Company Security Report

Name: Jakub Orlowski
Student ID: R00267077
Assigned Company Name: Cerberus Security

Abstract

In summary the purpose of this report is to educate the employees and management of Cerberus about the importance of cyber security and general security as a whole. The document outlines the purpose of security and how valuable it can be when it comes to protecting their valuable assets.

This document also contains a deep analysis of Cerberus' website. Proving flaws and showing that a strengthened security system must be put in place. In order to encourage this, Popular and dangerous malware was explained in the document, how it works, what the threat of it is, and why it would be capable of effecting Cerberus. Including how to remove and prevent this.

Digital footprinting is also outlined in the report, as well as social engineering and ways to minimise the threat that both can pose toward the company.

Cerberus has a very unsecured online presence. It is of high importance that the issues mentioned below are patched and fixed as they can have a detrimental effect on the Company's continuing wellbeing within the business. It is also indicative that the employees of Cerberus must be educated about the threat of social engineering and its dangers.

In conclusion the company is very vulnerable online, with 2 CVSS 7.5 vulnerabilities and with a unsecured website. It is advised that the company follows all the necessary steps to get rid of these issues. To continue operating with peace-of-mind.

Table of Content

Introduction

Task 1 (34 marks)

Company Overview

Cerberus is a Munster-based company, which offers a range of security services and training to private sectors and public sectors alike. The company was founded in 2008 and is currently led by Damian Romanowicz.

Cerberus offers a large range of security-based services, such as; Security personnel for hire, perimeter control, event security or guarding purposes. However, they also provide specialist security services ranging from risk assessments to test purchasing.

As a provider of such services, I believe it is key to create an always-present awareness of online security. A company providing any sort of security services should also be able to pride itself in its security, digital or not.

Figure 1. Cerberus Security Company Logo

Crown Jewels / Assets

To provide strong and confident security awareness, It is important that 2 of the 3 concepts in the CIA Triad are well understood. Those being Confidentiality, and, Integrity.

It is crucial to preserve authorized restrictions on information access and its disclosure, equally important is to ensure that the Integrity of our assets is impeccable at all times. Ensuring the modification or removal of any information is noted and kept safe under all circumstances so as to not risk any of our assets as mentioned previously.

Our company's key assets are the following;

~~Client Information~~

User information kept by our company is undeniably a very important asset we must keep safe. Our client's information is as important to us as it is to them, in nearly every regard. Instances of information such as names, addresses, billing information, bank details, and more are all extremely sensitive instances of information in our hands. By law, Cerberus is expected and required to keep this information private and gatekeep it, preventing any leakage of information whatsoever.

~~Personnel Information~~

A business is run by people, and those people are considered personnel, Just like the previously mentioned User/Client information, our personnel's information is just as important and requires just as much security. Information types between Client and Personnel overlap in a number of ways such as bank details or general identity information.

Under no circumstance can the personnel's sensitive information be leaked or spread without the explicit permission of the person in question and administrative oversight. Such events can cause cascading damages to the reputation of the company from both a potential client's point of view, as well as from a future employee's point of view.

~~On-Premises Devices/Equipment ~~

Business-owned devices and equipment are expensive and lucrative as they are key for the company to provide high-quality servers and preserve company data. A system compromise could possibly affect devices owned by the company either on-site or in the office where the company operates.

~~Security Controls~~

Security controls are a very sensitive data type that the company cannot lose or expose to the public or any other body. This could cause a compromise of data leading to cascading events which would open up other security risks for the company in many different sectors. Including but not limited to; Cyber security, on-site security, personnel safety, company integrity and confidentiality.

Four Websites for Details of Current Malware Threats

~~CrowdStrike~~ [1]

Crowd Strike is a must-read annual cyber security report, which provides incredible information about the malware threat trends and identified issues about the year of choice. Including cybercrime-enabling methods such as infiltration methods and malware delivery methods like "LUNAR SPIDER" and "APOTHECARY SPIDER" along with search engine poisoning.

The report also provides information on where intrusions are most popular, by region and by industry, A example of this year's data would be that 23% of interactive intrusions were toward the technology industry and 15% toward the telecommunications industry.

It explains how interactive intrusions work and are carried out and how an interception can be done. It also has up-to-date statistics for Access Broker advertisements by month.

~~ The Hacker News ~~ [2]

The Hacker News is an up-to-date, informative website about the most recent cyber attacks and critical vulnerabilities. With 8,000,000 monthly readers, this news site and optional newsletter are considered to

be a trusted and reliable news source. They provide links to their social media where they update the latest cyber news actively/
The Hacker News also provide courses and webinars for cyber security awareness and preventative methods and how to apply such. Such good resources should be considered for the company as the cyber security grounds are like an ever-lasting arms race.

~~CheckPoint~~ [3]
CheckPoint is a website that provides a lot of information about different particular malware, analyses them and gives a general overview of how things work. CheckPoint is also a cybersecurity company. Based on its very high-quality information and reputation, it is a very reliable source when it comes to finding out about the most recent threats. Especially when it comes to this year's or last year's reports. As they provide in-depth reports each year similar to CrowdStrike mentioned previously.

~~Dark Reading~~ [4]
Dark Reading is very similar to The Hacker News, it focuses on vulnerabilities and threats while also providing information on how to stay safe online. It's an informational resource that is used and posted by CyberSecurity experts. Dark Reading also provides a newsletter that you may subscribe to, in order to get the most up-to-date information about Cyber-Security.

Eight identified Malware

1. ***LokiBot*** - Trojan [5][6]
   -Justification and Description-
   Lokibot is a Tojan first discovered and documented in 2016, Since 2020 however it has seen a significant drop in use, however it remains the fourth most popular information stealing malware out there according to CheckPoint's 2023 Cyber Security Report. Loki bot primarily targets Windows and Android systems, the goal being to sneak into the system without being noticed and proceeding to steal data, such as bank details, login information and the likes. It does this by having the functionality of a keylogger, being able to save any and all key presses on the device of the infected user. It has also been known to run pop-up ads to be gain revenue and also create backdoors into the infected system to allow for follow up attacks. My justification of this malware is that Cerberus is very susceptible to drive by downloads and man in the middle attacks due to their unsecure website and their exposed File Transfer Protocol service (FTP).

   -Risk Analysis of Threat-

Upon further research into LokiBot, the primary way it makes its way onto a victim's computer is by using known vulnerabilities within windows document files. Which happen to exist in Ceberus' case. Due to Cerberus using WordPress. Microsoft Azure offers a way to easily manage wordpress websites, by extension this allows an attacker to utilise known vulnerabilities such as CVE-2022-30190 which is a remote executable code vulnerability. Due to Cerberus having a exposed FTP service and a unsecure website. A drive-by-download may be utilised by a attacker to force a file that contains LokiBot onto a device.

-Type of Threat-

The threat of LokiBot is considered to be Critical in terms of severity due to it opening backdoors, and stealing sensitive data off of a infected machine. A potential residue vulnerability after the removal of LokiBot could potentially allow worse threats to come into contact with the company.

