



UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Prednáška 4

Útočné nástroje, najčastejšie hrozby a útoky



Riešenie bezpečnostných incidentov
(CyberOps Associate v1.02)

Mgr. Jana Uramová, PhD.
Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU

Ktorý výsledok pokrýva táto prednáška

Výsledky vzdelávania

Študent po absolvovaní predmetu získa vedomosti a zručnosti potrebné na úspešné zvládnutie úloh, povinností a zodpovedností bezpečnostného analytika v operačnom centre bezpečnosti.

Študent po absolvovaní predmetu bude vedieť:

- Vysvetliť rolu analytika v rámci kybernetickej bezpečnosti
- Vysvetliť prostriedky operačného systému Windows a Linux a charakteristiky pre podporu analýzy v rámci kybernetickej bezpečnosti
- Analyzovať operácie v rámci sieťových protokolov a služieb
- Vysvetliť operácie sieťovej infraštruktúry
- Klasifikovať rôzne typy sieťových útokov
- Použiť sieťové monitorovacie nástroje na identifikáciu útokov proti sieťovým protokolom a službám
- Použiť rôzne metódy na prevenciu škodlivého prístupu do počítačových sietí, k používateľom a k dátam
- Vysvetliť vplyvy kryptografie v rámci monitorovania bezpečnostných sietí
- Vysvetliť, ako skúmať zraniteľnosti a útoky koncových zariadení
- Identifikovať hlásenia v rámci sieťovej bezpečnosti
- Analyzovať sieťovú prevádzku na overenie potencionálneho zneužitia siete
- Aplikovať reakčné modely na incident, a získať prostriedky na manažovanie sieťových bezpečnostných incidentov
- Prerekvizity:
 - Princípy IKS, Počítačové siete 1, Úvod do OS

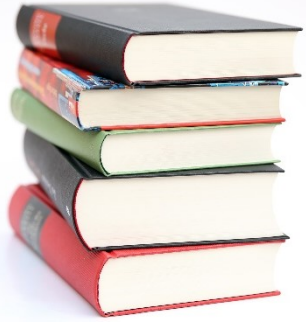


Preliminary version of topics for lectures

Planning

| Week | CyberOps Modules in lectures | Exam from: |
|------|--|------------|
| 1 | Chapter 1 The Danger Chapter 2 Fighters in the War Against Cybercrime Chapter 3: The Windows Operating System | none |
| 2 | Chapter 4: Linux Overview Chapter 5 Network Protocols Chapter 6 Ethernet and Internet Protocol (IP) Chapter 7 Connectivity Verification Chapter 8 Address Resolution Protocol Chapter 10 Network Services Chapter 11 Network Communication Devices | 1-2 |
| 3 | Chapter 9 The Transport Layer (+nmap) Chapter 12 Network Security Infrastructure | 3-4 |
| 4 | Chapter 13 Attackers and Their Tools Chapter 14 Common Threats and Attacks | 5-10 |

| Week | CyberOps Modules in Lectures | Exam from: |
|------|---|------------|
| 5 | Chapter 15 Network Monitoring and Tools (<i>SIEM, SOAR</i>) Chapter 16 Attacking the Foundation (<i>L2, L3 protocols vulnerabilities and attacks</i>) Chapter 17 Attacking What We Do (<i>L7 vulnerabilities and attacks</i>) | 11-12 |
| 6 | Chapter 18 Understanding Defense (<i>security management</i>) Chapter 19 Access Control (<i>AAA</i>) Chapter 20 Threat Intelligence (<i>commercials, CVE database</i>) | 13-17 |
| 7 | Chapter 21 Cryptography Chapter 22 Endpoint Protection | 18-20 |
| 8 | Chapter 23 Endpoint Vulnerability Assessment Chapter 24 Technologies and Protocols | none |
| 9 | Chapter 25 Network Security Data Chapter 26 Evaluating Alerts (in Security Onion) | 21-23 |
| 10 | Chapter 27 Working with Network Security Data (Security Onion and ELK) | 24-25 |
| 11 | Chapter 28 Digital Forensics and Incident Analysis and Response | none |
| 12 | Expert talk (invited lecture) | 26-28 |



Obsah dnešnej prednášky

- **Chapter 13 Attackers and Their Tools**
- **Chapter 14 Common Threats and Attacks**



Module 13: Attackers and Their Tools

Module Objective: Explain how networks are attacked

| Topic Title | Topic Objective |
|------------------------------|---|
| Who is Attacking our Network | Explain how network threats have evolved. |
| Threat Actor Tools | Describe the various types of attack tools used by Threat Actors. |

13.1 Who is Attacking Our Network?

Threat, Vulnerability, and Risk

- Attackers want to access our assets such as data and other intellectual property, servers, computers, smart phones, tablets, and so on.



Threat, Vulnerability, and Risk (Contd.)

- To understand network security, it is important to know the following terms:

| TERM | EXPLANATION |
|----------------|--|
| Threat | A potential danger to an asset (data or the network itself). |
| Vulnerability | A weakness in a system or its design that could be exploited by a threat. |
| Attack Surface | An attack surface is the total sum of the vulnerabilities in a given system that are accessible to an attacker. The attack surface describes different points where an attacker could get into a system, and where they could get data out of the system. |
| Exploit | The mechanism that is used to leverage a vulnerability to compromise an asset. Exploits may be remote or local. A remote exploit is one that works over the network without any prior access to the target system. In a local exploit, the threat actor has some type of user or administrative access to the end system. It does not necessarily mean that the attacker has physical access to the end system. |
| Risk | The likelihood that a particular threat will exploit a particular vulnerability of an asset and result in an undesirable consequence. |

Threat, Vulnerability, and Risk (Contd.)

- Risk management is the process that balances the operational costs of providing protective measures with the gains achieved by protecting the asset.

Four ways to manage risk:

| Risk Management Strategy | Explanation |
|--------------------------|--|
| Risk acceptance | When the cost of risk management options outweighs the cost of risk, the risk is accepted, and no action is taken. |
| Risk avoidance | This means avoiding any exposure to risk by eliminating the activity, thus resulting in losing any benefits from the activity. |
| Risk reduction | This reduces the exposure to risk. It is the most commonly used risk mitigation strategy. This strategy requires careful evaluation of the costs of loss, the mitigation strategy, and the benefits gained from the operation or activity that is at risk. |
| Risk transfer | Some or all of the risk is transferred to a willing third party such as insurance company. |

Threat, Vulnerability, and Risk (Contd.)

- **Common network security terms:**
 - Countermeasure – Actions taken to protect assets by mitigating a threat or reducing risk.
 - Impact - The potential damage to the organization that is caused by the threat
- **Note:** A local exploit requires inside network access such as a **user with an account** on the network. It does **not require an account on the network** to exploit that network's vulnerability.

Hacker vs. Threat Actor

‘Hacker’ is a common term used to describe a threat actor. Hacker has a variety of meanings that are as follows:

- A **clever programmer** capable of developing new programs and making coding changes to existing programs to make them more efficient.
- A **network professional** that uses sophisticated programming skills to ensure that networks are not vulnerable to attack.
- An individual who **run programs to prevent** or **corrupt data** on servers.

Types of hackers:

- White Hat hackers
- Gray Hat hackers
- Black Hat hackers

Hacker vs. Threat Actor (Contd.)

White Hat Hackers:

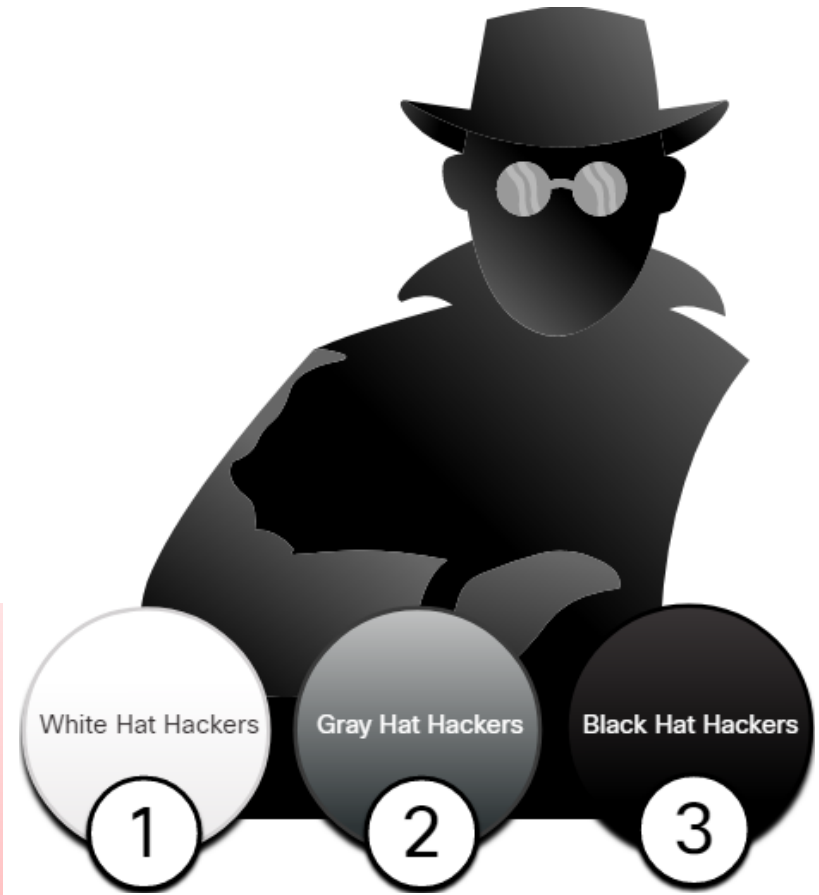
- White hat hackers are ethical hackers who use their programming skills for good, ethical, and legal purposes
 - Penetration tests – before vulnerability is exploited
 - Award prizes, bounties

Gray Hat Hackers:

- Grey hat hackers are individuals who commit crimes and unethical things, but not for personal gain or to cause damage.

Black Hat Hackers:

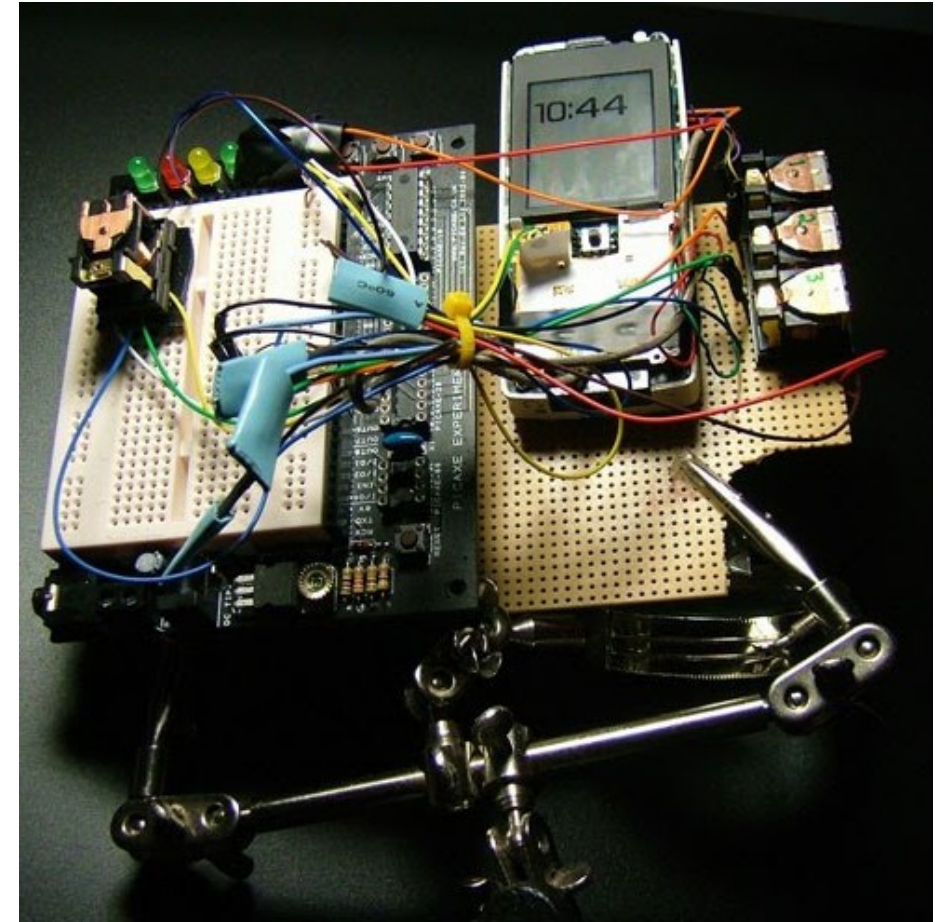
- Black hat hackers are unethical criminals who violate computer and network security for personal gain or malicious reasons



= Threat actors

Evolution of Threat Actors

- Hacking started in the 1960s with phone phreaking, which refers to using various audio frequencies to manipulate phone systems.
- In the early 1960's, threat actors realized that by mimicking a tone using a whistle, they could exploit the phone switches to make free long-distance calls.
- In the mid-1980's, threat actors wrote 'war dialing' programs which dialed each telephone number in a given area in search of computers, bulletin board systems, and fax machines.
- When a phone number was found, password-cracking programs were used to gain access.



phone phreaking, fraudulent manipulation of telephone signaling in order to make free phone calls

Evolution of Threat Actors (Contd.)

Types of Threat Actors:

- **Script kiddies** - It refers to teenagers or inexperienced threat actors running existing scripts, tools, and exploits, to cause harm, but typically not for profit.
- **Vulnerability brokers** - It refers to grey hat hackers who attempt to discover exploits and report them to vendors, for prizes or rewards.
- **Hacktivists** - It refers to grey hat hackers who rally and protest against different political and social ideas.
- **Cybercriminals** - It refers to black hat hackers who are either self-employed or working for large cybercrime organizations.
- **State-sponsored** - State-Sponsored hackers are threat actors who steal government secrets, gather intelligence, and sabotage networks of foreign governments, terrorist groups, and corporations.

Cybercriminals

- Cybercriminals are threat actors who are motivated to **make money** using any necessary means.
- At times, cybercriminals work **independently** or they are financed and **sponsored** by criminal organizations.
- They steal **billions** of dollars from consumers and businesses every year.
- They operate in **underground economy** and buy and sell personal information and intellectual property that they steal from victims.
- They target **small** businesses and consumers, as well as **large** enterprises and industries.



Cybersecurity Tasks

- Threat actors **target** the home users, small-to-medium sized businesses, as well as large public and private organizations.
- Hence, Cybersecurity is a shared responsibility which **all users must practice** to make the internet and networks safer and more secure.
- Organizations must **take action** and **protect** their assets, users, and customers. They must **develop and practice cybersecurity tasks** such as those mentioned in the figure.



Cyber Threat Indicators

Indicators Of Compromise (IOC)

- IOCs are the **evidence that an attack has occurred** and each attack has unique identifiable attributes.
- IOCs can be **features that identify malware files, IP addresses of servers that are used in attacks, filenames, and characteristic changes made to end system software, among others.**
- IOCs help cybersecurity personnel identify what has happened in an attack and **develop defenses** against the attack.

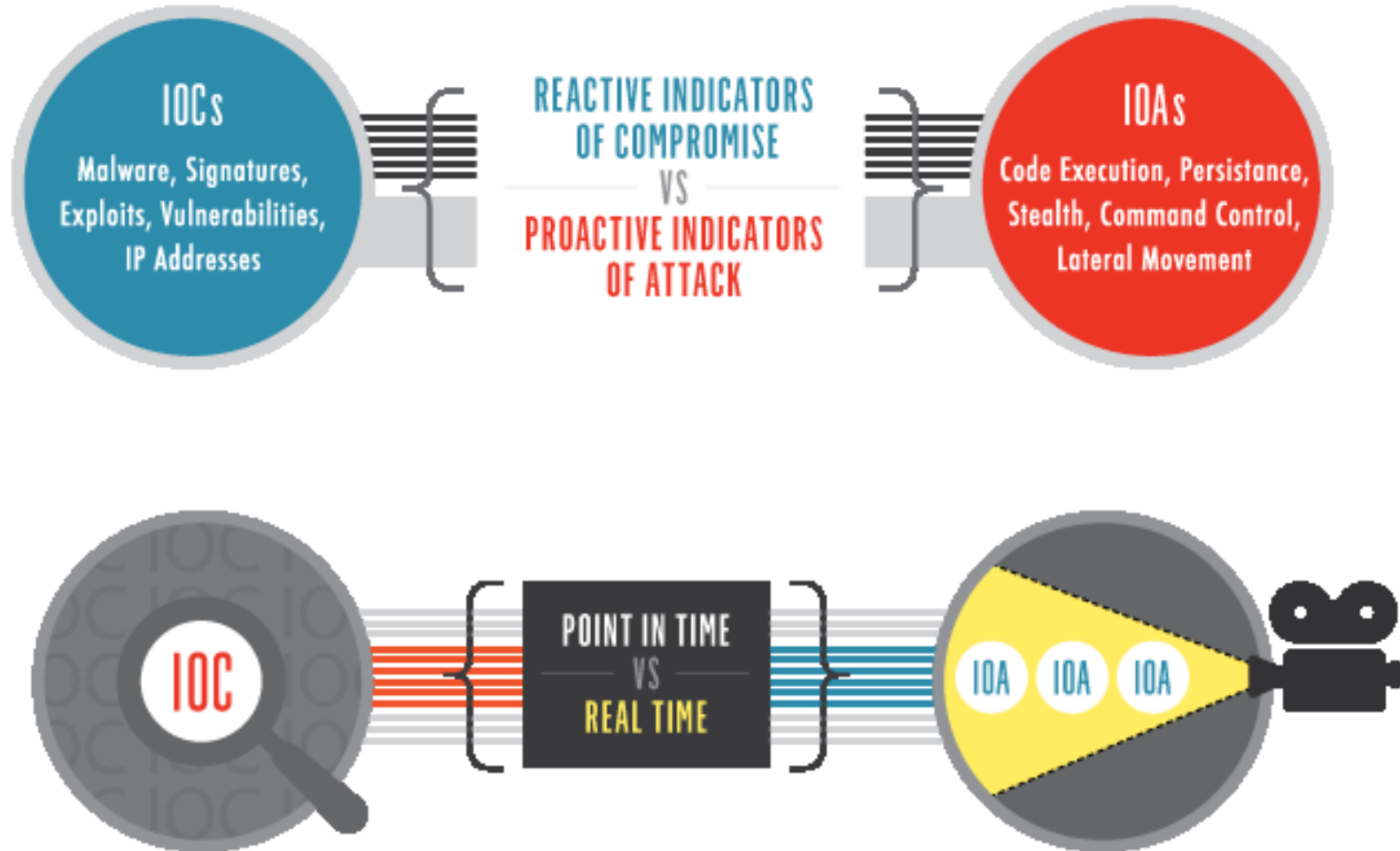
```
Malware File - "studiox-link-standalone-v20.03.8-stable.exe"
  sha256 6a6c28f5666b12beecd56a3d1d517e409b5d6866c03f9be44ddd9efffa90f1e0
  sha1   eb019ad1c73ee69195c3fc84ebf44e95c147bef8
  md5    3a104b73bb96dfed288097e9dc0a11a8
DNS requests
  domain log.studiox.link
  domain my.studiox.link
  domain _sips._tcp.studiox.link
  domain sip.studiox.link
Connections
  ip     198.51.100.248
  ip     203.0.113.82
```

Summary of the
IOC for a piece of
malware

Cyber Threat Indicators (Contd.)

Indicators of Attack (IOA)

- IOA focus more on the motivation and strategies behind an attack and the attackers to gain access to assets.
- IOAs helps to generate a proactive security approach that can be reused in multiple contexts and multiple attacks. Defending against a strategy can therefore prevent future attacks.



Threat Sharing and Building Cybersecurity Awareness

- Governments are now actively promoting cybersecurity.
- The US **Cybersecurity Infrastructure and Security Agency (CISA)** is leading efforts to automate the sharing of cybersecurity information with public and private organizations at no cost.
 - CISA use a system called **Automated Indicator Sharing (AIS)** which enables the **sharing of** attack indicators (**IOA**) between the US government and the private sector as soon as threats are verified.
- The **European Union Agency for Cybersecurity (ENISA, *2004)** delivers advice and solutions for the cybersecurity challenges of the EU member states.
- The CISA and the National Cyber Security Alliance (NCSA) have an annual campaign in every October called National Cybersecurity Awareness Month (NCASM) to **raise awareness about cybersecurity**. <https://www.cisa.gov/cybersecurity-awareness-month>
- Už aj ENISA (10 rokov): ECISM European Cybersecurity Month <https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month>



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**



Threat Sharing and Building Cybersecurity Awareness (Contd.)

