ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

AN INFORMATION GUIDE

Break Threats Chain

Why are we the targets

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Discussion points

Key topics covered in this presentation

- Malicious Software[Malware]
- Phishing
- Insider Threats
- Denial of Service[DoS] and Distributed Denial of Service[DDoS]
- Man-in-the-Middle[MitM]
- Weak Authentication and Password Attacks

Why attackers are interested in me?

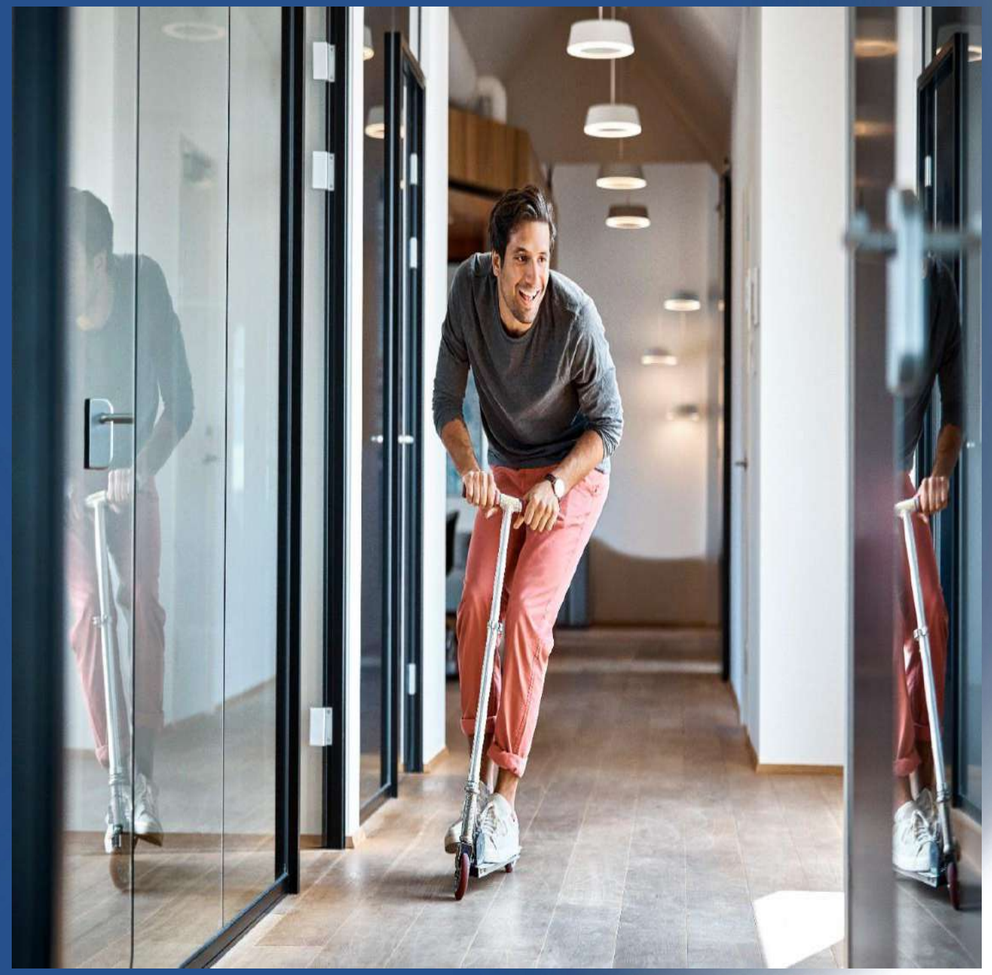
- Credit card & Financial Data
- Computer Resources
  - Advertising
  - Ransomware
  - Jump point
- User or Email Credentials
  - Sending Spam
  - Recovery/Reset other accounts
  - “More” access
- Medical Data
  - Prescription, insurance, or identity fraud
  - Far more valuable than financial data

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union



The Importance of Cybersecurity and Security Technology

Technology alone cannot protect you from everything.
Attackers go where security is weakest.

People are a link in the security chain and the FIRST line of defence.
A MUST to reduce cybersecurity risk.

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Malicious Software
“Malware”

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

The ease of getting infected by Web Malware

Step 1

Entry Point

You access a hijacked website and the malware downloads silently

Step 2

Distribution

The initial malware redirects an exploit server using fast-flux techniques

Step 3

Exploit

Commercially available and supported exploit packs will attempt to leverage vulnerabilities

Step 4

Infection

The malware downloads a malicious payload that will steal data or extort money from you

Step 5

Execution

Malware calls home with sensitive data like credentials, banking or credit card information

ncc.cy
NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Malicious Software “Malware”

What is malware and how can I defend against it?

