Kết quả phân tích mã độc

## Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | Monitor-2.exe |
| *MD5* | d537acb8f56a1ce206bc35cf8ff959c0 |
| *SHA-1* | 0bb491f62b77df737801b9ab0fd14fa12d43d254 |
| *SHA-256* | eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffcedd |
| *File type* | PE32 |
| *File size* | 7.00 KB |

## Kết luận chung

|  |  |
| --- | --- |
| *Loại mã độc* | Backdoor |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Mã độc tự sao chép vào hệ thống với tên ***:\WINDOWS\system32\vmx32to64***, tạo registry ***HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver*** tự khởi động cùng hệ thống  Connect với host [**www.practicalmalwareanalysis.com**](http://www.practicalmalwareanalysis.com) mỗi giây qua socket. |

## Phân tích cơ bản

### Phân tích tĩnh cơ bản

#### PE Header

*Target Machine*: x86

*Compilation Timestamp*: 2008-01-06 21:51:31

*Packer*: None

*PE Size*: 7.00 KB (7,168 bytes bytes) - So sánh với filesize

*Các hàm import đặc trưng của mã độc*:

* CreateFile
* CreateMutexA
* RegOpenKey
* RegQuerryValue
* RegCloseKey
* Bind
* Select
* Connect
* Listen

*Resource Language*: English

#### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 61/68
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Backdoor.Win32.Poison.aec |
| Microsoft | Backdoor:Win32/Poison.E |
| McAfee | BackDoor-DSS.gen.a |

### 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:\WINDOWS\system32\vmx32to64.exe | Copy bản thân vào thư mục Windows. |

Registry:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| RegSetValue | *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver* | Tạo key startup |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Name** | **Mô tả** |
| CreateMutextA | WinVMX32 | Kiểm tra xem mã độc đã tồn tại ở thư mục window |

Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| TCPConnect | www.practicalmalwareanalysis.com | Kết nối về máy chủ điều khiển. |