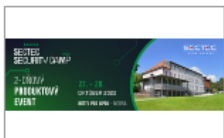
- The theme for the NCASM for 2019 was **Own IT. Secure IT. Protect IT.**
- Security topics provided through campaign:
 - Social media safety
 - Updating privacy settings
 - Awareness of device app security
 - Keeping software up-to-date
 - Safe online shopping
 - Wi-Fi safety
 - Protecting customer data



European Cybersecurity Month

- V SR v roku 2022 – 7 akcií:

27 OCT
22
28 OCT
22



Slovakia

SecTec Security Camp 2022

Pozývame Vás na SecTec Security Camp, kde Vám na základe skúseností u nás, našich partnerov a zákazníkov poskytneme inšpiráciu na postup budovania kybernetickej bezpečnosti, ktorú sme upravovali roky podľa štatistik a charakteristik útokov. Dvojdňový produktový event sa bude konať v krásnom lesnom prostredí pri Modre. Odborný program, ktorým Vás prevedie Martin Matuška zo...

Business users

09 NOV
22
10 NOV
22



Slovakia

Qubit Conference Tatry 2022

Pozývame vás na druhý ročník jedinečného formátu komunitnej konferencie o kybernetickej bezpečnosti na Slovensku Qubit Tatry 2022. Po úspešnom minuloročnom podujatí sa opäť môžete tešiť na panelové diskusie, zdieľanie praktických skúseností profesionálov v oblasti informačnej a kybernetickej bezpečnosti, klubové stretnutia a obľúbený networking. Konferencia Qubit Tatry 2022...

Business users

09 NOV
22
09 NOV
22



Slovakia

ESET European Cybersecurity Day

A hybrid event for Government employees in the European Union discussing the challenges of cybersecurity in a digitised world, this time focusing on the topic of EU cyber resilience. Taking place in Prague NH Carlo IV and online.

All users

All activities

Map view



NIS Directive

- As part of the [EU Cybersecurity strategy](#) the European Commission proposed
 - the EU Network and Information Security (NIS) directive
- The NIS Directive (see [EU 2016/1148](#)) is the **first piece** of **EU-wide cybersecurity legislation**
 - The goal is to **enhance cybersecurity** across the EU.
 - The NIS directive was adopted in **2016** and subsequently, because it is an EU directive, every EU member state has started to adopt national legislation, which follows or ‘transposes’ the directive.
 - EU directives give EU countries some level of flexibility to take into account national circumstances, for example to re-use existing organizational structures or to align with existing national legislation.
 - The national transposition by the EU member states happened on **9 May 2018**.
 - U nás – skoro všetko je datované k **1.4.2018** – zákony, normy, vznik orgánov, samostatných útvarov,
 - **NIS 2 proposed 6.12.2020**



NIS Directive

- Member States
- develop National Cybersecurity Strategies
 - **national CSIRT**, **perform cyber exercises**
 - collaborate cross-border / **EU CSIRT network**, the **strategic NIS cooperation group**, ...
 - identify **Operators of Essential Services (OES)** in critical sectors: energy, transport, banking, finance sector, healthcare, water, and digital infrastructure, and **Digital Service Providers (DPS)** (online market places, cloud and online search engines) and supervise security

OES operators

- **take minimum security measures**
- **report significant incidents.**

DPS providers

- **comply with these security and notification requirements**

- The European Commission maintains [a map showing the status of the transposition of the NIS Directive across the EU Member States.](#)

Sectors of OES and types of digital services in the scope of the NIS Directive



OESs Operators of Essential Services = prevádzkovatelia základných služieb

DSPs Digital Service Providers = prevádzkovatelia digitálnych služieb

What's the difference?

CERT vs. CSIRT vs. CIRT vs. SOC

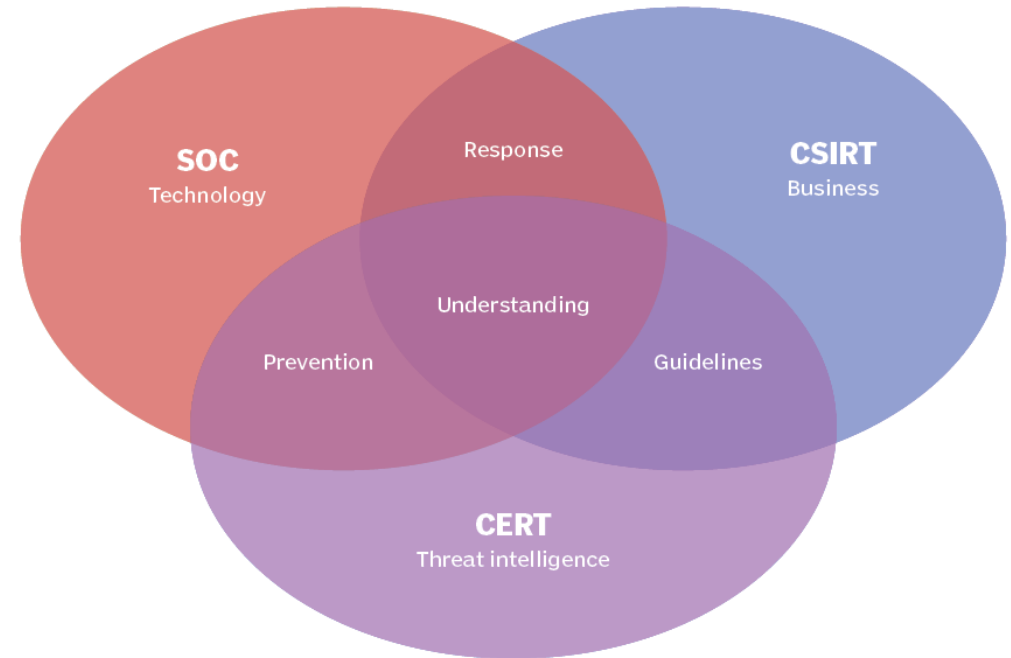


Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

- CSIRT - computer security incident response team
- CIRT - computer incident response team or, less frequently, cybersecurity incident response team
- CERT - computer emergency response (or readiness) team
- CSIRT, CERT and CIRT are often used interchangeably in the field
 - In fact, CSIRT and CIRT are almost always near-equivalent; essentially they are synonymous
 - An organization might prefer one or the other based on the organization's language or style
 - [Carnegie Mellon University](#) – nielen definície:
 - „CSIRT is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident.”
 - “CERT” is a registered trademark owned by Carnegie Mellon University.
 - CSIRT units which share the same responsibility for building the network and device security are advised to seek consent in order to adopt “CERT” in their name.
 - SK-CERT national unit is the owner of the certificate which authorizes the unit to use CERT in its name.

SOC is broader in scope

- SOC generally encompasses **multiple aspects of security operations**, while CSIRTs, CERTs and CIRTs focus specifically on **incident response**.
- A SOC's purview can include the incident response function (either in whole or in part) as well as other tasks. For example, a SOC can:
 - encompass monitoring operations and controls (such as an intrusion detection, system/intrusion prevention system, security information event management/security information management);
 - oversee evaluation of operational and security telemetry and information gathering; and,
 - manage tasks such as identity management and authorization, firewall and filtering ruleset maintenance (both review and change management), forensics and investigation support, or any other aspect of operational security.



Certifikácie CSIRT tímov

- “CERT” is a registered trademark owned by **Carnegie Mellon University**



Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

- Jednotkám CSIRT, ktoré majú rovnakú zodpovednosť za budovanie siete a zabezpečenie zariadení, sa odporúča požiadať o súhlas, aby mohli prijať „CERT“ vo svojom mene.
- SK-CERT national unit is the owner of the certificate

- Trusted Introducer Service (TI)

- international organization maintaining the database of CSIRTs and CERTs
- On 26 March 2020, SK-CERT national unit has become an certified member



- Forum of Incident Response and Security Teams (FIRST)

- international confederation of computer incident response teams
- main goal of FIRST is to create an environment for effective cyber security incident handling that enables
 - exchange of information, tools, methodologies and best practices between FIRST members
- On 23 April 2018, SK-CERT national unit has become a member of FIRST



Národné centrum kybernetickej bezpečnosti (SK-CERT)

- NBU - Národný bezpečnostný úrad
 - **ústredný orgán štátnej správy pre KB, od roku 2016**
 - buduje technické, personálne a organizačné kapacity v oblasti KB
 - rieši KB incidenty
 - buduje bezpečnostné povedomie
- NBU začiatkom roka 2018 zahájil prevádzku **špecializovaného pracoviska**, ktoré po prijatí **zákona o kybernetickej bezpečnosti** 1. apríla 2018 začalo plniť **úlohy národnej jednotky CSIRT**
- 1. septembra 2019 bola jednotka transformovaná na samostatný útvar **Národné centrum KB : SK-CERT**
 - Prostredníctvom SK-CERT úrad zabezpečuje služby spojené:
 - s riadením bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi týchto systémov
 - ďalšie jeho činnosti: analytické činnosti, výskum, budovanie bezpečnostného povedomia a realizovanie vzdelávania v oblasti kybernetickej bezpečnosti.



Riaditeľ NBU: Roman Konečný

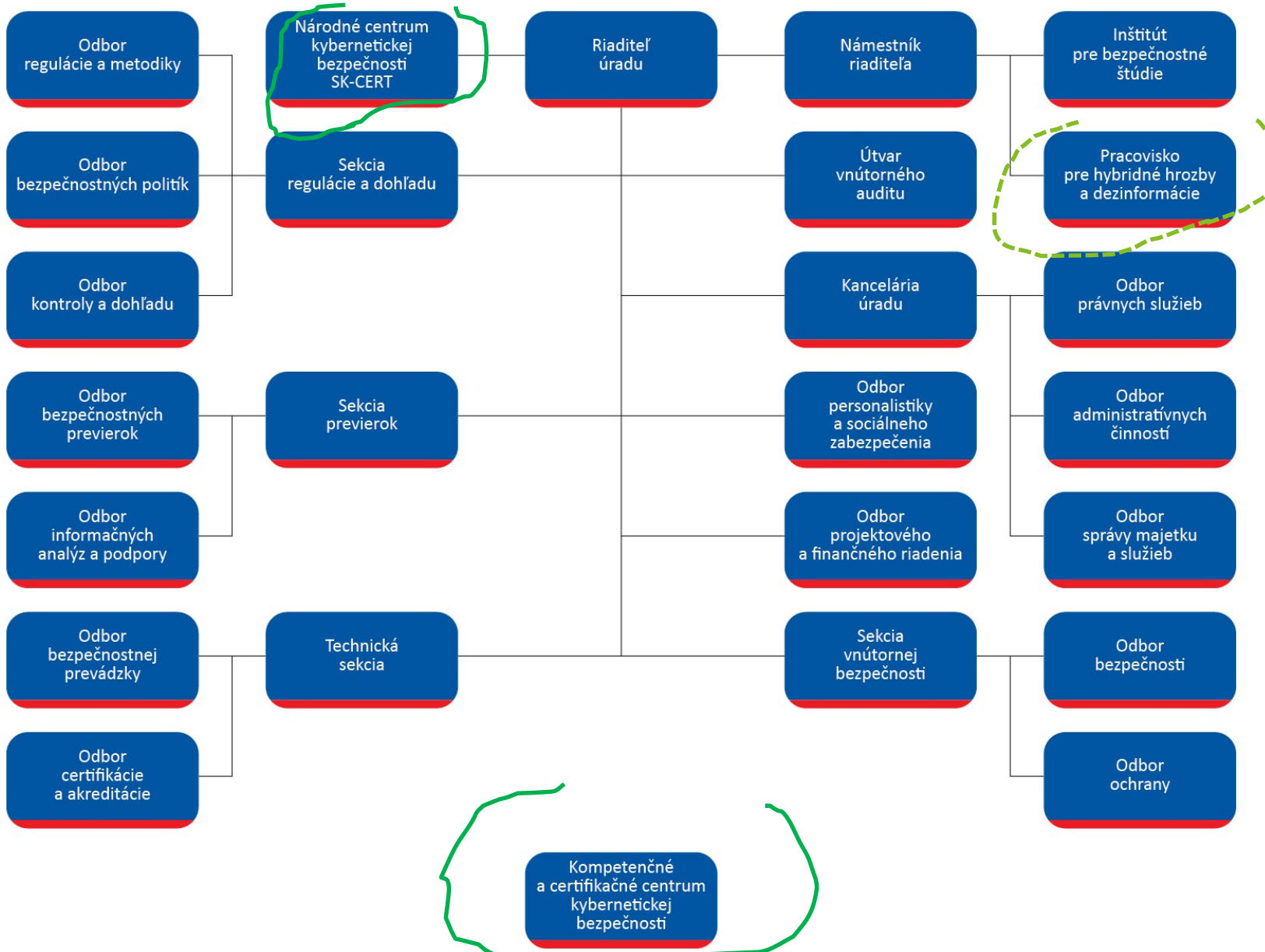
<https://www.nbu.gov.sk/>



Riaditeľ SK-CERT: Rastislav Janota

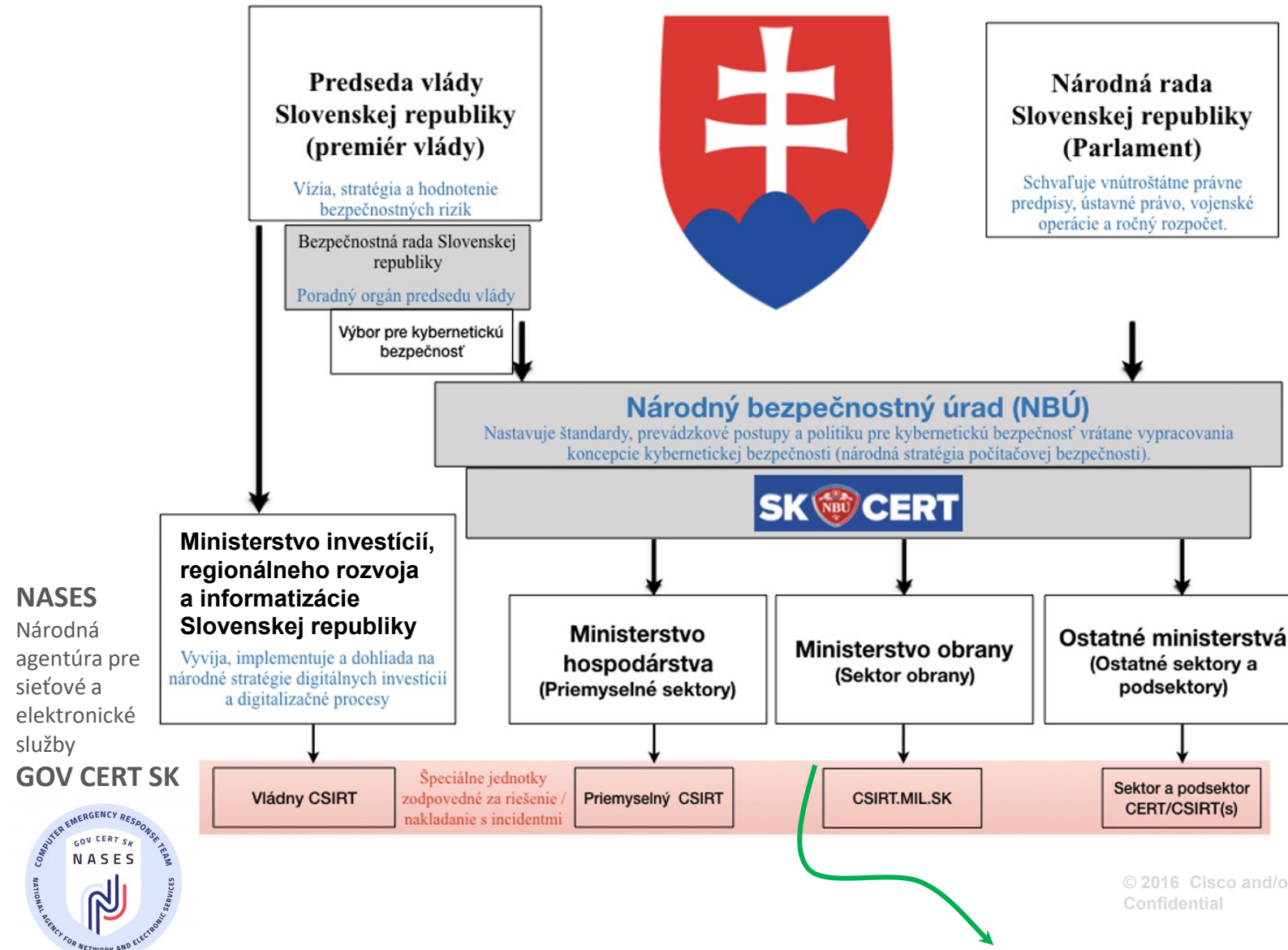


Organizačná štruktúra NBU



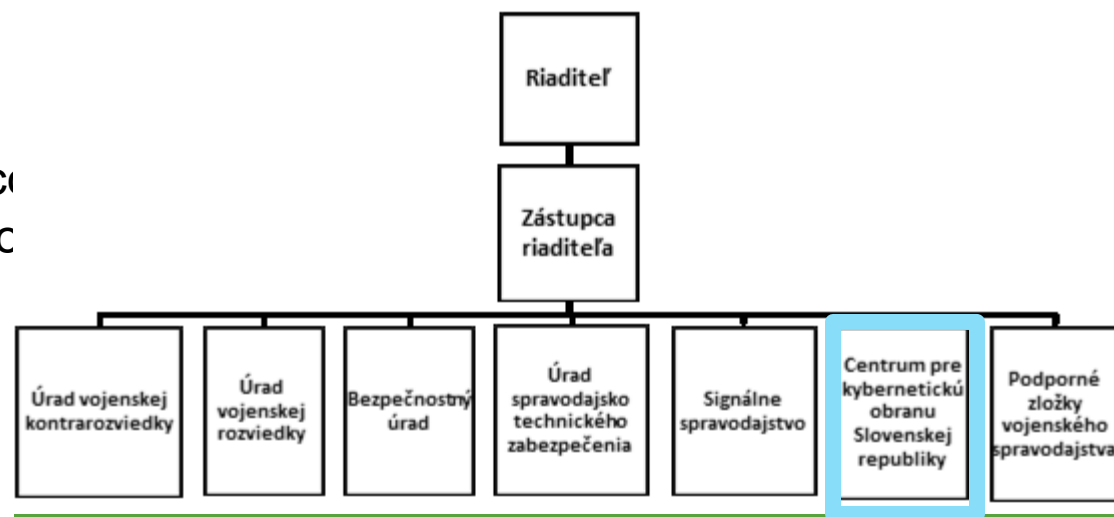
<https://www.nbu.gov.sk/urad/ourade/organizacna-struktura/index.html>

Organizačný graf kybernetickej bezpečnosti Slovenska



Centrum pre kybernetickú obranu (CKO) Slovenskej republiky

- je osobitnou organizačnou zložkou Vojenského spravodajstva plniacou úlohy na úseku obrany štátu v kybernetickom priestore
- CKO vzniklo 1. apríla 2018
- Úlohou CKO je získať, sústreďovať, analyzovať a vyhodnocovať dôležité pre zabezpečenie kybernetickej obrany, informovať dc aktuálnych hrozbách a navrhnúť vhodné opatrenia.
- Súčasťou centra je aj jednotka pre riešenie počítačových bezpečnostných incidentov CSIRT.MIL.SK.



