COS80013 Internet Security

Week 4

Presented by Dr Rory Coulter

24 March 2025

SWINBURNE UNIVERSITY OF TECHNOLOGY

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Week 3 Recap

Key topics and theories

Recap

Operating systems: *A collection of software that manages computer hardware resources and provides common services for computer programs*

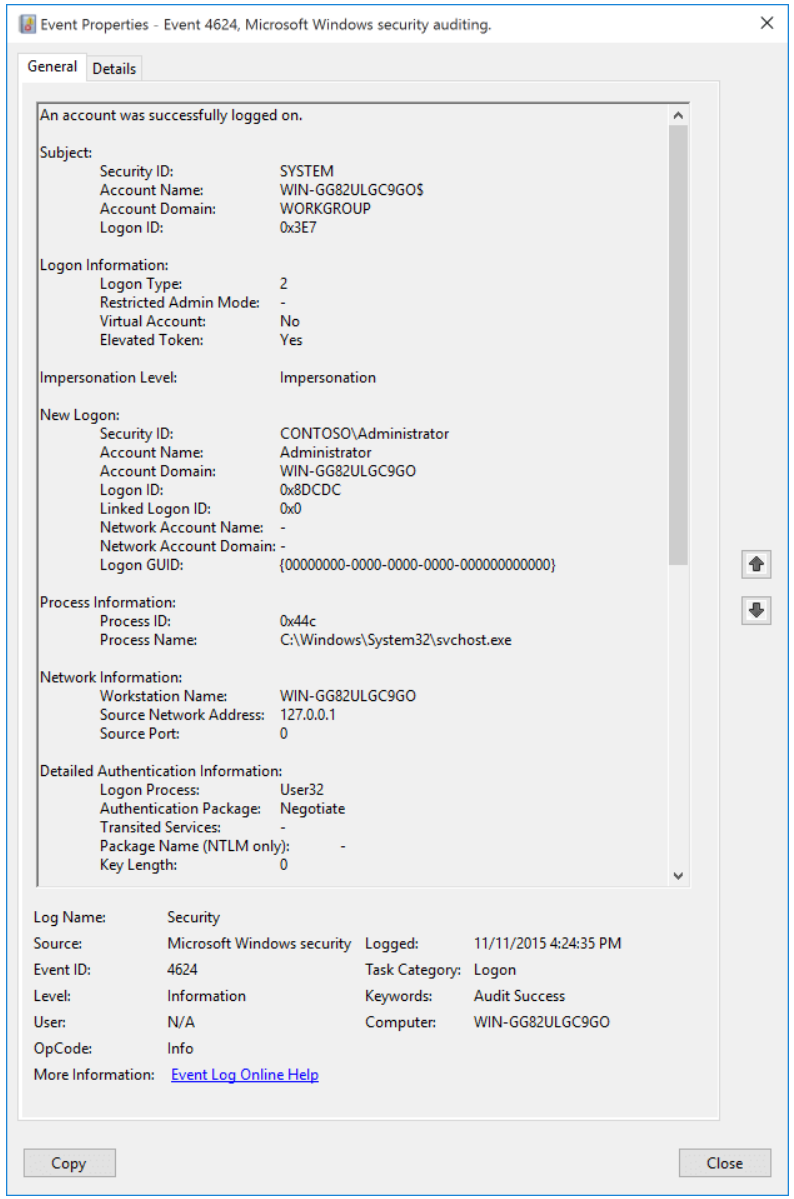
Signature and behaviour or anomaly-based detection

Controls are not one dimension, rather many layers

Access controls, policy, attack surface reduction, etc.

Systems should be hardened, usability vs security

Logging is valuable aspect of security



Terms

Let's set some common language

Across both topics today, and from a cyber security perspective

- Malware: Malicious Software
- Goodware, benign software: Safe, normal program
- Vulnerability: A flaw within an organisation per its controls or system procedures, implementation, software or hardware which could be exploited
- Exploit: Software or code (mostly) that takes advantage of a vulnerability to gain unauthorised access, disclosure, privilege or perform malicious actions on a system (see compromise)
- Implant: Code which is often injected or inserted into a system to maintain command and control (C2), or perform malicious actions after compromise
- Compromise: unauthorised disclosure, modification, substitution or use of sensitive data, unauthorised access or modification to systems, devices or processes
- Payload: Malicious action or function of malware
- Sandbox
  - Usually an application we can run malware in to analyse it

Malware

History

What a time to be a live

History in the making

- 1980s and Onward:
  - Virus concept from 1949 lecture by John von Neumann (“self-reproducing automata”)
  - Modern viruses start with Elk Cloner (1982) on Apple II
  - Harmless, but spread to all attached disks—first major outbreak
- 1990s:
  - Windows OS popularity increases
  - More viruses written for Windows platform
  - Macro viruses in Microsoft Word
- 2002-2007:
  - IM worms on AOL AIM, MSN, Yahoo Messenger
  - Social engineering lures—malicious IMs
  - IM worm spreads through contact lists
- 2005-2009:
  - Adware growth—unwanted ads on screens
  - Exploited legit software, led to lawsuits
  - Tech support scams have origins here
- 2007-2009:
- Malware targets Myspace, then Facebook, Twitter
- 2013:
  - Ransomware "CryptoLocker" targets Windows
  - Forced victims to pay $3M, spawned imitators
- 2013-2017:
  - Ransomware thrives via Trojans, malvertising
  - 2017 sees massive outbreaks impacting businesses
- 2017:
  - Cryptojacking emerges—secretly mining cryptocurrency on others' devices
- 2018-2019:
  - Ransomware resurgence, shifting to businesses
  - GandCrab, Ryuk ransomware spike in attacks
  - 365% increase in business attacks from 2018-2019

*what would we define good guys using malware, is it still malware?

https://www.malwarebytes.com/malware

SWINBURNE UNIVERSITY OF TECHNOLOGY

Malware (cont.)

Often developed and used by cyber actors*

Malware

- Trojans and Backdoors:
  - Trojans appear useful, perform malicious actions when run
  - May steal info, download more malware, provide hacker access
- Ransomware:
  - Locks computer/files, demands payment for access
  - Extortion by malware, difficult to defend against
- Keyloggers:
  - Logs keystrokes, sends data to scammers
  - Captures passwords, bank info, credit card numbers
- Viruses and Worms:
  - Viruses infect files, run with file use
  - Worms spread between computers independently
  - Both can steal, download, delete, or spam
- Adware and Spyware:
  - Adware displays unwanted ads in browsers
  - Spyware secretly observes user activities
- Rootkit:
  - Provides attacker with admin privileges (root access)
  - Stays hidden from users, OS, and software
- Exploits and Zero-Day Exploits:
  - Exploits use system bugs to grant access
  - Zero-day exploits are unpatched vulnerabilities
- Malicious Cryptomining (Cryptojacking):
  - Trojans install, mine cryptocurrency using your resources
  - Attacker gains coins, not you—resource theft
- Webshell
  - Software used on compromised web servers

SWINBURNE UNIVERSITY OF TECHNOLOGY

Malware (cont.)

