Chief District Judge for this case did not overrule the guilty pleas and after the concluding statements by the prosecuting and defending attorney, the defendant was sentenced to 10 years in federal prison and a maximum fine of $250,000. [54]

Recovery Efforts and Lessons Learnt

Lessons Learnt

After the breach, due to harassments, the CEO Gregg Steinhafel resigned his duty as the CEO of the company and TARGET immediately appointed a new chief information officer Bob DeRodes and he gave a statement that TARGET would need 100 million dollars to recover major things lost[7].

The following are part of the notes taken by TARGET as lessons from the sophisticated breach.

1. Paying more attention to always investigate security warnings generated by multiple orchestrated security tools such as FireEye, Symantec, and Fore scout and never to turn off auto-removal malware functionalities
2. Hardening critical point-of -sales terminals to ensure that unauthorized software installation and configurations are not allowed. [58]
3. Applying proper access control mechanisms to ensure that different groups and accounts don't have the same level of privilege especially with third party integrations
4. Proper segmentations must be done to isolate sensitive and critical networks from the general network. Configurations of stronger security methods aside Virtual LAN (VLAN).
5. Implementing proper data storages to keep data for longer periods with top security [56]

Recovery Efforts by Target

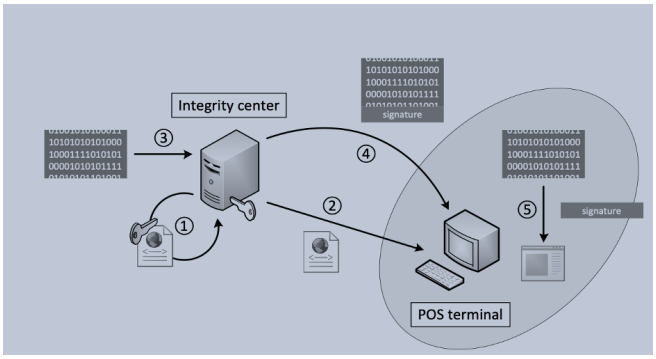
<u>Non-Technical Efforts</u>

- Advising its customers that they are not the ones responsible for the breach and that TARGET would be responsible to compensate them. [55]
- Proper Apology was done to customers to regain trust.
- Increasing communication channels to ensure that customers can reach out to make complains to regain trust.[56]
- Re-employing a new Chief Security Operations officer to implement stronger controls to prevent another breach.
- Improving the website to ensure that it was educative, helpful, and informative. [51]
- Proper investment was done with different cyber security education companies to educate staff.

Technical Efforts

Enforced Payment Security Integrity with POS Terminals

After BlackPOS was fully installed on the POS terminals because of poor security, notes were taken, and a better security was built on the POS terminals by enforcing integrity.[54]
The main purpose of enforcing integrity is to ensure that before software is installed on POS terminals they are properly checked and trusted. For a long time, executable verification techniques such as digital signatures have been used such as Microsoft Authenticode. However, today public key infrastructure **(PKI)** helps to relieve the issue with users having so many service providers that cannot be verified.[55]
There are two players that are very important in ensuring the proper implementation of enforced integrity on POS terminals. They include the integrity **centre** and the **POS terminals** used at the tills. The following is a diagram to explain the steps involved in enforcing integrity.[56]



From the above diagram, the following explains the process

Step 1, a public-private key pair is generated, and self-signed certificate is created by the integration center

Step 2, the certificate created in Step 1 is distributed across to all POS terminals in TARGET and this is placed in the root certificate by the integration center. [57]

Step 3, the binary to be executed on the POS terminal such as programs, patches and installers are audited by the integrity center. After audit is done, the binary is signed

Step 4, The POS terminals at all locations receive the signed binary [58]

Step 5, The POS terminals check the binary and verify with the hash of the binary, if it matches the POS terminals execute.[59]

The above steps are to ensure system integrity and program authenticity.

