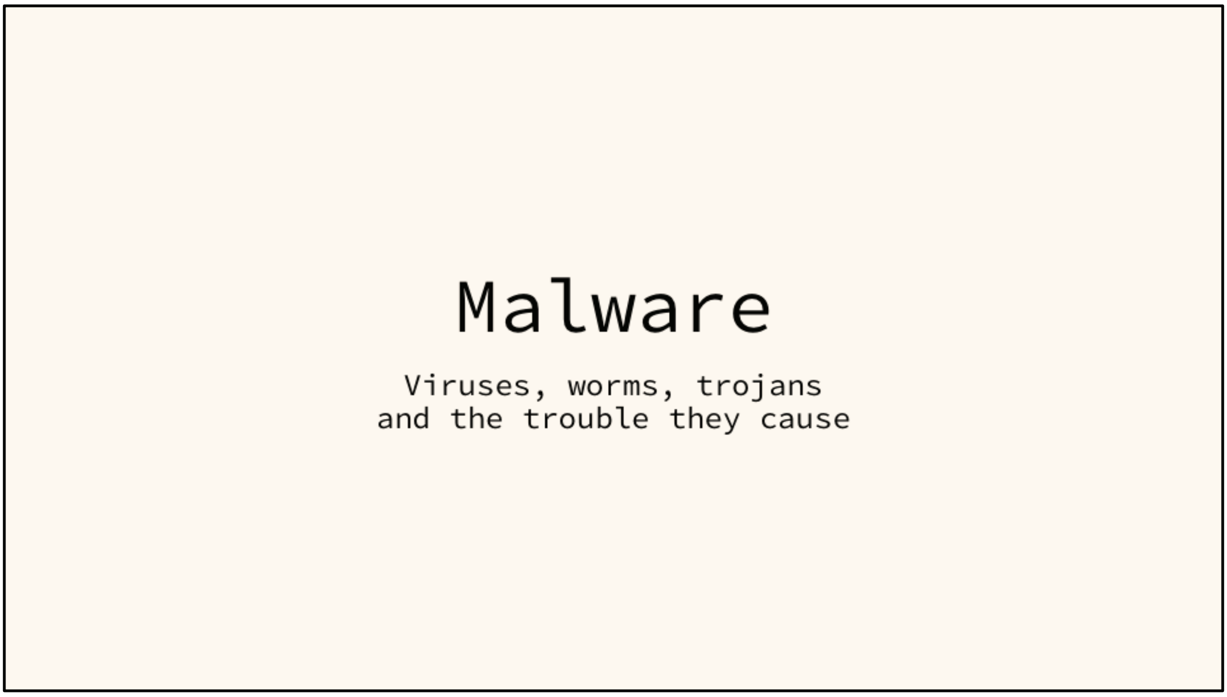
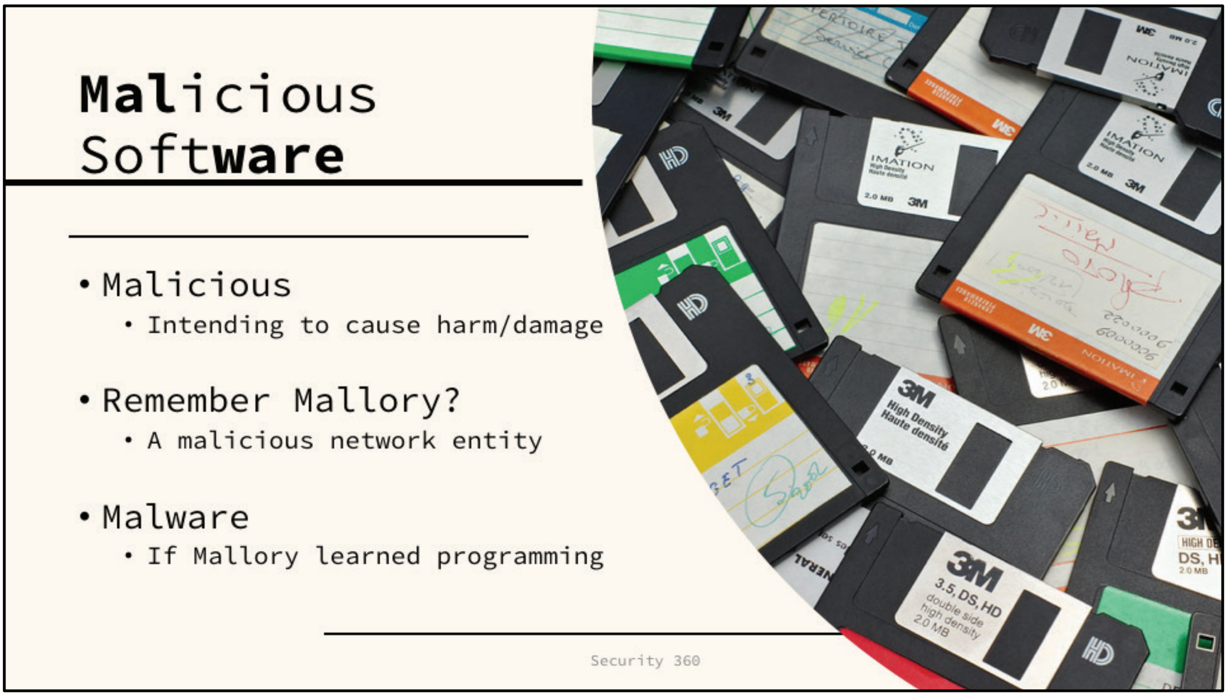


Malware

Viruses, worms, trojans
and the trouble they cause

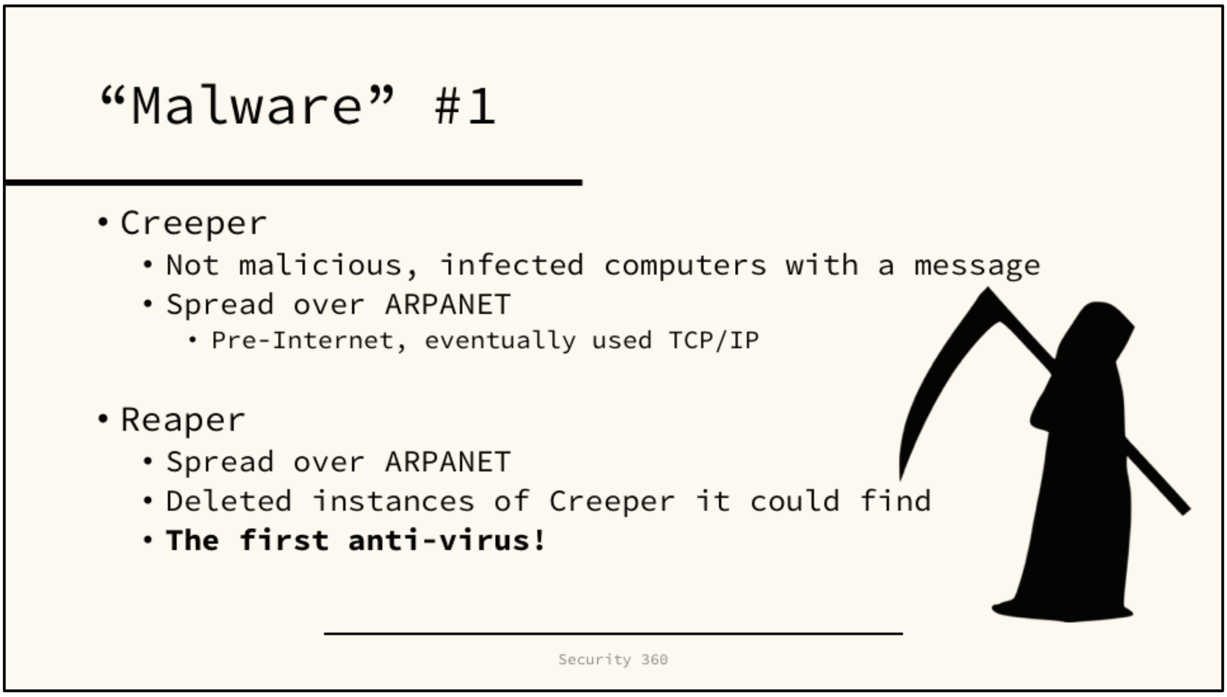


Malicious Software

- Malicious
  - Intending to cause harm/damage
- Remember Mallory?
  - A malicious network entity
- Malware
  - If Mallory learned programming

