Đợi xíu đợi xíu bạn ơi... :) Bạn có biết <http://www.visla.vn/> không nhỉ? Chắc chắn trong đời mình sẽ có một lần bạn cần đến đó, nhớ ghé xem sao nhé :) Visla cảm kích hành động này của bạn lắm đấy.

**Nhập môn Malware Analysis**

Bữa nay anh em CEH từ Admin trở xuống đang được nghỉ ngơi nên có thời gian ngồi chém gió đôi chút về Malware Analysis. Theo yêu cầu của một số bạn đang mong muốn tìm hiểu về Malware Analysis thì mình sẽ cố gắng "chém gió" thật cơ bản, bỏ bớt những thứ lằng nhằng. Xem xem Malware Analysis dưới góc nhìn của một tín đồ quản trị sẽ như thế nào :D

**NỘI DUNG BÀI VIẾT:**

1. Khài niệm Malware, Virus, Worm, Trojan, Spyware,...
2. Có nên sợ Malware không?
3. Các kỹ thuật phân tích mã độc
4. Môi trường phân tích mã độc
5. Các công cụ phục vụ cho quá trình phân tích tĩnh và động
6. Thử nghiệm phân tích mã độc đơn giản áp dụng Dynamic Analysis
7. Phòng tránh mã độc

Trước khi muốn động tới những thứ cao siêu khi bắt đầu phân tích một Malware thực sự thì ta nên bắt đầu với những định nghĩa cơ bản qua những câu hỏi thường gặp sau

**Malware là con gì vậy? Có ăn được không?**

Malware xuất phát từ cụm từ Malicious Software có nghĩa là phần mềm độc hại. Malware là cụm từ dùng để chỉ chung tất cả những phần mềm, công cụ, đoạn mã,.... Có khả năng làm hại máy tính hay gây ảnh hưởng trái phép tới người dùng. Chính vì thế định nghĩa malware đã bao gồm cả: Virus, Worm, Trojan, Spyware, Adware...

**Vậy Virus, Worm, Trojan, Spyware,... là gì?**

Có khá nhiều định nghĩa về những thứ này. Nhưng ta nên hiểu đơn giản:

* Virus: là một số dạng mã độc cần đến sự tác động của con người để lây lan, Ví dụ click tập tin mã độc, click tập tin có đính kèm mã độc, Truy cập website có mã độc,.......
* Worm: là một số dạng mã độc có thể tự lây lan, và chính vì thế nó thường lây lan rất kinh khủng :D Ví dụ: Tự động lây lan qua những máy tính có OS chứa lổ hổng trong cùng lớp mạng (ví dụ con conficker,...) ,....
* Trojan: Trước đây thì Trojan chỉ đơn giản là những dạng mã độc không thể tự lây lan, Và chức năng chủ yếu của nó đúng với tên gọi Trojan đó là chứa hoặc "Tuồn" những loại mã độc khác vào hệ thống. Tuy nhiên ngay nay trojan đã có nhiều biến tướng :D
* Spyware: Phần mềm gián điệp, thu thập những thông tin trái phép trong máy tính
* Adware: Phần mềm quảng cáo, Đây thường là nguyên nhân làm nên những hiện tượng như: Popup lạ, thông báo lạ thường xuyên nhảy ra trên máy tính, Trang chủ trình duyệt web bị thay đổi, Trang chủ tìm kiếm bị thay đổi,..... Đôi khi Adware cũng có thể bí mật ghi lại một số thông tin như lịch sử truy cập web, số điện thoại (đối với adware trên smartphone), địa chỉ Mail,..... Và gửi về cho chủ nhân, điều này làm nó gần chạm tới người anh em Spyware của nó.

Ngoài ra còn rất nhiều khái niệm như backdoor, Rootkit, w32,..... Tất cả được phân loại dựa trên khả năng và đặc tính của nó.

**Có nên sợ Malware không?**

Có nhiều người nói, Ui dào việc chi phải sợ, máy tính có gì quan trọng đâu, sống chung với malware cũng chả ảnh hưởng gì? Vậy xin đưa ra 1 số trường hợp thực tế đã gặp sau để mọi người tự rút ra là có nên sợ malware hay không

* Một ngày đẹp trời mở máy tính và phát hiện từ đó trở đi máy tính chạy chậm rì, tài nguyên sử dụng (CPU, RAM) tăng đột biến, .......
* Một ngày nọ bỗng mạng chậm rì, gọi lên tổng đài xuống kiểm tra thì không có gì hỏng hóc ở thiết bị, và thế là cam chịu số phận
* Một ngày kia thằng bạn cờ hó  lôi đâu ra tấm hình bạn đang thay đồ, quay tay, xem JAV,...... khoe cho cả lớp coi
* Một ngay nào đó đăng nhập facebook và thấy comment do chính mình đăng: I'm Gay :v (đôi khi có thể do FA lâu năm nên tự đăng thật :v ) hay trong inbox đang pm cho gấu tự nhiên có dòng: "Em iu anh đổi số điện thoại rồi, xoá số cũ đi, Gọi số này nè" :v
* Một này đi làm tự nhiên bị sếp nắm cổ lên cho coi tất cả các tập tin văn bản trong toàn bộ các máy tính ở công ty bị mã hoá RSA-2048 và chỉ có nước gửi tiền cho một thằng I-rắc nào đó để nó giải mã.

