Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | ExplorerEditor.dll |
| *MD5* | a42e212ee0cad5eb23da87e6fb9614ad |
| *SHA-1* | 846c0856f7b18c34cb786c75614c49ce10fbd612 |
| *SHA-256* | 8e398f0b5d98a231e544b4505ac7a873976e60093a54b7c3f5cecbab5796fd1b |
| *File type* | Win64 DLL |
| *File size* | 27.00 KB (27648 bytes) |

# Kết luận chung

|  |  |
| --- | --- |
| *Loại mã độc* | Trojan, Backdoor, Downloader |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Mã độc được cài vào hệ thống dưới dạng service SENS bằng cách sửa và tạo thêm các registry. Sau đó tạo thread kết nối đến server C&C  và tiến hành điều khiển máy victim bằng command. |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x64

*Compilation Timestamp*: 2016-09-29 03:18:04 UTC

*Packer*: None

*PE Size*: 27.00 KB (27648 bytes) - Bằng với File Size

*Các hàm import đặc trưng của mã độc*:

* KERNEL32.dll
  + CloseHandle
  + CreateFileA
  + CreatePipe
  + CreateProcessA
  + CreateThread
  + DisconnectNamedPipe
  + ExitThread
  + FindClose
  + FindFirstFileA
  + FreeLibrary
* urlmon.dll
* ADVAPI32.dll
  + RegCloseKey
  + RegDeleteKeyA
  + RegDeleteValueA
  + RegEnumKeyExA
  + RegisterServiceCtrlHandlerA
  + RegOpenKeyExA
* WS2\_32.dll
  + bind
  + closesocket
  + connect
  + inet\_addr
  + inet\_ntoa
  + recv
  + send
  + socket

*Các hàm export nghi ngờ*:

* + Install
  + InstallService
  + Remove
  + RemoveService
  + ServiceMain
  + SetNew
  + SetNewString

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 22/69
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Undetected |
| Microsoft | Undetected |
| Symantec | Undetected |
| McAfee | Artemis!A42E212EE0CA |
| BitDefender | Trojan.GenericKD.61012609 |

## Phân tích động cơ bản

File System:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| WriteFile | .\ExplorerEditor.dll | Copy bản thân |

Registry:

|  |  |  |
| --- | --- | --- |
| RegSetValue | HKLC\SYSTEM\CurrentControlSet\Services\SENS\Start | Key autoruns |
| RegSetValue | HKLC\SYSTEM\CurrentControlSet\Services\SENS\  Parameters\ServiceDll | Thay đổi đường dẫn đến Sens.dll là đường dẫn đến ExplorerEditor.dll |
| RegSetValue | HKLC\SOFTWARE\Microsoft\Internet Explorer\  ExplorerEditor\ServiceName | Tên của service đặt là SENS để fake service mặc định |
| RegSetValue | HKLC\SOFTWARE\Microsoft\Internet Explorer\  ExplorerEditor\ServiceDll | Lưu đường dẫn đến Sens.dll |
| RegSetValue | HKLC\SOFTWARE\Microsoft\Internet Explorer\  ExplorerEditor\ActiveString | "dargun" - String để kiếm tra khi chạy ServiceMain |
| RegSetValue | HKLC\SOFTWARE\Microsoft\Internet Explorer\  ExplorerEditor\Password | "158352692" – mật khẩu để kiếm tra khi chạy ServiceMain |
| RegSetValue | HKLC\SYSTEM\CurrentControlSet\Services\SENS\Start | Key autoruns |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| CreateProcess | C:\Windows\system32\cmd.exe | Shell để thực thi lệnh điều khiển |
| CreateProcessAsUserA | C:\Windows\system32\cmd.exe | Shell để thực thi lệnh điều khiển |

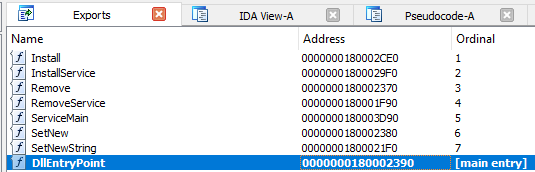
Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| gethostbyname | bobolili.dns-dns.com | Lấy địa chỉ IP của C&C |
| connect (Socket) | <địa chỉ IP của bobolili.dns-dns.com> | Kết nối socket đến C&C |
| send (Socket) | <địa chỉ IP của bobolili.dns-dns.com> | Gửi message đến C&C |
| recv (Socket) | <địa chỉ IP của bobolili.dns-dns.com> | Nhận command từ C&C |

# Phân tích nâng cao

## Luồng hoạt động của mã độc:

Kiểm tra các hàm export nghi ngờ.



Install/InstallService

Mã độc được cài vào hệ thống bằng cách tạo và sửa các Registry.

