



PHÂN TÍCH MÃ ĐỘC

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY



TỔNG QUAN VỀ PHÂN TÍCH MÃ ĐỌC

CHƯƠNG 1

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY



Giới thiệu

1. Tổng quan về mã độc

1.1. giới thiệu về mã độc.

1.2. Phân loại mã độc:

1.3 Nguyên tắc hoạt động của mã độc

1.4 Các định dạng dữ liệu nhiễm mã độc

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

1.6. Các công cụ rà soát mã độc và các phương pháp phòng chống mã độc

2. Khái quát về phân tích mã độc

2.1. Giới thiệu chung

2.2. Vai trò phân tích mã độc

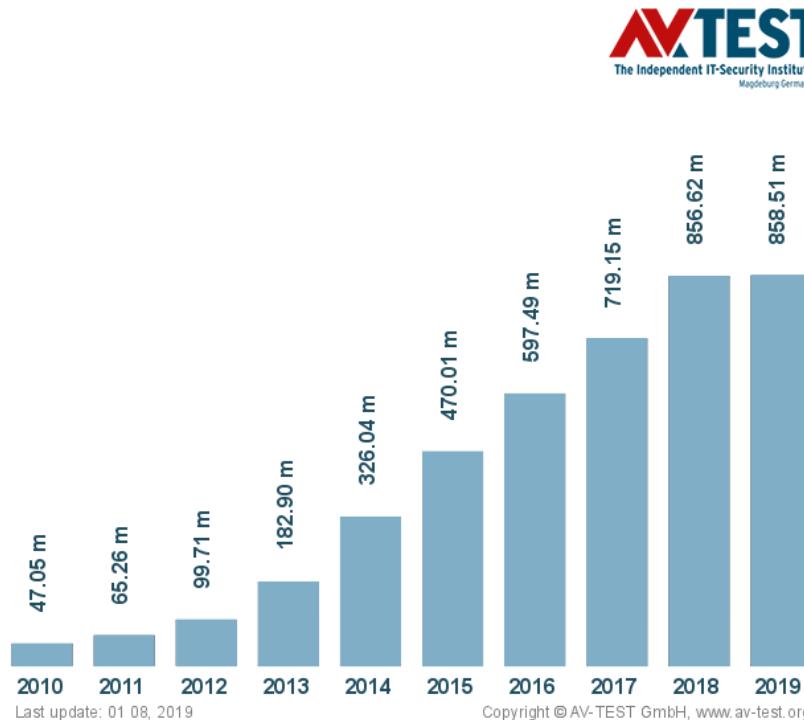
2.3. Phân loại kỹ thuật phân tích mã độc

1. Tổng quan về mã độc

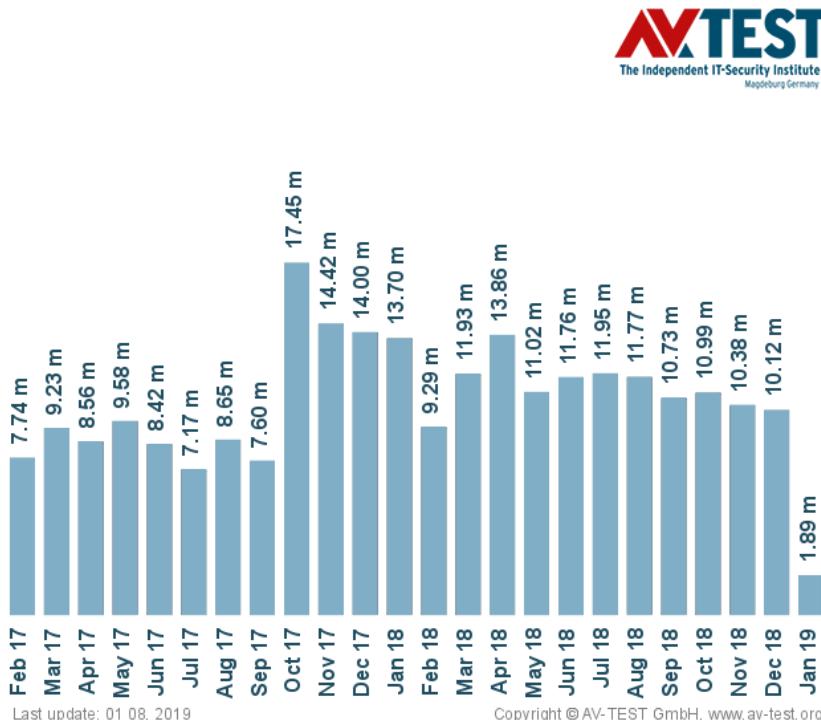
- 1.1. Giới thiệu về mã độc.
- 1.2. Phân loại mã độc
- 1.3. Nguyên tắc hoạt động của mã độc
- 1.4. Các hành vi và dấu hiệu cơ bản của mã độc

1.1. Giới thiệu về mã độc

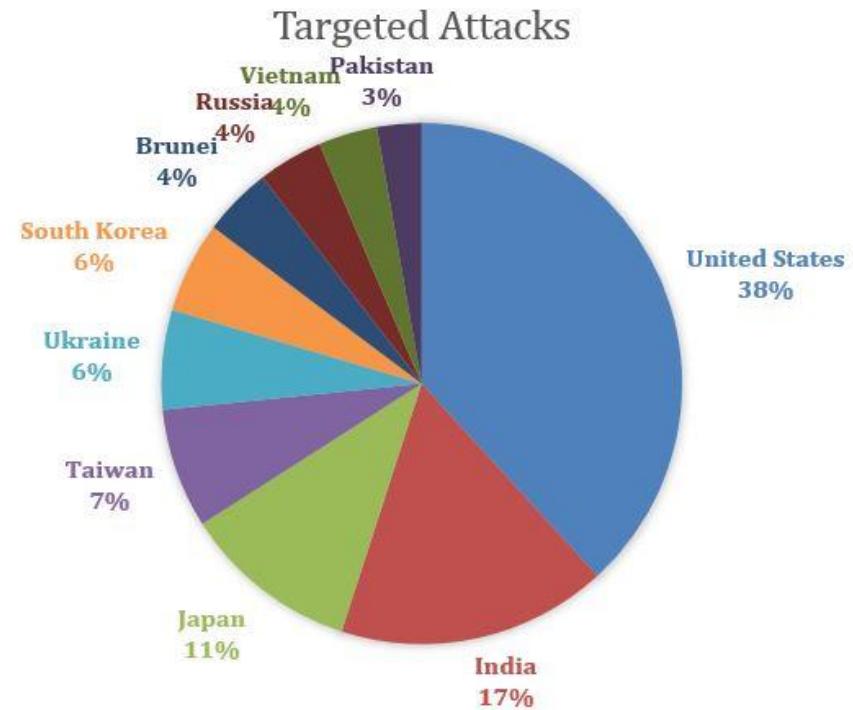
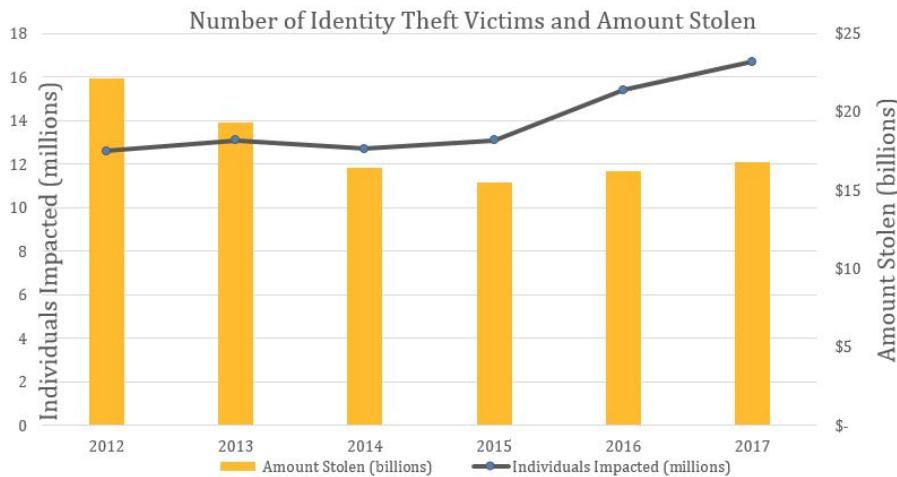
Total malware



New malware



1.1. Giới thiệu về mã độc



Source: Norton

1.1. Giới thiệu về mã độc

Vụ tấn công VietNam Airlines - 2016

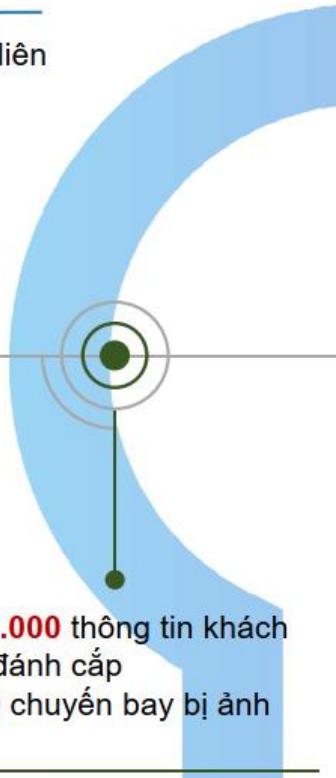
Cuộc tấn công dưới dạng APT nên đã được chuẩn bị kỹ lưỡng, mã độc được sử dụng vượt qua các công cụ giám sát, phần mềm chống virus...

7/2016



Cuộc tấn công được phát hiện vào cuối tháng 7/2016, tuy nhiên hacker có thể đã tấn công từ khoảng năm 2014.

Mục đích của cuộc tấn công liên quan đến chính trị



Các đối tượng tấn công thay đổi giao diện màn hình hiển thị tại nhà ga sân bay, website của Vietnam Airlines, phát tán thông tin khách hàng Bông sen vàng

Hơn **411.000** thông tin khách hàng bị đánh cắp
Hơn **100** chuyến bay bị ảnh hưởng

1.1. Giới thiệu về mã độc

Lịch sử của mã độc:

- Creeper Program (Sâu bướm) là virus đầu tiên được tạo ra vào năm 1971 bởi Bob Thomas. Nó sử dụng mạng ARPANET để tự sao chép giữa các máy tính.
- Reaper được tạo ra ngay sau đó bởi Ray Tomlinson với mục đích loại bỏ các bản sao của Creeper.
- Virus Wabbit (Rabbit) được viết vào năm 1974, là một trong những phần mềm tự sao chép đầu tiên. Tốc độ sao chép nhanh làm hệ thống bị quá tải và crash.

1.1. Giới thiệu về mã độc

Lịch sử của mã độc:

- Năm 1975, Trojan đầu tiên được viết mang tên ANIMAL. Nó sao chép bản thân sang mọi thư mục mà người dùng có quyền truy cập.
- Virus Elk Cloner xuất hiện năm 1982 là virus máy tính đầu tiên lây lan ngoài phòng thí nghiệm bằng đĩa mềm.
- Morris Worm năm 1988 là sâu máy tính lây lan trên Internet đầu tiên, gây tê liệt mạng do không kiểm tra các máy đã nhiễm.
- Cascade là loại độc hại đầu tiên sử dụng mã hoá để che giấu bản thân khỏi phát hiện.

1.1. Giới thiệu về mã độc

- Mã độc (Malware hay Malicious software) là một loại phần mềm được tạo ra và chèn vào hệ thống một cách bí mật với mục đích thâm nhập, phá hoại hệ thống, lấy cắp thông tin, làm gián đoạn hoặc tổn hại tới tính bí mật, tính toàn vẹn và tính sẵn sàng của hệ thống hay các máy tính cá nhân.