-How to remove it-

In the case that LokiBot has been loaded onto a machine. It is recommended to quarantine the device all together and take it off of any internet connection. Then running a up to date antivirus program which would be able to remove the Trojan. Due to the nature of Trojans, it is a good idea to teach staff about phishing practices and how to avoid them as LokiBot is often spread with malicious files sent via email or text. In this particular case it wouldn't be necessary to do that from a attackers perspective as they could simply utilise the already very present vulnerabilities within Cerberus' website.

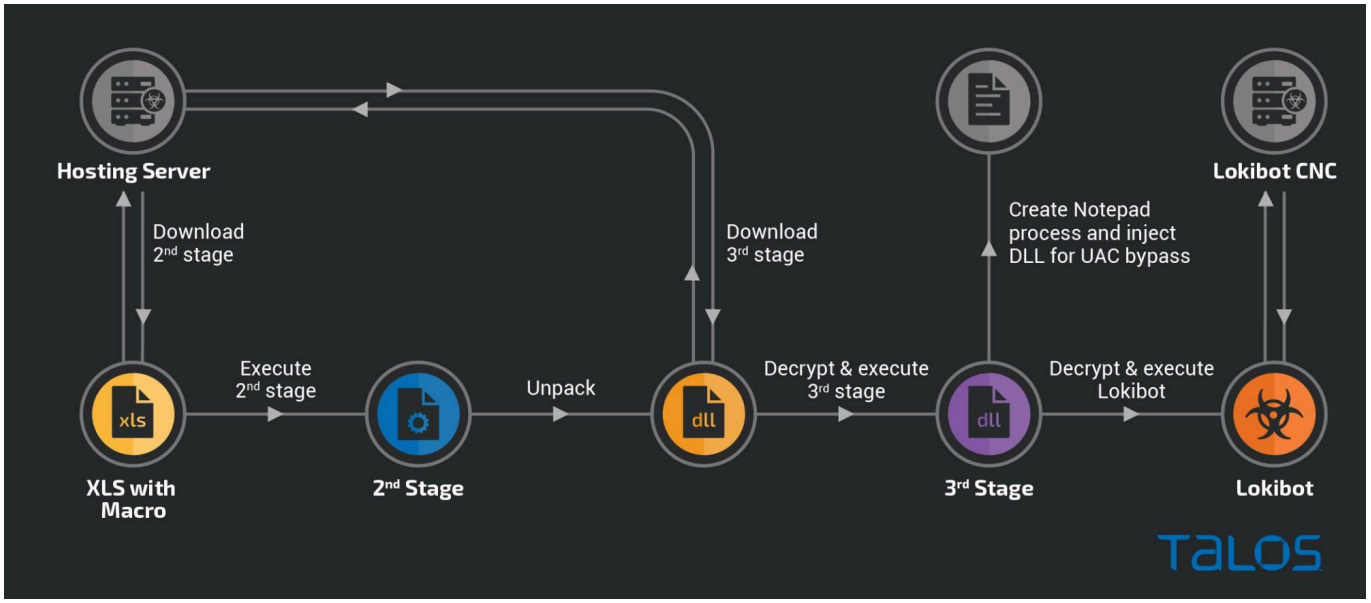

Figure 2. Lokibot infecrion chain

2. ***Phorpiex Malware*** - Worm // BotNet [8][9]

-Justification and Description-

Phorpiex is a very well established botnet, used for phishing attacks, malware delivery and cryptomining on infected machines. The primary function of this malware is to get onto a system and syphon it's resources enabling the attacker to make a monetary gain and free machine power. The malware responsible is sometimes referred to as "Trik". It is a computer worm which can spread throughout a network without any user interaction. It is known to create backdoors to infected devices and downloading more malware and stealing information. It is quite commonly spread using XSS (Cross Site Scripting). Once again due to Cerberus' website being unsecured it makes it very vulnerable to such a injection attack which could carry the worm.

-Risk Analysis of Threat-

Due to Phorpiex being a worm, the primary threat is the spread of the worm onto every other machine in the network. This could severely impact the integrity of the company and its confidential information as Phorpiex can be used to steal data as mentioned previously. Due to it being also a downloader and a backdoor. It could potentially lead to other malware being installed on all of the infected machines, or potentially leading to a ransomware attack.

-Type of Threat-

Phorpiex is a significant threat in its own right, being able to spread horizontally through a network, steal information and lead clients that go onto Cerberus' website to also be infected causing a cascading effect of infections. This could damage the company reputation if it already hasn't been done by the malware itself. The real threat from Phorpiex comes with its downloader and backdoor capabilities. Being able to harm the company more through other means than itself.

-How to Remove it-

Due to Phorpiex being a worm. It would be necessary to potentially quarantine the entire network and machines connected to it. Run deep scans on each machine and completely clear the network ensuring no residuals are left. As if a single machine remains infected and reconnects to the clean network. The worm will be unleashed once again. Running a up to date antivirus software, keeping a firewall active only allowing downloads from certain IP addresses would be key for this. Also securing the website by using the secure HyperTextTransferProtocol.

Figure 3. Phorpiex process graph

3. ***QBot // QakBot // QuackBot*** - Banking Trojan [7][10][11]

-Justification and Description-

QBot is a banking trojan that is still to this day a incredibly prevalent and dangerous threat to organizations and businesses and has become one of the leading banking trojans on a global scale. QBot is always under development with more techniques and capabilities being added with time. The primary purpose of QBot is to steal banking data and session information when in banking sites. The developers have also enabled it to spread other malware on infected machines. Therefore also working as a downloader. The most popularly downloaded malware through QBot happens to be ransomware.

-Risk analysis of threat-

QBot is a massive threat to any business, as its key purpose is to steal banking credentials. Causing a company to suffer and its clients also. Due to its high activity and it being listed as a most wanted malware on CheckPoint's list of Wanted Malware of May 2024. It is very likely that it may find its way into Ceberus' network. Due to QBot being constantly changed and reworked it is difficult to defend against the malware itself. As it can come again with different code and different actions. QBot often is distributed using phishing mails or infected files. Clicking such a file would cause it to wreck havoc on the machine. It has also been spotted as a malware that is dropped via malware that is already on a machine.

-Type of Threat-

The typical behaviour presented by QBot is Password brute-forcing, Registry Manipulation, moving through a network and collecting personal information via keylogging. Due to it also being used as a backdoor and downloader, the threat level of this malware would be considered Critical.

-How to remove it-

Simply running an up to date antivirus and quarantining the infected machine should do the job. However, to prevent this from happening in the first place. The best course of action would be to educate employees about phishing scams and instructing the use of a file scanner before downloading anything from a email with a attachment.