Thêm các key ***“ServiceName”, “ServiceDll”, “ActiveString”, “Password”*** vào path Registry ***“HKLC\SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor”.***

Thêm các key ***“Start”, “Parameters\ServiceDll”,*** vào path Registry ***“HKLC\SYSTEM\CurrentControlSet\Services\SENS”.***

Ta được các Registry:

* HKLC\SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\ServiceName
* HKLC\SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\ServiceDll
* HKLC\SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\ActiveString
* HKLC\SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\Password
* HKLC\SYSTEM\CurrentControlSet\Services\SENS\Start
* HKLC\SYSTEM\CurrentControlSet\Services\SENS\Parameters\ServiceDll



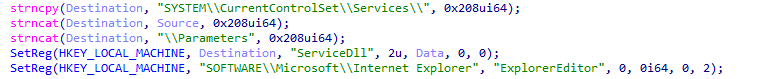
Remove/RemoveService

Xóa mã độc khỏi hệ thống bằng cách xóa các registry mã độc và sửa lại registry gốc.

Xóa các key ***“ServiceName”, “ServiceDll”, “ActiveString”, “Password”*** khỏi registry ***“HKLC\SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor”.***

Xóa các key ***“Start”*** vào path Registry ***“HKLC\SYSTEM\CurrentControlSet\Services\SENS”.***

* HKLC\SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor
* HKLC\SYSTEM\CurrentControlSet\Services\SENS\Parameters\ServiceDll

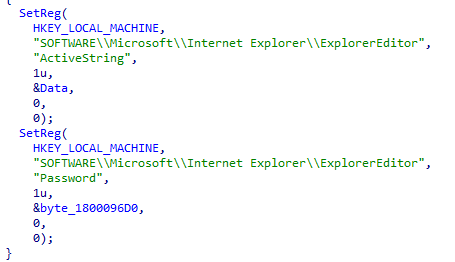


SetNew/SetNewString

Kiểm tra command nhập, nếu truyền vào 3 param và đọc thành công key ***"SOFTWARE\\Microsoft\\Internet Explorer\\ExplorerEditor"*** sẽ thay đổi thông tin service của mã độc.

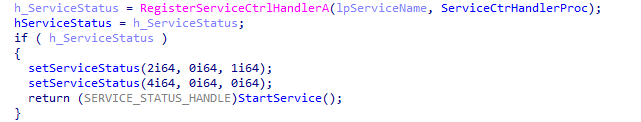


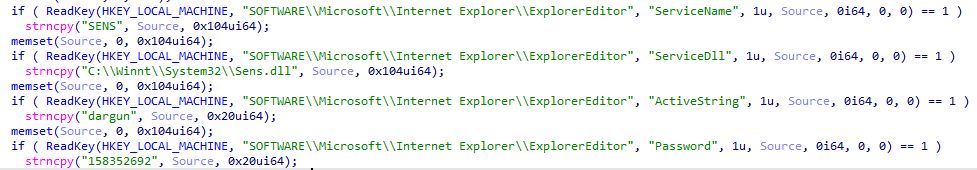
* HKLC\SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\ActiveString
* HKLC\SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\Password



ServiceMain

Sau khi đăng kí chức năng xử lý các yêu cầu kiểm soát dịch vụ thành công sẽ bắt đầu thực thi mã độc.

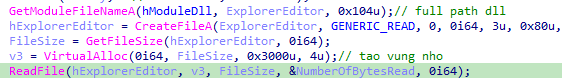


Kiểm tra lại tất cả các giá trị Registry được sửa trước đó.

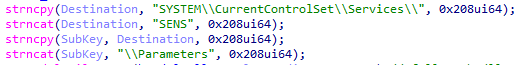
Nếu tất cả các Registry đều đúng sẽ tạo thread để đọc file ExplorerEditor.dll và set các Registry



* + Đọc file ExplorerEditor.dll



* + Set các Registry
    - HKLC\SYSTEM\CurrentControlSet\Services\SENS\Start
    - HKLC\SYSTEM\CurrentControlSet\Services\SENS\Parameters\ServiceDll