............

**Các kỹ thuật phân tích mã độc**

Có 2 kỹ thuật phân tích mã độc chính:

* Dynamic analysis: Phân tích động: Hiểu nôm na quá trình này có nghĩa là quan sát hành vi của mã độc khi nó đang chạy. Cụ thể là những công việc như: Khởi chạy mã độc trên một môi trường ảo, Quan sát xem khi mà mã độc chạy nó sẽ làm những gì,.... Debug mã độc sử dụng một công cụ Debugger nào đó Ví dụ winDBG, OllyDBG để quan sát từng bước hành vi của mã độc khi nó đang được thực thi bởi bộ nhớ và load trong RAM
* Static analysis: Phân tích tĩnh: Là quá trình dịch ngược mã độc (RCE - Đọc thêm về kỹ thuật reverse engineering). Dịch ngược mã độc từ mã máy ra ngôn ngữ mà con người có thể đọc hiểu (asm, IL,..). Trong quá trình này các nhà phân tích sẽ sử dụng những công cụ dịch ngược như IDA, khi thực hiện dịch ngược IDA không load mã độc vào RAM như ollyDBG,

Người phân tích có thể thực hiện chỉ 1 trong 2 quá trình trên hoặc là cả 2 tuỳ theo từng trường hợp. Và mục tiêu cuối cùng sau các quá trình là họ phải đáp ứng được 2 yêu cầu: Yêu cầu hàng đầu đó là: Xác định được dấu hiệu nhận diện của mã độc, Khi xác định những dấu hiện nhận diện mã độc thì có thể bàn đến chuyện loại bỏ mã độc. những dấu hiệu nhận diện này sẽ được bổ sung vào Cơ sở dữ liệu của các anti virus. Yêu cầu thứ 2 là hiểu mã độc sẽ làm những gì khi lây nhiễm vào hệ thống. Có một số trường hợp qua quá trình phân tích họ đã rút ra ngay dấu hiệu nhận diện mã độc và trang bị anti của mình khả năng nhận diện và tiêu diệt mã độc đó mà không cần thiết phải hiểu ngọn ngành từng dòng code, từng chức năng của mã độc.

**Môi trường phân tích mã độc**

Để phân tích mã độc người phân tích cần tạo ra những môi trường ảo để phân tích, đảm bảo mã độc không thể lấy nhiễm ra ngoài hay làm hại đến máy tính của chính mình. Giả sử bạn đang ngồi phân tích một mã độc có khả năng lây lan mạnh nhất trong lịch sử. Và bạn bắt đầu phân tích nó bằng cách chạy nó ngay trên máy tính có kết nối ra internet của mình, Việc đó sẽ khiến mã độc ngay lập tức có thể lây lan ra ngoài và gây ra hậu quả không lường trước được. Hơn nữa có một quy tắc khi phân tích mã độc đó là tuyệt đối không nên để cho chủ mưu nhận ra có người đang cố gắng phân tích mã độc của hắn. Chẳng hạn 1 attack điều hành nhiều mạng lưới Botnet lớn, Mình bắt được 1 mẫu trong đống Zombies của hắn. Trong quá trình phân tích và cố gắng tìm cách tóm gọn toàn bộ mạng lưới botnet đó, nếu vô tình attack nhận ra có người đang cố gắng phân tích mã độc của hắn, hắn sẽ nhanh chóng xoá hết dấu vết, Và ta sẽ chẳng bao giờ túm được nó :D

Môi trường ảo ở đây sẽ được xây dựng tuỳ trường hợp, tuỳ từng đơn vị phân tích. Đối với một người phân tích mã độc tự do không chuyên thì môi trường ảo đó chỉ đơn giản là:

- Một Vmware hay Virtualbox có cài sẵn windows xp,7,... cùng một số ứng dụng thông dụng như java, adobe flash, firefox,..... và máy ảo này sẽ không có kết nối mạng ra ngoài và ra máy thật (host only) hoặc có kết nối ra máy thật, máy thật sử dụng Linux và Không có kết nối mạng (offline) (Trong trường hợp này thường người ta sẽ đăng tcpdump ngoài máy thật và wireshark ở trong hoặc cũng có thể thực hiện sinkhole )

- Chuẩn bị đầy đủ các công cụ phục vụ cho quá trình phân tích tĩnh và phân tích động

- Chuẩn bị mẫu mã độc.