Developed Effective Security Alert Systems

After TARGET realized that the notifications from the intrusion prevention system, FireEye were turned off by the administrators, TARGET decided to improve the capabilities of the Fire Eye system through two separate designs below.[55]
1. When TARGET administrators do not notice and handle the alerts on time, the severity level of the alerts are increased which forms the Adaptive warning strength of the Intrusion prevention system.[65]
2. Ensuring that all security control solutions are orchestrated to ensure that all stages of any attack are linked and properly followed by the security professionals. A very good approach is to ensure that all malicious alerts are properly analyzed to connect multiple alerts.[60]
FireEye alerts are usually in XML formats as shown below. The type and severity of attack is shown. The malicious alert part tells the administrator that the attack is an anomaly. The class type also shows that the attack is tagged an anomaly. The attack is properly defined and described in the display and msg [61]

<?xml version="1.0" encoding="utf-8"?>
<alerts appliance="192.168.100.1" msg="extended" product="Web MPS" version="6.2.0.74484" xmlns="http://www.fireeye.com/

<alert id="1694305" name="malware-object" severity="majr"><explanation analysis="content" protocol=""><malware-detected
<os name="windows" sp="1" version="6.1.7601"/><os_monitor build="84486" date="Feb 28 2013" time="19:22:47" version="6.3
<uac mode="service"><value>Windows Time</value><status>running</status></uac>
<process mode="started"><value>C:\VoiceMail_Houston_(713)4584939.exe</value><pid>2736</pid><ppid>2696</ppid><parentname
<malicious-alert classtype="anomaly-tag"><msg>A new process has been launched</msg><display-msg>Startup behavior anomal
<uac mode="service"><value>Windows Error Reporting Service</value><status>running</status></uac>
<mutex><value/><processinfo><pid>2736</pid><imagepath>C:\VoiceMail_Houston_(713)4584939.exe</imagepath><md5sum>28401b27
<apicall><processinfo><pid>2736</pid><imagepath>C:\VoiceMail_Houston_(713)4584939.exe</imagepath><md5sum>28401b273110fb
<malicious-alert classtype="misc-anomaly"><msg>Debugger awareness detected</msg><display-msg>Process trying to detect t
<mutex><value>\Sessions\1\BaseNamedObjects\DBWinMutex</value><processinfo><pid>2736</pid><imagepath>C:\VoiceMail_Housto
<process mode="started"><value>C:\Windows\System32\svchost.exe</value><pid>2744</pid><ppid>2736</ppid><parentname>C:\Vo
<malicious-alert classtype="misc-anomaly"><msg>Process starting new instance of svchost.exe</msg><display-msg>New servi
<codeinjection mode="create process suspended section mapped code injection" suppressed="false"><source tainted="true">
<malicious-alert classtype="misc-anomaly"><msg>Check for Self Code Injection</msg><display-msg>Check for Self Code Inje
<malicious-alert classtype="misc-anomaly"><msg>Code injection detected</msg><display-msg>Code injection detected</displ
<mutex><value/><processinfo><pid>2744</pid><imagepath>C:\Windows\System32\svchost.exe</imagepath></processinfo></mutex>
<mutex><value>\Sessions\1\BaseNamedObjects\DBWinMutex</value><processinfo><pid>2744</pid><imagepath>C:\Windows\System32

Controlled Information with Network Segmentation

TARGET as a company failed to identify the most critical part of the network. Hence, no proper security solution was in place to segment network traffic. A good approach is to ensure that exterior security is kept strong so that only those that are trusted are allowed into the network. [65]
TARGET implemented VLAN however, this was not strong enough to provide a security defense because when an attacker gets into the network, the Virtual LANS cannot stop the attack from spreading to other parts of the network. [58]
A perfect solution TARGET implemented was the Zero-trust strategy, this means that no one is trusted. Proper monitoring, identification and authorization is done for every traffic, and this helps to eliminate false positives to

ensure that intruders do not gain access to other parts of the network. Zero-trust strategy helps to improve outbound/perimeter security and inbound security. Proper policies are also set in the zero-trust security to ensure that for any alterations proper systems are put in place to alert administrators. However, the only drawback to this model is **high computation power** [59]