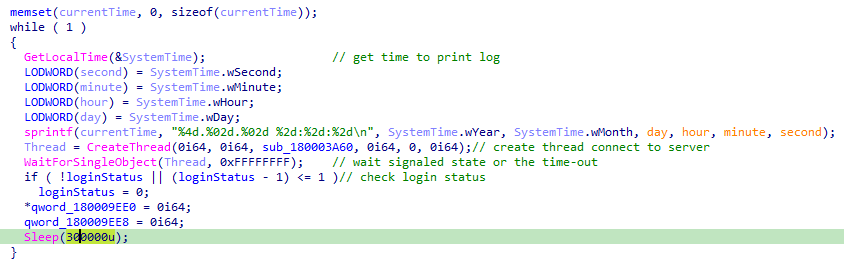




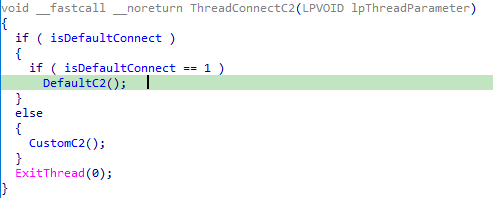
Tạo socket để kết nối đến Server



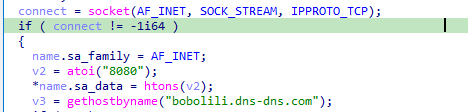
Thực hiện lấy thời gian để dễ dàng ghi log sau này. Sau đó tạo thread để xử lý các kết nối và giao tiếp với server. Chờ đến khi thread gửi cảnh báo hoặc hết thời gian chờ (time-out 300 giây) thì sẽ thực hiện lệnh tiếp theo.



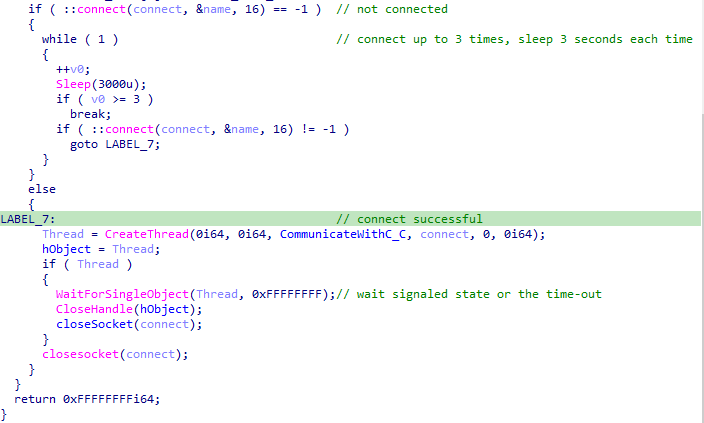
Kiểm tra giá trị isDefaultConnect, nếu giá trị này bằng 1 sẽ thực hiện kết nối đến server được chỉ định sẵn. Ngược lại sẽ kết nối đến server với địa chỉ IP được người dùng nhập vào.



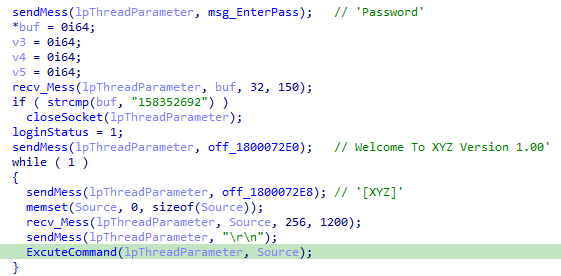
Thực hiện kết nối đến địa chỉ IP có domain name ***"bobolili.dns-dns.com"*** với cổng ***“8080”***



Thực hiện kết nối tối đa 3 lần tới địa chỉ trên, mỗi lần chờ 3 giây. Nếu kết nối thành công sẽ tạo thread giao tiếp với server. Sau đó chờ trạng thái cảnh báo hoặc time-out sẽ thực hiện đóng kết nối socket.

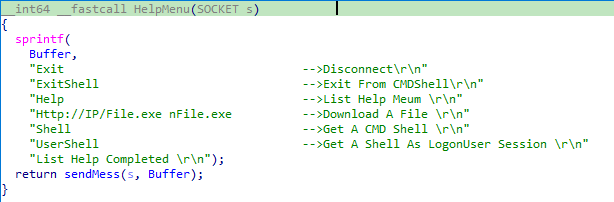


Gửi thông báo yêu cầu phía server nhập password. Nếu server nhập đúng password là ***"158352692"*** sẽ thực hiện nhận command và thực thi.



Mã độc thực hiện các 6 command với các chức năng sau:

* Exit: ngắt kết nối với server.
* ExitShell: thoát khỏi CMD Shell.
* Help: show HelpMenu.
* Http: thực hiện download file với đường dẫn url.
* Shell: thực hiện shell.
* UserShell: thực hiện shell dưới quyền người dùng.





## Hành vi hoạt động của loại mã độc:

### Trojan:

Mã độc được cài vào hệ thống dưới dạng service SENS.

### Backdoor:

Sau khi cài đặt thành công mã độc tạo kết nối đến C&C Server và cho phép điều khiển bằng command.

### Downloader

Thực hiện download file về hệ thống nếu nhận được lệnh từ server.

# Indicators of Compromise (IoC)

Hashes:

* 8e398f0b5d98a231e544b4505ac7a873976e60093a54b7c3f5cecbab5796fd1b

Network IoC:

* bobolili.dns-dns.com:8080