

Malware Hunting 101

Sun* Cyber Security Research



I. Tổng quan

Kiến thức cơ bản về:

- Hệ điều hành Windows
- Mã độc và các con đường lây lan của chúng
- Các bước tìm diệt mã độc
- Cách sử dụng một số công cụ trong bộ Sysinternals để tìm diệt mã độc

Nội dung chính:

- Windows Core Concepts
- Malware 101
- Sysinternals Suite
- Case Study

II. Windows Core Concepts

● Administrative Rights

Accounts trong Windows thường được chia thành hai loại chính:

- Administrator
- User

Administrator:

- Toàn quyền truy cập vào các tài nguyên của máy tính

User:

- Được phép truy cập đến một số tài nguyên nhất định, giới hạn truy cập đến các khu vực nhạy cảm

- **Windows Services**

Là một trong những thành phần chính của Windows, cho phép tạo và quản lý các process chạy trong thời gian dài.

Là các process chạy nền, thường khởi động khi máy tính khởi động.

Các services làm nhiều nhiệm vụ khác nhau, chẳng hạn: quản lý network connection, speaker sound, backup data,...

Được quản lý bởi Windows Services Control Manager.

Một số Windows Services:

- Active Directory Service
- DNS Client Service
- Remote Desktop Service
- ...

- **DLLs**

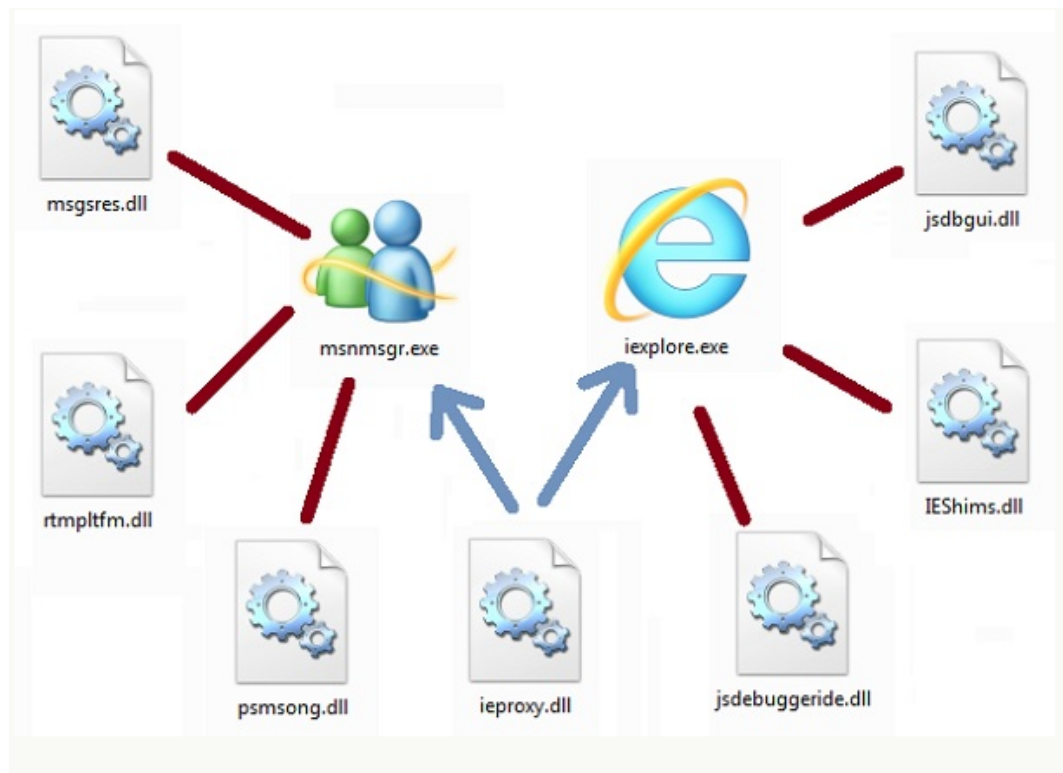
Dynamic Link Library

Là các chương trình nhỏ, có thể được các chương trình lớn hơn gọi lên và sử dụng khi cần

DLL không thể chạy trực tiếp mà phải được gọi bởi các chương trình khác

Ví dụ:

- Msvcrt dll
- Kernel32 dll



- **Programs, Processes, Threads**

Program (chương trình): là dãy các tập lệnh ở trạng thái tĩnh

Process (tiến trình): Khi chương trình được nạp vào RAM và CPU bắt đầu thi hành chương trình ở điểm nhập thì chương trình trở thành process, CPU thực thi hết lệnh này đến lệnh khúc từ trên xuống hay theo sự điều khiển của lệnh đang thực thi.

