Cyber threats: Email, Network, Malware

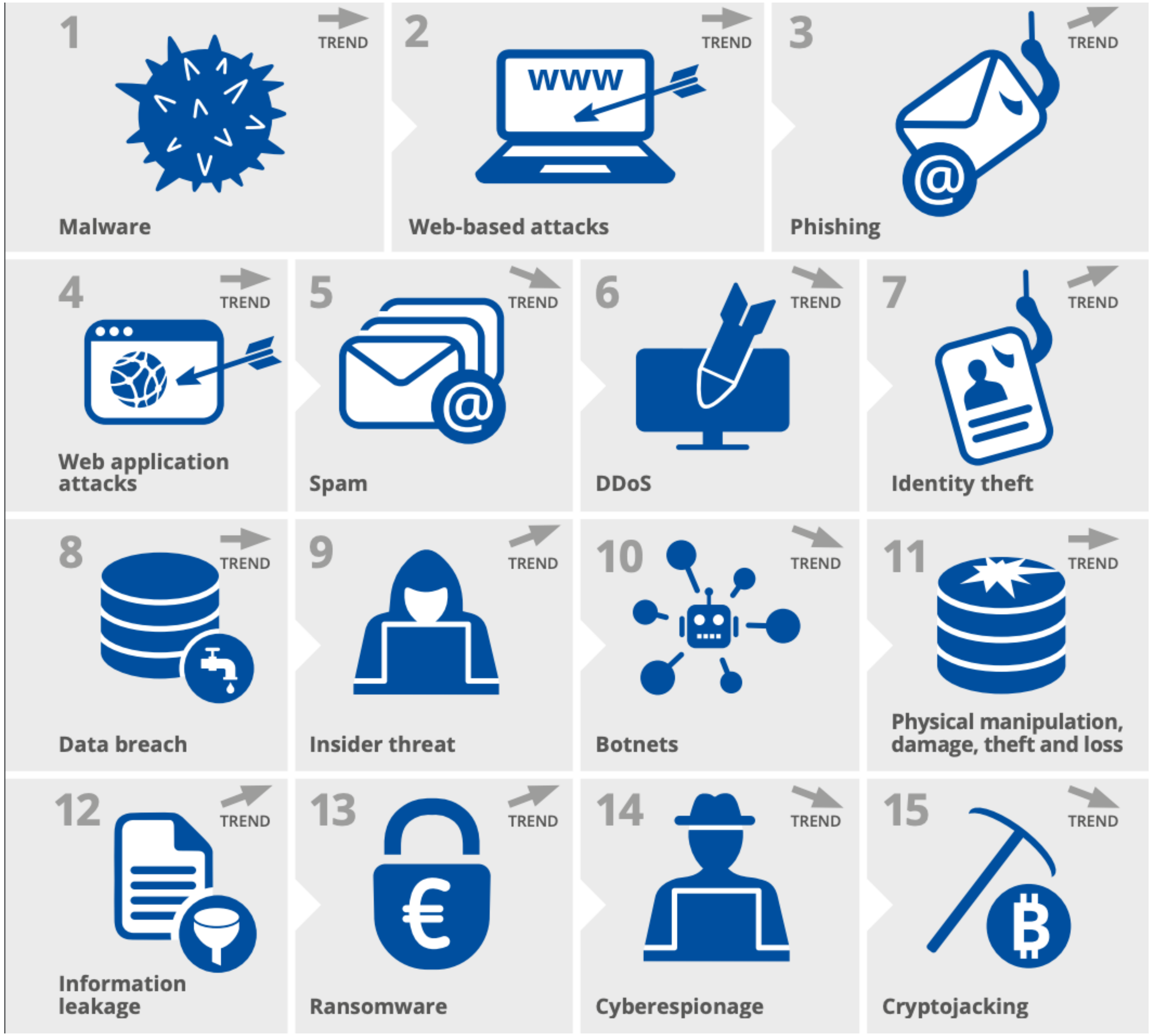
For CyBOK funded project:
Development of an active learning lesson plan and laboratory materials for AI for Security

