Module Code & Module Title

CC4004NI Cybersecurity Fundamentals

Assessment Weightage & Type 50%

Individual Coursework 1

Year and Semester

2021 - 22 Spring - 1

Student Name: Sharams Kunwar

London Met ID: 21049701

College ID: NP01NT4A210112

Assignment Due Date: 22nd August, 2022
Assignment Submission Date: 22nd August, 2022
Submitted to: Mr. Monil Adhikari

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to the Islington College and the module teacher Mr. Prayag Raj Koirala for assisting me in accomplishment of the coursework in the given time frame. Likewise, I would also like to convey my sincere appreciation to all the involved helping hands.

The guidance from lecturer Mr. Koirala led to accomplishment of the coursework. I would like to greatly thank him for assisting me day and night to solve my errors and helping me to conduxt researches on the topic. I would also like to express my sincere gratitude to Mr. Monil Adhikary for proper guidance.

At last, I would like to thank my friends and family and also seniors who helped me clear my confusions and solve problems I faced throughout the completion of the project.

Sincerely Yours,

Sharams Kunwar.

Table of Contents

Table of figures

ABSTRACT

In the report, we will be discussing the facts involved in the attack. Also, the impact it had on the victims are to be discussed in the report along with statements released from the victims of the attack. Similarly, how the malware was introduced to the system and the infection or life cycle of the malware is discussed in the report relating with the real-life attack scenario. Similarly, we are also going to discuss about the precautions measures to be applied in order to be safe from such attacks and also discuss on the causes that led to the attack.

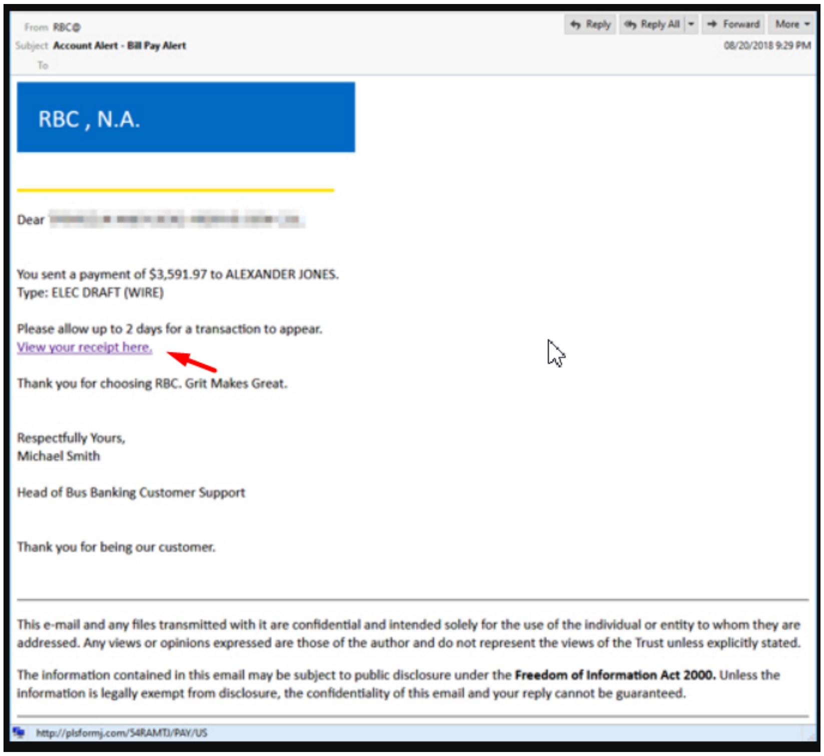
Likewise, another section would in the report would cover the incident response for a company under such attack where the company is subjected to be the victim of the attack resulting in a data breach. Similarly, the charges that could be imposed on the company are also to be discussed in the second section.

Third section of the report, I would write my thoughts on the attack on the company and would explain the actions I'd take if I were the Chief Information Security Officer (CISO) of the company under such attack. I would explain the preventive measures to not let such incident occur again in the final section of the report.

1. Introduction

Trends begin and they end at a certain point of time. Tiktok, Andrew Tate are the hottest topics around the world as of present days. Tracing back to 2014, Ice Bucket Challenges were the hot cakes but they soon faded away. Likewise, in 2014, a Trojan named Emotet which primarily spread through spam mails was another trending topic around the globe which unlike other trends never faded away and still hurts millions of computer users around the globe. So, everyone might wonder what kind of phenomenon an Emotet is, which would elude everyone's efforts to stop it.

Emotet is a Trojan actually. It primarily spreads through 'malspam' or in simple terms via spam mails. The spam mails contain familiar brandings which disguise receivers into thinking that it is a legitimate mail and lure them into malicious links or script or in most cases macro-enabled document files.



From RBC©
Subject **Account Alert - Bill Pay Alert**
To

08/20/2018 9:29 PM

RBC , N.A.

Dear [redacted]

You sent a payment of $3,591.97 to ALEXANDER JONES.
Type: ELEC DRAFT (WIRE)

Please allow up to 2 days for a transaction to appear.
View your receipt here.

Thank you for choosing RBC. Grit Makes Great.

Respectfully Yours,
Michael Smith

Head of Bus Banking Customer Support

Thank you for being our customer.

This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. Any views or opinions expressed are those of the author and do not represent the views of the Trust unless explicitly stated.

The information contained in this email may be subject to public disclosure under the **Freedom of Information Act 2000.** Unless the information is legally exempt from disclosure, the confidentiality of this email and your reply cannot be guaranteed.

http://plsformj.com/54RAMTJ/PAY/US

Figure 1 Emotet Email Example

For further information

1.1 Brief overview of the Report:

In Section 1 of this report, I am about to explain about the Emotet attack that occurred in one of the most renowned publishing houses of the Germany based in Hanover, Heise Online. On 13th of May, shortly before 3 P.M., the employee of the company opened an email that seemed legitimate and very tempting mentioning the real transaction between the publishing house and its business partners. It opened in MS Word and a fake error message popped up requesting the user to enable access for editing. Complying with such simple request became the root cause to unleash attack.

