Information Assurance and Security – ACIT 4630

Hesam Alizadeh

Week 3 – Winter 2024

Learning Outcomes

- CVSS calculation
- Malware types and prevention
- Social engineering attacks' success
- Zero-day vulnerabilities importance
- Advanced Persistent Threats
- Stuxnet malware attack characteristics

CVSS calculation

- Imagine you received the following brief description of a vulnerability in your system:
  "This vulnerability allow a remote unauthenticated user to execute arbitrary code on the target system, potentially gaining access to system components in the context of the current user"
- Analyze this vulnerability and apply CVSS 3.1 assessment methodology to generate a base score and a vector string:
  - Common Vulnerability Scoring System Version 3.1 Calculator (first.org)

Malwares propagation

- **Virus**: Spreads by attaching to legitimate programs.
- **Worm**: Self-replicates and spreads independently.
- **Trojan**: Disguises itself as a legitimate program.
  - Remote Access Trojan (RAT)

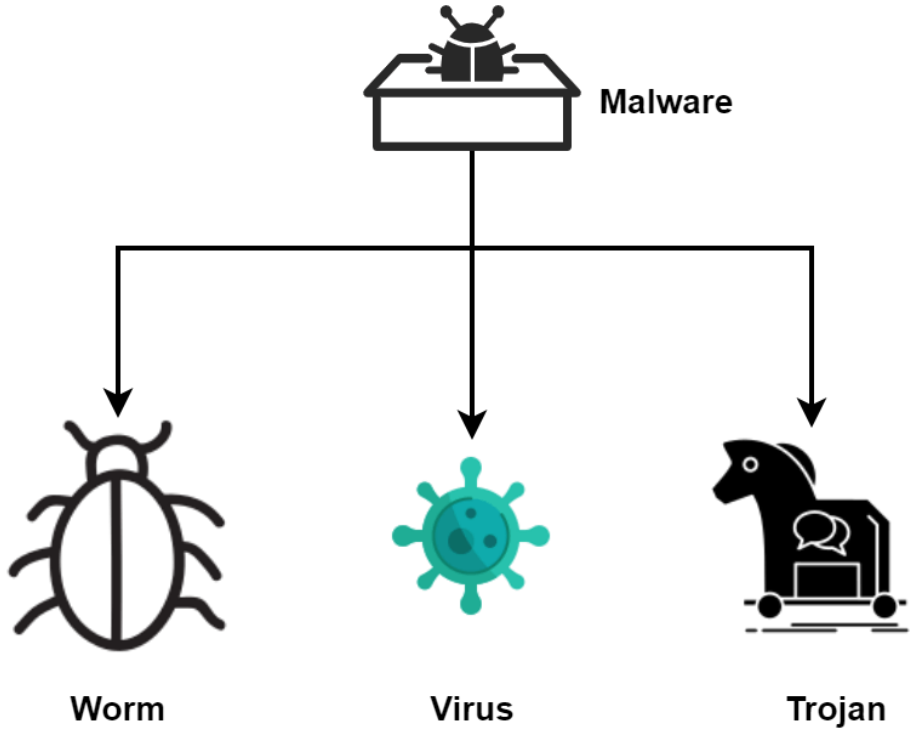


Image Source: [Differences Between Viruses, Worms and Trojans]

Malware Payloads

Spyware: gathers user's information

Adware: displays unwanted advertisements

Ransomware: encrypts user's data for ransom

[3 steps to prevent and recover from ransomware]

