Main Types of Cyberattacks

Cycle d'ingénieur Génie Informatique

Presented by : Zaid Baarab And Oussama Belqars

Module: Cryptographie et Sécurité Informatique

November 22, 2024

PLAN

1. Introduction
2. Main Types of Cyberattacks
   - Phishing
   - Malware
   - Denial of Service (DoS/DDoS)
   - Force Brute et Credential Stuffing
   - Man-in-the-Middle (MITM)
   - Exploitation de Vulnérabilités (Zero-Day)
3. Advanced Cyberattack Techniques
   - Social Engineering
   - Ransomware
4. Practical Demonstration
5. Conclusion
6. Références

Introduction

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks. It involves implementing technologies, processes, and controls to defend against threats like unauthorized access, data theft, and system damage.

Why is Cybersecurity Important?

- Protects Sensitive Data
- Ensures Business Continuity
- Mitigates Financial Losses
- Updates and Patches
- Builds Trust

Main Types of Cyberattacks

Definition

Cyberattacks exploit system vulnerabilities to gain unauthorized access, steal data, or disrupt services.
According to securite.developpez.com, global cyberattacks increased by 38 percent in 2022.
Understanding the main types of these attacks is essential to recognizing potential threats.

Some main Types of Cyberattacks:

- Phishing
- Malware
- DoS/DDoS
- Brute Force and Credential Stuffing
- MITM
- Zero-Day

Phishing

Definition

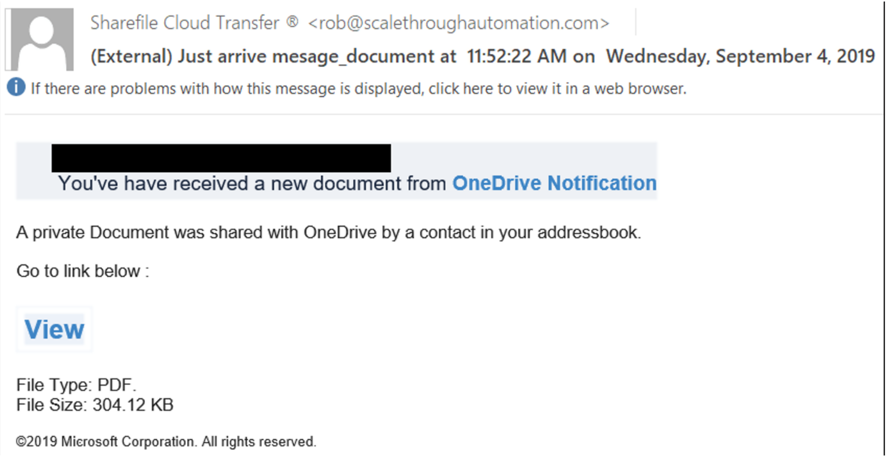
Phishing is a cyberattack that uses deceptive emails, messages, or websites to trick individuals into providing sensitive information such as passwords, credit card numbers, or personal details.

Common Phishing Tactics:

- Email Phishing
- Spear Phishing
- Smishing and Vishing

Objective: To gain access to personal information, financial data, or login credentials, which attackers can then use to commit fraud or infiltrate systems.

Phishing Examples



Sharefile Cloud Transfer ® <rob@scalethroughautomation.com>

(External) Just arrive mesage_document at 11:52:22 AM on Wednesday, September 4, 2019

If there are problems with how this message is displayed, click here to view it in a web browser.

[redacted]

You've have received a new document from OneDrive Notification

A private Document was shared with OneDrive by a contact in your addressbook.

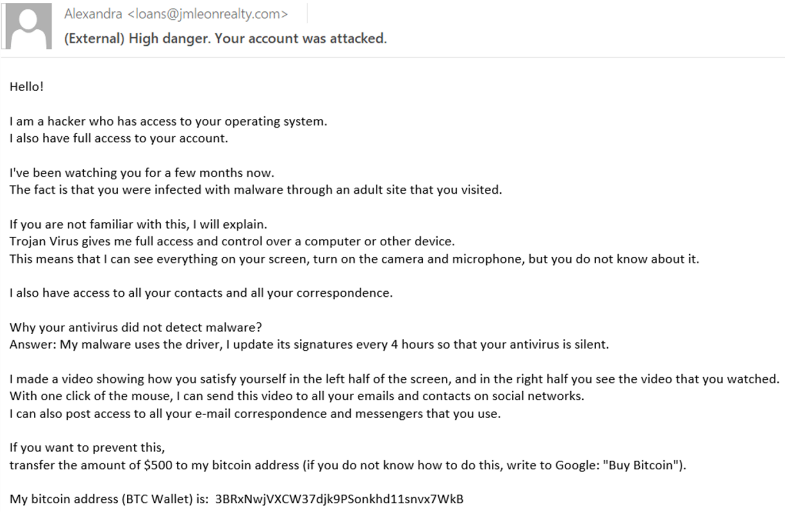
Go to link below :

File Type: PDF.
File Size: 304.12 KB

©2019 Microsoft Corporation. All rights reserved.