Process bao gồm:

- Process ID (PID)
- Ít nhất một thread
- Virtual Address Space
- Executable Code
- Open handles

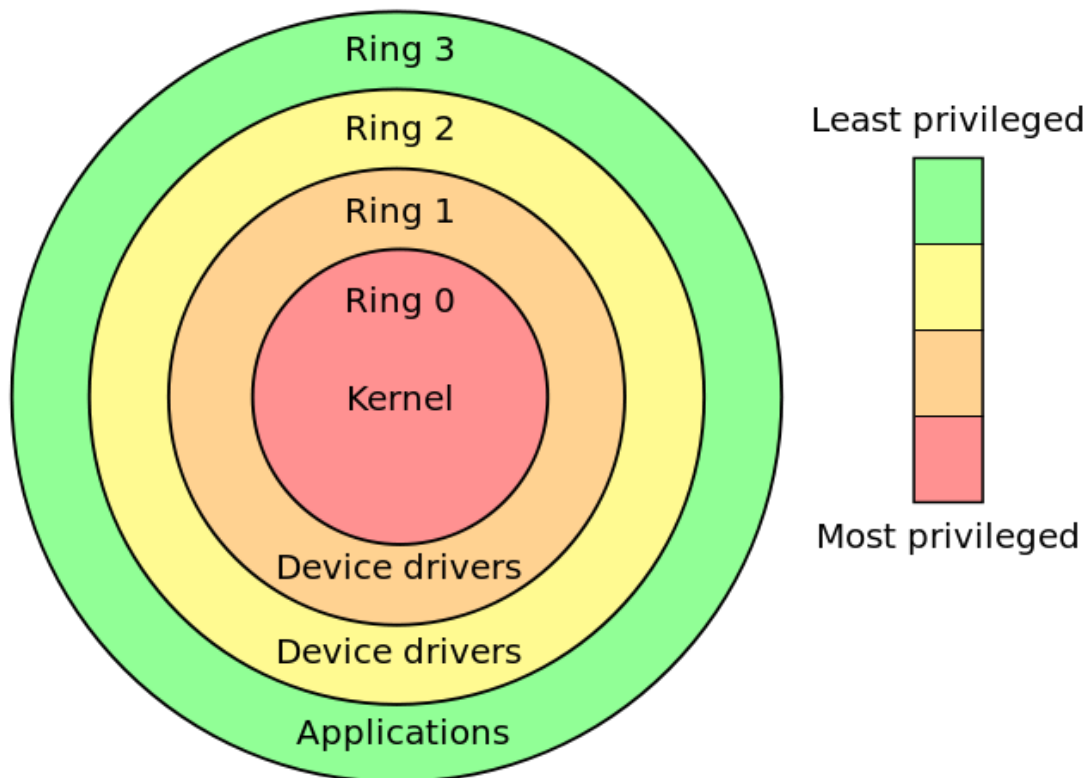
Thread:

Là một thành phần của process, có thể thực hiện một hoặc một vài chức năng một cách độc lập

- **User Mode, Kernel Mode**

Processor ở Windows chạy ở 2 chế độ: User Mode (ring 3) và Kernel Mode (ring 0)

- Phần lớn các ứng dụng chạy ở User Mode: chỉ được truy cập vào một số tài nguyên nhất định của hệ thống
- Các thành phần cốt lõi của hệ điều hành chạy ở Kernel Mode: toàn quyền truy cập vào các tài nguyên của hệ thống



- **User mode**

Các tiến trình của chế độ User mode phải được chế độ kernel mode cấp quyền trước khi thực thi.

Có khả năng truyền các yêu cầu I/O đến chế độ kernel mode phù hợp.

Được điều khiển bởi hệ thống quản lý vào/ra (I/O Manager)

Giao diện điều hành, với tất cả hệ thống con của chế độ User mode, xử lý các công việc liên quan tới vào ra, quản lý đối tượng, bảo mật và quản lý tiến trình.

- **Kernel mode**

Toàn quyền truy cập tới phần cứng và tài nguyên hệ thống.

Chạy các dòng mã trong vùng nhớ được bảo vệ.

Xác định luồng ưu tiên, quản lý bộ nhớ và làm việc với phần cứng.

Chế độ kernel mode ngăn các dịch vụ và ứng dụng của chế độ User mode vào việc truy cập tới vùng tài nguyên nguy hiểm.

- **Objects & Handles**

Object: là một cấu trúc dữ liệu biểu diễn tài nguyên của hệ thống, chẳng hạn file, thread,...