Often developed and used by cyber actors*

Comparisons

- Viruses and Worms:
- Both self-replicate, viruses attach to files
- Worms spread across systems independently

- Trojans and Ransomware:
- Trojans pretend to be useful, give hacker access
- Ransomware locks files, demands payment

- Keyloggers and Spyware:
- Keyloggers record keystrokes, send to scammers
- Spyware covertly observes user actions

*what would we define good guys using malware, is it still malware?

Malware Delivery Vectors

How does malware even get onto our systems?

Not an exhaustive list:

- Phishing Emails
- Spear Phishing
- Malvertising
- Drive-By Downloads
- Watering Hole Attacks
- Infected USB Drives
- Social Engineering
- Ransomware Payloads
- Exploit Kits
- Remote Desktop Protocol (RDP) Attacks
- Brute Force Attacks
- Social Media Attacks
- Instant Messaging and Chat
- Fake Software Updates
- Trojanised Applications
- Drive-by App Downloads
- Email Attachments
- Peer-to-Peer Networks
- Physical Media
- Wi-Fi Networks

Preventative Measures

Being cyber safe

Some thoughts

- Preventive Measures:
  - Use antivirus software with daily updates
  - Keep all software updated
  - Employ strong passwords/passphrases
  - Backup files daily
  - Disable unused Microsoft Office macros
  - Regularly review and uninstall unused software

- Secure Application Installation:
  - Malware distributed via spam emails, malicious websites, and fake applications
  - Use reputable app stores for downloads
  - Avoid third-party download sites
  - Don't click on online ads for downloads, use ad-blockers
  - Avoid peer-to-peer network downloads
  - Be cautious with email/instant message links or attachments
  - Scan applications before installing, especially from email/USB

SWINBURNE UNIVERSITY OF TECHNOLOGY

Malware Analysis

Three main types

Automated, Static, Dynamic

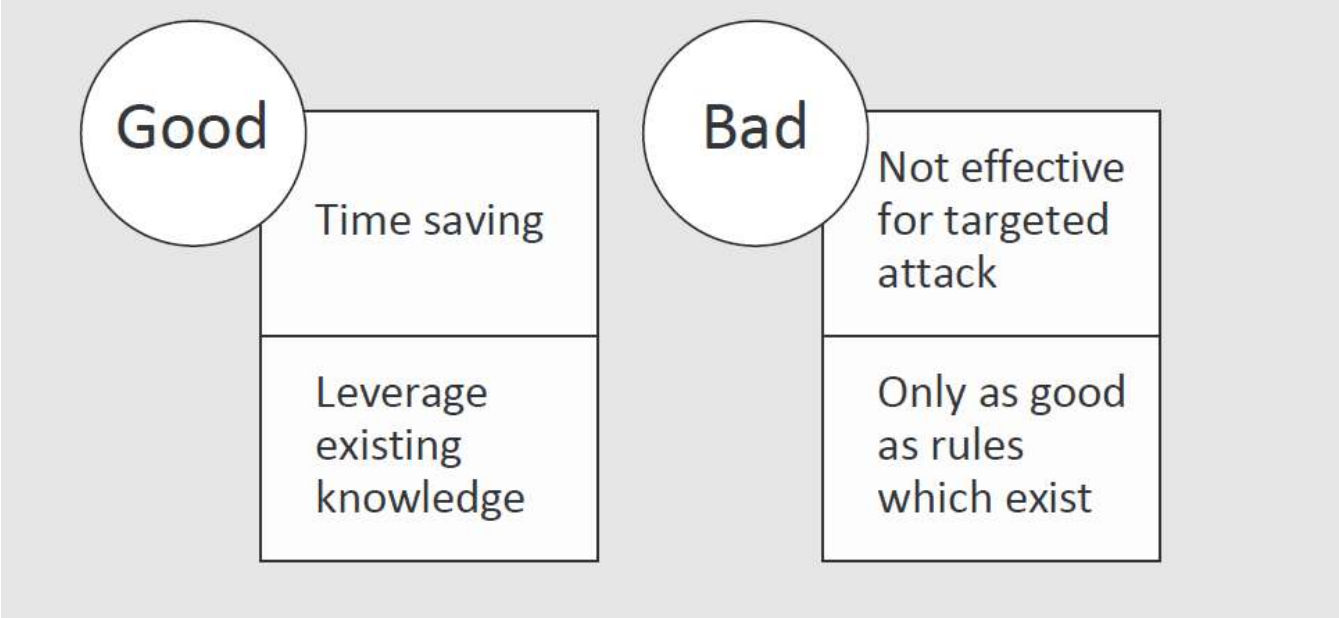
- Automated
  - Use tools to analyse it
- Static
  - Dump the contents and investigate
- Dynamic
  - Run it, and investigate

*what would we define good guys using malware, is it still malware?

Automated Analysis

Use of software tools and algorithms to <u>automatically</u> examine and analyse malicious software

Initial information source



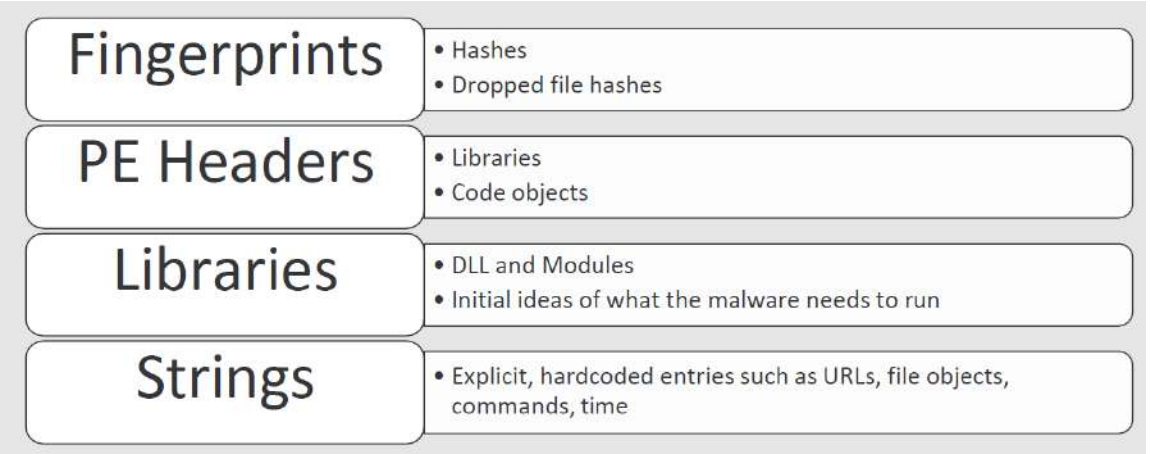
Static Analysis

A technique used to analyse and understand the behaviour and functionality of malicious software, without actually executing it.