Đối với những chuyên gia phân tích chuyên nghiệp trong các phòng thí nghiệm mã độc họ có thể xây dựng những mô hình phức tạp hơn, Chẳng hạn xây dựng nhiều máy ảo thông với nhau để thử nghiệm lây lan trong Lan, hay Xây dựng nhiều máy ảo với nhiều nền tảng khác nhau, nhưng máy chạy win 7, máy chạy xp, máy chạy win 8.1, máy chạy Linux,... Máy có .Net framwork và c++ redestributable,.... Máy không hỗ trợ....

Đối với 1 Chuyên gia phân tích mã độc chuyên nghiệp họ sẽ xây dựng những sandbox tự động để tiết kiệm thời gian, Thay vì tự khởi chạy mã độc, tự mở các trình quan sát, tự lấy số liệu từ từng trình quan sát một,... Thì các sandbox tự động  sẽ tự động giải quyết hết chuyện đó, Bạn chỉ cần submit mẫu vào và nó sẽ làm mọi thứ tự động sau đó in ra báo cáo cho bạn. Nếu bạn muốn tự xây dựng một hệ thống như thế thì nên tìm hiểu về Cuckoo Sanbox. Ngoài ra nếu lười bạn có thể dùng ngay các sandbox Online để tiết kiệm thời gian. Một số dịch vụ Sandbox online như

- [https://www.malwr.com](https://www.facebook.com/l.php?u=https%3A%2F%2Fwww.malwr.com%2F&h=qAQHBMdws&s=1)

- [https://anubis.iseclab.org](https://www.facebook.com/l.php?u=https%3A%2F%2Fanubis.iseclab.org%2F&h=MAQEJuOFh&s=1)  (mình thích cái này, mặc dù chậm nhưng nó báo cáo trực quan hơn)

Tuy nhiên sử dụng 1 số hệ thống tự động như vậy sẽ có một số nhược điểm, Chẳng hạn 1 số mã độc attacker quy định thời gian mã độc kết nối về ví dụ đúng 6h tối nó bắt đầu tạo kết nối, trong khi 7h sáng bạn bắt đầu phân tích ==> Nếu phân tích tự động nó chạy cái èo và thông báo rằng network không có gì cả (không có kết nối nào ra ngoài) ===> Bạn sẽ chủ quan cho rằng mẫu này không hề tạo kết nối về. Tuy nhiên nếu phân tích thủ công bạn có thể ngâm cứu mã độc ấy, quan sát nó ngày đêm thậm chí sau nhiều lần restart máy :v

Đối với 1 số Hãng lớn như Kaspersky họ thực hiện cả quá trình phân tích tĩnh và động một cách tự động (Áp dụng Machine Learning), Mỗi 2s họ phân tích xong 1 mẫu mã độc mới. Các Chuyên gia của họ thường dành thời gian để phân tích thủ công 1 số mã độc đặc biệt hay phân tích lại các biến thể mới,...

Có một điểm cũng cần chú ý. Một Số mã độc có thể bypass được sandbox của bạn ;) Cũng có 1 số mã độc mang mục đích không chỉ là phá hoại mà còn có nhiệm vụ "Chơi" lại chính người cố gắng phân tích nó :D

**Các công cụ phục vụ cho quá trình phân tích tĩnh và động**

- Công cụ môi trường:

+ Compiler, IDE ( Dev C++, visual C++, python, MASM, winasm, avtive perl,....)

+ thư viện hỗ trợ (.Net Framework, C++ redestributable, wincap,....)

- Công cụ phục vụ phân tích động

+ Công cụ theo dõi hành vi mã độc:

Cực kì nhiều, nhưng có thể kể đến 1 số như: Bộ SysinternalsSuite, Regshot, networkminer, wireshark, PC Hunter Một số công cụ check MD5, SHA-1

+ Công cụ Debugger

OllyDBG, winDBG, Immunity Debugger

- Công cụ phục vụ phân tích tĩnh:

+ IDA

+ Ngoài ra có nhiều trình Dịch ngược khác tuỳ từng loại mã độc, ví dụ mã độc code = autoit thì dùng Exe2Aut, code = Delphi thì dùng DeDe,....

Các công cụ dịch ngược / Debug trên các nền tảng khác nhau: x86, x64, Dịch ngược các tập tin thực thi khác nhau như python, ELF, Exe,.... dịch ngược các thư viện (Dll, so,...),.....

