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

|  |  |
| --- | --- |
| *Loại mã độc* | Stealer |
| *Dòng mã độc* | PatchWork APT |
| *Đặc điểm chính* | Đánh cắp thông tin của máy bị nhiễm 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*:

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

*Resource Language*: n/a

### 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 c2.
* Mã hóa string cộng mã ascii của từng ký tự lên 1 đơn vị

## Phân tích động cơ bản

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

* Mã độc tạo mutex tên “*com\_mycompany\_apps\_appname\_new*”. Không chạy lại trên máy đã bị lây nhiễm.
* Spin lock wait 80000 loop
* C2 server: 185.203.118.115.
* Thực hiện thu thập thông tin của máy bị lây nhiễm bao gồm username, hostname, system version, ip address và những thông tin khác, file log được lưu vào các file trong thư mục %temp% bao gồm:

1. edg499.dat lưu danh sách các file txt và file các office của Microsoft
2. 9PT568.dat lưu thông tin về hardware qua windows api *GetCurrentHwProfileA*.
3. TPX498.dat lưu thông tin về keylog và running process của máy nạn nhân.
4. TPX499.dat lưu screen shot

* Sau khi đã lấy được thông tin của máy nạn nhân, mã độc thực hiện connect với command-control (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.

# Indicators of Compromise (IoC)

Host IoC:

* com\_mycompany\_apps\_appname\_new
* %temp%\edg499.dat
* %temp%\9PT568.dat
* %temp%\TPX498.dat
* %temp%\TPX499.dat
* 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