Likewise, in Section 2 of the report, I've explained about how a company shall respond in case of a cyber-attack resulting in a data breach and the fines imposed on such companies who've violated the regulations.

Similarly, in Section 3, how my roles as a Chief Information Security Officer for Heise Online would have handled the situation have been explained.

The overall goal of the project is to research about a cyber attack and provide its documentation regarding that particular malware named 'Emotet', the effects it left on the victims and the causes behind it.

For further information

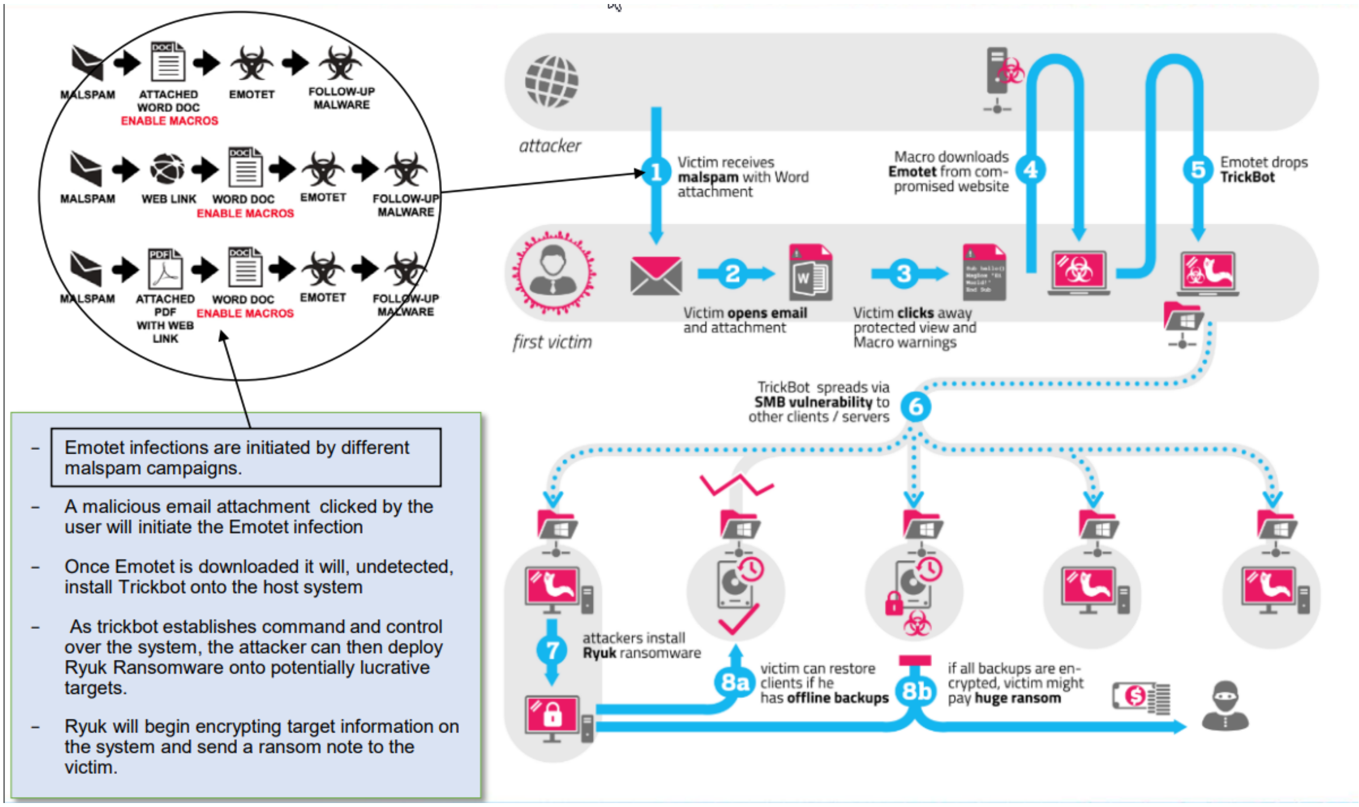
2. SECTION 1: Research into theft of personal data

2.1 Trojan Infestation: Emotet-at-Heise

Heise Group and the Heinz Heise publishing house is one of the most renowned German publishing houses based in Hanover. A serious ‘burglary’ was reported in the Heise network as per the statement published on its website on 6th June, 2019. (Schmidt, 2019). The trigger to the ‘burglary’ was an Emotet infection.

2.2 Lifecycle of Emotet

Emotet, unlike any other malware shares a similar lifecycle. It involves 4 phases: Infection via malspams, Persistence Establishment where it creates registry auto start keys and injects itself into running processes, Instructions Phase in which it receives instructions from C2 servers and Propagation through-out the Network using spreader modules like NetPass.exe, Outlook Scrapper, WebBrowserPassView, Mail PassView, Credential enumerator (CIS, 2022).



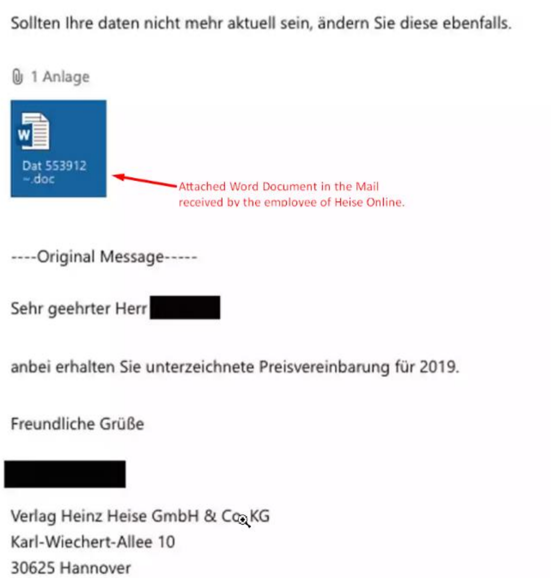
MALSPAM
ATTACHED WORD DOC
ENABLE MACROS
EMOTET
FOLLOW-UP MALWARE
MALSPAM
WEB LINK
WORD DOC
ENABLE MACROS
EMOTET
FOLLOW-UP MALWARE
MALSPAM
ATTACHED PDF WITH WEB LINK
WORD DOC
ENABLE MACROS
EMOTET
FOLLOW-UP MALWARE
attacker
1 Victim receives malspam with Word attachment
Macro downloads Emotet from compromised website 4
5 Emotet drops TrickBot
first victim
2 Victim opens email and attachment
3 Victim clicks away protected view and Macro warnings
TrickBot spreads via SMB vulnerability to other clients / servers 6
7 attackers install Ryuk ransomware
8a victim can restore clients if he has offline backups
8b if all backups are encrypted, victim might pay huge ransom

- Emotet infections are initiated by different malspam campaigns.
- A malicious email attachment clicked by the user will initiate the Emotet infection
- Once Emotet is downloaded it will, undetected, install Trickbot onto the host system
- As trickbot establishes command and control over the system, the attacker can then deploy Ryuk Ransomware onto potentially lucrative targets.
- Ryuk will begin encrypting target information on the system and send a ransom note to the victim.

