Analyzing Malware and Other Attacks

Module Overview

Indicators of Attack

- Malware
  - Ransomware, trojans, worms, etc.
- Password attacks
- Physical attacks
- Adversarial AI
- Supply chain attacks
- Cloud-based vs. on-prem attacks
- Cryptographic attacks

Indicator of Compromise (IOC)

Artifacts observed that indicate (with a high degree of confidence) a computer intrusion

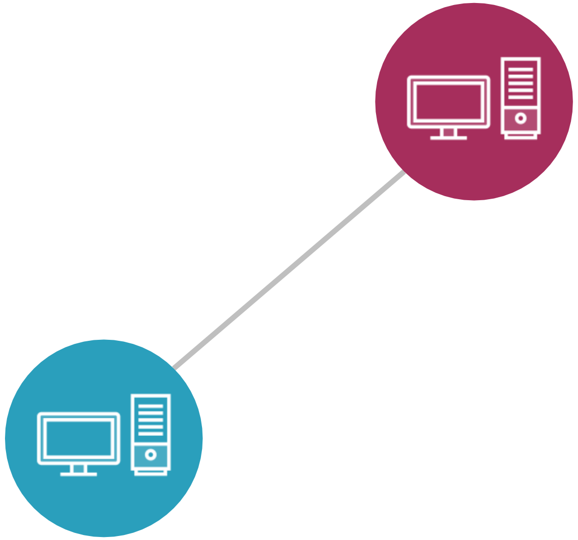
Some Potential Indicators of Compromise

- Unusual outbound network traffic
- DNS request anomalies
- Mismatch port-application traffic
- Anomalies in privileged user account activity

Virus

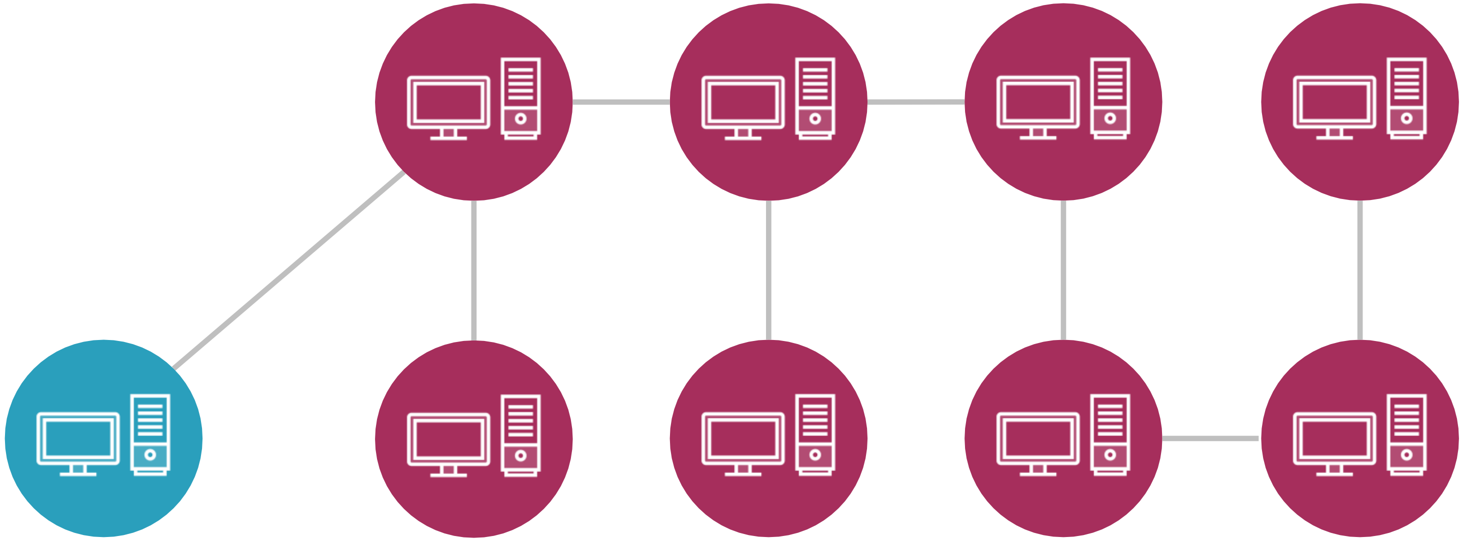
Malicious code that requires user interaction to install and replicate

