Command & Control - level 4 ✍

Title: Malware analysis

Point: 35 Points

Level: Medium

Description: Berthier, thanks to this new information about the processes running on the workstation, it's clear that this malware is used to exfiltrate data. Find out the ip of the internal server targeted by the hackers!

The validation flag should have this format : IP:PORT

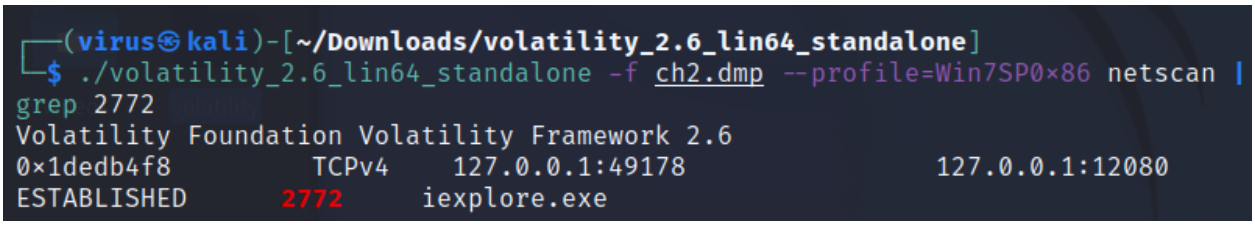
The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

Solution:

Công cụ sử dụng: `Volatility`

Tiếp tục từ bài **Command & Control - level 3**. Chúng ta đã biết có một malware đang chạy dưới PID `2772` – nó là backdoor. Bây giờ chúng ta sẽ "đào sâu" hơn và xem thông tin kết nối của nó. Dùng `netscan`:

```
./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 netscan | grep 2772
```



Đây không phải là port và IP đang tìm kiếm. Có lẽ attacker đã ngắt process thực sự đi trước khi chúng ta dump file. Giờ chúng ta hy vọng, hacker vẫn còn để lại lịch sử các lệnh trong **CONSOLE_INFORMATION**, dùng `consoles`:

```
./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 consoles
```

```
**************************************************
ConsoleProcess: conhost.exe Pid: 2168
Console: 0x1081c0 CommandHistorySize: 50
HistoryBufferCount: 3 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 1616 Handle: 0x64
----
CommandHistory: 0x427a60 Application: tcprelay.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x427890 Application: whoami.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x427700 Application: cmd.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
----
Screen 0x416348 X:80 Y:300
Dump:
```

Chúng ta cần biết sơ một số ứng dụng tiêu biểu

- tcprelay.exe – Tạo một TCP connection forwarder
- consolehost.exe – cho phép `cmd.exe` làm việc với Windows Explorer
- whoami.exe - Display user.

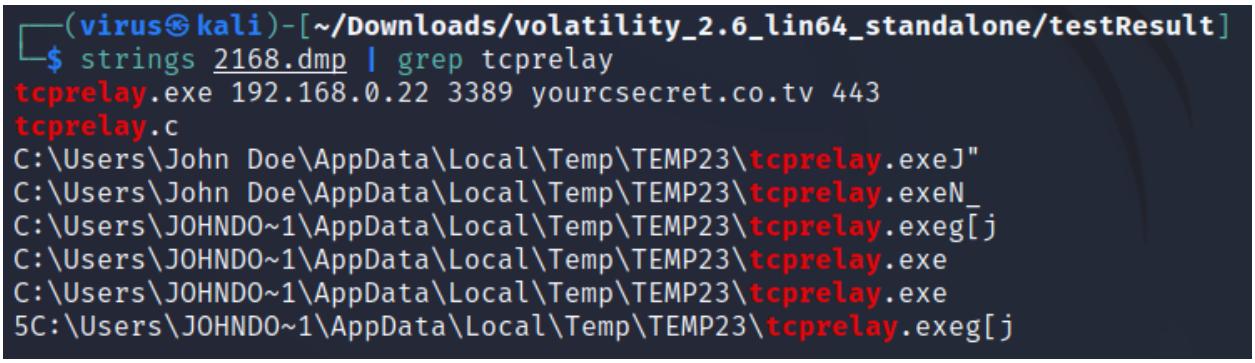
Vậy thì ta có thể đoán được attacker đã mở một shell `cmd.exe` , sau đó sử dụng `tcprelay.exe` cho TCP port forwarder và `whoami.exe` chắc là để kiểm tra xem shell có hoạt động với xem quyền của user (cái này mình cũng thường hay làm khi có được shell). Sau khi xong việc thì đóng cái session này đi. Cơ bản thì commands được nhập vào `cmd.exe` được xử lý bởi `conhost.exe` vậy nếu chúng ta may mắn , ta có thể lấy được thông tin từ bằng cách dump memory của `conhost.exe`

Tạo folder mới cho các **dumped files** và sử dụng `memdump` để dump process `2168`:

```
mkdir testResult && ./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 memdump -p 2772 -D testResult
```

Vào thư mục `testResult` và đọc các dữ liệu liên quan đến `tcprelay.exe` command:

```
strings 2168.dmp | grep tcpreplay
```



We can see the connection has been built by hacker

FLag: **192.168.0.22:3389**