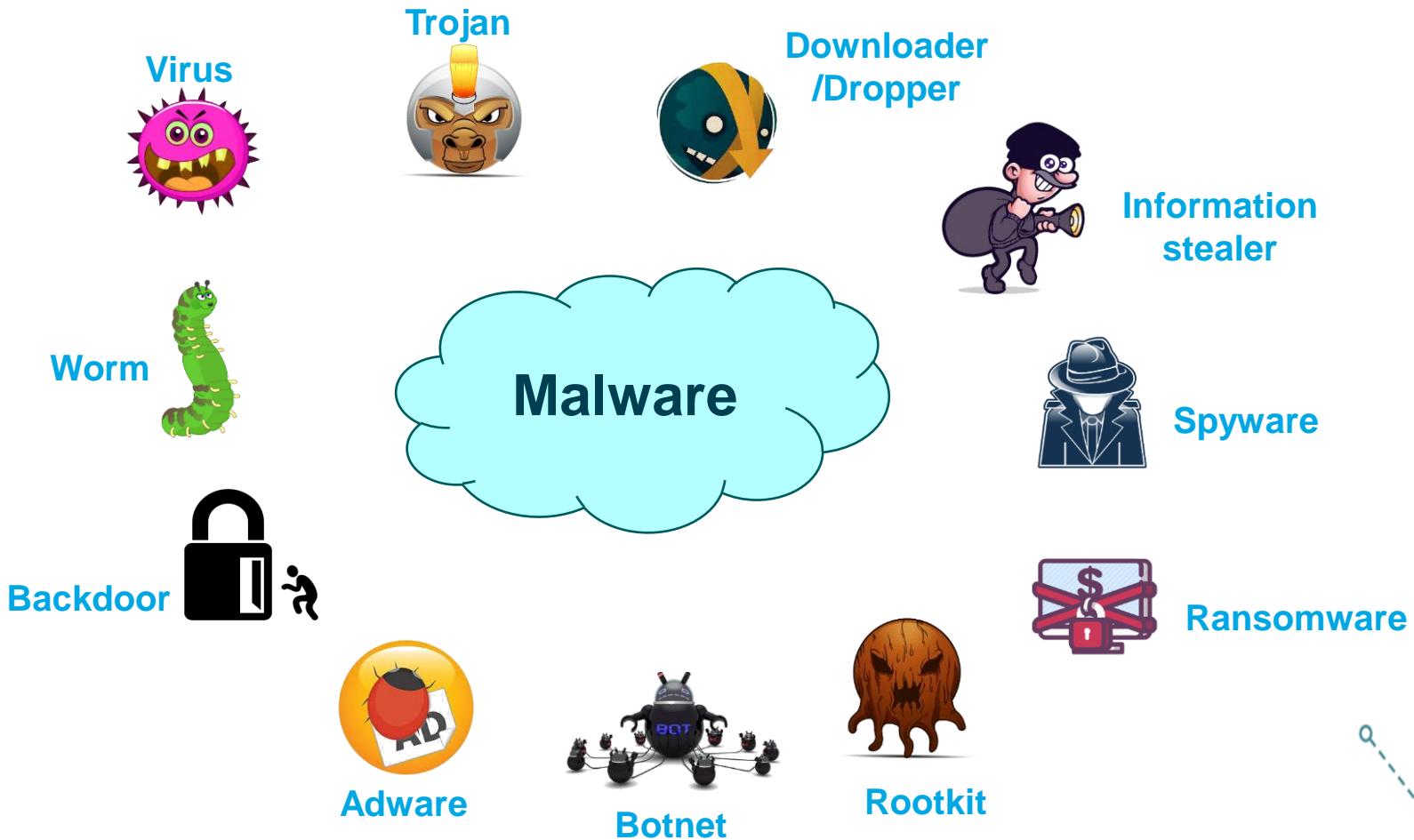
1.1. Giới thiệu về mã độc

- Nó có thể có dạng một tập tin thực thi, script, mã nguồn hoặc bất kỳ phần mềm nào khác.
- Kẻ tấn công sử dụng mã độc để đánh cắp thông tin nhạy cảm, giám sát hệ thống bị nhiễm và chiếm quyền kiểm soát hệ thống.
- Thông thường, mã độc xâm nhập trái phép vào hệ thống của nạn nhân và có thể lây lan qua các kênh truyền thông khác nhau như email, web hoặc ổ đĩa USB.

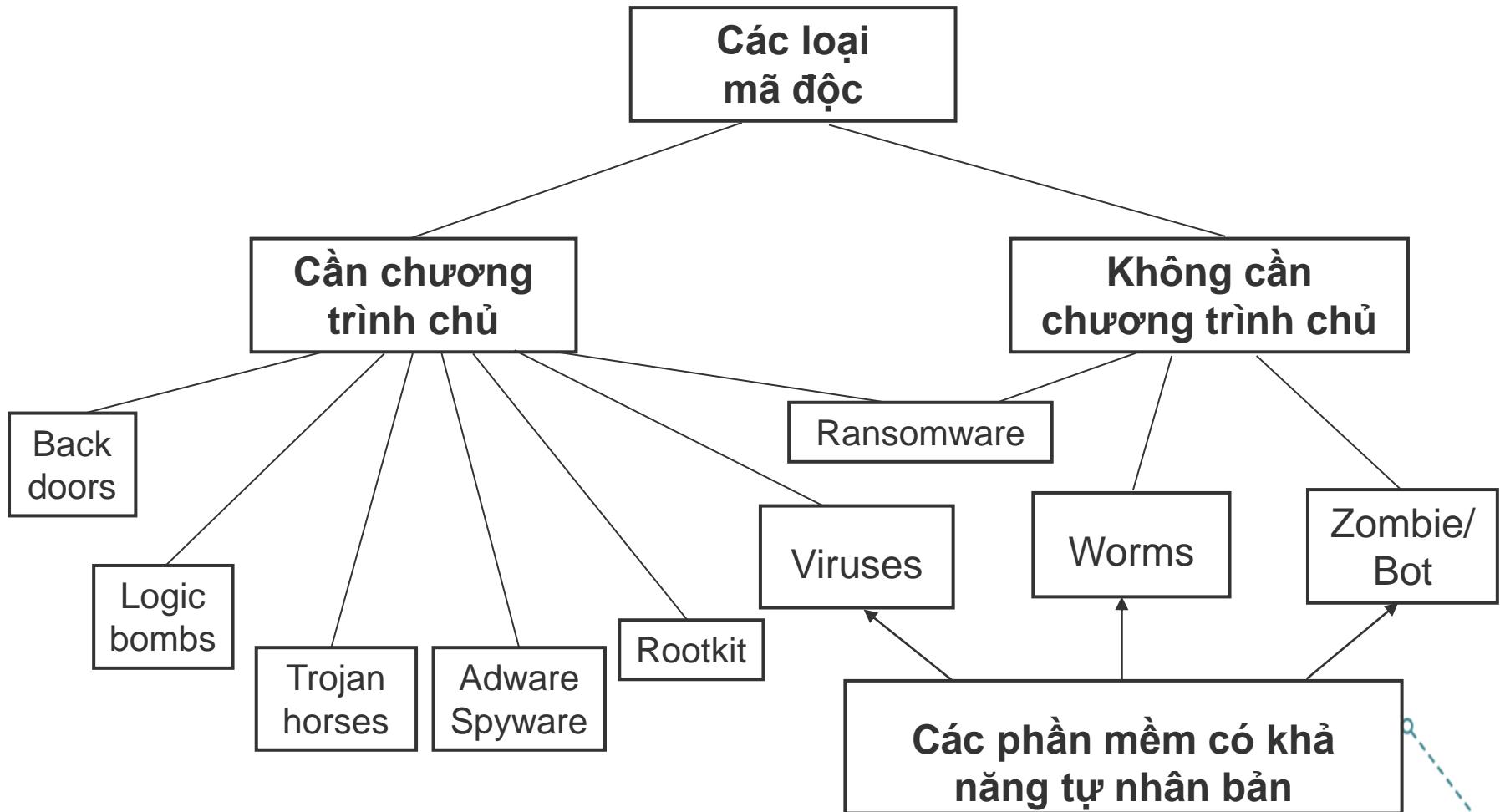
1.1. Giới thiệu về mã độc

- Các mục tiêu chính nhất có thể được phân loại thành:
 - Gây gián đoạn hoạt động của hệ thống máy chủ
 - Đánh cắp thông tin quan trọng, chẳng hạn như thông tin cá nhân và tài chính
 - Truy cập trái phép vào hệ thống hoặc tài khoản
 - Gián điệp
 - Gửi thư rác
 - Sử dụng hệ thống của nạn nhân để thực hiện tấn công DDoS
 - Khóa tệp tin của nạn nhân trên máy chủ và yêu cầu tiền chuộc để mở khóa.

1.2. Phân loại mã độc

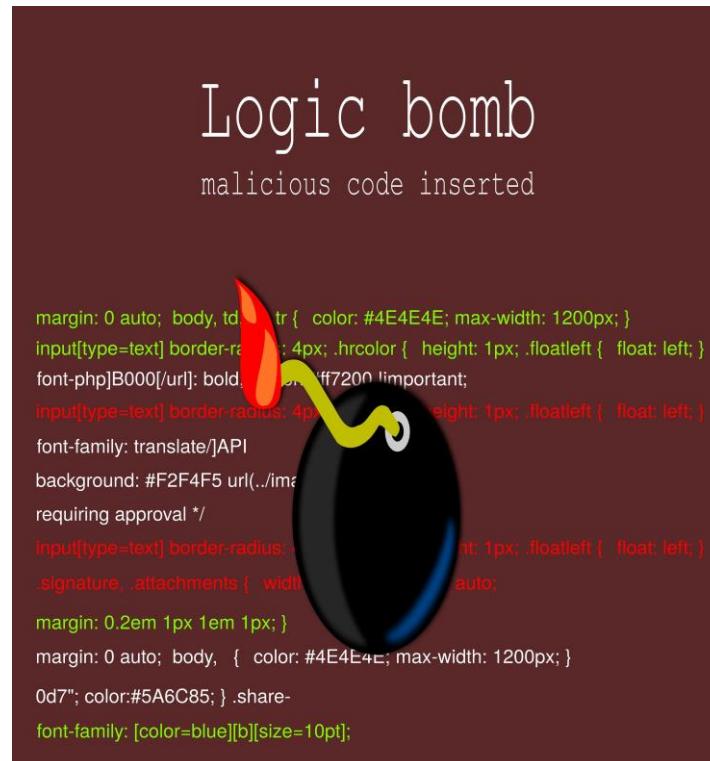


1.2. Phân loại mã độc



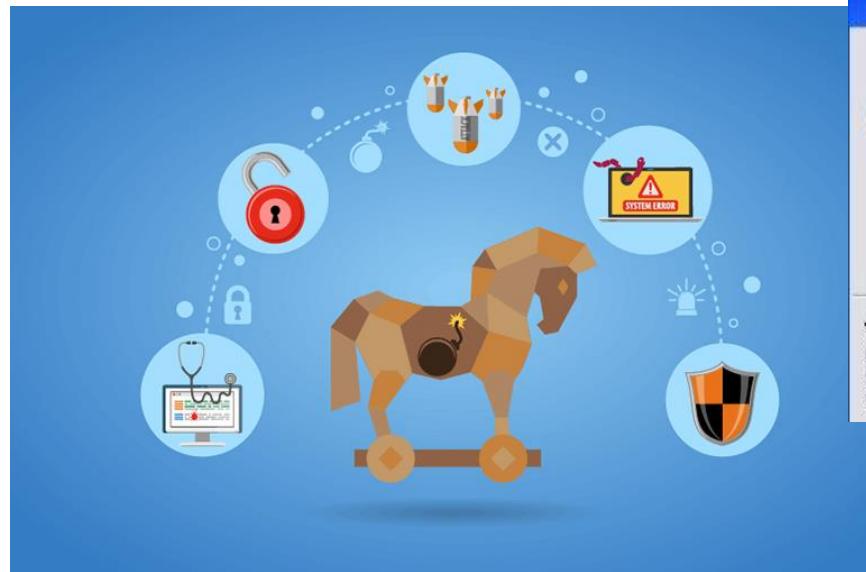
1.2. Phân loại mã độc

- **Bom logic** (Logic bombs) thường được “nhúng” vào các chương trình bình thường và thường hẹn giờ để “phát nổ” trong một số điều kiện cụ thể. Khi “phát nổ” bom logic có thể xoá dữ liệu, files, tắt cả hệ thống...



1.2. Phân loại mã độc

- **Trojan** horses chứa mã độc, thường giả danh những chương trình có ích, nhằm lừa người dùng kích hoạt chúng.



1.2. Phân loại mã độc

- **Back door** (cửa hậu) thường được các lập trình viên tạo ra, dùng để gỡ rối và test chương trình. Cửa hậu thường cho phép truy nhập trực tiếp vào hệ thống mà không qua các thủ tục kiểm tra an ninh thông thường. Do đó nó trở thành một mối đe doạ đến an ninh hệ thống.
- **Rootkit** là một loại phần mềm độc hại được thiết kế để ẩn danh trên hệ thống máy tính và cho phép kẻ tấn công có quyền truy cập cao nhất vào hệ thống mà không bị phát hiện. Rootkit thường được sử dụng để giấu các hoạt động độc hại khác trên hệ thống, như truy cập trái phép, sao chép dữ liệu hoặc thực hiện các cuộc tấn công khác.

1.2. Phân loại mã độc

- **Adware** (tên đầy đủ là advertising-supported software) là các phần mềm tự động hiển thị các bảng quảng cáo trong thời gian người dùng tải hoặc sử dụng các phần mềm. Adware thường được đóng gói chung với các phần mềm khác có thể dưới dạng như một phần của một phần mềm hoặc một dịch vụ miễn phí.
- **Spyware** là một dạng phần mềm độc hại được cài đặt tự động nhằm giám sát, thu thập và đánh cắp các thông tin nhạy cảm trên hệ thống nạn nhân.