Figure 2 lifecycle of Emotet (Anon., 2019)

2.2.1 Infection Phase in Emotet-at-Heise

On a Monday afternoon, May 13 around 3:00 P.M., an employee of the Heise Online received a mail that referred to a "real business transaction" between Heise Online and one of its business partners. The mail had a Word document attached and requested it to be checked and changed as per necessity. The mail looked something like this (Schmidt, 2019).



Sollten Ihre daten nicht mehr aktuell sein, ändern Sie diese ebenfalls.

1 Anlage

Dat 553912
~.doc

Attached Word Document in the Mail
received by the employee of Heise Online.

----Original Message-----

Sehr geehrter Herr [redacted]

anbei erhalten Sie unterzeichnete Preisvereinbarung für 2019.

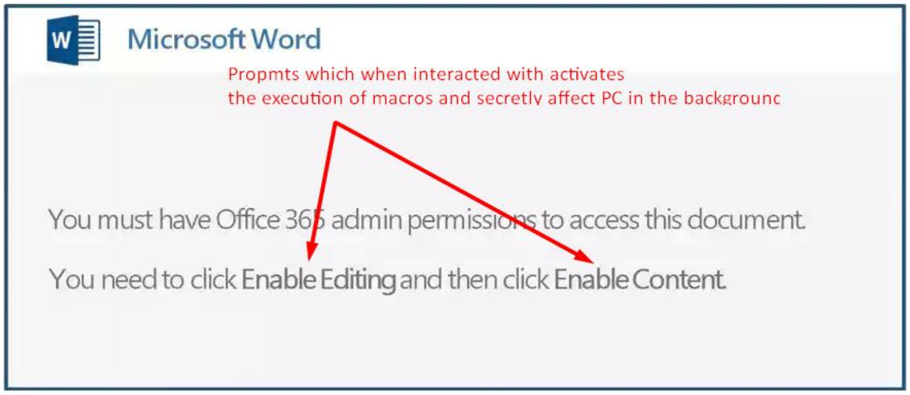
Freundliche Grüße

[redacted]

Verlag Heinz Heise GmbH & Co. KG
Karl-Wiechert-Allee 10
30625 Hannover

Figure 3 Phising Mail recieved by Heise Online

The mail seems very legitimate and tempting. The employee had found it the same too. He clicked on it without giving it a second thought as it involved a sensitive topic. After clicking on it a display message popped up looking like the following.



Microsoft Word

Propmts which when interacted with activates
the execution of macros and secretly affect PC in the backgrounc

You must have Office 365 admin permissions to access this document.

You need to click **Enable Editing** and then click **Enable Content**.

Figure 4 Fake error message at Heise Online

The employee didn't know about the threat. Hence, he pursued further and complied with the request. Then, the disaster to the Heise Online took its course. Emotet infected his Windows System and created a havoc on the Heise network triggering alarms from the antivirus software like Avira and Window Defender. The administrators were called in to clean it and they did their part as well and were initially convinced on the clearance of the malware.

2.2.2 Persistence and Instructions Phase in Emotet-at-Heise

This is where the deceptive nature of the Emotet comes into play. Everything was going fine until Wednesday afternoon, i.e., 15th May, 2019. Emotet had already created registry auto start keys and had already injected itself into running processes. A number of connections to Emotet servers were discovered in the firewall logs on Wednesday afternoon (Schmidt, 2019).

After quick checks and the scanning of ports revealed that multiple computers had already even started communicating with the outside servers via connections which were described to be strange, for example on TCP port 449.

2.2.3 Network Propagation in Emotet-at-Heise

After the initial infection, Emotet then downloaded additional modules of its own like Trickbot. The modules then quickly infected all Windows 10 workstations available in the network where the users were provided with local admin rights which actually was already against the policy. The Windows 10 workstations without local admin rights were spared from the infections. Meanwhile, the computers running Windows 7 which were still active on the network was affected by the malware downloaded by Emotet. Some of these infections were carried out using credentials of the domain administrator. The infections were then used to set up a new service on the targeted computers. The stealing of the credentials is still a mystery and yet the method of credentials extraction hasn't been known. However, after reviewing the log files a brute force attack on the password has been found but the strength of the password is very high to be cracked via Brute-force. Extraction of domain admin credentials from an infected system's RAM would be a much likely possibility (Schmidt, 2019).

2.3 Damage from the Trojan: Emotet-at-Heise

The infected computers had to be shut down immediately. Not only that, the clean windows 10 computers were also had to be disconnected from the networks which halted the operations and affected the functioning of the company. This led to economic loss and also a disruption in the work environment of the company.

The admins had to set up new computers and new Active Directory along with new tightened security measures. Existing data, tools are transferred to a new network with utmost care.

Likewise, also it is uncertain about the data criminals have gotten access to. So, it is a very dangerous circumstance as Heise online is largely independent of the Heise Network's IT and there should be no signs of Emotet compromise.

The company's reputation may have been heavily tarnished and the business partners may also have not been properly confident as their data was on risk along with data of subscribers. But the company was able to maintain transparency regarding the situation and made sure to raise awareness for other companies to take precautions against such threats (Schmidt, 2019).