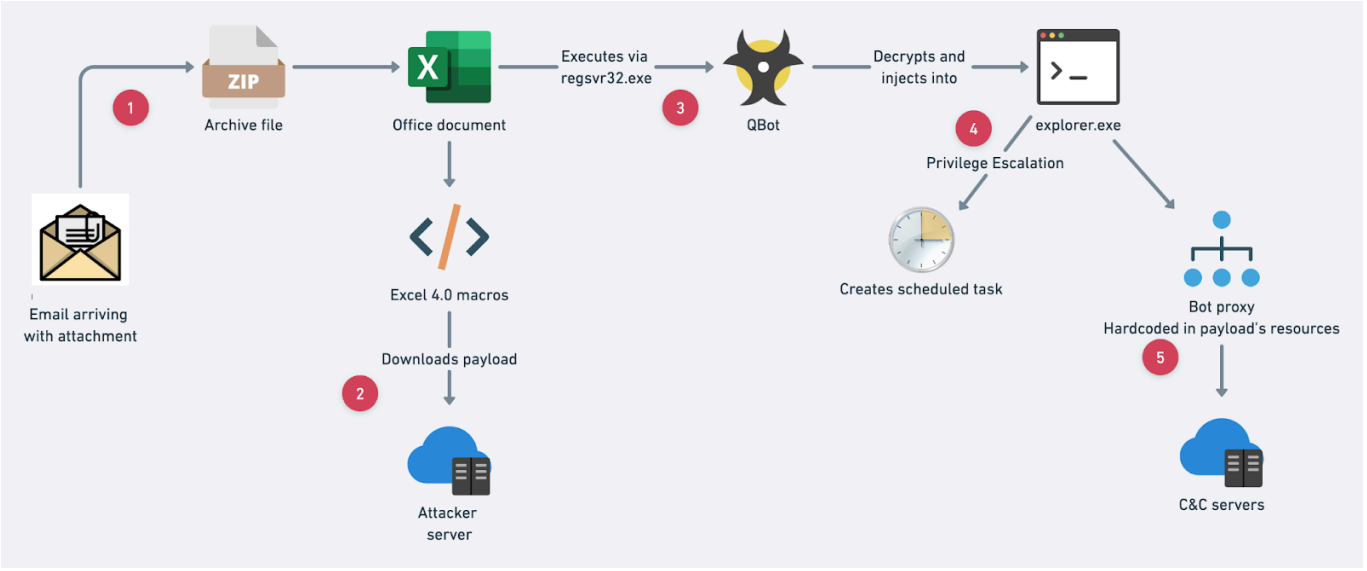

Figure 4. Qbot Attack Map

4. ***Whitesnake Stealer*** - Information Stealer [12][13][14]

-Justification and Description-

WhiteSnake Stealer is a very sophisticated .NET information stealer which was used to steal browser information and personal information. However as of recent it has been modified, with not being able to target windows and linux platforms. The primary reason Ceberus is susceptible to such a malware is because of their unsecure website. The threat of WhiteSnake Stealer is far too great to justify ignoring it's presence.

-Risk Analysis of Threat and Type-

WhiteSnake stealer is a significant threat to all of the above mentioned assets. It is capable of avoiding Virtual Machines by using a particular type of code. Making research on the threat very difficult from a professional point of view. However SonicWall has managed to provide very solid information about the malware. The first action the WhiteSnake stealer takes is to scour the machine for web browsers, FTP clients and cryptocurrency wallets. By doing this it then decides on what to steal. Being able to steal any of the following: Cookies, Autofills, Login Data, History

and Webdata. The malware has a particular way to trick the person using the machine. Once initially ran, it will copy itself into the %appdata% folder and delete the original file without a trace. Possibly leading the user to disregard the occurrence. It then is scheduled to run every minute.

On top of all of this, the stealer takes screenshots of possibly important pages, keylogs when particular specifications are met. It can eaves drop using your microphone and spy using your webcam. It also allows for remote access to the device. As a whole. This is the biggest threat possible. This puts whitesnake stealer in the catastrophic category of databreach.

-How to remove it-
Due to its good obfuscation, The whitesnake stealer most likely will never be detected until after the damage has been done. This means that educating personnel about the importance of careful scanning of files before downloading is key. However due to the unsecure and public FTP service that Cerberus has. The prevention should be first to plug the vulnerabilities such as the FTP situation and the unsecure website. To prevent Drive-By-Downloading the malware or a Man-in-the-middle attack where the malware is downloaded unknowingly.

5. ***"Fake Updates"*** *Also known as:* ***"SocGholish"*** - RAT (Remote Access Trojan) [15][16]
-Justification and Description-
Socgholish is a malware variant that act likes a RAT and like a Trojan-Dowloader. It was first discovered in 2018. The malware is delivered to systems via compromised websites by injection malicious Javascript. This could be considered XSS, which Cerberus', as i have mentioned before, is particularly vulnerable to, due to an unsecured website. The malware is associated with a Russian CyberCrime group called "Evil Corp", it is speculated that the group would sell remote access to compromised machines to third parties which could cause a large scale information leak or the download of further malware which would compromise the company further.

-Analysis of Threat-
The primary threat of Socgholish is its very unassuming and effective infection method. by entering an infected website a popup or prompt would show up asking you to update your browser. Upon clicking this the download would run a malicious javascript code. This would allow socgholish to do what it's made for. Which is to download more malware, and provide remote access to the attacker enabling remote malicious code execution. Socgholish is known for its affiliation with ransomware and information stealers, such as Dridex or even WhiteSnake Stealer mentioned previously. The threat posed would be put into the category of High. The true threat of the malware is entirely up to the decision of the attacker.

-Type of Threat-

The threat that Socgholish poses is one that could either do nothing to the victim or completely ruin the system affected or even the network due to its remote access capabilities. Being able to forge emails or communications or modify any file without people knowing is an incredibly high threat. Not only that but if the machine has administrative access funds can be transferred or clients may be susceptible to malware if socially engineered through the guise of Cerberus.

-How to remove-

Removal of Socgholish is quite difficult, using up to date antivirus software is a good start however if the attacker gets ahold of the machine they can ensure that it will not be detected before the software is run. The best preventative method is to ensure that websites visited by company machines are filtered. Also securing the Cerberus website would be an ideal choice to not infect clients or personnel. As it is evident that staff use the website by the presence of staff login.

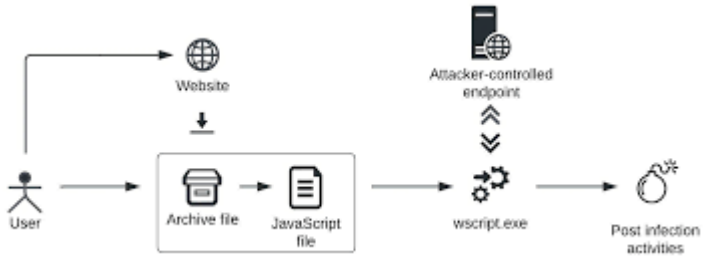

Figure 5. Infection Map Socgholish

6. ***Glupteba*** - Trojan [17][18]

-Justification and Description-

Glupteba is a trojan malware that was listed as a top ten most wanted and prevalent malware of 2021. After injecting the system it is used as a backdoor to install more malware and to steal authentication details such as the authentication cookie within browsers. Over time Glupteba has evolved into a botnet. Enrolling infected machines into a crypto mining botnet and steals as much available hardware resources as possible. It is commonly downloaded via “free” “desirable” software. Either from torrent sites or otherwise. Once installed, Glupteba opens a backdoor on your machine which allows the attacker access to your machine. It uses the HTTP protocol to contact the attackers C2 servers,[19] allowing it to protect the data, encrypting it and hiding it among legitimate traffic.