Ministerstvo obrany

Vojenské spravodajstvo

Centrum pre kybernetickú obranu SR

CSIRT.MIL.SK

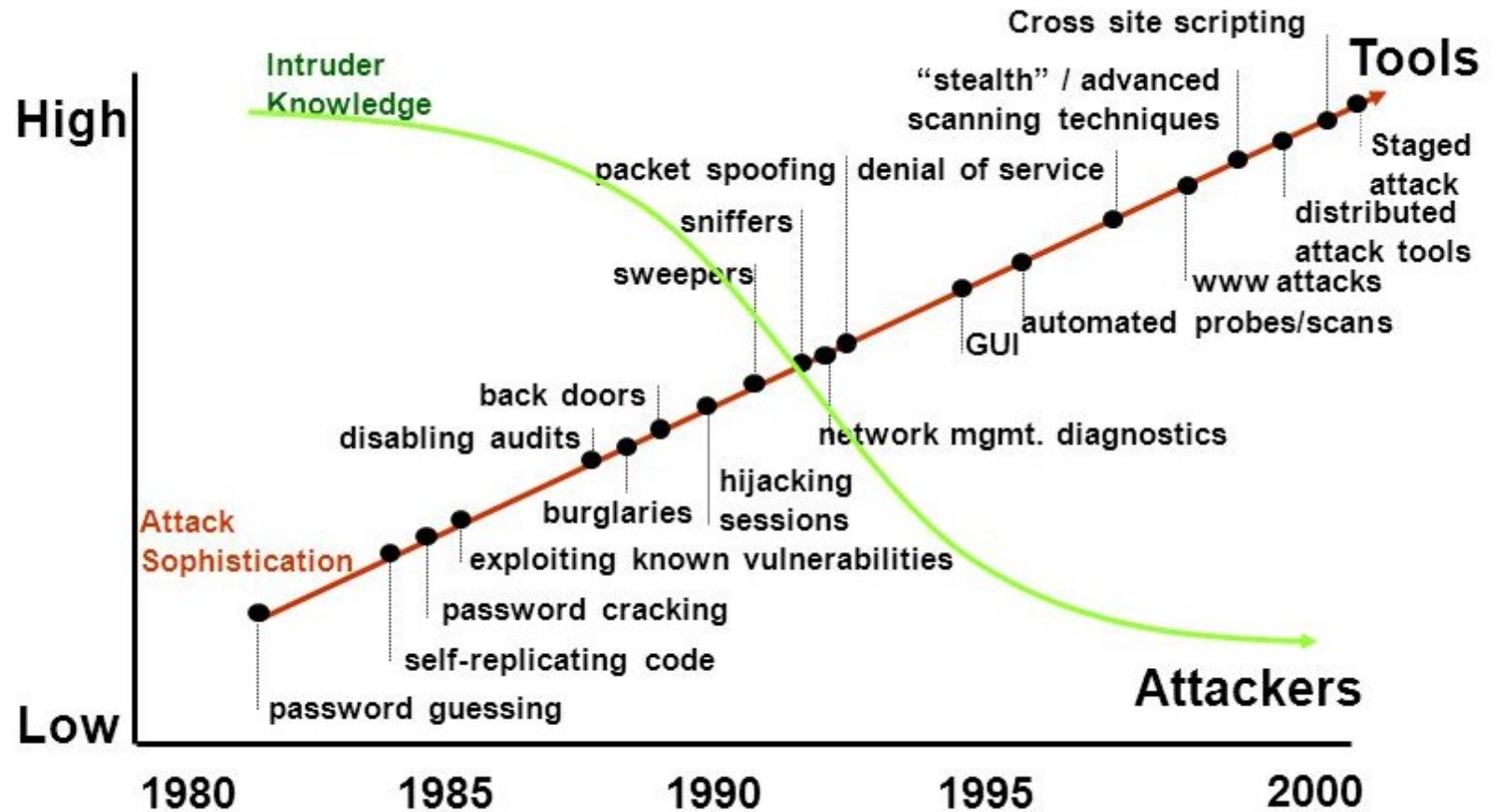


13.2 Threat Actor Tools

Introduction of Attack Tools

- To exploit vulnerability, a threat actor must have a technique or tool.
- Over the years, attack tools have become more sophisticated, and highly automated.
- These new tools require less technical knowledge to implement.

Attack sophistication vs. Intruder technical knowledge



Copyright: CERT, 2000

Evolution of Security Tools

- **Ethical hacking** involves using many **different types of tools** to test the network and end devices.
- To validate the security of a network and its systems, **many network penetration testing tools** have been developed
 - and many of these **tools can also be used by threat actors for exploitation.**
- **Threat actors** have also **created various hacking tools.**
 - **Cybersecurity personnel must also know** how to use these tools when performing network penetration tests.

Note: *Most of these tools are **UNIX or Linux based**; therefore, a security professional should have a strong UNIX and Linux background.*

Evolution of Security Tools (Contd.)

The following table lists some of the categories of common network penetration testing tools.

| Categories of Tools | Description |
|--------------------------|---|
| Password crackers * | Used to crack or recover the password. Eg:John the Ripper, Ophcrack |
| Wireless hacking tools * | Used to intentionally hack into a wireless network to detect security vulnerabilities. Eg:Aircrack-ng, Kismet |
| Packet crafting tools | Used to probe and test a firewall's robustness. Eg: Hping, Scapy, Netcat, Nemesis |
| Packet sniffers | Used to capture and analyze packets within traditional Ethernet LANs or WLANs. Eg: Wireshark, Tcpdump |
| Rootkit detectors | It is a directory and file integrity checker used by white hats to detect installed root kits. Eg: AIDE, Netfilter |
| Debuggers | Used by black hats to reverse engineer binary files when writing exploits and used by white hats when analyzing malware. Eg:GDB, WinDbg |
| Forensic tools | White hat hackers use these tools to sniff out any trace of evidence existing in a particular computer system. Eg: Sleuth Kit, Helix |

Evolution of Security Tools (Contd.)

| Categories of Tools | Description |
|------------------------------------|---|
| Hacking operating systems | These are preloaded with tools and technologies optimized for hacking. Eg: Kali Linux, SELinux, Backbox Linux, Blackarchlinux, Fedora security, Network security toolkit |
| Encryption tools | These tools use algorithm schemes to encode the data to prevent unauthorized access to the data. Eg: VeraCrypt, CipherShed |
| Network scanning and hacking tools | Used to probe network devices, servers, and hosts for open TCP or UDP ports. Eg: Nmap, SuperScan – IT Scanner, Angry IP Scanner, NetScanTools, MassScan |
| Vulnerability scanners | These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan VMs, BYOD devices, and client databases. Eg: Nessus, OpenVAS, Nikto, Nipper, Securia PSI |
| Fuzzers to search vulnerabilities | Used by threat actors when attempting to discover a computer system's security vulnerabilities. Eg: Skipfish, Wapiti, W3af |
| Vulnerability exploitation tools | These tools identify whether a remote host is vulnerable to a security attack. Eg: Metasploit, Core Impact, Social Engineering Toolkit, Netsparker |

Password Crackers

- Ide o proces obnovenia alebo uhádnutia hesla zo systému na prenos dát, alebo z úložísk, kde sa heslá nachádzajú.
- Tento proces používajú
 - **útočníci** na získanie neopraveného prístupu uhádnutím hesla
 - Patrí medzi najväčšie hrozby
 - **obrancovia** na obnovenie zabudnutého hesla
- Nástroje tohto typu môžu používať viacero metód
 - systematické skúšanie všetkých možných kombinácii hesla – **brute force**
 - závisí od zložitosti hesla, čím dlhšie heslo a použité špeciálne znaky tým dlhšie trvá zistiť správne heslo
 - slovníkový útok, kde útočník používa súbor, kde sa nachádzajú potencionálne správne heslá – **dictionary attack**
- Medzi nástroje na prelomenie hesiel patrí [19]:
 - John the Ripper
 - THC Hydra
 - Ophcrack
 - Medusa

Wireless Hacking Tools

- Bezdrôtové siete sú **viac náchylné** na sieťové bezpečnostné hrozby
- Bezdrôtové hackerské nástroje používajú neoprávnený prístup do bezdrôtových sietí na zistenie slabých miest v zabezpečení – hlavne 2 typy zraniteľností:
 - zlá konfigurácia
 - zlé šifrovanie
- Útočníci používajú tieto nástroje na generovanie útokov na bezdrôtové siete:
 - Aircrack-ng
 - Kismet
 - KisMac
 - FireSheep
 - Bully

13.3 Attackers and Their Tools

Summary

What Did I Learn in this Module?

- To understand network security, it is important to understand the terms such as threat, vulnerability, attack surface, exploit, and risk.
- Risk management is the process of providing protective measures by protecting the asset.
- Four common ways to manage risk are risk acceptance, risk avoidance, risk reduction, and risk transfer.
- Hacker is a term used to describe a threat actor. White hat hackers are ethical hackers that use their skills for good, ethical, and legal purposes.
- Grey hat hackers are individuals who commit crimes and do unethical things, but not for personal gain.
- Black hat hackers are criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks.

What Did I Learn in this Module? (Contd.)

- Many network attacks can be prevented by sharing information about Indicators of Compromise (IOC). CISA and NCSA are examples of cybersecurity promoting organizations.
- Attack tools have become more sophisticated, and highly automated.
- Many of the tools are Linux or UNIX based and knowledge of these are useful to a cybersecurity professional.
- Tools include password crackers, wireless hacking tools, network security scanning and hacking tools, packet crafting tools, packet sniffers, rootkit detectors, fuzzers to search vulnerabilities, forensic tools, debuggers, hacking operating systems, encryption tools, vulnerability exploitation tools, and vulnerability scanners.
- Categories of attacks include eavesdropping attacks, data modification attacks, IP address spoofing attacks, password-based attacks, denial-of-service attacks, man-in-the-middle attacks, compromised key attacks, and sniffer attacks.



Module 14

Common Threats and Attacks

Module Objective: Explain the various types of threats and attacks.

| Topic Title | Topic Objective |
|---|---|
| Malware | Describe types of malware. |
| Common Network Attacks - Reconnaissance, Access, and Social Engineering | Explain reconnaissance, access, and social engineering network attacks. |
| Network Attacks - Denial of Service, Buffer Overflows, and Evasion | Explain Denial of Service, buffer overflow, and evasion attacks. |

14.1 Malware

Types of Malware

- Malware is a code or software designed to damage, disrupt, steal, or inflict some other 'bad' or illegitimate action on data, hosts, or networks.
- The three most common types of malware are Virus, Worm, and Trojan horse a mnohé ďalšie

- Vírus \neq Malvér
- Vírus je podmnožinou malvéru



Viruses

- A virus is a type of malware that spreads by **inserting a copy of itself into another program.**
- After the program is run, viruses **spread** from one computer to another, thus infecting the computers.
- A simple virus may install itself **at the first line of code in an executable file.**
- Viruses can be harmless, for those that display a picture on the screen, or they can be destructive. They can also modify or delete files on the hard drive.
- Most viruses spread by
 - USB memory drives
 - CDs, DVDs
 - network shares
 - email. Email viruses are a common type of virus.
 - A ďalšie – vid' nasledujúce slajdy



Viruses

Zdroje nákazy

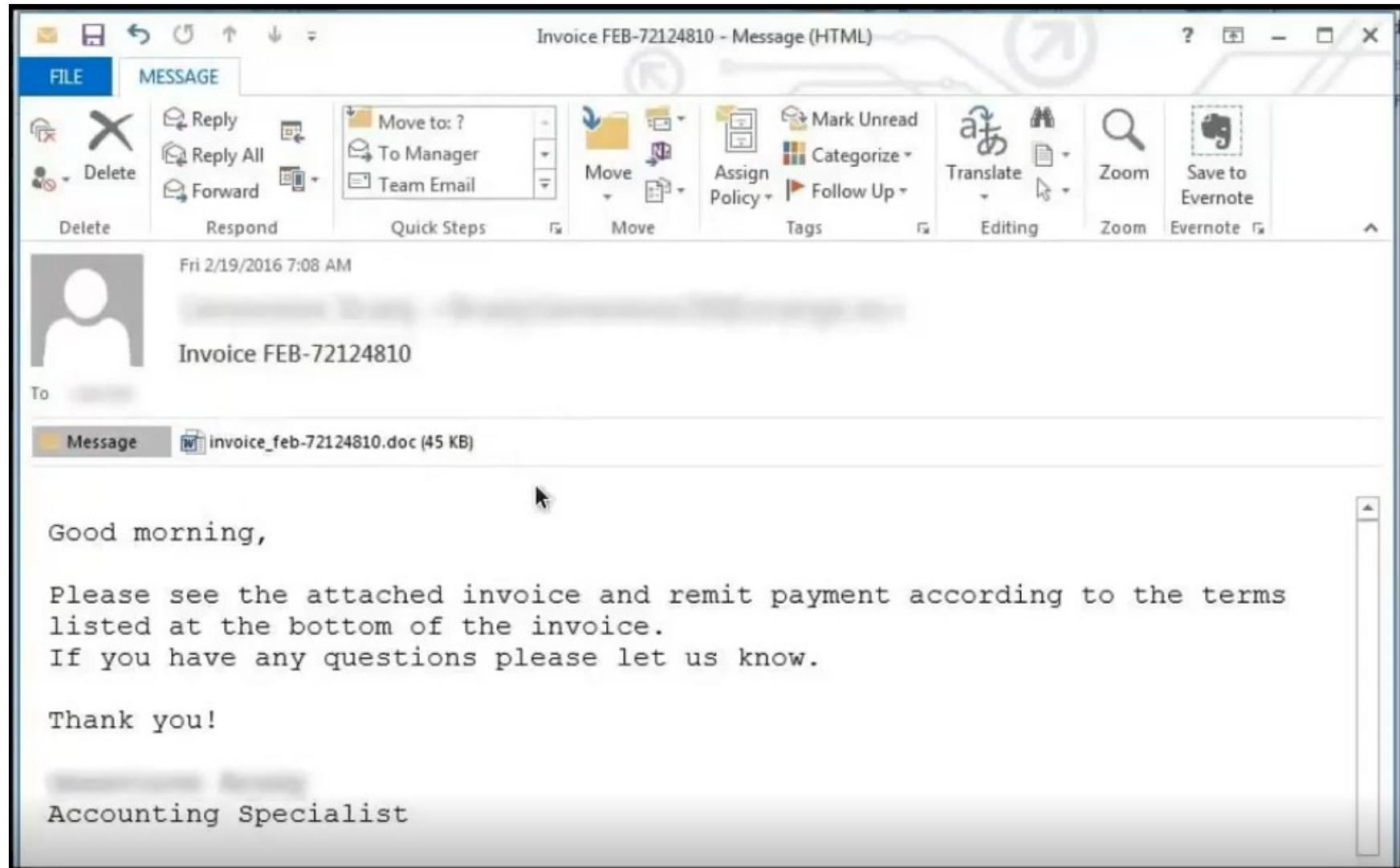
- „UltraSuper“ programy, hry

| NitroWar | | |
|---|----------------------|---|
| NitroWar | | |
| Important Announcements Rules, Tutorials and announcements. Please read carefully and leave your feedback. | 4 DISCUSSIONS | 6 MESSAGES Nitrowar uses now Xenforo! Ple... canduto, Aug 4, 2015 |
| -Downloadz- | | |
| Applications Source of free and latest computer programs and utilities for PC. Sub-Forums: 2 | 6,219 DISCUSSIONS | 6,223 MESSAGES Chief Architect Premier.v17.3.1... mitsumi, Today at 4:51 PM |
| Games Ultimate ISO resource for fast reliable games. Sub-Forums: 1 | 150 DISCUSSIONS | 161 MESSAGES HBA 2K16-CODEX EkThaTiger, Today at 1:01 PM |
| Movies Past movies to the very latest in various formats and qualities. Sub-Forums: 1 | 5,369 DISCUSSIONS | 5,369 MESSAGES San Andreas (2015) 720p BRRi... EkThaTiger, 9 minutes ago |
| TV Shows Newly released and/or completed shows & cartoons, so you won't have to miss an episode ever again. | 1,562 DISCUSSIONS | 1,577 MESSAGES The Player 2015 S01E01 720p ... andkas, 3 minutes ago |
| Anime Completed and on-going anime series/movies. | 0 DISCUSSIONS | 0 MESSAGES (Contains no messages) |
| Music Albums and singles in assorted qualities. | 1,146 DISCUSSIONS | 1,147 MESSAGES Danny Howard - BBC Radio 1s D... mitsumi, Today at 6:27 PM |
| E-Books & Tutorials Large collection of eBooks, magazines, and tutorials. Sub-Forums: 2 | 3,171 DISCUSSIONS | 3,181 MESSAGES LYNDA. - FOUNDATIONS OF NET... mitsumi, Today at 6:29 PM |

Viruses

Zdroje nákazy

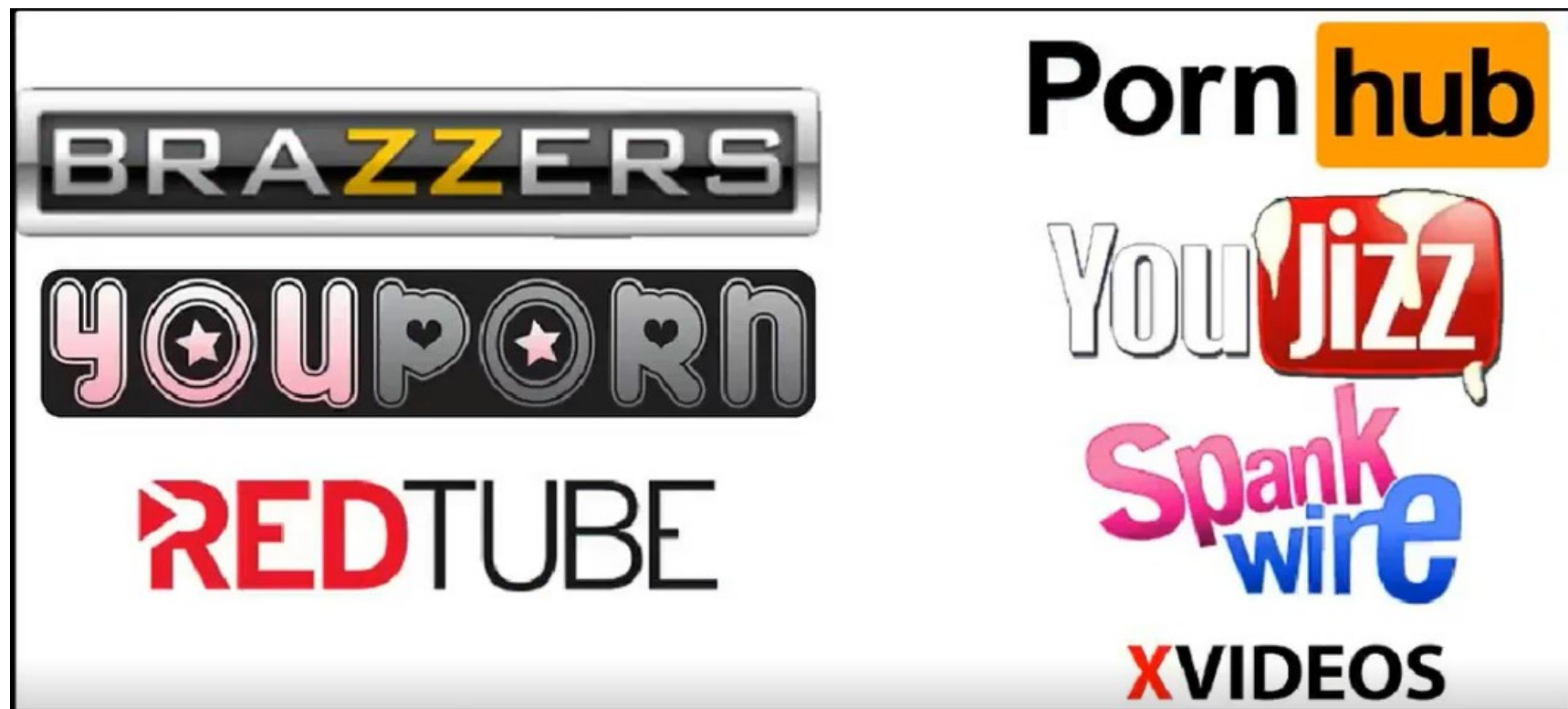
- „UltraSuper“ programy, hry
- **Prílohy emailov**



Viruses

Zdroje nákazy

- „UltraSuper“
programy,
hry
- Přílohy emailov
- **Pochybné
webstránky**



Viruses

Zdroje nákazy

- „UltraSuper“ programy, hry
- Přílohy emailov
- Pochybné webstránky
- **Dôveryhodné stránky**

EC-Council | iClass

Home Our CONTENT Our TECHNOLOGY Your EXPERIENCE About Us Schedule

Specials

Join the new Generation of **InfoSec** Leaders!

C|CISO
Certified Chief Information Security Officer

Student/Member login

Please login here to access your course, or to access any other member specific information.