1.2. Phân loại mã độc

- **Ransomware** là một loại phần mềm độc hại có khả năng mã hoá các tệp tin trên hệ thống của nạn nhân và yêu cầu nạn nhân phải trả tiền chuộc để nhận được chìa khóa giải mã. Ransomware là một trong những mối đe dọa an ninh mạng nguy hiểm nhất hiện nay và có thể gây thiệt hại nặng nề cho các tổ chức và cá nhân.

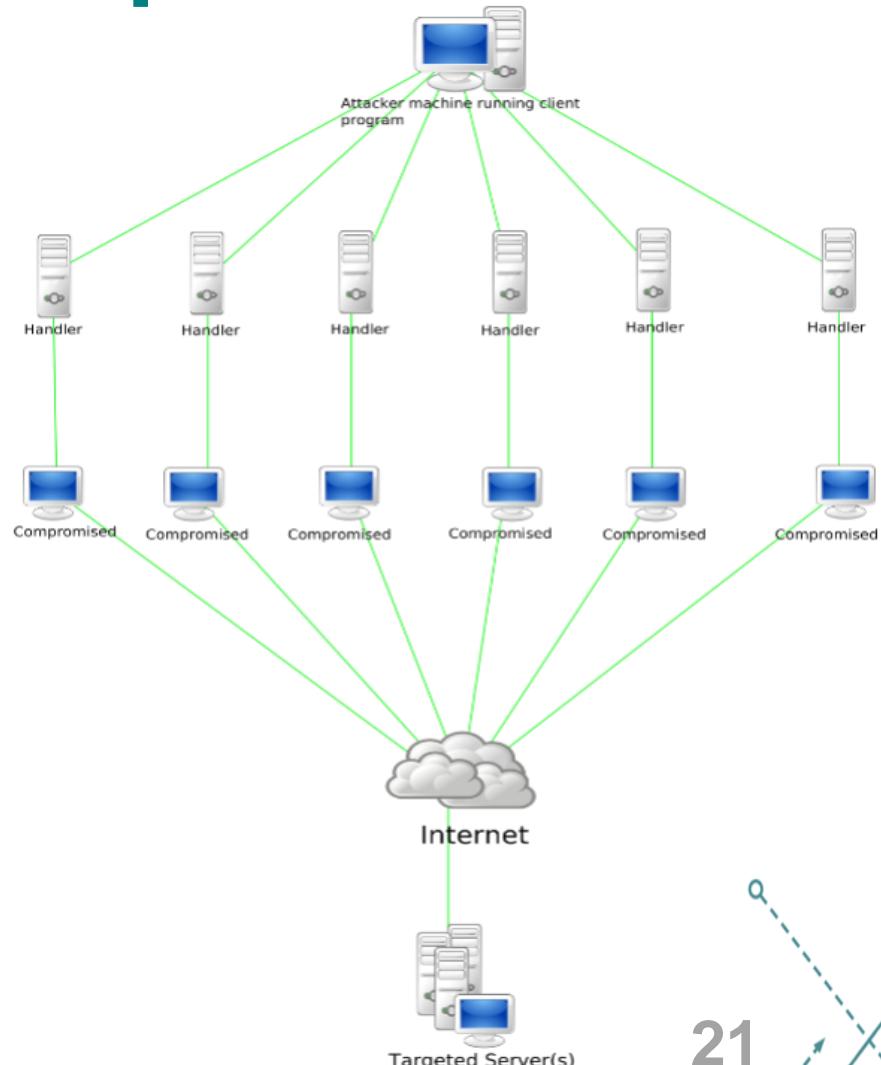


1.2. Phân loại mã độc

- **Vi rút (Virus)** là một chương trình có thể “nhiễm” vào các chương trình khác, bằng cách sửa đổi các chương trình này. Nếu các chương trình đã bị sửa đổi chứa vi rút được kích hoạt thì vi rút sẽ tiếp tục “lây nhiễm” sang các chương trình khác. Vi rút máy tính cũng có khả năng tự nhân bản, tự lây nhiễm sang các chương trình khác mà nó tiếp xúc. Có nhiều con đường lây nhiễm vi rút, như sao chép file, gọi các ứng dụng và dịch vụ qua mạng, email...
- **Sâu (Worm)** là một loại phần mềm độc hại có khả năng tự lây nhiễm từ máy này sang máy khác mà không cần chương trình chủ, vật chủ, hoặc sự trợ giúp của người dùng. Khi sâu lây nhiễm vào một máy, nó sử dụng máy này làm “bàn đạp” để tiếp tục rà quét, tấn công các máy khác. Các phương pháp lây lan chính của sâu gồm: lây lan qua thư điện tử, lây lan thông qua khả năng thực thi từ xa, lây lan thông qua khả năng log-in (đăng nhập) từ xa.

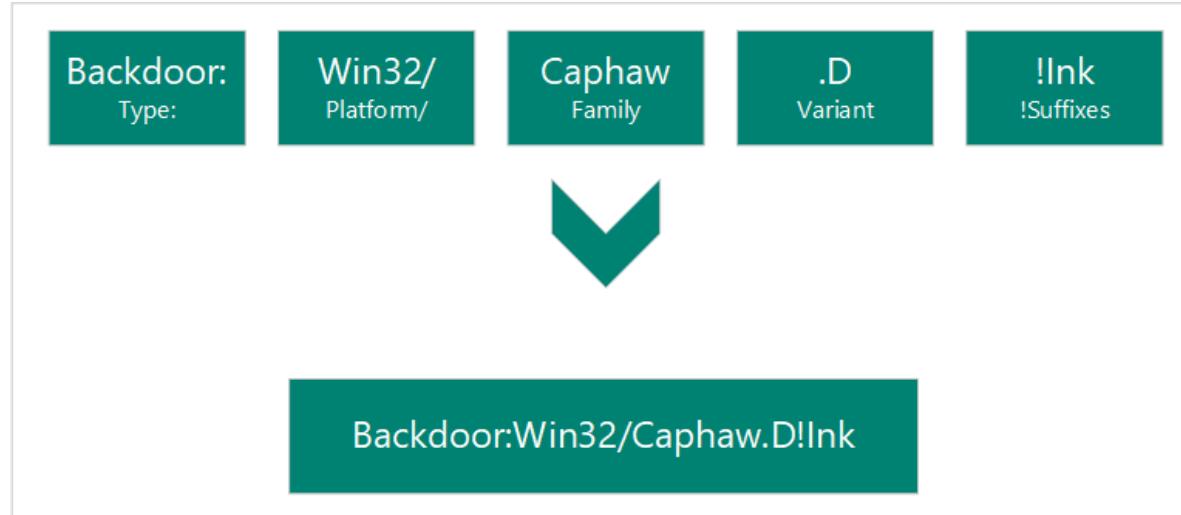
1.2. Phân loại mã độc

- **Zombie/Bot** là một chương trình được thiết kế để giành quyền kiểm soát một máy tính, hoặc thiết bị tính toán có kết nối Internet và sử dụng máy tính bị kiểm soát để tấn công các hệ thống khác, hoặc gửi thư rác. Botnet (mạng máy tính ma) là một tập hợp các máy tính bot dưới sự kiểm soát của một, hoặc một nhóm kẻ tấn công.



1.2. Phân loại mã độc

- Cách đặt tên mã độc



Malware Type	Microsoft Name Format	Example
Trojan	Trojan:Win32/<Family><variant>	Trojan:Win32/Kryptomix
Virus	Virus:Win32/<Family><variant>	Virus:W32/Sality
Ransomware	Ransom:Win32/<Family><variant>	Ransom: Win32/Tescrypt
Adware	PUA:Win32/<Family><variant>	PUA:Win32/CandyOpen
Worm	worm:Win32<Family><variant>	worm:win32/Allapple.0
BackDoor	Backdoor:Win32/<Family><variant>	Backdoor:Win32/Dridexed
Stealer	PWS:Win32/<Family><variant>	PWS:Win32/zbot
Downloader	TrojanDownloader:Win32/<Family><variant>	TrojanDownloader:Win32/Banload
Spying	TrojanSpy:Win32/<Family><variant>	TrojanSpy:Win32/Banker.GB

1.3. Nguyên tắc hoạt động chung của mã độc

Xâm nhập vào hệ thống



Điều khiển và kiểm soát hệ thống



Mở cửa hậu cho kẻ tấn công



Thực hiện các hoạt động độc hại



Che giấu sự hoạt động

1.3. Nguyên tắc hoạt động chung của mã độc

- **Xâm nhập vào hệ thống:** Mã độc thường sử dụng các lỗ hổng bảo mật hoặc phương pháp xâm nhập khác để xâm nhập vào hệ thống máy tính hoặc thiết bị khác.
- **Điều khiển và kiểm soát hệ thống:** Sau khi xâm nhập thành công, mã độc sẽ tìm cách lấy quyền điều khiển và kiểm soát hệ thống. Điều này cho phép kẻ tấn công có thể thực hiện các hoạt động độc hại trên hệ thống mà không bị phát hiện.

1.3. Nguyên tắc hoạt động chung của mã độc

- **Mở cửa hậu cho kẻ tấn công:** Mã độc thường sẽ tạo ra các lỗ hổng hoặc cửa sau trên hệ thống, cho phép kẻ tấn công có thể tiếp tục tấn công hoặc truy cập vào hệ thống sau này mà không cần phải xâm nhập lại.
- **Thực hiện các hoạt động độc hại:** Mã độc thường sẽ thực hiện các hoạt động độc hại trên hệ thống, bao gồm việc tạo ra các file giả mạo, thay đổi các cài đặt hệ thống, mã hóa các tệp tin quan trọng, đánh cắp thông tin cá nhân hoặc thông tin quan trọng, và thậm chí là điều khiển các thiết bị khác trong mạng của nạn nhân.

1.3. Nguyên tắc hoạt động chung của mã độc

- **Che giấu sự hoạt động:** Mã độc thường sẽ giấu kín hoạt động của mình để tránh bị phát hiện và gỡ bỏ khỏi hệ thống. Điều này có thể bao gồm việc tránh các chương trình chống virus, mã hóa các tệp tin hoặc các kết nối mạng bằng các phương thức mã hóa chéo, hoặc thay đổi các cài đặt hệ thống để tránh bị phát hiện.

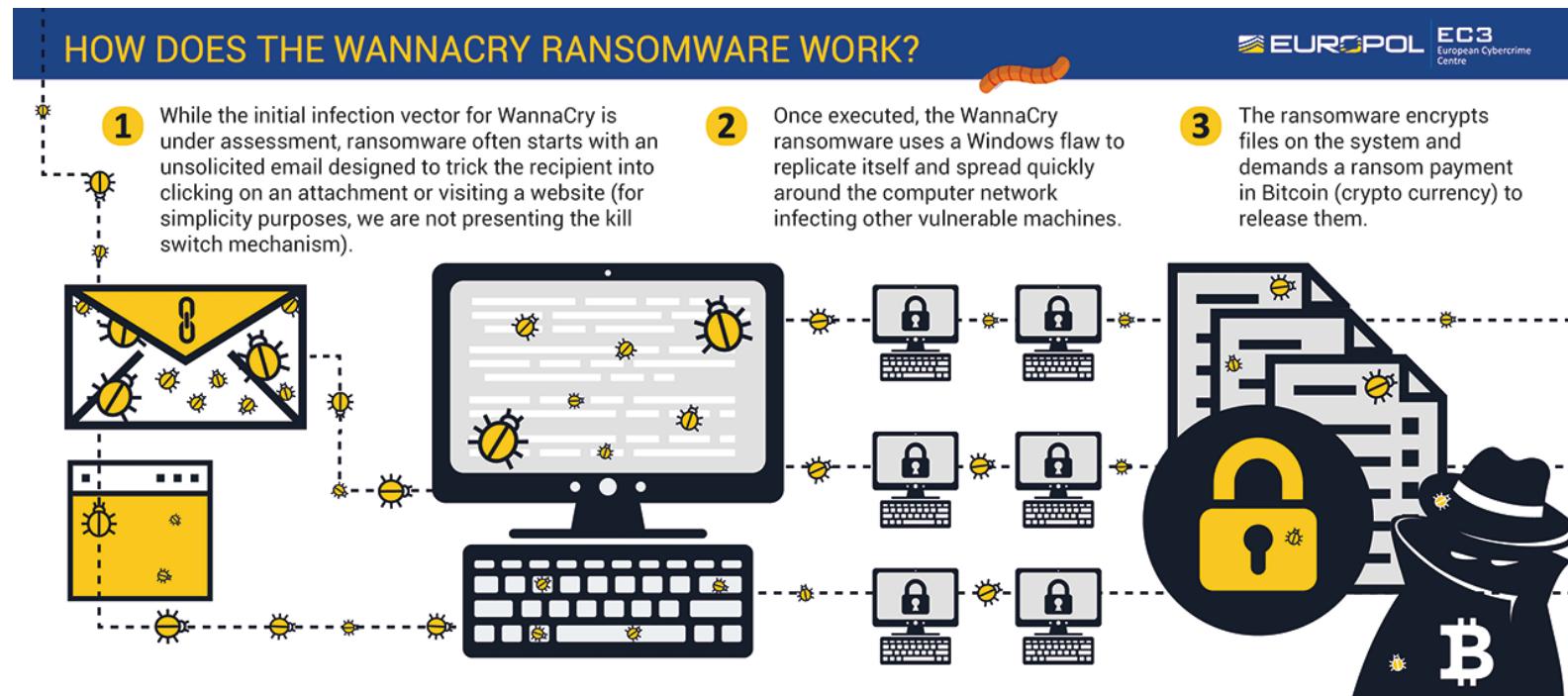
1.3. Nguyên tắc hoạt động chung của mã độc