Malicious Software

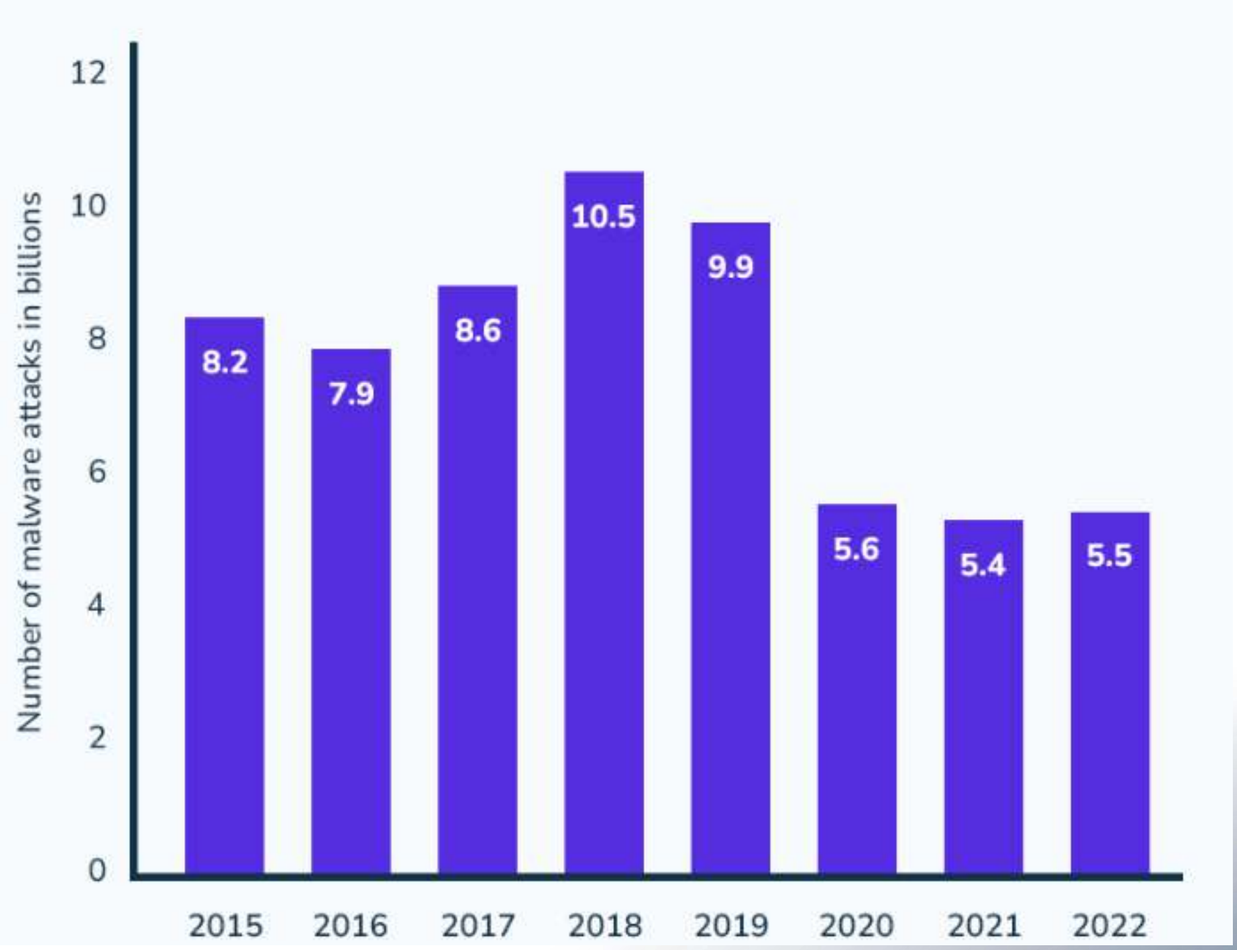
Malware, short for malicious software, refers to any software specifically designed to harm, exploit, or compromise the integrity of a computer system, network, or user's data. There are various types of malware, each with its own characteristics and methods of attack

Preventive Measures

- Install reputable antivirus and anti-malware software.
- Keep operating systems and applications updated with the latest security patches.
- Educate users on safe browsing habits and avoid clicking on suspicious links or downloading attachments from unknown sources

Malicious Software

Lets have a look on the number of attacks through the years



Malware Volumes

Overall the total amount of malware and potentially unwanted applications is 1.2 billion malicious programs

ncc.cy
NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets get Familiar with Malicious Software and its types

1 Viruses attach themselves to legitimate programs and replicate when the infected program runs. They can spread to other files and systems, causing damage to data and disrupting system functionality.