Login

iClass

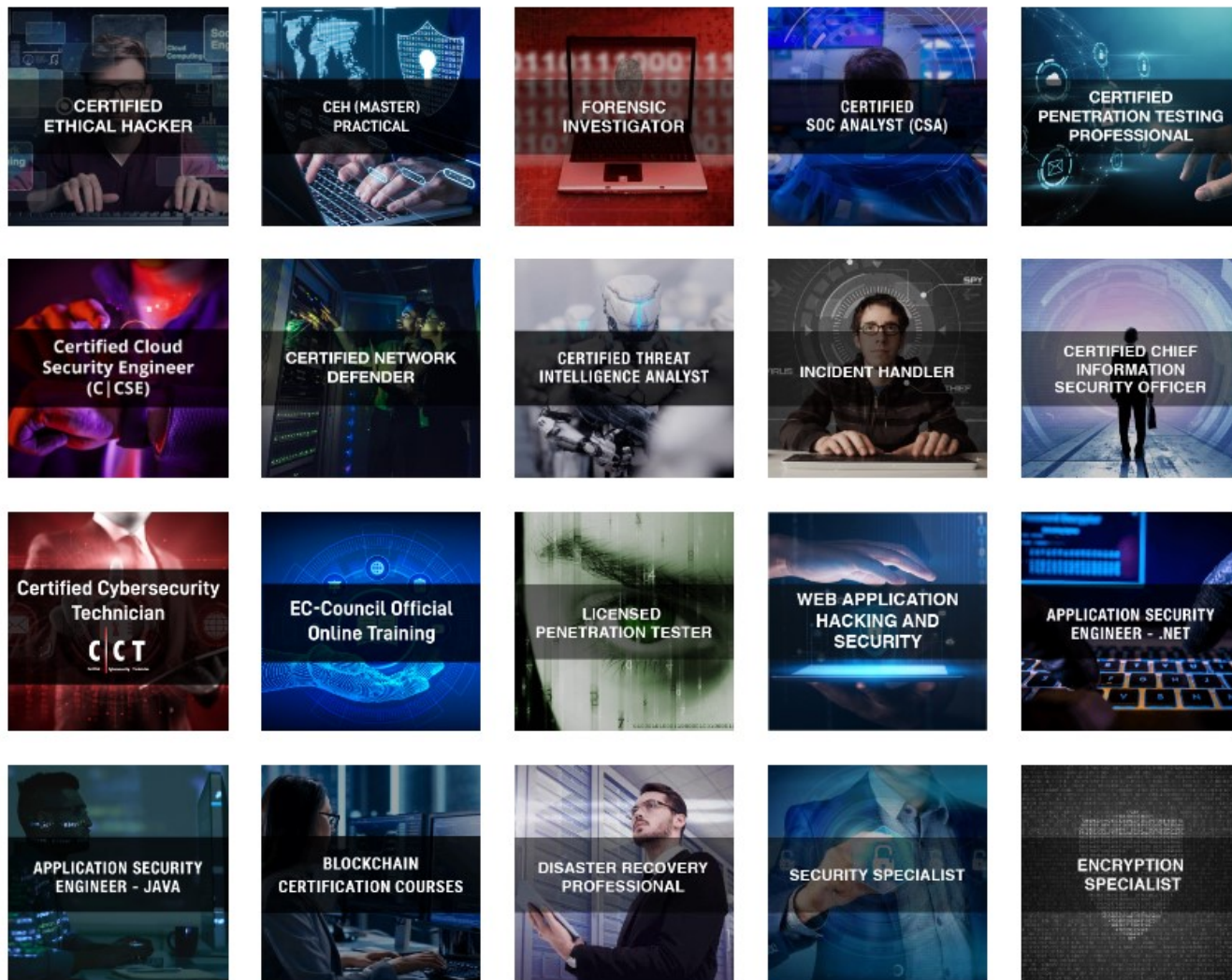
Featured Video: CSCU: If you aren't training, they aren't getting it!

iClass is EC-Council's Official Training Portal. Here you will find the most flexible, least expensive training options for

EC-Council

- Na okraj
 - Mnoho zaujímavých certifikácií a školení

Show all Advanced Core Fundamentals iClass Management Security Awareness Specialist



<https://www.eccouncil.org/>

Viruses

Zdroje nákazy

- „UltraSuper“ programy, hry
- Prílohy emailov
- Pochybné webstránky
- Dôveryhodné stránky
- **Reklamy na stránkach**
- Dokumenty a obrázky

**Make \$437.55
A DAY From Your
Facebook Account...!**

Start Now

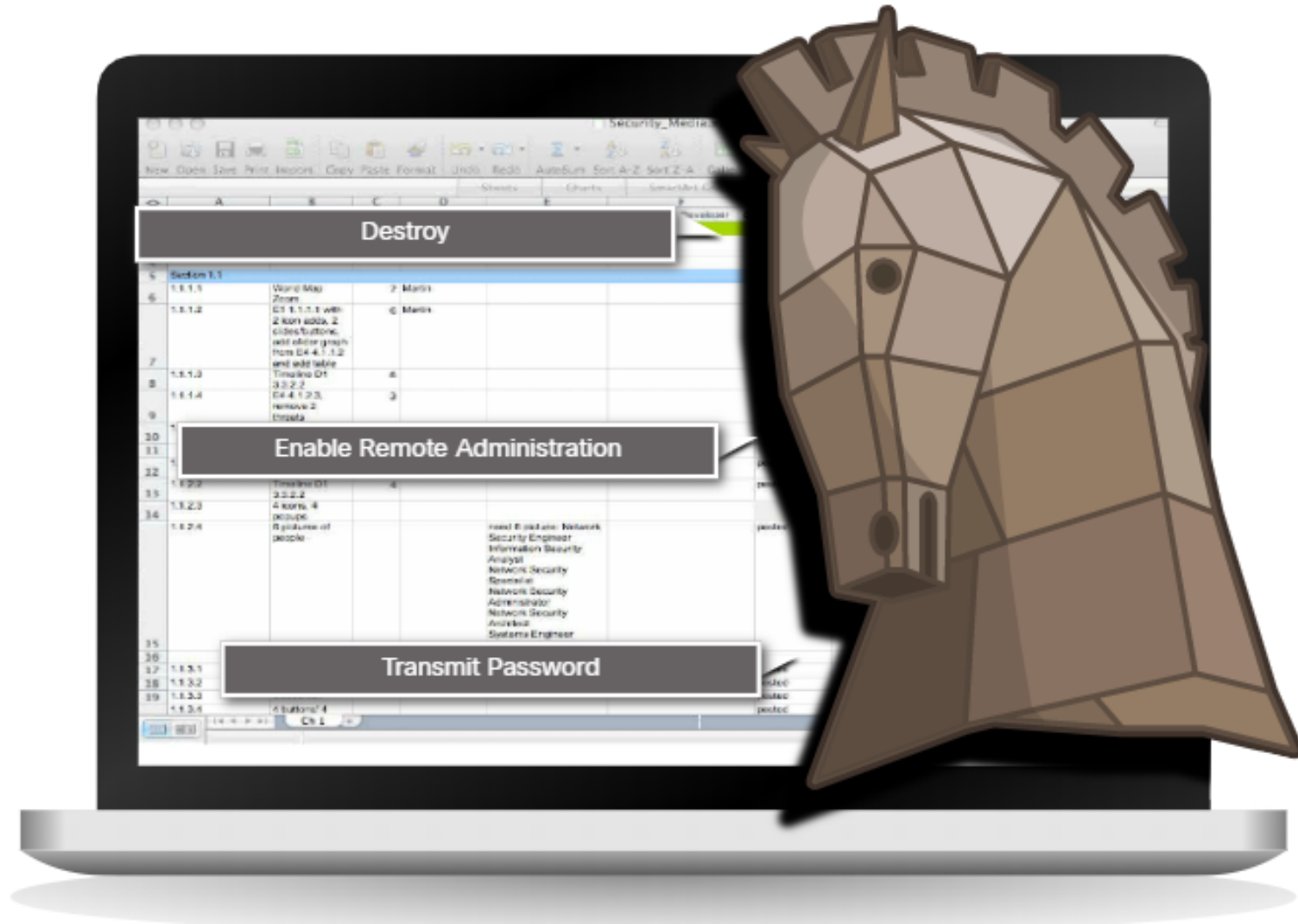
FREE iPad

Click Here

Common Threats and Attacks

Trojan Horses

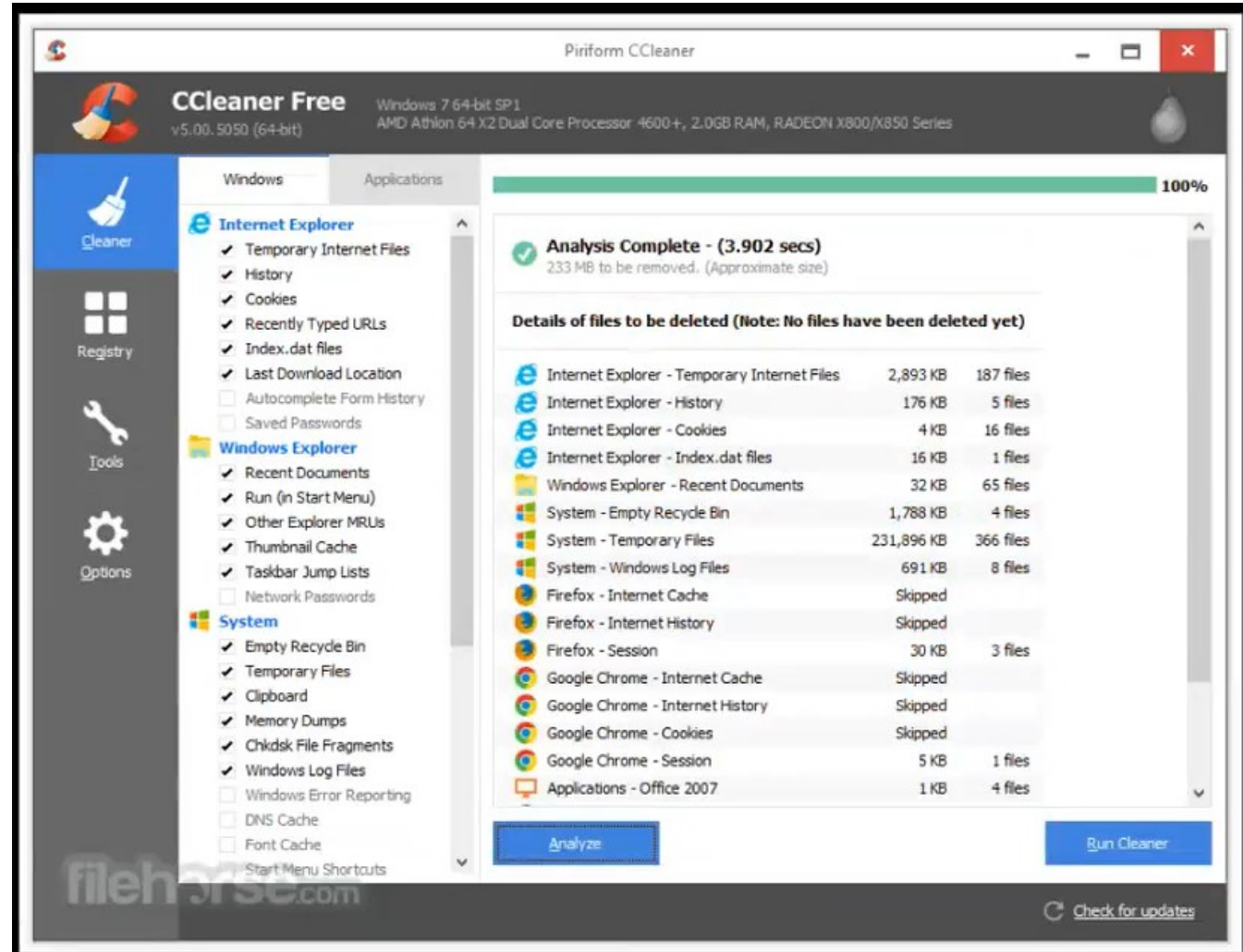
- Trojan horse malware is a **software** that appears to be **legitimate**, but it contains **malicious code** which exploits the privileges of the user that runs it.
- Trojans are found attached to online games.
- Users are commonly tricked into loading and executing the Trojan horse on their systems
- Custom-written Trojan horses with a specific target are **difficult to detect**.



Common Threats and Attacks

Trojan Horses - example

- Zrýchlíme váš počítač.
- Vyčistíme váš počítač.



Trojan Horses Classification

Trojan horses are usually classified according to the **damage** that they cause, or the **manner** in which they breach a system.

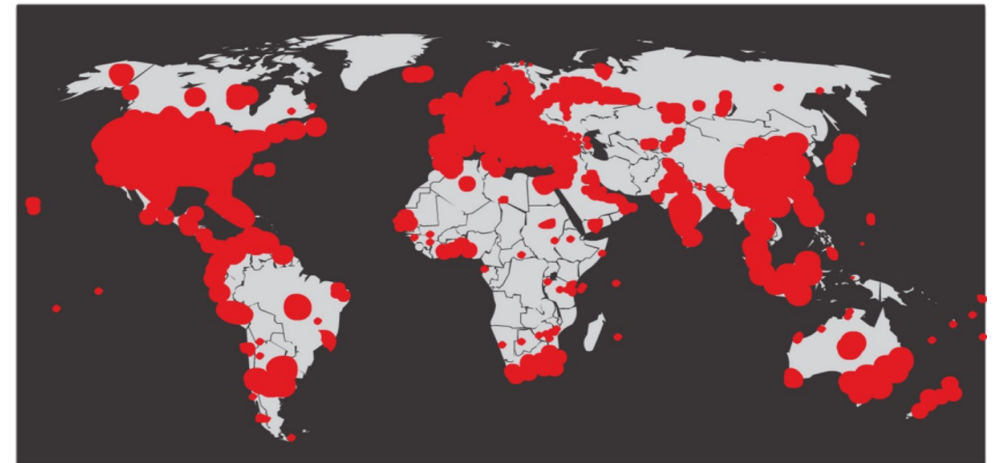
| Type of Trojan Horse | Description |
|----------------------------|--|
| Remote-access | Enables unauthorized remote access – immediate or through back door |
| Data-sending | Provides the threat actor with sensitive data, such as passwords. |
| Destructive / damage | Corrupts or deletes files. |
| Proxy | Uses the victim's computer as the source device to launch attacks and perform other illegal activities. |
| FTP | Enables unauthorized file transfer services on end devices. |
| Security software disabler | Stops antivirus programs or firewalls from functioning. |
| Denial of Service (DoS) | Slows or halts network activity. |
| Keylogger | Actively attempts to steal confidential information, such as credit card numbers, by recording keystrokes entered into a web form. |

Worms

- Computer worms are similar to viruses because they replicate themselves by independently exploiting vulnerabilities in networks.
- Worms can slow down networks as they spread from system to system.
- Worms can **run without a host program**.
- However, once the host is infected, the worm spreads rapidly over the network.
- In 2001, the Code Red worm had initially infected 658 servers. Within 19 hours, the worm had infected over 300,000 servers.



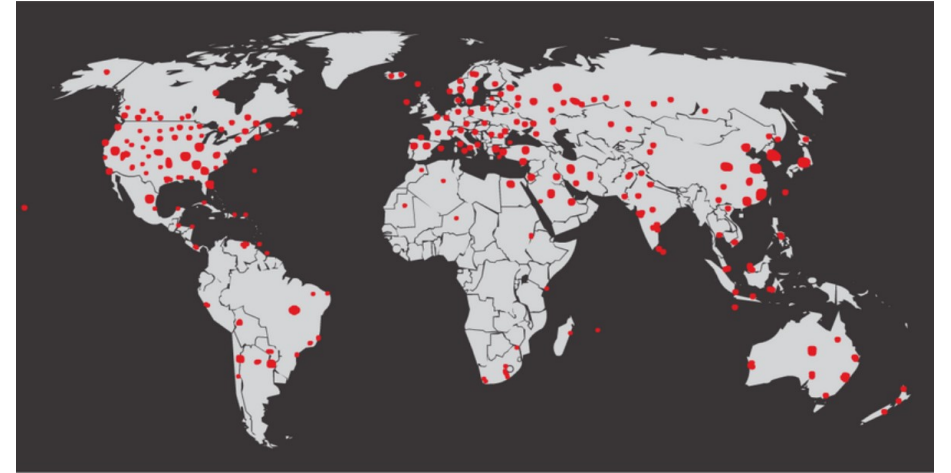
Initial Code Red Worm Infection



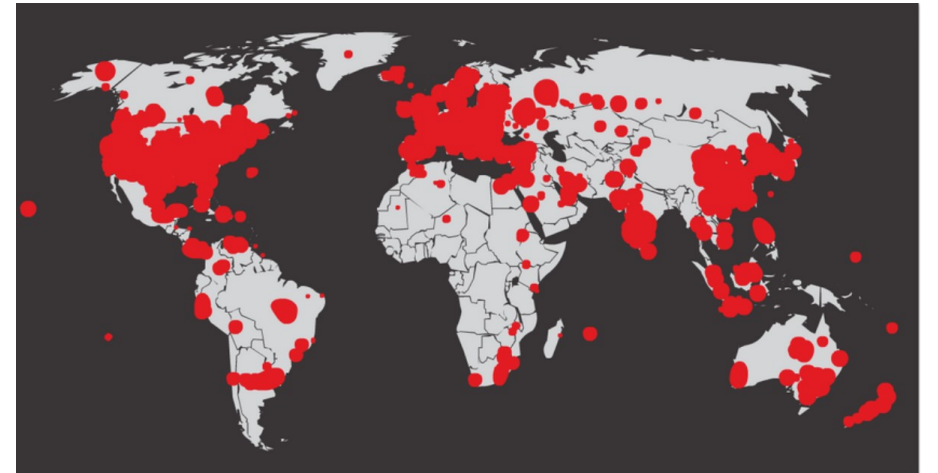
Code Red Infection 19 hours later

Worms (Contd.)

- The initial infection of the SQL Slammer worm is known as the worm that ate the internet.
- SQL Slammer was a Denial of Service (DoS) attack that exploited a buffer overflow bug in Microsoft's SQL Server.
- The number of infected servers doubled in size every 8.5 seconds.
- The infected servers did not have the updated patch that was released 6 months earlier.
- Hence it is essential for organizations to implement a security policy requiring updates and patches to be applied in a timely fashion.



Initial SQL Slammer Infection



SQL Slammer Infection 30 minutes later

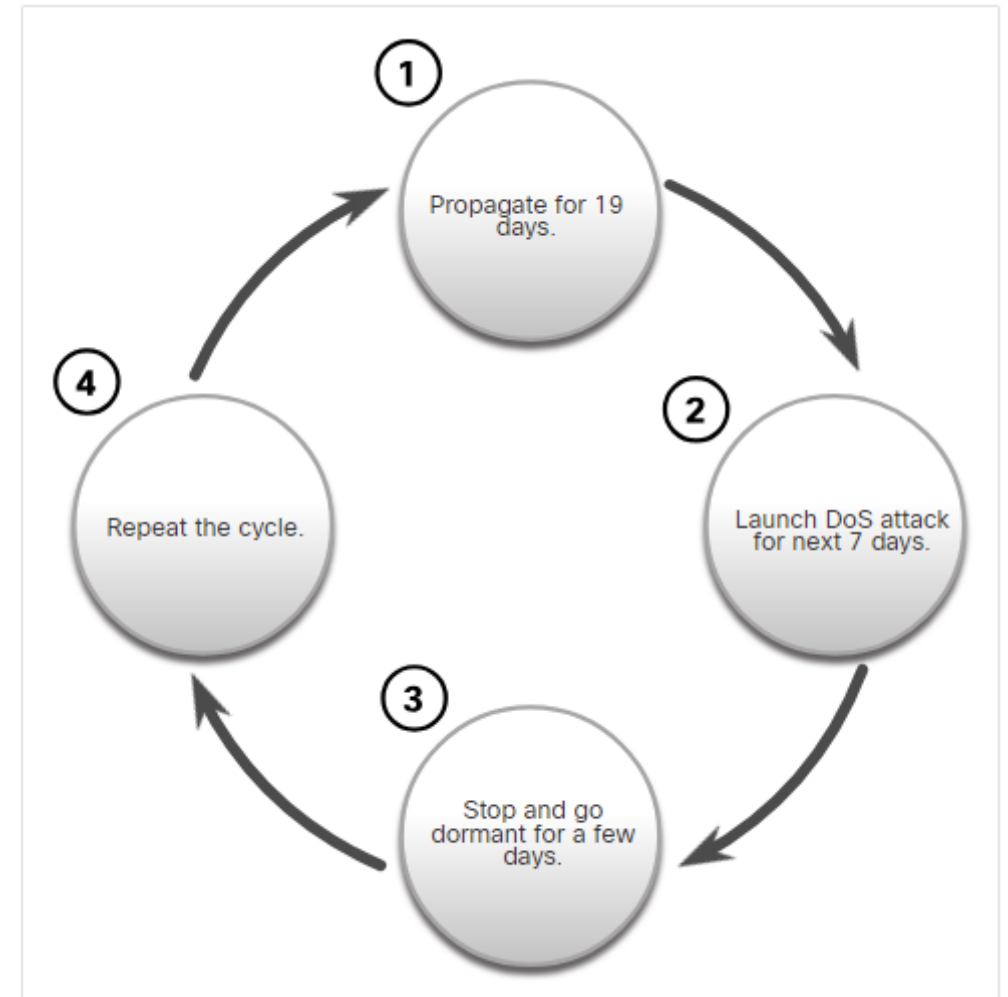
Worm Components

The three worm components are as follows:

- **Enabling vulnerability** - A worm installs itself using an exploit mechanism, such as an email attachment, an executable file, or a Trojan horse, on a vulnerable system.
- **Propagation mechanism** - After gaining access to a device, the worm replicates itself and locates new targets.
- **Payload** - Any malicious code that results in some action is a payload. Most often this is used to create a backdoor that allows a threat actor to access the infected host or to create a DoS attack.