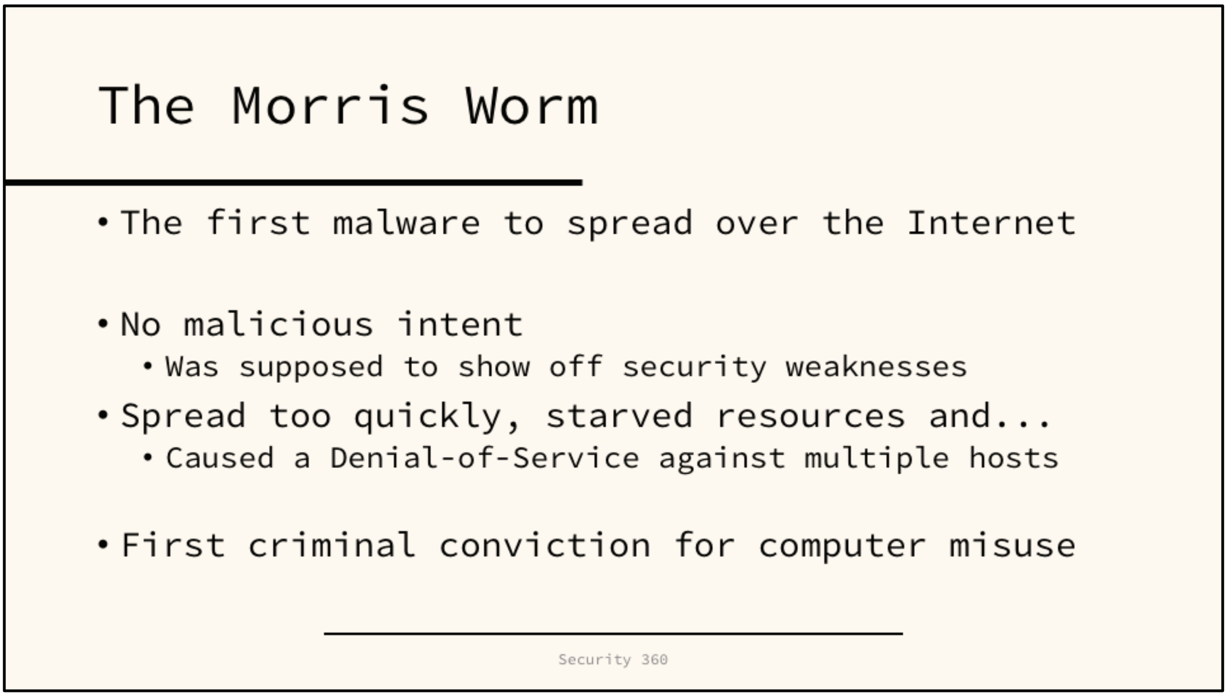
Security 360

"Vieilles disquettes" by zigazou76 is licensed under CC BY 2.0



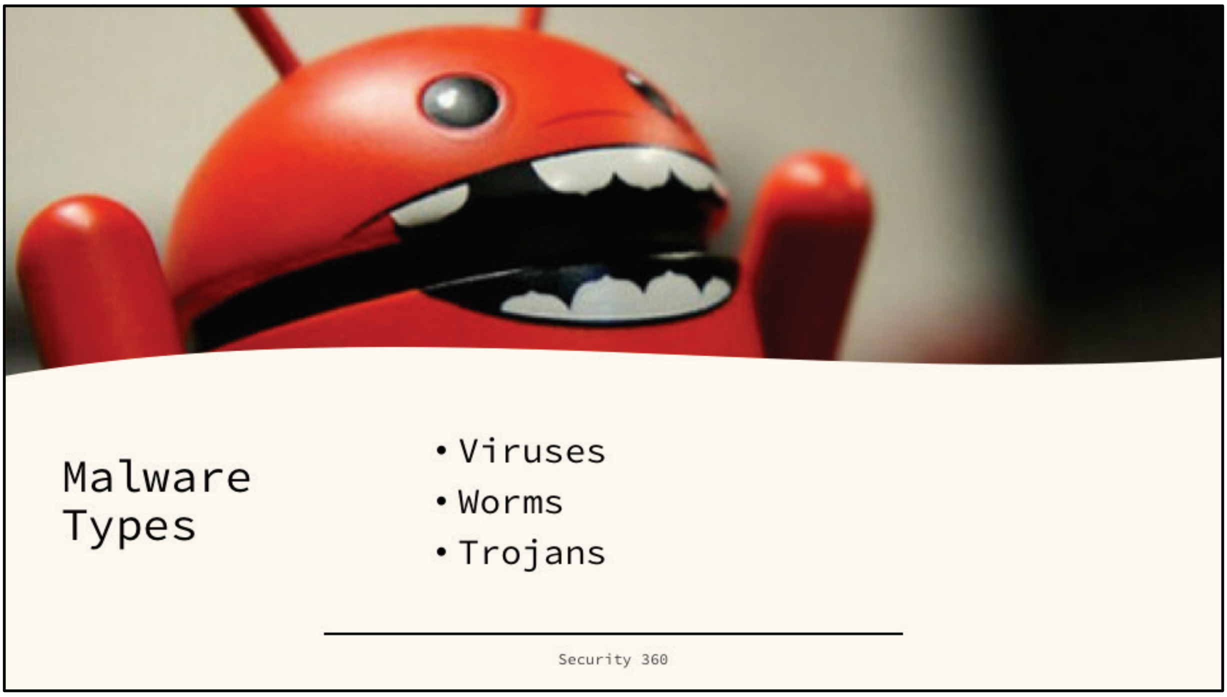
“Malware” #1

- Creeper
  - Not malicious, infected computers with a message
  - Spread over ARPANET
    - Pre-Internet, eventually used TCP/IP
- Reaper
  - Spread over ARPANET
  - Deleted instances of Creeper it could find
  - **The first anti-virus!**



The Morris Worm

- The first malware to spread over the Internet
- No malicious intent
  - Was supposed to show off security weaknesses
- Spread too quickly, starved resources and...
  - Caused a Denial-of-Service against multiple hosts
- First criminal conviction for computer misuse

