

BÁO CÁO BÀI TẬP

Môn học: Kỹ thuật phân tích mã độc

Tên chủ đề: BÀI THỰC HÀNH SỐ 2

GVHD: Ngô Đức Hoàng Sơn

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT137.Q11.ANTT.1

ST T	Họ và tên	MSSV	Email
1	Tù Chí Kiên	22520713	22520713@gm.uit.edu.vn
2	Hà Minh Quân	22521177	22521177@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Các tiến trình nào mới được tạo ra bởi mã độc? Mã độc có tạo ra các tiến trình con không?	100%
2	Mã độc kết nối đến những địa chỉ IP hoặc tên miền nào? Bạn có xác định được hoạt động truyền dữ liệu hoặc giao tiếp C2 không?	100%
3	Hãy tìm hiểu ransomware Dharma và miêu tả lại hành vi thu thập thông tin hệ thống của chúng.	100%
4	Sử dụng AutoRun để kiểm tra có Persistence trên các Register Key	100%
5	Sử dụng PowerShell để phát hiện và xác minh các cơ chế Persistence của phần mềm độc hại.	100%
6	Sử dụng đoạn script tự code ở YC 5. Hãy trả lời các câu hỏi.	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc

1. Các tiến trình nào mới được tạo ra bởi mã độc? Mã độc có tạo ra các tiến trình con không?.....	3
2. Mã độc kết nối đến những địa chỉ IP hoặc tên miền nào? Bạn có xác định được hoạt động truyền dữ liệu hoặc giao tiếp C2 không?.....	3
3. Hãy tìm hiểu ransomware Dharma và miêu tả lại hành vi thu thập thông tin hệ thống của chúng.	3
4. Sử dụng AutoRun để kiểm tra có Persistence trên các Register Key	4
5. Sử dụng PowerShell để phát hiện và xác minh các cơ chế Persistence của phần mềm độc hại.....	5
6. Sử dụng đoạn script tự code ở YC 5. Hãy trả lời các câu hỏi sau:.....	7

BÁO CÁO CHI TIẾT

1. Các tiến trình nào mới được tạo ra bởi mã độc? Mã độc có tạo ra các tiến trình con không?

Ở procwatch thì không tìm thấy tiến trình nào mới, có thể do mã độc không thực thi thành công trên máy nạn nhân.

Start	End	PID	PPID	User	CmdLine	path *
03:36:31	03:36:34	1A58	2F4	fare-vm		C:\Windows\System32\backgroundTaskHost.exe
03:36:31		1B64	C68	SYSTEM		C:\Windows\System32\SearchProtocolHost.exe
03:36:31	03:38:36	1640	C68	SYSTEM		C:\Windows\System32\SearchFilterHost.exe
03:36:34	03:37:15	1988	2F4	fare-vm		C:\Windows\System32\RuntimeBroker.exe
03:36:35	03:37:15	15A0	2F4	fare-vm		C:\Windows\System32\RuntimeBroker.exe
03:36:55	03:37:00	1D90	2F4	fare-vm		C:\Windows\System32\dllhost.exe
03:37:19	03:38:27	850	2F4	fare-vm		C:\Windows\System32\backgroundTaskHost.exe
03:37:19	03:37:55	1CF0	0	NETWORK SE...		

2. Mã độc kết nối đến những địa chỉ IP hoặc tên miền nào? Bạn có xác định được hoạt động truyền dữ liệu hoặc giao tiếp C2 không?

Mã độc kết nối đến tên miền magnificentpakistan.com nhưng không kết nối đến được trả về không tồn tại tên miền.

52 5.408369	89.39.246.14	192.168.248.138	HTTP	547 HTTP/1.1 200 OK (text/html)
53 5.408506	192.168.248.138	89.39.246.14	TCP	54 49929 → 80 [ACK] Seq=71 Ack=12150 Win=64240 Len=0
54 5.515108	192.168.248.138	192.168.248.2	DNS	83 Standard query 0x232a A magnificentpakistan.com
55 5.558845	192.168.248.2	192.168.248.138	DNS	159 Standard query response 0x232d No such name A magnificentpakistan.com SOA A.gtl-servers.net
56 5.612279	192.168.248.138	192.168.248.2	DNS	73 Standard query 0xe0df A www.qwqoo.com
57 5.708475	192.168.248.2	192.168.248.138	DNS	89 Standard query response 0xe0df A www.qwqoo.com A 38.38.14.29
58 5.709374	192.168.248.138	38.38.14.29	TCP	66 49930 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
59 5.892208	38.38.14.29	192.168.248.138	TCP	60 443 → 49930 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
60 5.892292	192.168.248.138	38.38.14.29	TCP	54 49930 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0

Do vậy, không có thiết lập kết nối C2, có thể ngay cả việc mã độc cũng không được tải xuống máy nạn nhân.