2.4 Errors leading to Trojan: Emotet-at-Heise

The errors leading to the disaster are shortlisted below:

- Failed to implement filters at the email gateway to filter out emails containing malspams.
- Password resets for both domain and local credentials weren't issued.
- Social engineering and phising training weren't given to the employees.
- Domain-based Message Authentication, Reporting and Conformance (DMARC) wasn't implemented which would minimize spam emails by detecting it using DNS records.
- Failed to disable all macros except digitally signed ones.

3. SECTION 2: Personal Data Loss in a Cyber-Attack

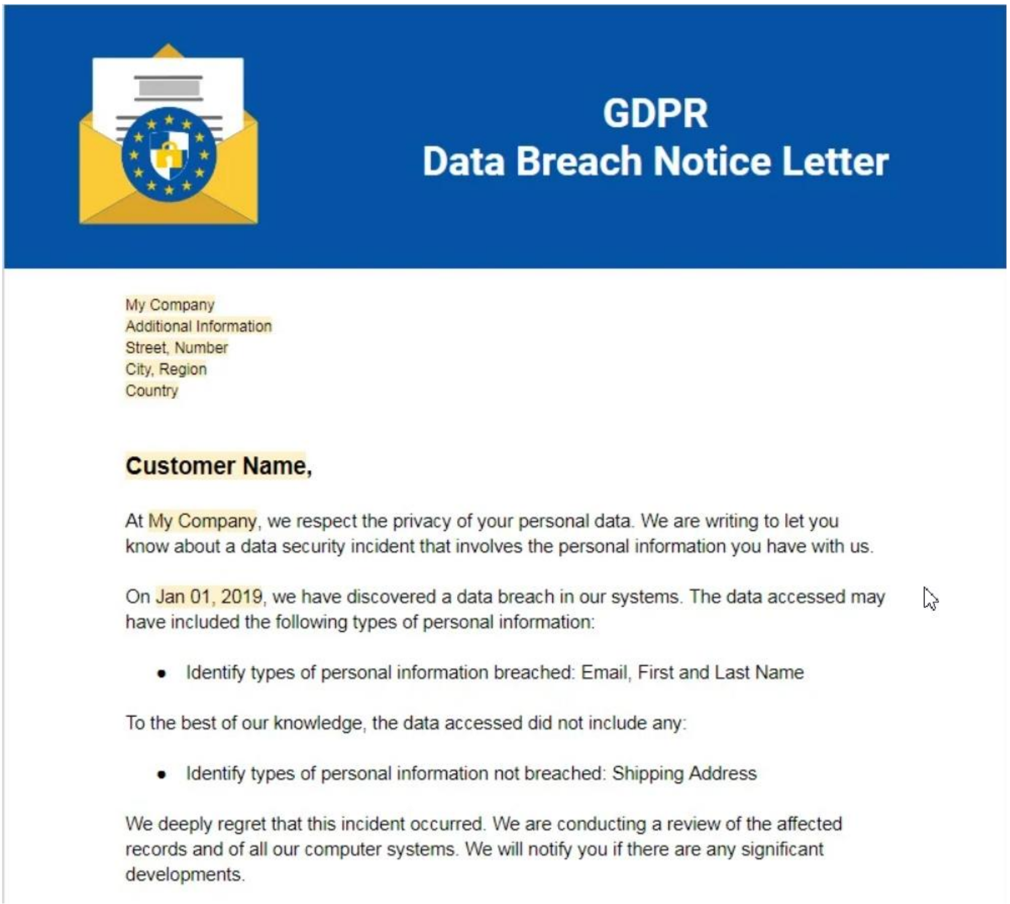
Any kind of a cyber-attack can cause a major damage to the victim organization. A major damage could be from the data which is breached in the attack. The victim of the attack may be subjected to fines and charges by the governing bodies which enforce General Data Protection Regulation (GDPR) like ICO, Data Protection Commission (DPC), CNIL or any other Data Protection Authorities for the violation of GDPR. The possibilities of a data breach can be definitely minimized by applying certain preventive measures and training employees. Even after that, if a data breach occurs, then the breach shall be responded to in a professional manner and not panicking in any way (Lu, 2022)

3.1 Appropriate Responses for a Company in a Data-Breach

What a company does after the wake of a data breach is just as crucial as the security measures the company takes to prevent such attacks. By taking appropriate steps, the company can minimize the consequences to themselves and their clients. Few of the steps are as follows:

- The company must react quickly to secure their systems and fix the probable vulnerabilities which may have caused the breach in the first place in order to avoid multiple data breaches and not let it happen again.
- Physical areas related to breach shall be secured by locking them or changing the access codes and resuming the regular operations only after proper consultation with forensic experts.
- Breach Response Team shall be mobilized immediately to avoid additional data loss and act accordingly according to nature of the breach.
- A team of independent data forensics team should be hired to determine scope and the source of the data breach and also capture affected systems, collect and analyze evidence.
- A legal counsel shall be consulted regarding the breach. If necessary, an outside legal counsel shall be hired with expertise in data security to get proper advice on federal and state laws that may have been implicated by the data breach.
- All affected equipment shall be taken off immediately but no machines shall be turned off until the forensics experts come to help.

- Also, credentials of the authorized users in the system shall be updated to avoid additional data loss and to prevent the system from being compromised.
- Web shall be searched for the leaked information or if any personal information is posted on the website, it shall be removed immediately. Also, the cache should be checked and cleared immediately.
- The people who discovered the breach shall be properly interviewed for the investigation of the case. The investigation shall be well documented.
- In the course of investigation and recovery, no evidence shall be destroyed as it can affect the investigation and remediation both.
- Also, appropriate parties shall be notified including law enforcement, affected businesses and affected individuals. Following could be the appropriate model letter for notifying affected ones (Commission, 2022).



GDPR
Data Breach Notice Letter

My Company
Additional Information
Street, Number
City, Region
Country

Customer Name,

At My Company, we respect the privacy of your personal data. We are writing to let you know about a data security incident that involves the personal information you have with us.

On Jan 01, 2019, we have discovered a data breach in our systems. The data accessed may have included the following types of personal information:

- Identify types of personal information breached: Email, First and Last Name

To the best of our knowledge, the data accessed did not include any:

- Identify types of personal information not breached: Shipping Address

We deeply regret that this incident occurred. We are conducting a review of the affected records and of all our computer systems. We will notify you if there are any significant developments.