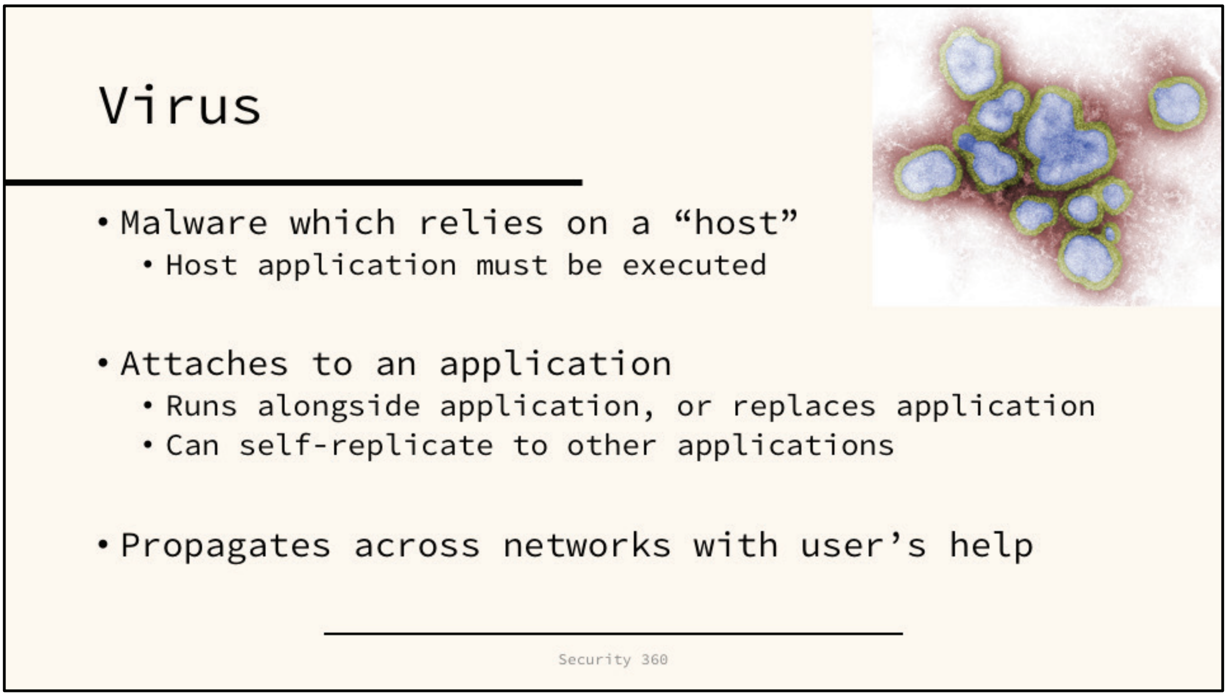


Malware Types

- Viruses
- Worms
- Trojans

Security 360

"android-tecnomovida" by tecnomovida is licensed under CC BY-NC-SA 2.0

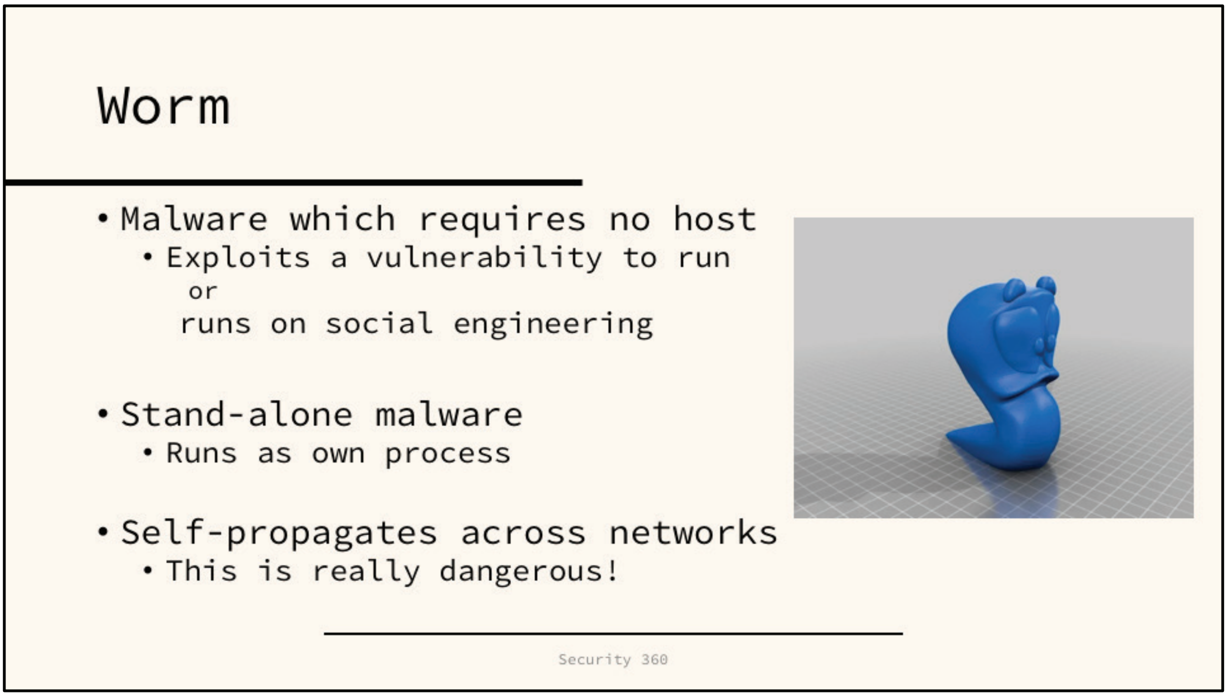


Virus

- Malware which relies on a “host”
  - Host application must be executed
- Attaches to an application
  - Runs alongside application, or replaces application
  - Can self-replicate to other applications
- Propagates across networks with user’s help

Security 360

"Influenza virus" by Sanofi Pasteur is licensed under CC BY-NC-ND 2.0

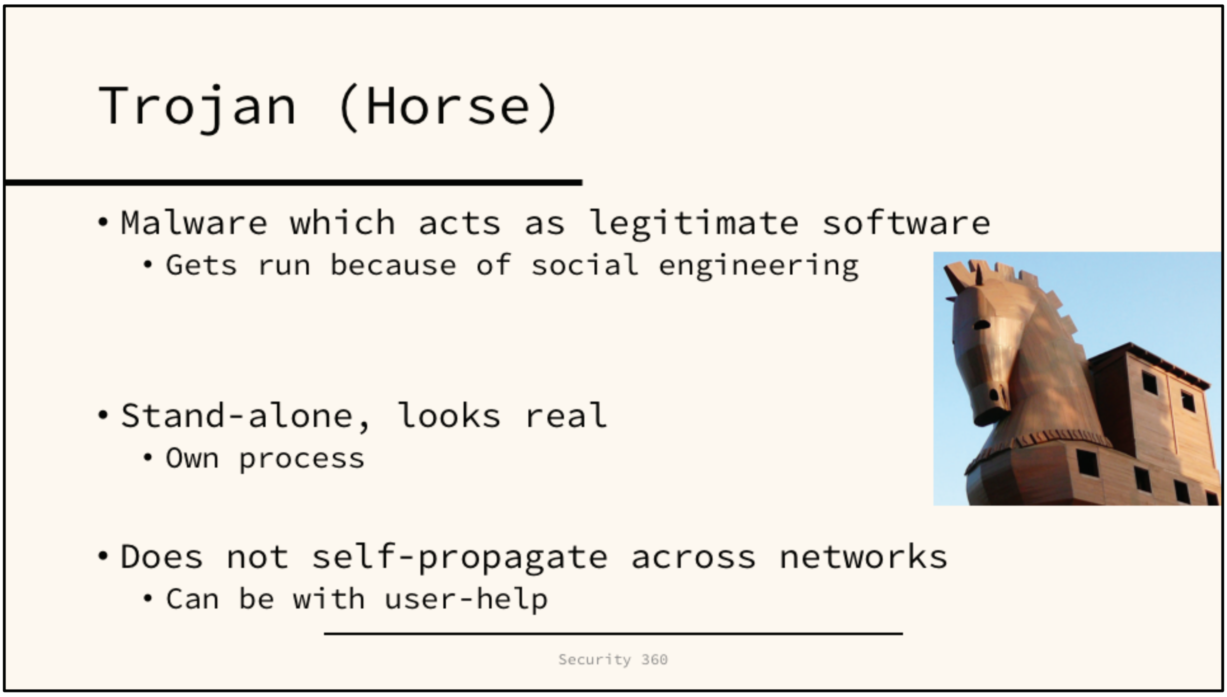


Worm

- Malware which requires no host
  - Exploits a vulnerability to run
    or
    runs on social engineering
- Stand-alone malware
  - Runs as own process
- Self-propagates across networks
  - This is really dangerous!

Security 360

"Worms Armaggedon" by andres motta is licensed under CC CC0 1.0

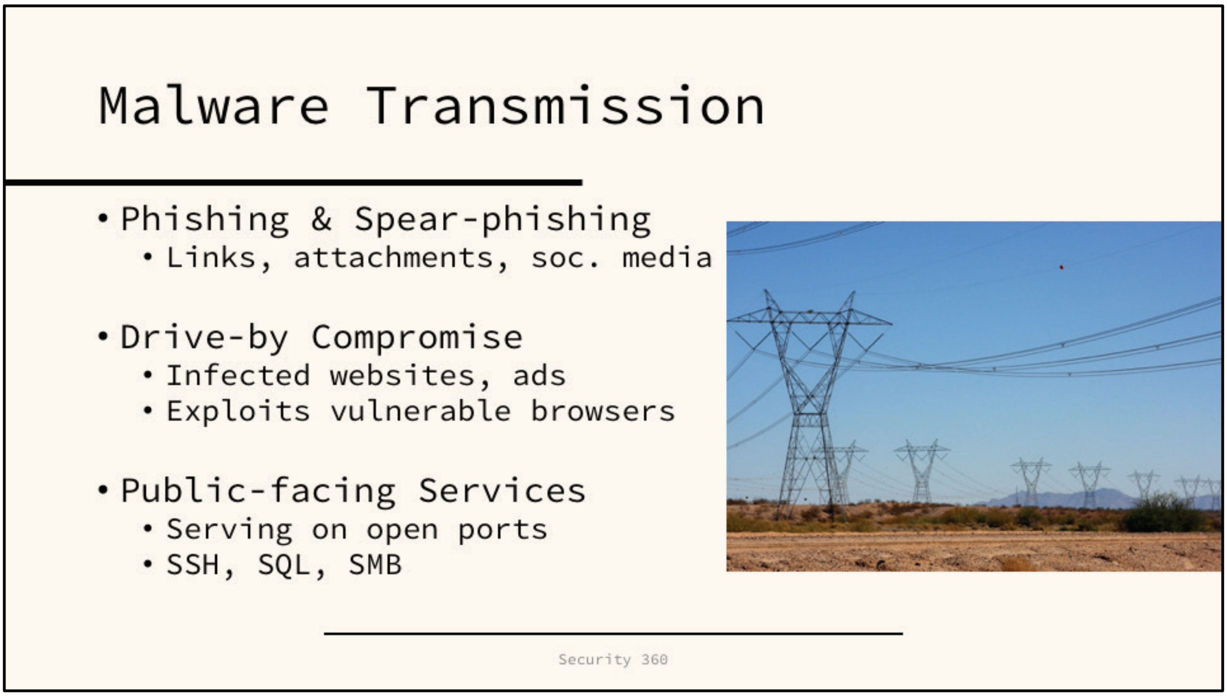


Trojan (Horse)