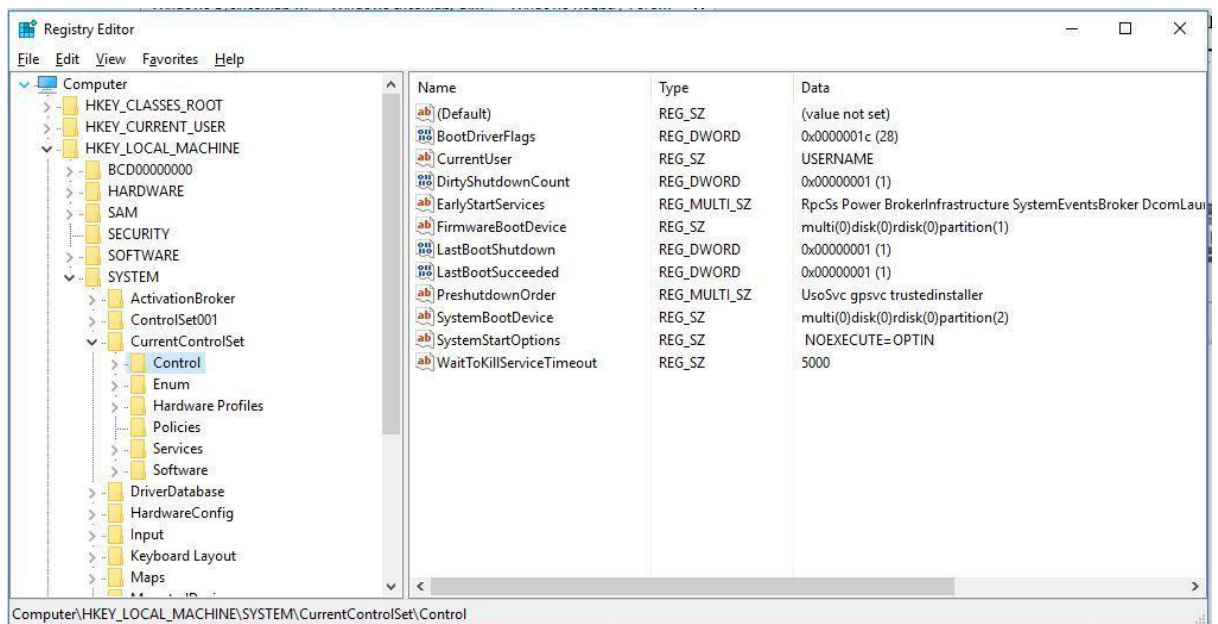
Ứng dụng (application) không thể truy cập trực tiếp đến các tài nguyên trên mà phải thông qua một object handle

- **Registry**

Thành phần rất quan trọng trong hệ điều hành Windows

Là cơ sở dữ liệu dùng để lưu trữ thông tin về những sự thay đổi, những lựa chọn, những cấu hình từ người sử dụng Windows. Registry bao gồm tất cả các thông tin về phần cứng, phần mềm, người sử dụng