 - Các công cụ khác

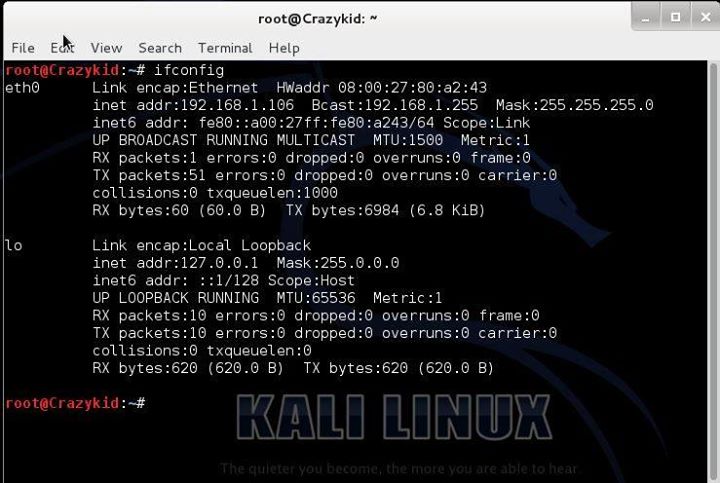
+ PE file format: ExePEinfo, PEiD, ...

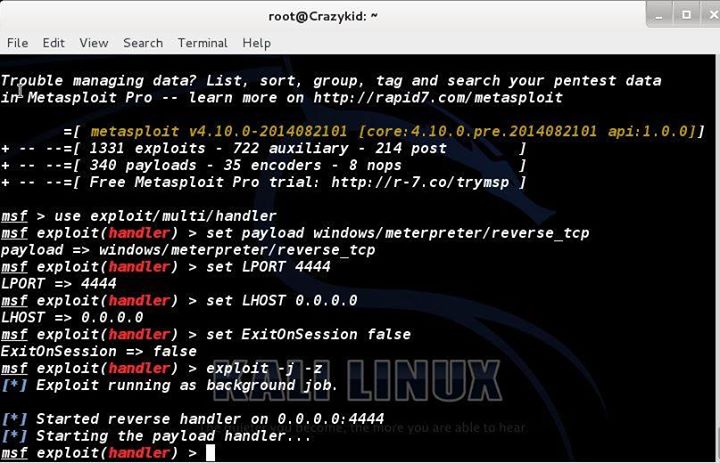
+ Các công cụ unpack auto: UPX,...

+ CFF Explorer, Hex workshop / FileInsight, OfficeMalScanner, Offvis, Pestudio, Notepad ++ , Peepdf,.....

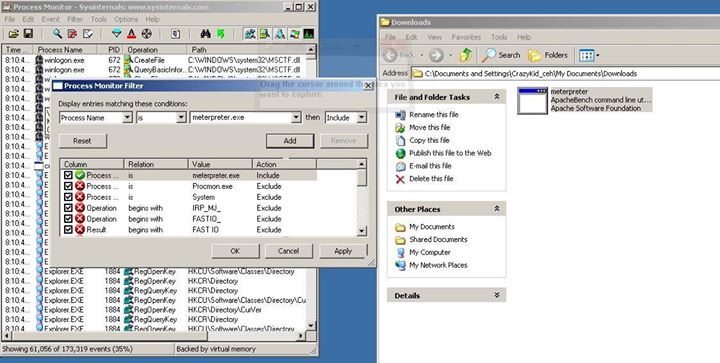
+ Các công cụ Dump và phân tích memory: volatility, Redline, DumpIt,....

