Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | MSBuild.exe.sample |
| *MD5* | 79AD2084B057847CE2EC2E48FDA64073 |
| *SHA-1* | F5A1BF349E82F1B044CFA375D119380F973AD0E5 |
| *SHA-256* | 290AC98DE80154705794E96D0C6D657C948B7DFF7ABF25EA817585E4C923ADB2 |
| *File type* | Win32 EXE |
| *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 |

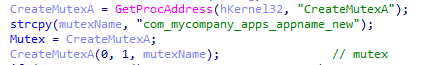
Network:

|  |  |  |
| --- | --- | --- |
| **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:

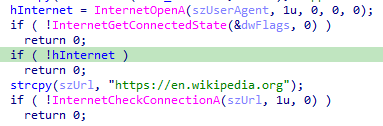
Mã độc tạo mutex với tên ***"com\_mycompany\_apps\_appname\_new"*** để tránh nhiều thread xung đột khi mã độc hoạt động.



Tiếp đến kiểm tra kết nối Interner bằng cách kết nối đến URL ***"https://en.wikipedia.org"*** và thực hiện sleep.



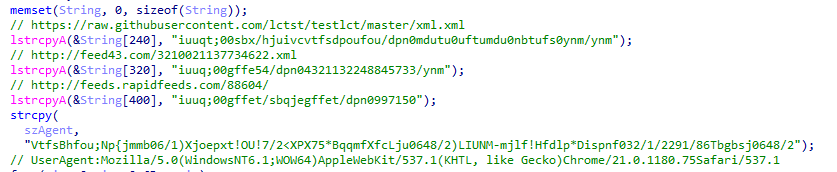
Sau khi kiểm tra kết nối mạng thành công mã độc thực hiện kiểm tra kết nối mạng lại một lần nữa.



* ***“UserAgent:Mozilla/5.0(WindowsNT6.1;WOW64)AppleWebKit/537.1(KHTL, like Gecko)Chrome/21.0.1180.75Safari/537.1”***

Thực hiện lấy dữ liệu trong 3 đường dẫn URL sau

* ***'https://raw.githubusercontent.com/lctst/testlct/master/xml.xml'***
* ***'http://feed43.com/3210021137734622.xml'***
* ***'http://feeds.rapidfeeds.com/88604/'***

******

Sau khi lấy dữ liệu và giải mã dữ liệu thành công ta thu được địa chỉ IP ***"185.203.118.115".***

## 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