- Malware which acts as legitimate software
  - Gets run because of social engineering
- Stand-alone, looks real
  - Own process
- Does not self-propagate across networks
  - Can be with user-help

Security 360

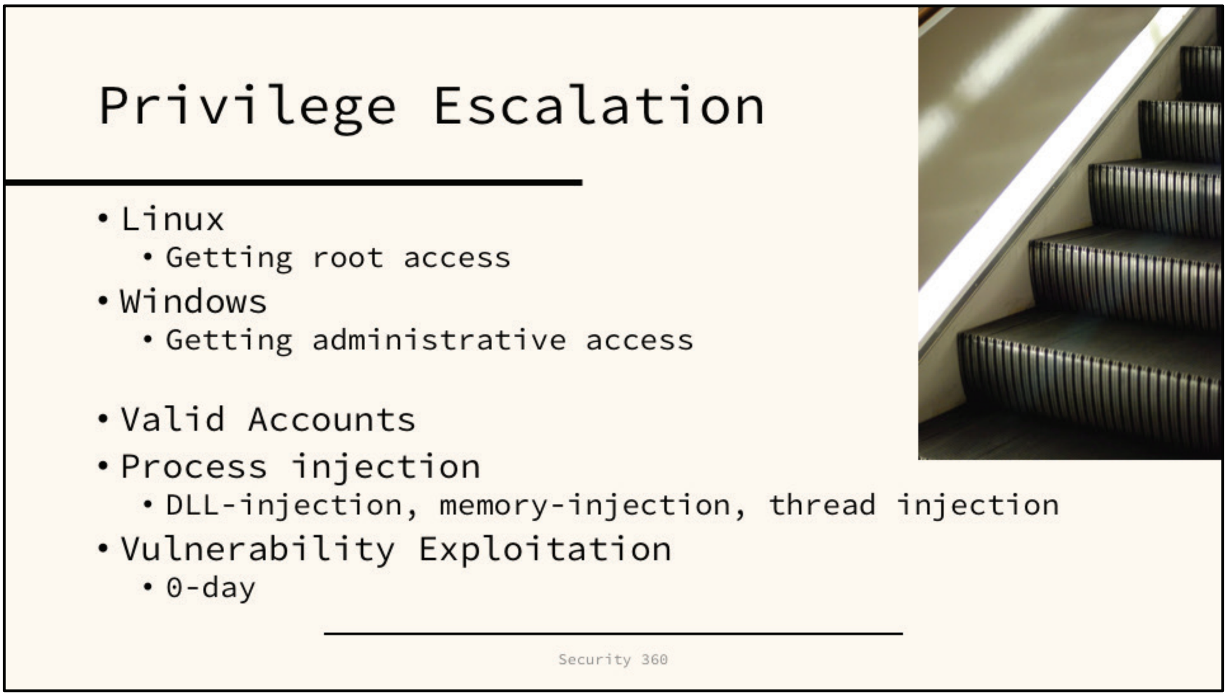
"P1010601a" by Marion Doss is licensed under CC BY-SA 2.0



Malware Transmission

- Phishing & Spear-phishing
  - Links, attachments, soc. media
- Drive-by Compromise
  - Infected websites, ads
  - Exploits vulnerable browsers
- Public-facing Services
  - Serving on open ports
  - SSH, SQL, SMB

"Tranmission" by kevin dooley is licensed under CC BY 2.0



Privilege Escalation

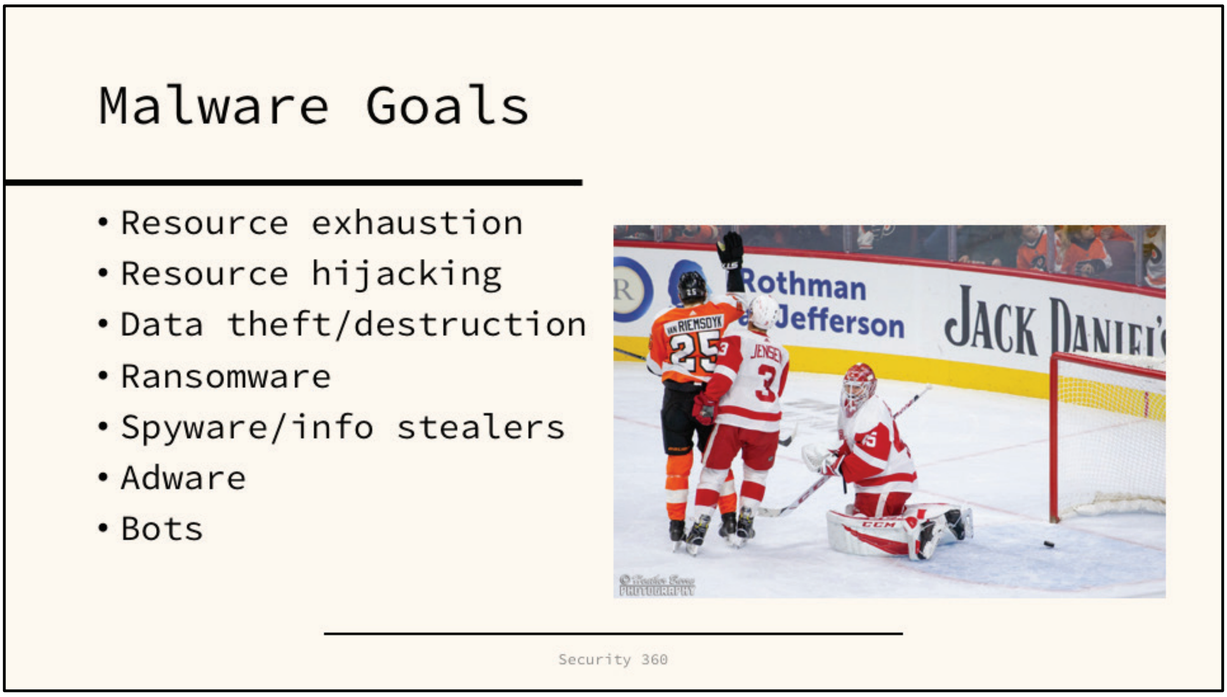
- Linux
  - Getting root access
- Windows
  - Getting administrative access

- Valid Accounts
- Process injection
  - DLL-injection, memory-injection, thread injection
- Vulnerability Exploitation
  - 0-day

"Escalator" by hyku is licensed under CC BY-SA 2.0

Remote Access, Backdoor, Rootkit

- Full access to victim machine
  - Remote Access Trojan (RAT)
- Often through a backdoor
  - Create a malicious entry route
  - Open ports, weak protocols
- Rootkit
  - Hidden / secret
  - Under the OS, run-on-boot
    - Firmware, drivers, kernel

