Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | ClickMe.exe |
| *MD5* | 9161A1C4FB04EC05096401DD3DECC5BB |
| *SHA-1* | 66C37BDE1CB95732F46D057F7E3AE3E1011AB6AE |
| *SHA-256* | E3A43D0A8014BD96026A1DFD3BCFD90823232A73D54523AACF7209E654D1E413 |
| *File type* | Win32 EXE |
| *File size* | 16.00 KB (16384 bytes) |

|  |  |
| --- | --- |
| *Filename* | EvilFile.dll |
| *MD5* | 50914483F16D49BAC564D242C1531161 |
| *SHA-1* | 2F03D0D28B9A589B0D2E5A3C966D3EEE7086BD76 |
| *SHA-256* | 4D14FF78E074C9FA04DD66B9F725D1DDEA6886162A5FA2D4BC2213C7B9041C7D |
| *File type* | Win32 DLL |
| *File size* | 160.00 KB (163840 bytes) |

# Kết luận chung

|  |  |
| --- | --- |
| *Loại mã độc* | Trojan, Backdoor |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Mã độc thực hiện chỉnh sửa import của tất cả các file thực thi với mục đích khi chạy bất kì file **.exe** nào trong ổ **C:\** thì đều thực thi payload trong **DLL**.  Thực hiện kết nối tới server C&C và tiến hành điều khiển máy vicim bằng command. |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### ClickMe.exe

#### PE Header

*Target Machine*: x86/x64

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

*Packer*: None

*PE Size*: 16.00 KB (16384 bytes) - Bằng với filesize

*Các hàm import đặc trưng của mã độc*:

* KERNEL32.dll
  + CopyFileA
  + FindFirstFileA
  + FindNextFileA
  + FindClose
  + CreateFileMappingA
  + CreateFileA
  + MapViewOfFile
  + UnmapViewOfFile

#### 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 |

### EvilFile.dl

#### PE Header

*Target Machine*: x86/x64

*Compilation Timestamp*: 2010-12-19 16:16:38 UTC

*Packer*: None

*PE Size*: 160.00 KB (163840 bytes) – Bằng với file size

*Các hàm import đặc trưng của mã độc*:

* KERNEL32.dll
  + OpenMutexA
  + CreateMutexA
  + Sleep
  + CloseHandle
  + CreateProcessA
* WS2\_32.dll
  + socket
  + closesocket
  + inet\_addr
  + send
  + WSACleanup
  + WSAStartup
  + connect
  + shutdown
  + htons
  + recv

#### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 20/67
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Undetected |
| Microsoft | Undetected |
| Symantec | Undetected |
| McAfee | Undetected |
| BitDefender | Trojan.GenericKD.42976873 |

## Phân tích động cơ bản

### ClickMe.exe

File System:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| CreateFileMappingA | C:\Windows\system32\Kernel23.dll | Đọc export table |
| CreateFileMappingA | EvilFile.dll | Đọc và sửa (nếu có thay đổi) export table |
| CreateFileMappingA | C:\\*.exe | Sửa IMPORT DESCRIPTOR của các file **.EXE** bằng giá trị ***kerne132.dll*** với mục đích khi chạy bất kì file **.EXE** nào trong ổ **C:\** thì đều thực thi payload trong **DLL** |
| CopyFileA | Source: EvilFile.dll  Destination: C:\Windows\system32\kerne123.dll | Copy file **DLL** có payload vào thư mục Windows\system32 |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| CreateProcess | <nhận từ socket> | Thực thi mã độc |

Network:

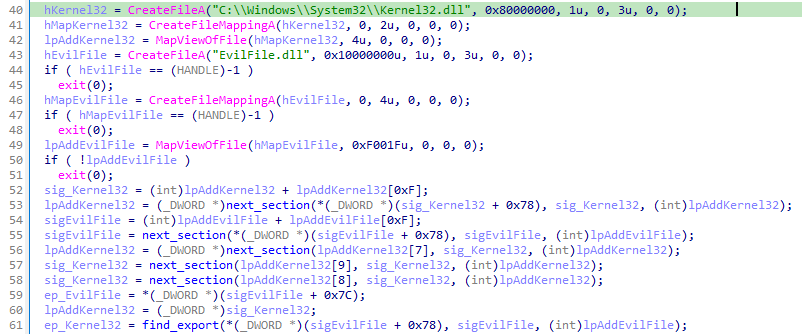
|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| Socket Connect | 127.26.152.13:80 | Kết nối socket về máy chủ |
| Socket Send | 127.26.152.13:80 | Gửi thông điệp “hello” đến máy chủ |
| Socket Recv | 127.26.152.13:80 | Nhận thông điệp từ máy chủ |

# Phân tích nâng cao

## Luồng hoạt động của mã độc:

### Clickme.exe

Mã độc tạo FileMapping đến *"****C:\Windows\System32\Kernel32.dll****"* và “***EvilFile.dll***” để lấy thông tin của IMAGE\_EXPORT\_DIRECTORY.