Figure 5 Model Letter for Notifying Data Breach (Bateman, 2022)

3.2 Fines Imposed on the violations of regulations

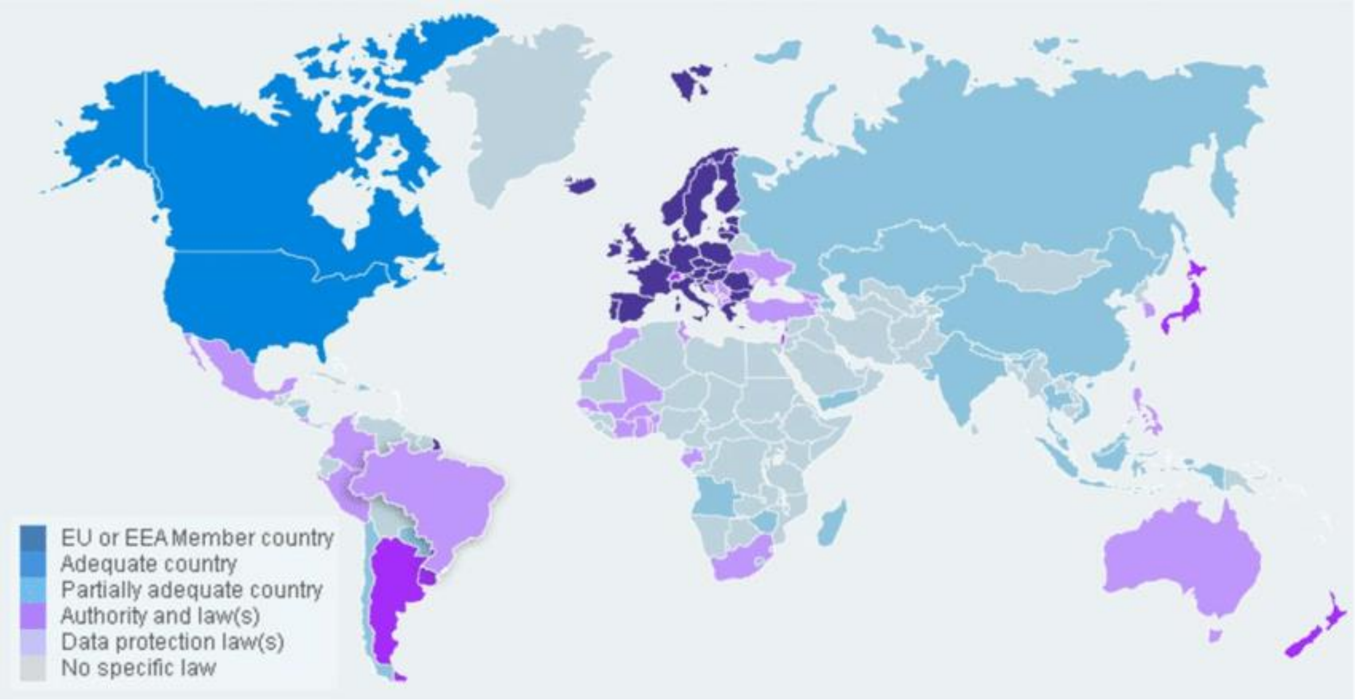


Figure 6 Data Protection Around the World (Souza, 2022)

More information

On the case of violations of the regulations, the company are imposed fines or charges accordingly depending upon the nature of violation. Since GDPR came in effect, over 900 fines have been imposed across Europe Economic Area (EEA). A company may be fined up to $20.3 Million or 4% of worldwide turnover – whichever is higher. (Tessian, 2022)

Among other violations, data breach is considered very dangerous as data leak is a serious issue. The prime examples of such fines imposed on the company for violations like data breach are as follows:

- Equifax (Federal Trade Commission, 2021)
  Equifax suffered from a data breach in 2017 resulting in breach of personal information of around 147 million people. A lawsuit was created against Equifax. It finally came to settlement in July 2019. They were made to spend up to $425 million to help affected ones in the data breach under their settlement agreement with FTC, CFPB and state attorney general.
- National Revenue Agency (Bulgaria) (Tessian, 2022)
  Bulgaria's National Revenue Agency was fined on August 2019 after it suffered a data breach which is reported to affect around 5 million people as their personal information were reportedly leaked. The agency failed to protect such personal data and was reportedly fined $3 million by GDPR.
- Cosmote Mobile Telecommunications (Tessian, 2022)
  A fine of $6.6 million was issued on Cosmote Mobile Telecommunications by the Greek Data Protection Authority and Hellenic Data Protection Authority in February 2022 following a data breach in September 2020 which led to leaking of customer data which was not even fully pseudonymized.
- Marriott (Tessian, 2022)
  Marriott acquired Starwood in 2016. The hack originated in Starwood Group Reservation System in 2014 and was undetected till September 2018 compromising the data of around 383 million guests. Consequently, they were fined $23.8 million which is significantly lesser than $123 million fine originally levied by ICO.
- British Airways (Tessian, 2022)
  British Airways were fined $26 million for a breach in 2018 which exposed personal data of around 400k customers which was actually preventable, but occurred eventually due to insufficient security measures. The fine is considerably lower than $238 million fine originally levied by ICO.

4. SECTION 3: CHIEF INFORMATION SECURITY OFFICER

In the infosec universe, Chief Infosec Officers are often referred to as crème de la crème – head of the class (cybersecurity guide, 2022). CISO is one of the most influential officers in any company. It requires immense experience, expertise and skills in various aspects comprising information security like governance, risk management, information security controls, its compliance, audit management, security program management and its operations, strategic planning, procurement and vendor management. A CISO must be a competent and motivational leader.

