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

STT	Họ và tên	MSSV	Email
1	Từ 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 hiểm 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.

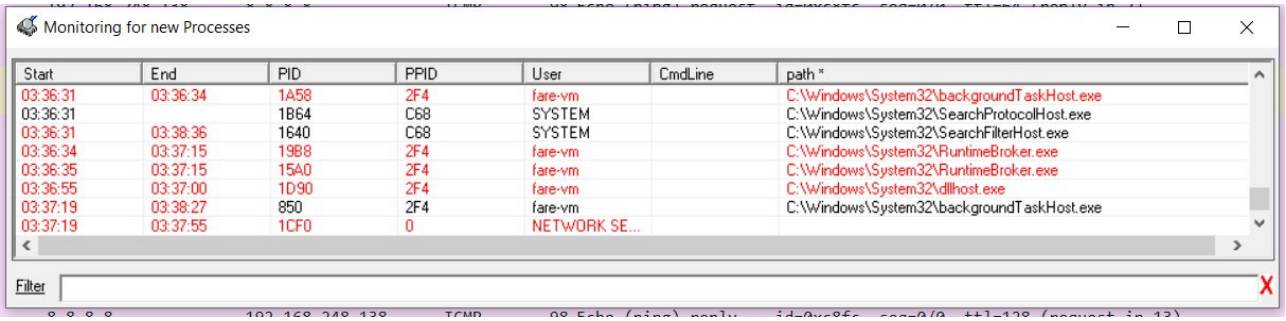
[1] Ghi nội dung công việc

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 hiểm 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

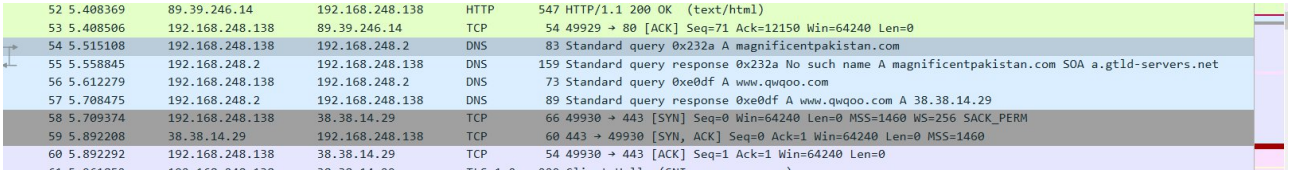
1. Các tiến trình nào mới được tạo ra bởi mã độc? Mã độc có tạo ra các tiến trình con không?

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



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.



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 hiểm 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 kĩ thuật presistent 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.

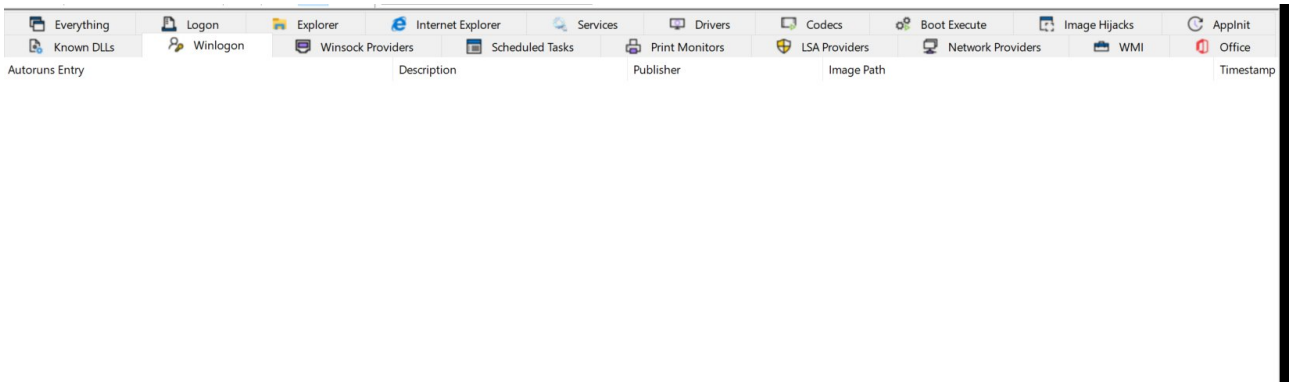
Lấy thông tin của số serial của đĩa hệ thống sử dụng hàmGetVolumeInformationW()