Logic Bombs

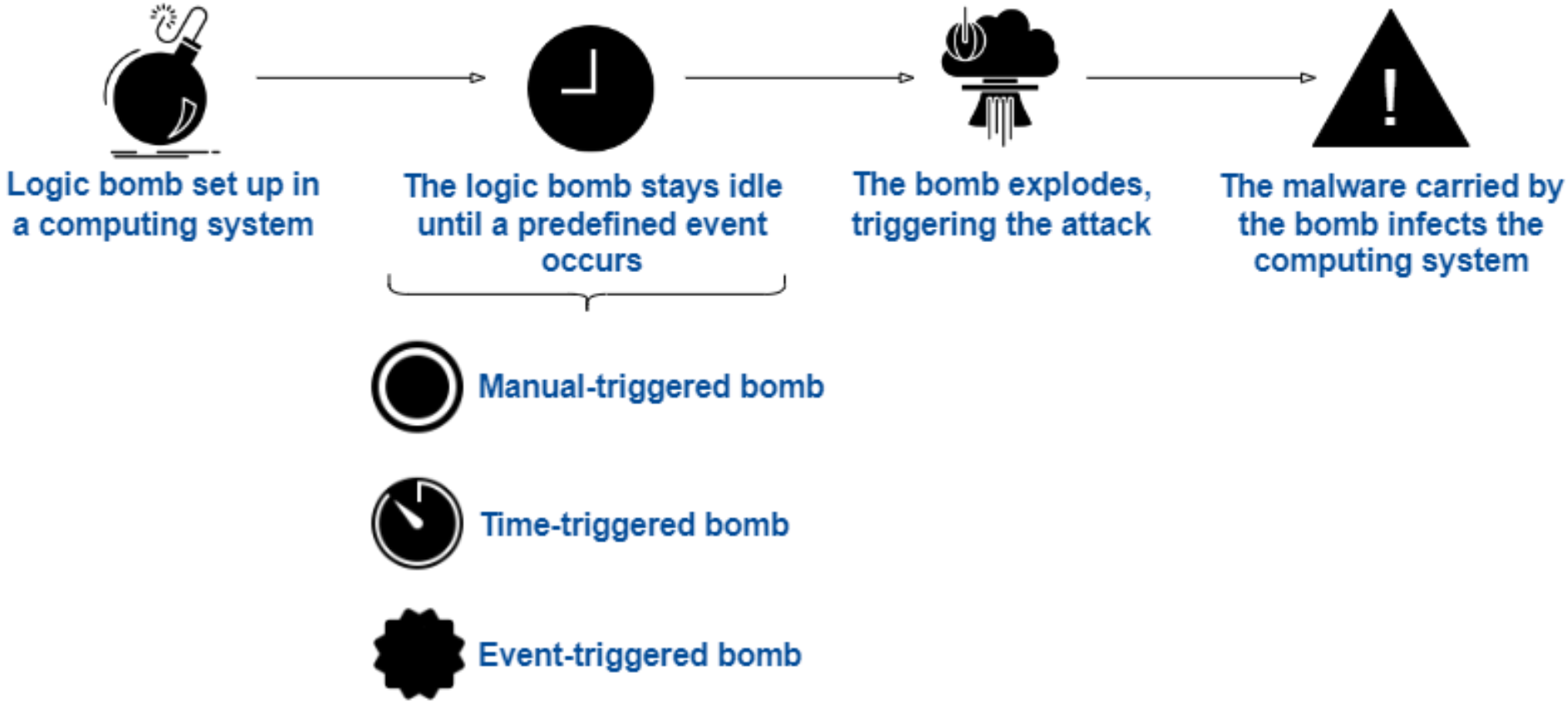
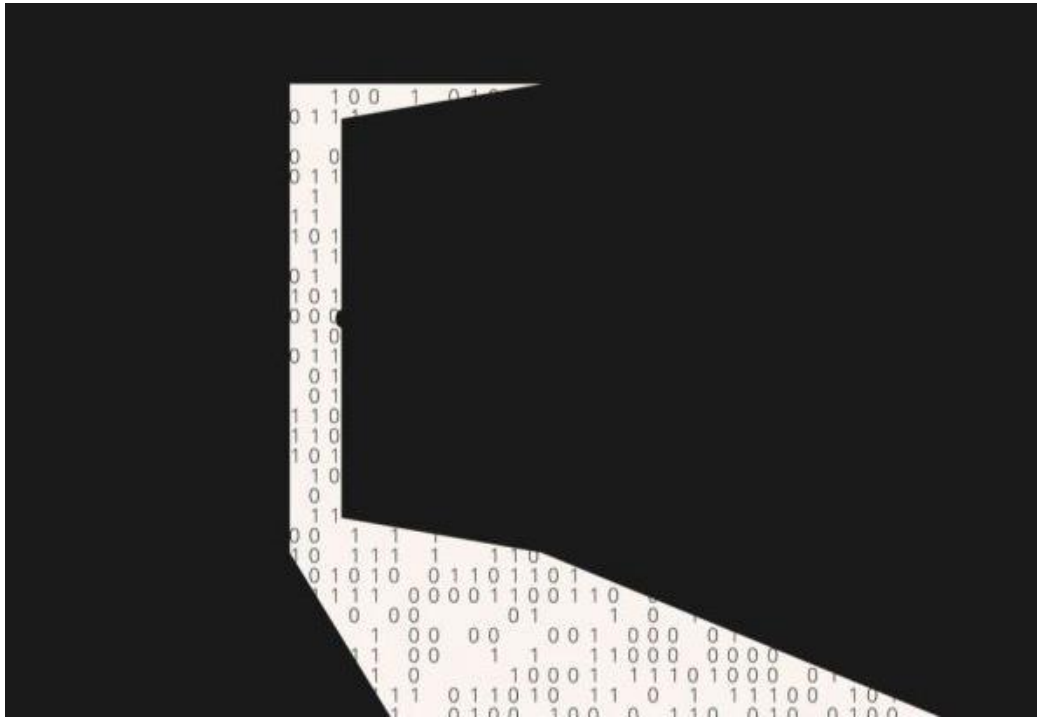