2 Worms are self-replicating programs that can spread across networks without the need for a host file. They often exploit vulnerabilities in operating systems or software to propagate and can consume network bandwidth.

3 Trojans disguise themselves as legitimate software to trick users into installing them. Once inside a system, they can create backdoors for attackers, steal sensitive information, or cause damage.

4 Ransomware encrypts a user's files and demands a ransom (usually in cryptocurrency) for the decryption key. Victims are denied access to their files until the ransom is paid.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets continue with Malicious Software

1 Spyware is designed to secretly gather information about a user's activities, often without their knowledge or consent. This information can include keystrokes, browsing habits, and sensitive data.

2 Adware displays unwanted advertisements on a user's computer, often in the form of pop-ups or banners. While not always malicious, it can be intrusive and negatively impact the user experience.

3 Botnets consist of a network of compromised computers "bots" controlled by a central server. Cybercriminals use botnets to perform various malicious activities, such as distributed denial-of-service "DDoS" attacks or spreading malware.

4 Rootkits are designed to hide malicious activities or processes from the operating system and antivirus software. They often give attackers unauthorized access to a system.

ncc.cy
NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Last one for Malicious Software

1 Keyloggers record keystrokes on a user's keyboard, capturing sensitive information such as login credentials, credit card numbers, or personal messages.

2 Backdoors provide unauthorized access to a system by creating a hidden entry point. They are often used by attackers to maintain persistent access after an initial compromise.

Beware what you have seen until now are only a few types of malware, quite a lot more of Malicious Software's exist and many more are being developed

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Denial of Service "DoS" and Distributed Denial of Service "DDoS"

ncc.cy
NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Denial of Service Distributed Denial of Service

What is DoS & DDoS and how can I defend against it?

Denial of Service (DoS) and Distributed Denial of Service (DDoS)

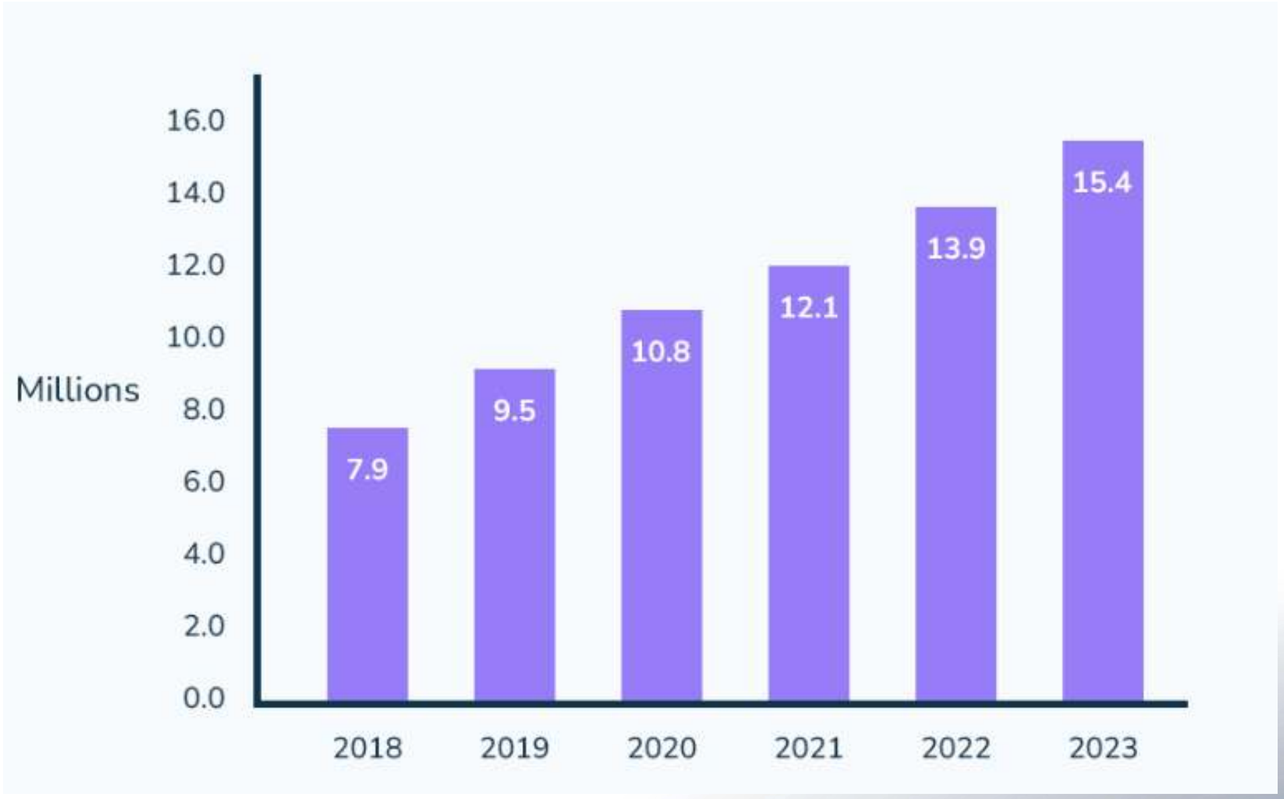
Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are cyber attacks aimed at disrupting the availability of a targeted system, service, or network. The primary goal is to overwhelm the target with an excessive amount of traffic or other malicious activities, rendering it inaccessible to legitimate users.