Thực hiện tìm kiếm đệ 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

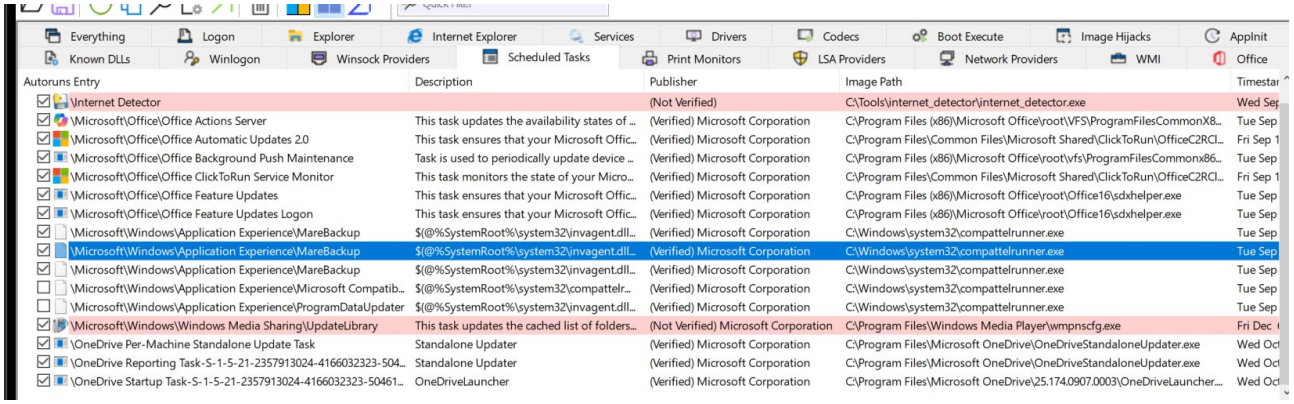
4. Sử dụng AutoRun để kiểm tra có Persistence trên các Register Key

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

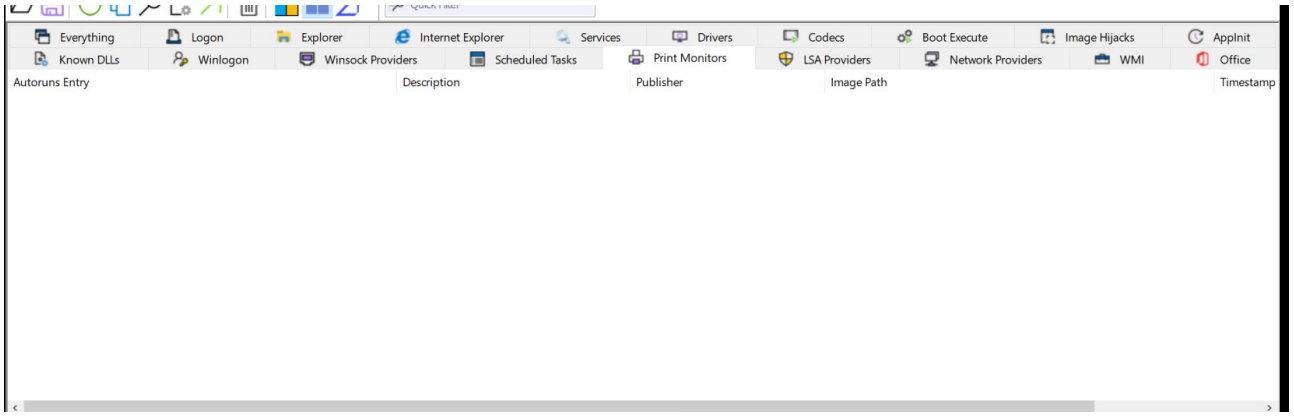
Register WinLogon cũng không có gì.



Scheduled Tasks cũng không có gì đáng nghi.



Print cũng không có tiến trình thêm.



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

```
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