-Analysis of threat-

The threat of the Glupteba trojan is that it is capable of account takeover by stealing information from infected machines and authentication cookies from the browser. Cerberus is vulnerable to this theft due to its critical risk of having a unsecure website. In addition, the infection of a device can be brute forced via the open FTP service that is public. Due to this a attacker can conduct a man-in-the-middle attack exploiting this obvious weakness to modify files and inject the trojan

directly. Forcing the download of the malware and thereby downloading the malware with nobody knowing any better.

-How to Remove-

The core way to deal with Glupteba is using a firewall to prevent downloads from unknown sources. Preventing the installation in the first place. Due to Glupteba's popularity, many antivirus databases have the characteristics of this malware allowing most antivirus software to remove it if successfully detected.

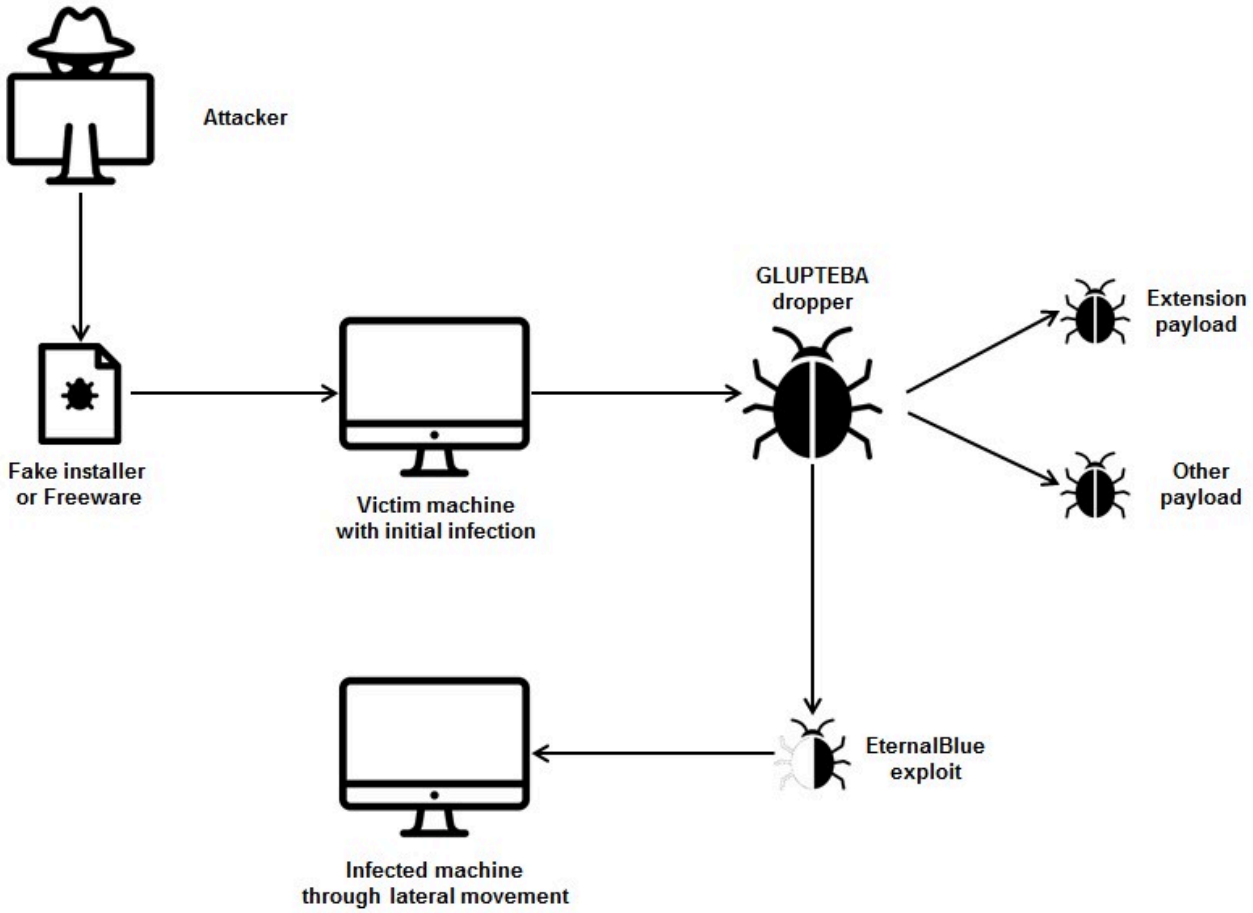

Figure 6. Infection Map Glupteba

7. ***SpinOk*** - Mobile Spyware Trojan [7][20]

- Justification and Description-

SpinOk is a mobile malware that is made in particular for the Android powered devices, It is a spyware that after infection, collects and returns information to the attacker. SpinOk disguises itself as an ad and a software development kit. Once installed on a user's device, SpinOk operates as spyware. Analysing and collecting data, including the gyroscope and magnetometer data to determine if it is in an emulated environment, if it is, it goes dormant. The purpose of the malware is to make money off of selling the stolen data to 3rd parties. Cerberus might be vulnerable to this

if they ever decide to try develop a app and fall for the inconspicuous software development kit that happens to be infected.

-Threat Type-
The threat posed by SpinOk is that it can completely devastated Cerberus' confidentiality, by stealing key information and selling it. This could include names of clients, their banking details or locations of individuals. This is a very high security breach that should be always taken into consideration

-How to Remove it-
It is crucial for the employees to know the difference between a company owned device and their own. They should not attempt to use devices that belong to the company as their own. MDM (Mobile Device Management) is handy here. In the case of company owned devices. This could completely prevent the chance of the malware infecting the device as it will not be permitted to be downloaded by a user. Intentionally running the device in an emulated environment is also a good idea since SpinOk will not activate. Then running routine scans could effectively remove a dormant instance of the malware.

8. ***NanoCore*** -Remote access trojan (RAT) [21][22]
-Justification and description-
NanoCore is a second stage malware, Meaning it establishes a C2 connection on the victims device. It is a remote access trojan which allows the attacker to execute malicious code remotely.
NanoCore usually infects via infected Microsoft Office Documents such as word files, presentations and so on. However it has been seen in .zip files or even .iso files allowing it to evade end point security.[23] NanoCore allows full control over a victim's device which allows keystroke logging, webcam access and access to any information on the device that isnt administration locked. In the case that the administrator device has been compromised, any and all files are accessible to the attacker. Due to Cerberus' open FTP service, files can be directly uploaded to the network allowing very easy infection onto devices.

-Threat Type-
The type of threat NanoCore poses is very similar to that of Socgholish, mentioned earlier, which is a catastrophic level of danger. Allowing an attacker to completely take apart a company at their will. However this is also subjective to the attackers intentions. Due to them having full control over what to do.