Figure: Phishing Example 1

Phishing Examples



Alexandra <loans@jmleonrealty.com>

(External) High danger. Your account was attacked.

Hello!

I am a hacker who has access to your operating system.
I also have full access to your account.

I've been watching you for a few months now.
The fact is that you were infected with malware through an adult site that you visited.

If you are not familiar with this, I will explain.
Trojan Virus gives me full access and control over a computer or other device.
This means that I can see everything on your screen, turn on the camera and microphone, but you do not know about it.

I also have access to all your contacts and all your correspondence.

Why your antivirus did not detect malware?
Answer: My malware uses the driver, I update its signatures every 4 hours so that your antivirus is silent.

I made a video showing how you satisfy yourself in the left half of the screen, and in the right half you see the video that you watched.
With one click of the mouse, I can send this video to all your emails and contacts on social networks.
I can also post access to all your e-mail correspondence and messengers that you use.

If you want to prevent this,
transfer the amount of $500 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin").

My bitcoin address (BTC Wallet) is: 3BRxNwjVXCW37djk9PSonkhd11snvx7WkB

Figure: Phishing Example 2

Malware

Definition

Malware (malicious software) is any software designed to harm, exploit, or otherwise compromise devices, networks, or data.

Common Types of Malware:

- Viruses : Attach to files and spread between devices, often causing damage to systems.
- Worms : Self-replicating programs that spread across networks, often without user action.
- Trojan Horses : Disguised as legitimate software but contain malicious code to exploit systems.
- Spyware : Monitors user activity to collect sensitive information.
- Adware : Delivers unwanted ads, often slowing down devices or invading privacy.

Objective: To gain unauthorized access, steal data, damage systems, or disrupt operations.

Other types of malware

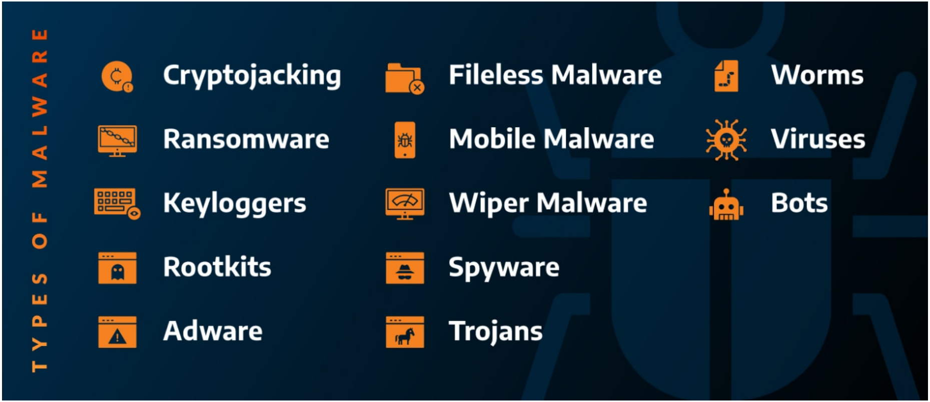


Figure: Other types of malware

Denial of Service (DoS/DDoS)

Definition

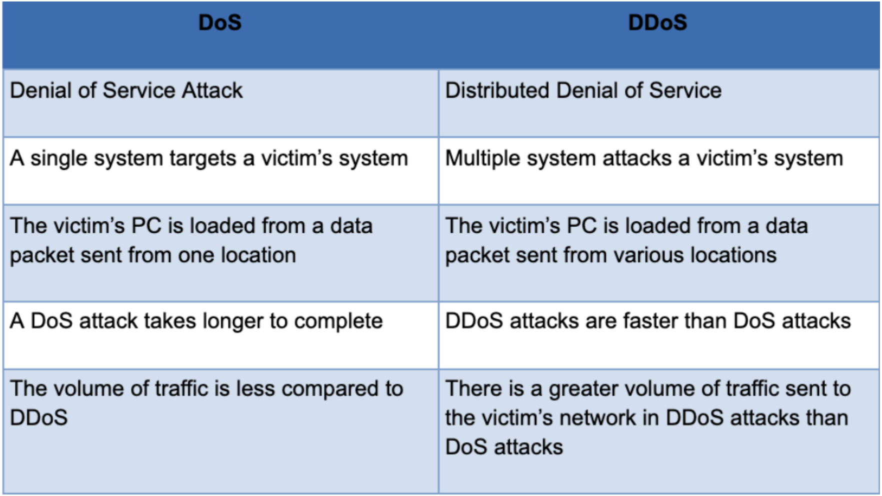
DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks aim to make a network, service, or website unavailable by overwhelming it with a flood of traffic or requests.