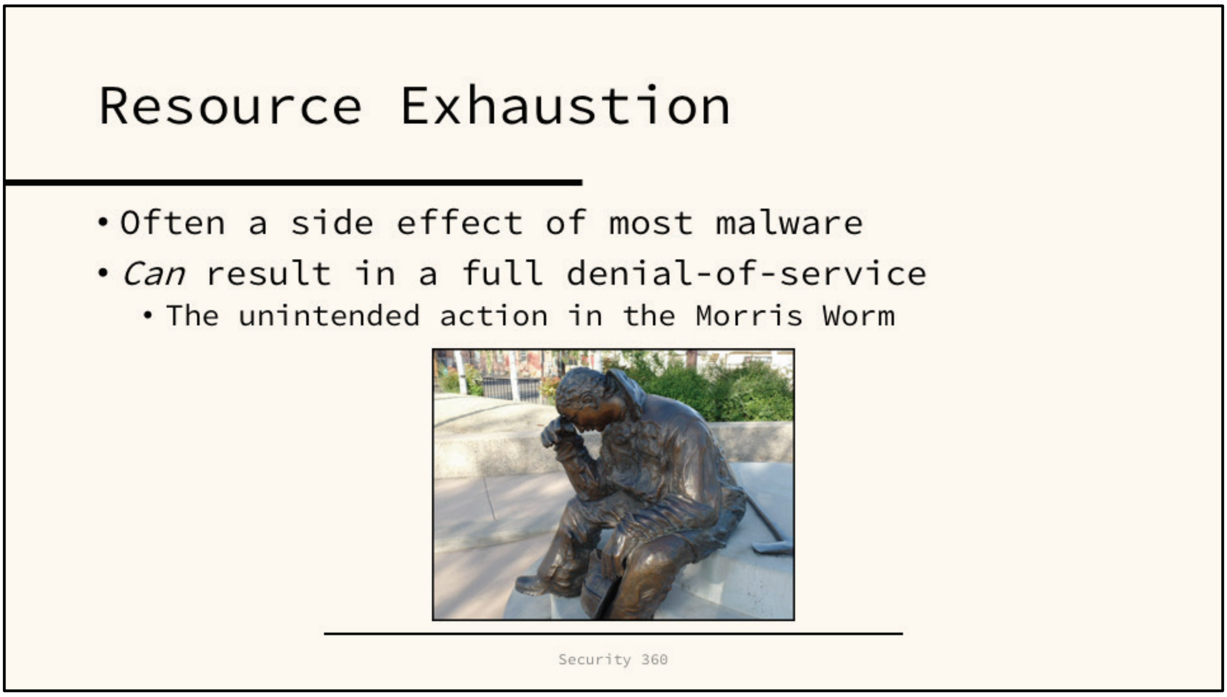


Malware Goals

- Resource exhaustion
- Resource hijacking
- Data theft/destruction
- Ransomware
- Spyware/info stealers
- Adware
- Bots

Rothman
Jefferson
JACK DANIEL'S
VAN RIEMSDYK
25
JENSEN
3

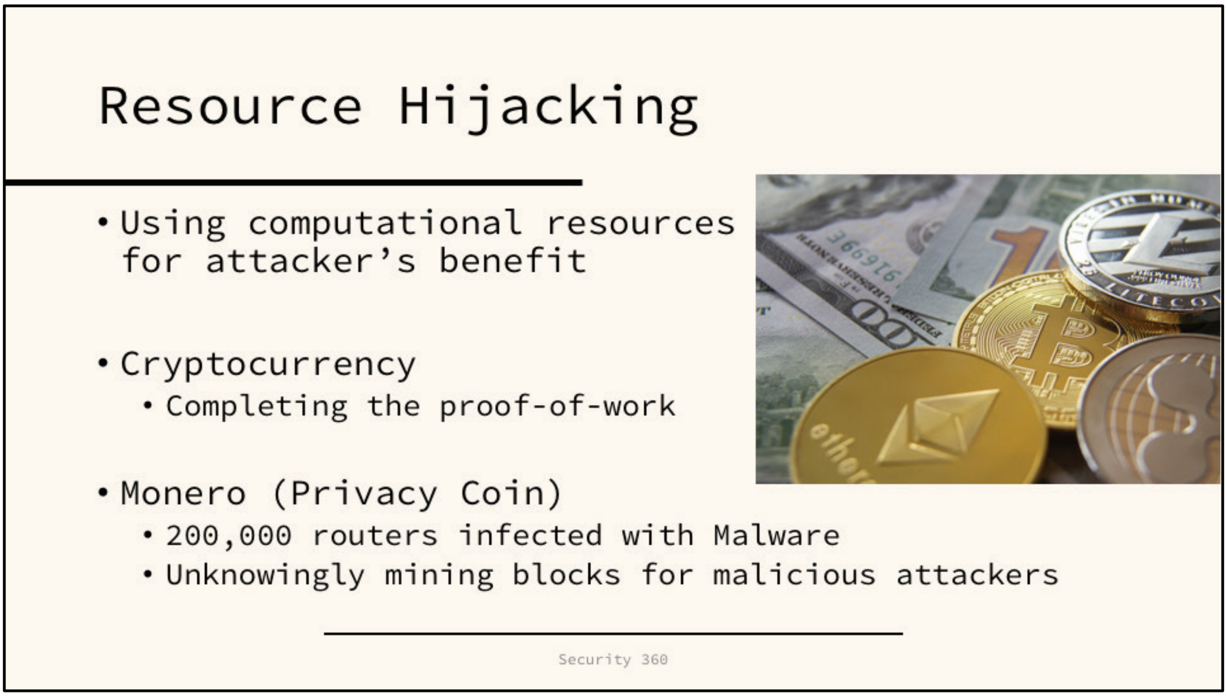
"PHI vs DET (Dec 18, 2018)" by Heather M Barry is licensed under CC BY-NC-ND 2.0



Resource Exhaustion

- Often a side effect of most malware
- *Can* result in a full denial-of-service
  - The unintended action in the Morris Worm

"ODCsleep97" by FolsomNatural is licensed under CC BY 2.0



Resource Hijacking

- Using computational resources for attacker’s benefit
- Cryptocurrency
  - Completing the proof-of-work
- Monero (Privacy Coin)
  - 200,000 routers infected with Malware
  - Unknowingly mining blocks for malicious attackers

Security 360

"Crypto coins on Benjamins" by QuoteInspector is licensed under CC BY-ND 2.0

Data Theft & Data Destruction

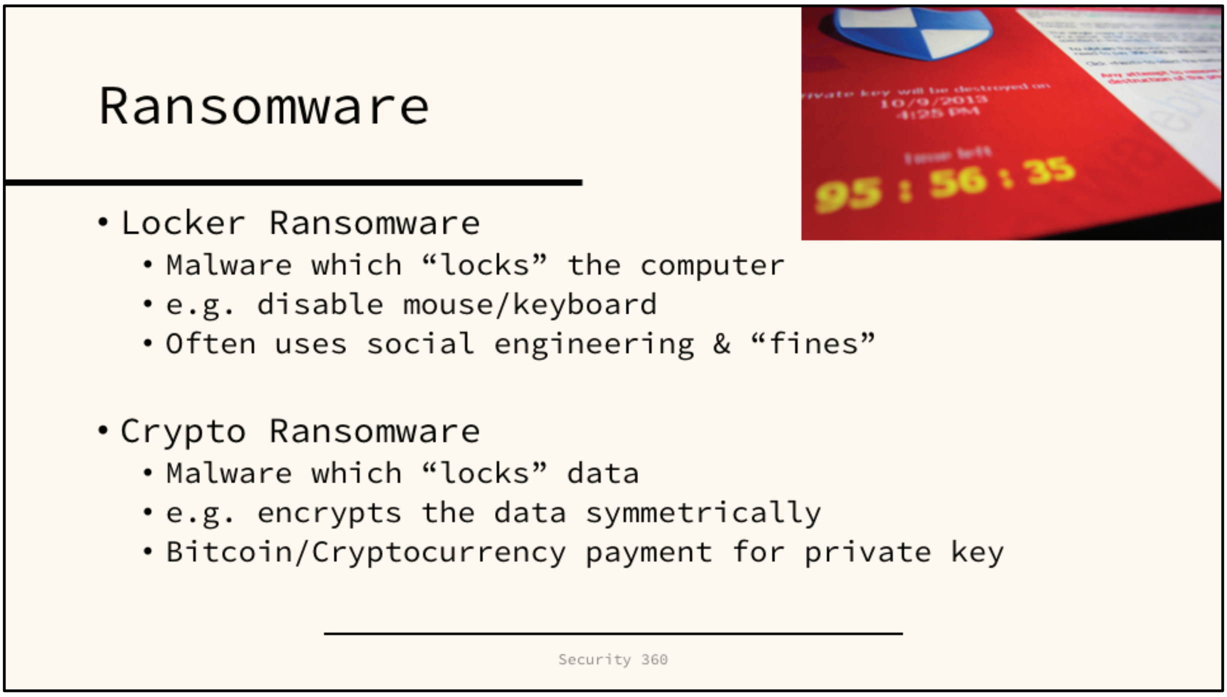
Stealing intellectual property (IP)