3. Hãy tìm hiểu ransomware Dharma và miêu tả lại hành vi thu thập thông tin hệ thống của chúng.

Theo thông tin của <https://www.acronis.com/en/blog/posts/dharma-ransomware/>

Dharma ransomware là loại mã độc tống tiền được phát tán một cách thủ công thông qua kết nối từ xa (RDP), thường qua cách khai thác thông tin bị rò rỉ.

Hành vi thu thập thông tin:

Bước cài đặt:

Sử dụng biến %System% để tìm vị trí thư mục System.

Sau khi sử dụng kỹ thuật persistent qua run key, tìm kiếm thư mục Startup sử dụng %AppData%\Microsoft\Windows\Start Menu\Programs\Startup để copy mã độc và.

Tìm các thư mục Startup khác qua tham số "Common Startup" trong 2 key:
 [HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders],
 [HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders]

Payload:

Tìm kiếm và dừng các dịch vụ FirebirdGuardianDefaultInstance, FirebirdServerDefaultInstance, sqlwriter, mssqlserver, sqlserveradhelper , 1c8.exe, 1cv77.exe, outlook.exe, postgres.exe, mysqld-nt.exe, mysqld.exe, sqlservr.exe.

Lấy thông tin của số serial của ổ đĩa hệ thống sử dụng hàmGetVolumeInformationW()

Thực hiện tìm kiếm để quy các tệp trên tất cả các ổ đĩa logic và kiểm tra xem chúng có nằm trong %WinDir% hay không.

Tìm kiếm các tất cả những tài nguyên mạng

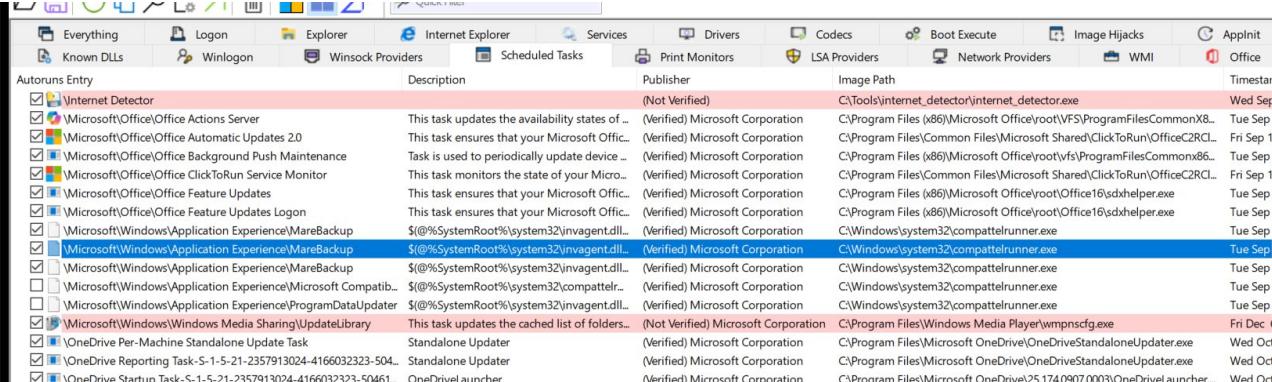
4. Sử dụng AutoRun để kiểm tra có Persistence trên các Register Key

Do mã độc không tồn tại trên máy nên cũng không có gì thay đổi.

Register WinLogon cũng không có gì.