Secured Credit and Debit Cards through EMV (Europay, MasterCard and Visa)

After the Target Breach, a more secure way for cards was discussed. This ensured that credit and debit cards had a chip called EMV. This ensures that payments are executed through the chip with a signature or a pin. The data on the chip is also encrypted to avoid any form of modification by hackers.
The major drawbacks to the EMV are [52]
· A no-pin attack, where an electric device is put between the card and the POS terminal. The POS terminal is tricked and assumes that the correct pin has been put and payment is authorized
· CNP (Card Not present), when a purchase is made online. With this, the chip on the cards (EMV) is not taken into consideration. Attacks exploit this a lot to make a lot of purchases on dark web websites [53]

Tokenization of Credit and Debit Cards
With this process, credit, and debit card 16 numbers are immediately hidden during payment processing to prevent credential stuffing and man-in-the-middle attacks. The process of tokenization can only be reversed by the acquirer. [64]
The acquiring companies help customers secure the payment process and protect their credentials by

- Getting the customer information
- Generating a one-time token
- Sends the one-time token via a secured channel to merchants to ensure secure payment processing [65].

Acquirers are of two forms

1. Available systems such as Google Pay, and Apple pay [62].
2. Some top banks such as Bank of America provide this service for its customers to shop safely.

V. Conclusion

The Internet, filled with its immense benefits, is very important in the world as we all know. Just like everything of value, there is a need for periodic checks so that it does not become abused for personal gains hence the reason for the detailed analysis of the case studies taken in this research work. Cybercrime investigations from the JP Morgan chase data breach, the Melissa virus 1999 and target attack of 2013 revealed that there is a need for strict compliance to acceptable user policy for the internet and any violation shall be met with dire consequences. To ensure more compliance, the court should enforce similar sanctions to physical crimes as it would to cyber crimes.

Acknowledgment

We would like to express our gratitude and deep appreciation to everyone in this group who made it possible for us to complete this report.
We would also like to express our deep and sincere gratitude to our professor, Mr. Ivan Pustogarov, for giving us the opportunity to do this research while providing invaluable guidance throughout the research. His vision, simulating suggestions, genuineness, encouragement, and motivation has deeply inspired us. He showed us the best methods for conducting research and communicating the findings in order to deliver the results in the most understandable way. Being able to work and study under his direction was a huge honor and privilege. We are incredibly appreciative of what he has given us.

References

[1] M. M. H. Alansari, Z. M. Aljazzaf, and M. Sarfraz, “On Cyber Crimes and Cyber Security,” in Developments in Information Security and Cybernetic Wars, IGI Global, 2019, pp. 1–41.

[2] K. T. Smith, M. Smith, and J. L. Smith, “Case Studies of Cybercrime and its Impact on Marketing Activity and Shareholder Value,” Academy of Marketing Studies Journal, Dec. 2010.

[3] Wikipedia contributors, “2014 JPMorgan Chase data breach,” Wikipedia, The Free Encyclopedia, 10-Oct-2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=2014_JPMorgan_Chase_data_breach&oldid=1049232780. [Accessed 05 July 2022]

[4] M. Goldstein, N. Perlroth, and D. E. Sanger, “Hackers’ attack cracked 10 financial firms in major assault,” 03-Oct-2014.

[5] “CIA triad,” Fortinet. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/cia-triad. [Accessed 15 July 2022].

[6] “JPMorgan hack exposed data of 83 million, among biggest breaches in history,” Reuters, Reuters, 02-Oct-2014.

[7] Sec.gov. [Online]. Available: https://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm. [Accessed 26 July 2022].

[8] K. Zetter, “Four indicted in massive JP Morgan chase hack,” Wired, 10-Nov-2015.

[9] A. Deilami, “Jewish, Israeli bank hackers bragged of plans, exploits,” Timesofisrael.com. [Online]. Available: https://www.timesofisrael.com/jewish-israeli-bank-hackers-bragged-of-plans-exploits/. [Accessed 26 July 2022].