Stealing trade secrets

Destroying data

Security 360

"076: Spring Shredding" by william couch is licensed under CC BY-NC-ND 2.0



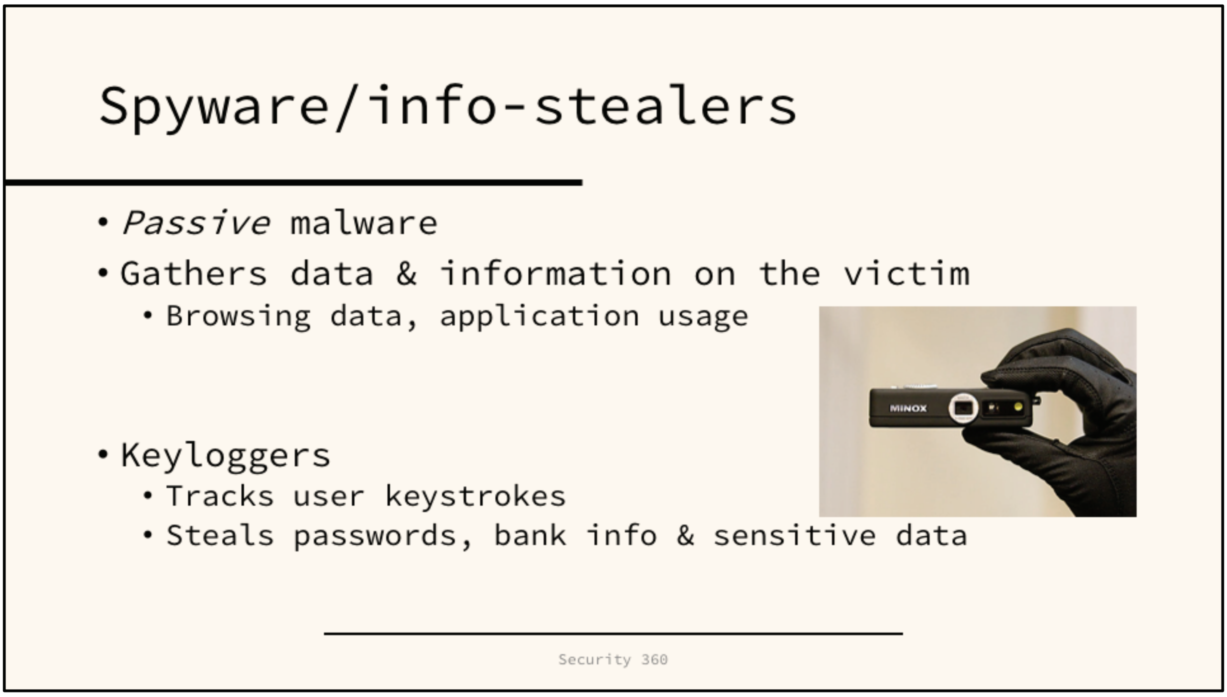
private key will be destroyed on
10/9/2013
4:25 PM
Time left
95 : 56 : 35

Ransomware

- Locker Ransomware
  - Malware which “locks” the computer
  - e.g. disable mouse/keyboard
  - Often uses social engineering & “fines”
- Crypto Ransomware
  - Malware which “locks” data
  - e.g. encrypts the data symmetrically
  - Bitcoin/Cryptocurrency payment for private key

Security 360

"Cryptolocker ransomware" by Christiaan Colen is licensed under CC BY-SA 2.0

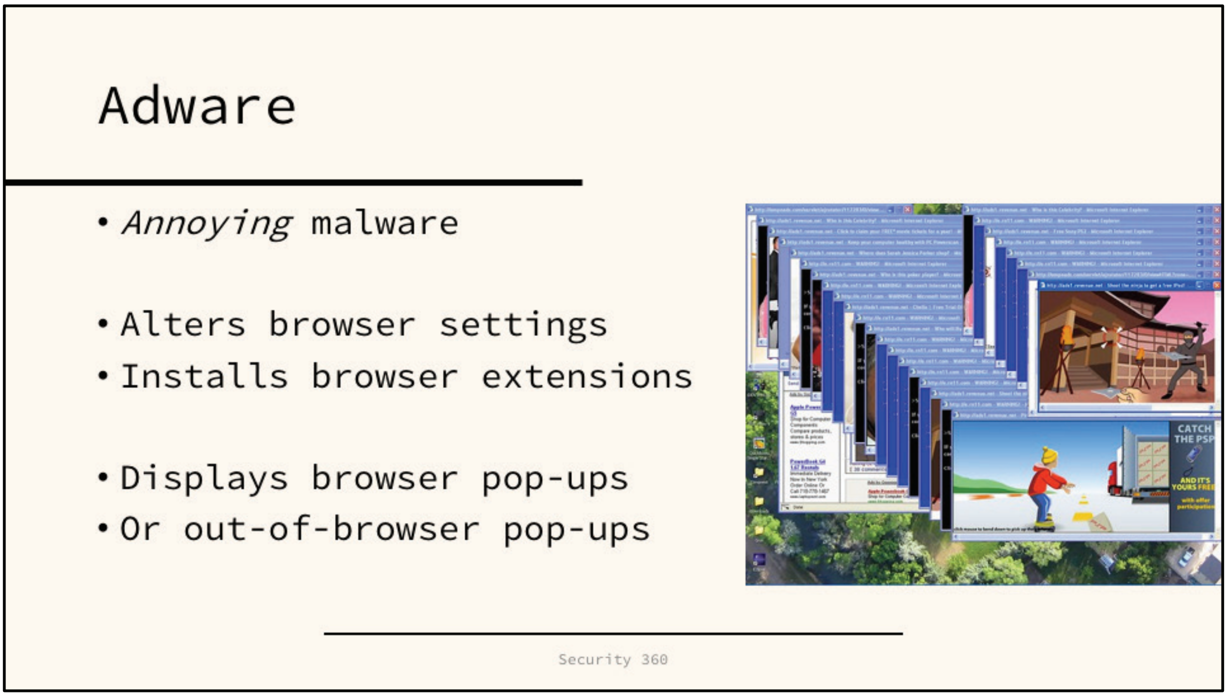


Spyware/info-stealers

- *Passive* malware
- Gathers data & information on the victim
  - Browsing data, application usage
- Keyloggers
  - Tracks user keystrokes
  - Steals passwords, bank info & sensitive data

Security 360

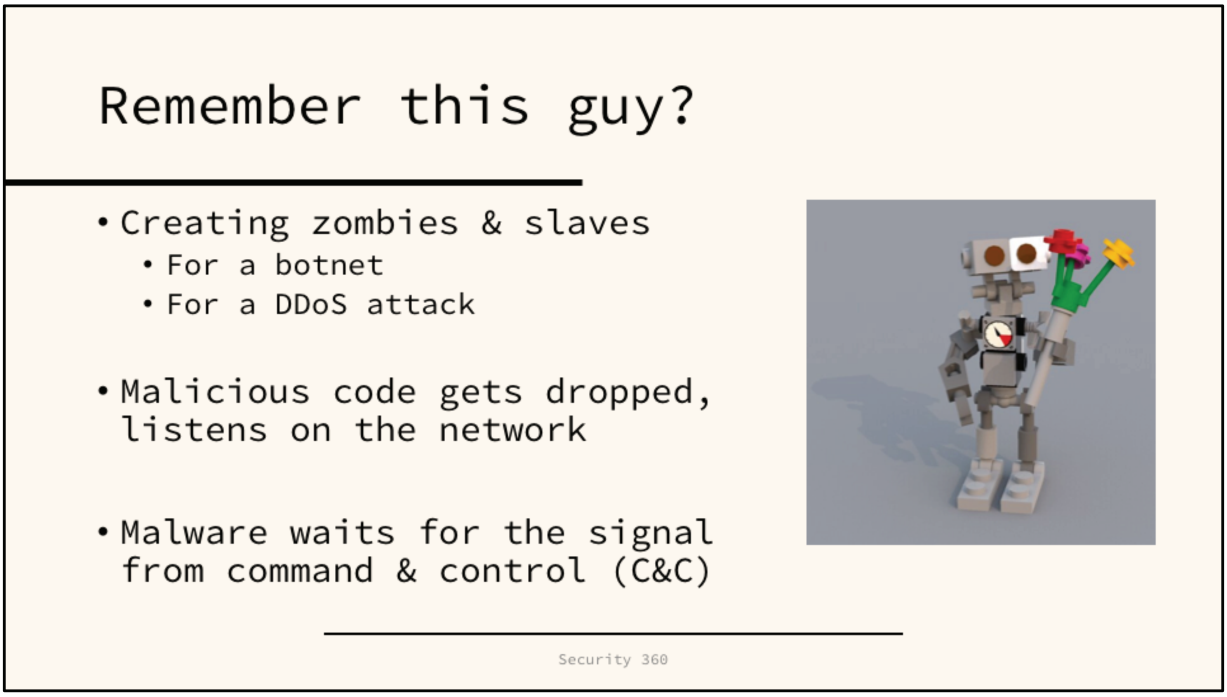
"minox-spy-cam" by kitleong is licensed under CC BY-NC-ND 2.0