Lưu trữ các thông tin cấu hình của Windows



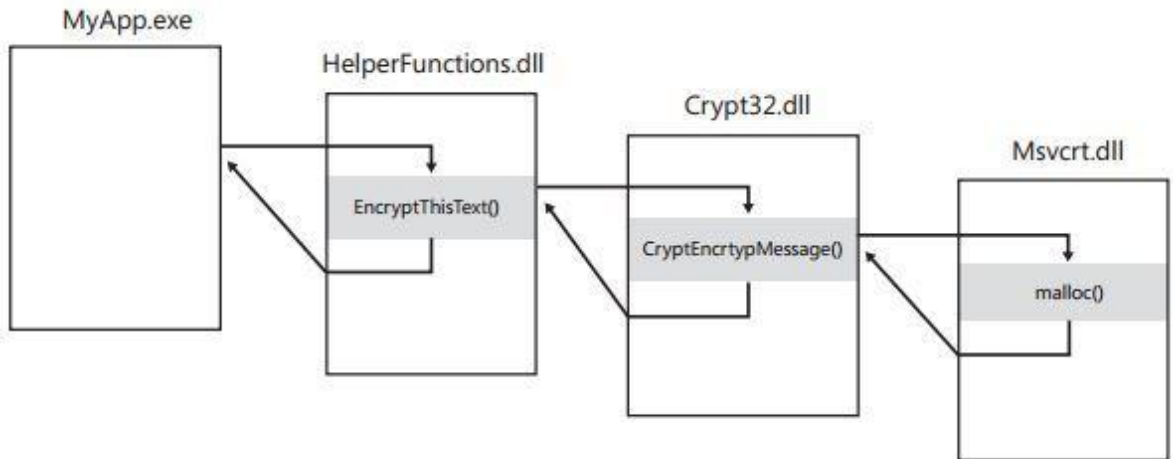
- **Call Stacks**

Chương trình thường gồm các function được sắp xếp rời rạc

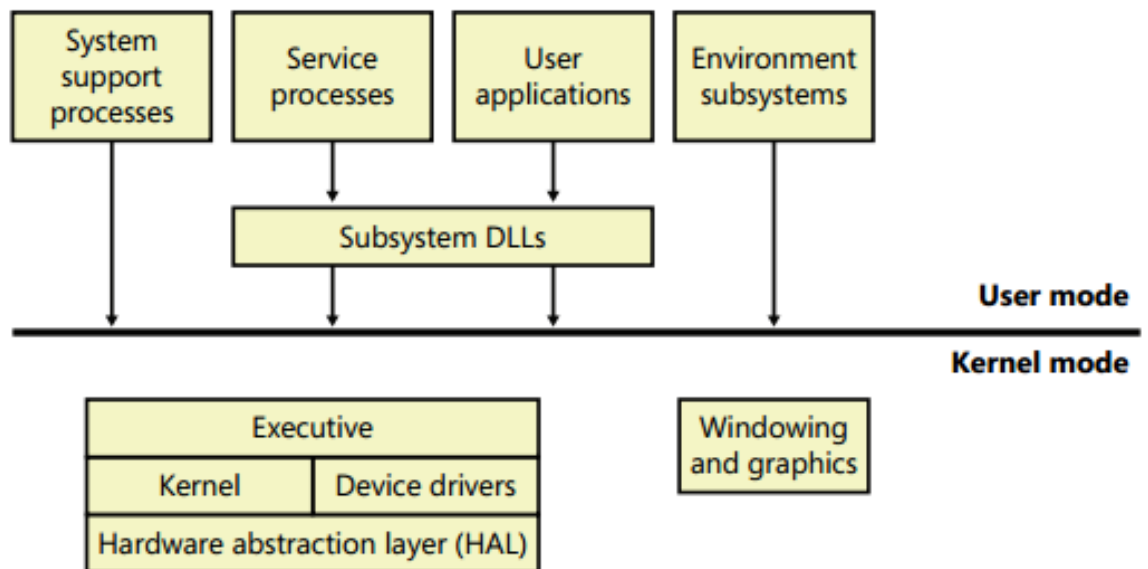
Để thực hiện chức năng của mình, một function có thể phải gọi đến các function khác.

Sau khi function kết thúc, nó trả điều khiển về cho function gọi nó

Call stacks là một cấu trúc dữ liệu lưu trữ thông tin về dãy các lời gọi này



- **Windows architecture**



- **User mode components**

System support processes (Include services not provided as a part of OS, logon process and session manager)

Service processes (other windows services: event logger)

User applications(Windows 64-bit, 32-bit, MS DOS..)

Environment subsystem server processes(includes DLLs that convert the user application calls to Windows call)

- **Kernel mode components**

Executive (Memory management, Process management, Thread management...)

Kernel

Device drivers (Include both file system and hardware drivers that translate user I/O function calls into specific hardware device I/O request)

Hardware abstraction layer (HAL)

Windowing and graphics system

III. Malware 101

1. Malware là gì?

Malware (mã độc) là bất kỳ phần mềm nào cố gắng lây nhiễm vào các thiết bị kỹ thuật số (PC, Laptop, Tablet, Smartphone,...), với mục tiêu là đánh cắp thông tin cá nhân, đánh cắp tiền bạc, phá hủy, làm hư hại hệ thống.

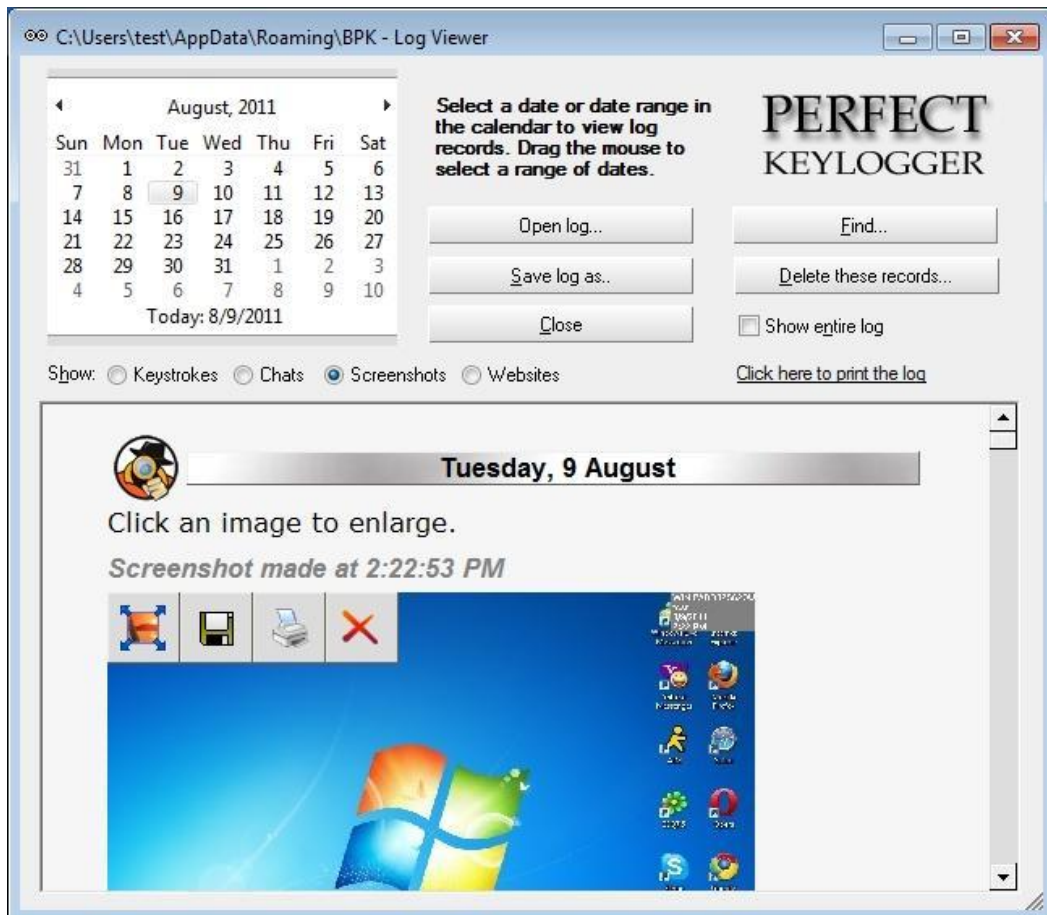
Malware bao gồm rất nhiều loại: spyware, adware, viruses, Trojan horses, worms, rootkits, ransomware,...