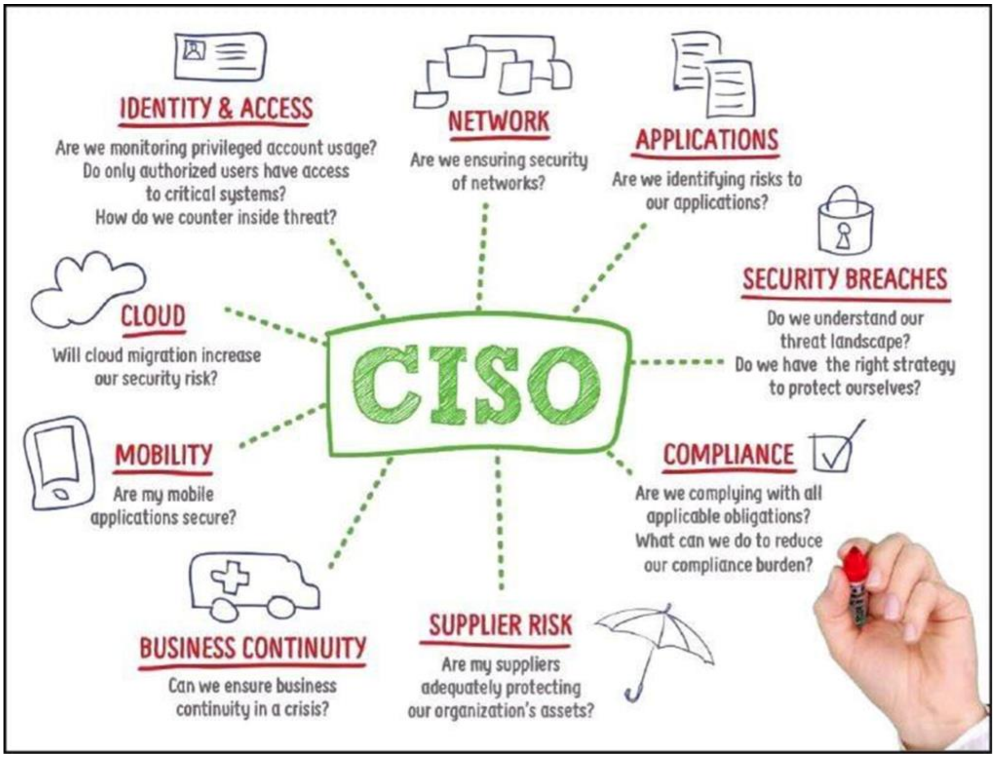

IDENTITY & ACCESS
Are we monitoring privileged account usage? Do only authorized users have access to critical systems? How do we counter inside threat?
NETWORK
Are we ensuring security of networks?
APPLICATIONS
Are we identifying risks to our applications?
SECURITY BREACHES
Do we understand our threat landscape? Do we have the right strategy to protect ourselves?
CLOUD
Will cloud migration increase our security risk?
CISO
MOBILITY
Are my mobile applications secure?
COMPLIANCE
Are we complying with all applicable obligations? What can we do to reduce our compliance burden?
BUSINESS CONTINUITY
Can we ensure business continuity in a crisis?
SUPPLIER RISK
Are my suppliers adequately protecting our organization's assets?

Figure 7 CISO

4.1 Role of CISO to prevent cyber-attack

Ransomware just doesn’t stop at ransomware. It further leads to DDoS and data breaches which ultimately results in catastrophic calamities which involves financial and reputational loss. The ransomware groups are being even more competitive nowadays as there is so much money in this lucrative business (Nicoletti, 2021).

As a CISO, there is a crucial role to play for such important personnel during such cyber-attack. For instance, if I were a CISO of Heise Online during Emotet attack in 2019. There are several roles I could have played to prevent the attack. Few of the roles are listed below.

- I would make my team under me aware of the basics like thinking before clicking on any kind of link or malspams even if they are from a trusted source. I would have instructed them to contact IT department even in a minor suspicion.
- I would apply various kinds of security measures beforehand, so the company Heise Online would be safer from dangers. The measures would include utilizing firewalls, screening incoming links, filtering the mails for malspams, blocking desired traffic, continuously checking computer for any kind of malware, etc.
- I would have ensured of API integration being in place, SEIM and SOAR are in a good communication and would use best of breed tools.
- I would instruct an officer to constantly overview the devices connected in the network and only allow permitted devices in the company’s network.
- I would shift my focus towards preventative posture and try reducing the damage rather than only detecting the threat.
- I would have invested in ransomware prevention and tools for preventing malware including system backups and vulnerability management and try to patch my systems all the time by requesting funds from higher authorities and would have hopefully prevented the attack.
- Along with the training to employees, I would have deployed API based email protection to prevent the attack, even if someone got enticed by the phishing mail and clicked on it (Nicoletti, 2021) (Hannan, 2021).

  Hence, I could have prevented Heise Online, 2019 by taking measures beforehand.

4.2 Taking Measures of Prevention against Cyber-Attack as a CISO

Similarly, I could have brought a lot of reforms and changes in the policy of the organizations to help prevent the Trojan Infestation. Here, are the few measures of prevention I would apply to prevent malware attacks.

- Keeping up to date:
  I would keep myself and the teams updated about the developments in the cyber news concerning new developments in the malware and constantly research on the latest developments.
- Security Updates:
  I would ask all of my employees to regularly update macOS or windows to not let someone expose the security gap and patch the vulnerabilities as soon as possible. Also, any application programs, browsers, email clients, outlook, etc. ’s updates shall be immediately installed to close possible security gaps.
- Use of ad-blocker:
  Spyware containing pop-ups are deployed in most cases to track the company’s network activity. Hence, using trusted ad-blocker would solve the issue and prevent the exploitation of vulnerabilities.
- Install virus protection:
  Use of reputable antivirus software ensures the device protection 24/7 and provides full protection against latest viruses, spyware, etc. and it could scan the computers regularly for vulnerabilities.
- Password Policy:
  I would encourage everyone to use only strong passwords for all logins by making it up oneself or have them generated via software and also use multiple factor authentication for extra safety.
- Intrusion Detection System (IDS):
  IDS looks for activities of suspicions on a network and alerts to administrator or collected centrally using SIEM when it finds it.

Hence, these are the policies I would implement to prevent cyber attack from taking place. Besides them, exercising caution with questionable links and displaying file extensions by default would add to prevention (geeksforgeeks, 2022) (Kaspersky, 2022) .