Dr Hossein Abroshan

Senior Lecturer in Cyber Security

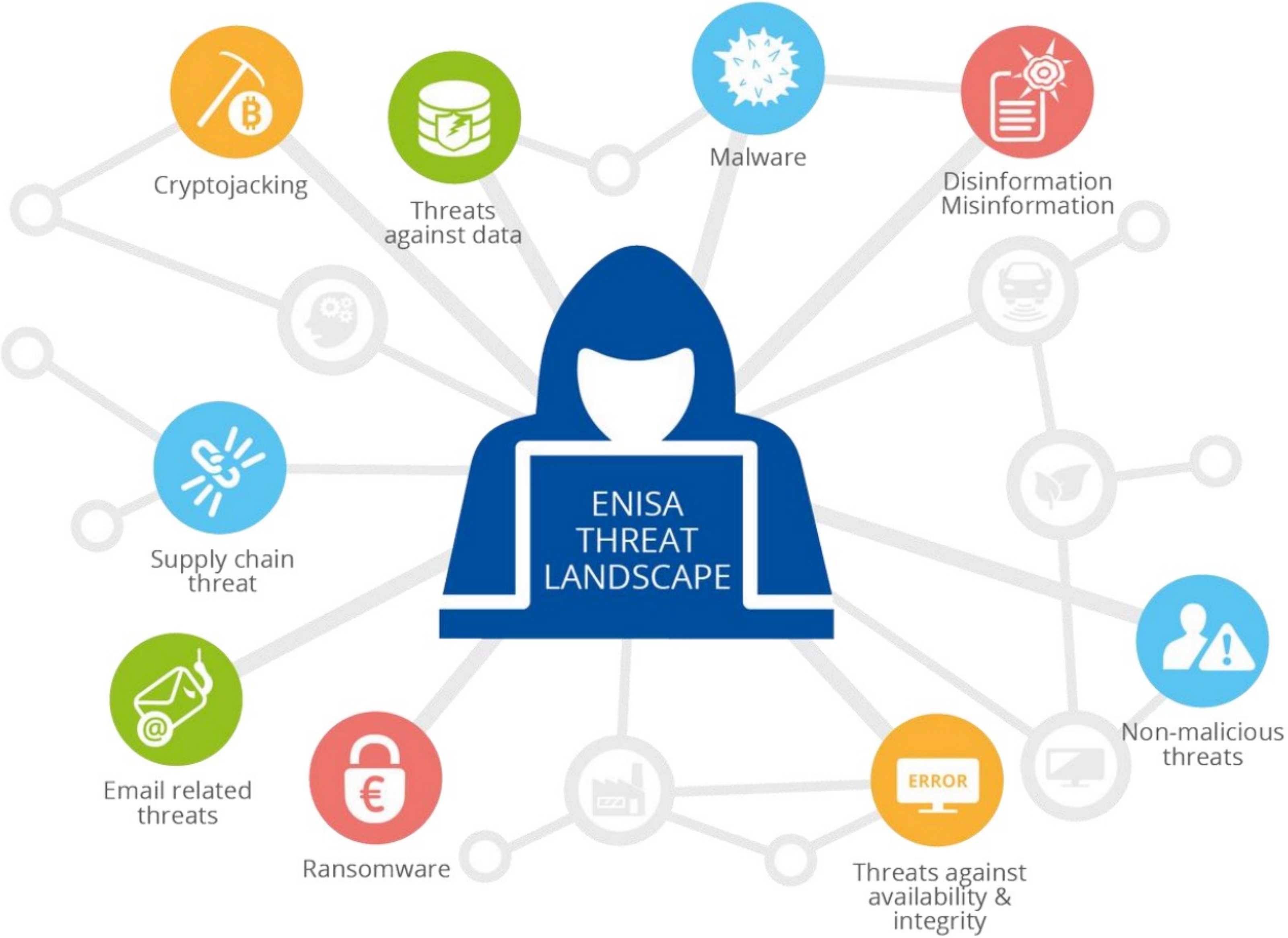
Anglia Ruskin University, Cambridge, UK

Cyber Threat Landscape (2020)



Source: ENISA

Cyber Threat Landscape (2021)



Source: ENISA

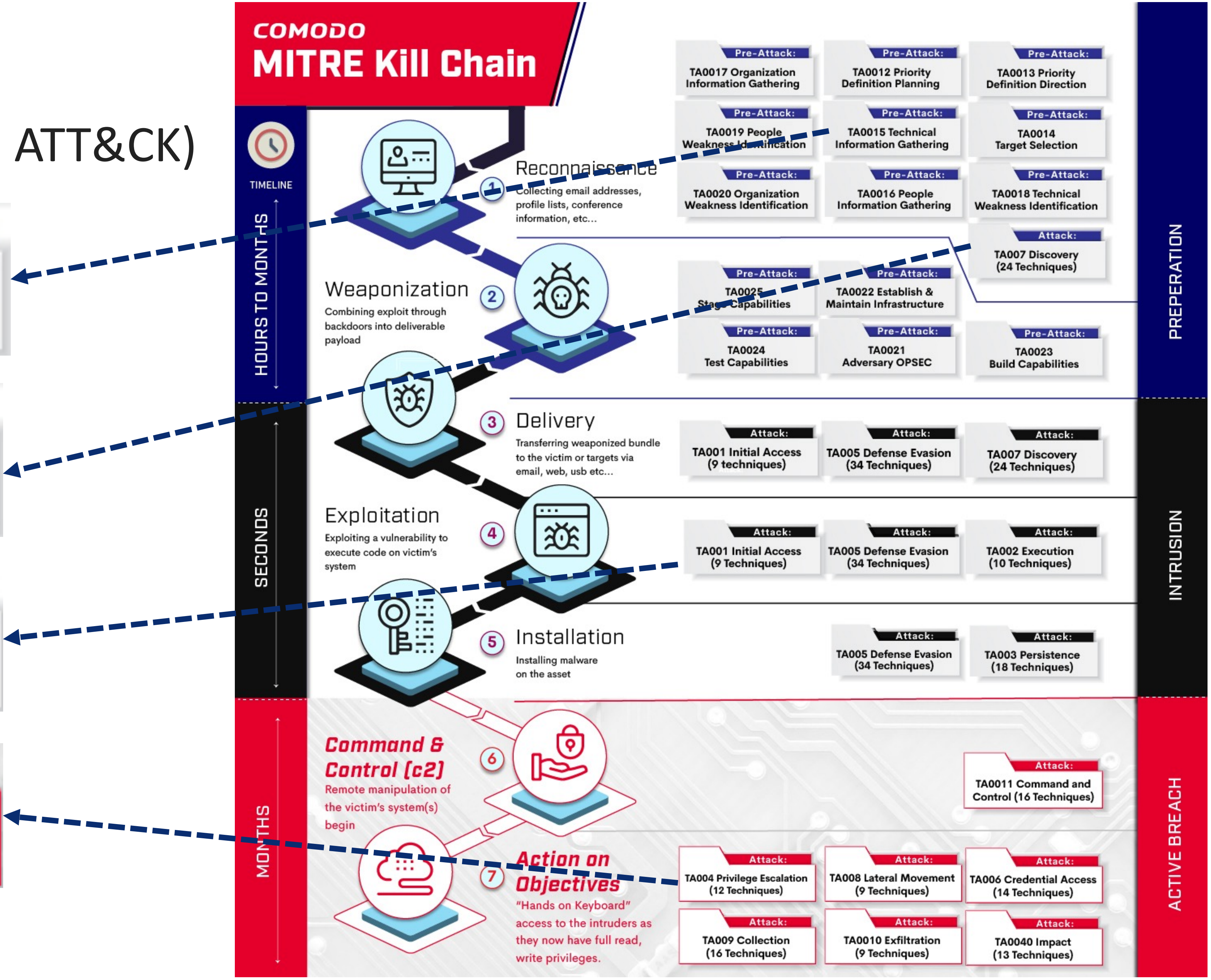
Cyber Attacks
Kill Chain (MITRE ATT&CK)

Pre-Attack:
TA0015 Technical Information Gathering

Attack:
TA007 Discovery (24 Techniques)

Attack:
TA001 Initial Access (9 techniques)

Attack:
TA004 Privilege Escalation (12 Techniques)



COMODO
MITRE Kill Chain

TIMELINE

HOURS TO MONTHS

SECONDS

MONTHS

1 Reconnaissence
Collecting email addresses, profile lists, conference information, etc…

2 Weaponization
Combining exploit through backdoors into deliverable payload

3 Delivery
Transferring weaponized bundle to the victim or targets via email, web, usb etc…

4 Exploitation
Exploiting a vulnerability to execute code on victim's system

5 Installation
Installing malware on the asset

6 *Command & Control [c2]*
Remote manipulation of the victim's system(s) begin

7 *Action on Objectives*
"Hands on Keyboard" access to the intruders as they now have full read, write privileges.