-How to Remove it-
Removing NanoCore would be difficult due to the fact that the attacker can establish methods to come back if it is removed such as various backdoors. The best method of defense would be to

install a firewall preventing suspicious and unauthorised files to be downloaded onto company devices. Patching the FTP and making it encrypted would do a good job aswell.

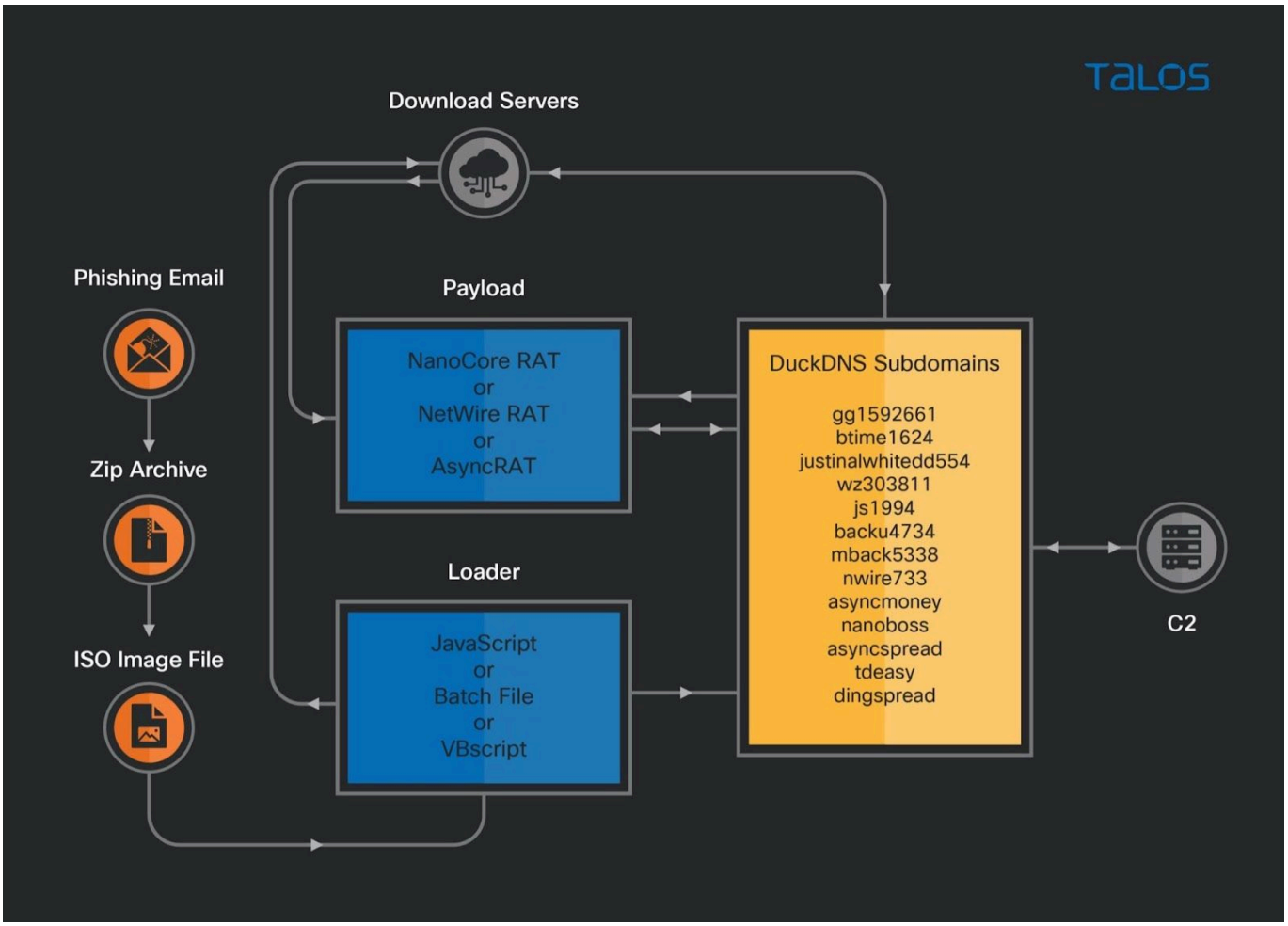

Figure 7. NanoCore Infection Map

Ransomware Overview

Ransomware is one of the scariest malware for any and all enterprises, As its purpose is to lock up and encrypt important information and then demand a ransom, typically in Bitcoin or another cryptocurrency, to unlock and release the information again. Usually, once the ransom is paid, the attacker goes AWOL and does not do anything to decrypt or return the stolen and locked-up data. Leaving a corporation in the dust completely. The EternalBlue exploit which has been used by the WannaCry ransomware allows the ransomware to move through a network similar to a worm in a way, then once a certain condition is met, all infected machines are encrypted and locked.

Ransomware usually has a lot of different attack types, Utilising many vectors such as phishing emails with infected attachments or toxic URLs, Exploits such as the above-mentioned EternalBlue or exploits within desktop apps such as Office or the Microsoft email app.
Ransomware, Petya//NotPetya is responsible for crippling a British Advertiser WPP group, which cost $ 18 billion in revenue, and the aforementioned WannaCry ransomware managed to infect over 300,000 computers in 150 countries including the UK NHS which included 1.7 Million employees.

Task 2 (33 marks)

Digital Footprinting, Methods and How Employed

A digital footprint is information that exists online about an individual, corporation or business. A part of your digital footprint would be something like your LinkedIn page or Instagram account. Everything put up on the internet that is in some way related to you is your individual digital footprint. A company that created a big positive digital footprint effectively puts itself in the spotlight for buyers and clients, but also in the crosshairs of cybercriminals. Allowing anyone to sniff and find any and all information, some of which can hint at important company directives, and decisions, or even reveal weaknesses within the infrastructure of the company.

Digital Footprinting is a method in which an attacker utilises OSINT (Open Source Intelligence) such as Instagram posts, Job offers, and LinkedIn profile information of any individual in the company. This can be used to understand and plan a better attack by being more familiar with the Company's personnel and its technology.

When it comes to a single individual's Digital Footprint, That is already being processed and taken in by companies you agree to work with. Such as Google or any website that you allow to use cookies.
There are two types of Digital Footprint;

- Active Digital Footprint, where the individual provides all the information intentionally and willingly, such as uploading photos or videos.
- Passive Digital Footprint, A passive footprint is significantly more subtle, this consists of cookie data, search data and results and settings regarding apps or websites

A company always wants to be more known, that is the purpose of advertising. One method utilised is having a website, Good search engine optimisations can make a company's or individual's presence on the internet much stronger. Increasing their digital footprint. Cerberus however does not have the best internet presence, the website used does not contain many meta tags and is unsecured, browsers rank this website lower making it more difficult to find.