Key Types:

- **DoS Attack:** A single source floods the target with excessive requests, causing slowdowns or crashes.
- **DDoS Attack:** Multiple compromised systems (often a botnet) launch a coordinated attack, making it harder to block and defend against.

Objective: To disrupt services, cause downtime, damage reputation, or incur financial losses for the target organization.

Difference between DoS and DDoS



DoS	DDoS
Denial of Service Attack	Distributed Denial of Service
A single system targets a victim's system	Multiple system attacks a victim's system
The victim's PC is loaded from a data packet sent from one location	The victim's PC is loaded from a data packet sent from various locations
A DoS attack takes longer to complete	DDoS attacks are faster than DoS attacks
The volume of traffic is less compared to DDoS	There is a greater volume of traffic sent to the victim's network in DDoS attacks than DoS attacks

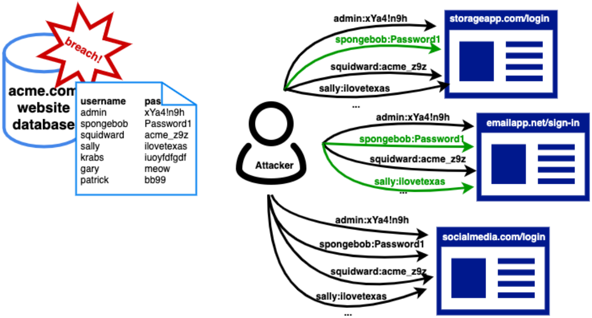
Figure: Difference between DoS and DDoS

Credential stuffing

Definition

Credential stuffing is the automated injection of stolen username and password pairs ("credentials") into website login forms, with the aim of fraudulently accessing user accounts. Since many users reuse the same password and username/email, when these credentials are exposed (through a database leak or a phishing attack, for example), submitting these stolen credential sets on dozens or even hundreds of other sites can allow an attacker to compromise those accounts as well.

Credential stuffing



username	pas
admin	xYa4!n9h
spongebob	Password1
squidward	acme_z9z
sally	ilovetexas
krabs	iuoyfdfgdf
gary	meow
patrick	bb99

Figure: credential stuffing schema

Credential stuffing

Techniques Of Protection

- Secure Password Policies: Encourage the use of unique and complex passwords
- Multi-Factor Authentication (MFA): Adds an extra layer of security beyond just the password.

Man-in-the-Middle

Man-in-the-Middle

is a type of cyberattack where a malicious actor intercepts and potentially alters communication between two parties who believe they are directly communicating with each other. In an MitM attack, the attacker places themselves between the victim and the entity they are trying to communicate with (like a website, server, or another user) and can eavesdrop, steal information, or modify the data being transmitted.

Man-in-the-Middle

How MitM Works

.

- **Interception:** The attacker sets up a fake Wi-Fi hotspot in a public space, often without requiring a password. When a victim connects to this hotspot, the attacker can intercept any online data exchanges, such as emails and website logins.
- **Positioning between victim and destination:** The attacker uses techniques like IP spoofing, where they alter IP packets to impersonate the victim's computer system and redirect the victim to the attacker's website.
- **Decryption :** Through techniques like HTTPS spoofing, SSL hijacking and SSL stripping, the hacker decrypts the intercepted data, making the victim's activity visible to the attacker.

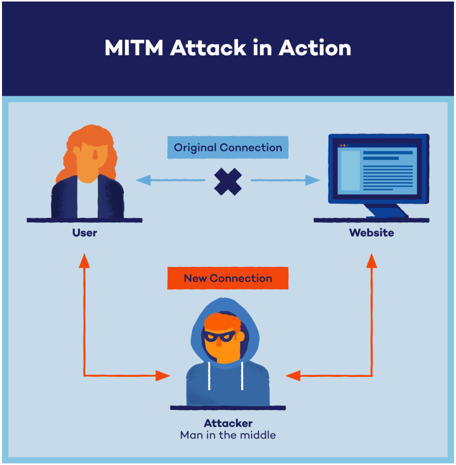


Figure: Man-in-the-Middle Attack

Zero-Day exploit

Definition

The term Zero-Day vulnerability refers to a flaw in software or hardware that is unknown to the vendor or developer, meaning that no patch or solution is available at the time the vulnerability is discovered. The term "zero-day" comes from the fact that the developer has had zero days to address the vulnerability once it becomes known.

Characteristics Of Zero-Day

Unknown Vulnerability

A zero-day vulnerability is a flaw or weakness in software that has not yet been disclosed or patched by the vendor. It is unknown to the public or developers, making it a significant security risk.becomes known.

