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

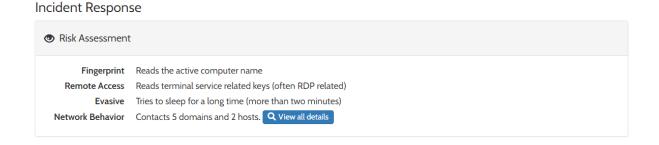
Rất có thể nó là file .exe . Nhưng cứ kiểm tra signature bằng lệnh **file** cho chắc cú:

(virus&kali)-[~/Downloads/volatility_2.6_lin64_standalone]

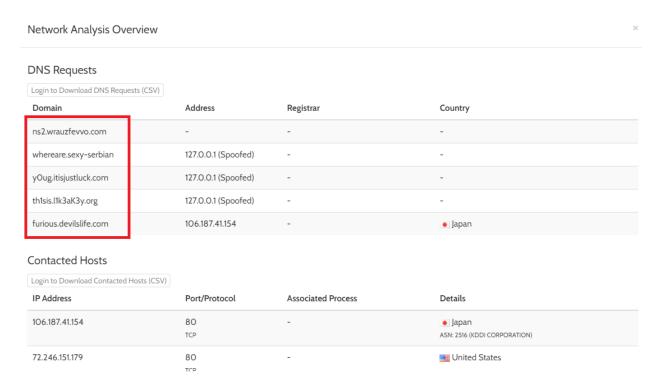
└─\$ cd BckDoorRev && file executable.2772.exe

executable.2772.exe: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows

OK. Đúng là một file *.exe trên **Window OS**. Bây thử reverse nó. Đây không phải là chủ đề Reverse Engineer nên mình sẽ nhờ <u>Hybrid Analysis</u> phân tích hộ. (Mình thử phân tích cơ bản bằng IDA nhưng không ra :v, nó được mã hóa và khó hơn mình tưởng (E) Xem "Network Behavior" trong phần "Incident Response"



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



Domain đúng cho challenge là th1sis.11k3aK3y.org

Flag: th1sis.l1k3aK3y.org