Identified Company Weaknesses

- Unsecure Website

i. The first thing I noticed is that the communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network.

ii. The risk is that an attacker who manages to intercept the communication a the network level can read and write or even modify the data transmitted including credit card information, security tokens, authentication tokens, passwords and others

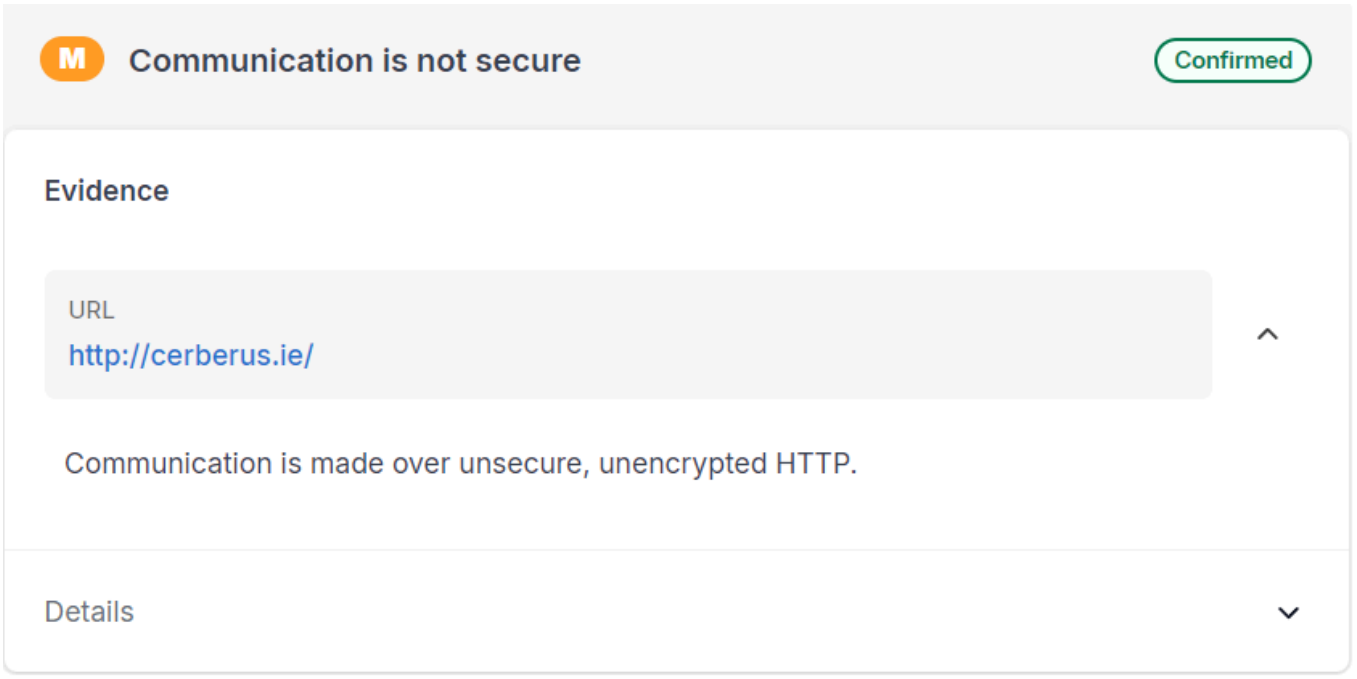

Figure 8 . Unsecured Website Evidence

- FTP service exposed to the internet

i. I have managed to detect a publicly accessible File Transfer Protocol (FTP) service.

ii. The FTP service enables the transfer of files and information, upload and download from a server. Nonetheless, there is no provided encryption within this service

iii. This allows for attackers to utilise man-in-the-middle attackers leaking potentially sensitive information that Cerberus would not like to have revealed. Potentially breaking the confidentiality and integrity of the information held by Cerberus

Figure 9. Publicly Accessible and Unsecured FTP

- Revealed Interesting Information

i. Lastly, I'd like to note that the website provides interesting information when looked through such as "License.txt" –http://cerberus.ie/license.txt– which states the version of WordPress used, this allows attackers to search for vulnerabilities within the website.

ii. Finding exploits for WordPress is not a difficult task, If the version of the software is known it allows for significantly easier breaching.

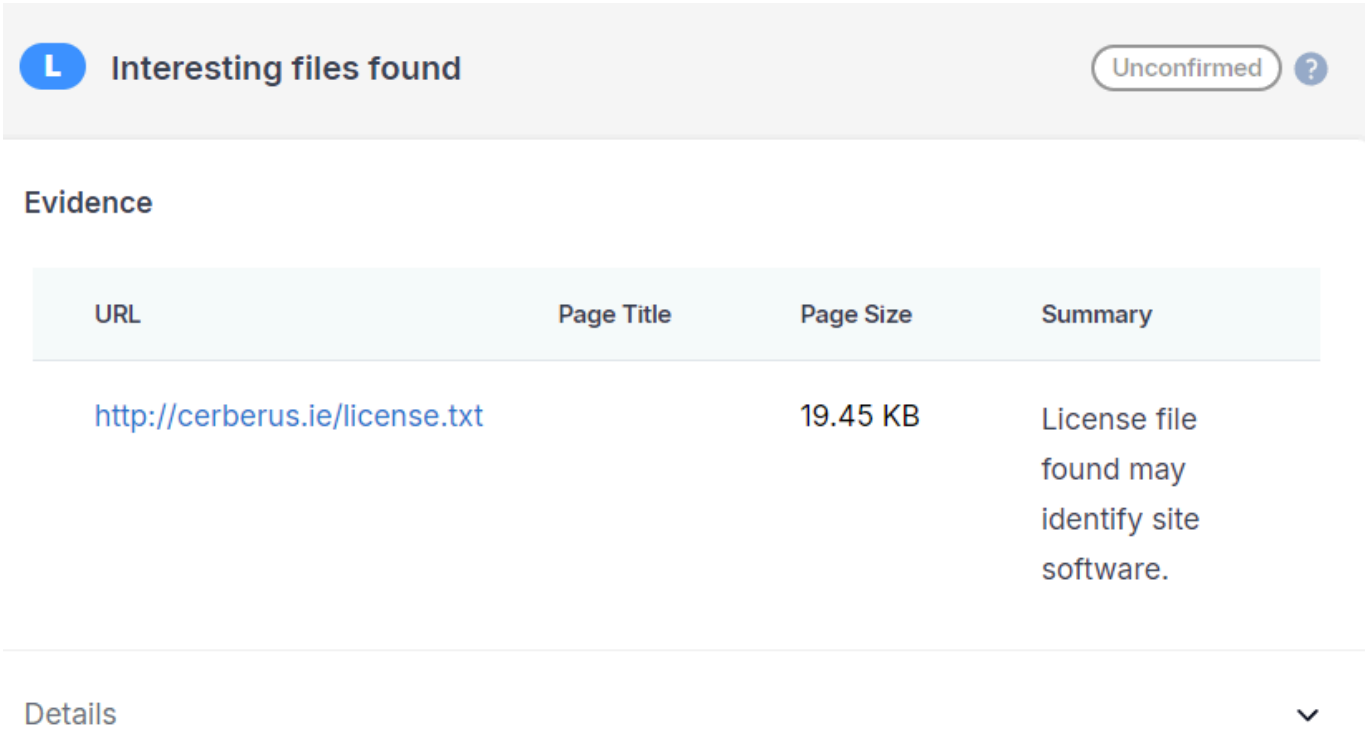

Figure 10. Publicly exposed License.txt file
http://cerberus.ie/license.txt

Solution to Identified Company Weaknesses

- Solution - Unsecured Website [24]

Ceberus' main weakness is the unsecured website they utilise, Therefore this should be of the highest priority when it comes to improving the company's cyber security. The way to cover up this weakness is incredibly easy.