Image source: Logic bombs

Backdoors

- Means to grant future access
- Mechanisms
  - Hardcoded accounts
  - Default passwords
  - Unknown access channels
- What are some detection mechanisms?



Advanced Malwares

- **Polymorphic viruses** change to avoid signature detection
  - Different encryption key for each system
- **Armored viruses** prevent reverse engineering
  - Obfuscated assembly language
  - Blocking the use of system debuggers
  - Preventing the use of sandboxing

Rootkits

"Gain root access!" Vs *"Software techniques designed to hide other software"*

- Rootkit payloads
  - Backdoors, botnet agents, spyware, anti-theft
- User-mode vs Kernel-mode

Botnets

- *A collection of zombie computers used for malicious purposes*
- Steal computing power or storage/network connectivity
- What are some hacker motives for building botnets?
- **Indirect** and **highly-redundant** command and control channels

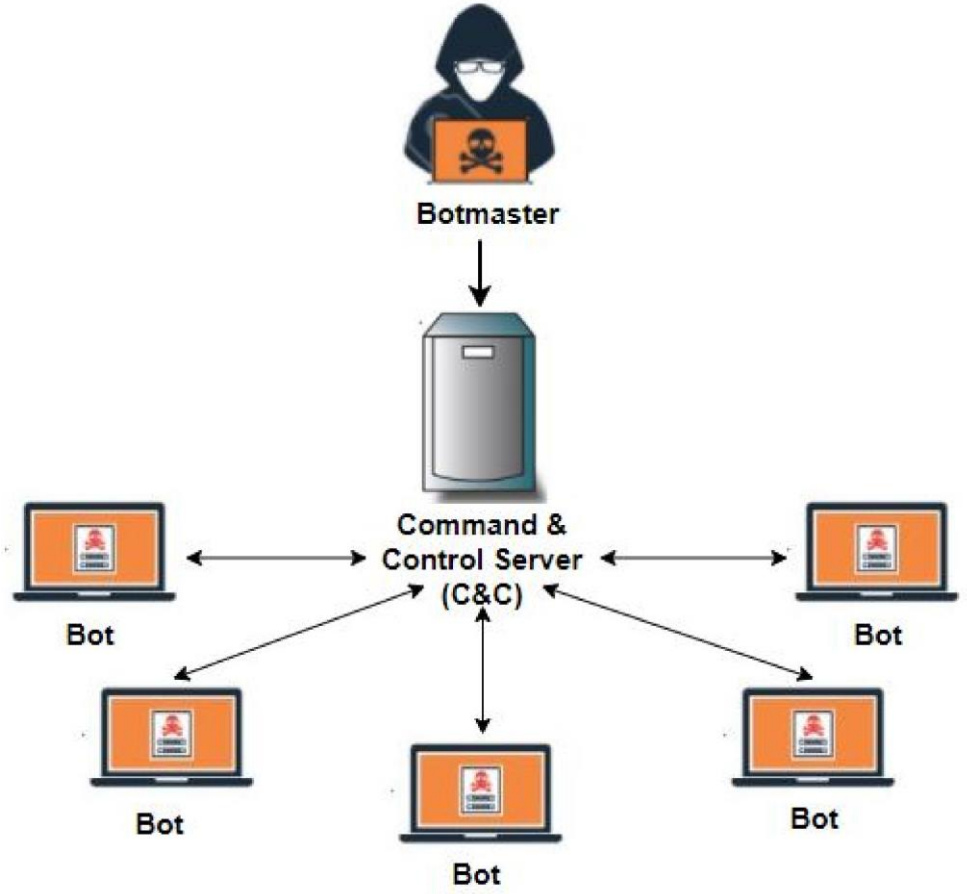
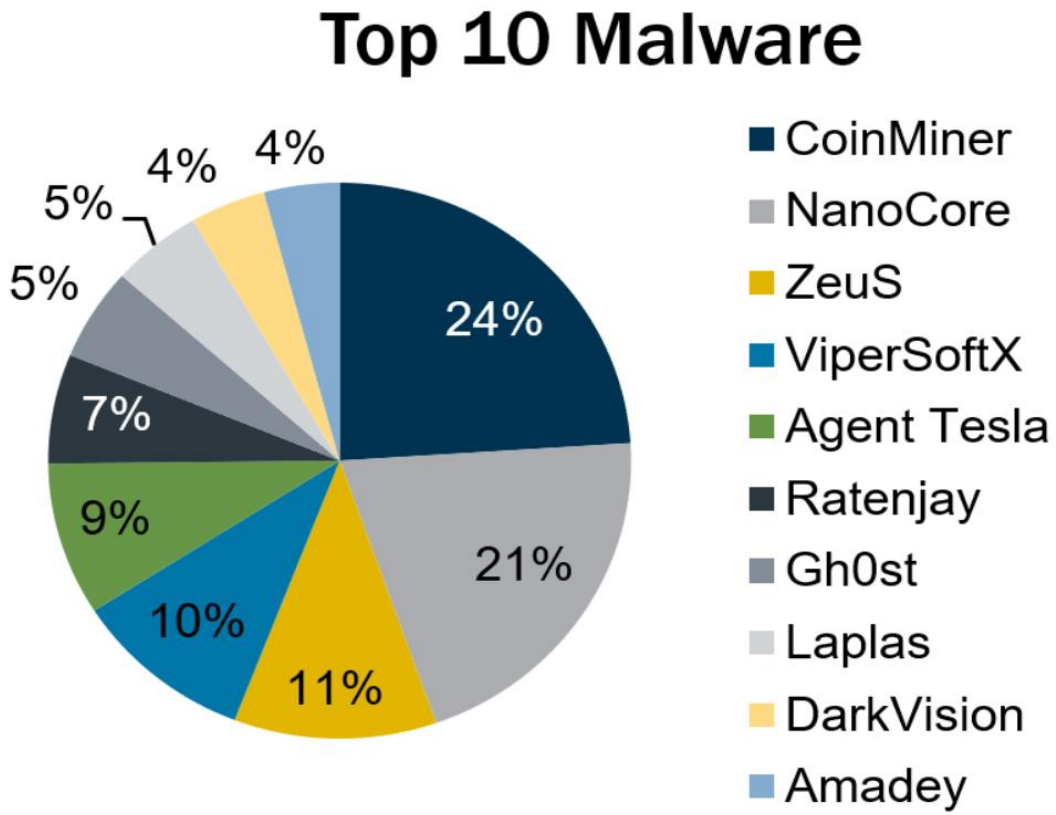


Image source: Machine Learning-Based Botnet Detection in Software-Defined Network: A Systematic Review

Malware prevention

- Signature detection – Suspicious activity
- Behavior detection – Deviation from normal activity
- Endpoint Detection and Response (EDR) solutions
  - Installed agents watch for signs of malicious activity.
  - Automated responses triggers
  - Sandboxing executables