Preventive Measures

- Deploy firewalls and intrusion prevention systems.
- Use content delivery networks (CDNs) to distribute traffic and absorb DDoS attacks.
- Implement rate limiting and traffic filtering to detect and mitigate suspicious activity.

DDoS & DoS

Lets have a look on the number of attacks through the years



DDoS & DoS Volumes

Prediction based on historic data analysis shows that in the upcoming years the attacks will keep rising with alarming rates

ncc.cy
NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS
COMMISSIONER OF COMMUNICATIONS Digital Security Authority
Co-funded by the European Union

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets get Familiar with DDoS and its types

1 Botnet-Based Attacks utilizes a network of compromised computers (botnet) to flood the target with traffic. The attacker controls the botnet remotely, making it challenging to trace the attack back to a single source.

2 Amplification Attacks exploits vulnerabilities in certain network protocols to amplify the volume of traffic directed at the target. DNS amplification and NTP amplification are common examples.

3 DNS Flood overwhelms the target's DNS servers with a large volume of fake requests, causing delays or disruptions in resolving domain names.

4 UDP Reflection Attack spoofs the source IP address and sends UDP packets to vulnerable servers, which then respond to the forged source, amplifying the traffic towards the target.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets continue with DoS

1. Ping Flood attackers send a large number of ping requests to a target system, overwhelming it with traffic and causing it to become unresponsive to legitimate requests.

2. SYN/ACK Flood exploits the TCP handshake process by flooding the target with SYN (synchronize) or ACK (acknowledge) packets, exhausting system resources and preventing the completion of legitimate connections.

3. HTTP/HTTPS Flood overloads a web server by sending a massive volume of HTTP or HTTPS requests, consuming bandwidth and server resources, and making the website slow or unresponsive.

4. Teardrop Attack manipulates packet fragmentation in a way that causes the target system to crash or become unstable. This is achieved by sending fragmented packets that overlap when reassembled.

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Man-in-the-Middle (MitM)

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Some of the ways attackers try to deploy MitM

Interception

IP Spoofing:

Attacker pretends to be a certain website or service by changing information in the data packets sent over the Internet.

Interception

ARP Spoofing:

Attacker tricks a network into thinking their computer is another computer on the network.

Interception

DNS Spoofing:

Commercially available and supported exploit packs will attempt to leverage vulnerabilities

Decryption

HTTPS Spoofing:

Attacker tricks your browser with a fake security certificate when you try to visit a secure site.

Decryption

SSL BEAST:

This method takes advantage of a weakness in older security protocols to sneak a look at secure information

ncc.cy
NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Man-in-the-Middle “MitM”

What is MitM and how can I defend against it?

Man-in-the-Middle

A Man-in-the-Middle (MitM) attack is a type of cyber attack where an unauthorized third party intercepts and potentially alters the communication between two parties without their knowledge. The attacker positions themselves between the communicating entities and can eavesdrop on or manipulate the data being exchanged.