**Thử nghiệm phân tích mã độc đơn giản áp dụng Dynamic Analysis**

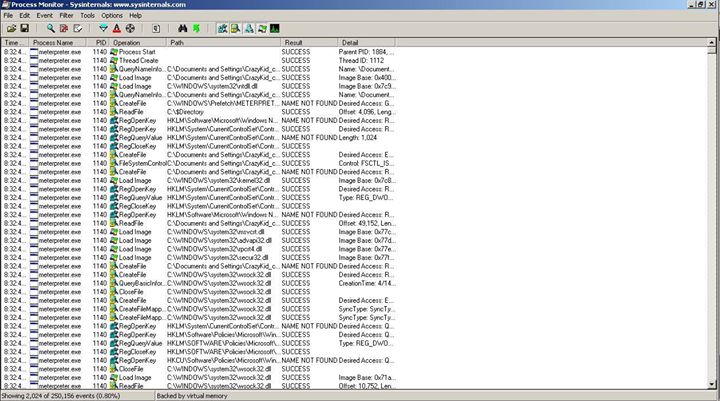
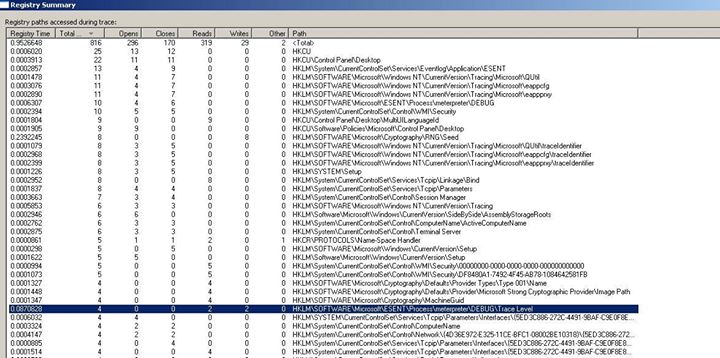
Ở phần này mềnh chỉ chỉ các bạn quá trình Dynamic Analysis cơ bản nhất mà ai cũng có thể thực hiện sau khi các bạn đã chuẩn bị môi trường đầy đủ. Đầu tiên cần chuẩn bị 1 mẫu mã độc để thí nghiệm, Mình sẽ sử dụng msfpayload để tạo ra 1 mẫu để ngâm cứu. Mình có máy attacker Chạy Kali-linux Có IP là 192.168.1.106

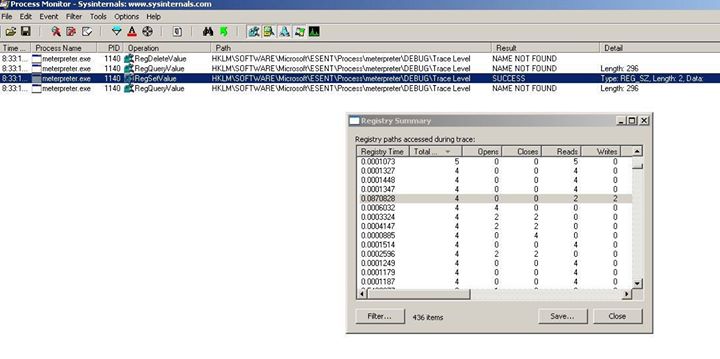
OK. Mình sẽ dùng msfpayload tạo ra 1 mã độc có khả năng tạo kết nối về máy attacker sau khi lây nhiễm (Chính là máy IP 192.168.1.106) thông qua port 4444. Mẫu này có tên meterpreter.exe  
  
Mình khởi động Handler Trong msfconsole trên máy attacker để bắt đầu nghe ngóng trên port 4444. Nếu mã độc lây nhiễm thành công trên victim và tạo kết nối về thì nhờ Handler mình có thể nghe được kết nối ấy.

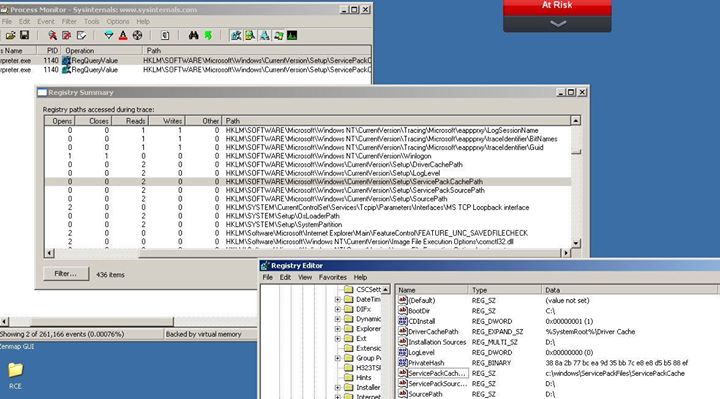
Ok. Tại victim Download mẫu mã độc về máy victim, ở đây máy victim cũng là máy mình thực hiện Dynamic analysis:   
  
Bắt đầu kiểm tra md5 và SHA-1 của mẫu bằng các công cụ MD5 checker, Sha-1 Checker. Cùng với đó kiểm tra những thông tin sơ bộ vì mẫu. Mình sẽ không nói về vụ này  
Chuẩn bị Các công cụ quan sát. Ở đây mình sẽ chọn công cụ ưa thích của mình đó là Process Monitor. Công cụ này có sẵn trong bộ SysinternalsSuite luôn. (Procmon.exe)   
Mình thích công cụ này bởi những tính năng sau:  
Có thể quan sát chỉ 1 tiến trình, và quan sát tất cả sự thay đổi do tiến trình ấy tạo ra, Đưa ra những chức năng của tiến trình ấy, Ví dụ Tạo, đọc những khoá nào trong registry, Có kết nối ra ngoài hay không, Tạo ra những tiến trình nào, file nào trong hệ thống, Nó còn có chức năng khởi động cùng hệ thống và theo dõi tiến trình, Giả sử bạn chỉ định cần theo dõi tiến trình tên meterpreter.exe, và bật chế độ khởi động cùng hệ thống thì Process Monitor sẽ theo dõi hoạt động của Meterpreter.exe mọi lúc mọi giây ngay cả khi hệ thống restart nhiều lần.

