Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | msbuild.exe |
| *MD5* | 79ad2084b057847ce2ec2e48fda64073 |
| *SHA-1* | f5a1bf349e82f1b044cfa375d119380f973ad0e5 |
| *SHA-256* | 290ac98de80154705794e96d0c6d657c948b7dff7abf25ea817585e4c923adb2 |
| *File type* | PE32 |
| *File size* | 132 KB |

# Kết luận chung

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

|  |  |
| --- | --- |
| *Loại mã độc* | Stealer |
| *Dòng mã độc* | PatchWork APT |
| *Đặc điểm chính* | Đánh cắp thông tin của máy tính nạn nhân và gửi về máy chủ điều khiển. |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x86

*Compilation Timestamp*: 2017-12-22 03:54:03

*Packer*: None

*PE Size*: 132KB (135,496 bytes) - So sánh với filesize

*Các hàm import đặc trưng của mã độc*:

* OpenProcess
* GetCurrentProcessId
* GetEnvironmentVariableW
* FindNextFileW
* GetLogicalDriveStringsW
* DeleteFileA
* WriteFile
* FindFirstFileW
* CreateProcessW
* GetEnvironmentStringsW
* GetExitCodeProcess
* SetEnvironmentVariableA
* GetCurrentThreadId
* CreateProcessA
* TerminateProcess
* RaiseException
* GetDesktopWindow
* MapVirtualKeyExW
* InternetOpenW
* InternetConnectA
* InternetOpenUrlW
* InternetReadFile
* HttpOpenRequestA
* InternetGetConnectedState
* InternetCheckConnectionA
* HttpSendRequestA
* InternetOpenA
* InternetCloseHandle

*Resource Language*: English.

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 53/70
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Trojan.Win32.JakyllHyde.p |
| Microsoft | Trojan:Win32/JakyllHyde.SA!MSR |
| Symantec | ML.Attribute.HighConfidence |
| McAfee | Trojan-FPIU!79AD2084B057 |

*Các kết quả tìm kiếm khác:*

* Mã độc thực hiện đánh cắp các thông tin như keylog, process, filename để gửi về máy chủ điều khiển.
* Mã độc thực hiện obfuscate string bằng cộng ascii của từng ký tự string lên 1 đơn vị

## 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** |
| GetTempPath | C:\Users\%User%\AppData\Local\Temp\edg499.dat | Tạo file để list các file txt và file office. |
| GetTempPath | C:\Users\%User%\AppData\Local\Temp\9PT568.dat | Lấy thông tin về hardware của máy nạn nhân. |
| GetTempPath | C:\Users\%User%\AppData\Local\Temp\TPX498.dat | Lấy keylog và running process của máy nạn nhân. |
| GetTempPath | C:\Users\%User%\AppData\Local\Temp\TPX499.dat | Lấy ảnh chụp màn hình của mày nạn nhân. |

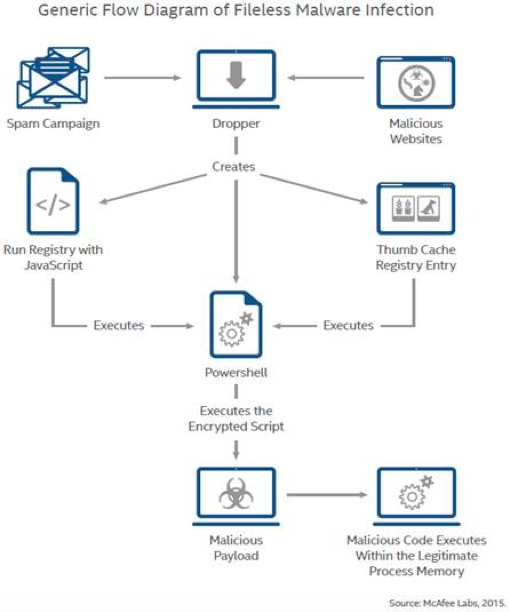
Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **IP** | **Mô tả** |
| TCPConnect | *http://185.203.118.115* | 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>*

* Mã độc tạo mutex tên “*com\_mycompany\_apps\_appname\_new*” để tránh bị lặp thực thi.
* Mã độc sau đó thực hiện sleep chương trình bằng cách chạy vòng lặp 80000 lần.
* C2 server sau khi được resolve là *http://185.203.118.115.*
* Sau khi resolve c2 server, mã độc thực hiện thu thập thông tin của máy nạn nhân bao gồm username, hostname, system version, ip addressvà những thông tin khác mã bị độc lấy lưu vào các file trong thư mục %temp% bao gồm:
  + edg499.dat lưu danh sách các file txt và file các office của Microsoft
  + 9PT568.dat lấy thông tin về hardware qua windows api *GetCurrentHwProfileA*.
  + TPX498.dat lấy thông tin về keylog và running process của máy nạn nhân.
* Sau khi đã lấy được thông tin của máy nạn nhân, mã độc thực hiện connect với c2 server thông qua command.
  + 8: upload file TPX498.dat(keylogger + running process) lên c2 server.
  + 23: upload file TPX499.dat(screenshot) lên c2 server.
  + 13: upload file AdbFle.tmp(time) lên c2 server.
  + 4: upload file edg499.dat(GetCurrentHwProfileA) lên c2 server.
  + 33: download payload từ c2 server về để thực thi.

# Indicators of Compromise (IoC)

*<Danh sách các IoC của mã độc>*

Host IoC:

* https://raw.githubusercontent.com/lctst/testlct/master/xml.xml
* http://feed43.com/3210021137734622.xml
* http://feeds.rapidfeeds.com/88604

Network IoC:

* 185[.]203.118.115