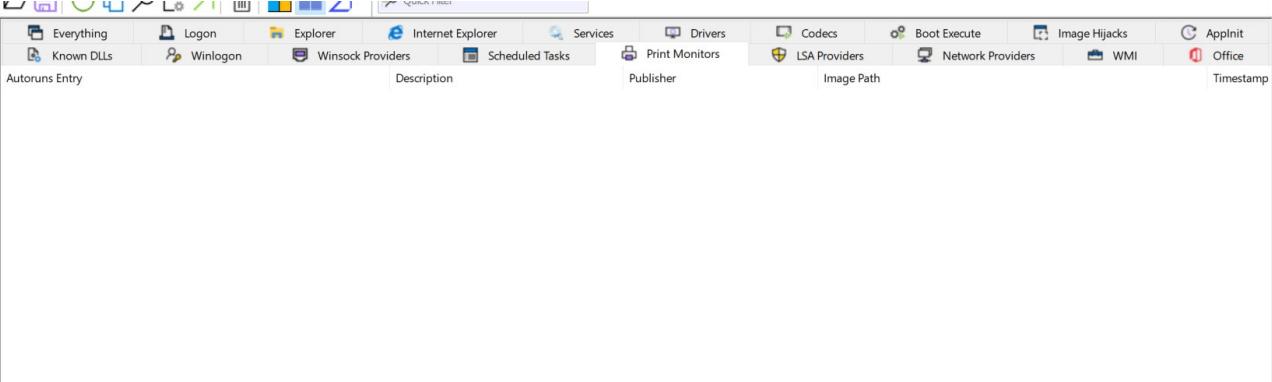
Autoruns Entry	Description	Publisher	Image Path	Timestamp
Known DLLs				

Scheduled Tasks cũng không có gì đáng nghi.



Autoruns Entry	Description	Publisher	Image Path	Timestamp
<input checked="" type="checkbox"/> Internet Detector	(Not Verified)		C:\Tools\internet_detector\internet_detector.exe	Wed Sep
<input checked="" type="checkbox"/> Microsoft\Office\Office Actions Server	This task updates the availability states of ...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX8...	Tue Sep
<input checked="" type="checkbox"/> Microsoft\Office\Office Automatic Updates 2.0	This task ensures that your Microsoft Offic...	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RCL...	Fri Sep 1
<input checked="" type="checkbox"/> Microsoft\Office\Office Background Push Maintenance	Task is used to periodically update device ...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\vfs\ProgramFilesCommonx86...	Tue Sep
<input checked="" type="checkbox"/> Microsoft\Office\Office ClickToRun Service Monitor	This task monitors the state of your Micro...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft Shared\ClickToRun\OfficeC2RCL...	Fri Sep 1
<input checked="" type="checkbox"/> Microsoft\Office\Office Feature Updates	This task ensures that your Microsoft Offic...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\Office10\sdxhelper.exe	Tue Sep
<input checked="" type="checkbox"/> Microsoft\Office\Office Feature Updates Logon	This task ensures that your Microsoft Offic...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\Office10\sdxhelper.exe	Tue Sep
<input checked="" type="checkbox"/> Microsoft\Windows\Application Experience\MarBackup	\$(@%SystemRoot%\system32\invagent.dll...	(Verified) Microsoft Corporation	C:\Windows\system32\compttelrunner.exe	Tue Sep
<input checked="" type="checkbox"/> Microsoft\Windows\Application Experience\MarBackup	\$(@%SystemRoot%\system32\invagent.dll...	(Verified) Microsoft Corporation	C:\Windows\system32\compttelrunner.exe	Tue Sep
<input checked="" type="checkbox"/> Microsoft\Windows\Application Experience\Microsoft Compatib...	\$(@%SystemRoot%\system32\compttel...	(Verified) Microsoft Corporation	C:\Windows\system32\compttelrunner.exe	Tue Sep
<input checked="" type="checkbox"/> Microsoft\Windows\Application Experience\ProgramData\Update...	\$(@%SystemRoot%\system32\invagent.dll...	(Verified) Microsoft Corporation	C:\Windows\system32\compttelrunner.exe	Tue Sep
<input checked="" type="checkbox"/> Microsoft\Windows\Windows Media Sharing\UpdateLibrary	This task updates the cached list of folders...	(Not Verified) Microsoft Corporation	C:\Program Files\Windows Media Player\wmprnscfg.exe	Fri Dec 1
<input checked="" type="checkbox"/> OneDrive Per-Machine Standalone Update Task	Standalone Updater	(Verified) Microsoft Corporation	C:\Program Files\Microsoft OneDrive\OneDriveStandaloneUpdater.exe	Wed Oct
<input checked="" type="checkbox"/> OneDrive Reporting Task-S-1-5-21-2357913024-4166032323-504...	Standalone Updater	(Verified) Microsoft Corporation	C:\Program Files\Microsoft OneDrive\OneDriveStandaloneUpdater.exe	Wed Oct
<input checked="" type="checkbox"/> OneDrive Startup Task-S-1-5-21-2357913024-4166032323-50461...	OneDriveLauncher	(Verified) Microsoft Corporation	C:\Program Files\Microsoft OneDrive\25.174.0907.0003\OneDriveLauncher...	Wed Oct