Viruses



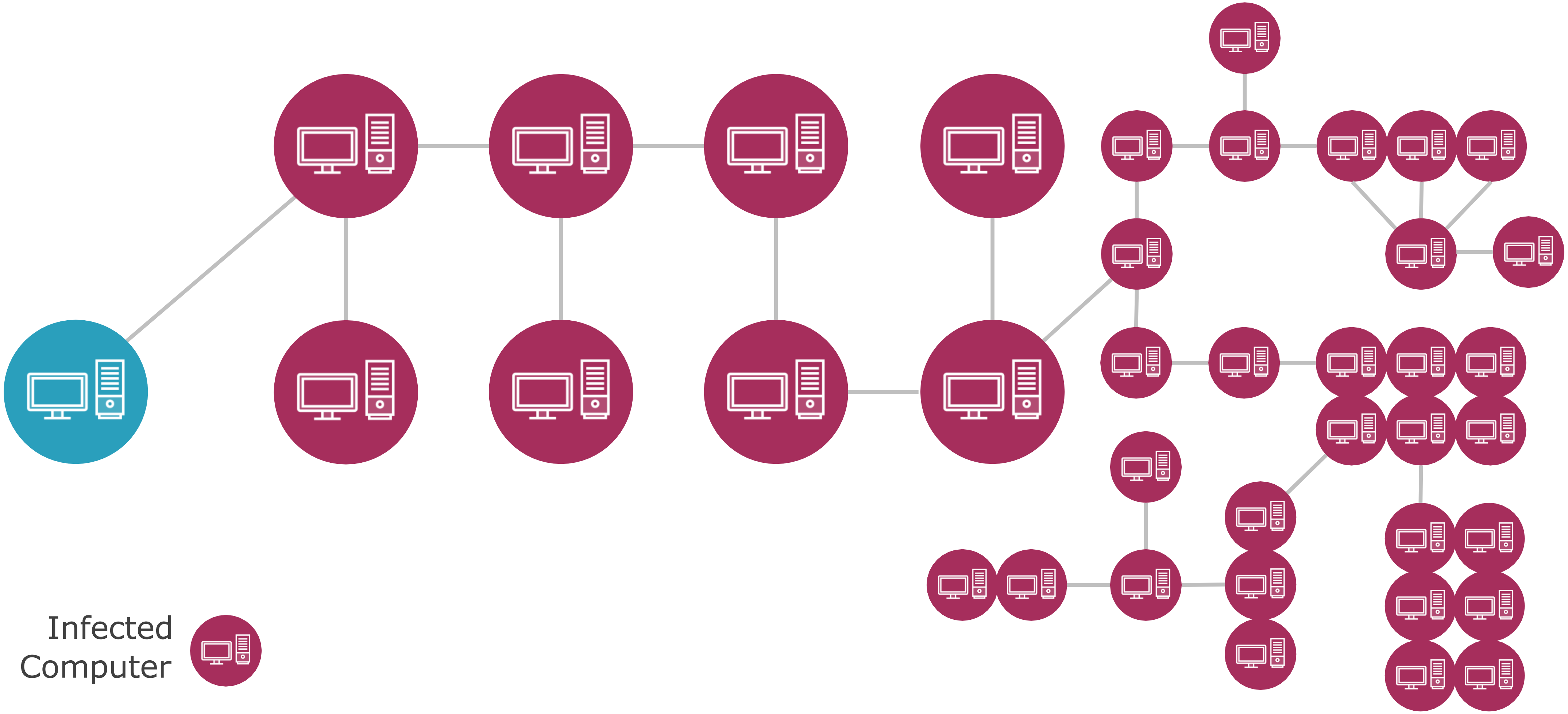
Infected Computer

Viruses



Infected Computer ●

Viruses



Infected Computer ●

Crypto-malware/Ransomware

Malicious applications that scare or scam users into taking some type of action

(Typically paying the creator for removal of the ransomware / decryption of files)

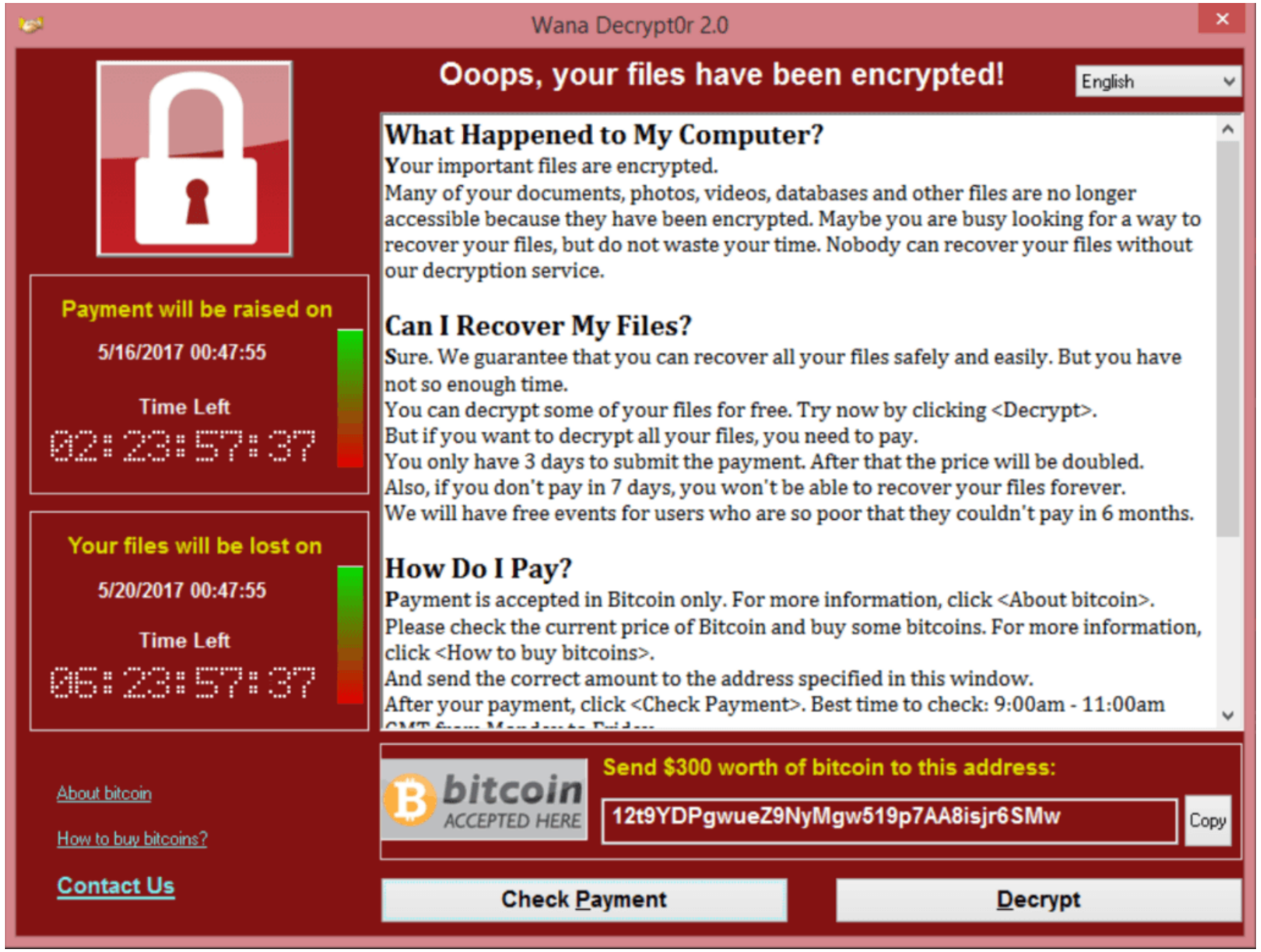
Crypto-malware / Ransomware

WannaCry Attack (Wcrypt)

Quickly spread to over 150 countries infected over 200,000 computers within just days