Pre-Attack: TA0017 Organization Information Gathering
Pre-Attack: TA0012 Priority Definition Planning
Pre-Attack: TA0013 Priority Definition Direction
Pre-Attack: TA0019 People Weakness Identification
Pre-Attack: TA0015 Technical Information Gathering
Pre-Attack: TA0014 Target Selection
Pre-Attack: TA0020 Organization Weakness Identification
Pre-Attack: TA0016 People Information Gathering
Pre-Attack: TA0018 Technical Weakness Identification
Attack: TA007 Discovery (24 Techniques)
Pre-Attack: TA0025 Stage Capabilities
Pre-Attack: TA0022 Establish & Maintain Infrastructure
Pre-Attack: TA0024 Test Capabilities
Pre-Attack: TA0021 Adversary OPSEC
Pre-Attack: TA0023 Build Capabilities

Attack: TA001 Initial Access (9 techniques)
Attack: TA005 Defense Evasion (34 Techniques)
Attack: TA007 Discovery (24 Techniques)

Attack: TA001 Initial Access (9 Techniques)
Attack: TA005 Defense Evasion (34 Techniques)
Attack: TA002 Execution (10 Techniques)

Attack: TA005 Defense Evasion (34 Techniques)
Attack: TA003 Persistence (18 Techniques)

Attack: TA0011 Command and Control (16 Techniques)

Attack: TA004 Privilege Escalation (12 Techniques)
Attack: TA008 Lateral Movement (9 Techniques)
Attack: TA006 Credential Access (14 Techniques)
Attack: TA009 Collection (16 Techniques)
Attack: TA0010 Exfiltration (9 Techniques)
Attack: TA0040 Impact (13 Techniques)

PREPERATION

INTRUSION

ACTIVE BREACH

Source: COMODO

Cyber Attacks Tactics, Techniques, and Mitigations

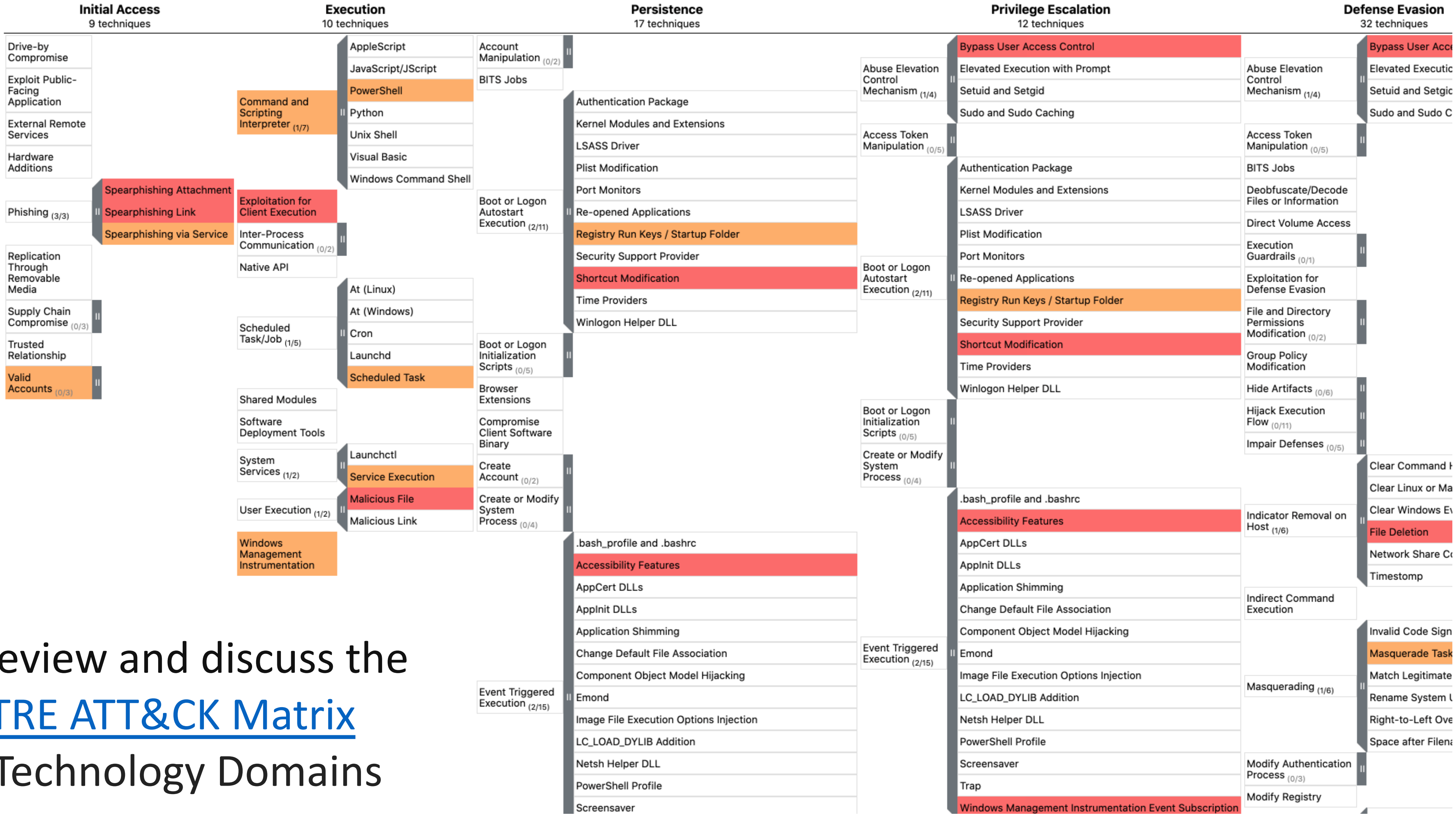
Tactics represent the "why" of an attack technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.

Techniques represent 'how' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

Source: MITRE

Cyber Attacks Matrix (MITRE ATT&CK)



Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/3)

Execution
10 techniques

- Command and Scripting Interpreter (1/7)
  - AppleScript
  - JavaScript/JScript
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (1/5)
  - At (Linux)
  - At (Windows)
  - Cron
  - Launchd
  - Scheduled Task
- Shared Modules
- Software Deployment Tools
- System Services (1/2)
  - Launchctl
  - Service Execution
- User Execution (1/2)
  - Malicious File
  - Malicious Link
- Windows Management Instrumentation

Persistence
17 techniques

- Account Manipulation (0/2)
- BITS Jobs
- Boot or Logon Autostart Execution (2/11)
  - Authentication Package
  - Kernel Modules and Extensions
  - LSASS Driver
  - Plist Modification
  - Port Monitors
  - Re-opened Applications
  - Registry Run Keys / Startup Folder
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/2)
- Create or Modify System Process (0/4)
- Event Triggered Execution (2/15)
  - .bash_profile and .bashrc
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Change Default File Association
  - Component Object Model Hijacking
  - Emond
  - Image File Execution Options Injection
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - PowerShell Profile
  - Screensaver

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (1/4)
  - Bypass User Access Control
  - Elevated Execution with Prompt
  - Setuid and Setgid
  - Sudo and Sudo Caching
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (2/11)
  - Authentication Package
  - Kernel Modules and Extensions
  - LSASS Driver
  - Plist Modification
  - Port Monitors
  - Re-opened Applications
  - Registry Run Keys / Startup Folder
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (2/15)
  - .bash_profile and .bashrc
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Change Default File Association
  - Component Object Model Hijacking
  - Emond
  - Image File Execution Options Injection
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - PowerShell Profile
  - Screensaver
  - Trap
  - Windows Management Instrumentation Event Subscription

Defense Evasion
32 techniques

- Abuse Elevation Control Mechanism (1/4)
  - Bypass User Acc
  - Elevated Executic
  - Setuid and Setgic
  - Sudo and Sudo C
- Access Token Manipulation (0/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (0/6)
- Hijack Execution Flow (0/11)
- Impair Defenses (0/5)
- Indicator Removal on Host (1/6)
  - Clear Command H
  - Clear Linux or Ma
  - Clear Windows Ev
  - File Deletion
  - Network Share Co
  - Timestomp
- Indirect Command Execution
- Masquerading (1/6)
  - Invalid Code Sign
  - Masquerade Task
  - Match Legitimate
  - Rename System U
  - Right-to-Left Ove
  - Space after Filena
- Modify Authentication Process (0/3)
- Modify Registry

Let's review and discuss the MITRE ATT&CK Matrix and Technology Domains

Source: MITRE

Malware

Malware (**mal**icious soft**ware**) is intrusive software that is intentionally designed to cause damage to computers and computer systems.