2. Một số loại malware cơ bản

• Spyware

Là một loại malware, được các hackers sử dụng để thu thập thông tin cá nhân (thói quen sử dụng máy tính, lịch sử duyệt web, tài khoản ngân hàng,...). Các thông tin này sẽ được cung cấp cho một bên thứ ba mà nạn nhân không hề hay biết.

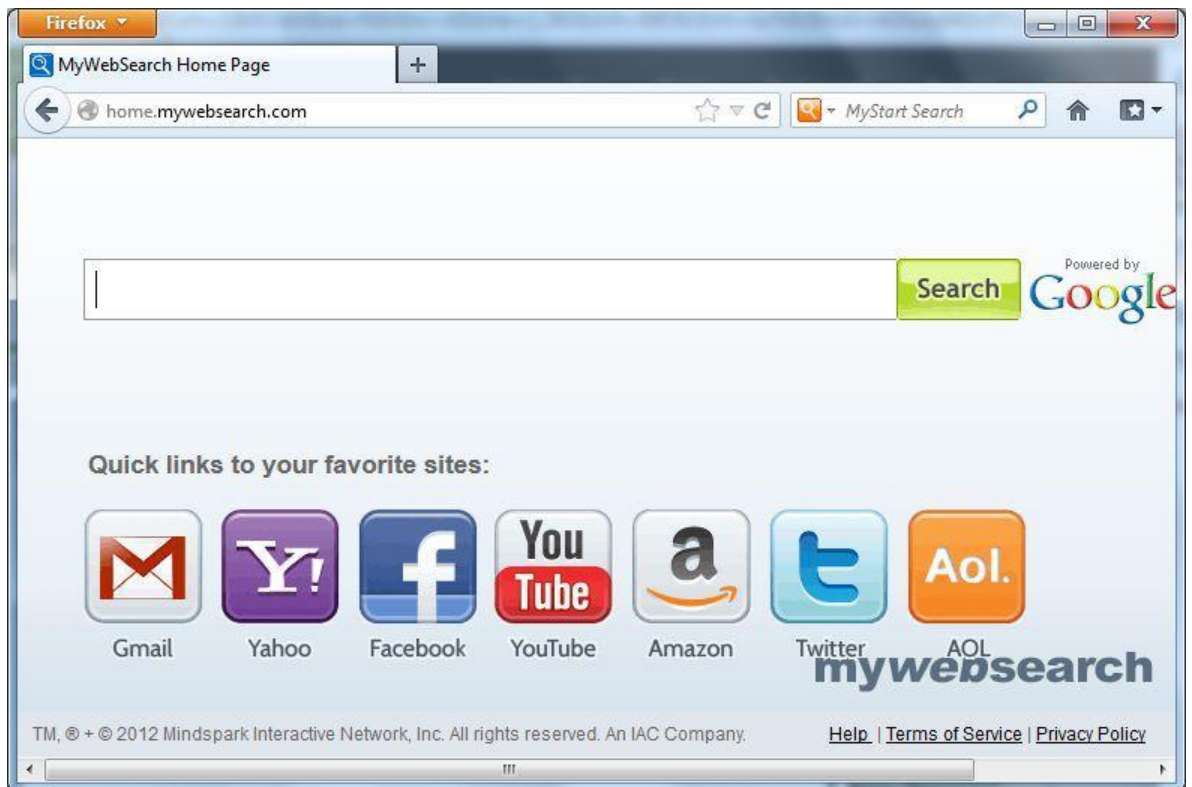
Spyware thường được đi kèm với một phần mềm thông thường khác, hoặc một file download từ các trang web chia sẻ (chẳng hạn các trang download nhạc, phim, phần mềm miễn phí...), hoặc cũng có thể xuất hiện trong các file đính kèm trong email.



• Adware

Là loại phần mềm gây phiền nhiễu bằng cách hiển thị hàng loạt các quảng cáo không mong muốn, chẳng hạn các cửa sổ pop-ups hiện ra khi duyệt web,...

Tương tự spyware, adware cũng được đính kèm trong các phần mềm miễn phí, hoặc cũng có thể được cài đặt vào máy tính nạn nhân thông qua lỗ hổng của trình duyệt hoặc hệ điều hành.