Characteristics Of Zero-Day

Immediate Threat

Once discovered by an attacker, a zero-day vulnerability can be used to launch attacks before the vendor has the chance to fix the issue. This makes zero-day exploits particularly dangerous.

Characteristics Of Zero-Day

High value:

Zero-day exploits can have significant value on the black market. Attackers can sell these exploits to other criminals or nation-states, leading to increased exploitation of the vulnerability.

Famous Zero Day Attacks

Stuxnet

Stuxnet : is malware which targeted Microsoft Windows machines running Siemens SIMATIC software for managing Programmable Logic Controllers (PLC) that automated, monitored, and operated physical assets including amusement parks, building alarms, chemical plants, energy pipelines, factory assembly lines, and nuclear power plants. Stuxnet infected more than 200,000 computers across the world including 14 industrial sites in Iran, damaged over 1,000 centrifuges in the Natanz facility that were essential to Iran's covert uranium enrichment program intended for developing nuclear weapons

Advanced Cyberattack Techniques

As cybercriminals become more sophisticated, they employ advanced techniques that are harder to detect and defend against. These attacks are often targeted, persistent, and can cause significant damage to both individuals and organizations. In this section.

we will cover two such techniques :

- Social Engineering.
- Ransomware

Social Engineering

Definition

Hacking using social engineering is the practice of manipulating individuals into revealing confidential information or granting access to systems, often by exploiting trust, psychology, or human error rather than technical vulnerabilities. Social engineering relies on deception, persuasion, or impersonation to trick targets into divulging sensitive data, such as passwords or financial information, or performing actions that compromise security. Examples include phishing, pretexting, baiting, and impersonation, where attackers create convincing scenarios to make the target feel comfortable or obligated to comply with requests

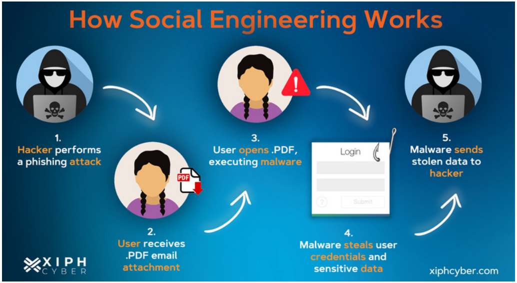

How Social Engineering Works
1.
Hacker performs a phishing attack
2.
User receives .PDF email attachment
PDF
3.
User opens .PDF, executing malware
Login
Submit
4.
Malware steals user credentials and sensitive data
5.
Malware sends stolen data to hacker
XIPH CYBER
xiphcyber.com

Figure: Social Engineering

Ransomware

Definition

Ransomware is a type of malicious software that encrypts or locks a victim's files, demanding a ransom payment for their release.

How It Works:

- **Encryption:** The attacker encrypts files, making them inaccessible without a decryption key.
- **Ransom Demand:** Victims are presented with a ransom note, typically demanding payment in cryptocurrency to restore access.
- **Double Extortion:** Attackers may also threaten to leak sensitive data if the ransom is not paid.

Objective: To extort money by holding data hostage, often causing financial, operational, and reputational damage.

WannaCry Ransomware and Its Impact

Overview:

- WannaCry hit in May 2017, exploiting the SMB vulnerability (EternalBlue).
- It affected 230,000+ computers across 150+ countries.

Impact:

- $4 billion in damages.
- Disrupted hospitals, telecoms, and businesses worldwide.

Figure: WannaCry Ransomware

Practical Demonstration: Ransomware Impact

Setup:

- Use a Virtual Machine (e.g., VirtualBox) in an **isolated and controlled network environment.**
- Install a fresh Operating System (e.g., Windows), ensuring no internet or host access.

Steps:

1. Execute a **ransomware simulation tool** or study case data (e.g., Wannacry simulation).
2. Observe file encryption, ransom notes, and changes in system behavior.

Objective:

- Analyze the **impact and behavior of ransomware** in a secure, ethical environment.

Conclusion

Conclusion

Cybersecurity is essential in our interconnected world to protect sensitive data, ensure operational continuity, and mitigate financial losses. Understanding the different types of cyberattacks, from phishing and malware to advanced threats like ransomware and social engineering, is key to building effective defenses.
By staying vigilant and understanding evolving cyber threats, individuals and organizations can maintain trust and resilience in an increasingly digital world.

Références

- URL : https://www.kaspersky.com/resource-center/threats/ransomware-wannacry https://www.kaspersky.fr/resource-center/definitions/firewall
- URL : https://www.accountablehq.com/page/the-difference-between-dos-and-ddos-attacks
- URL : https://www.hostinger.fr/tutoriels/iptables: :text=Iptablekjtcjgvg
- URL : https://linux.goffinet.org/certifications/securite/
- URL : https://github.com/Explodingstuff/WannaCry
- URL : https://chatgpt.com/

thank you