

Command & Control - level 6

Title: Reverse engineering

Point: 50 Points

Level: Medium

Description: Berthier, before blocking any of the malware's traffic on our firewalls, we need to make sure we found all its C&C. This will let us know if there are other infected hosts on our network and be certain we've locked the attackers out. That's it Berthier, we're almost there, reverse this malware!

The validation password is a fully qualified domain name : hote.domaine.tld

The uncompressed memory dump md5 hash is
e3a902d4d44e0f7bd9cb29865e0a15de

NB : This challenge require the clearance of the level 3.




Solution:

Công cụ sử dụng: Volatility, Hybrid Analysis

Tiếp tục từ series **Command & Control** . Nhiệm vụ là tìm các **C&C domain**.

Tạo một thư mục BckDoorRev cho các dumped files, dump toàn bộ process với PID 2772

```
mkdir BckDoorRev && ./volatility_2.6_lin64_standalone -f ch2.dmp --  
profile=Win7SP0x86 procdump -p 2772 --dump-dir=BckDoorRev
```

```
(virus@kali)-[~/Downloads/volatility_2.6_lin64_standalone]  
└─$ mkdir BckDoorRev && ./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 procdump -p 2772 --d  
ump-dir=BckDoorRev  
Volatility Foundation Volatility Framework 2.6     
Process(V) ImageBase Name Result  
0x87b6b030 0x00400000 iexplore.exe OK: executable.2772.exe
```

Rất có thể nó là file .exe . Nhưng cứ kiểm tra signature bằng lệnh **file** cho chắc cú:

```
(virus@kali)-[~/Downloads/volatility_2.6_lin64_standalone]  
└─$ cd BckDoorRev && file executable.2772.exe  
executable.2772.exe: PE32 executable (GUI) Intel 80386 (stripped to external  
PDB), for MS Windows
```

OK. Đúng là một file ***.exe** trên **Windows OS**. Bây thử reverse nó. Đây không phải là chủ đề Reverse Engineer nên mình sẽ nhờ [Hybrid Analysis](#) phân tích hộ. (Mình thử phân tích cơ bản bằng IDA nhưng không ra :v, nó được mã hóa và khó hơn mình tưởng 😞)

Xem "Network Behavior" trong phần "Incident Response"

Incident Response

Risk Assessment	
Fingerprint	Reads the active computer name
Remote Access	Reads terminal service related keys (often RDP related)
Evasive	Tries to sleep for a long time (more than two minutes)
Network Behavior	Contacts 5 domains and 2 hosts. View all details

Đây là tất cả các DNS Request tới một máy tính ngoài vùng mạng. Thử submit từng cái:

Network Analysis Overview

DNS Requests

[Login to Download DNS Requests \(CSV\)](#)

Domain	Address	Registrar	Country
ns2.wrauzfevvo.com	-	-	-
whereare.sexy-serbian	127.0.0.1 (Spoofed)	-	-
yOug.itisjustluck.com	127.0.0.1 (Spoofed)	-	-
th1sis.l1k3aK3y.org	127.0.0.1 (Spoofed)	-	-
furious.devilsife.com	106.187.41.154	-	Japan

Contacted Hosts

[Login to Download Contacted Hosts \(CSV\)](#)

IP Address	Port/Protocol	Associated Process	Details
106.187.41.154	80 TCP	-	Japan ASN: 2516 (KDDI CORPORATION)
72.246.151.179	80 TCP	-	United States

Domain đúng cho challenge là th1sis.l1k3aK3y.org

Flag: **th1sis.l1k3aK3y.org**