- **Hình thức phát tán**

- Phát tán qua email
- Phát tán qua usb
- Phát tán qua lỗ hổng
- Phát tán qua điểm yếu hệ thống
- Phát tán qua các file nguồn không an toàn:
crack, keygen, free, social



1.3. Nguyên tắc hoạt động chung của mã độc



1.4 Các định dạng dữ liệu nhiễm mã độc

Số thứ tự	Vật chủ	Loại virus	Các định dạng	Kiểu
1	Tập tin văn bản	File virus Worm Trojan	Tập tin lô	BAT
			Tập tin script	VBS, JS
			Tập tin registry	REG
			Tập tin siêu văn bản	HTT, HTA
2	Tập tin chương trình	File virus Worm Trojan	Tập tin lệnh	COM
			Tập tin thi hành	EXE, SCR
			Tập tin thư viện	DLL, CPL, SYS, VXD
3	Tập tin MS Office	Macro virus	Tập tin tư liệu	DOC, DOT
			Tập tin bảng tính	XLS, XLT
			Tập tin trình diễn	PPT, POT
4	Mẫu tin khởi động	Boot virus	Mẫu tin khởi động hệ điều hành đĩa mềm	#N/A
			Mẫu tin khởi động hệ điều hành đĩa cứng	#N/A
			Mẫu tin khởi tạo phân khu đĩa cứng	#N/A

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- Các thành phần của mã độc

Windows

- Files
- Registry keys
- Processes, memory
- Folders

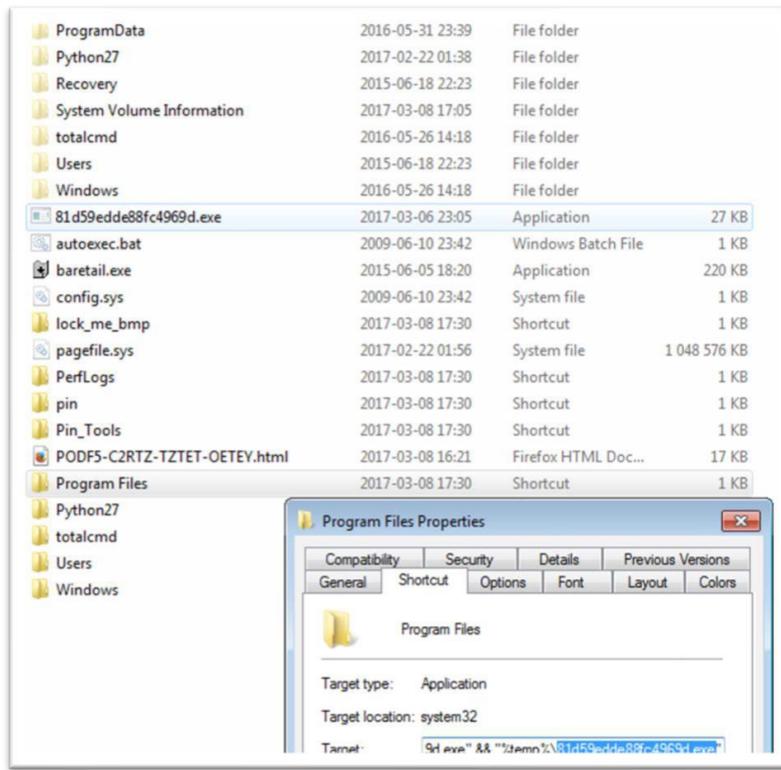
Linux

- Files
- Processes, memory
- Folders



1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- **Files:** Đây là thành phần chính của mã độc, chứa mã nguồn, encrypt data, payload và các thông tin của mã độc...



The screenshot shows a terminal window with the command 'ls' run in the directory '/home/user'. The output lists several subdirectories: Desktop, Documents, Downloads, Music, Pictures, Public, Templates, Videos, and examples.desktop. The terminal window has a dark theme and includes a title bar with the user's name and the current directory.

```
user@tecmint: ~
File Edit View Search Terminal Help
DIR: /home/user
> 2019-01-27 13:55 / Desktop/
2019-01-27 13:55 / Documents/
2019-01-27 13:55 / Downloads/
2019-01-27 13:55 / Music/
2019-01-27 13:55 / Pictures/
2019-01-27 13:55 / Public/
2019-01-27 13:55 / Templates/
2019-01-27 13:55 / Videos/
2019-01-27 13:50 8.8K examples.desktop
```



1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- **Registry keys** là các khóa trong hệ thống registry trên Windows, chứa các thông tin quan trọng về hệ thống và các ứng dụng. Mã độc có thể tạo, ghi, sửa đổi các key để khởi động và thực thi cùng hệ thống.

The screenshot shows the Windows Registry Editor interface. The title bar reads "Registry Editor". The menu bar includes "File", "Edit", "View", "Favorites", and "Help". The main window displays the registry path "Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv\Parameters". The left pane shows a tree view of registry keys: WpnUserService_2e7fz, ws2ifsl, wscsvc, WSearch, WSearchIdxPi, wuauserv, Parameters, and Security. The right pane is a table with columns "Name", "Type", and "Data". It lists four entries:

Name	Type	Data
(Default)	REG_SZ	(value not set)
ServiceDLL	REG_EXPAND_SZ	%systemroot%\system32\Malware.dll
ServiceDllUnlo...	REG_DWORD	0x00000001 (1)
ServiceMain	REG_SZ	WUServiceMain

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- Process, memory:** Mã độc có thể tạo ra các process (tiến trình) mới hoặc sửa đổi bộ nhớ (memory) của các tiến trình đang chạy trên máy tính để thực hiện các hoạt động độc hại.

The Task Manager screenshot shows several system processes running, including:

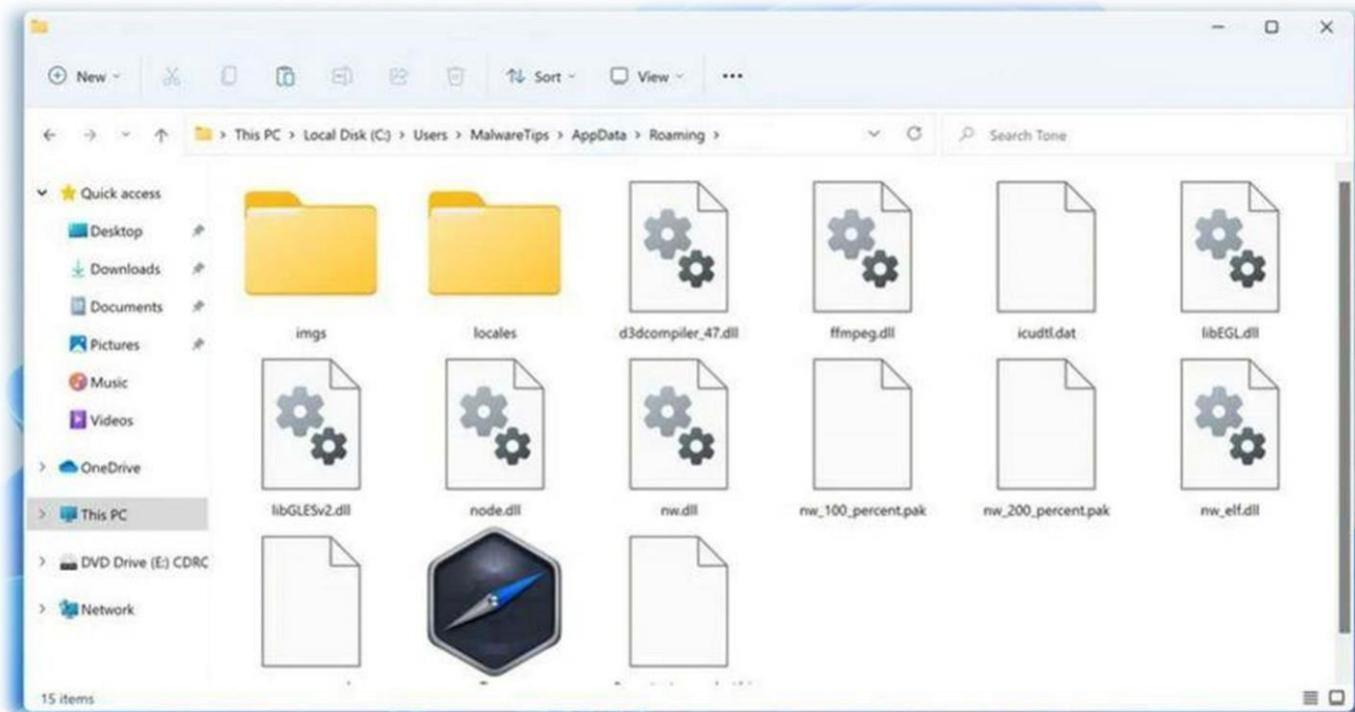
- System Settings Broker
- TeamViewer 11 (32 bit)
- Windows Command Processor
- Windows Shell Experience Host
- WMI Provider Host
- WMI Provider Host (32 bit)
- Wojeruyrre (32 bit) ← (highlighted with a red arrow)
- Zuofbe (32 bit) ← (highlighted with a red arrow)

```
root@sandflysecurity:/tmp# netstat -nlop
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*
tcp        0      0 0.0.0.0:22              0.0.0.0:*
tcp        0      0 0.0.0.0:31337            0.0.0.0:*
tcp        0    304 0.0.0.0:43308           0.0.0.0:*
tcp6       0      0 ::22                  ::*:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
raw6      0      0 ::58                  :::*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State         I-Node PID/Program name   Path
unix     2 [ ]           DGRAM    LISTENING   21563  1252/systemd
unix     2 [ ACC ]        SEQPACKET  LISTENING  11607  1/init
unix     3 [ ]           DGRAM    LISTENING   11583  1/init
unix     2 [ ACC ]        STREAM   LISTENING   21566  1252/systemd
unix     2 [ ACC ]        STREAM   LISTENING   11586  1/init
unix     2 [ ACC ]        STREAM   LISTENING   21570  1252/systemd
unix     2 [ ACC ]        STREAM   LISTENING   21571  1252/systemd
unix     2 [ ACC ]        STREAM   LISTENING   21572  1252/systemd
unix     7 [ ]           DGRAM    LISTENING   11592  1/init
unix     2 [ ACC ]        STREAM   LISTENING   21573  1252/systemd
unix     2 [ ACC ]        STREAM   LISTENING   21574  1252/systemd
unix     2 [ ACC ]        STREAM   LISTENING   11600  1/init
unix     2 [ ACC ]        STREAM   LISTENING   11609  1/init
unix     2 [ ]           DGRAM    LISTENING   11611  1/init
unix     2 [ ACC ]        STREAM   LISTENING   11613  1/init
unix     9 [ ]           DGRAM    LISTENING   11615  1/init
unix     2 [ ACC ]        STREAM   LISTENING   16375  1/init
unix     2 [ ACC ]        STREAM   LISTENING   16365  1/init
unix     2 [ ACC ]        STREAM   LISTENING   16383  1/init
unix     2 [ ACC ]        STREAM   LISTENING   16398  1/init
```

The netstat output shows various listening ports and socket connections. A red arrow points to the line for port 43308 (PID 1243), which corresponds to the highlighted process in the Task Manager.

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- **Folders:** Một số mã độc tạo ra các thư mục, thư mục ẩn để che dấu các tệp tin độc hại.