Worm Components (Contd.)

- Worms are self-contained programs that attack a system to exploit a known vulnerability.
- Upon successful exploitation, the worm copies itself from the attacking host to the newly exploited system and the cycle begins again.
- This propagation mechanism is commonly deployed in a way that is difficult to detect.
- **Note:** Worms never stop spreading on the internet. After they are released, worms continue to propagate until all possible sources of infection are properly patched.



Code Red Worm Propagation

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Ransomware

- Ransomware is a malware that denies access to the infected computer system or its data.
- Ransomware frequently uses an encryption algorithm to encrypt system files and data.
- Email and malicious advertising, also known as malvertising, are vectors for ransomware campaigns.
- Social engineering is also used, when cybercriminals pretending to be security technicians make random calls at homes and persuade users to connect to a website that downloads ransomware to the user's computer.

```
!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
  http://en.wikipedia.org/wiki/RSA_(cryptosystem)
  http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

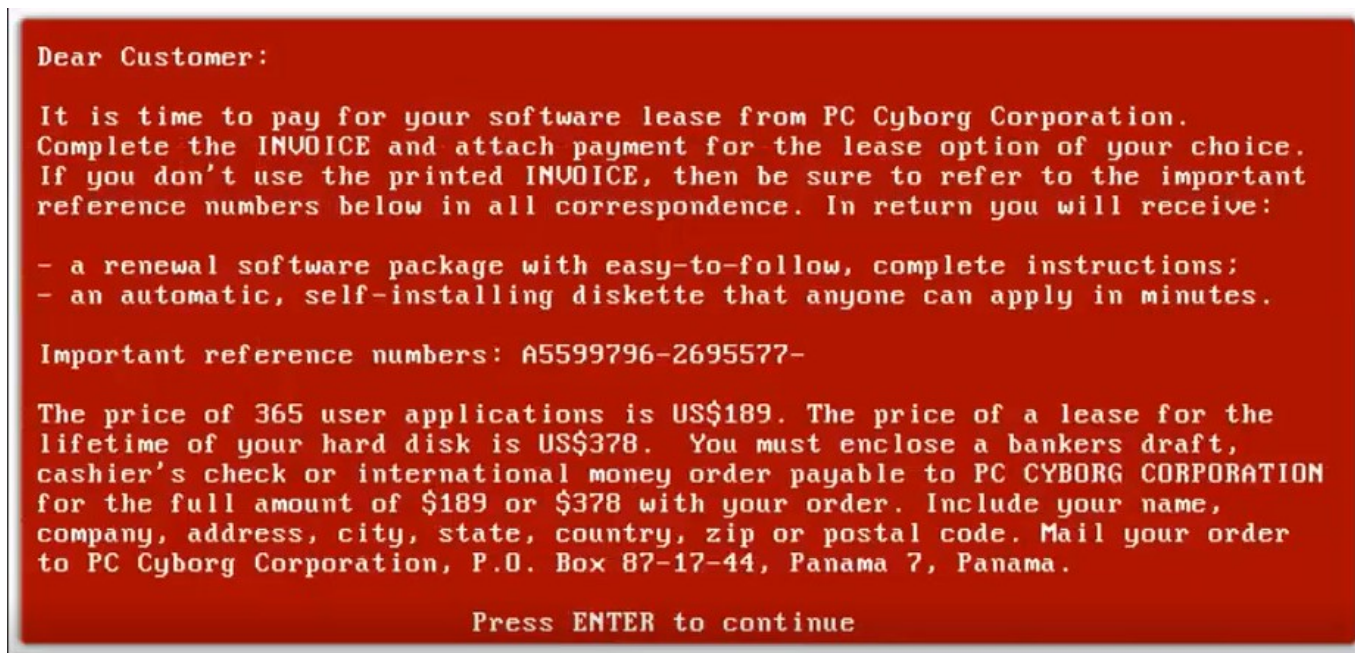
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
  1. http://6dbxgqam4crv6rr6.tor2web.org/F99C410F07678BEF
  2. http://6dbxgqam4crv6rr6.onion.to/F99C410F07678BEF
  3. http://6dbxgqam4crv6rr6.onion.cab/F99C410F07678BEF
  4. http://6dbxgqam4crv6rr6.onion.link/F99C410F07678BEF

If all of this addresses are not available, follow these steps:
  1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
  2. After a successful installation, run the browser and wait for initialization.
  3. Type in the address bar: 6dbxgqam4crv6rr6.onion/F99C410F07678BEF
  4. Follow the instructions on the site.

!!! Your personal identification ID: F99C410F07678BEF !!!
```

História ransomware

- 1989 AIDS Trojan
 - Šířený medzi účastníkmi konferencie WHO AIDS / 20 000 ľudí
 - \$189



História ransomware

- 1989 AIDS Trojan
 - Šírený medzi účastníkmi konferencie WHO AIDS / 20 000 ľudí
 - \$189
- 2004 GPCoder
 - Ransomnote
 - V adresári usera sa objaví textový súbor ako zaplatiť
- 2012 Policajný vírus
 - Odpustok za fiktívne trestné činy

IPA Najvyšší kontrolný úrad Slovenskej republiky
Ministerstvo vnútra
International Police Association

Podporovaný a Chránený

paysafe card Ukash

IP: [redacted]
Krajiny: SK Slovakia
Región: Bratislava
Mesto: Bratislava
ISP: [redacted]
Operačný Systém: Windows XP (32-bit)
Meno: [redacted]

POZOR! Váš počítač je zablokovaný kvôli aspoň jednému z dôvodov uvedených nižšie.

Bolí ste porušenie «autorského práva a súvisiacich práv» (Video, Hudba, Software) a nedovolené použitie alebo distribúciu obsah chránený autorskými právami, a tým porušil článok 128 trestného zákonníka Slovenskej Republiky.

Článok 128 trestného zákonníka stanovuje pokuty 200-500 minimálnej mzdy alebo pozbavenie slobody na 2 až 8 rokov.

Bolí ste chytení pri prezeraní alebo distribúciu zakázané produkcie pornografickým obsahom (Detská pornografia/Zoofilia a atď). A tým porušujete článok 202 trestného zákonníka Slovenskej Republiky.

Článok 202 trestného zákonníka stanovuje odňatia slobody na 4 až 12 rokov.

Protiprávne prístup k počítačovým údajom bol zahájený z počítača, alebo ste boli...

Článok 208 trestného zákonníka stanovuje pokutu až do výšky SKK 3.000.000 a/alebo odňatia slobody na dobu 4 až 9 rokov.

PIN kód Suma
[input] 2000
1 2 3 4 5 6 7 8 9 0
Zaplatiť PaySafeCard Zaplatiť Ukash

Kde môžem kúpiť PaySafeCard?
PaySafeCard dostaneš na viac ako 101 čerpacích staniaciach Agipu a OMV, vo vybraných pobočkách stávkovej kancelárie Tipsport a vo všetkých predajných miestach GG Tabaku.

GG TABAK Agip Tipsport OMV AXASOFT

Kde môžem kúpiť Ukash?
Dalo by sa kúpiť trestný zákonník na mnohých...

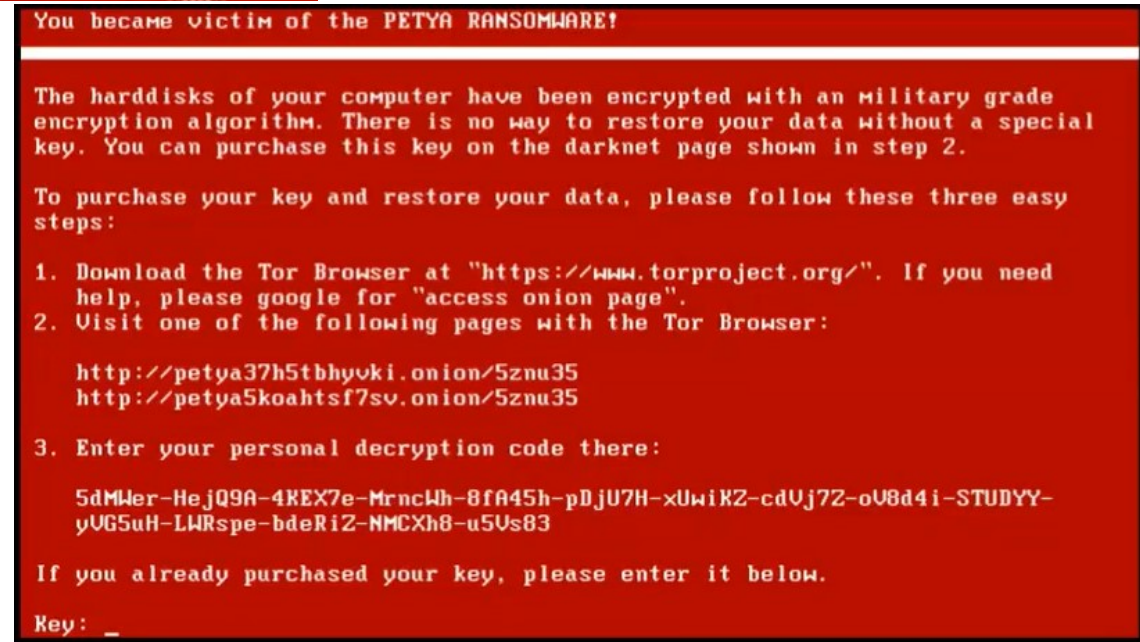
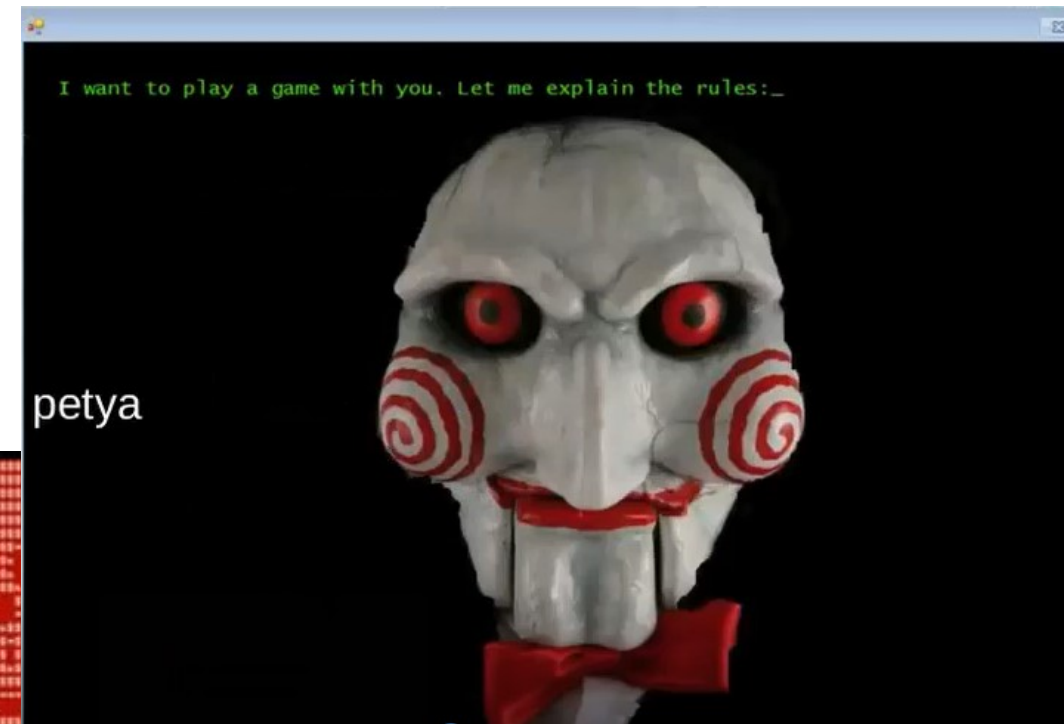
História ransomware

- 1989 AIDS Trojan
 - Šírený medzi účastníkmi konferencie WHO AIDS / 20 000 ľudí
 - \$189
- 2004 GPCoder
 - Ransomnote
 - V adresári usera sa objaví textový súbor ako zaplatiť
- 2012 Policajný vírus
 - Odpustok za fiktívne trestné činy
- **2013 Cryptolocker**
 - Už platby cez bitcoin
 - Od 2008 už ransomware s využitím asymetrických šifier (RSA)



História ransomware

- 2014 – 2016 Ransom boom
 - Locky, Cerber, **Jigsaw**
 - mal statický kľúč na symetrické šifrovanie, čiže dal sa aj takto dešifrovať
 - Autori predpokladali – že obeť zaplatí, a klikne na nejaký odkaz, ktorý overí, či na bitcoin peňaženke je daná suma.
 - Čo sa ale dalo urobiť... obeť odchytil odpoveď z nejakej služby, ktorá poskytovala informáciu o zostatkoch na bitcoin peňaženkách, zmenili tú hodnotu, povedali, áno, už tam máš tú sumu 200 \$ v bitcoinoch, a ransomver dešifroval PC
 - TeslaCrypt, **Petya**
 - Návrat späť o 20 rokov graficky
 - Nešifroval len dáta, ale aj samotný zavádzač OS – master boot record na disku
 - Čiže nenabootoval samotný Win, až kým systém nebol reinštalovaný, alebo petya nebola prelomená



História ransomware

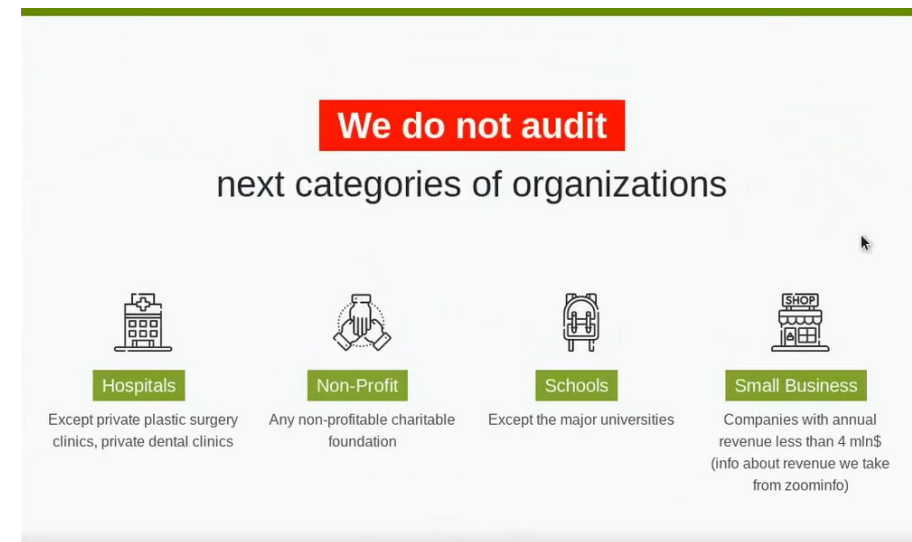
- 2017
 - WannaCry
 - Equation group je vysoko sofistikovaným aktérom hrozby
 - Dražili exploity od NSA
 - Jeden aj na OS Win od XP až po win 7 ...10
 - Na diaľku kompromitovať OS Win/ 445 samba
 - Širil sa z jedného PC na ďalšie a do celého sveta
 - v SR, Nemocnica v Nitre bola zašifrovaná
 - 2 týždne pred tým dostali všetky inštitúcie varovanie, že niečo takéto hrozí
 - Stačilo do internetu zakázať Windows zdieľanie
 - NotPetya
 - Cyber zbraň, voči ukrajinským inštitúciám
 - Iné farby ako Petya
 - Ničila zarádzač Windows
 - Skôr destroyer ako ransomware
 - Nenechala si kľúč, ani si ho nikam neposlala
 - Ako neskôr v čase olympijských hier – Tokyo – Olympic destroyer



https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Súčasnost' ransomware

- Ransomver je tu stále, stále vzniká nový
- 2021
 - DarkSide
 - Útok na pipeline, počítačový systém, nemohli palivo dopraviť do čerpacích staníc
 - Výkupné 70 mil., 40 mil, ... obnovili činnosť
 - REvil
 - sa zviditeľnil v 06/2021
 - Kaseya – poskytovala nástroje pre správu pre poskytovateľov, ktorí spravujú infraštruktúru svojich zákazníkov (managed service providers)
 - Partner Revilu zašifroval tisíce firiem
 - Revil ustúpil, vypol biznis, OČTK zapracovali
 - Bolo to dešifrované

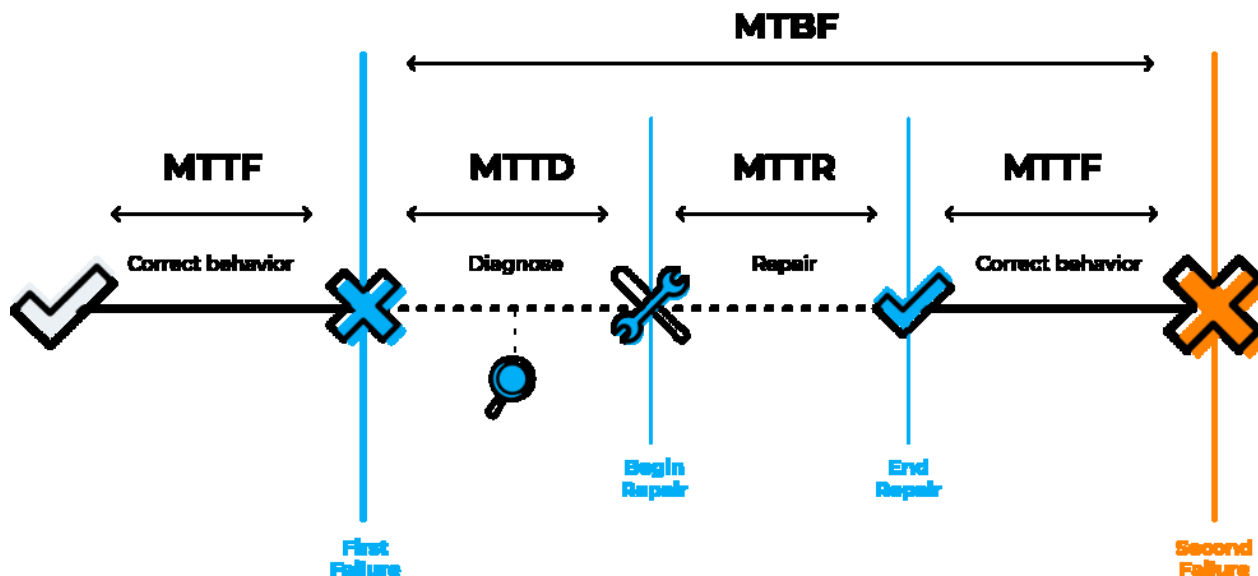


- Prepracovaná organizácia
 - Autori ransomvéru
 - Partneri / Sprostredkovatelia
 - Podpora pre obeť so zaplacením
 - Získanie zliav
 - Vyjednávanie s útočníkmi
 - „Etické princípy“
 - A ich výnimky
 - Fínsko – psychiatrická klinika – 400 tis. \$

Odhalenie útočníkov - limity

- Dlhodobá priemyselná špionáž
 - Tajné služby
 - Medzinárodné cyber crimi skupiny
 - Ciele dosiahnu do 120 dní
- MTTD
 - 160 – 240 dní

- Masové zraniteľnosti
 - Zraniteľnosť VPN softvéru
 - Zraniteľnosť MS exchange
 - Ciele dosiahnu...
 - Od počiatkovej fázy po exfiltráciu aj vynesenie nejakých citlivých informácií: 4 hod



MTTF - mean time to fix

MTBF - mean time between failure

Ransomware referencie

- Everything you need to know about ransomware: Understand. Prevent. Recover
<https://ransomware.org/>
- Pomoc s odomknutím digitálneho života bez platenia útočníkom
<https://www.nomoreransom.org>
- Spotify Podcast: Threat Report SK
<https://open.spotify.com/show/7Hug9kUtQ5xGXKn3qRWKNr>



The image shows a podcast episode cover for 'Threat Report SK'. The cover features a dark background with a globe and the text 'Kaseya Attack MS Vulnerabilities' and 'THREAT REPORT'. Below the globe are four circular portraits of the hosts: Richard Kiškováč, Lukáš Hlavička, Milan Kyselica, and Ladislav Bačo.