Two steps

- Malware sample is first disassembled or decompiled into its component parts, allowing analysts to examine its code structure and functions.
- Analysts then examine the code for known patterns of malicious behavior, such as calls to system APIs, use of encryption or obfuscation techniques, and the presence of known exploit payloads.

Tools include IDA Pro, OllyDbg, and Ghidra



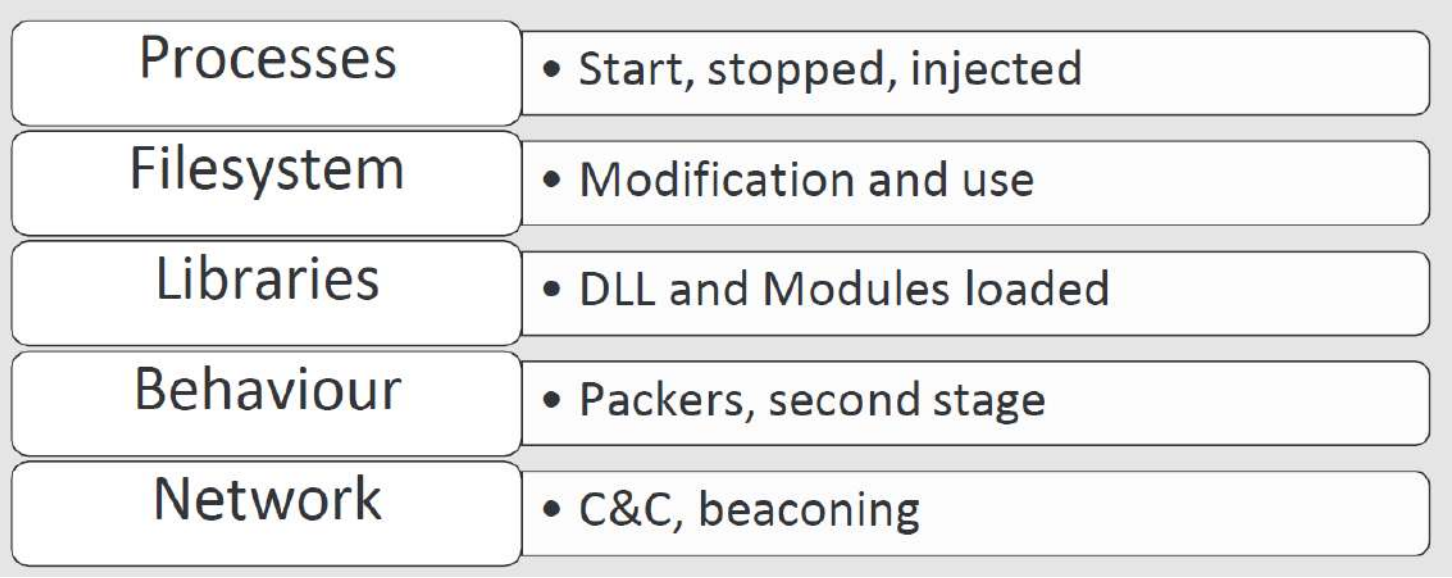
Dynamic Analysis

Analyse and understand the behaviour and functionality of malicious software by executing it in a controlled environment.

Running the malware sample in a sandboxed environment, a virtual machine, container or specialised tools

Used to identify previously unknown malware variants

Cuckoo, Cape v2, Joes Sandbox



SWINBURNE UNIVERSITY OF TECHNOLOGY

Vulnerabilities

Understanding Vulnerabilities

The good and the bad

Vulnerabilities

- Vulnerabilities are weaknesses in software or systems that can be exploited by attackers
- They can lead to unauthorised access, data breaches, or system crashes
- Vulnerabilities can be caused by coding errors, design flaws, or configuration issues
- CVEs (Common Vulnerabilities and Exposures) are standardised identifiers for known vulnerabilities
- Vulnerability databases like CVE Details and NVD list and provide information about CVEs
- Vulnerability scanning tools help identify weaknesses in systems and software
- Patches are updates released by software vendors to fix vulnerabilities
- Organisations should regularly update software and systems to protect against known vulnerabilities
- Zero-day vulnerabilities are exploited by attackers before vendors release patches
- Threat actors actively exploit unpatched vulnerabilities, making timely updates crucial

CVEs

What, types and how does something become a known vulnerability

The flow

- CVEs are standardised identifiers for publicly known cybersecurity vulnerabilities
- Assigned to vulnerabilities by the MITRE Corporation to aid in tracking and information sharing
- Importance of CVEs
  - CVEs provide a common language for discussing vulnerabilities across the industry
  - They help security professionals and vendors understand the nature and severity of vulnerabilities
- Types of CVEs
  - Buffer Overflow: Occurs when a program writes more data into a buffer than it can hold, potentially allowing attackers to execute malicious code
  - SQL Injection: Attackers inject malicious SQL queries into input fields to manipulate databases
  - Cross-Site Scripting (XSS): Malicious scripts are injected into web pages viewed by others, compromising user data
  - Denial of Service (DoS): Attackers flood a system to overload it, causing it to crash or become unresponsive
  - Privilege Escalation: Attackers exploit vulnerabilities to gain unauthorised access to higher levels of system privileges
  - Remote Code Execution (RCE): Allows attackers to execute code remotely, taking control of systems
  - Authentication Bypass: Exploits that let attackers circumvent authentication measures
  - Information Disclosure: Vulnerabilities that expose sensitive data
  - Man-in-the-Middle (MitM): Attackers intercept and manipulate communications between parties
  - Zero-Day: Exploited vulnerabilities before they are publicly known, leaving no time for mitigation
- Lifecycle of a CVE
  - Discovery: Researchers or attackers identify a vulnerability
  - Report: Vulnerability details are reported to the affected vendor or project
  - Mitigation: Vendor develops and releases patches or updates to fix the vulnerability
  - CVE Assignment: MITRE assigns a CVE identifier
  - Public Disclosure: Vulnerability details are published, helping users take action

SWINBURNE UNIVERSITY OF TECHNOLOGY

Zero Day

A special type of Vulnerability

Characteristics

- A zero-day vulnerability is a security flaw in software or systems that is exploited by attackers before the vendor becomes aware of it
- The term "zero-day" refers to the fact that developers have zero days to address and fix the vulnerability before it's exploited
- These vulnerabilities are highly valuable to attackers, as they can target users who are unaware of the issue
- Zero-day exploits can lead to unauthorised access, data breaches, and other malicious activities
- Attackers can sell zero-day exploits on the black market or use them for targeted attacks
- The discovery of zero-days may occur through independent research or by malicious actors
- Mitigation involves using intrusion detection systems, regularly updating software, and employing strong security practices
- Software vendors release patches as soon as the vulnerability is identified to minimise the window of opportunity for attacks