Malware is an umbrella term for a range of online threats, including viruses, spyware, adware, ransomware, and other types of harmful software.

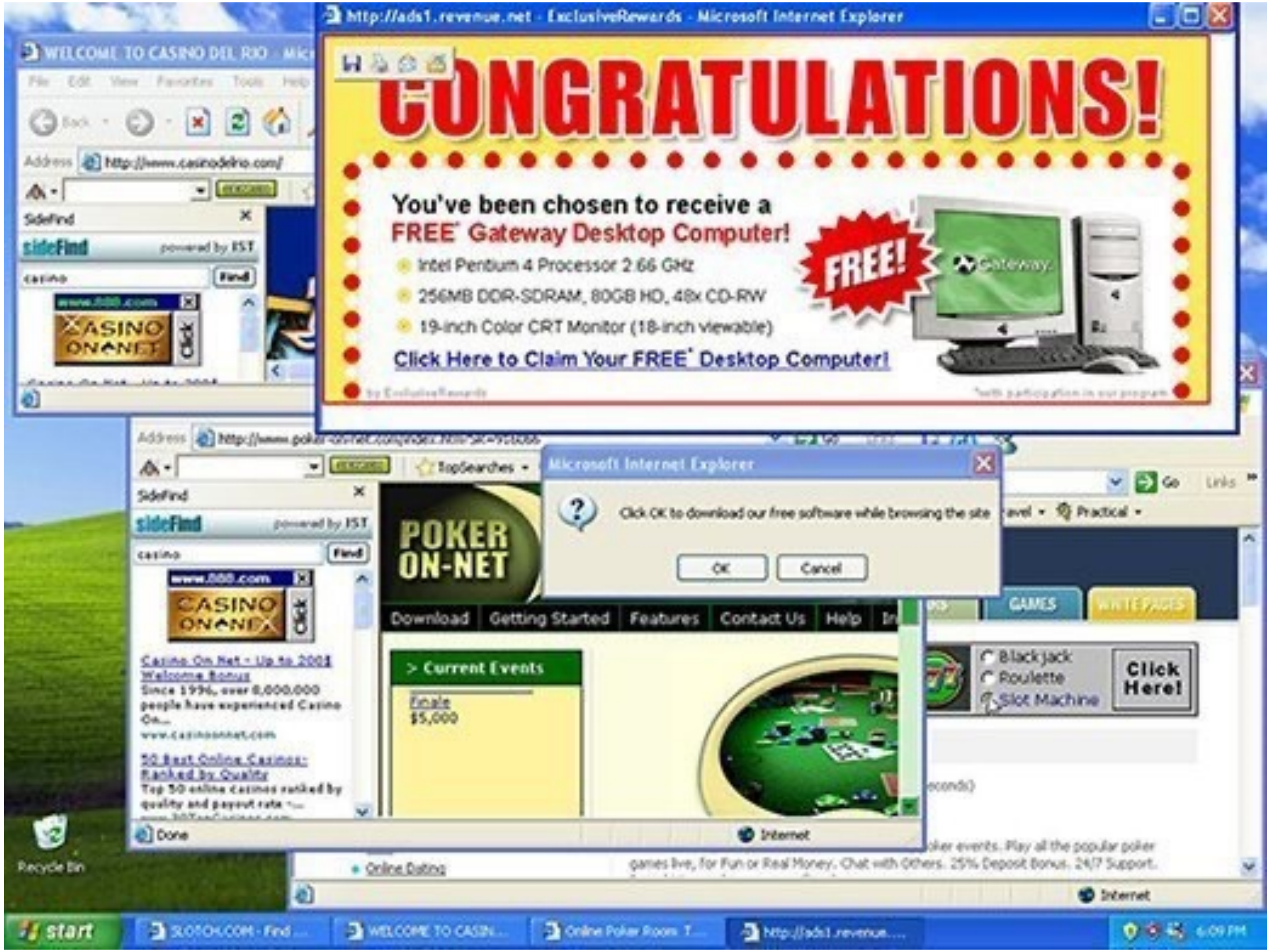
Source: Kaspersky

Types of Malware

Adware and Malvertising	**Bots and botnets**
Spyware	**PUP malware**
Ransomware	**Hybrids**
Trojans	**Fileless malware**
Worms	**Logic bombs**
Viruses	**Keyloggers** (a type of Spyware)

Source: Kaspersky

Adware and Malvertising



http://ads1.revenue.net - ExclusiveRewards - Microsoft Internet Explorer

CONGRATULATIONS!

You've been chosen to receive a FREE* Gateway Desktop Computer!

- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (18-inch viewable)

Click Here to Claim Your FREE* Desktop Computer!

Microsoft Internet Explorer

Click OK to download our free software while browsing the site

OK Cancel

Casino On Net - Up to 200$ Welcome Bonus
Since 1996, over 8,000,000 people have experienced Casino On...
www.casinoonnet.com

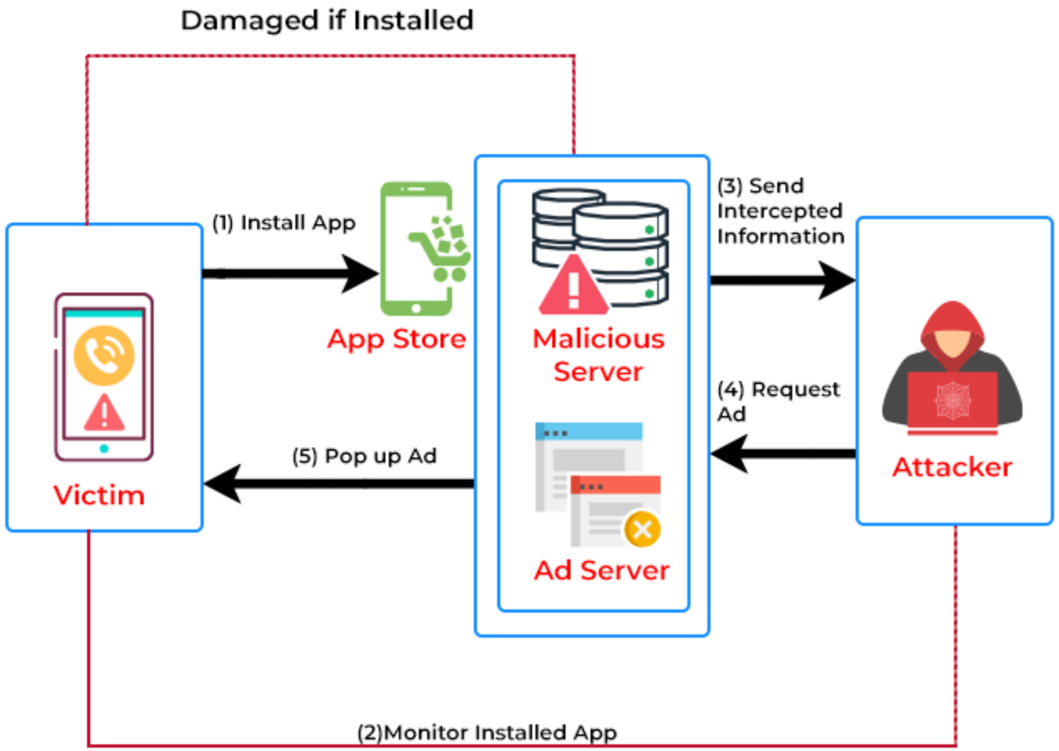
50 Best Online Casinos: Ranked by Quality
Top 50 online casinos ranked by quality and payout rate -...