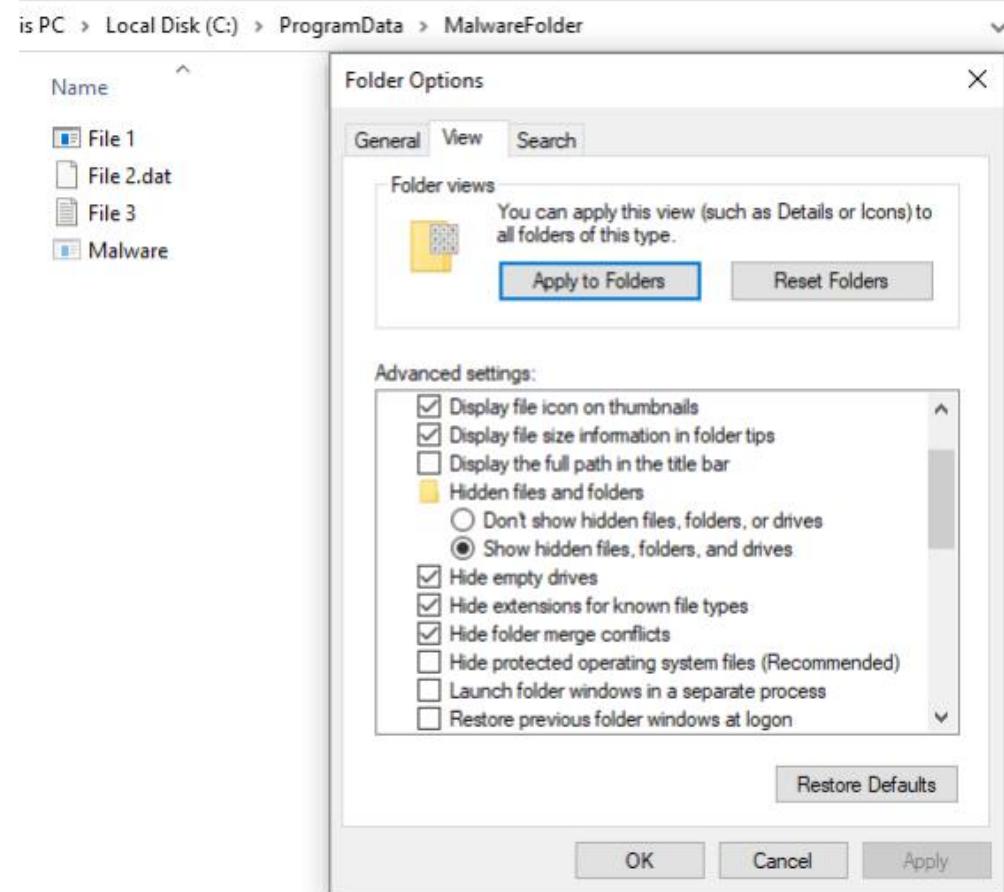
1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- Mã độc sử dụng nhiều kỹ thuật khác nhau để che dấu các thành phần, tránh bị phát hiện và ngăn chặn khả năng bị loại bỏ, kéo dài thời gian tồn tại trong hệ thống.

Che dấu	Rootkit	Chèn mã, system call	Khai thác lỗ hổng
<ul style="list-style-type: none">Sử dụng các kỹ thuật mã hóa, ẩn file....	<ul style="list-style-type: none">Mã độc ẩn đi các thành phần của chính nó	<ul style="list-style-type: none">Mã độc thực thi qua các lời gọi hệ thống hoặc chèn mã vào các tiến trình có sẵn	<ul style="list-style-type: none">Mã độc sử dụng các kỹ thuật và lỗ hổngmới

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- File có thuộc tính ẩn (hidden file, system file):** Theo mặc định, windows thiết lập không hiển thị các tệp có thuộc tính ẩn hoặc thuộc tính tệp hệ thống (system files) → Mã độc thường lợi dụng cơ chế này để ẩn các file độc hại.



1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

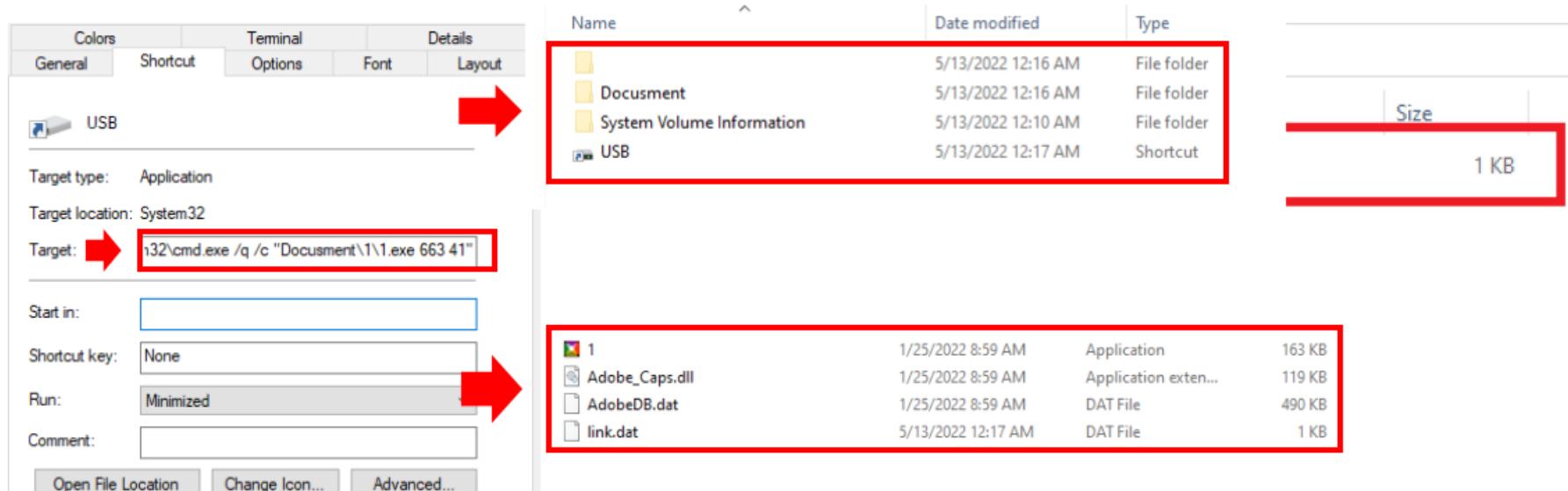
- Giả mạo icon

Name	Date modified	Type	Size
New folder	06-Jan-22 2:44 PM	File folder	
New folder (2)	07-Dec-21 11:46 AM	Application	1,172 KB
Tai lieu Tieng Anh	07-Dec-21 11:51 AM	Application	1,328 KB
zip file 2	06-Dec-21 11:09 AM	Application	97 KB
zip file	06-Jan-22 2:44 PM	Compressed (zipped)...	1 KB

→Mã độc có thể giả mạo các icon của thư mục, file nén, phần mềm chuẩn... để ẩn mình.

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

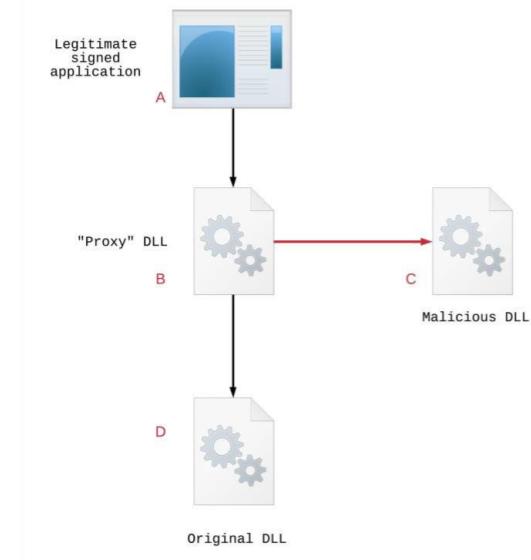
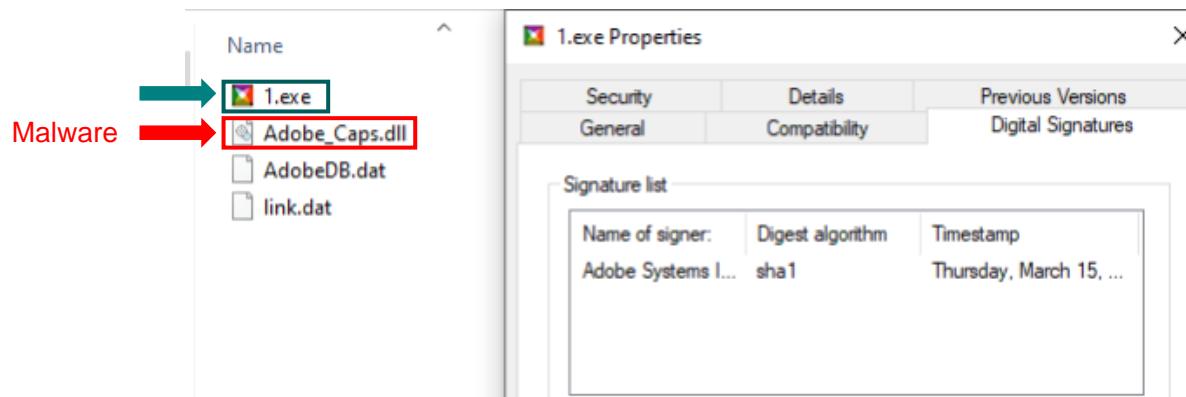
- Giả mạo shortcut



→ Mã độc có thể giả mạo shortcut để ẩn mình.

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

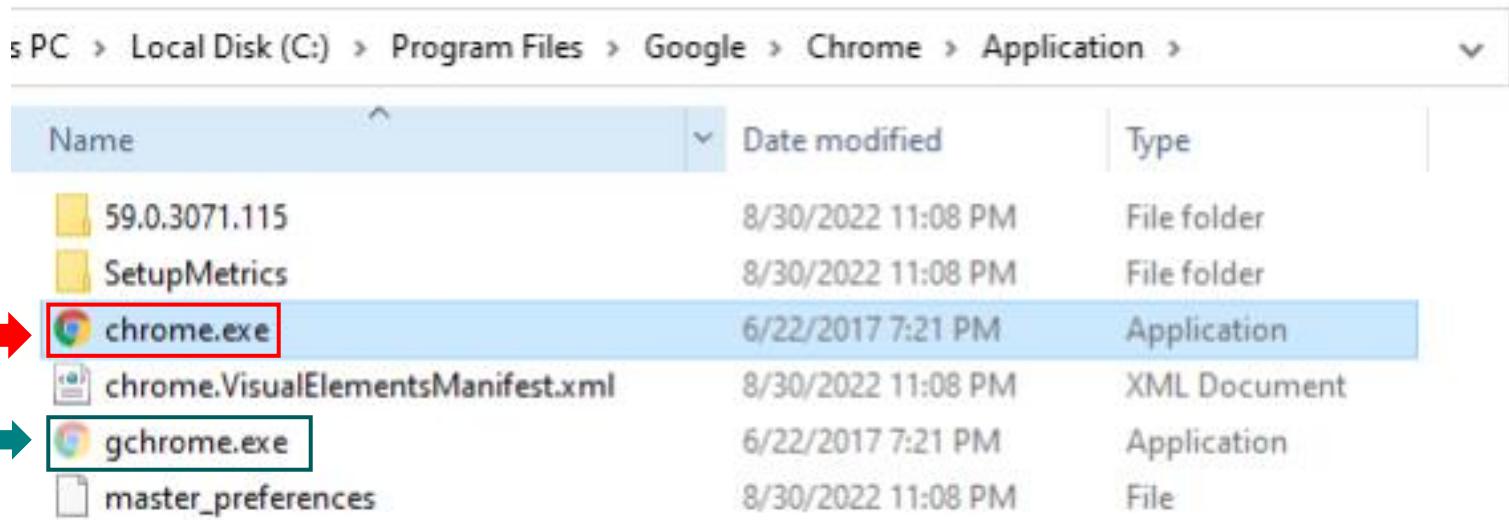
- Side-Loading, hijacking dll



→ Mã độc lợi dụng cơ chế load dll của hệ điều hành và phần mềm để ẩn mình.

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- Giả mạo file

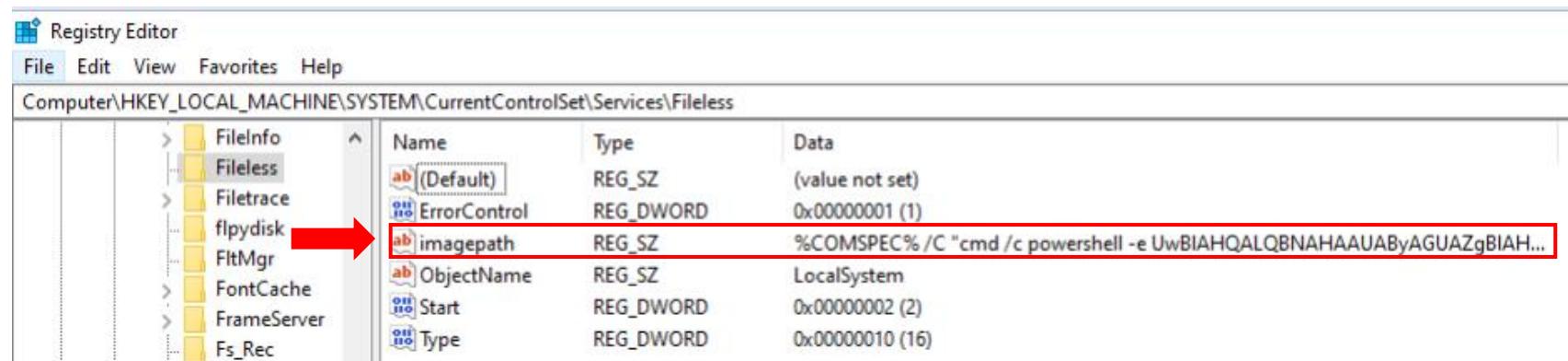


s PC > Local Disk (C:) > Program Files > Google > Chrome > Application >		
Name	Date modified	Type
59.0.3071.115	8/30/2022 11:08 PM	File folder
SetupMetrics	8/30/2022 11:08 PM	File folder
chrome.exe	6/22/2017 7:21 PM	Application
chrome.VisualElementsManifest.xml	8/30/2022 11:08 PM	XML Document
gchrome.exe	6/22/2017 7:21 PM	Application
master_preferences	8/30/2022 11:08 PM	File

→ Mã độc có thể giả mạo các phần mềm để ẩn mình.