Cerberus Security must purchase an SSL certificate,[25] ensure all their website configurations are compatible with the HTTPS protocol then simply complete the migration. It is key to update the website for Google search engine optimisation to increase the visibility to potential clients looking to use the service.

It is key that Cerberus takes action and updates its website protocol to secure, as otherwise the website is exposed to XSS and other possible hostile attacks launched by malicious bodies.

- Solution - Publicly accessible FTP service

As mentioned above, The FTP service does not provide any encryption. The best solution for this would be to implement the use of a Virtual Private Network (VPN) that mandates two-factor authentication. If this solution for whatever reason is not a possibility, the other two solutions to this would be by only permitting certain IP addresses to use the FTP service by utilising a firewall. The other valid option would

be to switch to using a Secure File Transfer Protocol (SFTP) which would provide adequate amounts of encryption to the data transfers.

- Solution - Revealing Interesting Information [26]

As I have stated above, The website exposes some "Interesting" files, in this particular case it was License.txt which stated the version of Wordpad the website uses. Information like this allows easier attacks to be mounted against the server. Manual validation of such files is required. As such Cerberus should check any and all exposed files such as the one mentioned previously and ensure that anything containing sensitive information is hidden or restricted from public access.

Extending Company Policy to Social Networking

It is key that the company security policy extends to social networking. Employees must be sure that whatever they post, and where is appropriate and does not violate the company policies. Furthermore, extending the company policy will ensure that the integrity and confidentiality of the business is not at risk at any stage.

An important policy is to maintain the privacy of sensitive data. Keeping everything confidential. Employees should not be sharing any sensitive information or secrets online regardless of who it is targeted toward. Employee information, Client information, site locations, patrol swap timings and banking information should at no stage ever have a presence online apart from within in the Cerberus confidential and secure network. A leak in this information could lead to the business being dissolved or being prosecuted under GDPR. GDPR also known as General Data Protection Regulations regulate breaches of information and can be used as a foundation in a lawsuit. For this exact reason, it is key that every employee is trained under GDPR standards.

It is important that employees of Cerberus do not speak out about political or sensitive issues online while also representing the business. As this could lead to a bad Public Reputation for the company, This also extends vice versa, the Cerberus company should avoid announcing their views as this could cause outrage and bring Cerberus into the crosshairs of cybercriminals.

Task 3 (33 marks)

Social Engineering Overview and Effects on Assigned Company

Social Engineering is a term that is used to categorise typically malicious activities that include human interaction. It utilises the human attack surface, human error, and empathy to trick another person into making security mistakes or revealing sensitive information.

Social Engineering is quite complex, and often is a coinflip, if the victim is aware of this and is careful, social engineering will not work. Social engineering takes more than one step, Normally involving reconnaissance about the victim, and gathering personal information that is available publicly. Also known as OSINT. This would include the name of someone close or someone in a higher position, to typically be able to convince the victim that they are trustworthy. Knowing weak points of entry such as this allows the attacker to move on to the next steps. Using the gathered information to gain the victim's trust. Usually, the victim would be coerced into believing an urgent story, becoming the sheep in the interaction so that the attacker has control over what is said and what the topic is.
Over the duration of the conversation, the attacker would fish for information that could slip from the victim, or potentially set up the person to elaborate or reveal sensitive data. Once what is needed by the attacker is gained, the attack would end in a casual manner so that it would not arouse suspicion.

Social engineering is an incredibly dangerous attack as with the right information and words used by the attacker, The victim might make critical mistakes by either thinking what they are doing is right or by thinking they are speaking with higher authority and therefore must do as told. This could lead to leaks in critical data or even a transfer of funding.

There are many different types of methods that may be employed within a social engineering interaction. One of the most popular would by far be phishing campaigns. Those are the emails or texts you get from your bank asking you to click a suspicious link and log in because something went wrong. Or by scaring you that you must take action now.

Defence against such attacks is quite simple, it is simply to educate the employees about social engineering and how it works to prevent any leaks in the first place. Explaining what spear phishing is or scareware.
A good safety net would also be to set up multi-factor authentication, such as using Google's auth app [28] to prevent access to people who are not permitted. Securing logins to core applications via IP whitelisting can also be done using a firewall.
[27]

Physical and Digital Authentication Best Practices

~Physical Access Authentication~

Best practices for Physical and Digital Authentication tend to be pricey however it is almost required in some cases. Cerberus security, a manned security company is expected to have good authentication in their own buildings let alone at clients'.

Physical access control security (PACS) is a type of security method that is used to restrict access to parts of, or the entirety of an area, property or building. Access control ensures that people who are not permitted to be in a certain area are not in there. Preventing intruders, robberies and the likes. Usually, basic security can be employed via installing a PIN system by a door or entrance. Only people with the particular code would be able to get in, however. As mentioned in the section above, information via social engineering is quite easy to get access to. Therefore using something like an entry card that uses NFC technology is better. As only a certain amount of those would be given out. Ideally, the card would have a unique code within it, so that if the card is lost. The code can be changed for that particular person and a new one can be provided. Rendering the lost access card obsolete.

Physical access control plans and systems can be linked directly to a network and accessed remotely by someone with administrative permission. Allowing the trigger of lockdowns in the event of an emergency, either by locking all the doors to keep someone inside, or unlocking all of them in the event of an emergency, for example, a fire. The access cards being specific to each individual would also allow for the tracking of locations so that in the event of an evacuation. An efficient role call can be used with the knowledge of who was and was not in the building. This extends further to even burglary and theft and whether it is an internal problem or not.
[29]

~Digital Access Authentication~ [31]

Digital authentication is the process of verifying the identity of a person or device that attempts to interface with a system, network or application through the internet. Most people know what this is, As everyone have some kind of password for something, pin or some even have biometric access authenticators on their phones with fingerprints.

Those are basic methods of authorizing access to a service online, however digital authentication is also the first line of defence against cyber attacks, and hence they are commonly targeted by cyber criminals, and for that exact reason it is a very good idea to have more authentication factors, namely 2FA also known as 2 factor authentication. Which would include sending the user a text with a code or message to confirm if it is really them logging in.

In special cases, where very sensitive and confidential data is in question. MFA may be used, that being Multi-Factor authentication. Where it is required to use more than 2 different independant verification elements to grant access. This would commonly be seen in the government. Where multiple people must approve of providing access to a certain service or data.