Spread via Microsoft “EnternalBlue” vulnerability

Patched with MS17-010



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

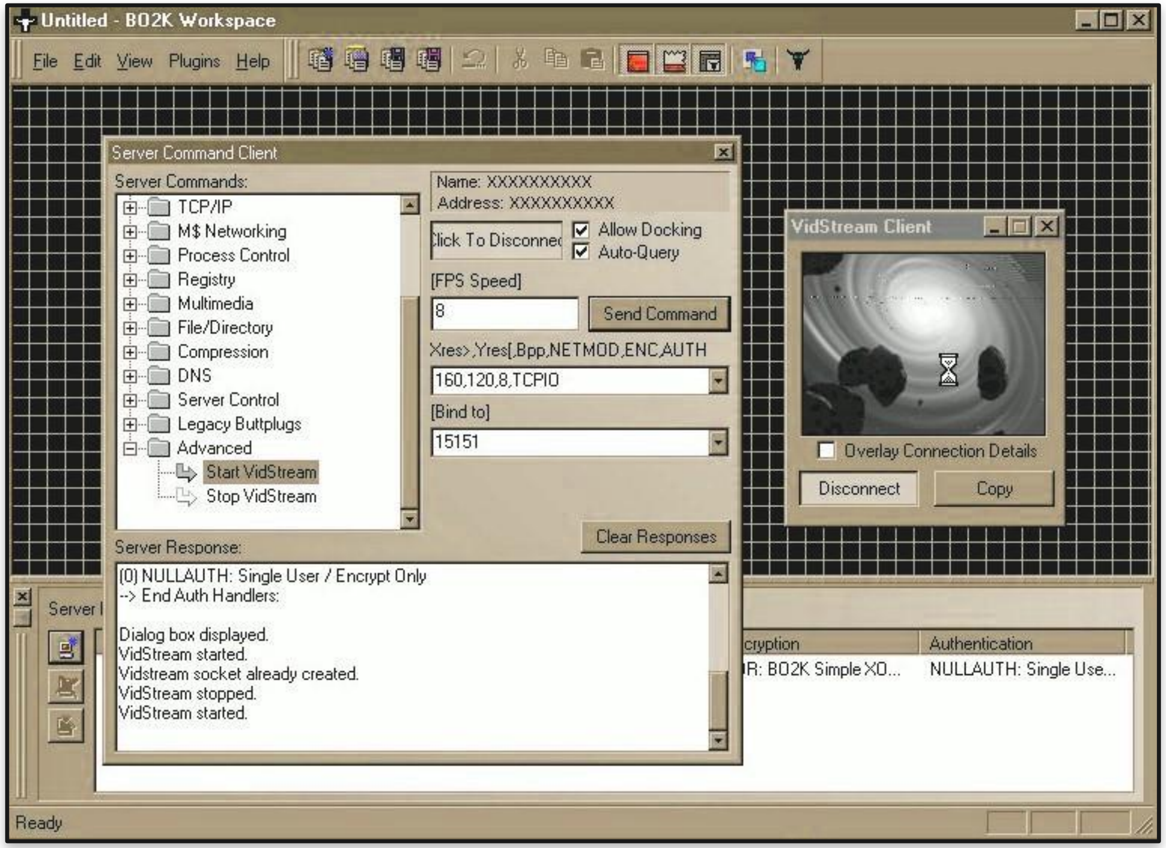
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Trojan

Seemingly friendly software that contains hidden malicious software

Trojan

Trojan



Name: XXXXXXXXXX
Address: XXXXXXXXXX

☑ Allow Docking
☑ Auto-Query

[FPS Speed]
8

Xres>,Yres[,Bpp,NETMOD,ENC,AUTH
160,120,8,TCPIO

[Bind to]
15151

□ Overlay Connection Details

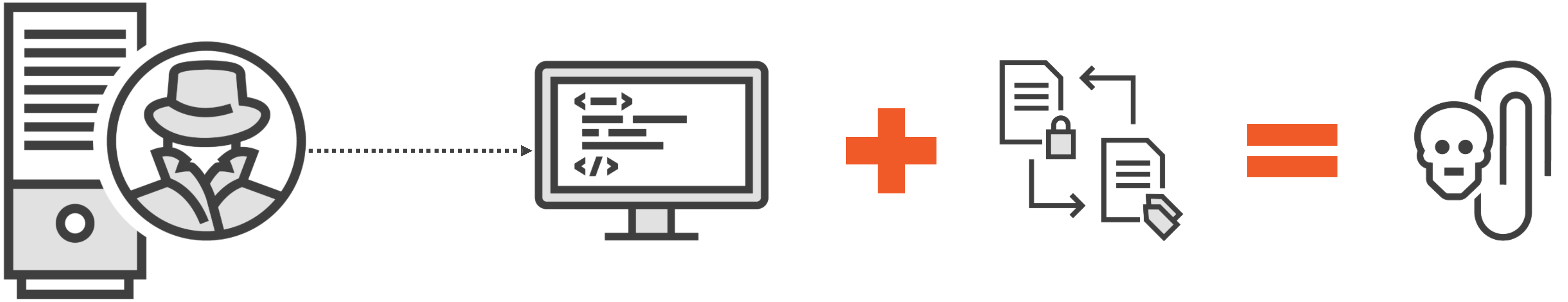
```
(0) NULLAUTH: Single User / Encrypt Only
--> End Auth Handlers:

Dialog box displayed.
VidStream started.
Vidstream socket already created.
VidStream stopped.
VidStream started.
```

R: BO2K Simple XO... NULLAUTH: Single Use...

Common Remote Access Tools (RAT)

- Project BioNET
- NetBUS
- Sub7
- Back Orifice
- BO2k (Back Orifice 2k)
- Beast
- Lost Door

Trojan



Hacker

Original Code

Bound w/ new program

Malicious RAT

Worms

Worms

- Self-replicating program that is usually self-contained and can execute and spread without user interaction