PODCAST EPISODE

Kaseya ransomware útok a zraniteľnosti MS Windows

Threat Report SK

Jul 2021 · 1 hr 5 min

▶ + ...

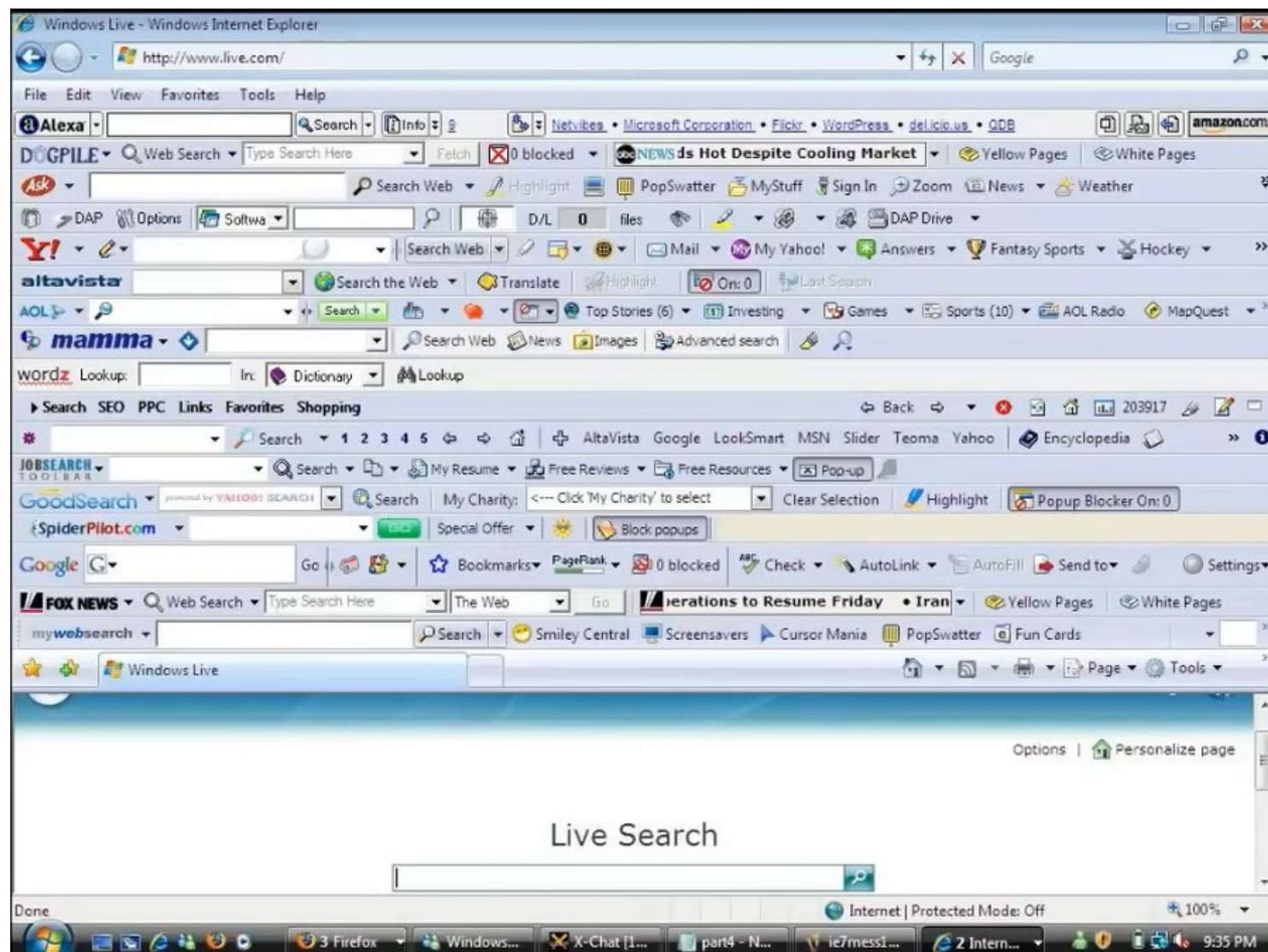
Episode Description

Detailný popis ransomware útoku prostredníctvom riešenia Kaseya a analýza nových zraniteľností operačného systému MS Windows. Diskutujú Richard Kiškováč, Laco Bačo, Lukáš Hlavička a Milan Kyselica

See all episodes

Adware

- Toolbary v prehliadači
 - Obsahujú aktívny kód
 - Užitočný
 - Ale aj adware – reklamný softvér
 - Využitý na škodlivú činnosť
 - Pri aktualizácií
 - Alebo spojené s trójskym koňom



Extrém roku 2005

Spyware / špionážny SW

- zhromažďovanie informácií o používateľovi
- a odosielanie informácií inému subjektu bez súhlasu používateľa
- Realizácia cez
 - systémový monitor
 - trójsky kôň
 - Adware
 - sledovacie súbory cookie
 - **Keyloggery**
 - Zaznamenáva stlačené klávesy

```
[*Local Area Connection 2 - 11:24]
[Alt + Tab]

[Task Switching - 11:24]
[Tab][Tab]

[Process Monitor - Sysinternals: www.sysinternals.com - 11:39]
[Next][Next][Next][Next][PageUp][PageUp][PageUp][Control + L]

[Process Monitor Filter - 11:39]
wwritewrite

[Process Monitor - Sysinternals: www.sysinternals.com - 11:40]
[Control + L]

[Process Monitor Filter - 11:40]
ccleaner

[Event Properties - 11:40]
[Control + C]

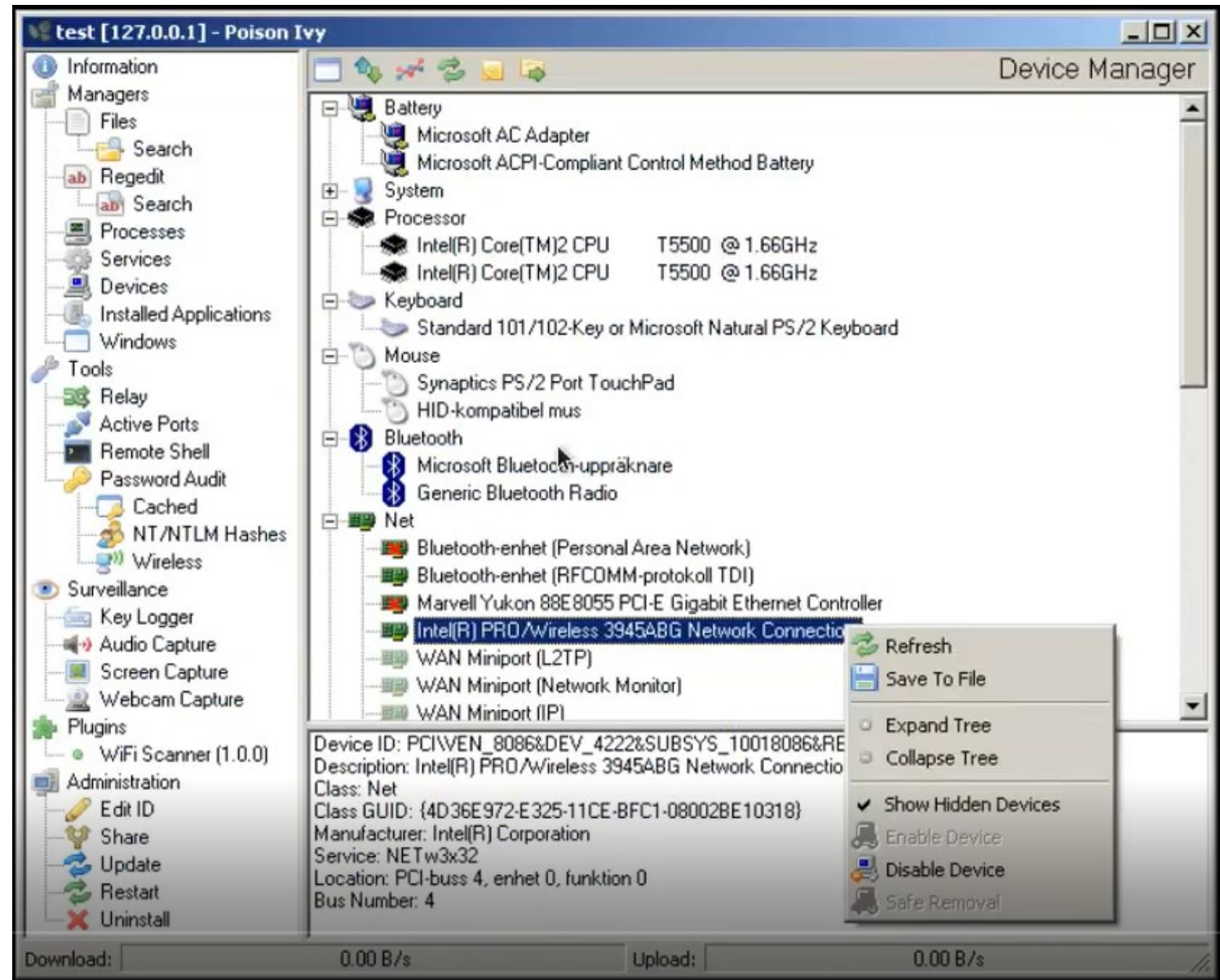
[tracing - 11:40]
[Control + V][Enter]
```

Report z keyloggeru, naformátovaný v HTML, odosielaný každú minútu

Remote Access Tools

RAT

- Infikovanie PC
- Vytvorenie back door
- Ovládanie PC
 - Prezerá súborový systém
 - Vidí bežiacie procesy
 - Otvorí príkazový riadok
 - Vidí info o PC
 - Špionáž
 - Zapne keylogger (odchytí heslá)
 - Zapne zvukové nahrávky
 - Snímky obrazovky, web kamery



Starší RAT tool - Poison Ivy

Other Malware

The examples of modern malware are as follows:

| Type of Malware | Description |
|-----------------|---|
| Scareware | Zahŕňa podvodný softvér, ktorý využíva sociálne inžinierstvo na šokovanie alebo vyvolanie úzkosti vytváraním vnímania hrozby. Vo všeobecnosti je zameraný na nič netušiaceho používateľa a pokúša sa ho presvedčiť, aby infikoval počítač podniknutím krokov na riešenie falošnej hrozby. |
| Phishing | Attempts to convince people to divulge sensitive information. Examples include receiving an email from their bank asking users to divulge their account and PIN numbers. |
| Rootkits | Nainštalované na kompromitovanom systéme. Po nainštalovaní naďalej skrýva svoje narušenie a poskytuje privilegovaný prístup k aktérovi hrozby. |
| Spyware | Used to gather information about a user and send the information to another entity without the user's consent. Spyware can be a system monitor, Trojan horse, Adware, tracking cookies, and key loggers. |
| Adware | Displays annoying pop-ups to generate revenue for its author. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites. |

Common Malware Behaviors

- Computers infected with malware often exhibit one or more of the following symptoms:
 - Appearance of strange files, programs, or desktop icons
 - Antivirus and firewall programs are turning off or reconfiguring settings
 - Computer screen is freezing or system is crashing
 - Emails are spontaneously being sent without your knowledge to your contact list
 - Files have been modified or deleted
 - Increased CPU and/or memory usage
 - Problems connecting to networks
 - Slow computer or web browser speeds
 - Unknown processes or services running
 - Unknown TCP or UDP ports open
 - Connections are made to hosts on the Internet without user action
 - Strange computer behavior
- **Note:** Malware behavior is not limited to the above list.

Categories of Network Attacks

Malware is a means to get a payload delivered .

When a payload is delivered and installed, it can be used to cause a variety of network-related attacks from the inside as well as from the outside.

Threat actors use the previously mentioned tools or a combination of tools to create various attacks.

1. Reconnaissance attacks / Prieskumné útoky
2. Útoky na získanie prístupu / Access attacks
3. Sociálne inžinierstvo
4. DoS, DDoS
5. Útok využívajúci pretečenie vyrovnávacej pamäte
6. Útoky využívajúce zraniteľnosti sieťových protokolov a služieb

14.2 Common Network Attacks - Reconnaissance, Access, and Social Engineering

Reconnaissance Attacks

- Reconnaissance is information gathering.
- Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities.
- Ak sa útočníci zameriavajú na koncový bod v sieti, napr. počítač alebo server tak v tomto prípade sa prieskumný útok môže nazývať aj ako profilovanie hostiteľa
- Recon attacks precede access attacks or DoS attacks.

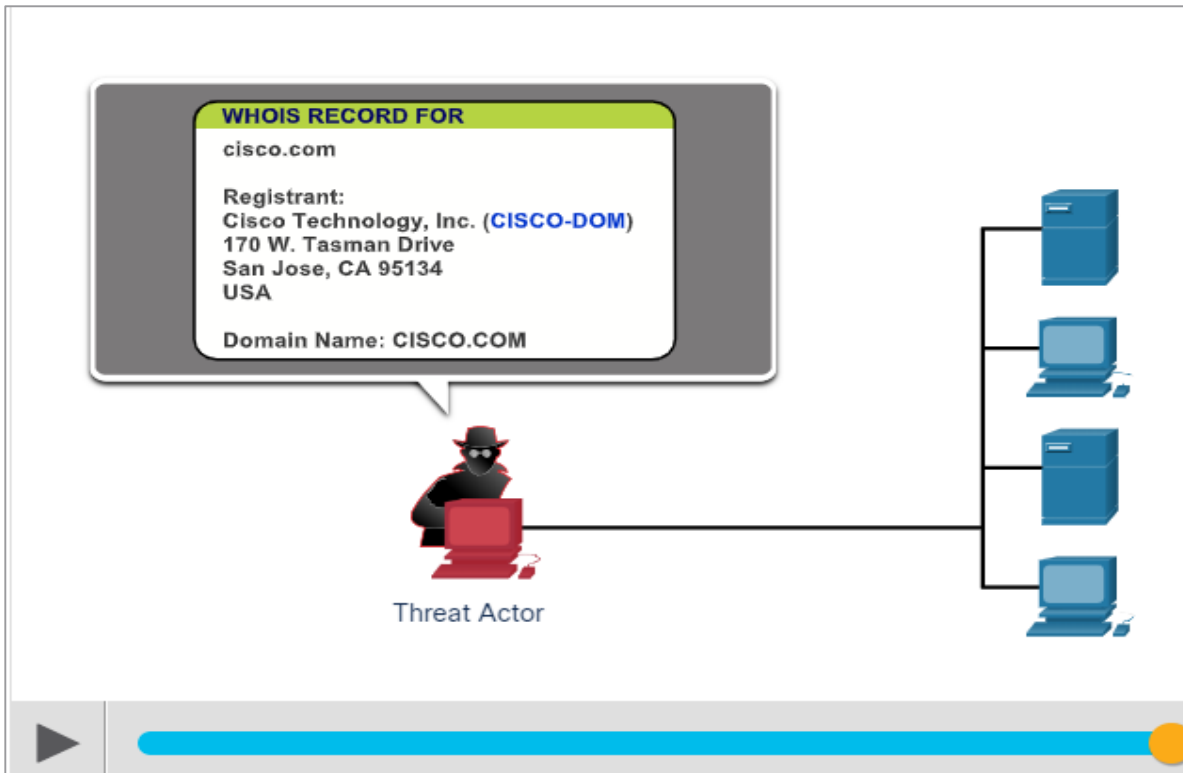
Reconnaissance Attacks (Contd.)

The techniques used by malicious threat actors to conduct reconnaissance attacks are as follows:

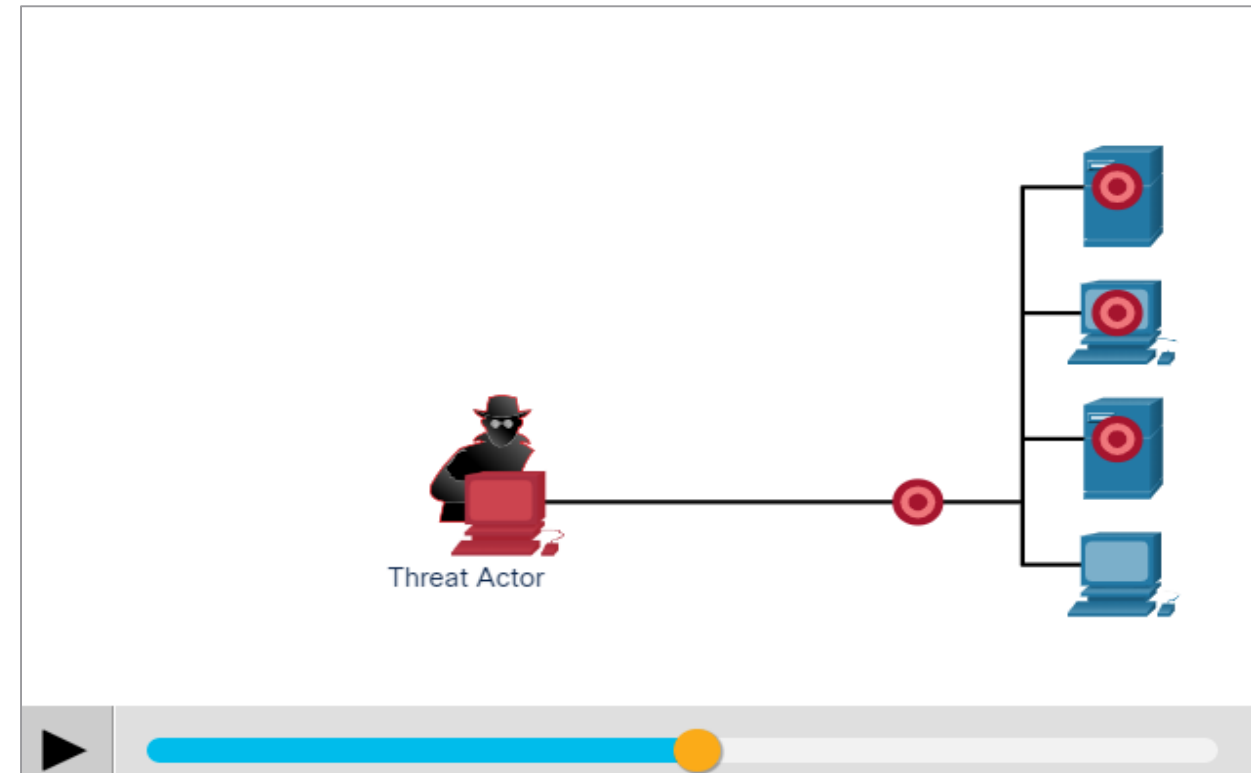
| Technique | Description |
|---|---|
| Perform an information query of a target | The threat actor is looking for initial information about a target. Various tools can be used, including the Google search, organizations website, whois, and more. |
| Initiate a ping sweep of the target network | The information query usually reveals the target's network address. The threat actor can now initiate a ping sweep to determine which IP addresses are active. |
| Initiate a port scan of active IP addresses | This is used to determine which ports or services are available. Examples of port scanners include Nmap, SuperScan, Angry IP Scanner, and NetScanTools. |
| Run vulnerability scanners | This is to query the identified ports to determine the type and version of the application and operating system that is running on the host. Examples of tools include Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT, and Open VAS. |
| Run exploitation tools | The threat actor now attempts to discover vulnerable services that can be exploited. A variety of vulnerability exploitation tools exist including Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker. |

Reconnaissance Attacks (Contd.)

Internet Information Queries: Click Play in the figure to view an animation of a threat actor using the who is command to find information about a target.

