Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* |  |
| *MD5* |  |
| *SHA-1* |  |
| *SHA-256* |  |
| *File type* |  |
| *File size* |  |

# 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*: x86/x64

*Compilation Timestamp*: 2018-09-24 04:47:10

*Packer*: None/UPX/Manual…

*PE Size*: 342.5 KB (350720 bytes) - So sánh với filesize

*Các hàm import đặc trưng của mã độc*:

* …
* …

*Các hàm export nghi ngờ*:

* …
* …

*Resource Language*: Chinese

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 34/50
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky |  |
| Microsoft |  |
| Symantec |  |
| McAfee |  |
| BitDefender |  |

*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 | HKCU\Software\... | Tạo key autoruns |
|  |  |  |
|  |  |  |
|  |  |  |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| CreateProcess | C:\Windows\a.exe | Thực thi mã độc sau khi cài đặt |
|  |  |  |
|  |  |  |
|  |  |  |

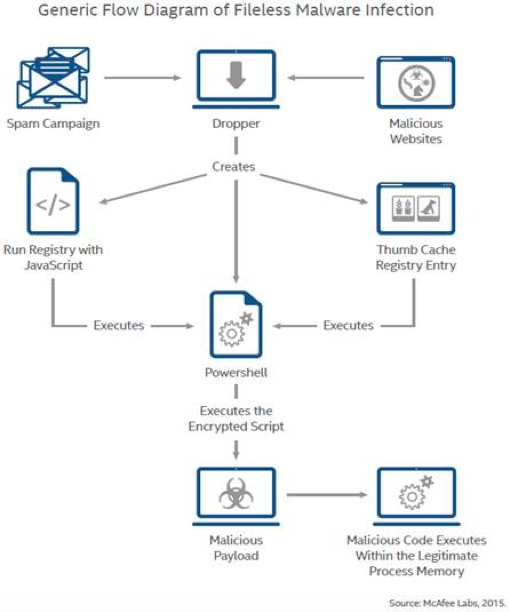
Network:

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

# Phân tích giao thức điều khiển của mã độc

*<Phân tích giao thức điểu khiển của mã độc (nếu có)>*

*<Xây dựng rule yara phát hiện traffic mạng của mã độc>*

# Indicators of Compromise (IoC)

*<Danh sách các IoC của mã độc>*

Hashes:

* …

Host IoC:

* …

Network IoC:

* …

Yara rules:

* …