SWINBURNE UNIVERSITY OF TECHNOLOGY

Vulnerability

Weaknesses or flaws in a computer system, network, application, or device

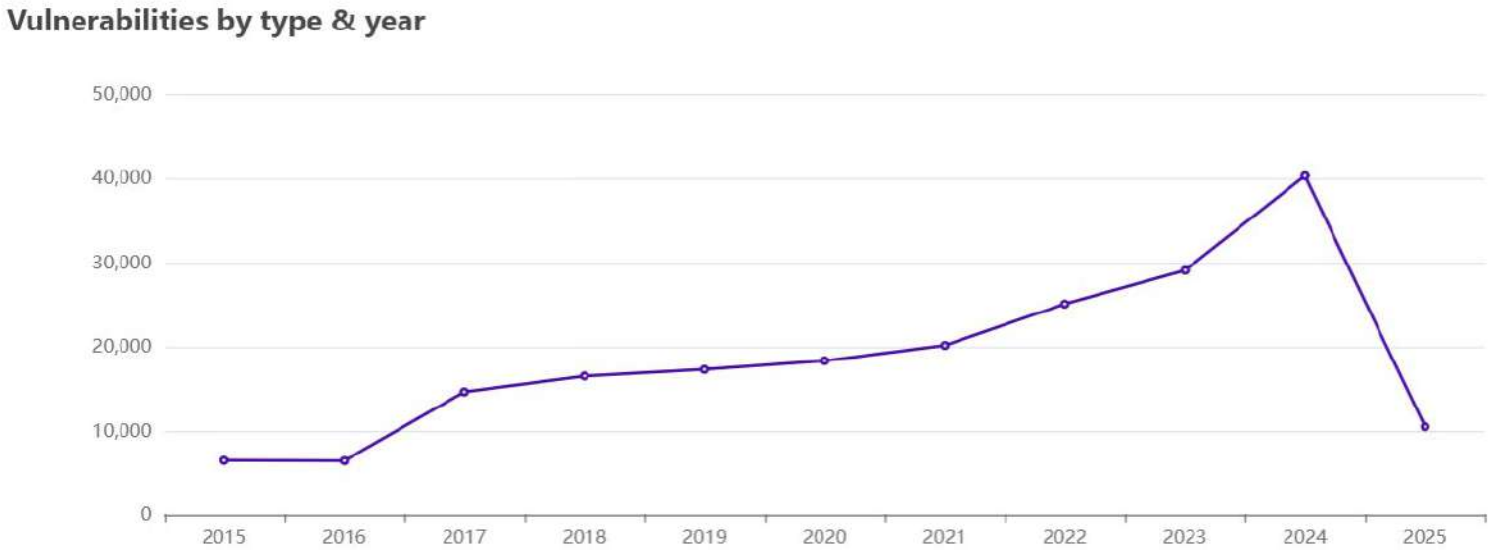
Exploited by attackers to gain unauthorised access, steal sensitive information

Threat

- Vulnerability is exploited
- malware, phishing attacks, social engineering

Risks

- The likelihood and impact of harm or damage caused by a threat
- Risks management : risk assessment, risk mitigation, risk avoidance of vulnerabilities
- Financial losses, reputational damage, loss of confidential information



SOURCE: https://www.cvedetails.com/browse-by-date.php

Vulnerability Types

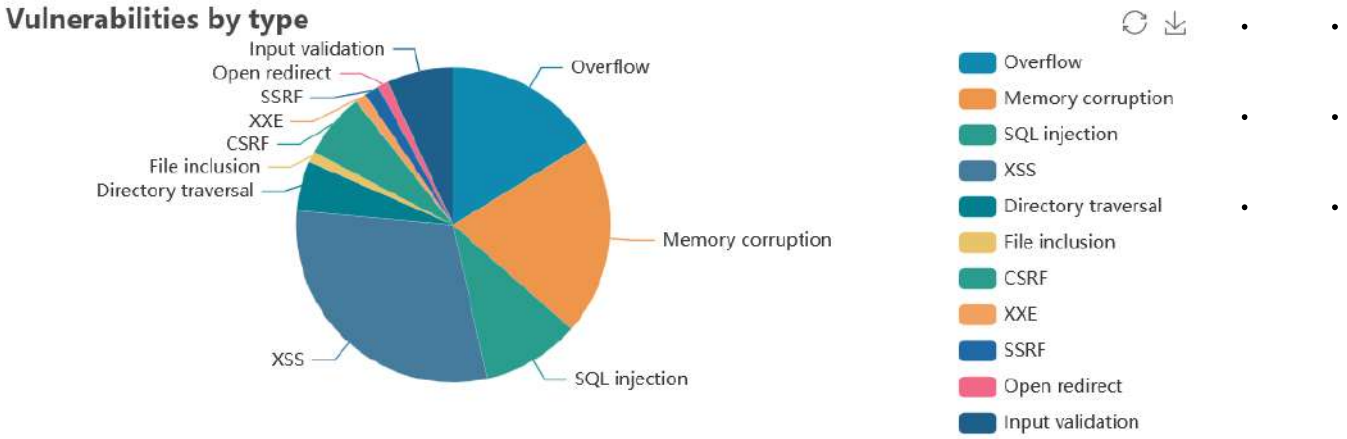
Vulnerabilities can exist in any type of software

Types

- Code Execution
- Bypass
- Privilege Escalation
- Denial of Service
- Information Leak

Categories

- Overflow
- Memory
- Corruption
- Sql Injection
- XSS
- Directory Traversal
- File Inclusion
- CSRF
- XXE
- SSRF
- Open Redirect
- Input Validation



SOURCE: https://www.cvedetails.com/browse-by-date.php

Vulnerability Categories

- Overflow: Occurs when a program writes more data to a buffer than it can hold, potentially allowing attackers to execute malicious code
- Memory Corruption: Happens when a program's memory content is unintentionally modified, leading to unpredictable behavior or exploitation
- SQL Injection: Allows attackers to manipulate a database by injecting malicious SQL queries via user input fields
- XSS (Cross-Site Scripting): Involves injecting malicious scripts into webpages, which are then executed in users' browsers
- Directory Traversal: Exploits vulnerabilities to access unauthorised files and directories on a server
- File Inclusion: Enables attackers to include external files into a web application, often leading to code execution
- CSRF (Cross-Site Request Forgery): Tricks users into performing unintended actions on a website without their consent
- XXE (XML External Entity Injection): Exploits XML parsers by injecting malicious external entities, potentially compromising sensitive data
- SSRF (Server-Side Request Forgery): Forces a server to make unauthorised requests to other servers or services
- Open Redirect: Redirects users to unintended, potentially malicious URLs by exploiting insecure redirects
- Input Validation: Refers to the lack of proper validation for user inputs, which can lead to vulnerabilities like injections or overflows

CVSS Score

A framework to assign a severity score to software vulnerabilities based on the potential impact and likelihood of exploitation

To help prioritise vulnerability remediation efforts, with higher-scored vulnerabilities typically given higher priority for mitigation