- **Virus**

Là một chương trình hoặc một đoạn mã được tải vào máy tính mà nạn nhân không hề hay biết. Một số virus chỉ gây phiền toái, tuy nhiên, hầu hết chúng được thiết kế để lây nhiễm và chiếm quyền điều khiển các hệ thống có lỗi hổng.

Virus có thể lây lan qua các máy tính trong mạng bằng cách tự sao chép chính mình.

Virus thường ẩn mình trong một số phần mềm phổ biến (ví dụ: game hoặc chương trình PDF viewer), hoặc cũng có thể đến từ các file đính kèm trong email, các file được chia sẻ qua các kênh truyền thông (facebook, skype, messenger,...)



- **Trojan**

Là một loại malware tồn tại dưới dạng một phần mềm hữu ích, trong khi mục đích chính của nó là gây hại hoặc đánh cắp dữ liệu. Trojan thường âm thầm download và cài đặt các mã độc khác vào máy tính nạn nhân (ví dụ: spyware, adware, ransomware,...).

Trojan cũng thường ẩn mình trong các file đính kèm email hoặc các phần mềm miễn phí.



Trojan Zeus: Một khi hệ thống bị nhiễm Zeus, tất cả mật khẩu đều bị lộ, những tổ hợp phím bị theo dõi và thói quen dùng web (các form nhập dữ liệu, form đăng nhập...) có thể bị can thiệp nhằm thu thập thông tin cá nhân

- **Worm**

Là một chương trình máy tính tự sao chép chính nó, xâm nhập vào máy tính và lây lan sang các máy tính khác trong cùng mạng.

Nhiều loại worm được thiết kế chỉ với mục đích lây lan, nhưng cũng có loại có khả năng phá hủy hệ thống bị nhiễm.

Worm được lây lan chủ yếu qua các file đính kèm, mạng chia sẻ file hoặc các đường link trên các trang mạng xã hội, các phần mềm chat (facebook, skype, messenger,...)

- **Rootkit**

Là một chương trình được thiết kế nhằm mục đích che giấu sự tồn tại của một phần mềm khác, thường là virus. Một khi đã được cài đặt, rootkit sẽ "ngụy trang" bản thân sao cho các phần mềm diệt virus thông thường khi quét qua chỉ thấy nó một ứng dụng vô hại. Rootkit là một trong những loại malware khó bị phát hiện nhất.

- **Ransomware**

Là một loại malware được thiết kế để mã hóa dữ liệu của nạn nhân. Nếu máy tính bị nhiễm ransomware, dữ liệu của nạn nhân sẽ bị mã hóa, và hầu như không thể giải mã được nếu không trả tiền cho hacker. Một số ransomware nguy hiểm có thể kể đến như: CryptoLocker, WannaCry, Petya,...



Ransomware Wannacry: Loại malware mã hóa toàn bộ file của người dùng và tổng tiền Bitcoin

- **Browser hijackers**

Là loại malware làm thay đổi các cấu hình của trình duyệt, chuyển hướng nạn nhân đến các trang web mà nạn nhân không hề có ý định truy cập.

Hầu hết các browser hijackers ẩn mình dưới dạng những tiện ích mở rộng (browser extension).

3. Các con đường lây nhiễm

- Thường đi kèm với các phần mềm không rõ nguồn gốc (phần mềm lậu, các bản crack, một số phần mềm miễn phí,...)
- File đính kèm trong email
- Click vào các files, đường dẫn bất thường qua Facebook, Skype,...
- Qua máy tính bị nhiễm nằm trong cùng mạng

4. Cách phòng tránh

- Cài đặt phần mềm Anti-virus
- Thường xuyên update các phần mềm sử dụng lên phiên bản mới nhất
- Cẩn thận với các files đính kèm trong email
- Không click vào các đường link lạ trên facebook, skype, messenger
- Không sử dụng các phần mềm lậu, phần mềm crack

5. Phương pháp phân tích malware

- Phương pháp phân tích tĩnh: Phân tích dựa vào đặc điểm, dấu hiệu, source code của malware:
 - Mã hash

- Pattern code
- String
- Assembly code
- File struct
- Digital signature
- Packer, Bulder, Programming language...
- Phương pháp phân động Phân tích quá trình malware khởi động, chạy và các hành vi liên quan trong quá trình malware thực thi trong môi trường sandbox.

IV. Sysinternal Suite (Microsoft)

1. Giới thiệu bộ công cụ Sysinternal Suite (Microsoft)



- Sysinternals là tập hợp hơn 70 công cụ giúp giải quyết các vấn đề thường gặp đối với hệ điều hành windows.
- Được viết bởi tác giả chính là Mark Russinovich, một trong những chuyên gia hàng đầu của Microsoft, hiện là CTO của Microsoft Azure.
- Sysinternals giúp:
 - Xử lý các sự cố đối với Windows
 - Giám sát hệ thống
 - Tìm và xử lý malware