Preventive Measures

- Use encryption protocols such as HTTPS for secure communication.
- Implement secure Wi-Fi protocols and avoid public Wi-Fi for sensitive transactions.
- Verify the authenticity of websites and use digital certificates.

Man-in-the-Middle

Lets have a look on the number of attacks through the years

MitM Statistics

- MITM attacks represent 19% of all successful cyber attacks, according to one 2021 study.
- 6% of all attacks observed by IBM in 2022 were due to business email compromise.
- Cofense identified a 35% increase in the volume of MITM-compromised messages reaching their customers' inboxes between Q1 2022 and Q1 2023.

ncc.cy
NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS
COMMISSIONER OF COMMUNICATIONS Digital Security Authority
Co-funded by the European Union

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets get Familiar with MitM and its types

1 Wi-Fi Eavesdropping

The attacker sets up an unauthorized Wi-Fi hotspot or compromises an existing one. When users connect to the compromised network, the attacker can intercept and monitor their communications.

2 Email Hijacking

The attacker gains unauthorized access to an email account, allowing them to read, send, or manipulate emails. This can lead to the compromise of sensitive information or the impersonation of the account owner.

3 Wi-Fi Pineapple Attack

Involves the use of a rogue Wi-Fi access point to trick nearby devices into connecting. Once connected, the attacker can intercept and manipulate the traffic passing through the compromised access point.

4 DNS Spoofing Attacks

The attacker injects false DNS responses into the target's DNS cache, redirecting users to malicious websites or phishing pages.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets continue with MitM

1. **Packet Sniffing**
   The attacker intercepts unencrypted network traffic to capture and analyze packets. This allows them to view sensitive information, such as login credentials, personal data, or financial details.

2. **DNS Spoofing/Poisoning**
   The attacker manipulates the Domain Name System (DNS) to redirect users to malicious websites. By providing false DNS responses, the attacker can control the target's web traffic and potentially perform phishing attacks.

3. **HTTP Session Hijacking**
   Also known as session sniffing or session hijacking, this attack involves intercepting and stealing a user's session token or cookie. With this information, the attacker can impersonate the victim and gain unauthorized access to their accounts.

4. **SSL Stripping**
   The attacker downgrades a secure HTTPS connection to an unsecured HTTP connection. This enables them to intercept and view the data exchanged between the user and the website without the user's knowledge.

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Weak Authentication and Password Attacks

ncc.cy
NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Weak Authentication and Password Attacks

What is WAPA and how can I defend against it?

Weak Authentication and Password Attacks

Weak authentication and password attacks are security threats aimed at exploiting vulnerabilities in user authentication processes, particularly when weak or easily guessable passwords are in use.

Preventive Measures

- Enforce strong password policies, including length and complexity requirements.
- Implement multi-factor authentication (MFA) to add an extra layer of security.
- Regularly audit and update user credentials.

Weak Authentication & Weak Password

Lets have a look on some statistics

WAPA Statistics

- 93% of the passwords used in brute force attacks include 8 or more characters
- 54% of organizations do not have a tool to manage work passwords
- The Cincinnati Reds top the list of most popular baseball teams found in compromised password lists
- 48% of organizations do not have user verification in place for calls to the IT service desk
- 41% of passwords used in real attacks are 12 characters or longer
- 42% of seasonal passwords contained the word “summer”
- 68% of passwords used in real attacks include at least two character types

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets get Familiar with Password Attacks and its types

1 Shoulder surfing involves an attacker observing or recording a user's password as it is entered. This can occur in crowded public places or through more targeted means like using binoculars or surveillance cameras.

2 Keyloggers capture and log keystrokes entered by a user. This includes passwords and other sensitive information. Attackers may use software or hardware-based keyloggers to record user input.

3 In credential stuffing attacks, attackers use username and password pairs obtained from previous data breaches or other sources to gain unauthorized access to user accounts on various online platforms. This exploits the common practice of users reusing passwords across multiple sites.

4 In a brute force attack, an attacker systematically tries all possible password combinations until the correct one is found. This method is time-consuming but can be effective if passwords are weak.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets continue with Weak Authentication

1. Brute force attacks: Attackers use automated tools to systematically try different combinations of usernames and passwords until they find the correct credentials. Weak passwords or easily guessable usernames make it easier for attackers to succeed.

