Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | 7zFM.exe |
| *MD5* | e2b6c32d4ed3b253ca750b03b55acad1 |
| *SHA-1* | e630f10249f521c5802e79d6f44c67f310384ad1 |
| *SHA-256* | a0b92392ade4ad7218239ac6a3e96ec6a626b71c187960cd077c92dc34d2330d |
| *File type* | PE32 |
| *File size* | 557 KB |

# Kết luận chung

|  |  |
| --- | --- |
| *Loại mã độc* | Trojan/dropper |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Mã độc drop 1 file *7zFMmgr.exe* để thực thi mở 1 process IExplorer liên lạc với các host lạ và kill tiến trình gốc. |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x86

*Compilation Timestamp*: 2010-11-18 08:09:00

*Packer*: Manual

*PE Size*: 557 KB (570,389 bytes) - So sánh với filesize

*Các hàm import đặc trưng của mã độc*:

* srand
* rand
* WNetCloseEnum
* WNetAddConnection2W
* WNetAddConnection2A
* UnmapViewOfFile
* SystemParametersInfoA
* ShellExecuteA
* RegSetValueExA
* RegDeleteKeyA
* OpenClipboard
* MoveFileW
* MoveFileA
* MapVirtualKeyA
* MapViewOfFile
* SetPriorityClass
* SetFileAttributesW
* SetFileAttributesA
* SetClipboardData
* SHGetSpecialFolderLocation
* SHGetPathFromIDListA
* SHGetFileInfoA
* SHFileOperationA
* SHChangeNotify
* ShellExecuteExA
* SHBrowseForFolderA
* RemoveDirectoryW
* RemoveDirectoryA
* RegisterClipboardFormatA
* RegSetValueExW
* GetTempFileNameW
* GetTempFileNameA
* GetLogicalDriveStringsW
* GetLogicalDriveStringsA
* GetKeyState
* GetCapture
* FindNextFileW
* FindNextFileA
* FindNextChangeNotification
* FindFirstFileW
* FindFirstFileA
* FindFirstChangeNotificationW
* FindFirstChangeNotificationA
* FindCloseChangeNotification
* EmptyClipboard
* DeviceIoControl
* DeleteFileW
* DeleteFileA
* CreateProcessW
* CreateProcessA
* WriteFile
* WNetOpenEnumW
* WNetOpenEnumA
* WNetGetResourceParentW
* WNetGetResourceParentA
* WNetGetResourceInformationW
* WNetGetResourceInformationA
* WNetEnumResourceW
* WNetEnumResourceA

*Resource Language*: n/a

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 64/72
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Virus.Win32.Nimnul.a |
| BitDefender | Win32.Ramnit.N |
| Microsoft | Virus:Win32/Ramnit.P |
| Symantec | W32.Ramnit.B!inf |
| McAfee | W32/Ramnit.a |

## Phân tích động cơ bản

File System:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| WriteFile | %AppData%/local/temp/~TM…tmp | Copy dll vào temp để gọi thực thi mã độc |

Registry:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| RegSetValue | Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\htmlfile\shell\open\command | Tạo key autoruns |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| CreateProcess | 7zFMmgr.exe | Tạo process IEXPlORER |
| CreateProcess | C:\Program Files\Internet Explorer\IEXPLORE.EXE | Thực hiện kết nối với các host |

Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| TCPConnect | fkjdeljfeew32233.com | Kết nối về máy chủ điều khiển |
|  | pornoliks.com | Kết nối về máy chủ điều khiển |
|  | stromoliks.com | Kết nối về máy chủ điều khiển |
|  |  |  |