Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | swprv.dll |
| *MD5* | ceece2e184484d31ff0dc83e2b7d3238 |
| *SHA-1* | 13cd958b50a4affa8573372daf0e9371548d8d0c |
| *SHA-256* | ab12d69965a13f8929249c62f50af58113ebd8c54666792ac420f78ad41f74b5 |
| *File type* | PE32 dll |
| *File size* | 108 KB |

# Kết luận chung

<Nhận định của người phân tích về mã độc này>

|  |  |
| --- | --- |
| *Loại mã độc* | RAT |
| *Dòng mã độc* | PlugX |
| *Đặc điểm chính* |  |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x64

*Compilation Timestamp*: 2016-03-02 10:31:26

*Packer*: None

*PE Size*: 108 KB (111,104 bytes) - So sánh với filesize

*Các hàm import đặc trưng của mã độc*:

* DeleteService
* RegSetValueExA
* CreateServiceA
* RegCreateKeyA
* ControlService
* 12 (inet\_ntoa)
* 115 (WSAStartup)
* 17 (recvfrom)
* 11 (inet\_addr)
* 21 (setsockopt)
* 20 (sendto)
* 116 (WSACleanup)
* 16 (recv)
* 23 (socket)
* 19 (send)
* RaiseException
* GetCurrentProcessId
* CreateRemoteThread
* WriteFile
* TerminateThread
* CreateProcessA
* TerminateProcess
* WriteProcessMemory
* GetCurrentThreadId
* RtlLookupFunctionEntry
* GetEnvironmentStringsW
* RtlPcToFileHeader

*Các hàm export nghi ngờ*:

* IJA
* INA
* UNA
* UPA

*Resource Language*: Endglish

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 43/71
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Trojan-Spy.Win64.SpyEyes.l |
| Microsoft | Trojan:Win32/Casur.A!cl |
| Symantec | Trojan.Gen.2 |
| McAfee | RDN/Generic PWS.qf |
| BitDefender | Trojan.Generic.23019675 |

*Các kết quả tìm kiếm khác:*

* Nêu các thông tin về mã độc tìm được (dòng mã độc, hành vi, các cuộc tấn công, các thông tin khác…)

## Phân tích động cơ bản

*<Thực hiện monitor hành vi của mã độc, liệt kê các hành vi đặc trưng>*

File System:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| WriteFile | C:\Windows\a.exe | Copy bản thân vào thư mục Windows |
|  |  |  |
|  |  |  |
|  |  |  |

Registry:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| RegSetValue | Software\Microsoft\Windows\CurrentVersion\Run | Auto run hàm IJA của DLL qua process rundll32.exe với giá trị của registry là ctfmon |
| RegSetValue | SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost | Tạo giá trị tham số với giá trị netsvcs tại registry này để thực thi mã độc với svchost.exe |
| RegSetValue | SYSTEM\CurrentControlSet\Services\Parameters | Lưu trữ thông tin về service của mã độc khởi chạy trong value ServiceDll |
|  |  |  |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| CreateProcess | C:\Windows\a.exe | Thực thi mã độc sau khi cài đặt |
| CreateServiceA | %SystemRoot%\\System32\\svchost.exe -k netsvcs | Khởi chạy service svchost.exe để thực thi mã độc |
|  |  |  |
|  |  |  |

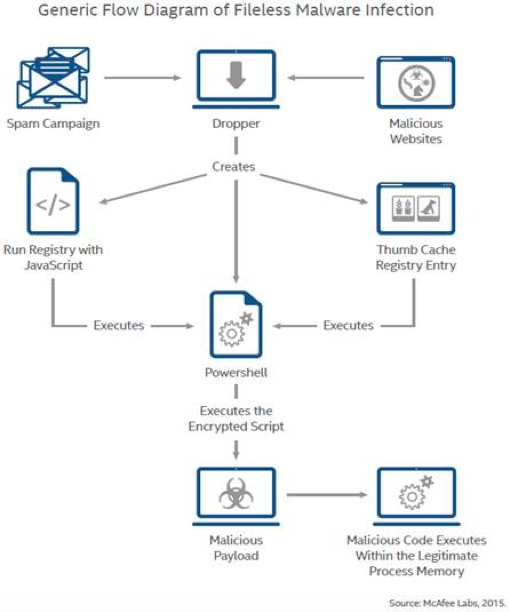
Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| TCPConnect | 12.34.56.78:6789 | Kết nối về máy chủ điều khiển |
|  |  |  |
|  |  |  |
|  |  |  |

# Phân tích nâng cao

*<Kết hợp phân tích tĩnh bằng IDA và debug bằng OllyDbg/x64dbg/… mô tả chi tiết luồng hoạt động của mã độc>*

*<Vẽ hình minh họa >*



*<Mô tả luồng hoạt động chi tiết, bao gồm cả các bước hoạt động, các thuật toán mã hóa, giao thức điều khiển, nếu cần có thể tách làm nhiều đầu mục nhỏ hơn>*

* Spam Campaign:
* Dropper:
* …

# Indicators of Compromise (IoC)

*<Danh sách các IoC của mã độc>*

Hashes:

* …

Host IoC:

* …

Network IoC:

* …