CVSS v2.0 Ratings	
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings	
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVE-2022-45608	An issue was discovered in ThingsBoard 3.4.1, allows low privileged attackers (CUSTOMER_USER) to gain escalated privileges (vertically) and become an Administrator (TENANT_ADMIN) or (SYS_ADMIN) on the web application. It is important to note that in order to accomplish this, the attacker must know the corresponding API's parameter (authority : value). **Published:** 三月 01, 2023; 11:15:09 上午 -0500	*V3.1:* 8.8 HIGH *V2.0:*(not available)
CVE-2023-26281	IBM HTTP Server 8.5 used by IBM WebSphere Application Server could allow a remote user to cause a denial of service using a specially crafted URL. IBM X-Force ID: 248296. **Published:** 三月 01, 2023; 3:15:14 上午 -0500	*V3.1:* 7.5 HIGH *V2.0:*(not available)
CVE-2023-26039	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain an OS Command Injection via daemonControl() in (/web/api/app/Controller/HostController.php). Any authenticated user can construct an api command to execute any shell command as the web user. This issue is patched in versions 1.36.33 and 1.37.33. **Published:** 二月 24, 2023; 9:15:13 下午 -0500	*V3.1:* 8.8 HIGH *V2.0:*(not available)
CVE-2023-26038	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain a Local File Inclusion (Untrusted Search Path) vulnerability via web/ajax/modal.php, where an arbitrary php file path can be passed in the request and loaded. This issue is patched in versions 1.36.33 and 1.37.33. **Published:** 二月 24, 2023; 9:15:13 下午 -0500	*V3.1:* 6.5 MEDIUM *V2.0:*(not available)
CVE-2023-26036	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain a Local File Inclusion (Untrusted Search Path) vulnerability via /web/index.php. By controlling $view, any local file ending in .php can be executed. This is supposed to be mitigated by calling detaintPath, however dentaintPath does not properly sandbox the path. This can be exploited by constructing paths like ".../../", which get replaced by "../". This issue is patched in versions 1.36.33 and 1.37.33.	*V3.1:* 9.8 CRITICAL *V2.0:*(not available)

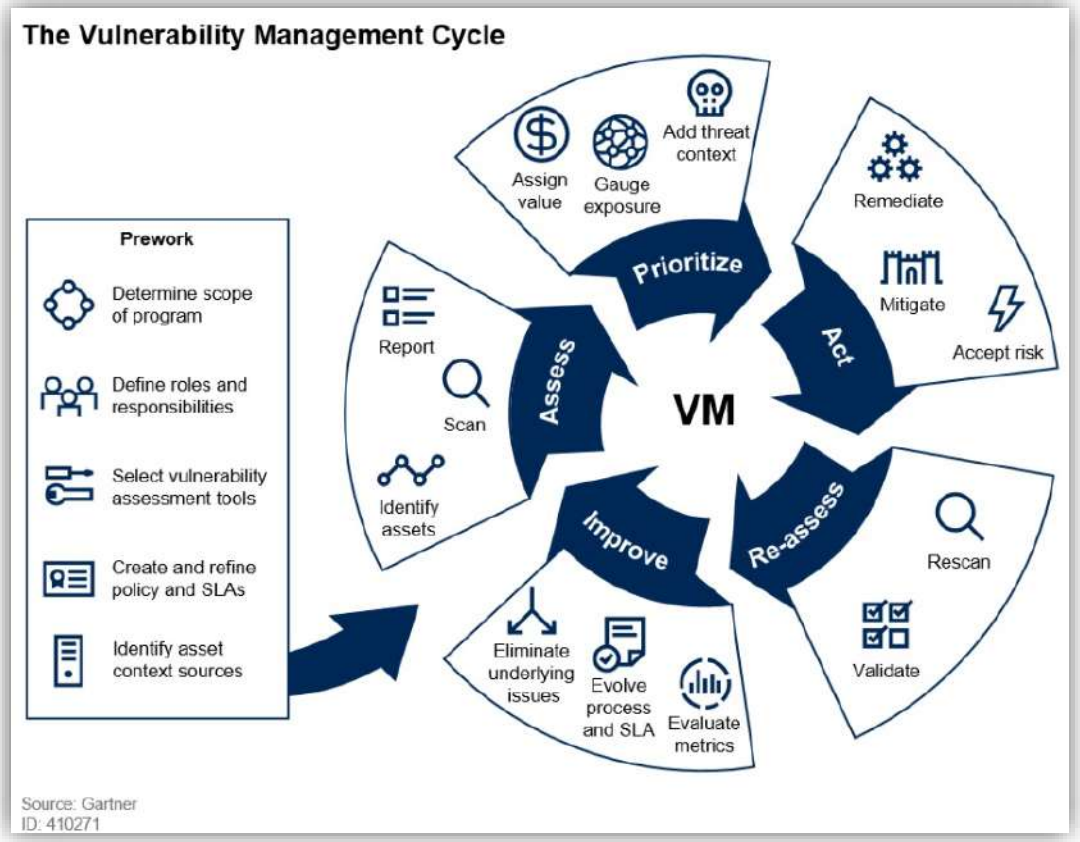
https://nvd.nist.gov/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Vulnerabilities Management

The process of identifying, prioritising, and addressing vulnerabilities in software, hardware, and other IT assets

- Identification: Identifying potential vulnerabilities in the system, such as security assessments, network scans, or vulnerability reports.
- Assessment: Evaluating the severity and impact of each vulnerability, such as risk analysis, threat modelling, or vulnerability testing.
- Prioritisation: based on their severity and potential impact, such as through a risk rating system
- Remediation: Developing and implementing a plan to mitigate or eliminate vulnerabilities, such as software updates, security patches, or configuration changes.
- Monitoring: Continuously monitoring the system for new vulnerabilities and security threats and updating the vulnerability management plan as needed.



Detecting Vulnerabilities

Identifying security weaknesses in software, hardware, or other IT systems that could be exploited by attackers

- Automated Scanners: typically use predefined attack patterns to test
- Penetration Testing
- Code Review: involves examining the website's code, such as code injection, buffer overflows, or insecure API calls.
- Log Analysis: analysing the website's server, such as repeated failed login attempts or unusual traffic patterns.

Tools

- Nessus
- Nmap + Metasploit
- Qualys

Patching (Essential 8)

A set of mitigation strategies developed by the Australian Cyber Security Centre to help organisations protect against cyber threats.

Maturity Model levels (0-3)

Based on the ACSC's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

https://www.cyber.gov.au/acsc/view-all-content/essential-eight

Criticality vs Asset Information vs Vulnerability Details

All important factors in assessing and managing cybersecurity risks.

Criticality

- degree of impact that a security incident could have on an organisation.
- This can be based on the importance of the asset that is at risk, the sensitivity of the data that is being protected, and the potential consequences of a breach.
- a risk rating or severity level, such as high, medium, or low.