...oker events. Play all the popular poker games live, for Fun or Real Money. Chat with Others. 25% Deposit Bonus. 24/7 Support.

Source: Techtarge

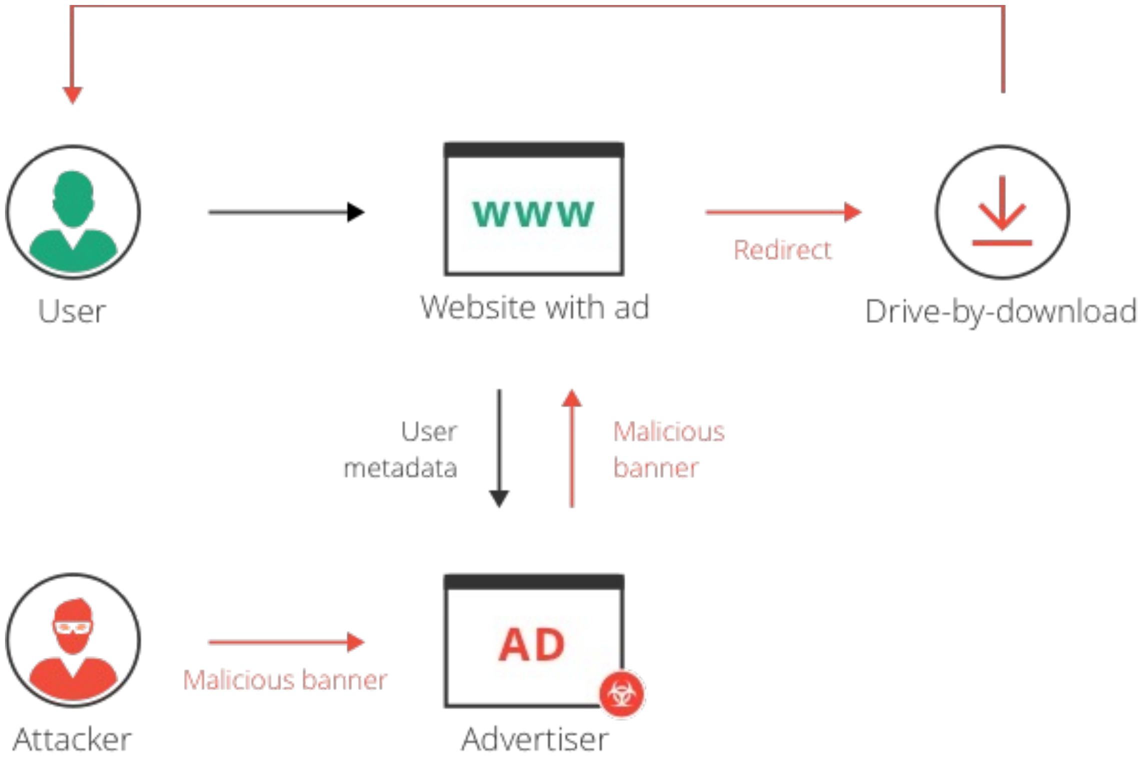
Adware and Malvertising

Adware



Source: Spiceworks

Malvertising



Source: Imperva

Spyware

A malware which infects your PC or mobile device and gathers information about you, including the sites you visit, the things you download, your usernames and passwords, payment information, and the emails you send and receive.

Types of Spyware:
Password stealers, Banking Trojans (e.g. Emotet), Infostealers, Keyloggers.

Question: how you get spyware?

Source: Malwarebytes

Ransomware

A type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.

Types of Ransomware:
Scareware, screen lockers, and encrypting ransomware.

Questions:
How you get ransomware?
How do you protect yourself from ransomware?

Source: Malwarebytes

Trojans

A Trojan is a delivery strategy that hackers use to deliver any number of threats, from ransomware that immediately demands money, to spyware that conceals itself while it steals valuable information like personal and financial data.

Types of Trojan:
Backdoors, Spyware, Zombifying, Downloader, Rootkit, Dialer.

Source: Malwarebytes, Imperva

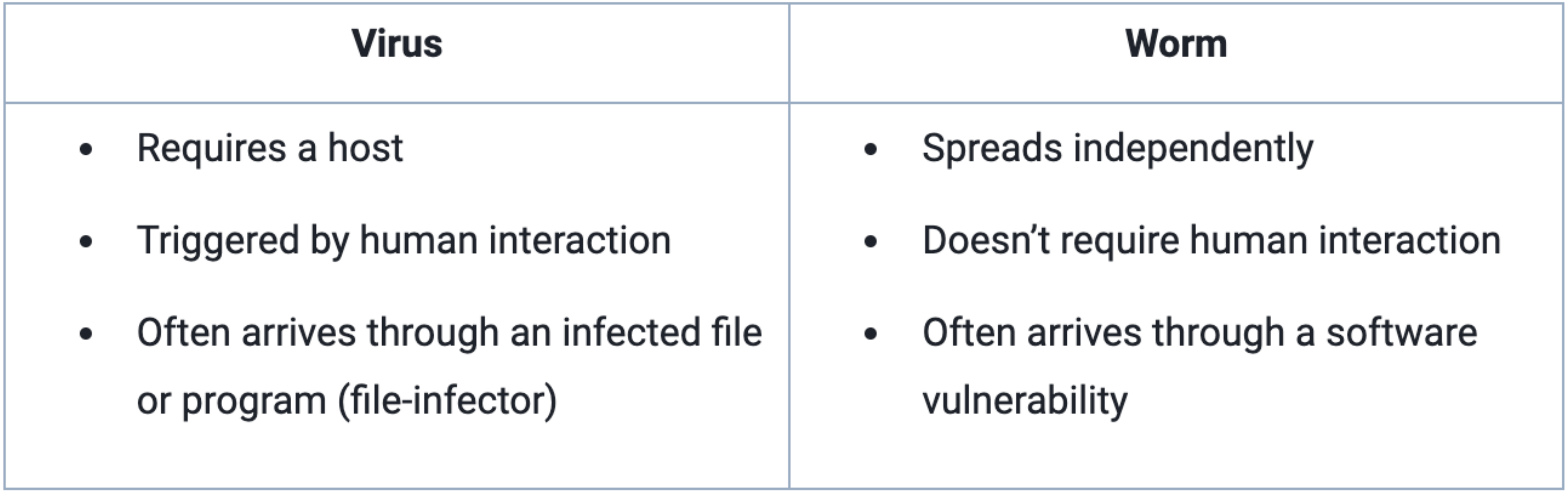
Worms and Viruses

A computer **virus** is a program made of malicious code that can propagate itself from device to device. A virus spreads when the infected file or program migrates through networks, file collaboration apps, email attachments, and USB drives.