  
Vậy nên mình khởi động Process Monitor lên trước. Nhấn Ctrl + L để mở hộp thoại Filter. Tại Hộp thoại Filter Các bạn chọn các khung đổ xuống lần lượt là: Process Name ==> Is ===> gõ vào Meterpreter.exe (Tên mẫu mã độc mình sắp khởi chạy) ==> Include như hình. Sau đó nhấn ADD. Bạn cũng nhớ để ý cái biểu tượng hình kính lúp phải như trong hình, Không được có dấu gạch đỏ (Chứng tỏ chương trình đang theo dõi) Sau đó nhấn OK. Từ nay Process Monitor sẽ chỉ tập trung tìm và quan sát Mẫu tiên Meterpreter.exe của bạn mà thôi  
  
  
Ngoài Process Monitor mình Còn khởi động sẳn wireshark và Comodo Firewall (đã tắt tính năng firewall chỉ bật tính năng nghe ngóng) để phân tích network trực quan hơn.  
Bước kế tiếp sau khi đẵ khởi động hết những trình quan sát, theo dõi cần thiết sẽ là bước ta khởi chạy mẫu mã độc và bắt đầu quan sát xem mã độc làm những gì.   
Vậy có một câu hỏi ở đây, ***Chúng ta cần quan sát những hành vi nào của mã độc ?***  
Chúng ta Cần quan sát những hành vi thường thấy của một mã độc, đó là:

1. ***Tạo ra hay xoá đi hay chỉnh sửa những tập tin nào trên hệ thống?***
2. ***Tạo ra những tiến trình (Process) nào? Loại bỏ (Kill) những tiến trình nào đang chạy?***
3. ***Ghi / Đọc / Mở những giá trị nào từ Registry?***
4. ***Network có gì thay đổi? Có tạo kết nối ra ngoài nào không? Có tạo lắng nghe trên port nào hay mở socket nào không? Có download hay upload cái gì không? ...***
5. ***Có khởi động cùng hệ thống hay không***

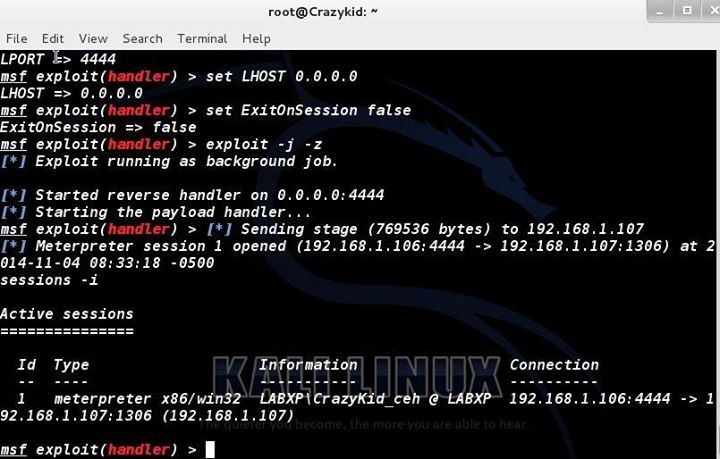
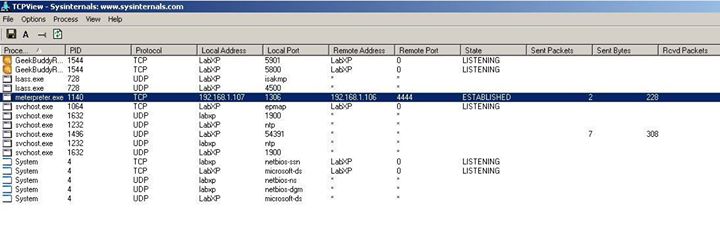
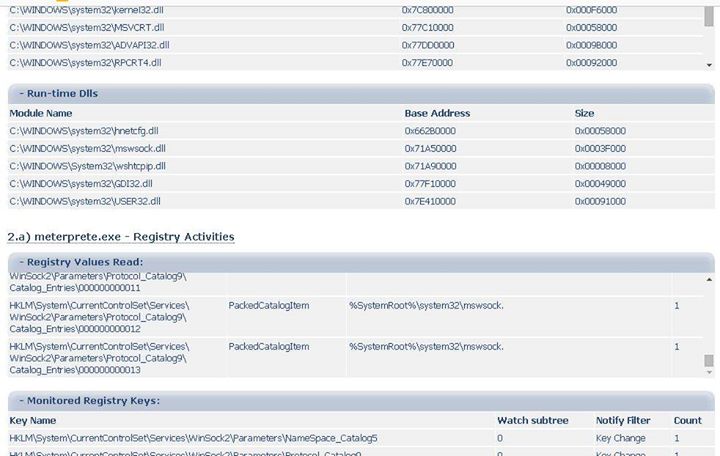
OK. Sau khi hiểu những gì cần phải quan sát thì ta bắt đầu khởi chạy mã độc bằng cách click đúp vào nó. Quan sát Process Monitor ta thấy Mẫu của ta đã thực hiện hàng loạt các hành động  
Nhìn vào Process Monitor các bạn có thể thấy rõ ràng từng hành động giúp bạn trả lời hết những câu hỏi ở trên, Như:  
  