Another good idea that commonly over laps with physical access control would be to have biometrics included. Such as a Iris Scan,[30] facial recognition technology or fingerprint technology.

User Verification Recommendations against Physical Access

User verification is an excellent way to ensure no unauthorized access is granted to private premises. A very strong recommendation is to utilise biometric data such as an iris scan or fingerprint authorization. Utilising those is safer than using plastic badges or keycards as you cannot misplace such a thing. Enabling this also grants information on who has gone into the building and if they have left.

The use of AI is a very good idea if the company can afford it. Allowing for anomaly detecting, like if someone is in a place where they shouldn't be, or even analysing tail-gating by detecting if the amount of people who have entered the premises is equal to that of the number of keycards or "verified entries".

Automating as much as possible is the key to physical access as it minimises human error which is, as mentioned before, the biggest attack surface when it comes to data breaches, whether this is through physical theft, digital attacks or manipulation with social engineering.
[32]

References (IEEE Format)

[1] CrowdStrike, “CrowdStrike 2024 Global Threat Report | CrowdStrike,” crowdstrike.com, Aug. 07, 2024. https://www.crowdstrike.com/global-threat-report/

[2] The Hacker News, “Researchers discover command injection flaw in Wi-Fi alliance’s test suite,” The Hacker News. https://thehackernews.com/2024/10/researchers-discover-command-injection.html

[3] “Cyber Security Report 2023 | Check Point Software.” https://pages.checkpoint.com/cyber-security-report-2023.html

[4] D. R. Staff, “Microsoft: Healthcare sees 300% surge in ransomware attacks,” Oct. 24, 2024. https://www.darkreading.com/cyberattacks-data-breaches/microsoft-healthcare-300-percent-surge-ransomware-attacks

[5] Michali, “Lokibot malware,” Check Point Software, Jul. 18, 2022. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/lokibot-malware/

[6] “LokiBot campaign targets Microsoft Office document using vulnerabilities and macros | FortiGuard Labs,” Fortinet Blog, Jul. 12, 2023. https://www.fortinet.com/blog/threat-research/lokibot-targets-microsoft-office-document-using-vulnerabilities-and-macros

[7] "June 2023's Most Wanted Malware: Qbot Most Prevalent Malware in First Half of 2023 and Mobile Trojan SpinOk Makes its Debut - Check Point Software," Check Point Software, Feb. 14, 2024. https://www.checkpoint.com/press-releases/june-2023s-most-wanted-malware-qbot-most-prevalent-malware-in-first-half-of-2023-and-mobile-trojan-spinok-makes-its-debut/

[8] "BSI - Phorpiex," BSIWEB. https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/Phorpiex/phorpiex_node.html

[9]Michali, "Phorpiex Malware," Check Point Software, Sep. 19, 2022. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/phorpiex-malware/

[10] O. Yaakobi, "QBot Malware: What is it and how does it work," Datto, Apr. 16, 2024. https://www.datto.com/blog/qbot-malware-what-is-it-and-how-does-it-work/

[11] Gmcdouga and Gmcdouga, "May 2024's most wanted malware: Phorpiex Botnet unleashes phishing frenzy while LockBit3 dominates once again," Check Point Blog, Jun. 10, 2024. https://blog.checkpoint.com/research/may-2024s-most-wanted-malware-phorpiex-botnet-unleashes-phishing-frenzy-while-lockbit3-dominates-once-again/

[12] F. Fkie, "WhiteSnake Stealer (Malware family)." https://malpedia.caad.fkie.fraunhofer.de/details/win.whitesnake

[13] "White Snake stealer attacks Windows & Linux systems to steal login credentials," cybersecruitynews.com. https://cybersecuritynews.com/white-snake-stealer-malware/

[14] SonicWall, "WhiteSnake Stealer: Unveiling the latest version – Less obfuscated, more dangerous," SonicWall, Mar. 18, 2024. [Online]. Available: https://blog.sonicwall.com/en-us/2024/03/whitesnake-stealer-unveiling-the-latest-version-less-obfuscated-more-dangerous/

[15] "SoCGholish - Red Canary Threat Detection Report," Red Canary, Apr. 17, 2024. https://redcanary.com/threat-detection-report/threats/socgholish/

[16] Netalit, "Socgholish malware," Check Point Software, Jan. 14, 2024. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/socgholish-malware/

[17] F. Fkie, "Glupteba (Malware family)." https://malpedia.caad.fkie.fraunhofer.de/details/win.glupteba

[18] Michali, "Glupteba malware," *Check Point Software*, Sep. 19, 2022. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/glupteba-malware/

[19] "What are command & control (C2) servers?," *SentinelOne*, Sep. 13, 2024. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-are-command-control-c2-servers/#:~:text=C2%20servers%20send%20commands%20to,reconnaissance%20on%20the%20target%20environment

[20] Netalit, "SpinOk Malware," *Check Point Software*, Aug. 14, 2023. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/spinok-malware/

[21] "What is nanocore?" https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/nanocore

[22] Global Security Mag Online, "December 2023's most wanted malware: The resurgence of QBot and FakeUpdates – Global Security Mag online," *Global Security Mag Online*, Jan. 10, 2024. https://www.globalsecuritymag.com/december-2023-s-most-wanted-malware-the-resurgence-of-qbot-and-fakeupdates.html

[23] "What Is Endpoint Security?," *Trellix.com*. https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-security/

[24] R. C. Writer, "Learn why and how to convert your site from HTTP to HTTPS," *Rock Content*, May 24, 2023. https://rockcontent.com/blog/convert-http-to-https/

[25] "What is an SSL certificate?," *Cloudflare*. https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/

[26] "OWASP Top Ten 2017 | A6:2017-Security Misconfiguration | OWASP Foundation." https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

[27] R. Masas, *What is Social Engineering | Attack Techniques & Prevention Methods | Imperva*. 2023. [Online]. Available: https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Social%20engineering%20is%20the%20term,in%20one%20or%20more%20steps

[28] "Get verification codes with Google Authenticator - Android - Google Account Help." https://support.google.com/accounts/answer/1066447?hl=en&co=GENIE.Platform%3DAndroid#:~:text=The%20Google%20Authenticator%20app%20can,in%20to%20your%20Google%20Account

[29] "Physical Access Control System (PACS): Components + examples," *Avigilon*, Sep. 24, 2024. https://www.avigilon.com/blog/physical-access-control

[30] "Iris Recognition: Biometric Authentication | NEC," *NEC*. https://www.nec.com/en/global/solutions/biometrics/iris/index.html

[31] T. LegalProd, "Digital Authentication," *LEGALPROD*, Feb. 15, 2024. https://www.legalprod.com/en/digital-authentication/#:~:text=Digital%20authentication%20is%20the%20first,intrusions%2C%20protecting%20their%20critical%20resources

[32] "How to prevent unauthorized Physical access in the workplace | LEnELS2," *LenelS2*. https://www.lenels2.com/en/news/insights/How_to_Prevent_Unauthorized_Access.html