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- Fileless

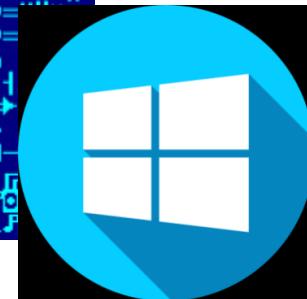


→ Mã độc fileless không tồn tại dạng file trên hệ thống.

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- Pre-OS boot

00	00	00	00-00	00	00	00-00	00	00	00-00	00	55	AA		Unk
EB	04	68	6A-6D	63	FB	E8-4E	01	BE	7A-7E	E8	21	01		♦HjmcsJwN@Hz~w!@
BE	B8	7F	E8-1B	01	BB	7A-7E	31	FF	B4-10	CD	16	80		ow<@z~1 >=A
FC	01	74	2B-80	FC	0E	74-34	80	FC	1C-74	3D	80	FC		Net+ANRt4AN-t=AN
E0	74	38	3C-21	72	E4	3C-7E	77	E0	83-FF	10	73	DB		pt8<!rφ<~wpΓ ▷s■
88	01	47	53-B8	2A	0E	BB-07	00	CD	10-5B	EB	CC	85		IOGSz*θl* ⇒ [m]E
FF	74	C8	4F-B0	20	88	01-E8	E8	00	EB-F2	85	FF	74		t@o] IΩωa aCE t
BA	4F	B0	20-88	01	E8	DA-00	EB	BB	53-B8	0D	0E	BB		o] IΩωg a S@JF@l
07	00	CD	10-B8	0A	0E	BB-07	00	CD	10-5B	BB	20	83		* ⇒ zθl* ⇒ [I_ Γ
FF	10	73	05-88	01	47	EB-F6	B1	10	31-D2	BE	7A	7E		►sSMGw9►1p^z~
FC	AC	E8	D3-00	FE	C9	75-F8	3B	16	FA-7F	74	13	BE		Ηηηηη ΙΓμο;-Δt!!F
DA	7F	E8	8C-00	E8	B0	00-FE	0E	79	7E-0F	85	60	FF		γωωM ω pυ~ωE
EB	6B	BB	00-7E	B9	05	00-BA	80	00	B8-01	02	CD	13		ωκj ~ o a zΩz==!!
73	08	BE	81-7D	E8	69	00-EB	FE	BF	FE-7F	81	3D	BE		s@B>ωi wIτ IΔB=F
AF	74	08	BE-8D	D8	E8	58-00	EB	FE	BA-55	AA	89	15		ntCHN>ωX a ΩκΙS
B9	01	00	BA-80	00	B8	01-03	CD	13	73-08	BE	81	7D		o a zΩv=!!s@B>
E8	3E	00	EB-FE	B9	00	02-BF	00	7E	30-C0	F3	AA	BB		ω> ω o a zΩeκn
00	7E	B9	02-00	BA	80	00-B8	01	03	CD-13	B9	03	00		~ o a zΩv=
B8	01	03	CD-13	B9	05	00-B8	01	03	CD-13	B8	40	00		zΩv=!! o a zΩv=
8E	C0	BB	72-00	31	C0	26-89	07	68	FF-FF	68	00	00		0 p 1^&N-h
CB	60	FC	AC-20	C0	74	09-BB	07	00	BA-0E	CD	10	EB		π Nn i τo> i
F2	61	C3	60-BB	07	00	B8-08	0E	CD	10-B8	20	0E	CD		Ca l' n* p⇒
10	B8	08	0E-CD	10	61	C3-60	BB	07	00-B8	0D	0E	CD		►p►p►a p*⇒
10	B8	0A	0E-CD	10	61	C3-50	51	88	C4-30	C0	31	C2		►p►p►a PQI-
B1	08	D1	E2-73	04	81	F2-21	10	FE	C9-75	F4	59	58		Ca ts♦Bc?►Ig
C3	49	2F	4F-20	65	72	72-6F	72	0D	0A-00	44	61	74		H/O error P
61	20	63	6F-72	72	75	70-74	65	64	0D-0A	00	00	00		a corrupted



→ Mã độc có thể ghi đè MBR để ẩn mình.

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- Chỉ chạy khi có môi trường

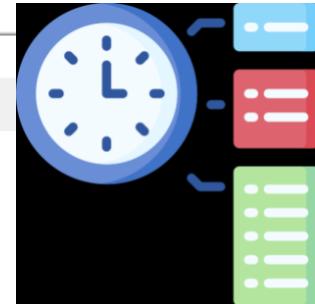


Name	Status	Triggers	Next Run Time	Last Run Time
Malware	Ready	At 1:00 AM every day	9/1/2022 1:00:00 AM	11/30/1999 12:00:00 AM

General Triggers Actions Conditions Settings History (disabled)

When you create a task, you can specify the conditions that will trigger the task. To change these triggers, open the task property pages using the Properties button.

Trigger	Details	Status
Daily	At 1:00 AM every day	Enabled



→ Mã độc chỉ chạy khi có một điều kiện nào đó để ẩn mình.

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- Lợi dụng các tiến trình, service hệ thống

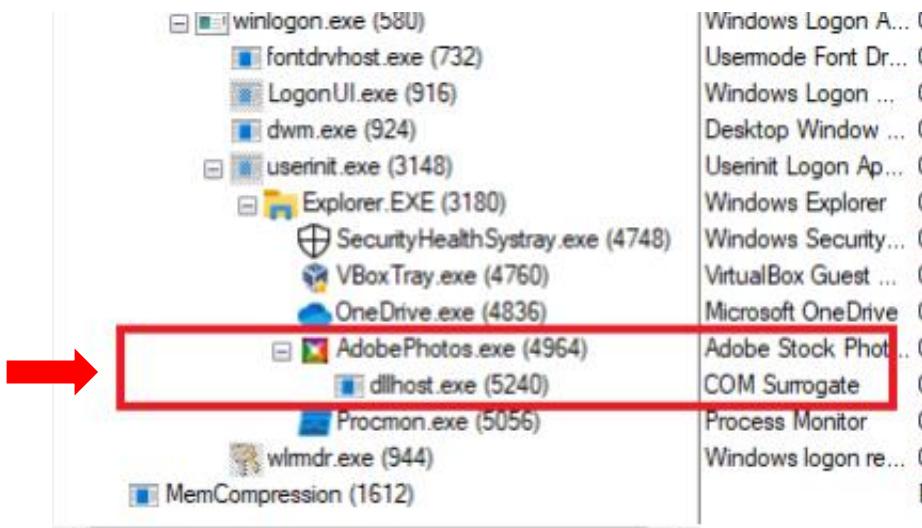
Name	Type	Data
(Default)	REG_SZ	(value not set)
ServiceDll	REG_EXPAND_SZ	%systemroot%\system32\Malware.dll
ServiceDLLUnloa...	REG_DWORD	0x00000001 (1)
ServiceMain	REG_SZ	WUServiceMain



→ Mã độc ẩn mình dưới các tiến trình, service hệ thống.

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- Lợi dụng các tiến trình, service hệ thống Injection



→ Mã độc ẩn mình dưới các tiến trình, service hệ thống.

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- Virus lây file

Program.exe										
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics	
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword	
.text	00000520	00001000	00000600	00000400	00000000	00000000	0000	0000	60000020	
.rdata	00000174	00002000	00000200	00000A00	00000000	00000000	0000	0000	40000040	
.data	00000414	00003000	00000600	00000C00	00000000	00000000	0000	0000	C0000040	
.rsrc	00000010	00004000	00000200	00001200	00000000	00000000	0000	0000	40000040	
_virus	0000092B	00005000	0000092B	00001400	00000000	00000000	0000	0000	E0000060	



→ Mã độc ẩn mình bằng cách lây nhiễm vào các chương trình, tệp thực thi.

1.5. Các hành vi, kỹ thuật ẩn mình và dấu hiệu cơ bản của mã độc

- Máy tính chạy chậm bất thường, chậm kết nối mạng
- Máy tính bị khóa hoặc không trả lời (stop responding) liên tục, không cho chạy các chương trình hệ thống (cmd, regedit, task manager, gpedit, run,...)
- Máy tính tự động khởi động lại hoặc bị lỗi (crashes).
- Khi chạy một chương trình thường thông báo lỗi, chạy các file *.exe, *.com,... đều bị thay thế bởi các chương trình khác.
- Ẩn file, thư mục, tạo các thư mục lạ, các biểu tượng lạ. Xuất hiện icon mới hoặc icon cũ tự mất

1.5. Các hành vi và dấu hiệu cơ bản của mã độc

- Xuất hiện các cửa sổ pop-up hoặc thông báo lạ, những tin nhắn báo lỗi không bình thường
- Hiển thị hoặc file in ra bị biến dạng
- Xuất hiện cặp đôi phần mở rộng của file. Ví dụ: vbs.txt...
- Phần mềm diệt virus không chạy hoặc không thể cài đặt
- Tệp bị lỗi hoặc thư mục được tạo ra một cách tự động hoặc bị thay đổi, bị xóa, bị mã hóa.
- Hệ thống bị thay đổi cài đặt hay bị kiểm soát từ xa

1.6 Các công cụ rà quét mã độc

Đối tượng	Tools
File	Explorer, cmd...
Process	Task manger, Process Explorer, Process Hacker...
Network	TcpView, Wireshark...
Startup	Regedit, AutoRuns...
Rootkit	PC Hunter, Rootkit Remover...
Logs	Event Viewer, Process Monitor...
Scanner	KVRT, TDSSKiller, Norton Power Eraser, ClamAV...

1.6 Các công cụ rà quét mã độc

- Autoruns



Autoruns - Sysinternals: www.sysinternals.com (Administrator)			
File	Search	Entry	User
Options	Category	Help	
 AppInit	 Known DLLs	 WinLogon	 Winsock Providers
 Everything	 Logon	 Explorer	 Internet Explorer
			 Print Monitors
			 Scheduled Tasks
			 Services
			 LSA Providers
Autoruns Entry		Description	Publisher
<input checked="" type="checkbox"/>	OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation
<input checked="" type="checkbox"/>	UniKey	UniKey Program	(Verified) PHAM KIM LONG
<input checked="" type="checkbox"/>	Viber	Viber	(Verified) Viber Media S.à r.l.
 HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
<input checked="" type="checkbox"/>	cmd.exe	Windows Command Processor	(Verified) Microsoft Windows
 HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
<input checked="" type="checkbox"/>	Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation
<input checked="" type="checkbox"/>	n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation
 HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/>	SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.
 HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components			
<input checked="" type="checkbox"/>	n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation
 Explorer			
 HKCU\Software\Classes\"\$ShellEx\ContextMenuHandlers			
<input checked="" type="checkbox"/>	FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation
 HKCU\Software\Classes\Directory\ShellEx\ContextMenuHandlers			
<input checked="" type="checkbox"/>	FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation

<https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns>

1.6 Các công cụ rà quét mã độc

- Process Explorer



Process Explorer - Sysinternals: www.sysinternals.com

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		9,512 K	107,300 K	100		
System Idle Process	87.94	60 K	8 K	0		
System	< 0.01	200 K	2,076 K	4		
Interrupts	< 0.01	0 K	0 K		n/a Hardware Interrupts and DPCs	
smss.exe		1,072 K	1,084 K	448	Windows Session Manager	Microsoft Corporation
Memory Compression		1,000 K	404,200 K	1880		
csrss.exe	< 0.01	1,936 K	5,444 K		600 Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,376 K	5,392 K		684 Windows Start-Up Application	Microsoft Corporation
services.exe		5,960 K	9,728 K		828 Services and Controller app	Microsoft Corporation
svchost.exe	< 0.01	12,480 K	30,456 K	976	Host Process for Windows S...	Microsoft Corporation
dllhost.exe		3,080 K	9,612 K	6192	COM Surrogate	Microsoft Corporation
StartMenuExperienceHos...		25,188 K	68,000 K	3444		
RuntimeBroker.exe		6,600 K	25,524 K	8428	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	128,808 K	214,512 K	8540	Search application	Microsoft Corporation
RuntimeBroker.exe	0.37	17,380 K	45,952 K	8628	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		7,344 K	7,924 K	9120	Host Process for Setting Syn...	Microsoft Corporation
RuntimeBroker.exe		4,376 K	21,384 K	4296	Runtime Broker	Microsoft Corporation
Name	Description	Company Name	Path			
ACPBackgroundMa...	<d> ACP Background Manager Poli...	Microsoft Corporation	C:\Windows\System32\ACPBackgroundManagerPolicy.dll			
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll			
AppExtension.dll	AppExtension API	Microsoft Corporation	C:\Windows\System32\AppExtension.dll			
apphelp.dll	Application Compatibility Client Libr...	Microsoft Corporation	C:\Windows\System32\apphelp.dll			
AppXDeploymentCli...	AppX Deployment Client DLL	Microsoft Corporation	C:\Windows\System32\AppXDeploymentClient.dll			
BackgroundMediaP...	<d> Background Media Policy DLL	Microsoft Corporation	C:\Windows\System32\BackgroundMediaPolicy.dll			
BCP47Langs.dll	BCP47 Language Classes	Microsoft Corporation	C:\Windows\System32\BCP47Langs.dll			