Tiến hành sao chép thông tin Export Table của *“****Kernel32.dll”*** sang “***EvilFile.dll***”



|  |  |
| --- | --- |
| “***EvilFile.dll***” trước khi sửa Export Table | “***EvilFile.dll***” sau khi sửa Export Table |
|  |  |

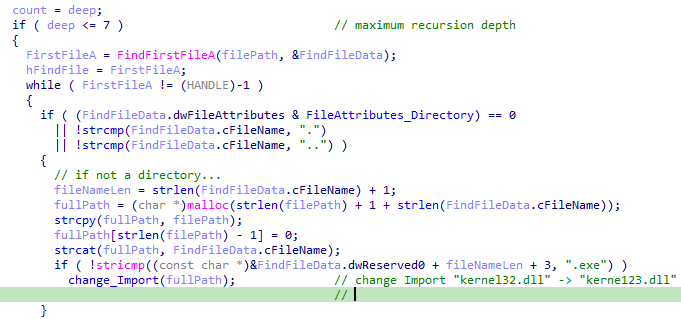
Sau đó mã độc copy file *“****EvilFile.dll”*** đến *"****C:\windows\system32\kerne132.dll****"* (với chữ ‘l’ được thay thế bằng số ‘1’) khiến ta dễ nhầm lẫn với file



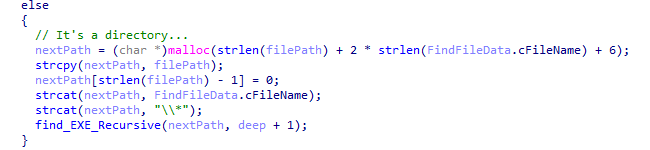
Sau khi sao lưu file “***EvilFile.dll***” thành công, mã độc thực hiện duyệt đệ quy tối đa 7 bậc tìm kiếm các file ***.exe*** trong ổ ***"C:\\*"*** để sửa thông tin Import Directory.



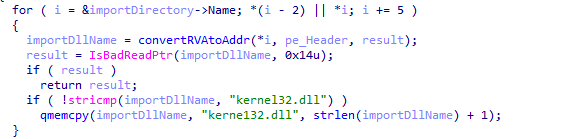
Trong mỗi bậc, tiến hành kiểm tra nếu là file ***.exe*** thực hiện sửa import của file từ ***“kernel32.dll”*** thành ***“kerne132.dll”*** (file được sao lưu từ “***EvilFile.dll***”).



Nếu là thư mục tiếp tục duyệt bậc tiếp theo.



Hàm **change\_Import()** tìm kiếm DLL Name của ***“kernel32.dll”*** sau đó thay thế bằng ***"kerne132.dll"***

******

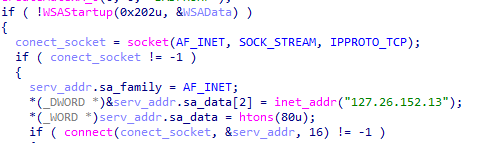
|  |  |
| --- | --- |
| ***“Scylla\_x86.exe”*** trước khi bị thay đổi Import | ***“Scylla\_x86.exe”*** sau khi bị thay đổi Import |
|  |  |

### EvilFile.dll

Mã độc kiểm tra xem đã có mutex "SADFHUHF" hay chưa, nếu chưa có sẽ tạo Mutex đó với mục đích tại một thời điểm chỉ có một mã độc hoạt động để tránh xung đột.



Mã độc kết nối đến máy chủ ***127.26.152.13:80.***

**

Và gửi thông điệp ***“hello”*** đến server và chờ server phản hồi.



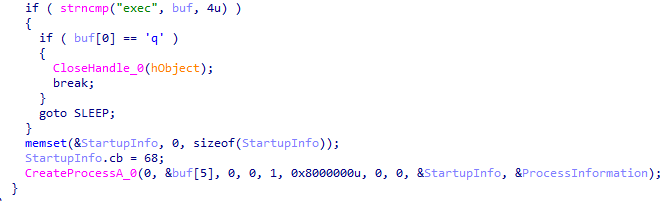
Mã độc nhận thông điệp từ server với các command:



* Nếu command có 5 bytes đầu là ***“sleep”*** thì sẽ thực hiện sleep 393216 mili giây (hơn 6 phút)



* Nếu 4 bytes đầu là ***“exec”*** thì sẽ tạo một process bằng hàm **CreateProcess** với tên tiến trình là đoạn string sau ***“exec”.*** Sau đó cũng sleep 393216 mili giây.



* Nếu byte đầu là ***“q”*** mã độc sẽ tự kết thúc chính nó.

## Hành vi hoạt động của loại mã độc:

### Trojan:

Mã độc copy các Export Table từ ***Kernel32.dll*** sang ***EvilFile.dll*** sau đó copy vào thư mục Windows với tên ***kerne132.dll***.

Sau đó sẽ tìm tất cả các file có đuôi ***.exe*** trong thư mục ***C:\\**** và thay thế DLL name Import Directory từ ***kernel32.dll*** thành ***kerne132.dll***.

### Backdoor:

Các file ***.exe*** sau khi bị thay đổi import khi thực thi thì ***DLLMain*** của ***kerne132.dll*** được thực thi như một backdoor tạo kết nối đến server C&C có địa chỉ **127.26.152.13** port **80** và nhận command (lệnh từ sever).

# Indicators of Compromise (IoC)

Hashes:

* 4d14ff78e074c9fa04dd66b9f725d1ddea6886162a5fa2d4bc2213c7b9041c7d
* e3a43d0a8014bd96026a1dfd3bcfd90823232a73d54523aacf7209e654d1e413

Network IoC:

* 127.26.152.13:80