Asset information

- details about the IT systems, applications, and data that an organisation is trying to protect.
- such as the location of the assets, the types of data stored on them, and the access controls that are in place to protect them.
- helps organisations to prioritise their security efforts based on the value of the assets at risk.

Vulnerability details

- information about the specific vulnerabilities that exist in an organisation's IT systems.
- such as the software versions that are affected, the types of attacks that are possible, and the severity of the vulnerability.
- help organisations to prioritise their patching efforts and to implement other mitigation strategies to reduce the risk of exploitation.

SET: Social Engineering Toolkit, open-source pen test framework geared for social engineering bundled within Kali Linux

Malware

Defining Malware

Malicious Soft**ware**

~ Malware

Comes in various forms

- **Software**
- **Code**

Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.

https://csrc.nist.gov/glossary/term/malware

Malware Categories

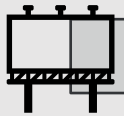
Virus

Worm

Trojan

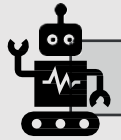
Ransomware

Rootkit



Adware

Spyware



Bot

Malware Aims

- Damage/Sabotage
- Persistent Access
- Espionage
- Money
- Information gathering
- Spam
- Phishing

Delivery Vectors

Malware finds its way onto devices through many different methods:

- Email attachments (Word, PDF, Xcel, etc.)
- Email links
- Drive-by-download
- Directly installed
- Advertising
- Watering Hole
- USB
- Remote injection

Attribution

Seeks to determine who was responsible

Original of attack and code

Novice attackers are likely to reveal more information than experienced attackers

- Active efforts to conceal
- Add bogus code
- Different compile/language pre-set
- Dummy comments in code in different language

Malware Production

A range of different actors produce malware
From APT, Cyber Criminals, to disgruntled software engineers

A good portion contain reused code
New variants

Track the evolution of code bases, functionality, behaviour

Malware Detection

A variety of tools are used in which to detect malware:

- Antivirus
- IDS
- End point protection
- Next-gen detection
- Machine learning

Antivirus & Hashes

A key portion of antivirus operations is the comparison of known malware hashes to unknow

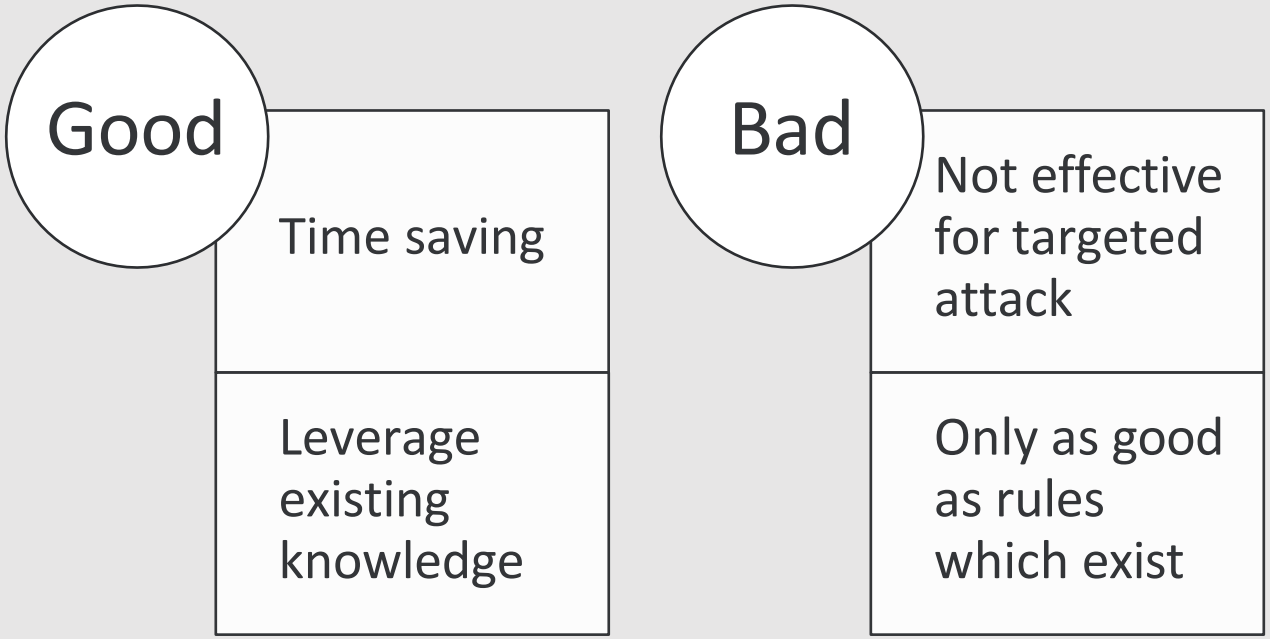
Malware Analysis

Automated Analysis

Leverage existing tools and platforms

Automate common tasks

Initial information source



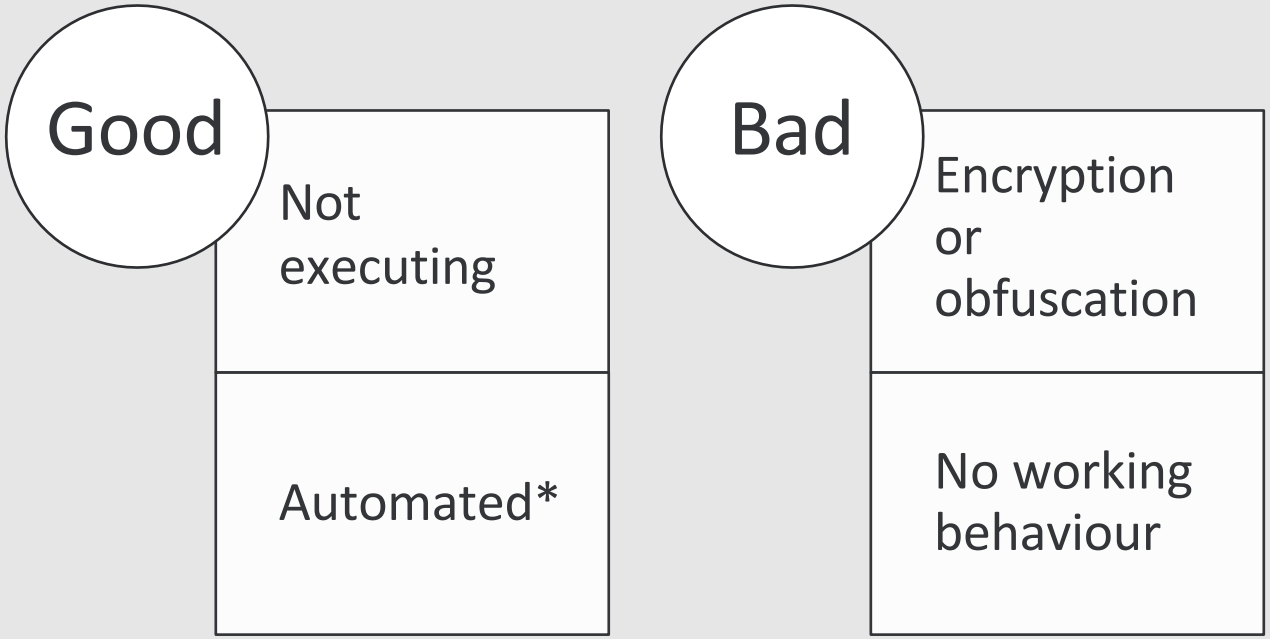
Static Analysis

Analysis of malware without execution

Fingerprints	• Hashes • Dropped file hashes
PE Headers	• Libraries • Code objects
Libraries	• DLL and Modules • Initial ideas of what the malware needs to run
Strings	• Explicit, hardcoded entries such as URLs, file objects, commands, time

Static Analysis Cont.