Adware

- *Annoying* malware
- Alters browser settings
- Installs browser extensions
- Displays browser pop-ups
- Or out-of-browser pop-ups

Security 360

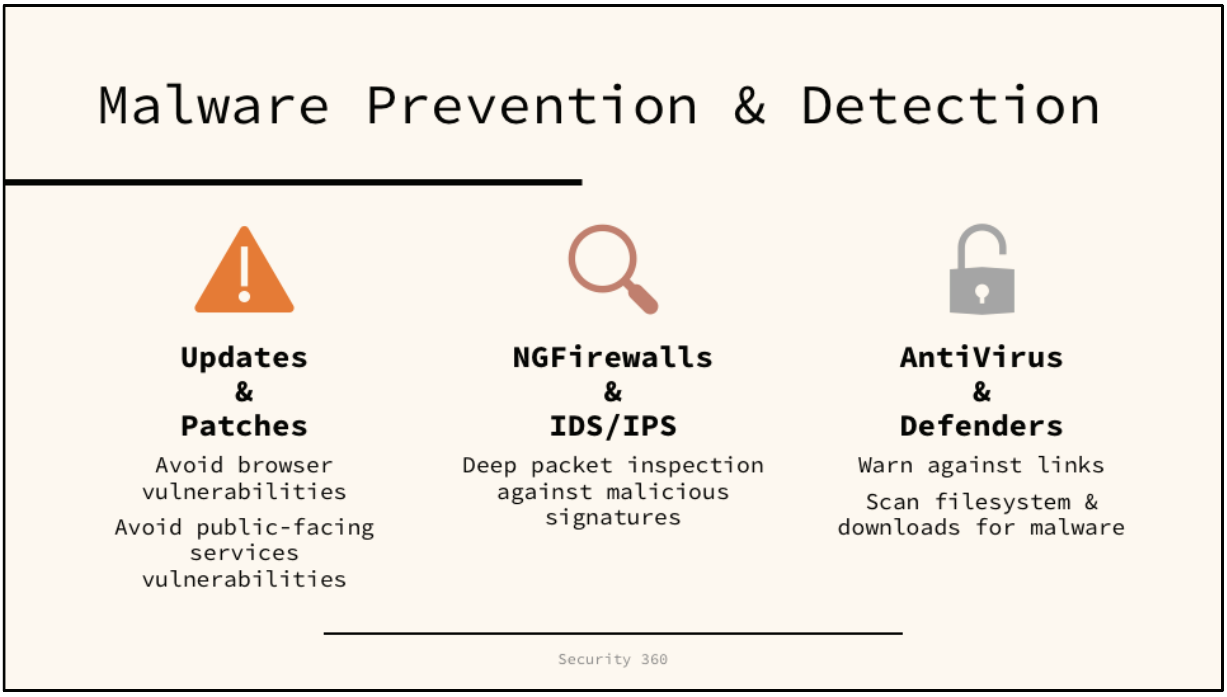


Remember this guy?

- Creating zombies & slaves
  - For a botnet
  - For a DDoS attack
- Malicious code gets dropped, listens on the network
- Malware waits for the signal from command & control (C&C)

Security 360

"A little 'bot of kindness is sometimes all that is needed." by Swijak is licensed under CC PDM 1.0



Malware Prevention & Detection

Updates
&
Patches

Avoid browser vulnerabilities

Avoid public-facing services vulnerabilities

NGFirewalls
&
IDS/IPS

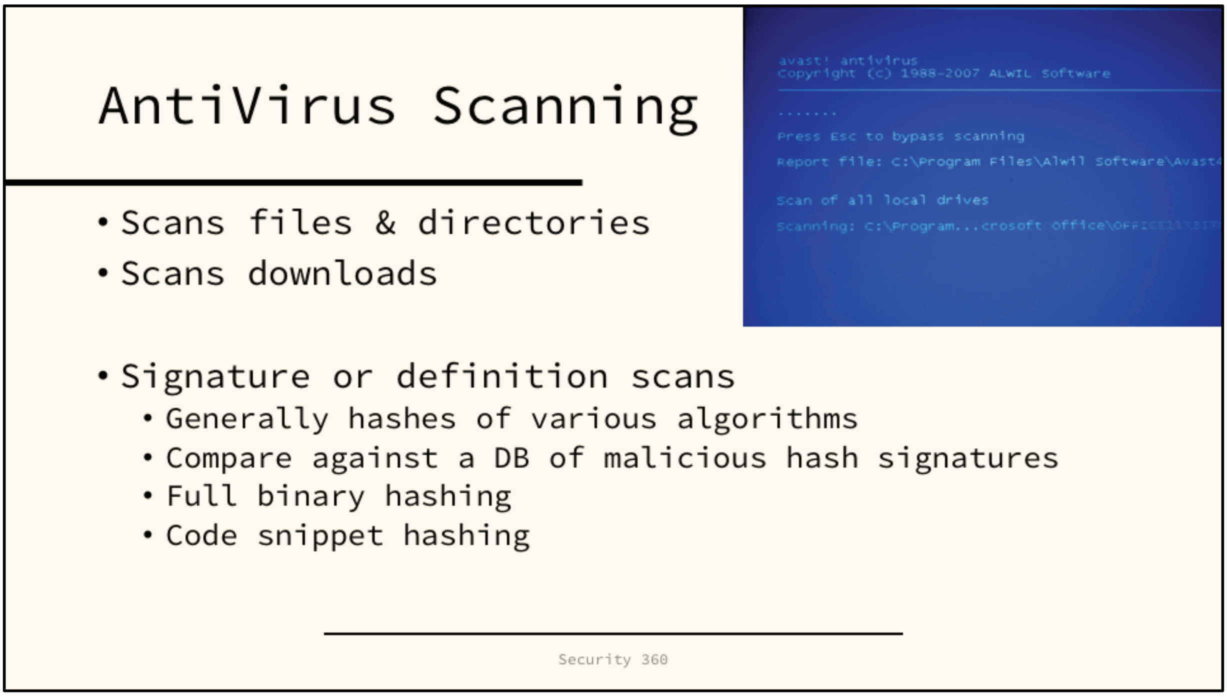
Deep packet inspection against malicious signatures