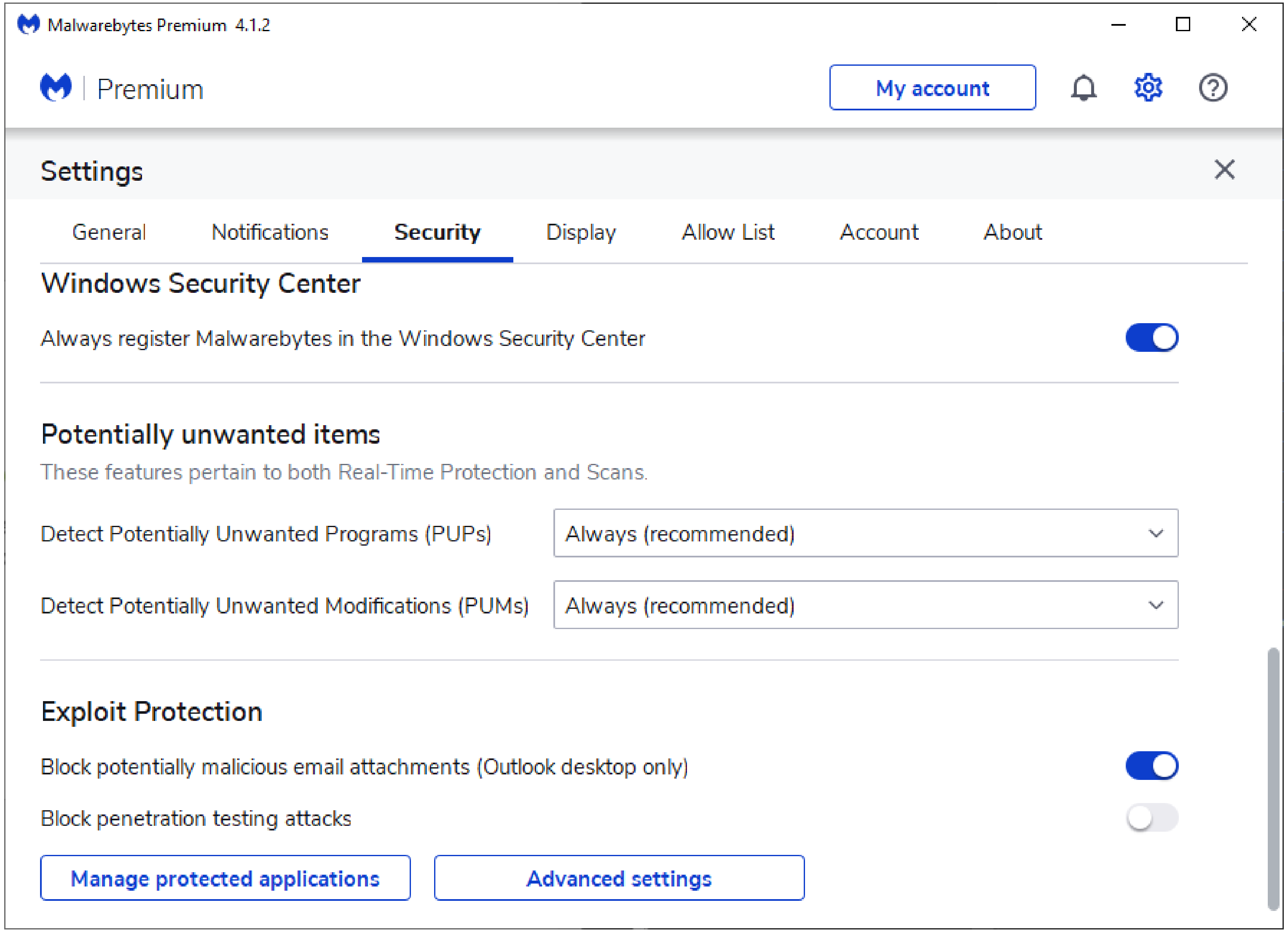
Two main types of worms

- Network Service Worms
  - Exploits network vulnerability to propagate and infect others
- Mass Mailing Worms
  - Exploits email systems to spread and infect others

Potentially Unwanted Program (PUP)

Applications that are typically downloaded as part of another program (adware, spyware, etc.)

Potentially Unwanted Programs (PUP)



Windows Security Center

Always register Malwarebytes in the Windows Security Center ●

Potentially unwanted items

These features pertain to both Real-Time Protection and Scans.

Detect Potentially Unwanted Programs (PUPs): Always (recommended)

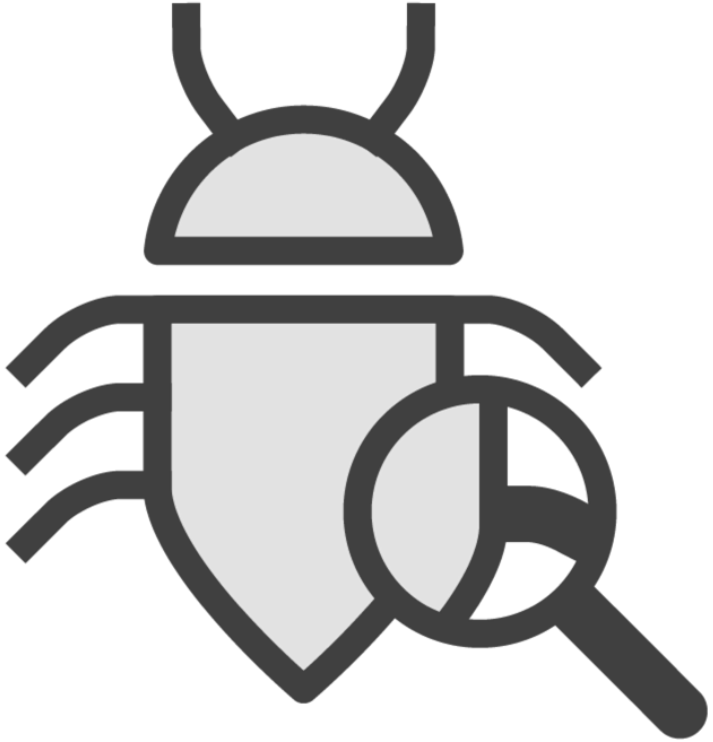
Detect Potentially Unwanted Modifications (PUMs): Always (recommended)

Exploit Protection

Block potentially malicious email attachments (Outlook desktop only) ●

Block penetration testing attacks ○

Fileless Virus



Malware that operates in memory

- Not stored in a file nor installed on a victim’s machine
- Typically hooks into a Windows PC via PowerShell or WMI
- 2017 Ponemon Institute study estimates that 77 percent of detected attacks were fileless