4.3 Measures to be taken after attack for it to not occur again

Despite, security measures taken, the attack is not completely prevented. It can occur despite the prevention. In case of an attack, it shall be treated with a proper response. The following points would summarize my actions as a CISO of Heise Online at Trojan Infestation: Emotet-at-Heise:

- I would enforce on taking the system offline and disconnecting computers on network.
- I would reset credentials but would not lock myself out of recovery systems.
- I would restore from the backup after ensuring it is free of viruses.
- Then, after reinstalling OS, I would reconnect with network and ensure proper monitoring of network traffic and conduct anti-malware scans.

After the attack, to not let it reoccur I would take following steps:

- I would train my staffs and learn from the incident simultaneously.
- I would enforce on keeping my systems up-to-date.
- I would ensure endpoint protection.
- A proper firewall shall be installed.
- I would also enforce on keeping backup of data and ensure its safety.
- I would control access to the systems and WIFI security as well.
- New passwords with higher strength shall be selected.

Hence, in this way I would prove to be an efficient CISO in the organization.

5. Conclusion

The given coursework was about to fabricate the research on Emotet cyber-attack. The research was done on the Heise Online Emotet attack which occurred on 2019. To be brief, the research was done on the weakness which were exploited for the attack to take place. Two aspects of the cyber threat shine out: the individuals executing the attack and the targeted technologies. The attackers have additional advantages as the technologies develops. The organizations shall develop as the attacker advance to keep up.

I learned more about the attack after proper investigation on occurrence of the attack. The details of the attack on what, when and why it had happen led to further enlighten my knowledge on the attack. The Emotet attack on Heise Online, 2019 paralyzed one of the most recognized publishing houses in the Europe. The Heise Online went temporarily offline and it never recovered from the attack as no one still doesn’t know the data leaked in the breach. The experts had patched it temporarily but the malware was still active on the background and the system had to be downed.

My investigation on the attack led to enlighten me more on the topic of the Emotet. I learned about the impact of the cyber-attack on organization and the measures to be taken to prevent it. Accordingly, I also learned to handle the situation with the proper incident response. I conducted my research using web articles, journals and going through the case studies. I also consulted my module leader to accomplish the project.

References

Anon., 2019. *HHS.gov.* [Online]
Available at: https://www.hhs.gov/sites/default/files/emotet-update.pdf
[Accessed 2022].

Anon., 2022. *cisecurity.org.* [Online]
Available at: https://www.cisecurity.org/insights/white-papers/ms-isac-security-primer-emotet
[Accessed 2022].

Bateman, R., 2022. *TermsFeed.* [Online]
Available at: https://www.termsfeed.com/blog/gdpr-data-breach-notice-letter/
[Accessed 2022].

CIS, 2022. *MS-ISAC Security Primer- Emotet.* [Online]
Available at: https://www.cisecurity.org/insights/white-papers/ms-isac-security-primer-emotet

CNIL, 2022. *Data protection around the world.* [Online]
Available at: https://www.cnil.fr/en/data-protection-around-the-world

Commission, F. T., 2022. *Data Breach Response: A Guide for Business.* [Online]
Available at: https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

cybersecurity guide, 2022. *How to become a chief information security officer: A complete career guide.* [Online]
Available at: https://cybersecurityguide.org/careers/chief-information-security-officer/

Federal Trade Commission, 2021. *Federal Trade Commission.* [Online]
Available at: https://www.identitytheft.gov/#/Info-Lost-or-Stolen
[Accessed 2022].

geeksforgeeks, 2022. *Virtual CISO.* [Online]
Available at: https://www.geeksforgeeks.org/virtual-ciso-vciso/

Hannan, N., 2021. *6 ways to prevent insider threats every CISO should know.* [Online]
Available at: https://www.techtarget.com/searchsecurity/post/6-ways-to-prevent-insider-threats-every-CISO-should-know

Kaspersky, 2022. *Emotet: How to best protect yourself from the Trojan.* [Online]
Available at: https://www.kaspersky.com/resource-center/threats/emotet

Lu, D. C. &. A. H., 2022. *Board Oversight of Cyber Risks and Cybersecurity.* [Online]
Available at: https://www.imd.org/research-knowledge/articles/Board-Oversight-Cyber-Risks-Cybersecurity/

Nicoletti, P., 2021. *CISO Talk: How to respond to and prevent ransomware attacks.* [Online]
Available at: https://www.cybertalk.org/2021/12/07/ciso-talk-how-to-respond-to-and-prevent-ransomware-attacks/

Schmidt, J., 2019. *Trojan Infestation: Emotet at Heise,* Hanover: Heise network.

Securities, H., 2022. *emotet-malware-history.* [Online]
Available at: https://heimdalsecurity.com/blog/emotet-malware-history/
[Accessed 2022].

Souza, J. S. d., 2022. *Research Gate.* [Online]
Available at: https://www.researchgate.net/figure/Data-protection-around-the-world-25_fig5_347583331

Tessian, 2022. *Top data breaches.* [Online]
Available at: https://www.tessian.com/blog/biggest-gdpr-fines-2020/
[Accessed 2022].

Thales, 2022. *BEYOND GDPR: DATA PROTECTION AROUND THE WORLD.* [Online]
Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyond-gdpr-data-protection-around-world

Bibliography

Anon., 2022. *cisecurity.org.* [Online]
Available at: https://www.cisecurity.org/insights/white-papers/ms-isac-security-primer-emotet
[Accessed 2022].

ATT&CK, M., 2022. *Enterprise Matrix.* [Online]
Available at: https://attack.mitre.org/matrices/enterprise/

COMODO CYBERSECURITY, 2022. *Malware Infection.* [Online]
Available at: https://enterprise.comodo.com/malware-infection.php

Europol, 2022. *World's most dangerous malware EMOTET disrupted through global action.* [Online]
Available at: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

IMD, 2022. *Board Oversight of Cyber Risks and Cybersecurity.* [Online]
Available at: https://www.imd.org/research-knowledge/articles/Board-Oversight-Cyber-Risks-Cybersecurity/

Menn, J., 2019. *Cult of the Dead Cow.* s.l.:s.n.

