Networking and Security – Cyber Threats

Contents

Introduction

This report covers sophisticated threats in computer networks and security, starting with social engineering. This type of attack exploits human psychology and trust in order to manipulate individuals (usually employees of the target company) into giving access to sensitive information or performing actions for attackers.

On the other hand, attackers carry out DoS and DDoS attacks with an aim to disrupt the availability of essential services or networks by overwhelming the target company's servers with malicious traffic, causing downtime, financial loss, and reputational damage.

This report delves into each of these types of cyberattacks, including how they are carried out, the effect it has on the target company and how companies can better protect their data, employees and reputation by minimalizing the threat of these attacks.

Social Engineering

Illustration 1

What is Social Engineering?

Social engineering is the manipulation of individuals to gain unauthorized access to information or systems. It often relies on psychological tactics, as opposed to traditional 'hacking' methods which use technical means; this can make it much harder to defend against as it is usually easier to exploit a person's natural inclination to trust than it is to hack software. Attackers are often exploiting human behaviour and trust to trick people into taking action for them or revealing confidential information to enable them to bypass security measures. Cybercriminals used social engineering techniques in 20% of all data breaches last year* (Aura, 2023).

The 4 stages to a Social Engineering attack

There are usually 4 main stages to a social engineering attack:
Information Gathering, Attack Planning, Attack Execution and Attack Report.

Information Gathering

In this stage, the attacker aims to collect as much information as they can. The information they are looking to access is about the target or organization that they are planning to exploit, which usually includes details about the company's organisation structure which can give the attackers more information about the employees' roles and responsibilities which in turn can help them to identify which employees will have access to key databases as well as other systems and information that the attackers are interested in.

Attackers also look into the technical infrastructure of the company's systems and investigate further to find as many of the security measures that may cause problems for them during the later stages of the social engineering attack. (Tripwire, 2023) It is not rare for attackers to not restrict themselves to using just the target company and its systems for reconnaissance; they will often dig much deeper into individual employees via their social media profiles to attain any further information they can to form a better understanding of the person.

This information can also be gathered from the company's websites, search engines by using dorks or more sophisticated and possibly intrusive kali tools, WHOIS Protocol and public reports. This information can be key to 'hacking' into the employee's psychology in order to get them to behave a certain way and perform actions for the attacker's benefit.

Attack Planning

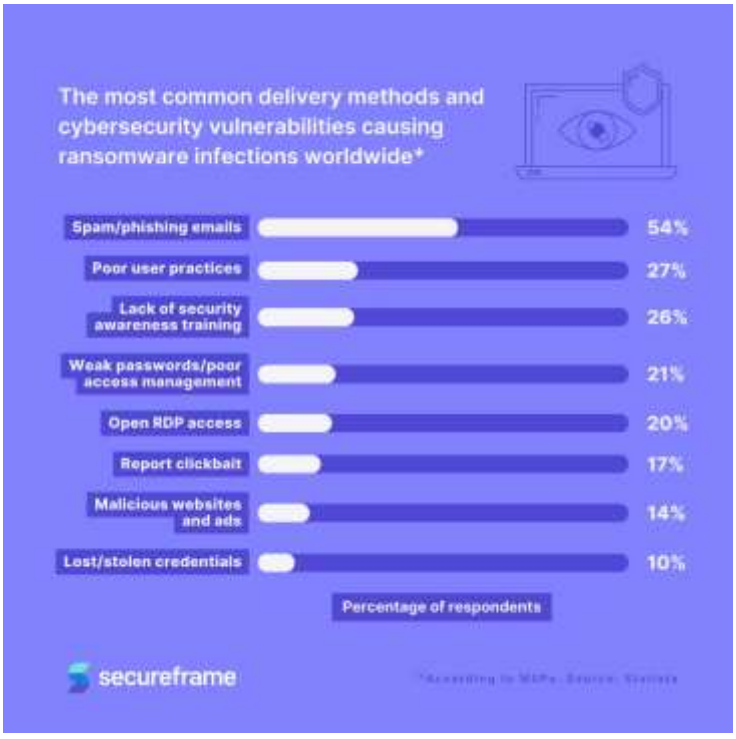

Figure 1 (Secureframe, 2023, July)

Once the attacker has compiled enough evidence about the target company and has an overview of the company's security measures, key employees, employees with access to certain systems, they will start to plan the attack. Using all of the aforementioned information that they have gathered; they will determine the weak points of the company and use this conclusion to work on the best approach to form an attack. (Tripwire, 2023) This includes choosing between the most affective social engineering techniques and evaluating a perfect target by looking deeper into the employees. Once a target (or targets) has been chosen for the social engineering attack, the attackers will work on crafting a false scenario to manipulate the target into giving them sensitive information or performing actions for them. They will take the information gathered from the information gathering stage into account and identify potential challenges with each of the strategies they have devised.