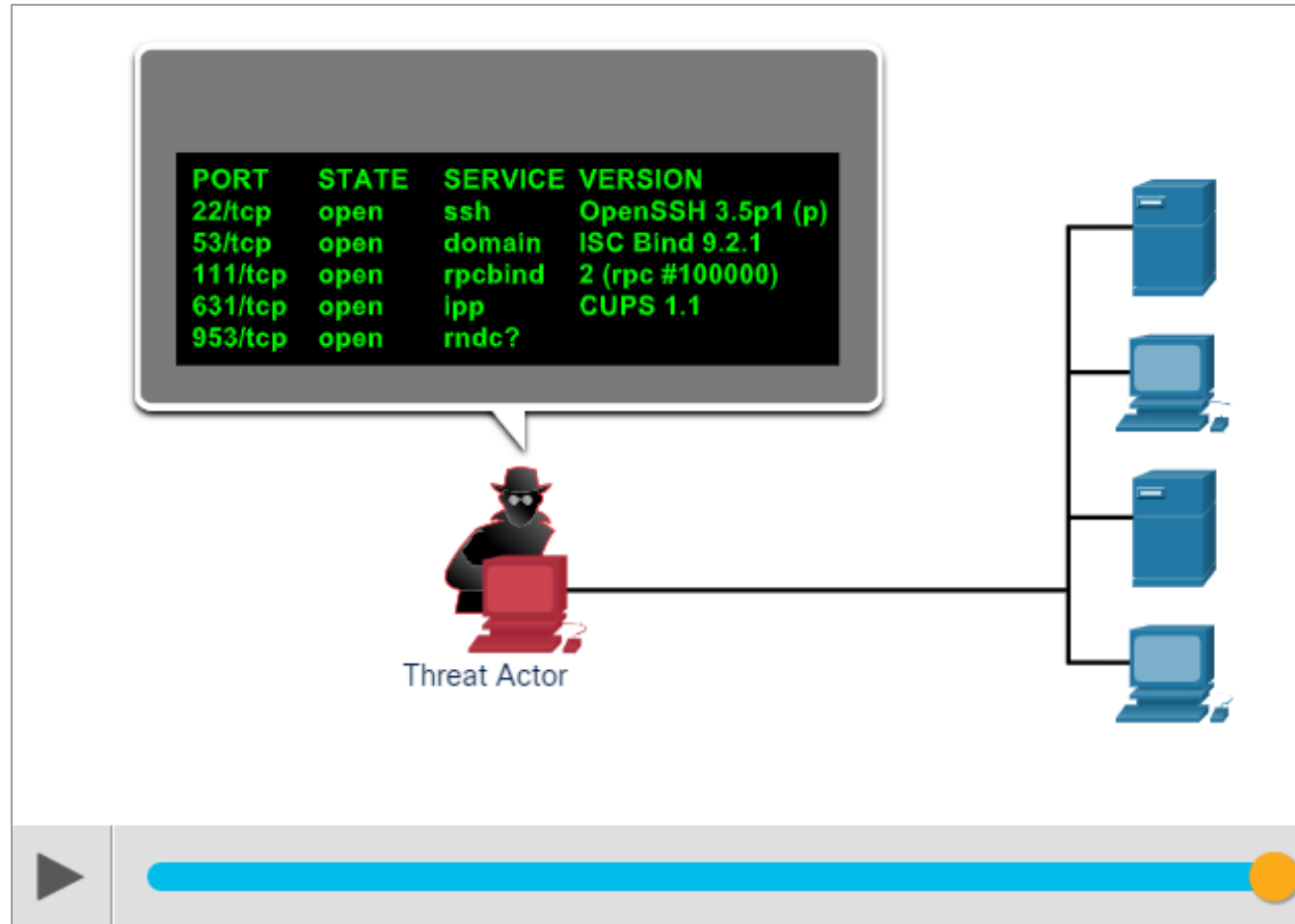


Performing Ping Sweep: Click Play in the figure to view an animation of a threat actor doing a ping sweep of the target's network address to discover live and active IP addresses.



Reconnaissance Attacks (Contd.)

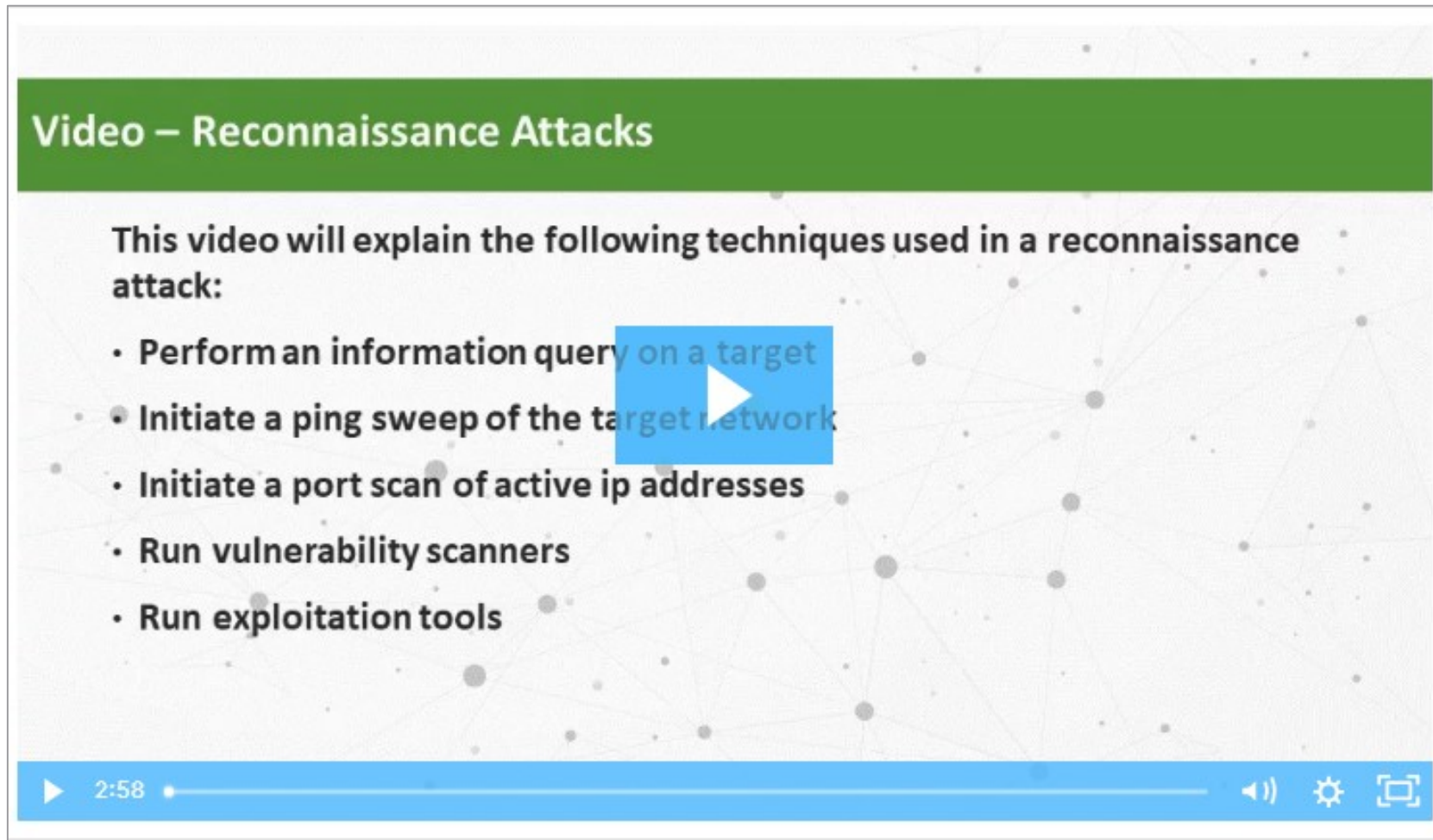
Performing Port Scan: Click Play in the figure to view an animation of a threat actor performing a port scan on the discovered active IP addresses using Nmap.



Common Network Attacks - Reconnaissance, Access, and Social Engineering

Video - Reconnaissance Attacks

Watch the video to learn about the different techniques in a reconnaissance attack.



Video – Reconnaissance Attacks

This video will explain the following techniques used in a reconnaissance attack:

- Perform an information query on a target
- Initiate a ping sweep of the target network
- Initiate a port scan of active ip addresses
- Run vulnerability scanners
- Run exploitation tools

2:58

Access Attacks

- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry into web accounts, confidential databases, and other sensitive information.

Password Attacks

- The threat actor attempts to discover critical system passwords using a variety of password cracking tools.

| Category of Attack | Description |
|--------------------------|---|
| Data modification attack | Data modification attacks occur when a threat actor has captured enterprise traffic and has altered the data in the packets without the knowledge of the sender or receiver. |
| Password-based attacks | Password-based attacks occur when a threat actor obtains the credentials for a valid user account. |
| Compromised key attack | A compromised-key attack occurs when a threat actor obtains a secret key. A compromised key can be used to gain access to a secured communication without the sender or receiver. |

Access Attacks

- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry into web accounts, confidential databases, and other sensitive information.

Spoofing Attacks

- The threat actor device attempts to pose as another device by falsifying data.
- Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing.
 - **Trust exploitations** - Zneužitie dôvery – Útočníci majú prístup do dôveryhodného hostiteľa, pomocou ktorého získajú prístup k vnútornej sieti. Napríklad získajú prístup do zariadenia, ktoré pomocou VPN pristupuje do vnútornej siete
 - **Port redirections** - Útočník používa kompromitované zariadenie, pomocou ktorého môže vykonať útok na ďalšie zariadenie
 - **Man-in-the-middle attacks** - Útočník dokáže čítať, upravovať alebo presmerovať údaje, ktoré si posielajú dve zariadenia. Útočníci to dokážu pomocou toho, že je umiestnený medzi týmito dvoma zariadeniami.
 - **Buffer overflow attacks**

Access Attacks

Types of MiTM attacks:

1. DNS spoofing.
2. IP spoofing, MAC, DHCP spoof
3. Wi-Fi eavesdropping
4. HTTPS spoofing.
5. SSL hijacking.
6. Email hijacking.
7. Session Hijacking
8. Man in the Browser

MiTM vs. Eavesdropping:

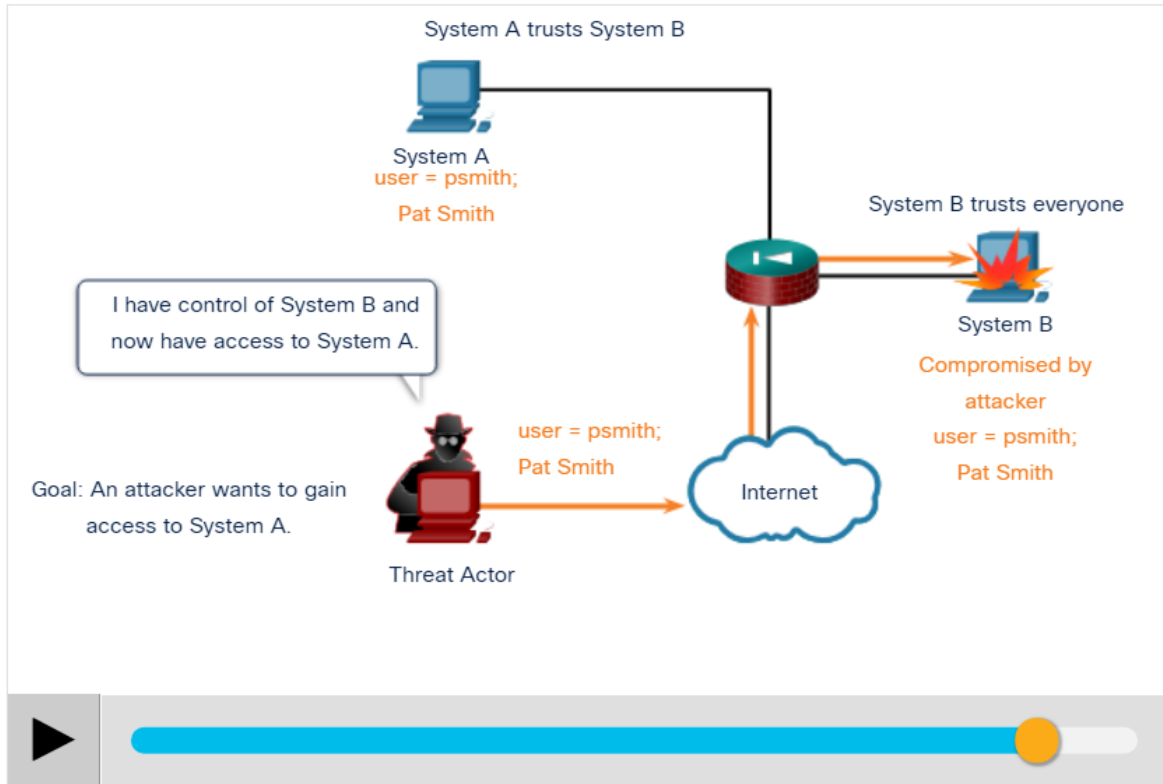
A MitM attack enables eavesdropping, but MitM can be used to carry out other nefarious activities such as stealing data and tampering with communications. Eavesdropping is also enabled using other forms of attack.

| Category of Attack | Description |
|---------------------------------|--|
| Eavesdropping attack | An eavesdropping attack is when a threat actor captures and listens to network traffic. This is also called as sniffing or snooping . |
| Sniffer attack | A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. |
| Man-in-the-middle attack (MiTM) | A MiTM attack occurs when threat actors have positioned themselves between a source and destination. |
| IP address spoofing attack | An IP address spoofing attack is when a threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet. |

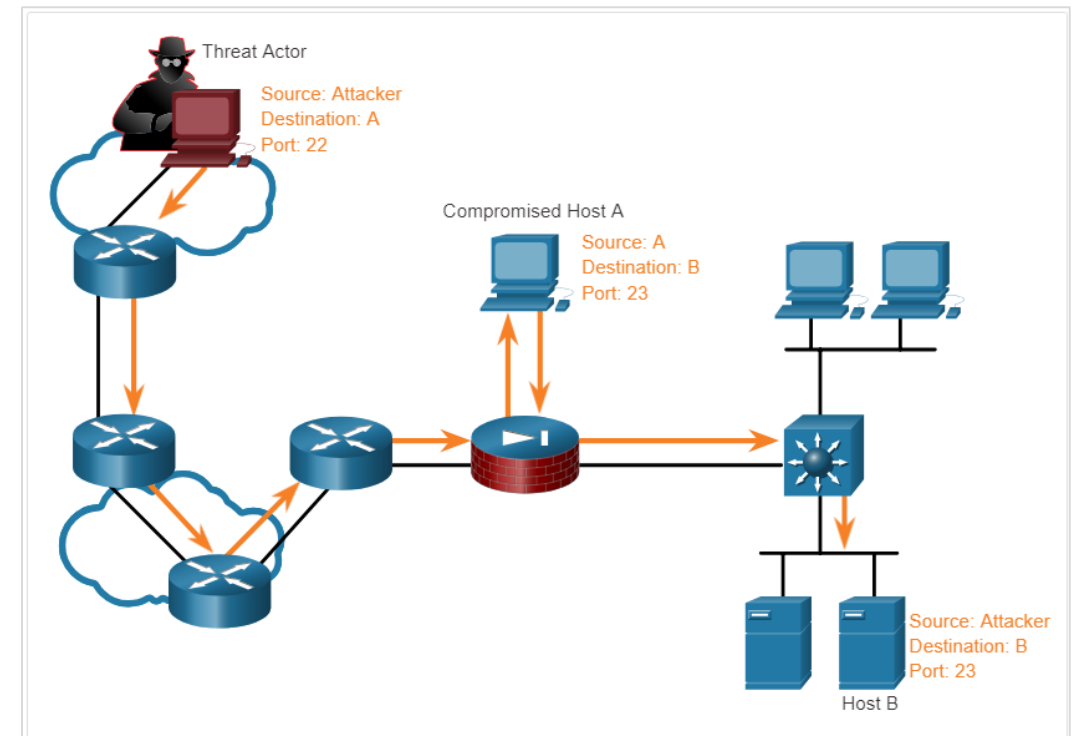
Common Network Attacks - Reconnaissance, Access, and Social Engineering

Access Attacks (Contd.)

Trust Exploitation Example: Click Play in the figure to view an example of trust exploitation.

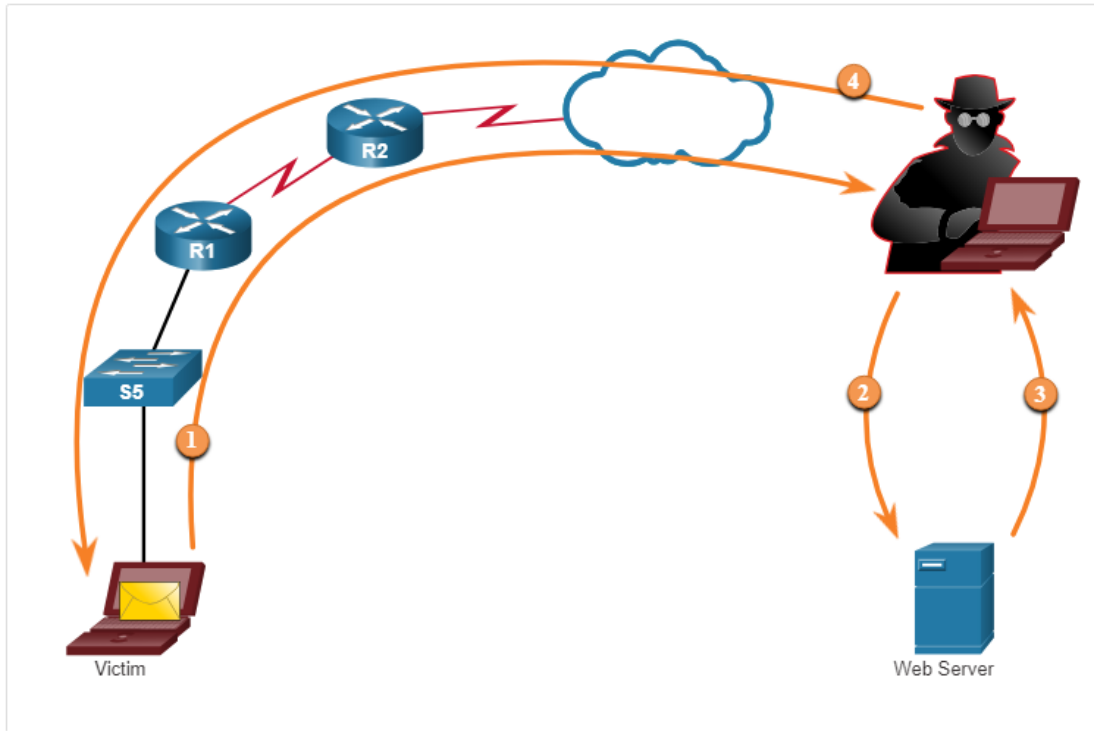


Port Redirection Example: The example shows a threat actor using SSH (port 22) to connect to a compromised Host A trusted by Host B. Hence, the threat actor can use Telnet (port 23) to access it.

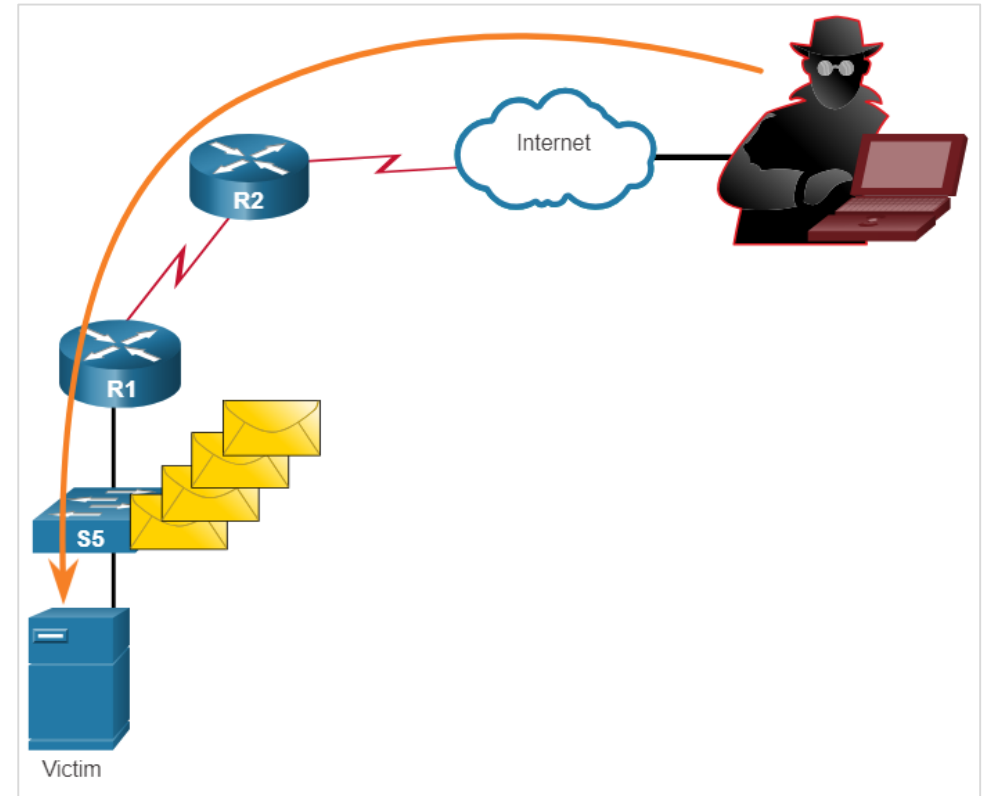


Access Attacks (Contd.)

Man-in-the-Middle Attack Example: The figure displays an example of a man-in-the-middle attack.