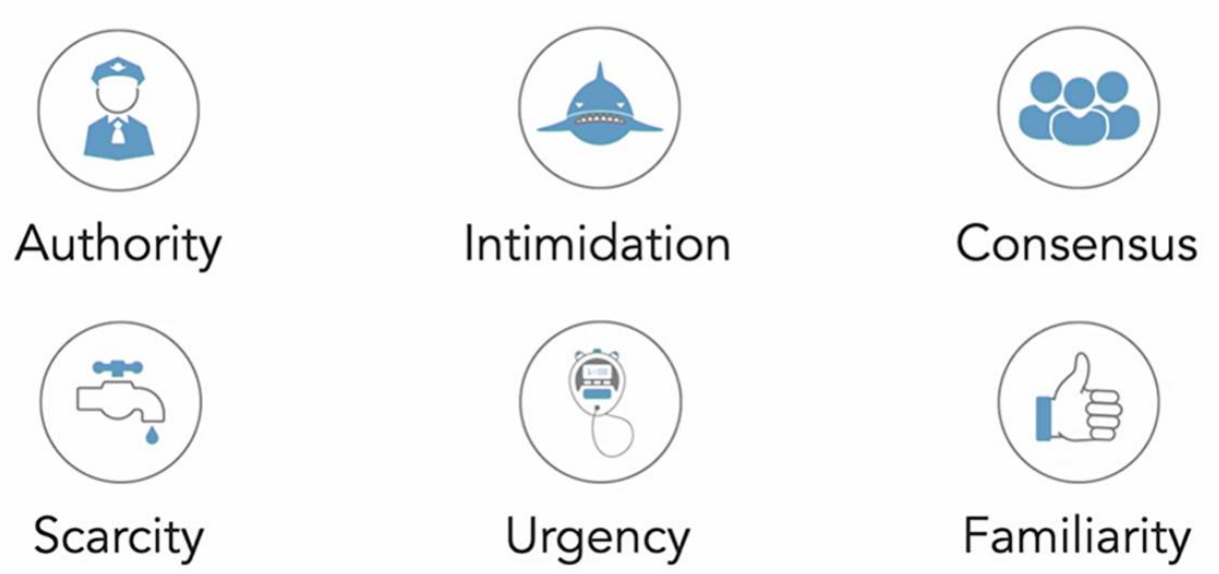
Top 10 Malware Q2 2023



Source: [Top 10 Malware Q2 2023]

Social Engineering

- Reasons for success:



- How to defend?

Video: Social Engineering

Impersonation attacks

- **Spam** – Unsolicited email
  - **Phishing** – Elicit sensitive information
    - **Pharming** – Using fake similar websites
  - **Spear Phishing** – Highly targeted attacks
- **Prepending** – Add fake “safe” tags
- **Credential Harvesting** – Use compromised credentials
- **Spoofing** – Faking the identity of someone else

Attack Vectors & Attack Surface

- **Vector**: Path to obtain initial access
- **Surface**: The entire area of that is susceptible to hacking

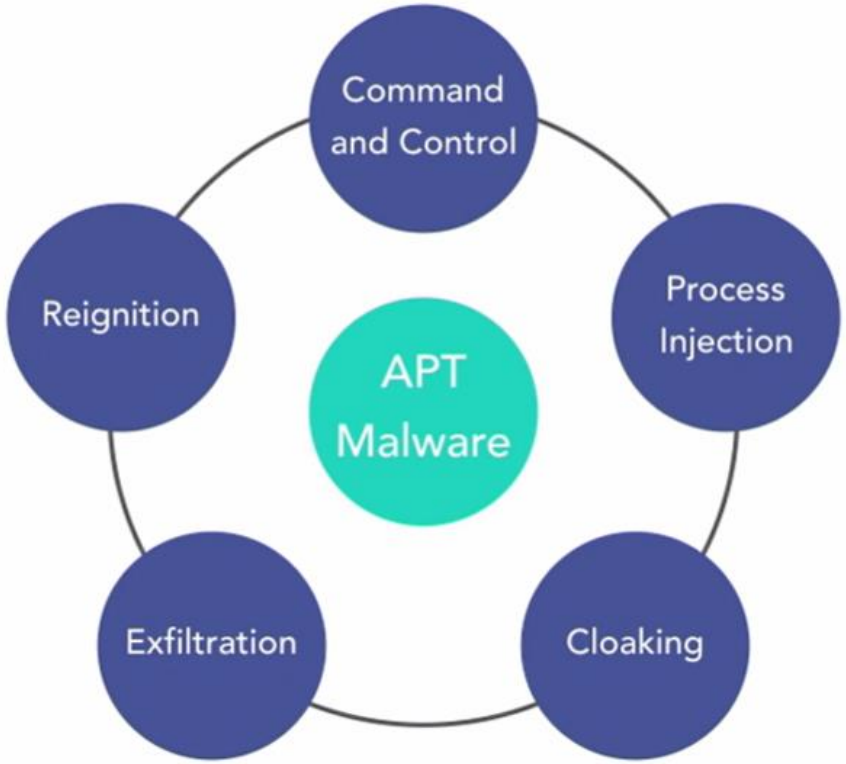
- **Email**: Phishing and malicious attachments/links.
- **Social Media**: Malware spread and influence campaigns.
- **Removable Media**: USB drives spreading malware.
- **Magnetic Stripe Cards**: Skimming attacks at ATMs/card readers.
- **Cloud Services**: Accessing insecure files, exploiting security flaws.
- **Physical Access**: Unsecured network jacks, endpoint device access.
- **IT Supply Chain:** Pre-delivery device tampering for backdoor access.
- **Wireless Networks**: Exploitation of insecure wireless networks.