2. Credential stuffing: Attackers use lists of stolen usernames and passwords from other data breaches and try them on different websites or systems. Since many people reuse passwords across multiple accounts, this method can be effective if weak authentication is in place.

3. Phishing: Attackers create fake login pages or emails that mimic legitimate websites or services to trick users into entering their credentials. If users fall for the phishing attempt and provide their login information, the attacker can gain unauthorized access to their accounts.

4. Session hijacking: Attackers intercept or steal session cookies or tokens used for authentication. This allows them to impersonate the legitimate user and gain access to their account without needing to know the actual credentials.

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Zero-Day Exploits

ncc.cy
NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Zero-Day Exploits

What is Zero-Day Exploits and how can I defend against it?

Zero-Day Exploits

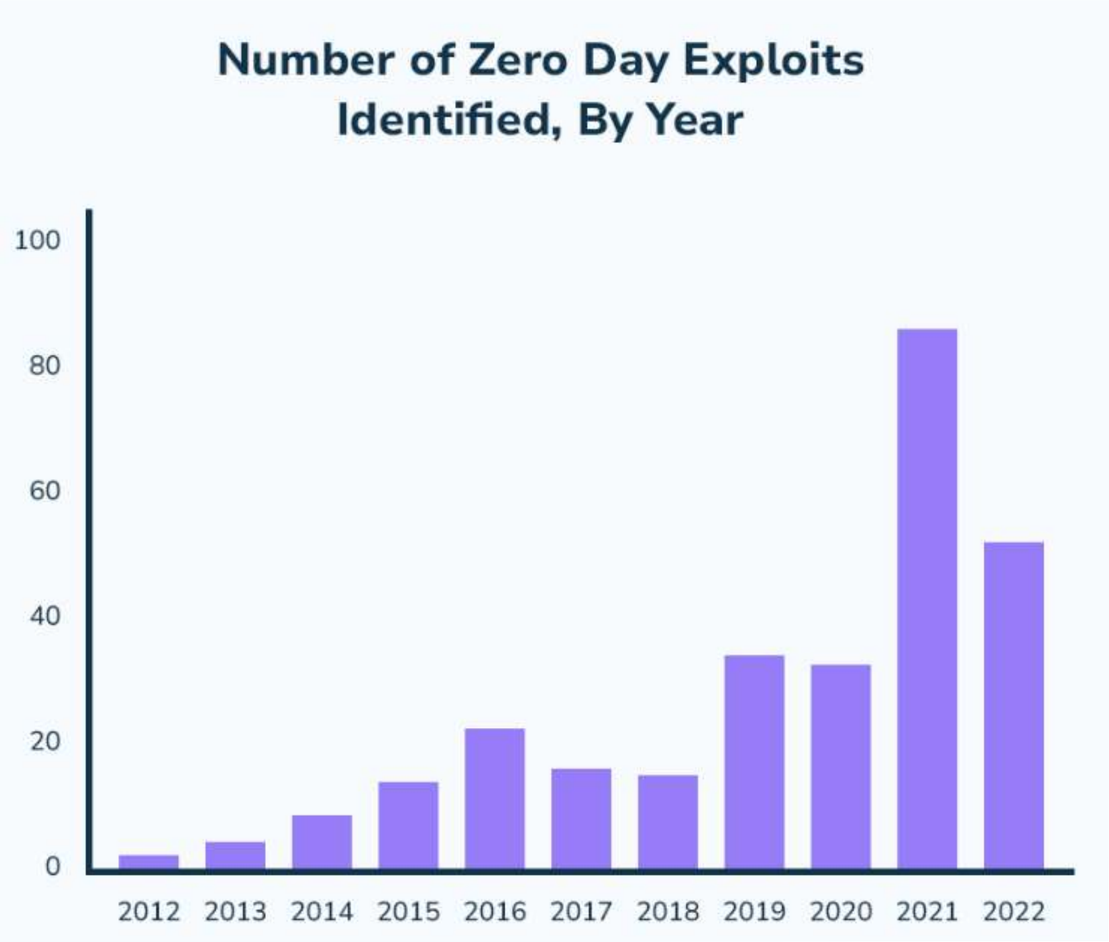
Zero-day exploits refer to attacks that target vulnerabilities in software or hardware that are unknown to the vendor or the security community. These vulnerabilities are called "zero-day" because there are zero days of protection—no patches or fixes exist at the time of the attack. Cybercriminals or threat actors exploit these vulnerabilities to compromise systems, steal data, or carry out other malicious activities

Preventive Measures

- Keep software and systems updated with the latest security patches.
- Employ intrusion detection and prevention systems to detect unusual activity.
- Consider using virtual patching solutions to mitigate vulnerabilities temporarily.