2. Các bước xử lý malware cơ bản

2.1. Ngắt kết nối máy tính khỏi mạng

2.2. Xác định các malicious processes

- **Tập trung vào các processes...**
 - Không có icon
 - Không có description hoặc computer name
 - Không được verified bởi Microsoft
 - Tồn tại trong folder của Windows hoặc user profile
 - Được đóng gói
 - Chứa các URLs lạ
 - Tự động mở port và connect đến các máy khác trong mạng
 - Chứa các DLLs hoặc services khả nghi
- **Task manager:** Cung cấp thông tin các process đang chạy trên hệ thống:

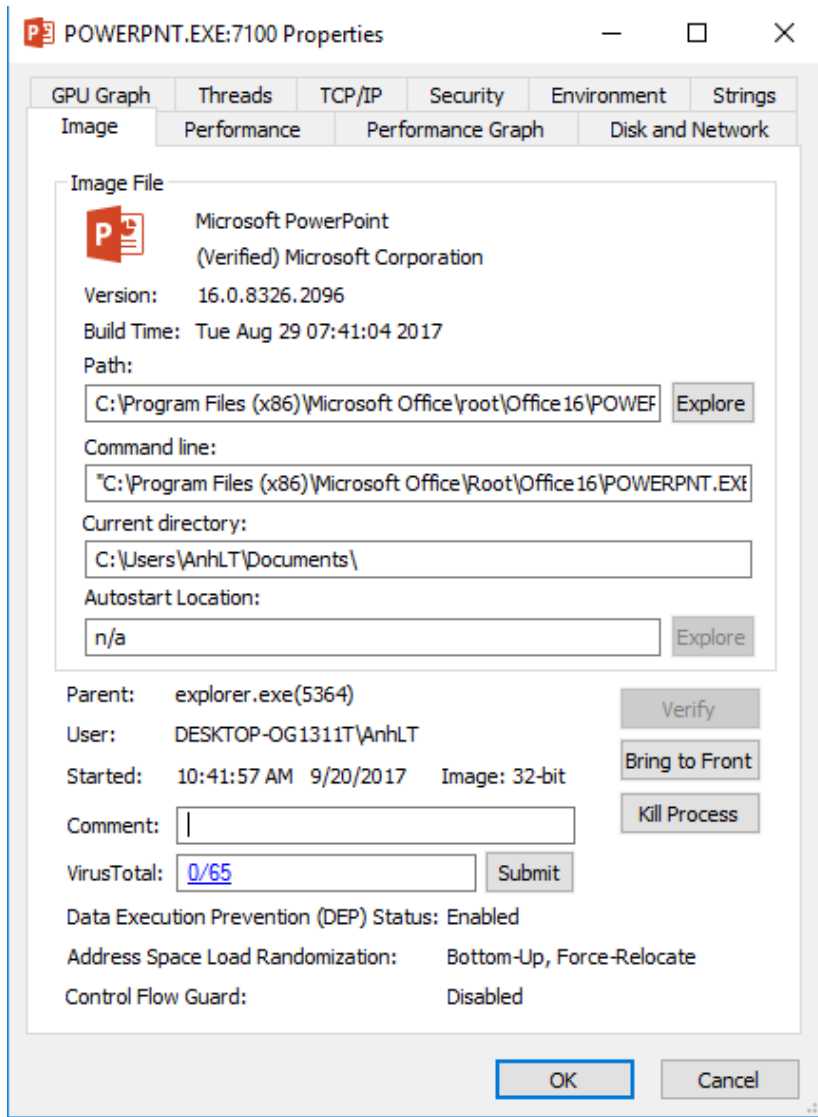
| Name | CPU | Memory | Disk | Netv |
|--|------|----------|----------|------|
| Cortana | 5.7% | 68.3 MB | 1.2 MB/s | 0. |
| > Foxit Reader 8.0, Best Reader for Everyday Use! (32 bit) | 2.9% | 40.9 MB | 0 MB/s | |
| Windows Audio Device Graph Isolation | 2.6% | 13.5 MB | 0 MB/s | |
| Google Chrome | 2.6% | 266.0 MB | 0 MB/s | |
| > Microsoft Windows Search Indexer | 2.1% | 15.8 MB | 3.3 MB/s | |
| > Task Manager | 1.7% | 13.7 MB | 0 MB/s | |
| Shell Infrastructure Host | 1.7% | 5.2 MB | 0 MB/s | |
| > Service Host: DCOM Server Process Launcher (6) | 1.7% | 6.8 MB | 0 MB/s | |

- **Process Explorer:** Là “Super Task Manager” giúp cung cấp thêm thông tin các process đang chạy trên hệ thống:
 - Process tree
 - Icon, description, company name
 - Search Online
 - Check virustotal
 - Verify image
 - ...

