Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | ClickMe.exe |
| *MD5* | 9161A1C4FB04EC05096401DD3DECC5BB |
| *SHA-1* | 66C37BDE1CB95732F46D057F7E3AE3E1011AB6AE |
| *SHA-256* | E3A43D0A8014BD96026A1DFD3BCFD90823232A73D54523AACF7209E654D1E413 |
| *File type* | executable |
| *File size* | 16384 bytes |

# Kết luận chung

|  |  |
| --- | --- |
| *Loại mã độc* | Backdoor |
| *Dòng mã độc* | Trojan |
| *Đặc điểm chính* | Tạo backdoor và nhận lệnh điều khiển từ bên ngoài |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x86

*Compilation Timestamp*: Sun Dec 19 16:16:19 2010 UTC Microsoft Visual C++ v5.0/v6.0 (MFC)

*Packer*: None

*PE Size*: 16384 bytes

*Các hàm import đặc trưng của mã độc*:

* UnmapViewOfFile
* MapViewOfFile
* FindNextFileA
* FindFirstFileA

*Các hàm export nghi ngờ*:

* CreateFileMappingA
* MapViewOfFile

*Resource Language*: n/a

### Kết quả tìm kiếm online

*VirusTotal:*

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

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

*Các kết quả tìm kiếm khác:* n/a

## Phân tích động cơ bản

File System:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| WriteFile | C:\Windows\SysWOW64\kerne132.dll | Tạo một phiên bản giả của kernel32.dll, dllmain chứa code độc hại |
|  |  |  |
|  |  |  |
|  |  |  |

# Phân tích nâng cao

Chương trình đi kèm với một file DLL evil.dll. file evil.dll này được chỉnh sửa, copy những hàm export của kernel32 vào. Những hàm export này ko có code thật mà chỉ forward lại các export của kernel32. Sau khi đã craft xong dll fake thì dll fake này sẽ được copy vào Syswow64.

Chương trình sẽ tìm kiếm đệ quy tất cả các file thực thi (.exe) ở trong đĩa C:\. Nếu file .exe có import là kernel32.dll thì sẽ bị sửa thành kerne132.dll.

Phần DLL main có chứa code độc hại, dll main sẽ được gọi mỗi khi dll được nạp. dll main kết nối tới máy chủ điều kiển ở địa chỉ ip 127.26.152.13

Các command để điều kiển:

Sleep: chương trình sleep 393216ms

Exec: Toàn bộ payload đằng sau sẽ là command thực thi, bao gồm cả executable path. (a.exe command)

# Indicators of Compromise (IoC)

Hashes:

* n/a

Host IoC:

* Kerne132.dll

Network IoC:

* 127.26.152.13