Zero-Day Exploits

Lets have a look on the number of attacks through the years



Zero-Day Exploits

The Zero-Day.cz tracking project logged a total of 53 ZDEs in the first seven months of 2023, compared to 52 in all of 2022.

ncc.cy
NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS
COMMISSIONER OF COMMUNICATIONS Digital Security Authority
Co-funded by the European Union

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets get Familiar with ZDE and its types

1 Zero-Day Attacks on Software

This type of zero-day exploit targets vulnerabilities in software applications. Common targets include web browsers, operating systems, office productivity software, and other widely used applications. Attackers often craft malicious code to take advantage of these vulnerabilities.

2 Zero-Day Web Browser Exploits

Web browsers are frequent targets for zero-day exploits. Attackers may compromise websites with malicious code that exploits vulnerabilities in the browser, allowing them to execute arbitrary code on the victim's system.

3 Zero-Day Operating System Exploits

Zero-day exploits targeting operating systems can be particularly dangerous because they can compromise the core functionalities of a computer or device. These exploits often provide attackers with elevated privileges or the ability to execute arbitrary code.

4 Zero-Day Mobile Exploits

Mobile devices, including smartphones and tablets, are not immune to zero-day exploits. Malicious apps or crafted content can exploit vulnerabilities in mobile operating systems, leading to unauthorized access or data theft.

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Phishing

Phishing

What is Phishing and how can I defend against it?

Phishing

Phishing is a type of cyberattack in which attackers use deceptive tactics to trick individuals into revealing sensitive information, such as login credentials, personal details, or financial information. Phishing attacks typically involve impersonating a trustworthy entity or using social engineering techniques to manipulate the target.

Preventive Measures

- Implement email filtering to detect and block phishing emails.
- Conduct regular phishing awareness training for employees.
- Encourage the use of multi-factor authentication (MFA) to enhance account security.

ncc.cy
NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS
COMMISSIONER OF COMMUNICATIONS Digital Security Authority
Co-funded by the European Union

Phishing

Lets have a look on some statistics

Industry	Percentage of phishing attacks
Financial Institutions	27.7%
Software-as-a-Service Providers	17.7%
Other	18.2%
Social Media Providers	10.4%
Logistics / Shipping	9.0%
Payment Services	6.0%
eCommerce / Retail	5.6%
Telecom	3.1%
Cryptocurrency	2.3%

Phishing Statistics

- 84% of organizations were the targets of at least one phishing attempt in 2022 - a 15% increase on the year before
- In 2022, APWG logged ~4.7 million phishing attacks. Since 2019, the number of phishing attacks has increased by more than 150% yearly

ncc.cy
NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS
COMMISSIONER OF COMMUNICATIONS Digital Security Authority
Co-funded by the European Union

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

WHITE

Lets get Familiar with Phishing and its types

1 Attackers send deceptive phishing emails that appear to be from a legitimate source, such as a bank, government agency, or reputable company. These emails often contain urgent messages, requesting the recipient to click on a link or download an attachment that leads to a fake website designed to capture sensitive information.

2 Spear phishing is a targeted form of phishing where attackers tailor their messages to a specific individual or organization. The attackers research their targets to make the phishing attempts more convincing, often using information gathered from social media or other sources.

3 Vishing involves using phone calls to trick individuals into providing sensitive information. Attackers may impersonate legitimate entities, such as banks or government agencies, and use social engineering to convince the target to disclose personal details or financial information over the phone.

4 Smishing involves phishing attacks conducted through text messages (SMS). Similar to email phishing, smishing messages contain links or prompts that lead recipients to fake websites or encourage them to provide sensitive information via text.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets continue with Phishing

1 Pharming involves redirecting website traffic to fraudulent websites without the user's knowledge. Attackers manipulate the domain name system (DNS) settings or use other techniques to redirect users to fake websites where they may unwittingly enter sensitive information.

2 Clone phishing involves creating a replica (clone) of a legitimate email or communication. The attacker makes slight modifications to the content, such as changing links or attachments, and then sends the modified version to the target, attempting to deceive them into taking malicious actions.