[10] “Manhattan U.s. attorney announces charges against three defendants in multi-million-dollar stock manipulation scheme — FBI,” Fbi.gov, 21-Jul-2015. [Online]. Available: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/manhattan-u.s.-attorney-announces-charges-against-three-defendants-in-multimillion-dollar-stock-manipulation-scheme. [Accessed 27 July 2022].

[11] L. Constantin, “Two-factor authentication oversight led to JPMorgan breach,” Computerworld, 23-Dec-2014. [Online]. Available: https://www.computerworld.com/article/2862578/twofactor-authentication-oversight-led-to-jpmorgan-breach-investigators-reportedly-found.html. [Accessed 27 July 2022].

[12] “Why use 2FA? : TechWeb : Boston university,” Www.bu.edu. [Online]. Available: https://www.bu.edu/tech/support/information-security/why-use-2fa/. [Accessed 27 July 2022].

[13] “What is Patch Management? Benefits & Best Practices,” Rapid7. [Online]. Available: https://www.rapid7.com/fundamentals/patch-management/. [Accessed 27 July 2022].

[14] “What is Intrusion Prevention System?,” VMware, 01-Aug-2022. [Online]. Available: https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html. [Accessed 27 July 2022].

[15] A. Gajawada, “Heartbleed bug: How it works and how to avoid similar bugs,” Application Security Blog, 06-Sep-2016. [Online]. Available: https://www.synopsys.com/blogs/software-security/heartbleed-bug/. [Accessed 30 July 2022].

[16] A. Jeng, “Minimizing Damage from J.P. Morgan’s Data Breach,” Mar. 2015.

[17] A. Artiningsih and A. S. Sasmita, “Data breaches and identity theft: A case study of U.s. retailers and banking,” Core.ac.uk. [Online]. Available: https://core.ac.uk/download/pdf/291262002.pdf. [Accessed 04 August 2022].

[18] K. Best and J. Lewis, "Hacking the Democratic Mainframe: The Melissa Virus and Transgressive Computing", *Media International Australia*, vol. 95, no. 1, pp. 207-226, 2000. Available: 10.1177/1329878x0009500118.

[19] L. Garber, “Melissa Virus Creates a New Type of Threat,” *Computer*, vol 32, no. 6, pp. 16-19, 1999. Available: 10.1109/mc.1999.769438 [Accessed 1 August, 2022].

[20] G. Mohay, A. Anderson, B. Collie, R. McKemmish and O. De Vel, *Computer and intrusion forensics by George Mohay ... [et al]*. Artech House, 2003, pp 236-242

[21] K. Rhodes, *The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data*. 2015.

[22] T. Schwartz, "A DYNAMIC CYBER-BASED VIEW OF THE FIRM", Graduate School, Temple University, Fox School of Business, 2019.

[23] *1999 CERT Advisories*. Carnegie Mellon University, 1999.

[24] [.D.|.F.-S.Labs”,“F-SecureLabs,”[Online].Available: https://www.f-secure.com/v-desc/melissa.shtml.. [Accessed 1 August 2022].

[25] M. L. Podcast, “Cybereason,”Cybereason, 14 June 2018. [Online]. Available: https://www.cybereason.com/blog/malicious-life-podcast-the-melissa-virus. [Accessed 20 July 2022].

[26] M. Richtel, “New York Times,” New York Times Company, 2 April 1999.[Online].Available: https://archive.nytimes.com/www.nytimes.com/library/tech/99/04/biztech/articles/02virus.html. [Accessed 21 July 2022].

[27] M. Grunwald, “Washington Post,” Washington Post Company,3 April 1999.[Online].Available: https://www.washingtonpost.com/wp-srv/business/longterm/melissavirus/melissa040399.htm. [Accessed 20 July 2022].

[28] D. Kocieniewski, “The New York Times,” The New York Times Company,3April,1999.[Online].Available: https://archive.nytimes.com/www.nytimes.com/library/tech/99/04/biztech/articles/03melissa.html. [Accessed 21 July 2022].