Print cũng không có tiến trình thêm.



Autoruns Entry	Description	Publisher	Image Path	Timestamp

5. Sử dụng PowerShell để phát hiện và xác minh các cơ chế Persistence của phần mềm độc hại.

Kiểm tra Registry Run

```
$Registry_path = @(
    'HKLM:\Software\Microsoft\Windows\CurrentVersion\Run'
    'HKCU:\Software\Microsoft\Windows\CurrentVersion\Run'
    'HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce'
    'HKCU:\Software\Microsoft\Windows\CurrentVersion\RunOnce'
)
```

Write-Host "1.Listing key" -ForegroundColor Blue

```
#https://stackoverflow.com/questions/66528639/how-to-iterate-through-an-array-of-objects-in-powershell
```

```
ForEach ($Path in $Registry_path){
```

```
#https://stackoverflow.com/questions/2038181/how-to-output-something-in-powershell
```

```

Write-Host "Listing all key name and value in $Path" -ForegroundColor Yellow
Write-Host "Start-----"
try{
    #https://www.reddit.com/r/PowerShell/comments/9lpsmo/how_to_use_invokecomm
    #and_for_getitemproperty/
    Get-ItemProperty -Path $Path
}
catch{
    Write-Host "Path $Path not found"
}
Write-Host "End-----"
}

```

Kiểm tra nhiệm vụ đã lập lịch (Scheduled Tasks)

```

Write-Host "2.ScheduleTasks" -ForegroundColor Blue
#Check Schedule Task
Get-ScheduledTask | Format-Table

```

Kiểm tra các dịch vụ đã cài đặt

```

Write-Host "3.Service" -ForegroundColor Blue
#Check Service
Get-Service | Format-Table

```

Kiểm tra file shortcut (LNK): Do không xác định được mã độc sẽ tạo

Kiểm tra WMI Subscriptions

```

Write-Host "4.WMI" -ForegroundColor Blue
Write-Host "WMI filters" -ForegroundColor Yellow
# List all WMI event filters
Get-CimInstance -Namespace root\Subscription -ClassName __EventFilter

```

Write-Host "WMI consumers" -ForegroundColor Yellow

```
# List all WMI event consumers
Get-CimInstance -Namespace root\Subscription -ClassName __EventConsumer

Write-Host "WMI consumers to filters" -ForegroundColor Yellow
# List all WMI filter-to-consumer bindings
Get-CimInstance -Namespace root\Subscription -ClassName
__FilterToConsumerBinding
```

L

Kiểm tra Start up folders

```
Write-Host "5.All startup folder" -ForegroundColor Blue
#All user startup folders
Get-ChildItem -Path "C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\StartUp"
```

Kiểm tra user logons

```
Write-Host "6.Local user logons" -ForegroundColor Blue
Get-LocalUser
```

Kiểm tra các tập tin được ghi vào ngày hôm trước

```
Write-Host "7.All change file" -ForegroundColor Blue
Get-ChildItem -Path "C:\" -File | Where-Object {
    $_.LastWriteTime -gt (Get-Date).AddDays(-1)
}
```

6. Sử dụng đoạn script tự code ở YC 5. Hãy trả lời các câu hỏi sau:

Mã độc sử dụng cơ chế Persistence nào?

Mã độc đã ghi bao nhiêu tập tin? Ghi ở vị trí nào, mã băm SH256 là gì?

Có dữ liệu nào ẩn không (Gợi ý NTFS alternate data streams)

Do mã độc không tải xuống được và thực thi do đường dẫn đến mã độc không còn tồn tại nên không thể trả lời những câu hỏi trên.

8

HẾT