Static analysis helps guard against accidental contamination of malware



Dynamic Analysis

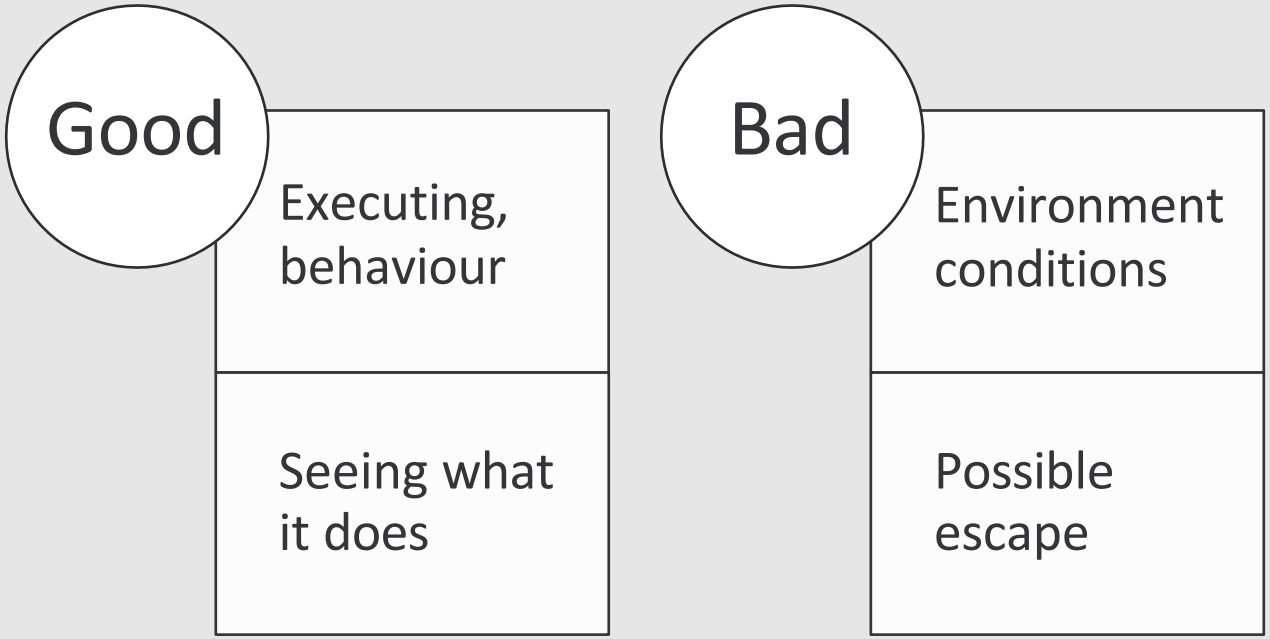
Analysis of malware through execution

VM, sandbox, container, specialised tools

Processes	• Start, stopped, injected
Filesystem	• Modification and use
Libraries	• DLL and Modules loaded
Behaviour	• Packers, second stage
Network	• C&C, beaconing

Dynamic Analysis Cont.

Dynamic execution helps reveal true behaviour*



Virus

*"A **computer virus:** Infect a computer with the ability to replicate itself and infect other programs through its own code.*

- "Old-school" malware was viruses written by hackers for fun and mischief.
- Had to be transmitted by BBS, disk (floppy).
- Capable of destroying data, crashing programs and general computer vandalism.
- Not the biggest problem now* –
  - other types of malware (worms, trojans) have more sinister ways of infecting computers and making money for their writers.
- Detection is by comparing a virus signature in a database with the code in a suspect file (using anti-virus software).

Historic Viruses

- Brain (1986) overwrite the boot sector of a DOS- formatted floppy disk, slowed the drive and displayed this message:

  Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt)
  Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA
  IQBAL TOWN LAHORE-PAKISTAN PHONE:
  430791,443248,280530. Beware of this VIRUS....
  Contact us for vaccination...

- Stoned (1987) is a boot-sector virus which displays the message:

  Your PC is now Stoned!

Neither of these viruses destroyed data.

Worms

- (originally) “Network worm”
- Spread through a network-aware program with a vulnerability
- May just spread
- May contain a payload
  - Downloader
  - Malware
  - RAT
  - Virus (for bridging air-gaps)

Worms

- A worm is a virus that can propagate without human intervention.
- Typically propagate through internet connections.
  - May be attached to web page:
  - ` <br></body></html><iframe src="http://uadrenal.com/qaqa/?daf02d89f0bb66c3b4a9ff31da01e10a" width=0 height=0 style="hidden" frameborder=0 marginheight=0 marginwidth=0 scrolling=no></iframe>`
- May carry a 'payload' – a virus, or other type of malware.

http://www.cruc.es/what-to-do-when-youve-been-hacked/

SWINBURNE UNIVERSITY OF TECHNOLOGY

CodeRed

- Ancient, but still out there.

```
203.110.29.108  - - [10/Aug/2010:19:43:02 +1000] "GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%
u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u909
0%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a
HTTP/1.0" 404 1024  "-" "-"
```

- Why? Old versions of IIS used in appliances - phones, printers, copiers.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Example: Conficker worm

Discovered November 2008

SN193.mpg

multi-threaded worm

- checks for and disables A/V, Windows update, Wireshark
- disables multiple and localhost DNS replies (anti-spyware and adware blocking techniques)
- checks for security web sites
- tiny downloader using port 445 (MS08-67 vulnerability)

Conficker worm..

- uses uPnP to open a port on the router
- filters network traffic to block other worms
- multiple forms of propagation
  - MS08-67 vulnerability,
  - dictionary attacks on LAN,
  - jumps to USB drive + *autorun.inf*
  - SMB
  - peer to peer sharing of downloads

Conficker worm…

- hides from user
  - very small bandwidth use (slow / infrequent)
  - **.dll** compressed with ups algorithm
  - randomly generated **dll** name
  - sets creation date to date of kernel32.dll
  - hides in svchost process
  - fails to return to OS when started – Windows never lists process. Name is set to NULL.
  - defies analysis by checking timing to detect debuggers

Conficker worm....