Attack Execution

In this stage, the attacker works on putting their plans into action. They are now very much ready to devise a way to contact the target employee. This often, but not always, involves cold calling the employee, sending phishing emails, creating a new social media account to resemble someone close to the employee (using information gathered in the information gathering stage) or many of the other tactics that are used for deception. (Tripwire, 2023)

The attacker will now follow the plan that they have previously devised and make contact with the employee and whilst doing so they will use psychological tactics to manipulate the target's emotions to firstly build trust. It is this trust that enables the attacker to control the employee's actions and allows them to blindly follow the attacker's instructions. Employees can give out critical information including, but not limited to system information, passwords, access to keycards or taking action on behalf of the attacker all whilst thinking they are working to benefit the company.

Attack Report

As soon as criminals complete their mission, they'll vanish with as little evidence as possible. The average time to detect a cyber-attack or data breach is close to 200 days, so you won't even know what's happened until they're long gone. (Aura, 2023, para 5).

The attack report stage is where the attacker will make sure that they are able to maintain access to the systems/networks they have worked to gain access to. As well as this, they will try to cover their tracks by ensuring that nothing regarding the attack can be linked to them, including all contact with any employees, and they can do this by slowly reducing the contact they have with the employee as to not raise suspicion. They will delete any possible records of

their actions that can be traced back to them by deleting any data logs (user history) from the identity concealing services or methods that they have used including VPNs.

They can also monitor the activities within the company if they have gained access to their network and services to see if any red flags have been raised or if their access has been revoked entirely. If not, then they are able to maintain their connections and attempt to further exploit any and all information that they can for their malicious activities that they have planned which can include planning another attack.

How you can keep yourself safe from social engineering attacks

Firstly, you should familiarise yourself with hoe to recognise social engineering attacks.

Some of the key measures that you should take are to:

Check email addresses, speak to the IT team to ensure that any suspicious emails are verified – get a second opinion if you are unsure, don't click on suspicious links and contact the sender directly. Organisations should be conducting regular phishing testing to identify areas that need improvement and educating employees to ensure that they understand the importance of the security protocols that are in place.

DoS Attacks

DoS stands for Denial of Service.

DDoS stands for Distributed Denial of Service.

A DoS attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network. This is done by overwhelming it with a flood of illegitimate (artificial) traffic. Most services become overwhelmed from DoS attacks, which sends this flood of traffic from one single source. The goal for DoS attacks is to make the targeted system/server overwhelmed and therefore unavailable to its usual traffic, making it inaccessible for them.

In DoS attacks the malicious traffic originates from a single source, which is where the flood of traffic is sent from by the attacker(s). This traffic floods the target with an excessive amount of traffic (usually much more than the system's usual traffic). (Imperva) This consumes a lot of the resources such as CPU power, memory and bandwidth, causing the server to initially slow down until it eventually crashes and becomes unresponsive for all visitors, including the legitimate traffic.

DoS attacks are usually short lived. Some of the common types of DoS include saturating devices which include malicious injection of excessive workload or traffic, including connection

flooding and Syn flood. Syn flood exploits the 3-way TCP handshake process by sending a flood of connection requests without completing the handshake, which eventually exhausts the target's resources. HTTP flood floods the target with a high volume of HTTP requests, and Ping flood floods the target with ICMP Echo Request (ping) packets. The key goal of all DoS attacks is to exhaust the server's resources to cause a denial of service.