Mitnick, K., 2017. *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data.* s.l.:s.n.

6. Appendix

Figure 1 demonstrates the type of 'malspam' which persuades the users into clicking such malicious links by using tempting languages like "Payment Details" or in the above case "View your receipt here.". If I were the one receiving the mail, I would have absolutely clicked on the link just because I was unaware and the link is very tempting for a normal user.

For it to stay relevant for this many years, it went through few updates to stay effective. The early versions of Emotet arrived with a JavaScript file. Likewise, in the later versions, it evolved to take use of macro-enabled documents which would fetch the virus payload from command & control servers which were run by the attack initiators.

Also, Emotet is very deceptive. If only it hadn't been less deceptive, the trend would have ended before it even started. It uses cunning tricks to hide from several kind of detection and prevention. For example, it would know if it was running inside a virtual machine or, VM and would lay dormant to detect a sandbox environment. It is used by a cybersecurity professional to observe malware's behaviors within a safe and controlled space. Hence, Emotet is very smart and deceptive to detect and analyze it. Not only that, it also receives constant updates using C&C servers without any outward signs which also enables attackers to install additional malwares in the system like banking Trojans seamlessly.

1.2 History of Emotet

Emotet was first identified by Joie Salvio, an experienced threat analyst who published her initial analysis on the malware on 27th of June, 2014. The 1st version of the malware was analyzed at first. Later on, the 2nd version of the Emotet was discovered with some improvements over the 1st generation (Securities, 2022).

The 2nd version used Automatic Transfer System (ATS) to instantly steal money from the accounts of victims, who mostly were a small number of German and Austrian Bank's clients. 2nd Version ceased its activity on 10th December, 2014 (Securities, 2022).

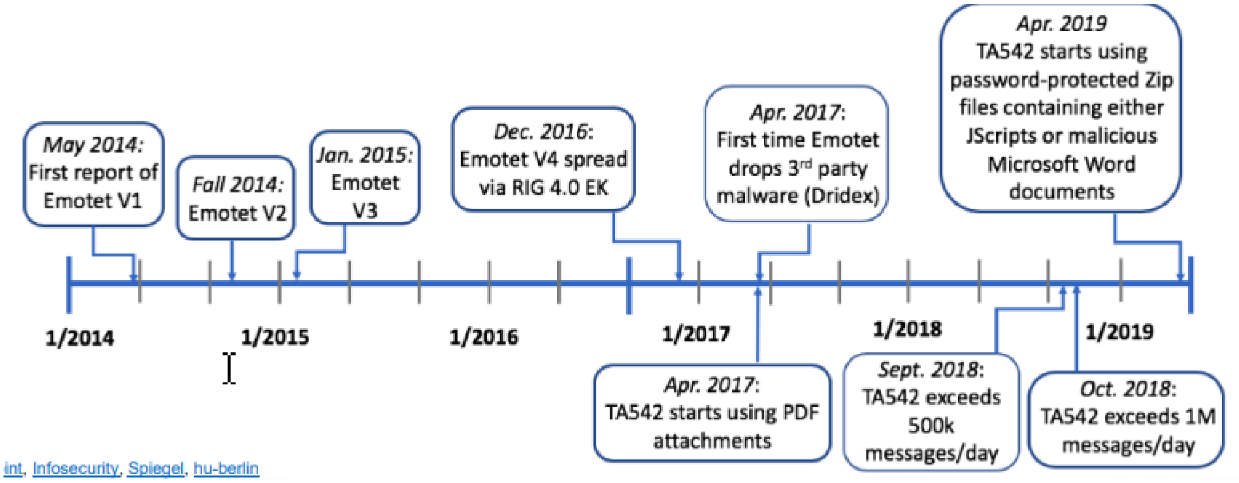
But soon, the 3rd version of the malware was released on the January of the next year, i.e., 2015 staying prominent on its undetectability and few other improvements as well including public RSA key and a partial cleanup of the ATS script and adding DDoS attacks and email login thefts to roster. The third version was a headache to the Swiss Banks and also German and Austrian Banks as well (Securities, 2022).

In 2016, the malware went through two notable phases. It was reconfigured to be a loader which would intrude a network and successively enable operators to deploy second-stage payloads. Secondly, it shifted its focus on Germany alone to keep a low profile (Securities, 2022).

The following year of 2017, Mealybug's Malware-as-a-Service (MaaS) took off which would deliver the IceID banking Trojan through the established infrastructure and Emotet was also seen distributing Trickbot Trojan and the UmbreCrypt Strain of ransomware expanding area of damage to countries like China, Mexico, Canada and UK (Securities, 2022).

As of 2018 and 2019, Emotet managed to gather quite a high-profile-victims. They ranged from local governments to private organizations including educational facilities and state institutions as well. Few notable infections are as follows:

- Allentown, Pennsylvania (13th February, 2018)
- Heise Online (13th May, 2019)
- Humboldt University of Berlin (29th October, 2019)
- Frankfurt, Germany (December, 2019)


May 2014: First report of Emotet V1
Fall 2014: Emotet V2
Jan. 2015: Emotet V3
Dec. 2016: Emotet V4 spread via RIG 4.0 EK
Apr. 2017: First time Emotet drops 3rd party malware (Dridex)
Apr. 2019 TA542 starts using password-protected Zip files containing either JScripts or malicious Microsoft Word documents
1/2014
1/2015
1/2016
1/2017
1/2018
1/2019
Apr. 2017: TA542 starts using PDF attachments
Sept. 2018: TA542 exceeds 500k messages/day
Oct. 2018: TA542 exceeds 1M messages/day

int, Infosecurity, Spiegel, hu-berlin

Figure 8 Timeline of history of Emotet (Anon., 2019)

More than 120 countries in the world are engaged in any of the form of International Privacy Laws for Data Protection in order to ensure the data of their citizens are rigorously protected and controlled. The EU General Data Protection Regulation (GDPR) is one of the toughest data protection regulations among the world and many companies abide by to it and are under it. The regulations focus on data protection from threats and also assists in mitigating the risks of fraud, corruption and it has become indispensable in the modern scenario (CNIL, 2022), (Thales, 2022).