**Kết quả phân tích mã độc**

* **Thông tin mẫu**

|  |  |
| --- | --- |
| *Filename* | Monitor1.exe |
| *MD5* | 625ac05fd47adc3c63700c3b30de79ab |
| *SHA-1* | 9369d80106dd245938996e245340a3c6f17587fe |
| *SHA-256* | 0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126 |
| *File type* | PE32 |
| *File size* | 36.00 KB |

* **Kết luận chung**

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

|  |  |
| --- | --- |
| *Loại mã độc* | Dropper, Trojan |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Mã độc thực hiện disable Windows File Protection (SfcTerminateWatcherThread). Copy *wupdmgr.exe* thành *winup.exe,* và thực hiện extract payload ra *wupdmgr.exe* để thực thi*.* |

* **Phân tích cơ bản**
* ***Phân tích tĩnh cơ bản***
* *PE Header*

*Target Machine*: x86

*Compilation Timestamp*: 2019-08-30 15:26:59

*Packer*: None

*PE Size*: 36.00 KB (36,864 bytes) - So sánh với filesize

*Các hàm import đặc trưng của mã độc*:

* CreateRemoteThread
* OpenProcessToken
* AdjustTokenPrivileges
* WinExec
* URLDownloadToFileA

*Resource Language*: English

*VirusTotal:*

* Tỉ lệ nhận diện: 55/69
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | HEUR:Trojan-Downloader.Win32.Generic |
| Microsoft | TrojanDownloader:Win32/Small!MSR |
| Symantec | ML.Attribute.HighConfidence |
| McAfee | GenericRXEW-DZ!625AC05FD47A |

*Các kết quả tìm kiếm khác:*

* Disable Window File Protection bằng cách inject hàm SfcTerminateWatcherThread vào winlogon.exe.
* Mã độc chứa 1 resource có tên 101 là một executable thực thi *wupdmgr.exe* từ file *%temp% (dưới tên là winup.exe),* thực hiện download binary từ [*http://www.practicalmalwareanalysis.com/updater.exe*](http://www.practicalmalwareanalysis.com/updater.exe)*,* dump vào file wupdmgr.exevà 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:\system32\wupdmgr.exe | Copy bản thân vào thư mục Windows |
| WriteFile | C:\system32\winup.exe | Thay thế thư mục Windows |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| CreateProcess | C:\Windows\ winlogon.exe | Lợi dụng thư mục Windows để thay đổi quyền sửa file hệ thống |
| CreateRemoteThread | C:\Windows\ winlogon.exe | Inject hàm vào process -> disable Window File Protection |

Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| TCPConnect | <http://www.practicalmalwareanalysis.com/updater.exe> | Tải file về và dump vào wupdmgr.exe |