AntiVirus
&
Defenders

Warn against links

Scan filesystem & downloads for malware

Security 360



AntiVirus Scanning

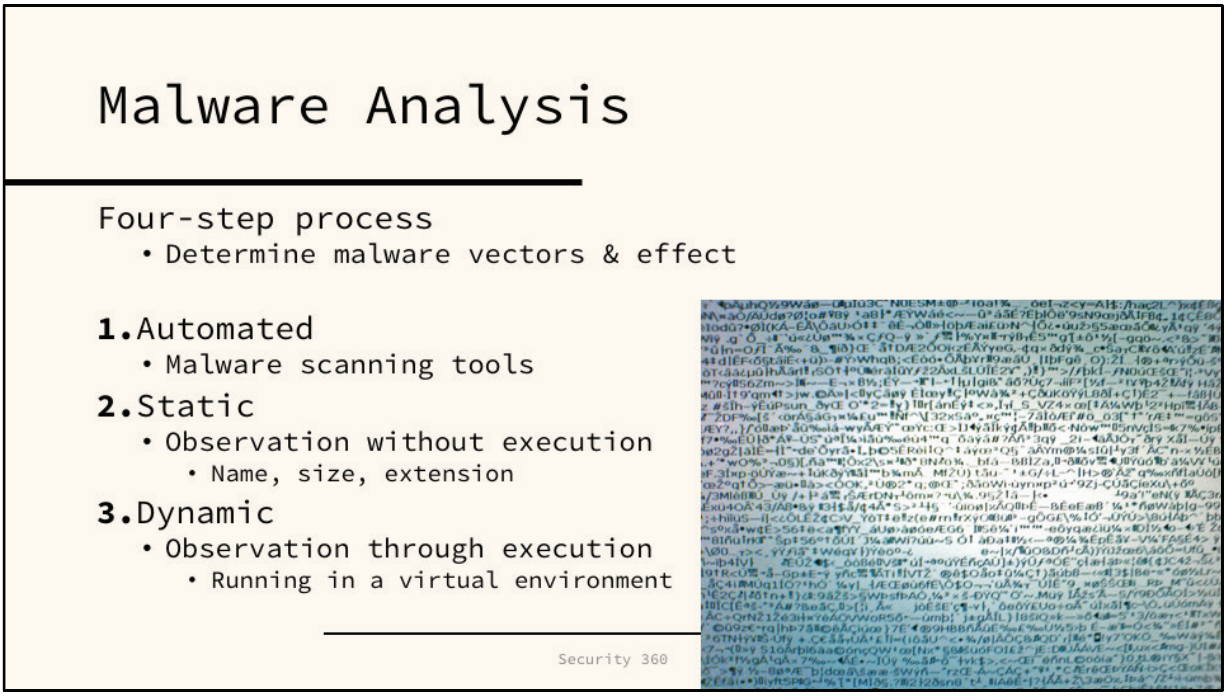
- Scans files & directories
- Scans downloads

```
avast! antivirus
Copyright (c) 1988-2007 ALWIL Software

.......
Press Esc to bypass scanning
Report file: C:\Program Files\Alwil Software\Avast4

Scan of all local drives
Scanning: C:\Program...crosoft Office\OFFICE11\BIT
```

- Signature or definition scans
  - Generally hashes of various algorithms
  - Compare against a DB of malicious hash signatures
  - Full binary hashing
  - Code snippet hashing

Security 360

"Scan for Virus" by trustmeiamnotageek is licensed under CC BY-NC-ND 2.0



Malware Analysis

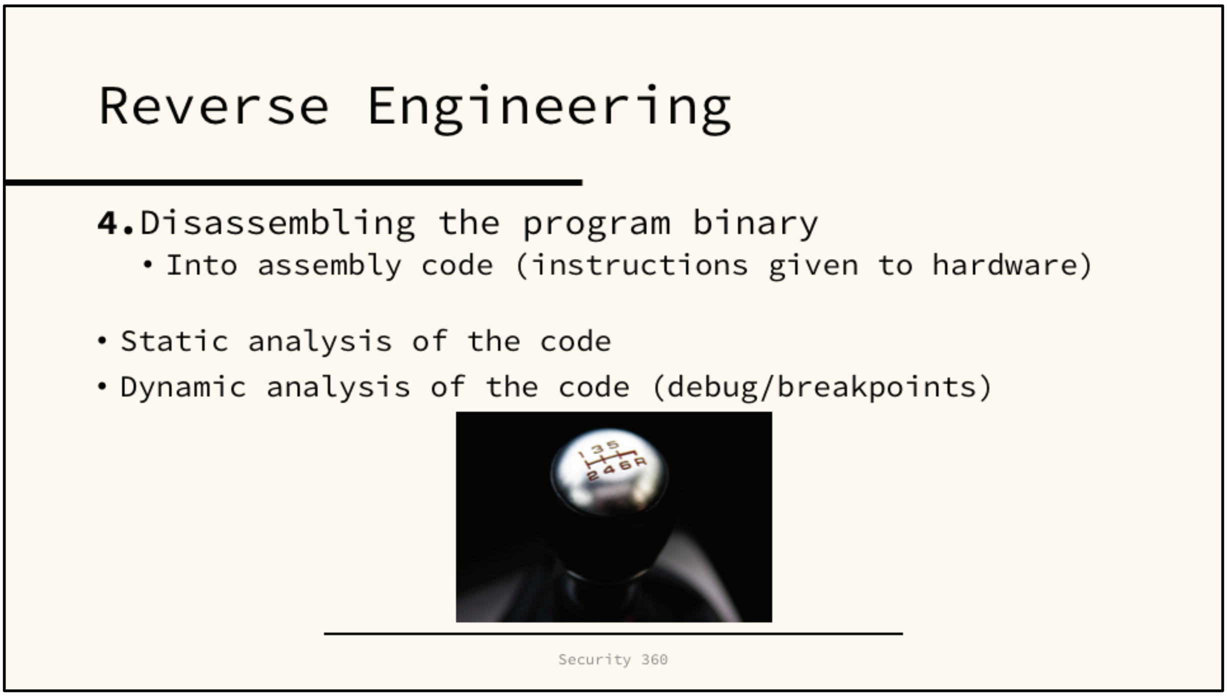
Four-step process

- Determine malware vectors & effect

1. Automated
   - Malware scanning tools
2. Static
   - Observation without execution
     - Name, size, extension
3. Dynamic
   - Observation through execution
     - Running in a virtual environment

Security 360

"Code Error" by DESQie is licensed under CC BY-NC-SA 2.0



Reverse Engineering

4. Disassembling the program binary
   - Into assembly code (instructions given to hardware)

- Static analysis of the code
- Dynamic analysis of the code (debug/breakpoints)

Security 360

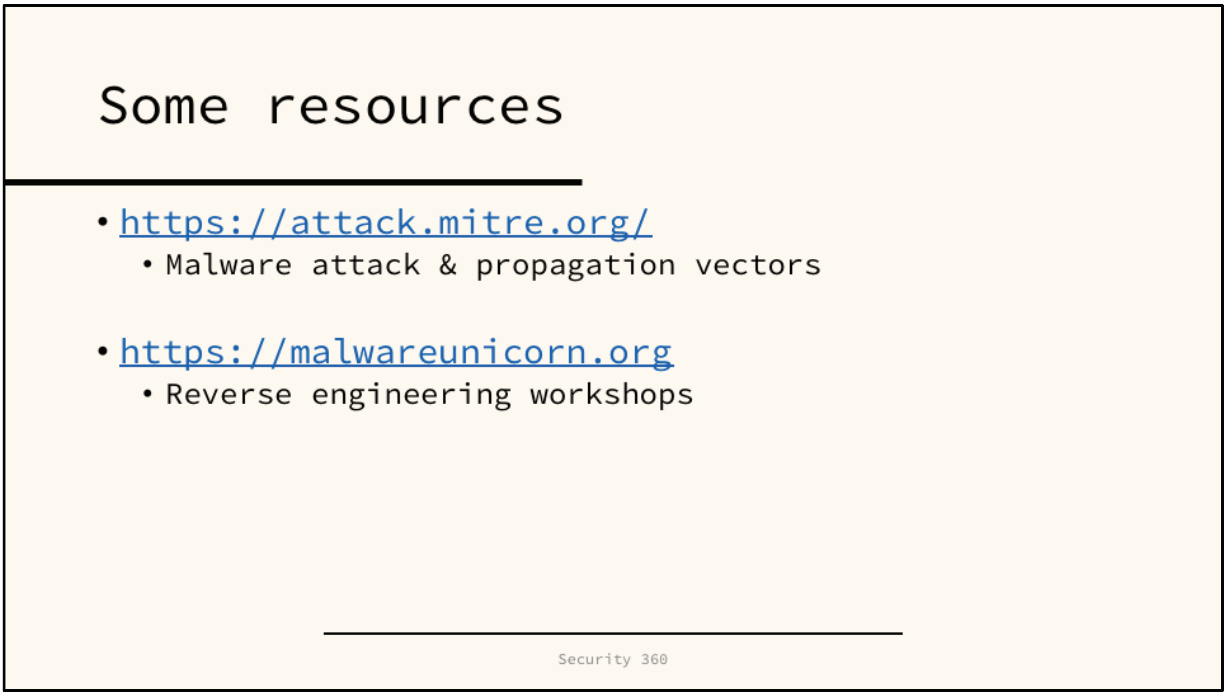
"Six Speed" by corey.wagehoft is licensed under CC BY-NC-ND 2.0

Incident Response

- Stay calm, we’ll talk about it Friday

Security 360

"364/365:Red Alert" by practicalowl is licensed under CC BY-NC 2.0



Some resources

- https://attack.mitre.org/
  - Malware attack & propagation vectors
- https://malwareunicorn.org
  - Reverse engineering workshops