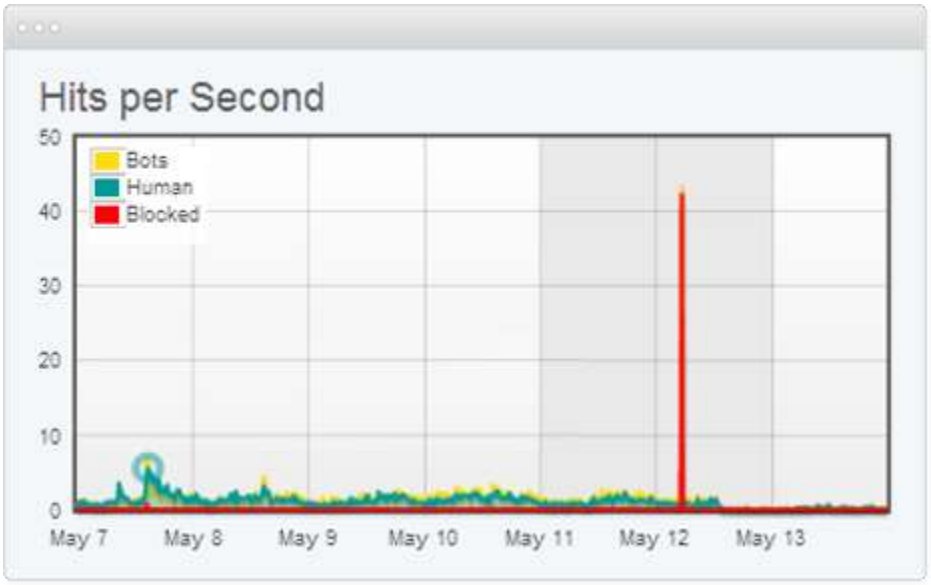

Illustration 2 (imperva.com)

DDoS Attacks

A DDoS attack is a more sophisticated version of a DoS attack.

The attacker plants trojans on a number of target machines. These target machines attacked by trojans are known as zombies. The attacker harnesses a network of these zombie machines to launch coordinated attacks against a single target, with each zombie launching a separate DoS attack, and these attacks are combined to form one DDoS attack. (Imperva)

DDoS attacks involve a large number of compromised devices. This can include computers, servers, IoT devices, or even smartphones and this is collectively known as a botnet. (Imperva) The attacker then gains control of these devices to launch DDoS attacks to disrupt the servers that are targeted. Just like with DoS attacks, the key goal of all DDoS attacks is to exhaust the server's resources to cause a denial of service, using multiple devices instead of just the one.

Impact of DoS/DDoS Attacks

DoS and DDoS attacks are simple but extremely powerful attack mechanisms which are an immense threat to the internet community affecting many services around the world. These attacks can render websites, online services and networks to become unavailable for users. This downtime can cause great financial losses for the company/organisation that is targeted. Ongoing and extensive periods of downtime can damage a company's reputation and the break the trust that they have built with their consumers. This can lead to financial losses for the company as their productivity takes a halt during these periods of inactivity caused by DoS/DDoS attacks. (ResearchGate, 2017)

Conclusion

In summary, while DoS/DDoS attacks can disrupt services effectively with minimal technical skills, they carry significant legal risks and have temporary impacts. (ResearchGate, 2017) On the other hand, social engineering attacks can bypass technical security measures but depend heavily on human factors and raise ethical considerations. All of the Cyberattacks mentioned in this report require careful consideration of risks and consequences by potential attackers.

Companies looking to protect themselves from such attacks must implement network security measures by deploying firewalls and intrusion detection in their systems and utilise rate-limiting mechanisms to ensure that the traffic flow is maintained with load balancing, which will help alleviate the risk of a flood of requests crashing their servers. Employees must be provided with comprehensive training programs to educate them of the risks of social engineering attacks and make them aware of how their interactions could pave the way for an attacker gaining access to the company's sensitive data and systems.

References

- Joe Pettit, Tripwire (2023, March 1) **Social Engineering: Definition & 6 Attack Types**

https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for

- Todd Jones (2023, December) **The 12 Latest Types of Social Engineering Attacks (2024)**

https://www.aura.com/learn/types-of-social-engineering-attacks

- Illustration 1 (2013, March) **Royalty Free picture**

https://www.istockphoto.com/

- Table 1, Secureframe (2023, July) **Emily Bonnie, Rob Gutierrez - 60+ Social Engineering Statistics for 2023**

https://secureframe.com/blog/social-engineering-statistics

- Illustration 2, references Imperva **Learning Centre - DDoS Attacks**

https://www.imperva.com/learn/ddos/ddos-attacks/

- ResearchGate - A survey of distributed denial-of-service attack, prevention, and mitigation techniques (2017) **Tasnuva Mahjabin, Yang Xiao, Guang Sun and Wangdong Jiang**

https://www.researchgate.net/publication/321775189_A_survey_of_distributed_denial-of-service_attack_prevention_and_mitigation_techniques