- does not infect hosts on Ukranian domains
  - downloads IP – location database to exempt Ukranian hosts
- uses IP-checking web sites to send public IP
- downloads itself from pseudo-randomly generated domain name (seeded using UTC clock).
  - *a* variant chooses 1 of 250 (changes daily)
  - *b* variant chooses 50 of 50000 (changing daily)
- updates itself over port 80 using SSL / signed certificates (public key crypto)
  - 5 versions so far – constant improvements
  - now being used to install various malware infections
  - History: http://www.youtube.com/watch?v=fvs2-YH1jFE

MyDoom

- MyDoom (*W32.Mydoom.A@mm*, *W32.Novarg.A*)
  - A worm that propagates by e-mailing itself to each address in the 'address book' as an executable attachment.
  - Contains a TCP server accepting connections on ports 3127 to 3198.
  - Used to launch a DDOS against *www.sco.com,* a company which "owned" UNIX and an open source Linux supplier Caldera, and tried to sue IBM, Novell, Red Hat, Sun other Linux distributors for copyright infringement.

Trojans

- "An unauthorized program contained within a legitimate program." (http://www.windowsecurity.com/faqs/Trojans/)
  - A some evil task when executed. trojan is a container which distributes malware hidden inside itself, using un-used bytes at the end of the file.
    - May be written from scratch to mimic some trusted program.
  - Performs some 'normal' task (e.g. game, screensaver) but also performs

Trojans

- Commonly distributed in downloaded 'free' software and game patches.
- The payload is usually a network client or server, but may act as both or neither.
- Uses for remote control, keyloggers, data miners (passwords, e-mail addresses) and DDOS, to distribute bots.
- Trojans are one of the most prevalent type of malware on home PCs.
- Simple anti-virus and firewalls offer little protection.

Examples

- **Just about all ransomware and many viruses uses trojans for distribution:**
- Vundo, Gh0st, Arucer, TrickBot, WannaCry, Ryuk, Anubis, Zeus, Emotet, Coinminer
- **Defences rely on A/V scanning of downloads, application layer firewalls, deep packet inspection.**
- A/V and OS vendors are slowly improving scanning and detection.

Rootkit

- Rootkits are a technology used by malware. They evade detection by patching the operating system kernel so that programs like *explorer.exe*, *task manager*, *ls* and *ps* cannot see them.
  - Root-kits have been used to enforce copy protection by Sony and game manufacturer UbiSoft (http://www.glop.org/starforce/).
  - Bugs in root-kits have become the targets of other exploits.

Rootkit

- Root-kits can be used to deliver and hide other malware such as trojans and worms.
- Rootkits are hard to remove
- Typically need to boot into another (uninfected and immune) OS to detect and delete files.
- Code can be hidden in other places. (see the notes)

Adware

- Adware is software which controls the downloading of advertisements onto web-browsers and "free" software. The distinction between adware and “spyware” is blurred. Few anti-spyware companies make a distinction.
  - Ben Edelman has made extensive studies of the infection processes of spyware, and the ethics of companies making money from it (https://www.benedelman.org/topics/adware/)

Spyware/Adware

- Spyware is persistent software that installs itself as a service, opens a TCP or UDP socket and sends information about the user's computer to some other party.
- Discovered during testing a new software firewall called ZoneAlarm. Unlike other firewalls at the time, ZoneAlarm monitored out-going connections as well as in-coming connections.
- Out-bound TCP connections can also be detected with Netstat.

Spyware/Adware

- Uses of spyware include keylogging, browser hijacking, theft of information such as passwords, user's surfing habits (cookies) and registry entries, push-advertising and other forms of un-ethical marketing.
- Social networking sites love spyware!
  - Nice description of an infection process here: http://isc.sans.org/diary.html?date=2004-11-24

Spyware/Adware

- Spyware is persistent and difficult to remove.
  - An infection will involve an installer, a downloader, scripts in *Temp* folders and *.ini* files, a *.dll* library, and entries including executable code in the registry.
  - If one part of the spyware is deleted, the other parts re-create it. Some parts are locked by the OS and can't be easily deleted.
  - Some spyware uses root-kits to evade detection and removal.

Spyware/Adware

- Microsoft use spyware in Windows 10 to mine data for sale.
  - https://www.scmagazine.com/home/security-news/privacy-compliance/article-29-working-party-still-not-happy-with-windows-10-privacy-controls/359412/
  - Facebook... Cambridge Analytica. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html
  - Russian Troll farms...
- Purchases of data include spammers, advertisers, marketers, political parties and services which advertise the ability to change election outcomes.
- Data collection and sale is the main income stream for many web services and software developers.

Flame

- Flame / *Flamer*, sKyWIper, Skywiper
  - Nation-state-grade spyware (2012)
  - Uses lots of new 0-days to install itself and to maintain itself.
  - Estimated to have cost $n00,000 to develop.
  - Has some code in common with Stuxnet.
  - used to gather intelligence to allow development of Stuxnet

Bots and Botnets

- AI or proxy malware designed to allow attacker remote control of “zombie” computer.
- Used for spying, DDOS attacks, relaying SPAM, anything the customer wants.

BOTs

- Uploaders
- Droppers
- Downloaders
- Relays
- RATs
- Attack tools (e.g.TFN2K)

WannaCry


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
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
Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59
Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

WannaCry

- Creates the mssecsvc2.0 service
  - Changes registry keys
- Encrypts a massive number of data file types
  - Deletes volume shadow copies (backups)
  - Demands $300, $600 in Bitcoin
  - Spreads throughout LAN on port 445
  - Uses DOUBLEPULSAR shellcode to spread infection
  - 32 and 64-bit OS support

WannaCry

- 12-15 May 2017
- Infected >250,000 computers in the first day
- Spread to >150 countries
- Suspected to have been stolen from the NSA's cache or weaponised malware.
- Security researcher (Darien Huss) found "Kill Switch" by analysing code – 3 URLs which if successfully contacted by worm would cause it to shut down.

Detection / Removal

- Detection of malware is patchy. Relying on a single security product is unwise. You should keep several products in use
  - keep them updated with the latest virus / spyware signatures.
- Be prepared to boot into safe mode – this disables many drivers, and may disable the spyware long enough for you to remove it.
- Boot into another OS – Live CD running Linux – and scan / remove malware from there.

Detection / Removal

- Use the internet (on a different PC) to search for tools / procedures for removing specific threats
- Some may be impossible to remove by normal means.
- If all else fails, reformat the hard disk and install everything fresh.
- The best protection is NOT TO GET INFECTED!

Detection / Removal

- To prevent re-infection, reduce risky practices:
  - Use a limited account.
  - Never go on the internet while logged on as admin/root.
  - Spyware will not be able to write to the registry or *system32* folder.
  - Be cautious of what you install – many games (including some versions of Warcraft) and amusing toys (are trojans) install malware along with the intended application.
  - Never install anything that you didn't go looking for.
  - Test suspect programs in a sandbox, VM or test machine