[29] D. Scoblionkov, “Wired,” Conde Nast, 2 April 1999. [Online]. Available: https://www.wired.com/1999/04/melissa-police-work-lauded/?redirectURL=https://www.wired.com/1999/04/melissa-police-work-lauded/. [Accessed 21 July 2022].

[30] A. D. J. G. Leslie Helm, “Los Angeles Times,” California Times,3 April,1999.[Online].Available: https://www.latimes.com/archives/la-xpm-1999-apr-03-mn-23832-story.html. [Accessed 20 July].

[31] R. B. Standler, “www.rbs2.com,” 17 September 2002. [Online]. Available: http://www.rbs2.com/dls.htm. [Accessed 24 July 2022].

[32] “ITRC breach report,” Identity Theft Resource Center, 2014. Accessed: Jul. 18, 2022. [Online]. Available: http://www.idtheftcenter.org/images/breach/ITRC Breach Report 2014.pdf.

[33] C. Timberg, J. Yang, and H. Tsukayama. “Target says 40 million credit, debit cards may have been compromised in security breach.” washingtonpost.com. https://www.washingtonpost.com/business/technology/target-data-breach-affects-40-million-accounts-payment-info-compromised/2013/12/19/5cc71f22-68b1-11e3-ae56-22de072140a2_story.html

[34] W. Hartzog and D. Solove. “We Still Haven’t Learned the Major Lesson of the 2013 Target Hack.” Slate.com. https://slate.com/technology/2022/04/breached-excerpt-hartzog-solove-target.html#:~:text=Through%20the%20Trojan%20horse%2C%20the,just%20a%20few%20thousand%20dollars (Accessed Jul. 26, 2022).

[35] X. Shu, K. Tian, A. Ciambrone and D. Yao, “Breaking the Target: An Analysis of Target Data Breach and Lessons Learned,” 2017. [Online]. Available: arXiv:1701.04940v1

[36] “A “Kill Chain” Analysis of the 2013 Target Data Breach”. US Senate. Committee on commerce, science, and transportation, USA, Majority Staff Rep. Mar. 26, 2014.

[37] Fazio Mechanical Services, Statement on Target Data Breach, Available: http://faziomechanical.com/Target-Breach-Statement.pdf (Accessed Jul. 12, 2022).

[38] E. Harris, N. Perlroth, N. Popper, and H. Stout, “A Sneaky Path Into Target Customers’ Wallets.” Nytimes.com. http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html (Accessed Aug. 1, 2022).

[39] B. Krebs, “Target Hackers Broke in Via HVAC Company.” krebsonsecurity.com. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ (Accessed Jul. 15, 2022).

[40] B. Krebs, “A First Look at the Target Intrusion Malware.”, krebsonsecurity.com. http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/ (Accessed Jul. 15, 2022)

[41] M. Oh, “An evolution of BlackPOS malware,” Jan. 2014.

[42] B. Krebs, “New clues in the Target breach.” krebsonsecurity.com. http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach / (Accessed Jul. 15, 2022).

[43] X. Sun. Carey Business School Johns Hopkins University. Target Breach Case Study Executive Summary. [Online]. Available: https://cpb-us-w2.wpmucdn.com › files › 2017/06

[44] G. Washington, “Target Breach Impact Survey.” Silo.tips. https://silo.tips/download/target-breach-impact-survey (Apr. 13, 2016)

[45] C. Smith, “It turns out Target could have easily prevented its massive security breach.” Bgr.com. https://bgr.com/general/target-data-hack-how-it-happened/ (Accessed Mar. 13, 2014).

