Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* |  |
| *MD5* | 5ea7be193d22f7c0ac0f541be33645b7 |
| *SHA-1* | d2b25acfce47031b48361592d60c8f5b8e6c79de |
| *SHA-256* | 18576950eb9eb965cb49bcde31ce4bcc7f2803b1f42cc7ff6a4354800748d711 |
| *File type* | PE32 |
| *File size* | 40.00 KB |

# Kết luận chung

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

|  |  |
| --- | --- |
| *Loại mã độc* | stealer |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Lấy thông tin từ file signons.txt của trình duyệt firefox. |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x86

*Compilation Timestamp*: 2008-06-05 13:11:12

*Packer*: None

*PE Size*: 40.00 KB (40960 byte) - So sánh với filesize

*Các hàm import đặc trưng của mã độc*:

* TerminateProcess
* GetEnvironmentStrings
* GetEnvironmentStringsW
* GetCurrentThreadId
* WriteFile
* OpenProcessToken
* GetUserProfileDirectoryA

*Các hàm export nghi ngờ*:

* …
* …

*Resource Language*: English

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 25/72
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | UDS:DangerousObject.Multi.Generic |
| Microsoft | Trojan:Win32/Wacatac.C!ml |
| Symantec | Trojan Horse |
| McAfee | Generic.djt |
| BitDefender | Undetected |

*Các kết quả tìm kiếm khác:*

* Nêu các thông tin về mã độc tìm được (dòng mã độc, hành vi, các cuộc tấn công, các thông tin khác…)

## Phân tích động cơ bản

*<Thực hiện monitor hành vi của mã độc, liệt kê các hành vi đặc trưng>*

File System:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Name** | **Mô tả** |
| ReadFile | signons.txt | Đọc nội dung file signons.txt chứa thông tin về password và username của firefox. |
| ReadFile | signons2.txt | Đọc nội dung file signons.txt chứa thông tin về password và username của firefox. |
| ReadFile | signons3.txt | Đọc nội dung file signons.txt chứa thông tin về password và username của firefox. |

Registry:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| RegQuerryValue | SOFTWARE\Clients\StartMenuInternet\firefox.exe\shell\open\command | Querry registry để lấy path của firefox |

# Phân tích nâng cao

*<Kết hợp phân tích tĩnh bằng IDA và debug bằng OllyDbg/x64dbg/… mô tả chi tiết luồng hoạt động của mã độc>*

*<Mô tả luồng hoạt động chi tiết, bao gồm cả các bước hoạt động, các thuật toán mã hóa, giao thức điều khiển, nếu cần có thể tách làm nhiều đầu mục nhỏ hơn>*

* Mã độc thực hiện đọc file profile.ini để lấy profile path của firefox và lấy querry registry *SOFTWARE\Clients\StartMenuInternet\firefox.exe\shell\open\command* để lấy path của firefox qua value của registry này.
* Khi đã có path của firefox, mã độc thực hiện load các dll
  + nspr4.dll
  + plc4.dll
  + plds4.dll
  + softokn3.dll
  + nss3.dll
* profile path của firefox dùng để
* …