Buffer Overflow Attack: The figure shows that the threat actor is sending many packets to the victim in an attempt to overflow the victim's buffer.



Common Network Attacks - Reconnaissance, Access, and Social Engineering

Video - Access and Social Engineering Attacks

Watch the video to see the demonstration of the types of access and social engineering attacks.



Video – Access and Social Engineering Attacks

This video will cover the following:

- Techniques used in access attacks (password attacks, spoofing attacks, trust exploitations, port redirections, man-in-the-middle attacks, buffer overflow attacks)
- Techniques used in social engineering attacks (pretexting, phishing, spear phishing, spam, something for something, baiting, impersonation, tailgating, shoulder surfing, dumpster diving)

3:35

CC

⏪

⚙️

🖥️

Social Engineering Attacks

- Social Engineering is an access attack that attempts to manipulate individuals into performing actions or divulging into confidential information.
- Some social engineering techniques are performed in-person or via the telephone or internet.
- Social engineering techniques are explained in the below table.

| Social Engineering Attack | Description |
|---------------------------|--|
| Pretexting | A threat actor pretends to need personal or financial data to confirm the identity of the recipient. |
| Phishing | A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information. |
| Spear phishing | A threat actor creates a targeted phishing attack tailored for a specific individual or organization. |
| Spam | Also known as junk mail, this is unsolicited email which often contains harmful links, malware, or deceptive content. |

Common Network Attacks - Reconnaissance, Access, and Social Engineering

Social Engineering Attacks (Contd.)

| Social Engineering Attack | Description |
|---------------------------|--|
| Something for Something | Sometimes called “Quid pro quo”, this is when a threat actor requests personal information from a party in exchange for something such as a gift. |
| Baiting | A threat actor leaves a malware infected flash drive in a public location. A victim finds the drive and unsuspectingly inserts it into their laptop, unintentionally installing malware. |
| Impersonation | In this type of attack, a threat actor pretends to be someone else to gain the trust of a victim. |
| Tailgating | This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area. |
| Shoulder surfing | This is where a threat actor inconspicuously looks over someone’s shoulder to steal their passwords or other information. |
| Dumpster diving | This is where a threat actor rummages through trash bins to discover confidential documents. |

Social Engineering Protection Practices

- The Social Engineer Toolkit (SET) was designed to help white hat hackers and other network security professionals to create social engineering attacks to test their own networks.
- Enterprises must educate their users about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.



Common Network Attacks - Reconnaissance, Access, and Social Engineering

Strengthening the Weakest Link

- Cybersecurity is as strong as its weakest link.
- The weakest link in cybersecurity can be the personnel within an organization, and social engineering is a major security threat.
- One of the most effective security measures that an organization can take is **to train its personnel** and **create a 'security-aware culture'**.

14.3 Network Attacks - Denial of Service, Buffer Overflows, and Evasion

Video – Denial of Service Attacks

Watch the video to learn about Denial of Service attacks.



Video – Denial of Service Attacks

This video will cover the following:

- Techniques used in Denial-of-Service attacks (overwhelming quantity of traffic, maliciously formatted packets)
- Techniques used in Distributed Denial-of-Service attacks (zombies)

2:02

CC

⏪

⚙️

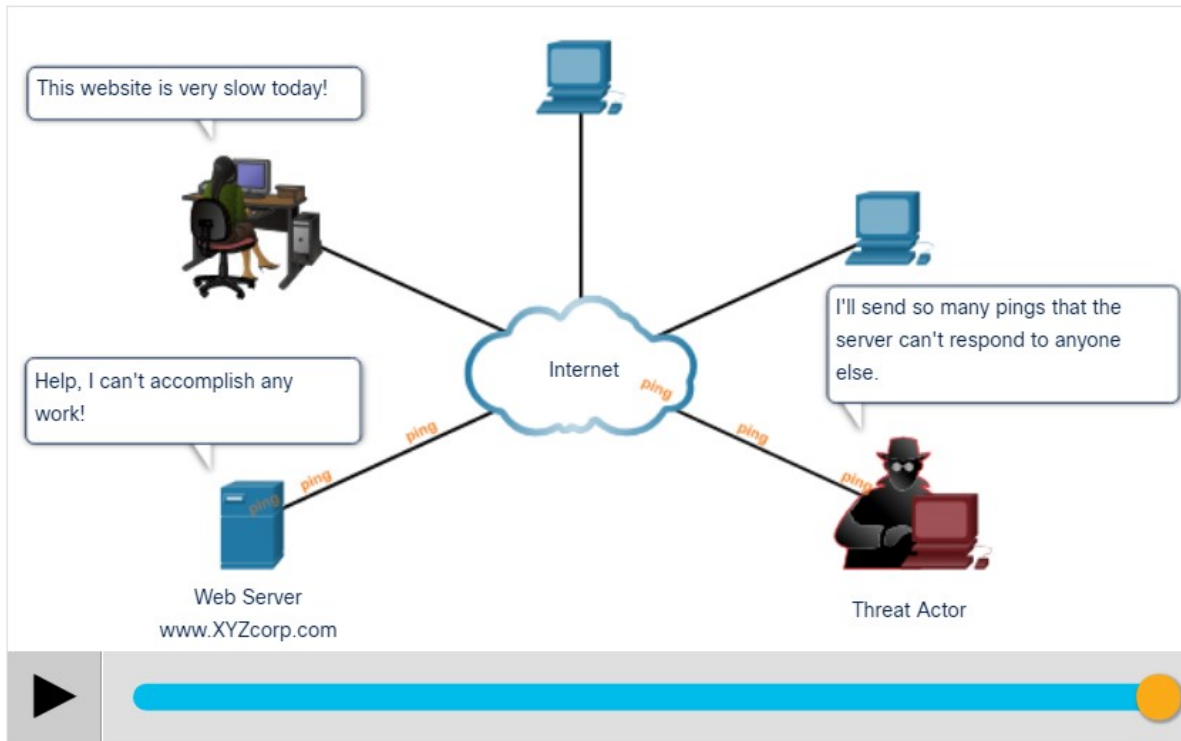
🖥️

DoS and DDoS Attacks

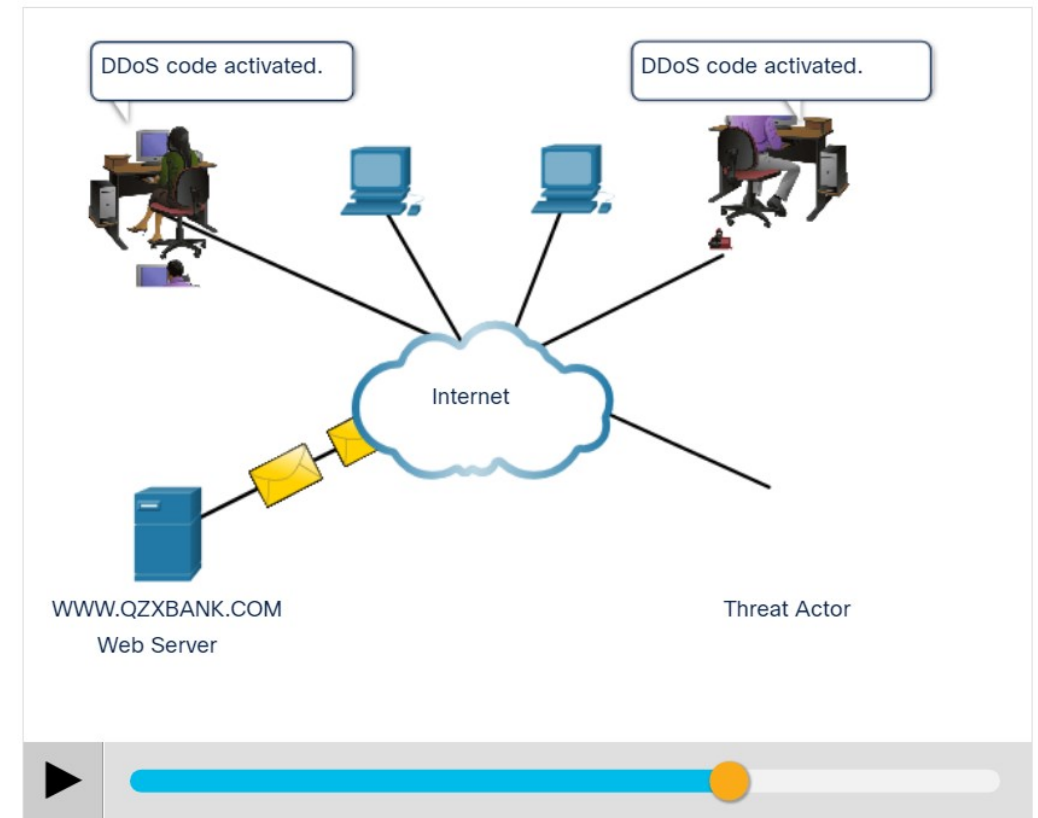
- A Denial of Service (DoS) attack creates some sort of interruption in network services to users, devices, or applications. The two types of DoS attacks are as follows:
- **Overwhelming Quantity of Traffic** - The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle.
- **Maliciously Formatted Packets** - The threat actor sends a maliciously formatted packet to a host or application and the receiver is unable to handle it.

DoS and DDoS Attacks (Contd.)

DoS Attack: Click Play in the figure to view the animation of a DoS attack.



DDoS Attack: Click Play in the figure to view the animations of a DDoS attack.

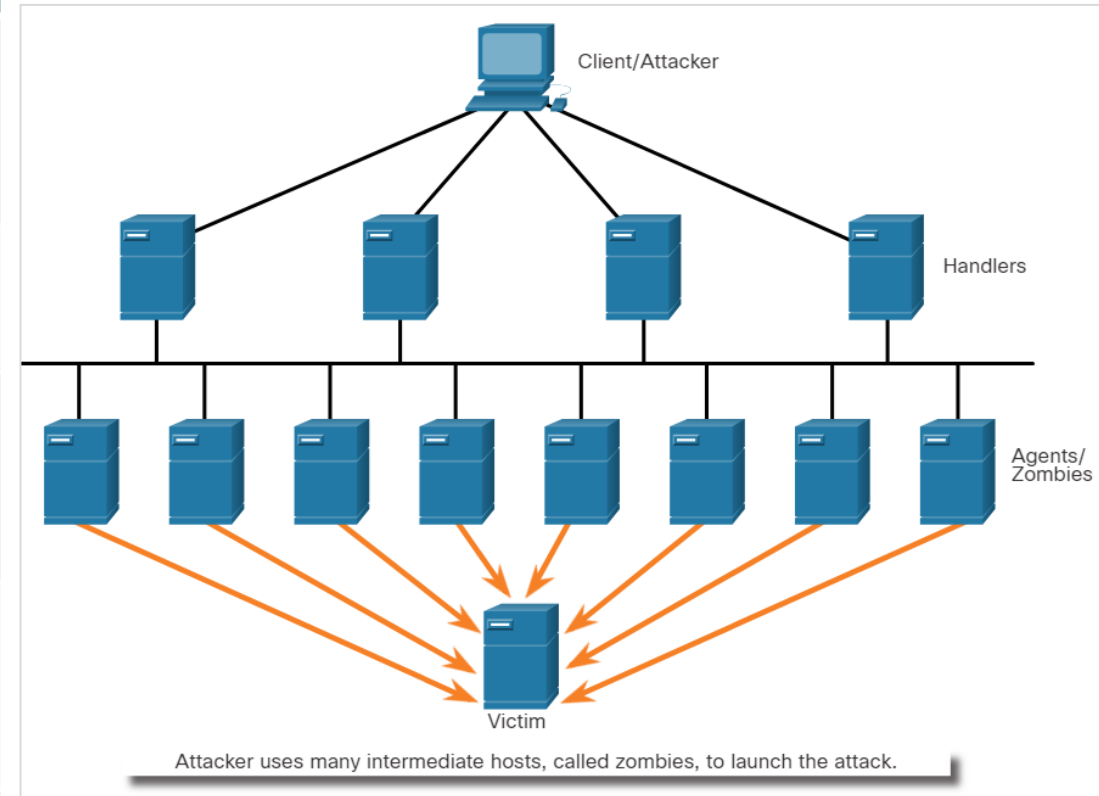


Network Attacks - Denial of Service, Buffer Overflows, and Evasion

Components of DDoS Attacks

The following terms are used to describe the components of a DDoS:

| Component | Description |
|-----------|---|
| zombies | A group of compromised hosts, ktoré kúpil alebo získal pomocou malvéru. These hosts run malicious code, alebo „spia“. |
| bots | Bots are malware that is designed to infect a host and communicate with a handler system. |
| botnet | A group of zombies that have been infected using self-propagating malware and are controlled by handlers. |
| handlers | A master command-and-control (CnC or C2) server controlling groups of zombies. |
| botmaster | Enables unauthorized file transfer services on end devices. |



Video Demonstration – Mirai Botnet

- Mirai is a malware that targeted IoT devices configured with default login information.
- The botnet was used as part of a Distributed Denial of Service (DDoS) attack.

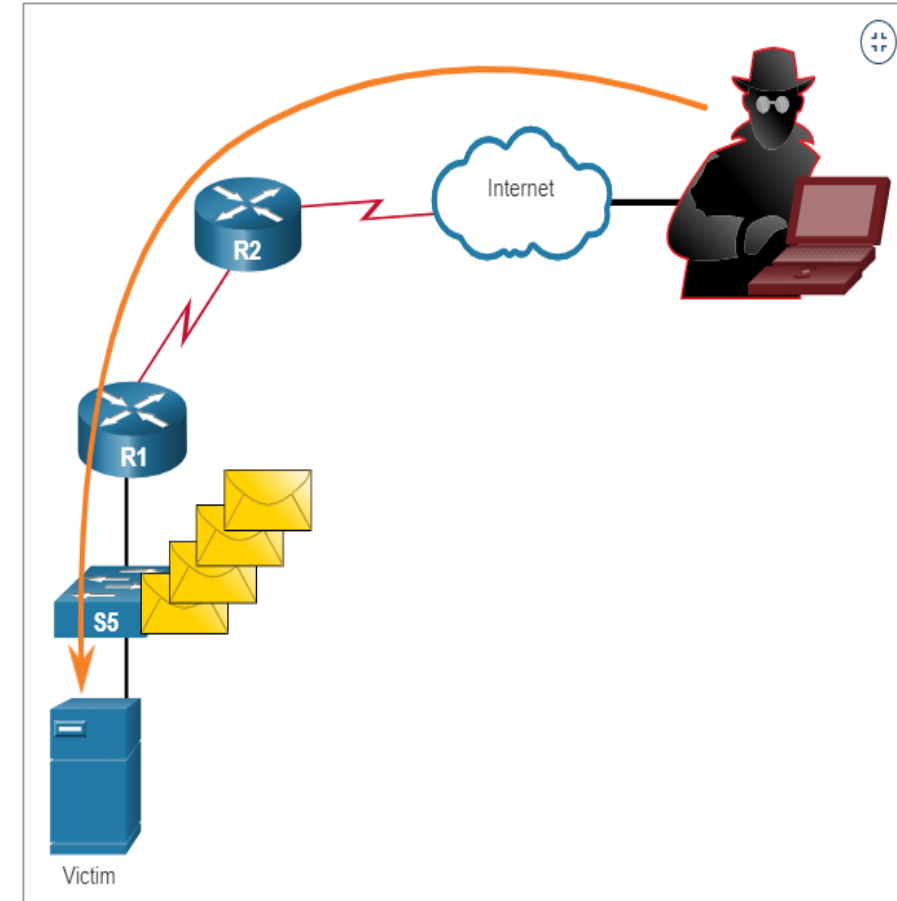
Video Demonstration – Mirai Botnet (Contd.)

Play the video to view a demonstration of how a botnet-based DDoS attack makes services unavailable.



Buffer Overflow Attack

- The threat actor uses the buffer overflow DoS attack to find a system memory-related flaw on a server and exploit it.
- For instance, a remote denial of service attack vulnerability was discovered in Microsoft Windows 10, where the threat actor created malicious code to access out-of-scope memory.
 - Ak k tomuto kódu pristúpil proces Windows AHCACHE.SYS, spôsobilo to zlyhanie systému.
- Another example is **ping of death**, where a threat actor sends a ping of death, which is an echo request in an IP packet that is larger than the maximum packet size.
- The receiving host cannot handle a packet size and it would crash.
- **Note:** It is estimated that one third of malicious attacks are the result of buffer overflows.



Únikové metódy / Evasion Methods

The evasion methods used by threat actors include:

| Evasion Method | Description |
|--------------------------|---|
| Encryption and tunneling | Táto technika úniku používa tunelovanie na skrytie alebo šifrovanie na zakódovanie súborov škodlivého softvéru. To sťažuje mnohým bezpečnostným technikám detekciu a identifikáciu malvéru. Tunelovanie môže znamenať skrytie ukradnutých údajov v rámci legitímnych paketov. |
| Resource exhaustion | Táto technika úniku spôsobuje, že cieľový hosťiteľ je príliš zaneprázdnený na to, aby správne používal techniky detekcie zabezpečenia. |
| Traffic fragmentation | Táto úniková technika rozdeľuje škodlivý obsah na menšie pakety, aby obišla detekciu zabezpečenia siete. Potom, čo fragmentované pakety obídu bezpečnostný detekčný systém, malvér sa znova zloží a môže začať odosielať citlivé údaje zo siete. |

Evasion Methods (Contd.)

| Evasion Method | Description |
|----------------------------------|--|
| Protocol-level misinterpretation | keď sieťová obrana správne nespracúva položky PDU, ako je kontrolný súčet alebo hodnotu TTL. To môže oklamať bránu firewall, aby ignorovala pakety, ktoré by mala kontrolovať. |
| Traffic substitution | aktér hrozby sa pokúša oklamať IPS zahmlievaním údajov v payloade. To sa dosiahne zakódovaním v inom formáte. Napríklad aktér hrozby môže namiesto ASCII použiť kódovaný prenos v Unicode. IPS nerozpozná skutočný význam údajov, ale cieľový koncový systém dokáže údaje prečítať. |
| Traffic insertion | Podobne ako pri nahrádzaní prevádzky, ale aktér hrozby vkladá ďalšie bajty údajov do škodlivej sekvencie údajov. Pravidlá IPS si nevšimnú škodlivé údaje a akceptujú celú sekvenciu údajov. |

Common Threats and Network Attacks - Denial of Service, Buffer Overflows, and Evasion

Evasion Methods (Contd.)

| Evasion Method | Description |
|----------------|--|
| Pivoting | This technique assumes the threat actor has compromised an inside host and wants to expand their access further into the compromised network. An example is a threat actor who has gained access to the administrator password on a compromised host and is attempting to login to another host using the same credentials . |
| Rootkits | A rootkit is a complex attacker tool used by experienced threat actors. It integrates with the lowest levels of the operating system. When a program attempts to list files, processes, or network connections, the rootkit presents a sanitized version of the output, eliminating any incriminating output. The goal of the rootkit is to completely hide the activities of the attacker on the local system. |
| Proxies | Sieťová prevádzka môže byť presmerovaná cez sprostredkujúce systémy, aby sa skryl konečný cieľ pre ukradnuté dáta. Týmto spôsobom podnik neblokuje známe príkazy a ovládanie, pretože cieľ proxy sa javí ako neškodný. Okrem toho, ak dôjde k odcudzeniu údajov, cieľ ukradnutých údajov môže byť distribuovaný medzi mnoho proxy serverov, čím sa neupozorňuje na skutočnosť, že jediný neznámy cieľ slúži ako cieľ pre veľké množstvo sieťovej prevádzky.. |

14.4 Common Threats and Attacks Summary

What Did I Learn in this Module?

- Malware is short for malicious software or malicious code.
- Most viruses are spread through USB memory drives, CDs, DVDs, network shares, and email.
- Trojans are found in online games.
- Three common types of malware are virus, worm, and Trojan horse.
- Threat actors can also attack the network from outside.
- The three major categories are reconnaissance, access, and DoS attacks.
- Recon attacks precede access or DoS attacks.
- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services.
- DoS attacks create some sort of interruption of network services to users, devices, or applications.

What Did I Learn in this Module? (Contd.)

- DDoS attacks are similar in intent to DoS attacks, except that the DDoS attack increases in magnitude because it originates from multiple, coordinated sources.
- Mirai is a malware that targets IoT devices configured with default login information.
- The goal of a threat actor when using a buffer overflow DoS attack is to find a system memory-related flaw on a server and exploit it.



UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Ďakujem za pozornosť

Obsahom boli moduly:

Chapter 13 Attackers and Their Tools

Chapter 14 Common Threats and Attacks

Vyjadrite spätnú väzbu na prednášku a/alebo cvičenie v anonymnej ankete cez google form: [link](#)