Nó bắt đầu tác vụ Process start và Thread Create ==> Khởi động một tiến trình tên Meterpreter.exe và tạo 1 Thread có ID là 1112  
đọc các thư viện và thông tin cần thiết  
Tạo ra 1 file tên meterpreter.exe trong C:\Windows\Prefect\ Tuy nhiên hầu hết các tác vụ tạo file này như các bạn thấy đều bị thât bại do Access Deny (Củ chuối thặc :v )  
Ghi / Đọc các giá trị từ Registry,....  
......  
Và còn nhiều thông tin chi tiết nữa, Tuy nhiên bây giờ mình muốn xem cụ thể chỉ những thông tin về Registry thôi. Mình chọn Tools trên thanh công cụ --> Registry Summary

 Các bạn có thể thấy rõ từng thông tin mà mẫu mã độc đã động vào Registry như thế nào. Nó đã đọc Các giá trị Trong registry 319 lần và viết vào đó 29 lần. Các bạn có thể thấy dòng mình bô đen. Con số 2 ở cột dọc Write và 2 ở cột Read cho thấy mẫu mã độc đã đọc giá trị registry này 2 lần và ghi đè 2 lần lên giá trị đó  
Ta click vô từng dòng và quay ra giao diện chính để xem chi tiết 

Khi xem chi tiết ta thấy rằng nó đã ghi thành công giá trị vào đó (RegSetValue) lần đầu nó chỉ đọc để xem thử giá trị có tồn tại hay không, nếu giá trị chưa tồn tại thì ghi vào rồi kiểm tra lại một lần nữa

Chúng ta quan sát tiếp một giá trị được đọc trong registry. Đó là ServicePackCachePatch. Mã độc đang cố gắng xác định thông tin về OS, version HĐH và quyền hạn, xác định ổ đĩa chứa HĐH... Có nhiều hành động can thiệp vào registry khác được ghi lại cũng chứng mình điều này, Nếu quan sát kỹ từng hành động này các bạn cũng đã phần nào đoán ra được hầu hết những công việc mà mã độc sẽ làm khi lây nhiễm vào hệ thống.

Ngoài registry các bạn còn có thể quan sát chi tiết Network, Process,..... bằng cách chọn Tools -> mục tương ứng.  Đối với chức năng Network Summary của Process Monitor nó làm việc không hiệu quả cho lắm. Vì thế ta thử gác Process Monitor qua một bên và quan sát xem Comodo và wireshark quan sát được những trên Network rồi. 

Đối với Comodo ta thấy:  
  
IP 192.168.1.107 là IP của máy victim (máy đang phân tích) nó đang mở một kết nối ra port  1306 và chạy về port 4444 của của IP 192.168.1.106 ==> 192.168.1.106 là attack đang ngồi nghe ngóng. Chúng ta cũng có thể thấy có lưu lượng ra và vào máy có nghĩa là attacker đang làm gì đó trên máy ta. Lưu lượng vào khá cao 2MB. Có thể attacker đang tiếp tục tiêm payload khác vào hoặc gửi tập tin nào đó qua đây  
  
Ta thử xem Ở bên máy attacker coi đúng vậy không nhé  
  
   
  
  
  
Đúng rồi nhé ;)  
Ngoài Comodo Thì wireshark là sự lựa chọn Hoàn Hảo nhất để qua sát network. Nó có thể cho ta xem chi tiết từng gói tin ra vô, thậm chí nếu nó bắt được quá trình attacker gửi payload vô victim bạn có thể extract payload đó ra bằng chức năng follow. Hoặc nếu một con zombies đang cố gắng kết nối với Cpannel điều khiển bạn cũng có thể thấy được những gói tin chứa tài khoản và địa chỉ đăng nhập CPannel điều khiển đó.....  
Ngoài wireshark một số người có thể dùng TCPview cũng cho kết quả tương tự nhưng TCPview chỉ quan sát được các kết nối TCP mà thôi.  
  