Common Fileless Virus/Malware Tools

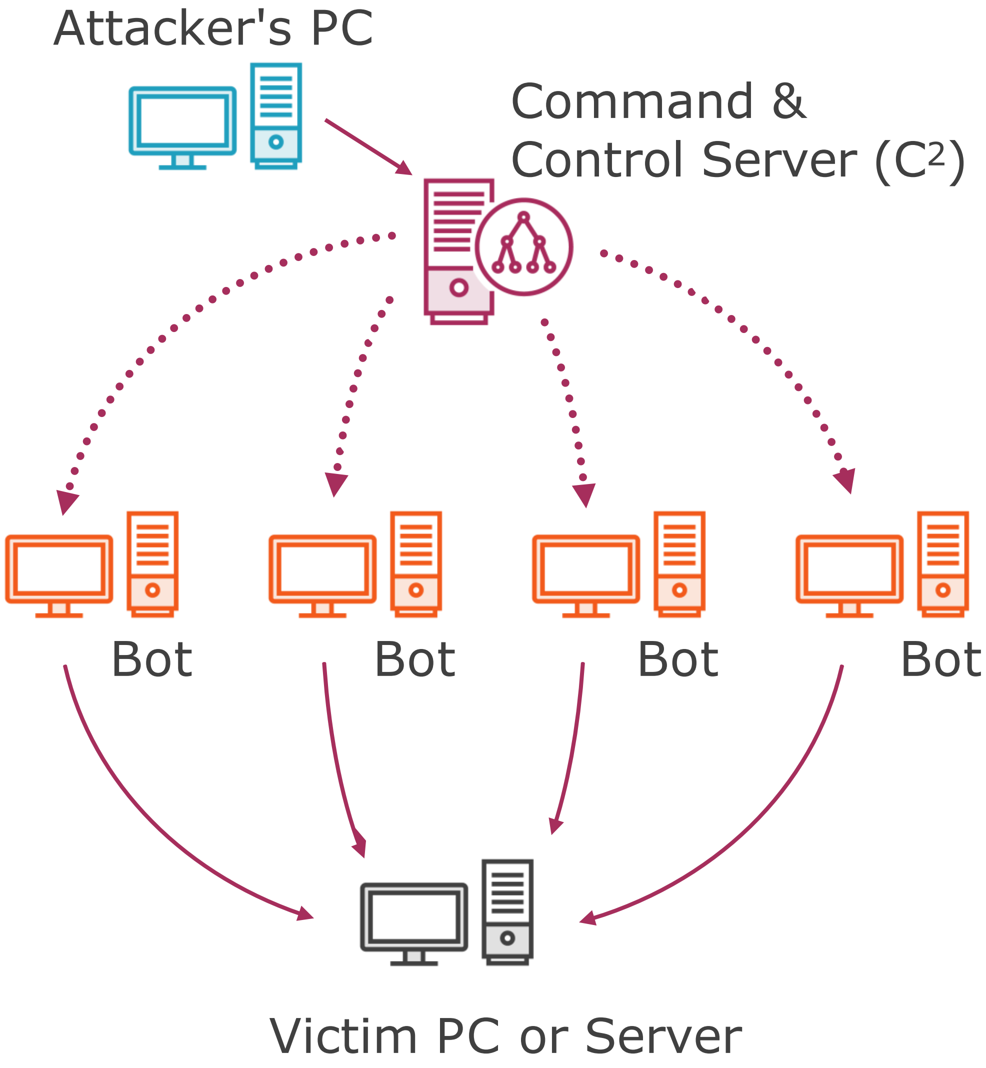
Fileless/attack frameworks examples

- Empire
- PowerSploit
- MetaSploit
- CobaltStrike

Enables fileless malware creation and Powershell post-exploit framework

Botnets

Malicious code that infects large numbers of hosts for the purpose of launching large scale attacks on specific targets



Botnets

Attacker can be located anywhere in the world

Control one or more Command and Control (C^2 or C&C) Servers

C&C servers can control thousands of bots (zombies) for massive DDoS attacks

Logic Bomb

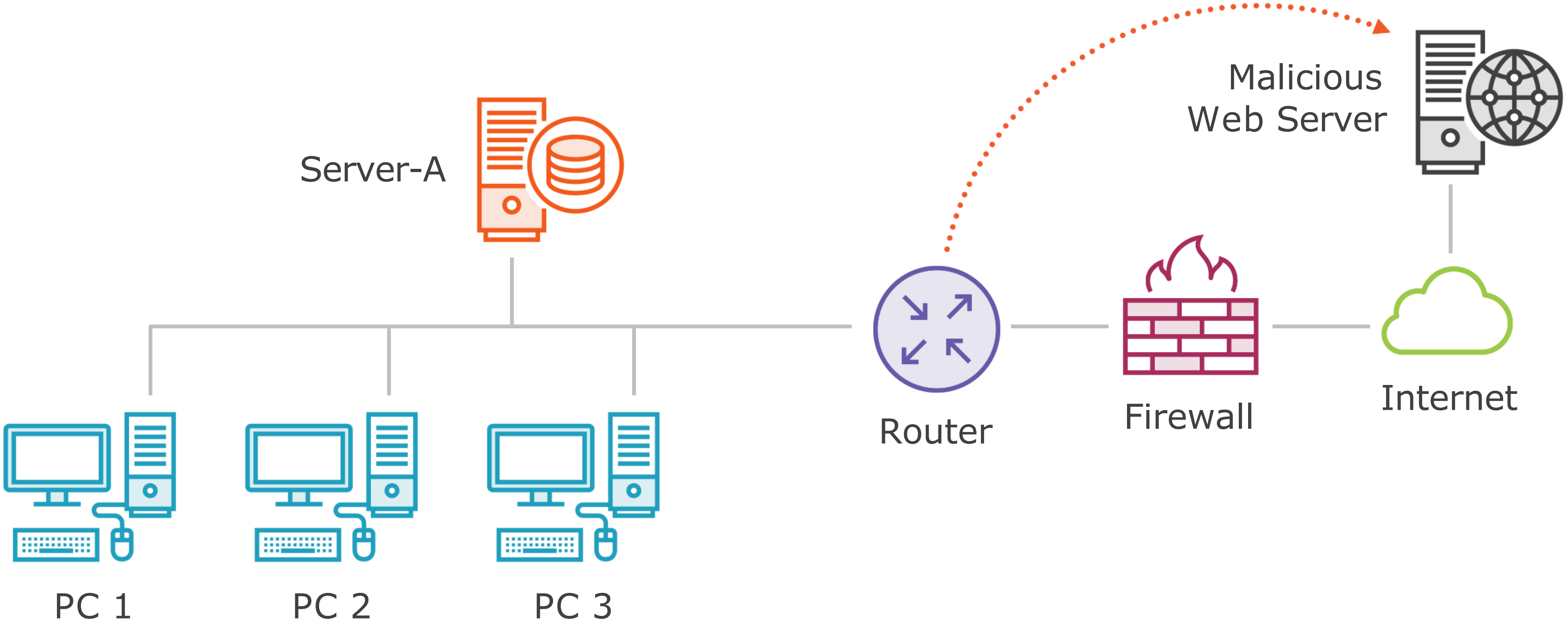
Malicious code that triggers after a period of time based on some date or specific activity

Spyware

Malicious software that captures user activity and reports back

(keystrokes, web browsing activity, etc)

Spyware


Server-A
Malicious
Web Server
Router
Firewall
Internet
PC 1
PC 2
PC 3

Keylogger

Malicious application that once installed on a host can capture all keystrokes

- Usernames/Passwords
- Sensitive information
- Emails / chats / instant messages

Captured files can be uploaded to a remote location, emailed, or stored locally for later retrieval

