Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | Monitor-3.exe |
| *MD5* | e2bf42217a67e46433da8b6f4507219e |
| *SHA-1* | daf263702f11dc0430d30f9bf443e7885cf91fcb |
| *SHA-256* | ae8a1c7eb64c42ea2a04f97523ebf0844c27029eb040d910048b680f884b9dce |
| *File type* | PE32 |
| *File size* | 52.00 KB |

# Kết luận chung

|  |  |
| --- | --- |
| *Loại mã độc* | Keylogger |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Mã độc thực hiện tạo process svchost.exe trong hệ thống rồi kill tiến trình gốc. Khi thực thi, mã độc tạo một file txt có tên practicalmalwareanalysis lưu lại bàn phím nhập. |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x86

*Compilation Timestamp*: 2011-04-09 00:54:23

*Packer*: None

*PE Size*: 52.0 KB (53,248 bytes)

*Các hàm import đặc trưng của mã độc*:

* GetThreadContext
* WriteProcessMemory
* ReadProcessMemory
* TerminateProcess
* FindResourceA
* LoadResource
* CreateProcessA

*Resource Language*: English

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 57/67
* Dòng mã độc:

|  |  |
| --- | --- |
| McAfee | GenericRXCM-BE!E2BF42217A67 |
| Kaspersky | Trojan.Win32.Agent.hwkc |
| Microsoft | Clean |
| BitDefender | Gen:Trojan.ExplorerHijack.dqW@aO9ui3p |

*Các kết quả tìm kiếm khác:*

Phần mã thực thi nguy hại được chứa ở trong resource của file thực thi, được mã hóa xor key là 65. Mã độc thực hiện dump resource ra để inject persistent vào thư mục hệ thống với ***GetModuleHandleA*** tên ***svchost.exe*** ghi lại input người dùng vào file log. Chỉ log những process dạng console. Terminate tiến trình gốc và chạy lại để bắt đầu keylog.

## Phân tích động cơ bản

File System:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| WriteFile | Currentdirectory\practicalmalwareanalysis.log | Ghi lại bàn phím vào file log |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Name** | **Mô tả** |
| LoadResource | LOCALIZATION | Load code đã được mã hóa vào để inject persistent **svchost.exe** |