OK. ngoài Process Monitor thì Regshot cũng là công cụ ưa thích của Kid. Nó cung cấp những thông tin mà Process Monitor có thể  quan sát thiếu. Cùng với đó trong bộ Sysinternals Suite cũng có rất nhiều công cụ tuyệt vời khác mà các bạn có thể tự chạy thử và tìm hiểu, Chọn nên sử dụng cái nào cho phù hợp tuỳ vào từng tình huống.  
  
Nãy giờ ta phân tích thủ công hết. Giờ ta thử quăng mẫu lên sandbox online cho nó phân tích tự động coi sao, có gì khác biệt hay không?  
  
  
  
  
  
Kết quả cũng tương tự ;) anubis Cho ra báo cáo trực quan ở nhiều dạng như HTML, PDF, .... và cung cấp cả file PCAP lưu trữ luồng dữ liệu khi nó phân tích Network

Ay da Do thời lượng bài viết nên tạm dừng ở đây thôi. Vụ Memory Analysis, Rootkit analysis và Debug mẫu cũng như Static Analysis sẽ nói trong dịp lần sau nhé ;)  
  
Từ bài viết trên tuy mới là cực kì cực kì cơ bản nhưng chắc các bạn cũng đã nhận ra ngành Mã độc đòi hỏi lượng kiến thức như thế nào rồi chứ? cần trang bị những kiến thức về các định dạng tập tin, Cấu trúc tập tin, Hex, Am hiểu nhiều nền tảng hệ thống khác nhau, Nhuyễn lập trình như cháo,  Kỹ thuật RCE,... Nên tự tìm tọi tự code các mẫu mã độc từ A-Z, cải tiến nó để hiểu được ví trí của một kẻ chuyên viết mã độc, đoán được ý đồ và thông thuộc những API, những đoạn code đặc trưng thì sẽ dễ dàng để phân tích  
  
**Phòng tránh mã độc  
  
1. Không Click bậy  
2. Cấp nhật các bản vá lỗi ứng dụng / Hệ điều hành quan trọng (Không nên cập nhật tất cả)  
3. Sử dụng 1 Antivirus cập nhật liên tục và 1 Firewall, Sử dụng usb Secure để quét máy tính định kì  
4. Theo dõi Hệ thống thường xuyên và liên tục nếu có kinh nghiệm**Có người thấy điều thứ 3 sẽ nói chung quy lại cũng là tiền, Cách phòng tránh đáng giá nhiều tiền, mà sử dụng Anti thì nói làm chi......  
Xin trả lời rằng đối với một người dùng phổ thông thậm chí người dùng có trình độ IT thì việc phát hiện và loạt bỏ malware thủ công khá khó khăn và không thể tuyệt đối + mất rất nhiều thời gian.   
Ví dụ bạn đang quản lý một server. Server của bạn dính Malware. Bạn sẽ chọn phương án Bug backup và Convert để vô hiệu malware có trên backup nếu có. Hay bạn sẽ ngồi lần mò và gỡ từng tập tin, từng giá trị 1?  
Ngay cả khi Có Anti thì cũng không thể đảm bảo hệ thống an toàn tuyệt đối. Bởi vì tấn công Malware là 1 cuộc tấn công dựa phần lớn vào tâm lý người dùng.  
Ví dụ:  
Giả sử bạn có 1 ông sếp máy cá nhân có Bitdefender Total key bản quyền. Vậy làm thế nào để tấn công sếp đó?  
Giả sử trong quá trình làm việc bạn nhận ra sếp có bồ nhí. Bạn cũng biết Email Của sếp (Biết những điều này không khó)  
Bạn gửi 1 Mail từ địa chỉ Mail nặc danh gửi đến mail sếp với 1 tập tin jpg đính kèm cùng nội dung: Ảnh ông cùng bồ nhí, Yêu cầu đã được ghi luôn trong ảnh, nếu không làm theo yêu cầu ảnh sẽ tới tay vợ ông trong 2 ngày tới.  
Vậy bạn nghĩ đối với trường hợp này Bit có tác dụng hay không? Ổng sẽ bỏ qua tập tin hình đó theo cảnh báo của Bit hay tắt Bit để mở tập tin đó bằng mọi giá? ;)  
  
Hi vọng bài viết có ích cho các bạn. Like nếu thấy hay và share thoải mái nếu muốn, Nhớ ghi nguồn CrazyKID - Ceh.vn  để mình còn phe gấu :3 Còn không hay thì thôi xin đừng quăng gạch, buồn 5p