3 In MitM phishing attacks, attackers position themselves between the victim and a legitimate website or communication channel. This allows them to intercept and alter the communication, potentially capturing sensitive information in the process.

4 Attackers manipulate search engine(phishing) results to promote malicious websites. When users search for specific terms, the manipulated results lead them to fake websites designed to capture sensitive information.

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Insider Threat

ncc.cy
NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Insider Threat

What is Insider Threat and how can I defend against it?

Insider Threat

Phishing is a type of cyberattack in which attackers use deceptive tactics to trick individuals into revealing sensitive information, such as login credentials, personal details, or financial information. Phishing attacks typically involve impersonating a trustworthy entity or using social engineering techniques to manipulate the target.

Preventive Measures

- Implement email filtering to detect and block phishing emails.
- Conduct regular phishing awareness training for employees.
- Encourage the use of multi-factor authentication (MFA) to enhance account security.

Insider Threat

Lets have a look on some statistics

Insider Threat Statistics

- In the Past Two Years, Insider Attacks Have Grown by Over 47%.
- The Cost of Insider Threats in 2022 was $15.38 Million.
- Over Two-thirds of Insider Threat Incidents Result from Negligence.
- Statistics Reveal that Approximately 74% of Businesses See More Frequent Insider Breaches.
- Larger Companies Spend $10.24 Million More Than Smaller Companies on Insider Attacks

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Lets get Familiar with Insider Threat and its types

1 Malicious Insiders intentionally misuse their access privileges to cause harm to the organization. This can include stealing sensitive data, conducting espionage, sabotaging systems, or disrupting operations. Malicious insiders may have various motivations, such as financial gain, revenge, or ideological beliefs.

2 Negligent insiders pose a threat due to their unintentional actions or failure to follow security policies and procedures. This could involve mishandling sensitive data, falling victim to phishing attacks, using weak passwords, or neglecting security best practices. Negligent insiders may not have malicious intent but can still contribute to security incidents.

3 In cases of compromised insiders, individuals have had their credentials or access rights compromised by external actors, such as through phishing attacks or malware. Once compromised, attackers can exploit the insider's privileges to gain unauthorized access to systems, steal data, or carry out other malicious activities.

4 Infiltrators or moles are individuals who deliberately join an organization with the intent of causing harm from within. They may be recruited by external entities or have malicious motives from the start. Infiltrators often work to gain trust and access over time before executing their plans.

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
ncc.cy
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Lets continue with Insider Threat

1 Unintentional insiders are individuals who unknowingly contribute to security risks. This may involve sharing sensitive information without realizing the potential consequences, falling for social engineering attacks, or inadvertently introducing malware into the organization's systems.

2 Disgruntled employees, often motivated by personal or professional dissatisfaction, may pose a significant insider threat. Their actions may range from stealing intellectual property to intentionally damaging systems or engaging in other harmful activities as a form of retaliation.

3 Contractors, vendors, or other third-party individuals with access to an organization's systems and data can also pose insider threats. Whether intentionally or unintentionally, they may compromise security through actions like unauthorized access, data leaks, or other security lapses.

4 In some cases, multiple individuals within an organization may collaborate to carry out insider threats. This could involve employees working together to steal sensitive data, commit fraud, or disrupt operations.

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Benefits on Company Growth

How technology affects company growth

Increases efficiency and productivity

More efficient operations and higher productivity leads to success and expansion.

Boosts innovation

The right tools encourage businesses to develop better products, better processes, and better ways to do business.

Improves management

Systems and platforms keep the company organized and on track to achieving business goals.

ncc.cy
NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

Benefits on Employee Satisfaction & Commitment

How technology affects the staff

Improves connection among employees

Having more channels to communicate fosters communication and collaboration - enabling employees to work more efficiently.

Raises productivity

Having the right systems and tools in place helps increase employees' productivity, boosting their performance and allowing them to have a sense of accomplishment.

Encourages learning and development

Technology provides employees with access to resources and the means to learn and evolve.

ncc.cy
NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS
COMMISSIONER OF COMMUNICATIONS
Digital Security Authority
Co-funded by the European Union

“As John Chambers famously said, ‘There are only two types of organizations: Those that have been hacked and those that don’t know it yet!”

“We shouldn’t worry about getting hacked, that’s illegal.”

ncc.cy

NCC
CYBERSECURITY NATIONAL COORDINATION CENTRE
CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

Co-funded by the European Union

Do you have any questions?