Worms are a self-replicating type of malware (and a type of virus) that enter networks by exploiting vulnerabilities, moving quickly from one computer to another.

Source: Varonis

Worms vs. Viruses



Virus	Worm
• Requires a host • Triggered by human interaction • Often arrives through an infected file or program (file-infector)	• Spreads independently • Doesn’t require human interaction • Often arrives through a software vulnerability

Question: which one is more dangerous? Why?

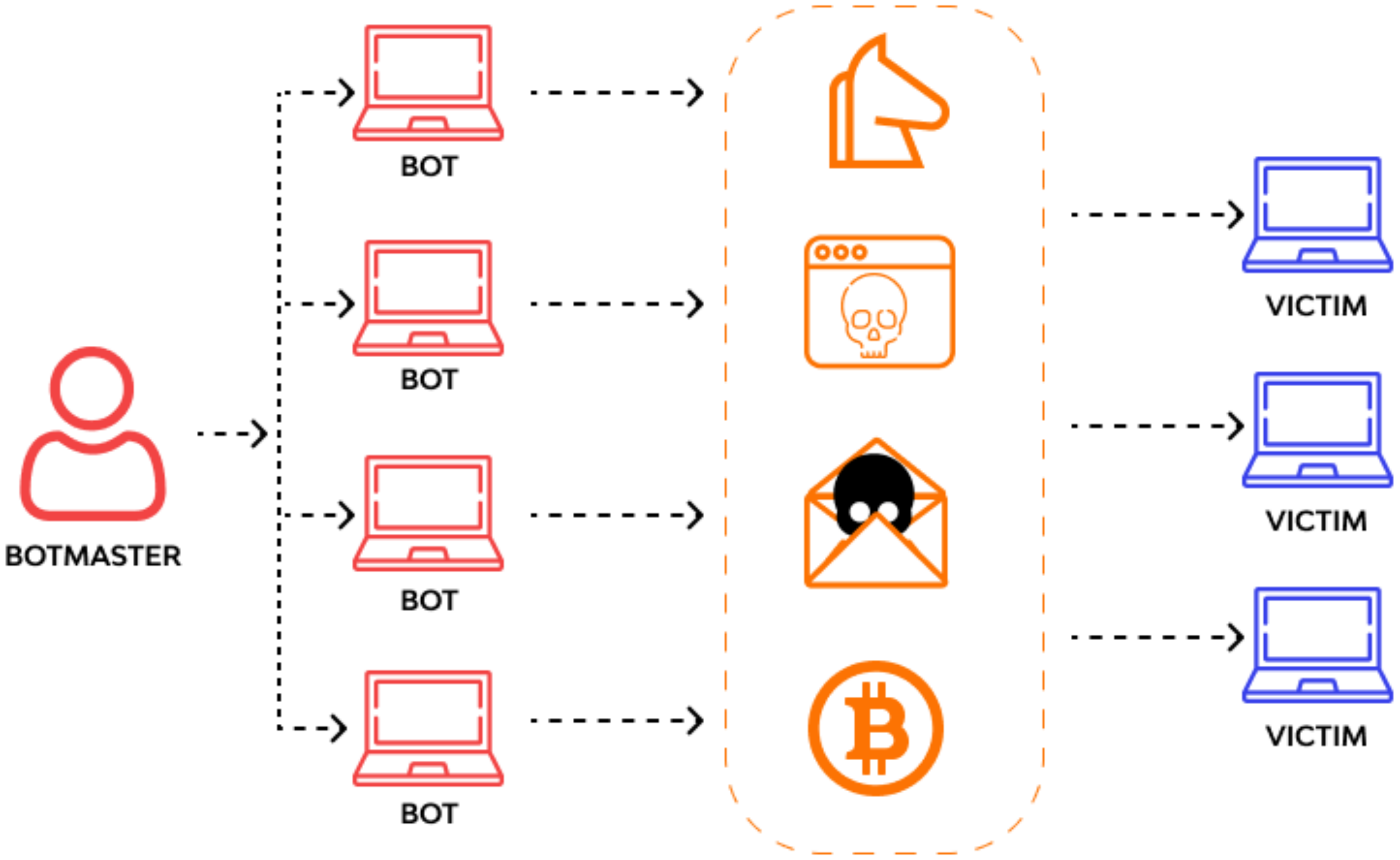
Source: AVG

Botnet

A botnet is a network of computers infected with **malware** that are controlled by a **bot herder**. The bot herder is the person who operates the botnet infrastructure and uses the compromised computers to launch attacks designed to crash a **target's network, inject malware, harvest credentials or execute CPU-intensive** tasks. Each individual device within the botnet network is called a bot.