Advanced Persistent Threats

Characteristics:

- Customized code
- Focused objectives
- Multi-threat capability
- Human intervention
- Low and slow

Anatomy



Zero-day Vulnerability

A vulnerability that is discovered but not patched yet.

- Why is it hard to exploit a zero-day vulnerability?
- Why are there so many?

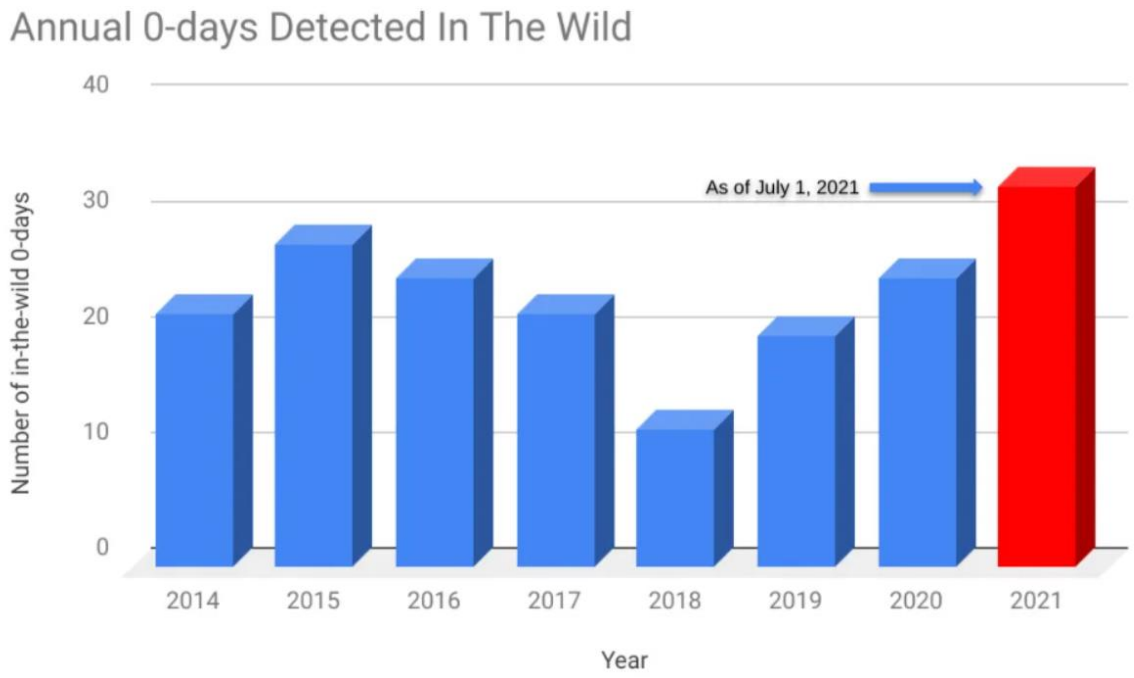


Image Source: [How we protect users from 0-day attacks (blog.google)]

Stuxnet Virus

- The goal of the attacker?
- What was done in the reconnaissance stage?
- What assets were targeted?
- What kind of malware was used?
- What was the attack vector?
- Why is it referred to as APT?
- What kinds of vulnerability were exploited?
- Why embed sabotage functions instead of using remote commands?
- How the attack could have been prevented?