[46] “Computer Fraud and Abuse Act (CFAA) | Practical Law,” *ca.practicallaw.thomsonreuters.com*. https://ca.practicallaw.thomsonreuters.com/2-508-3428?transitionType=Default&contextData=(sc.Default)&firstPage=true

[47] “Hacker linked to Target data breach gets 14 years in prison,” The Washington Post, Sep. 21, 2018. [Online]. Available: https://www.washingtonpost.com/local/public-safety/hacker-linked-to-target-data-breach-gets-14-years-in-prison/2018/09/21/839fd6b0-bd17-11e8-b7d2-0773aa1e33da_story.html

[48] S. L. Latta, Investigating Cybercrime. Enslow Publishing, LLC, 2017. Accessed: Aug. 13, 2022. [Online]. Available: https://books.google.ca/books?id=FA9iDwAAQBAJ&pg=PA19&lpg=PA19&dq=andrey+hodirevski&source=bl&ots=ctxr-AihDs&sig=ACfU3U3flKk9mqFTImi6OlbD0D53ivSkcw&hl=en&sa=X&ved=2ahUKEwjv-J-DrKv5AhWwGFkFHdkhDjcQ6AF6BAgvEAM#v=onepage&q=andrey%20hodirevski&f=false

[49] “Mexican Pair Pleads Guilty to Debit/Credit Card Conspiracy In $35K McAllen Shopping Spree,” www.justice.gov, Apr. 30, 2015. https://www.justice.gov/usao-sdtx/pr/mexican-pair-pleads-guilty-debit credit-card-conspiracy-35k-mcallen-shopping-spree (accessed Aug. 13, 2022).

[50] M. Plachkinova and C. Maurer, “Teaching Case: Security Breach at Target,” Print) Journal of Information Systems Education, vol. 29, no. 1, pp. 1055–3096, 2018, [Online]. Available: https://jise.org/Volume29/n1/JISEv29n1p11.pdf

[51] J. Finkle and S. Heavey, “Target says it declined to act on early alert of cyber breach,” March 2014.

[52] M. Riley, B. Elgin, D. Lawrence, and C. Matlack, “Missed alarms and 40 million stolen credit card numbers: How Target blew it,” March 2014.

[53] Rachel Weiner, https://www.washingtonpost.com/local/public-safety/hacker-linked-to-target-data-breach-gets-14-years-in-prison/2018/09/21/839fd6b0-bd17-11e8-b7d2-0773aa1e33da_story.html, Sep 21 2018,

[54] Tiffany hsu, https://www.latimes.com/business/la-fi-target-arrests-20140121-story.html, Jan 20, 2014.

[55] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, “Crying wolf: An empirical study of SSL warning effectiveness.” in USENIX Security Symposium, 2009, pp. 399–416.

[56] D. Akhawe and A. P. Felt, “Alice in warningland: A large-scale field study of browser security warning effectiveness,” in USENIX Security Symposium, 2013.

[57] D. Modic and R. J. Anderson, “Reading this may harm your computer: The psychology of malware warnings,” 2014

[58] Payment card industry payment application data security standard, https://www.pcisecuritystandards.org/documents/ PA-DSS v3.pdf.

[59] R. Anderson and S. J. Murdoch, “EMV: why payment systems fail,” Communications of the ACM, vol. 57, no. 6, pp. 24–28, 2014.

[60] S. J. Murdoch, S. Drimer, R. J. Anderson, and M. Bond, “Chip and PIN is broken,” in 31st IEEE Symposium on Security and Privacy, S&P 2010, 16-19 May 2010, Berleley/Oakland, California, USA, 2010, pp. 433–446.

[61] “Challenges & opportunities for merchant acquirers,” 2012, Capgemini.

[62] Operator of Counter Antivirus Service "Scan4you" Sentenced to 14 Years in Prison. (2018). Department of Justice. Retrieved from https://www.justice.gov/opa/pr/operator-counter-antivirus-service-scan4you- sentenced-14-years-prison

[63] Pigni, F., Bartosiak, M., Piccoli, G., & Ives, B. (2018). Targeting Target with a 100-million-dollar data breach. Journal of Information Technology Teaching Cases, 8(1), 9–23. https://doi.org/10.1057/s41266-017-0028-0

[64] Radichel, T. (2014). Case study: Critical controls that could have prevented target breach. SANS Institute InfoSec Reading Room.

[65] Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the target: An analysis of target data breach and lessons learned. arXiv preprint arXiv:1701.04940