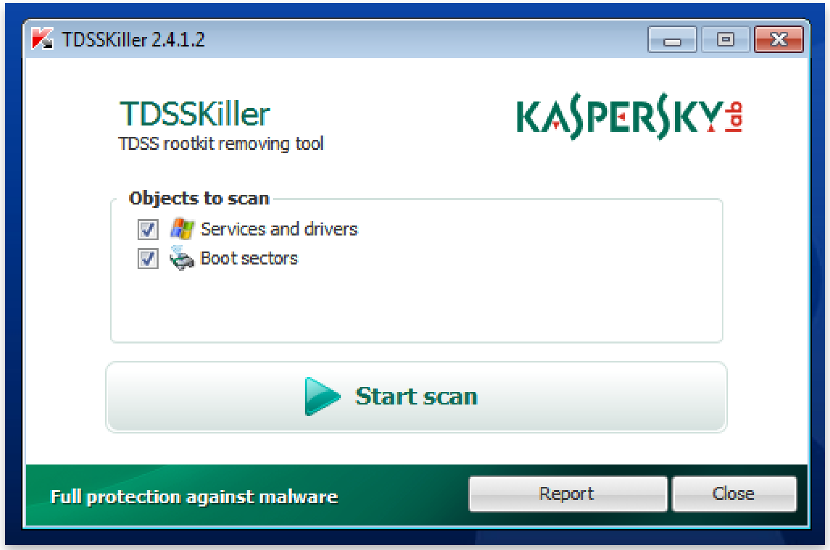
Rootkits

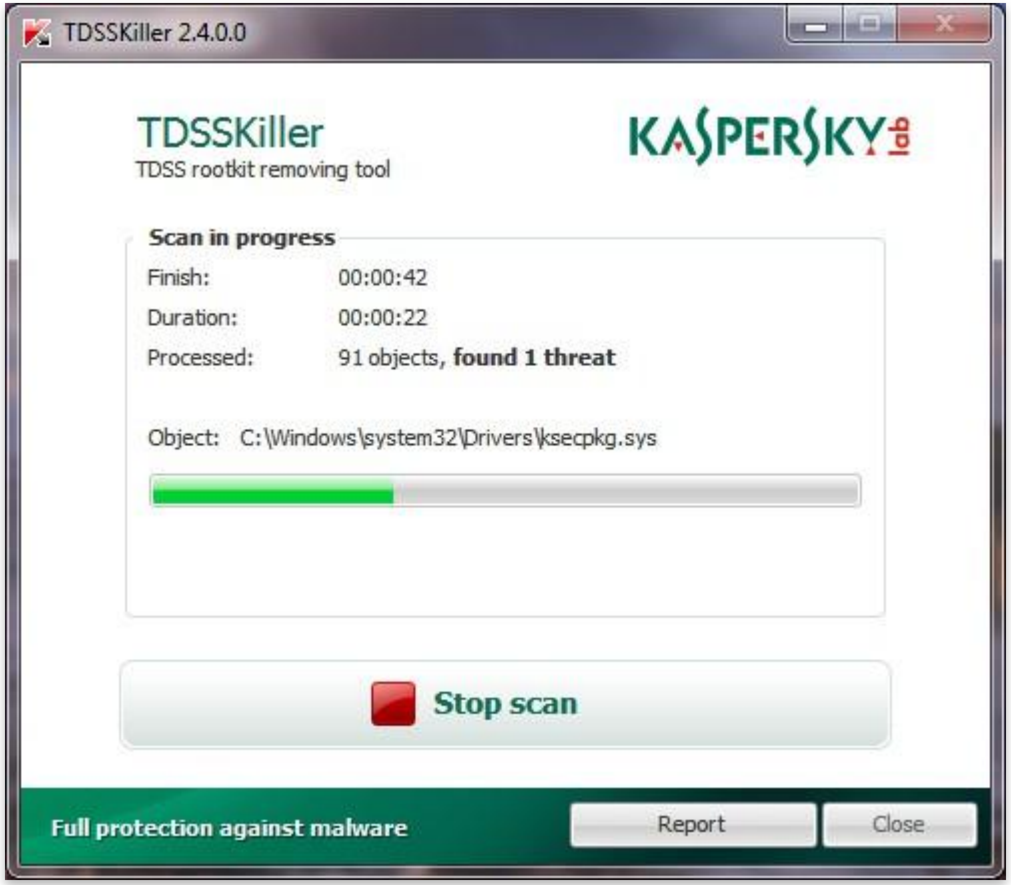
Malicious code that installs itself at the OS or Kernel level to avoid detection

Rootkits

Rootkits are very difficult to get rid of

- Load before the OS loads
- Can disable anti-virus and anti-malware





Finish: 00:00:42
Duration: 00:00:22
Processed: 91 objects, **found 1 threat**

Object: C:\Windows\system32\Drivers\ksecpkg.sys

Backdoors

Software that installs for the purpose of opening ports and installing additional software

Spraying

- Feeding a large number of usernames into program that loops through passwords
- Brute force type of attack that can be used with dictionary attacks or a database of compromised passwords

Can be mitigated by using two-factor authentication (2FA)

Dictionary

Using known words to try and defeat a cipher

- Using words in a dictionary or a pre-defined set of possible words
- Faster than brute force in that only words that are likely to succeed are used

Hybrid Attack combines dictionary attack along with word variations

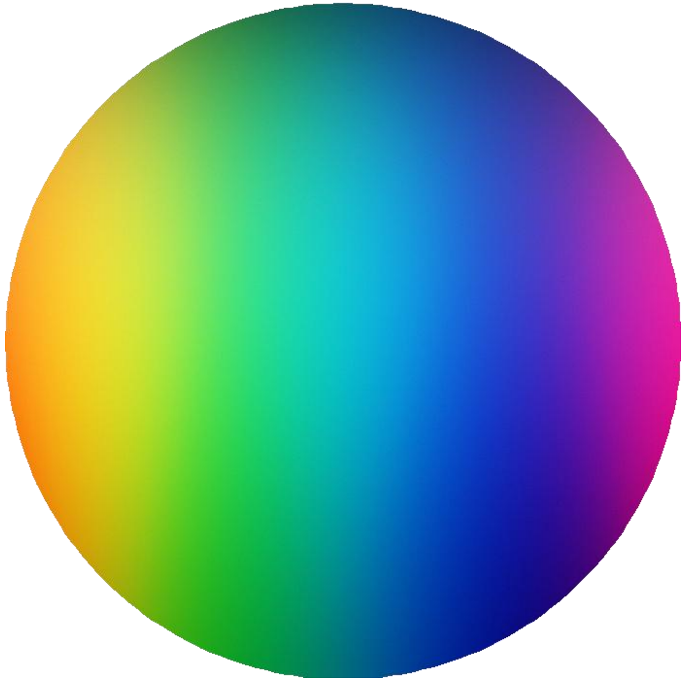
- Used prior to resorting to plain brute-force attack

Brute Force Attack

- Systematic approach trying every possible combination of passwords or passphrases
  - Time consuming
  - Resource intensive

- Mitigations
  - Most accounts will lock out after “x” number of attempts
  - Length of password increases time to crack