1.6 Các công cụ rà quét mã độc

- Process Hacker



Process Hacker [DESKTOP-SFU5AVD\tuong1]+ (Administrator)						
Hacker View Tools Users Help Refresh Options Find handles or DLLs System information 						
	Processes	Services	Network	Disk		
Name	PID	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0	93.69		40 kB	NT AUTHORITY\SYSTEM	
System	4	0.61		64 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	344			324 kB	NT AUTHORITY\SYSTEM	Windows Session Manager
Memory Compression	1624			320 kB	NT AUTHORITY\SYSTEM	
Interrupts	1.69			0		Interrupts and DPCs
Registry	72			5.16 MB	NT AUTHORITY\SYSTEM	
csrss.exe	448			1.01 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	516			972 kB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	608			2.73 MB	NT AUTHORITY\SYSTEM	Services and Controller app
svchost.exe	740			7 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
StartMenuExperie...	3820			11.89 MB	DESKTOP-SFU...\\tuong1	
RuntimeBroker.exe	3972			2.66 MB	DESKTOP-SFU...\\tuong1	Runtime Broker
SearchApp.exe	2052			61.63 MB	DESKTOP-SFU...\\tuong1	Search application
RuntimeBroker.exe	1604			8.59 MB	DESKTOP-SFU...\\tuong1	Runtime Broker
MicrosoftEdge.exe	928			15.47 MB	DESKTOP-SFU...\\tuong1	Microsoft Edge
ApplicationFrame...	1704			8.4 MB	DESKTOP-SFU...\\tuong1	Application Frame Host
SkypeBackground...	3232			1.57 MB	DESKTOP-SFU...\\tuong1	Microsoft Skype
browser_broker.exe	3304			1.82 MB	DESKTOP-SFU...\\tuong1	Browser_Broker
RuntimeBroker.exe	4164			1.09 MB	DESKTOP-SFU...\\tuong1	Runtime Broker
MicrosoftEdge...	4308			3.83 MB	DESKTOP-SFU...\\tuong1	Microsoft Edge Web Platform
MicrosoftEdgeCP....	4188			5.27 MB	DESKTOP-SFU...\\tuong1	Microsoft Edge Content Proce...
RuntimeBroker.exe	4348			2.28 MB	DESKTOP-SFU...\\tuong1	Runtime Broker
dllhost.exe	5160			960 kB	DESKTOP-SFU...\\tuong1	COM Surrogate
TextInputHost.exe	5596			6.4 MB	DESKTOP-SFU...\\tuong1	
WinStore.App.exe	6388			10.19 MB	DESKTOP-SFU...\\tuong1	Store
RuntimeBroker.exe	6468			1.08 MB	DESKTOP-SFU...\\tuong1	Runtime Broker
dllhost.exe	2960			2.63 MB	DESKTOP-SFU...\\tuong1	COM Surrogate

1.6 Các công cụ rà quét mã độc

- **TCPView**



TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6

Process Name Process ID Protocol State Local Address Local Port Remote Address

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address
svchost.exe	756	TCP	Listen	0.0.0.0	135	0.0.0.0
System	4	TCP	Listen	192.168.43.17	139	0.0.0.0
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0
svchost.exe	7640	TCP	Listen	0.0.0.0	5040	0.0.0.0
lsass.exe	848	TCP	Listen	0.0.0.0	49664	0.0.0.0
wininit.exe	684	TCP	Listen	0.0.0.0	49665	0.0.0.0
svchost.exe	1580	TCP	Listen	0.0.0.0	49666	0.0.0.0
svchost.exe	2056	TCP	Listen	0.0.0.0	49667	0.0.0.0
svchost.exe	2592	TCP	Listen	0.0.0.0	49668	0.0.0.0
spoolsv.exe	3636	TCP	Listen	0.0.0.0	49669	0.0.0.0
services.exe	828	TCP	Listen	0.0.0.0	49670	0.0.0.0
[Time Wait]		TCP	Time Wait	127.0.0.1	49690	127.0.0.1
[Time Wait]		TCP	Time Wait	127.0.0.1	49692	127.0.0.1
[Time Wait]		TCP	Time Wait	127.0.0.1	49694	127.0.0.1
[Time Wait]		TCP	Time Wait	127.0.0.1	49696	127.0.0.1

1.6 Các công cụ rà quét mã độc

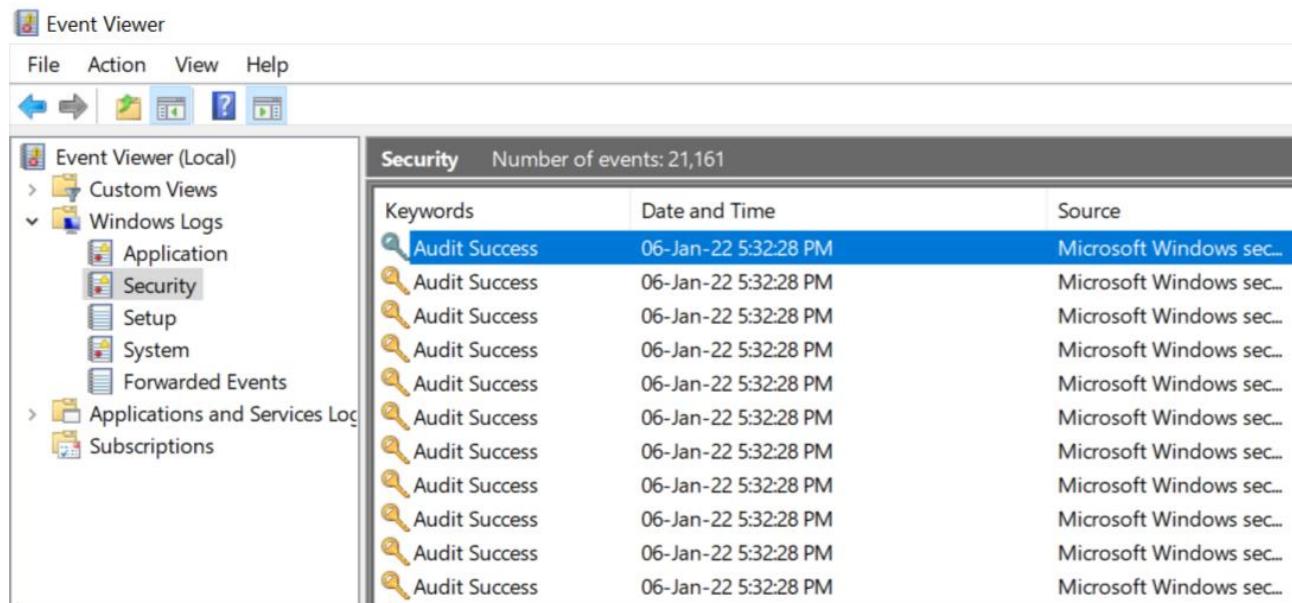
- PC Hunter



Image File Name	PID	Parent Pid	Image File Path
System	4	-	System
smss.exe	260	4	C:\Windows\System32\smss.exe
csrss.exe	336	328	C:\Windows\System32\csrss.exe
wininit.exe	384	328	C:\Windows\System32\wininit.exe
lsm.exe	496	384	C:\Windows\System32\lsm.exe
lsass.exe	488	384	C:\Windows\System32\lsass.exe
services.exe	480	384	C:\Windows\System32\services.exe
svchost.exe	1536	480	C:\Windows\System32\svchost.exe
svchost.exe	1424	480	C:\Windows\System32\svchost.exe
taskhost.exe	1396	480	C:\Windows\System32\taskhost.exe
spoolsv.exe	1344	480	C:\Windows\System32\spoolsv.exe
svchost.exe	1132	480	C:\Windows\System32\svchost.exe
svchost.exe	1056	480	C:\Windows\System32\svchost.exe
SearchIndexer.exe	988	480	C:\Windows\System32\SearchIndexer.exe
SearchProtocolHost.exe	2324	988	C:\Windows\System32\SearchProtocolHost.exe
SearchFilterHost.exe	1504	988	C:\Windows\System32\SearchFilterHost.exe
SearchProtocolHost.exe	968	988	C:\Windows\System32\SearchProtocolHost.exe
svchost.exe	888	480	C:\Windows\System32\svchost.exe
taskeng.exe	1620	888	C:\Windows\System32\taskeng.exe
GoogleUpdate.exe	288	1620	C:\Program Files\Google\Update\GoogleUpdate.exe
GoogleUpdate.exe	1588	288	C:\Program Files\Google\Update\GoogleUpdate.exe
GoogleCrashHandler.exe	1156	288	C:\Program Files\Google\Update\1.3.36.112\GoogleCr

1.6 Các công cụ rà quét mã độc

- **Event Viewer**



1.6 Các công cụ rà quét mã độc

- Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com												
Time ...	Process Name	Sess...	PID	Arch...	Operation	Path	Result	Detail	Date & Time	Image Path		
12:42...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLML\SYSTEM\Setup	SUCCESS		5/25/2021 12:42...	C:\Windows\syste...		
12:42...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLML	SUCCESS	Desired Access: M...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	RegQueryKey	HKLML	SUCCESS	Query: HandleTag...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLML\system\Setup	SUCCESS	Desired Access: R...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLML	SUCCESS		5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	RegQueryValue	HKLML\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWO...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLML\SYSTEM\Setup	SUCCESS		5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLML	SUCCESS	Desired Access: M...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	RegQueryKey	HKLML	SUCCESS	Query: HandleTag...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLML\system\Setup	SUCCESS	Desired Access: R...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLML	SUCCESS		5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	RegQueryValue	HKLML\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWO...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLML\SYSTEM\Setup	SUCCESS		5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Desired Access: M...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Query: HandleTag...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Desired Access: R...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS		5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Type: REG_DWO...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS		5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,766,144...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,864,448...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 11,190,272...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,856,256...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,749,760...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,897,216...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,782,528...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,823,488...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,807,104...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,733,376...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 23,044,096...	5/25/2021 12:42...	C:\Windows\syte...		
12:42...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,880,832...	5/25/2021 12:42...	C:\Windows\syte...		

1.6 Các công cụ rà soát mã độc

- Lưu ý khi rà soát mã độc
 - Phát hiện dựa vào các thành phần khởi động
 - Phát hiện dựa vào thông tin file
 - Phát hiện dựa vào thông tin tiến trình
 - Phát hiện dựa vào thông tin kết nối mạng
 - Sử dụng nguồn tham khảo: virustotal, sandbox

1.6. Các phương pháp phòng chống mã độc

- Sử dụng phần mềm diệt mã độc, cập nhật thường xuyên.
- Quét virus định kỳ.
- Luôn quét các USB, ổ cứng gắn ngoài khi cắm vào máy tính.
- Duyệt web an toàn, thiết lập bảo mật cho trình duyệt, tránh click những link quảng cáo hoặc bất thường.
- Quét các file tải về từ Internet
- Không kích vào link hay tệp đính kèm trong email khi chưa chắc chắn về độ an toàn của chúng.
- Tải và cài đặt phần mềm từ các website tin cậy.
- Sử dụng Sandbox, máy ảo, các trang kiểm tra trực tuyến để kiểm thử chương trình nếu không chắc chắn về tính an toàn của nó.

1.6. Các phương pháp phòng chống mã độc

- Vận dụng kinh nghiệm sử dụng máy tính
 - Phát hiện sự hoạt động khác thường của máy tính
 - Kiểm soát các ứng dụng đang hoạt động
 - Loại bỏ một số tính năng của HĐH có thể tạo điều kiện lây nhiễm cho virus
 - Cập nhật các bản vá lỗi hệ điều hành
- Bảo vệ dữ liệu máy tính
 - Sao lưu dữ liệu theo chu kỳ
 - Tạo các dữ liệu phục hồi cho toàn hệ thống

2. Khái quát về phân tích mã độc

2.1. Giới thiệu chung

2.2. Vai trò phân tích mã độc

2.3. Phân loại kỹ thuật phân tích mã độc

2.1. Giới thiệu chung

- Phân tích mã độc là việc nghiên cứu hành vi của mã độc.
- Mục tiêu của phân tích mã độc là hiểu cách thức hoạt động của mã độc và cách phát hiện và loại bỏ nó.