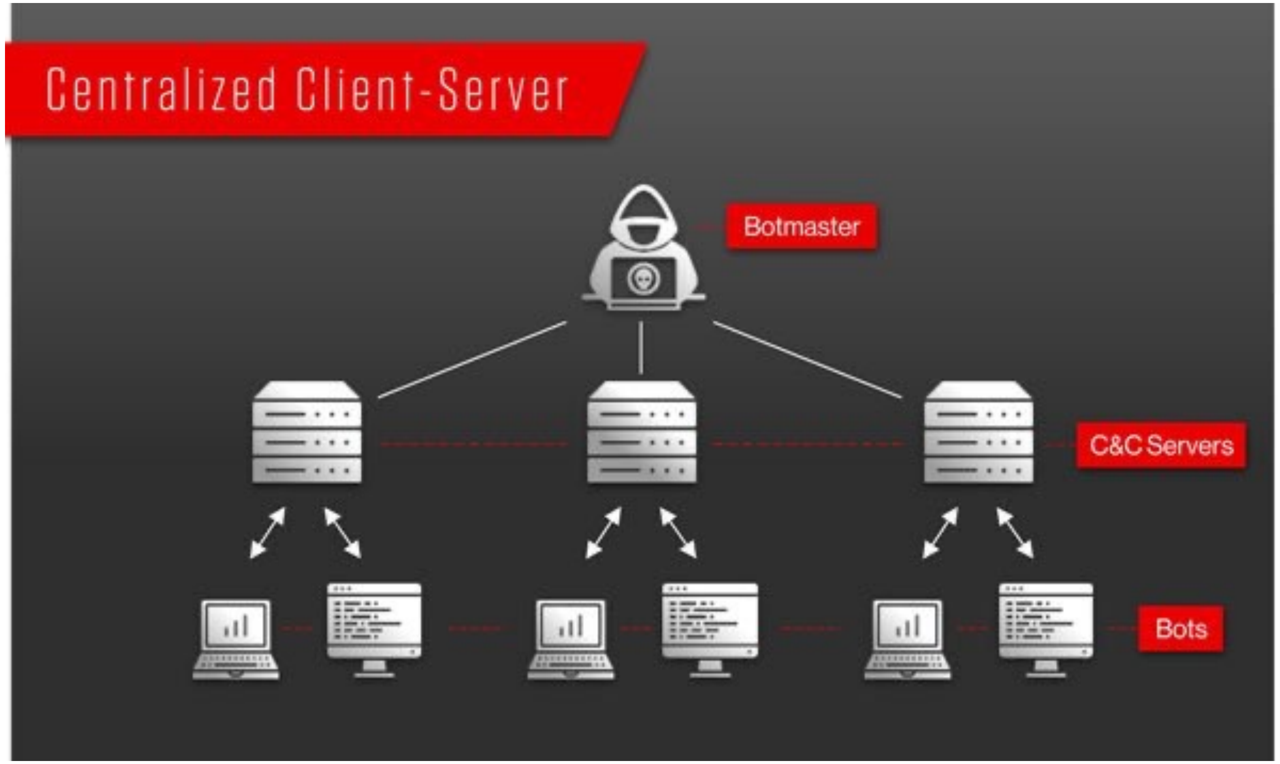
Source: CrowdStrike

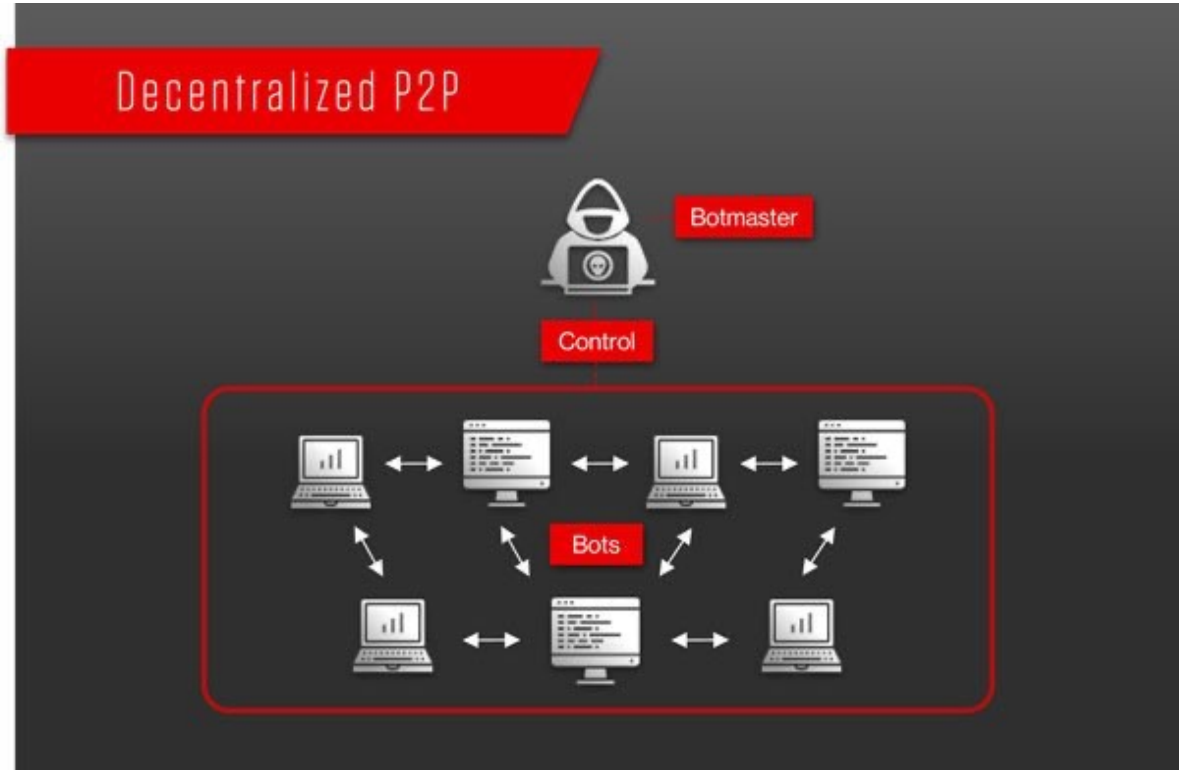
Botnet



Source: Wallarm

Botnet Types





Source: [CrowdStrike]()

PUP malware

PUPs (**potentially unwanted programs**) are programs often bundled with a software installation package from a download site. PUP software can refer to **unwanted** toolbar extensions, shopping assistants, or system optimization tools.

PUPs usually deliver ads or collect user data for their developers. They can also **hijack your browser, change your search results, or steal sensitive information**. Although a PUP is not a computer virus, they can compromise the security of your computer and infect both mobile and desktop devices.

Source: Avast

Hybrids

A hybrid malware is a combination of two or more different types of attacks. This combination is usually a Trojan horse or worm with adware or a virus attached, though other forms exist.

Unlike traditional malware, hybrid malware utilizes the strengths of various threats (e.g., worms, viruses, spyware, or Trojans) to create a more powerful hazard. For example, a cybercriminal can combine a Trojan and spyware to bypass security programs and easily download spyware onto a target's computer.