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|------------------------|---------|---------------|-------------|-------|------------------------------|--------------|
| audiodg.exe | 1.77 | 32,448 K | 25,280 K | 11412 | | |
| csrss.exe | 0.01 | 2,040 K | 5,016 K | 592 | | |
| csrss.exe | 0.51 | 2,500 K | 8,900 K | 692 | | |
| dasHost.exe | | 1,240 K | 4,728 K | 1720 | | |
| dwm.exe | 0.74 | 81,256 K | 80,572 K | 380 | | |
| esif_assist_64.exe | < 0.01 | 1,520 K | 4,452 K | 5644 | | |
| ETDCtrlHelper.exe | 0.06 | 2,784 K | 7,972 K | 5988 | | |
| fontdrvhost.exe | | 804 K | 2,576 K | 8668 | | |
| Intempts | 0.70 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | |
| Memory Compression | < 0.01 | 1,404 K | 455,888 K | 3572 | | |
| nvsvsc.exe | < 0.01 | 5,116 K | 13,892 K | 1408 | | |
| nvxdsync.exe | | 7,588 K | 20,336 K | 1400 | | |
| RAVBg64.exe | | 5,892 K | 10,480 K | 2284 | | |
| RAVBg64.exe | | 5,584 K | 9,816 K | 2320 | | |
| SearchFilterHost.exe | | 1,448 K | 6,648 K | 15564 | | |
| SearchProtocolHost.exe | | 2,348 K | 8,468 K | 4712 | | |
| services.exe | | 3,664 K | 6,996 K | 876 | | |
| smss.exe | | 392 K | 1,088 K | 424 | | |
| System | 0.47 | 128 K | 140 K | 4 | | |
| System Idle Process | 90.77 | 0 K | 4 K | 0 | | |
| taskhostw.exe | | 9,936 K | 19,972 K | 4008 | | |
| wininit.exe | | 1,064 K | 4,456 K | 716 | | |
| winlogon.exe | | 2,208 K | 9,244 K | 776 | | |
| WmiPrvSE.exe | | 12,724 K | 11,956 K | 4168 | | |
| WUDFHost.exe | | 25,208 K | 14,316 K | 1132 | | |
| WUDFHost.exe | < 0.01 | 2,664 K | 10,184 K | 1748 | | |
| UniKeyNT.exe | 0.12 | 2,208 K | 9,580 K | 8536 | | |
| Video.UI.exe | Susp... | 75,168 K | 81,224 K | 12324 | | |
| SkypeHost.exe | | | | | | |

CPU Usage: 9.23% Commit Charge: 64.04% Processes: 156 Physical Usage: 63.59%

- **Process Detail:** Double click vào một process để xem thông tin chi tiết:
 - Image: chữ ký, version,...
 - Path
 - Command line
 - Autostart location
 - ...



- **VirusTotal check:** Sử dụng virustotal để kiểm tra tiến trình

| Process | VirusTotal |
|--------------------|--|
| Memory Compression | The system cannot find the file specified. |
| UniKeyNT.exe | 4/64 |
| Video.UI.exe | 1/65 |
| WUDFHost.exe | 0/65 |
| WUDFHost.exe | 0/65 |
| WmiPrvSE.exe | 0/65 |
| WINWORD.EXE | 0/65 |
| winlogon.exe | 0/65 |
| wininit.exe | 0/65 |




Analyze suspicious files and URLs to detect types of malware including viruses, worms, and trojans.

File

URL

Search



Upload and scan file

By using VirusTotal you consent to our [Terms of Service](#) and [Privacy Policy](#) and allow us to share your submission with the security community. [Learn more.](#)

- DLL view: Malware có thể ẩn nấp dưới dạng một DLL bên trong một process hợp lệ:
 - Thường ẩn nấp sau các process svchost, rundll32,...
 - Load thông qua autostart
 - Load thông qua "dll injection"

2.3. Terminate các processes xác định ở trên

- Không kill process: Malware có thể tự động restart nếu malicious process bị terminate
- Thay vào đó, hãy suspend: Chú ý: có thể dẫn đến treo hệ thống

2.4. Xác định và xóa malware autostarts

- Task manager -> Startup
- Sử dụng: Autoruns: Hiển thị mọi vị trí trong hệ thống được config để chạy lúc khởi động máy tính
 - Run keys & Startup folders
 - Shell, userinit

- Services & drivers
- Tasks
- Winlogon notifications
- **Xác định Malware Autostart**
Sử dụng các tính năng:
 - Verify image
 - Submit to VirusTotal
 Sử dụng filters:
 - Hide Microsoft Entries
 - Hide VirusTotal Clean Entries

2.5. Tracing malware activities

- **Process Monitor**: Là công cụ theo dõi hoạt động của các process trong hệ thống:
 - Xác định mọi thay đổi xảy ra trong hệ thống
 - Nhận biết các hoạt động bất thường
 - Chỉ ra nguyên nhân của các thông báo lỗi
 - Chỉ các vấn đề khiến cho hệ thống bị chậm
 - ...
- **Process Monitor**: Là công cụ theo dõi hoạt động của các process trong hệ thống:
 - Registry
 - File System
 - Network
 - Process
- **Event Properties**
 - Event details
 - Process Information
 - Thread stack

2.6. Xóa file malware

- Thực hiện loại bỏ malware phát hiện được ở các bước trên

2.7. Reboot và lặp lại các bước trên

- Thực hiện cho đến khi malware được xử lý hoàn toàn