Rainbow Tables



Precomputed table to reversing cryptographic hashes

- Reduces time to brute-force a password
- Increases amount of storage necessary to storage rainbow tables
- Rainbow table needed for each has type (MD5, SHA1, etc)

Can be mitigated using “Password Salting”

- Adding random data to the hashing algorithm so that each user's hash is unique even if both have the same password
  - Larger salts increase security

Known Plain Text / Ciphertext

Access to both the plaintext and the encrypted output (ciphertext)

- The attack can be used to reveal further information such as secret keys or code books used to encrypt subsequent messages

Advanced Encryption Standard (AES) cipher is not vulnerable to this type of attack

Physical Attacks

Malicious Universal

Universal Serial Bus (USB)

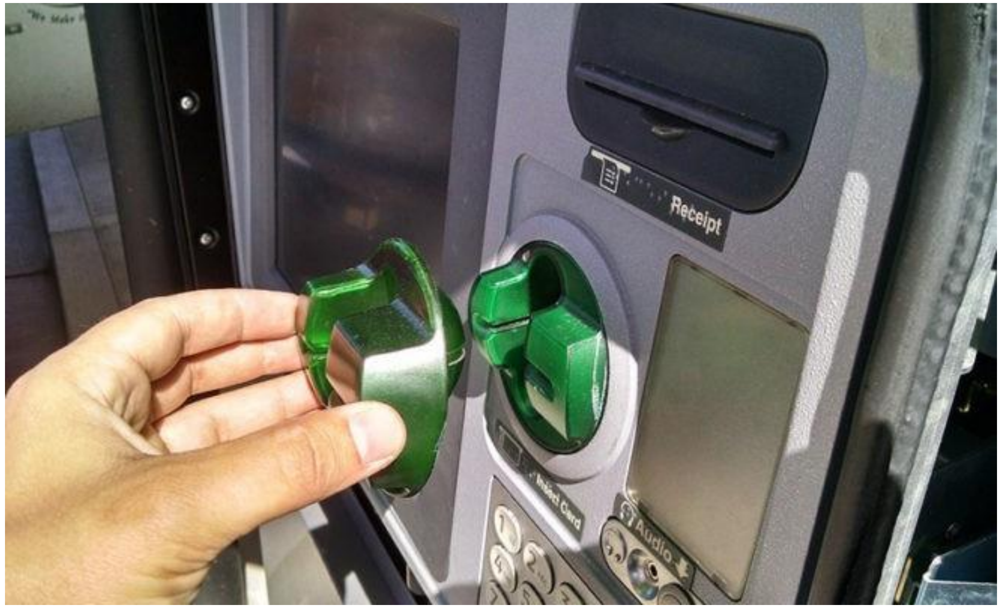
Malicious Flash Drive

Card Cloning

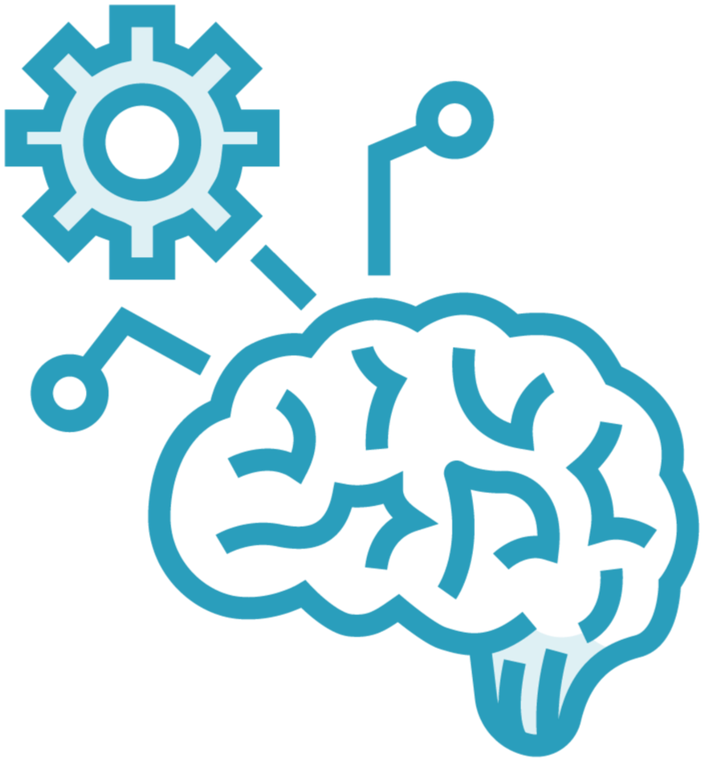
Skimming

Skimming techniques

- Card reader used at checkout counter that scans magnetic strip
- Duplicate card reader that slips over ATM card reader and downloads magnetic strip info



Adversarial Artificial Intelligence (AI)



Tainted training data for ML

- Technique to fool models by supplying deceptive (tainted) input

Security of ML algorithms

- Threat modeling
- Attack simulations
- Countermeasure simulations
- Secure learning algorithms

Supply Chain Attacks

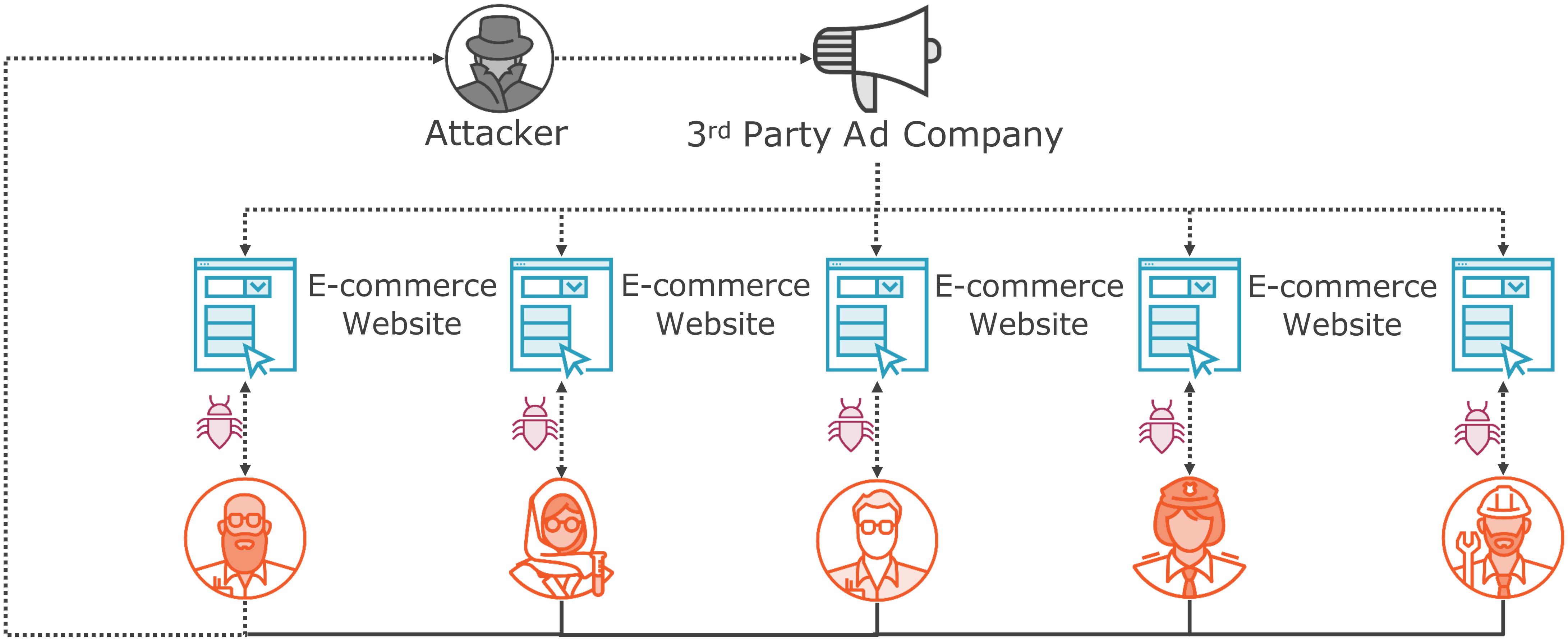
Attack on an organization by targeting less-secure elements in a supply network