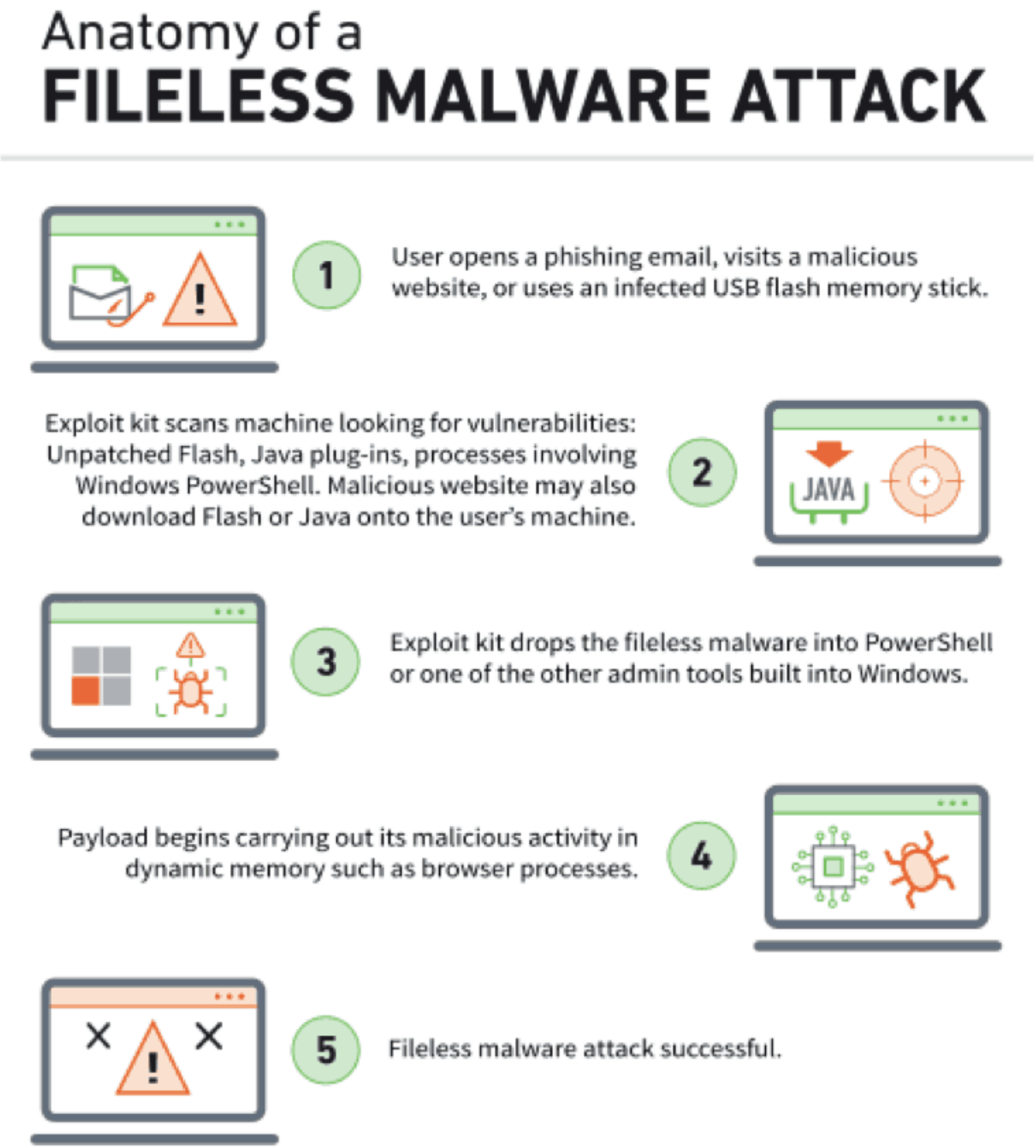
Source: Nexthop

Fileless malware

Fileless malware is a type of malicious activity that uses native, legitimate tools built into a system to execute a cyber attack. Unlike traditional malware, fileless malware does not require an attacker to install any code on a target’s system, making it hard to detect

Source: Crowdstrike

Fileless malware



Anatomy of a FILELESS MALWARE ATTACK

1 User opens a phishing email, visits a malicious website, or uses an infected USB flash memory stick.

2 Exploit kit scans machine looking for vulnerabilities: Unpatched Flash, Java plug-ins, processes involving Windows PowerShell. Malicious website may also download Flash or Java onto the user's machine.

3 Exploit kit drops the fileless malware into PowerShell or one of the other admin tools built into Windows.

4 Payload begins carrying out its malicious activity in dynamic memory such as browser processes.

5 Fileless malware attack successful.

Source:.Exabeam

Logic bombs

A logic bomb is a set of instructions in a program carrying a malicious payload that can attack an operating system, program, or network. It only goes off after certain conditions are met. A simple example of these conditions is a specific date or time.

- Embedded in some legitimate program
- "Explode" or perform malicious activities when certain conditions are met

Source: Malwarebytes

Keylogger

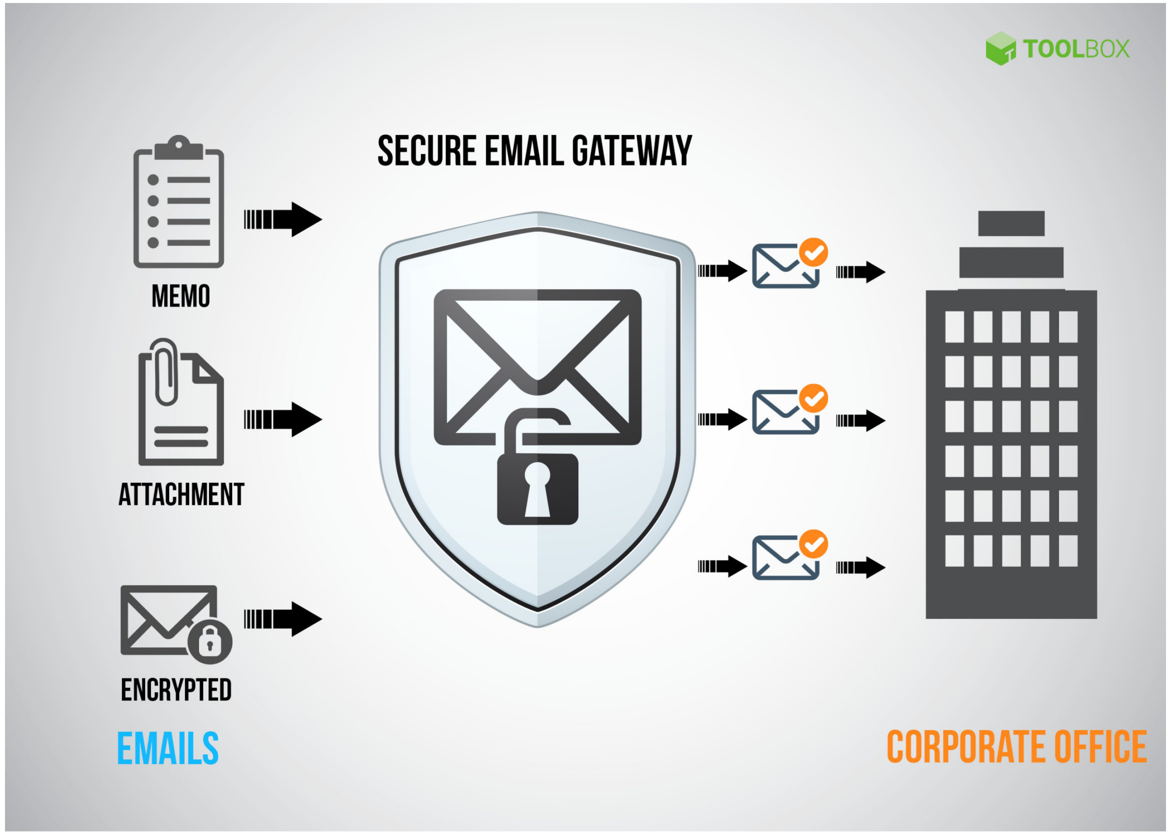
A type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device.

Software and Hardware Keyloggers

Source: Malwarebytes

Email Security

Email security is a term for describing different **procedures** and **techniques** for **protecting email accounts, content, and communication** against unauthorized access, loss or compromise. Email is often used to spread **malware**, **spam** and **phishing** attacks.



Source: Proofpoint