2.2. Vai trò phân tích mã độc

- Mục đích chính khi thực hiện phân tích mã độc là thu thập thông tin từ mẫu mã độc. Từ đó xác định được khả năng của mã độc, phát hiện và ngăn chặn nó.
- Ngoài ra phân tích mã độc cũng làm nguồn cung cấp, xác định mẫu mã độc để hỗ trợ việc phát hiện và ngăn chặn trong tương lai.

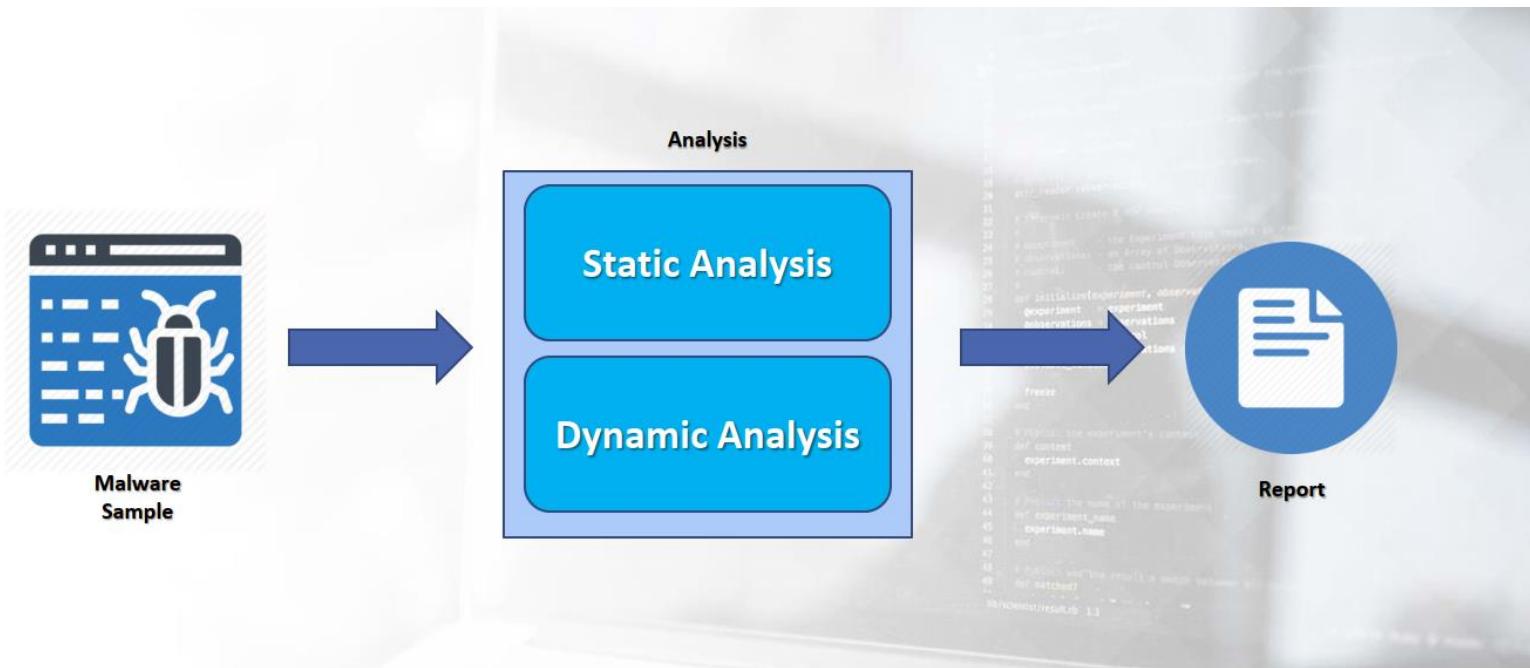
2.2. Vai trò phân tích mã độc

- Các nguyên nhân chính để thực hiện phân tích mã độc như sau:
 - Xác định bản chất và mục đích của mã độc. Ví dụ, xác định liệu mã độc có phải là kẻ đánh cắp thông tin, bot HTTP, bot spam, rootkit, keylogger, RAT...
 - Hiểu rõ hệ thống bị xâm phạm như thế nào và ảnh hưởng của nó.

2.2. Vai trò phân tích mã độc

- Xác định các chỉ số mạng liên quan đến mã độc, sau đó có thể sử dụng để phát hiện mã độc tương tự bằng cách theo dõi mạng.
- Thu thập các chỉ số dựa trên máy chủ như tên tập tin, khóa registry, sau đó có thể sử dụng để xác định mã độc tương tự bằng cách theo dõi trên máy chủ.
- Xác định ý định và động cơ của kẻ tấn công. Ví dụ, trong quá trình phân tích, nếu thấy mã độc đánh cắp thông tin ngân hàng → động cơ của kẻ tấn công là tiền.

2.3. Phân loại kỹ thuật phân tích mã độc



2.3. Phân loại kỹ thuật phân tích mã độc

- **Phân tích tĩnh (static analysis):**

- Phân tích mã nguồn hoặc file thực thi của mã độc mà không cho mã độc hoạt động. Thường thực hiện trên máy tính an toàn không kết nối mạng. Cho phép khám phá cấu trúc và chức năng bên trong của mã độc. Phát hiện các công cụ và kỹ thuật được sử dụng.
- **Ưu điểm:** An toàn hơn, dễ thực hiện.
- **Nhược điểm:** Khó nắm bắt hành vi thực tế của mã độc.

2.3. Phân loại kỹ thuật phân tích mã độc

- Phân tích tinh cơ bản: tìm cách hiểu mã độc bằng cách phân tích chính file, cấu trúc file, các chức năng được sử dụng bởi mã độc ...
- Phân tích tinh nâng cao: phân tích sâu hơn và tìm cách hiểu được mã độc dựa trên dịch ngược (disassembled).

2.3. Phân loại kỹ thuật phân tích mã độc

- **Phân tích động (dynamic analysis):**

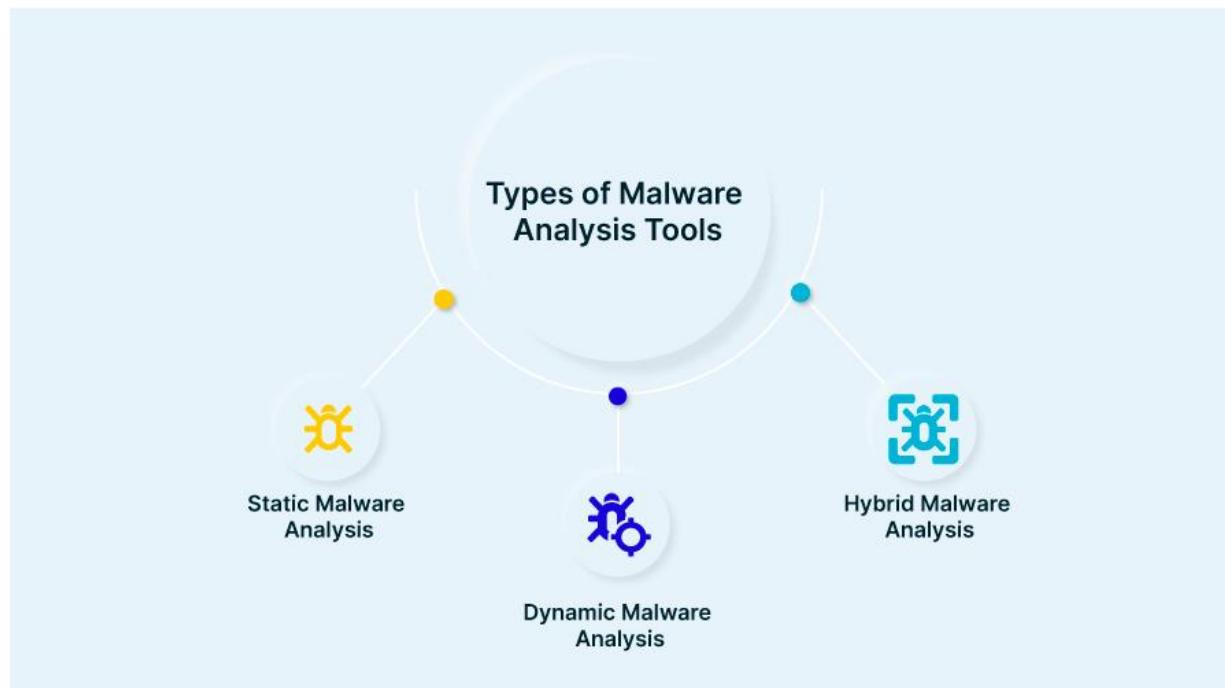
- Phân tích mã độc bằng cách cho mã độc thực thi và giám sát và phân tích hoạt động của nó. Thường thực hiện trong môi trường cô lập để đảm bảo an toàn. Cho phép nghiên cứu hành vi của mã độc trên máy chủ, tương tác với mạng và hệ thống. Có thể phát hiện các chỉ số mạng và máy chủ liên quan đến mã độc.
- **Ưu điểm:** Hiểu được hành vi và tác động của mã độc.
- **Nhược điểm:** Cần môi trường cô lập và có thể nguy hiểm.

2.3. Phân loại kỹ thuật phân tích mã độc

- Phân tích động cơ bản: Chạy mã độc trong môi trường cô lập có trang bị sẵn các công cụ giám sát khác nhau và cố gắng hiểu mã độc đang làm gì dựa trên đầu ra của các công cụ đó.
- Phân tích động nâng cao: nếu phân tích cơ bản không đem lại kết quả hoặc muốn tìm hiểu kỹ hơn thì cần thực hiện phân tích nâng cao mã đ bằng cách sử dụng một bộ gỡ lỗi (debuger). Bằng cách này, chuyên gia có nhiều quyền kiểm soát hơn về cách mã độc được thực thi.

2.3. Phân loại kỹ thuật phân tích mã độc

- Trên thực tế các chuyên gia thường kết hợp phân tích tĩnh và phân tích động để đem lại hiệu quả cao nhất. Được gọi là phân tích lai (hybrid malware analysis)

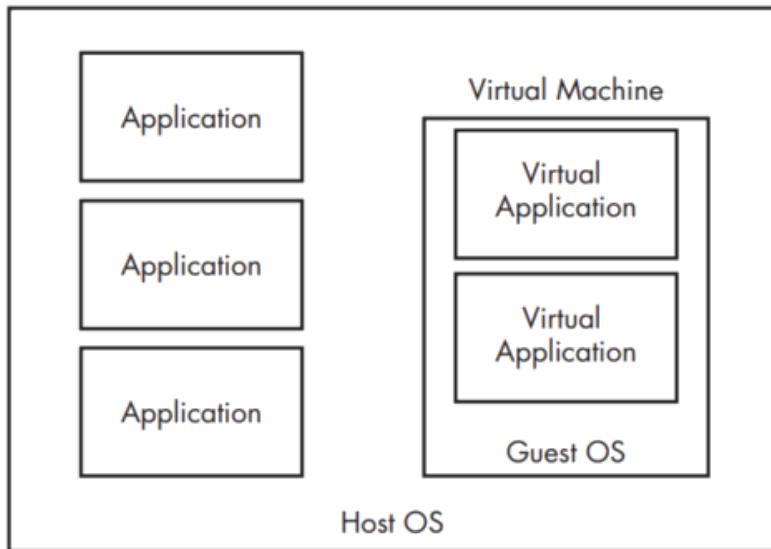


Thiết lập môi trường thực hành

Lab requirements

- Virtualization software (VMware or VirtualBox)
- Tools for analyzing + Snapshot tool
- Malware samples
- Sandbox

Physical Machine



Malware sources

- Hybrid Analysis:** <https://www.hybrid-analysis.com/>
- KernelMode.info:** <http://www.kernelmode.info/forum/viewforum.php?f=16>
- VirusBay:** <https://beta.virusbay.io/>
- Contagio malware dump:** <http://contagiodump.blogspot.com/>
- AVCaesar:** <https://avcaesar.malware.lu/>
- Malwr:** <https://malwr.com/>
- VirusShare:** <https://virusshare.com/>
- theZoo:** <http://thezoo.morirt.com/>

Tham khảo: phần 5 chapter 1.

Monnappa, K. A. (2018). *Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware*. Packt Publishing Ltd.

Bài tập

- Tìm mỗi loại mã độc đã học 1 mẫu. Phân tích nguồn gốc, chức năng, cách hoạt động của nó
- Tìm hiểu cách dựng được môi trường để phân tích mã độc. Thực hiện chạy 3 mẫu mã độc và đưa ra kết quả.