- Advanced Persistent Threats (typically)
- Targets victims further down the supply chain network

Examples

- POS malware / Infected USB sticks
- Malware (or hardware) installed on computer equipment or network gear before it reaches target company

Supply Chain Attack Example



Skimmed transaction data sent to attacker

Cloud-Based vs. On-Premises Attacks

- Effectiveness of security depends on many factors
  - Type of company / datacenter(s)
  - Industry (regulations, compliance)
- Costs, expertise, data-mobility
- Infrastructure refreshes
- Frequency of data access

Cloud Provider Security

- Large security staff
- Deep expertise across a wide range of industries
- 24x7 monitoring
- Compliance and regulatory expertise

Birthday Attacks

Example of Birthday Paradox

Room full of people, what is the probability that two will share the same birthday

23 people = 50%

30 people = 70%

70 people = 99.9%

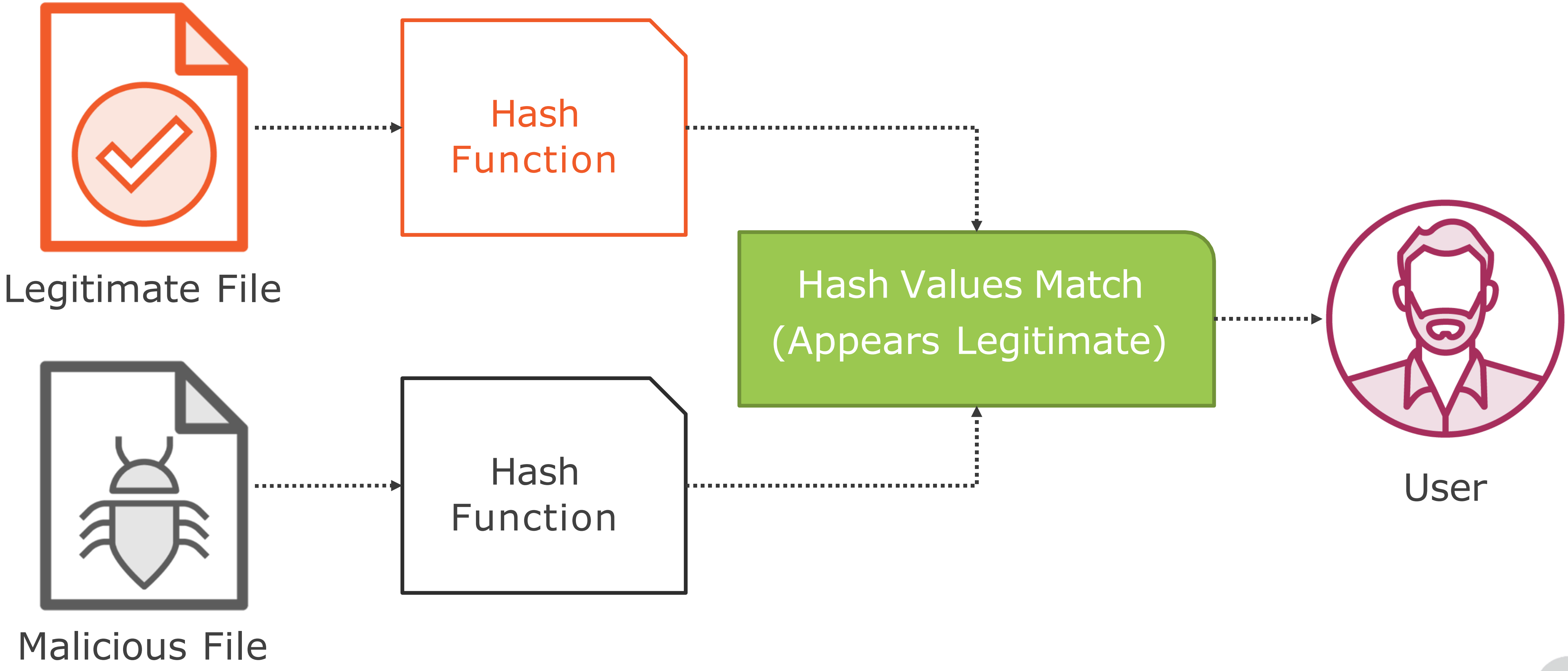
253 people = 100%

Collision Attack

Attack that tries to find two hash inputs that have the same output

- Two separate inputs that produce the same output is referred to as a collision
- Could be used to bypass security and enable a malicious file to appear legitimate if the hash values are the same

Collision Attack



Legitimate File

Hash Function

Malicious File

Hash Function

Hash Values Match (Appears Legitimate)

User

Downgrade Attack

Attack that forces a system to negotiate down to a lower-quality method of communication

- Allows an attacker to force a lower-grade, less secure method of communication
- Typically allowed to enable communication with legacy systems
- Often used with MiTM attacks

Module Review

Indicators of Attack

- Malware
  - Ransomware, trojans, worms, etc.
- Password attacks
- Physical attacks
- Adversarial AI
- Supply chain attacks
- Cloud-based vs. on-prem attacks
- Cryptographic attacks