Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | ClickMe.exe |
| *MD5* | 9161a1c4fb04ec05096401dd3decc5bb |
| *SHA-1* | 66c37bde1cb95732f46d057f7e3ae3e1011ab6ae |
| *SHA-256* | e3a43d0a8014bd96026a1dfd3bcfd90823232a73d54523aacf7209e654d1e413 |
| *File type* | PE |
| *File size* | 16.0 KB |

# Kết luận chung

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

|  |  |
| --- | --- |
| *Loại mã độc* | Trojan/backdoor |
| *Dòng mã độc* | PlugX |
| *Đặc điểm chính* | Mã độc thực hiện sao chép export tables của kernel32 vào export tables của EvilFile.dll(kerne132.dll). Sau đó tìm kiếm các file .exe trong thư mục “C\\” rồi thay thế import directory của các file này từ kernel32 thành kerne132 |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x86

*Compilation Timestamp*: 2010-12-19 08:16:19

*Packer*: None

*PE Size*: 16.0 KB (16,384 bytes) - So sánh với filesize

*Các hàm import đặc trưng của mã độc*:

* UnmapViewOfFile
* MapViewOfFile
* FindNextFileA
* FindFirstFileA
* CreateProcessA
* WSAStartup
* send
* shutdown
* recv
* WSACleanup

*Resource Language*: English

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 45/72
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Undetected |
| Microsoft | Trojan:Win32/Aenjaris.CT!bit |
| Symantec | ML.Attribute.HighConfidence |
| McAfee | RDN/Generic.grp |
| BitDefender | Trojan.GenericKD.42948263 |

*Các kết quả tìm kiếm khác:*

* EvilFile.dll hay kerne132.dll thực chất là một backdoor cho phép nhận lệnh từ máy chủ điều khiển và thực thi.

## 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\System32\Kerne131.dll | Copy bản thân vào thư mục Windows |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| CreateMutex | SADFHUHF | Tạo mutex để tránh việc lặp instance |

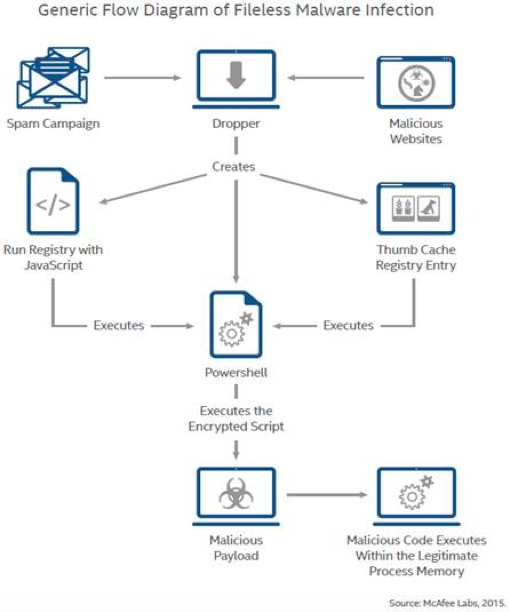
Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| TCPConnect | 127.26.152.13 | Nhận lệnh từ 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>*

* Trojan:
  + Mã độc copy các export tables từ kernel32.dll sang EvilFile.dll.
  + Sau khi copy mã độc đổi tên từ EvliFile.dll thành Kerne132.dll rồi copy bản thân vào thư mục Windows.
  + Sau thi copy thì sẽ tìm tất cả các file có đuôi .exe trong thư mục và thay thế import tables từ kernel32 thành import tables của Kerne132.dll.
* Backdoor:
  + Mã độc sau khi đã thay đổi import table thì có thể sử dụng Kerne132.dll như một backdoor.
  + Kernel132.dll nhận lệnh điều khiển thông qua winsocket tới địa chỉ ip 127.26.152.13 port 80.
  + Backdoor nhận lệnh điều khiển qua command “exec” bằng cách thực thi command với api CreateProcessA.

# Indicators of Compromise (IoC)

*<Danh sách các IoC của mã độc>*

Network IoC:

127.26.152.13:80