Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | dependencies.exe |
| *MD5* | 5ea7be193d22f7c0ac0f541be33645b7 |
| *SHA-1* | d2b25acfce47031b48361592d60c8f5b8e6c79de |
| *SHA-256* | 18576950eb9eb965cb49bcde31ce4bcc7f2803b1f42cc7ff6a4354800748d711 |
| *File type* | Win32 EXE |
| *File size* | 40.00 KB (40960 bytes) |

# Kết luận chung

|  |  |
| --- | --- |
| *Loại mã độc* | Stealer |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Mã độc lấy thông tin của người dùng 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 20:11:12 UTC

*Packer*: None

*PE Size*: 40.00 KB (40960 bytes) - Bằng với File Size

*Các hàm import đặc trưng của mã độc*:

* ADVAPI32.dll
  + RegOpenKeyExA
  + RegQueryValueExA
* KERNEL32.dll
  + GetEnvironmentStringsW
  + GetCommandLineA
  + GetCurrentThreadId
  + WriteFile
  + OpenProcessToken
  + LoadLibraryA
  + GetProcAddress
* USERENV.dll
  + GetUserProfileDirectoryA

*Các hàm export nghi ngờ*:

* + start

### 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 |

## Phân tích động cơ bản

File System:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **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. |

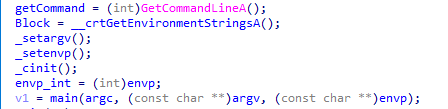
Registry:

|  |  |  |
| --- | --- | --- |
| RegQueryValueExA | SOFTWARE\\Clients\\StartMenuInternet\\firefox.exe\\shell\\open\\command | Thực hiện lấy đường dẫn của firefox. |

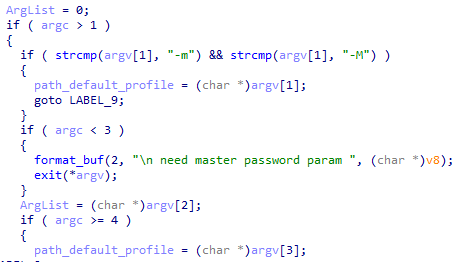
# Phân tích nâng cao

## Luồng hoạt động của mã độc:

Trong hàm ***start()*** mã độc thực hiện gọi hàm ***main()*** với command line argument được người dùng nhập vào.



Thực hiện kiểm tra command line, yêu cầu nhập ***“password param”*** nếu số lượng param truyền vào nhỏ hơn 3.



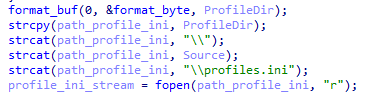
Sau đó mã độc thực hiện đọc file ***profile.ini*** để lấy profile path của ***firefox***.



Truy xuất đường dẫn đến thư mục root của người dùng và lấy path của file profile.ini.

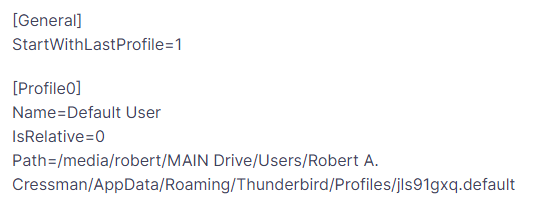






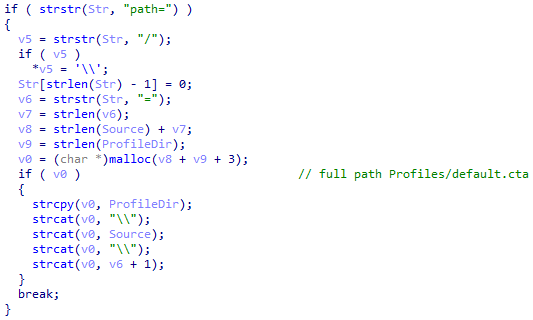
Thực hiện đọc file ***profile.ini*** và nội dung trong file có dạng sau.





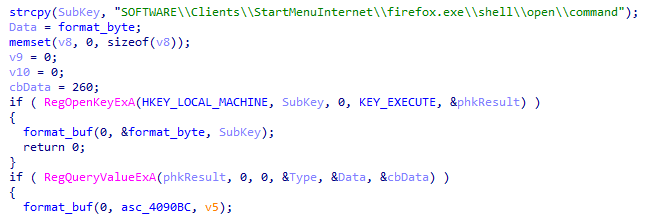
Lấy default profile path.





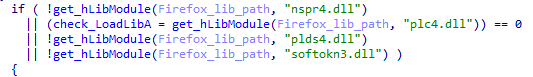
Tiếp theo mã độc lấy path của firefox thông qua value của registry “***SOFTWARE\Clients\StartMenuInternet\firefox.exe\shell\open\command”***





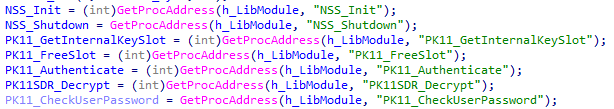
Sau khi lấy được path của firefox mã độc thực hiện load các dll:

* + nspr4.dll
  + plc4.dll
  + plds4.dll
  + softokn3.dll
  + nss3.dll





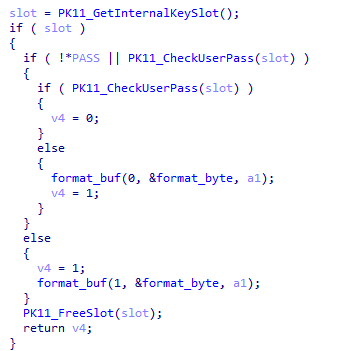
Và truy xuất địa chỉ của các hàm cần dùng.

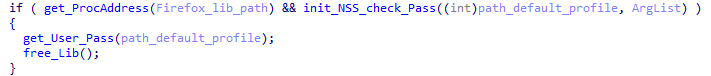




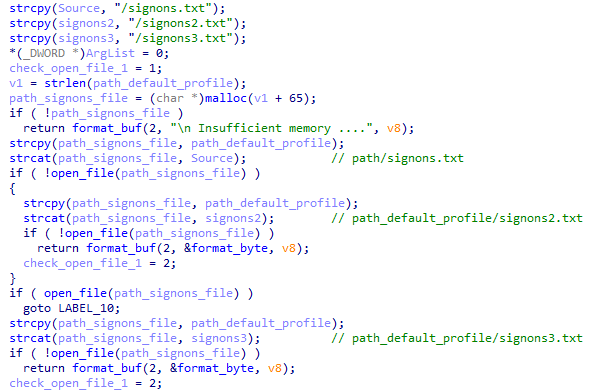
Mã độc kiểm tra password do người dùng nhập khi gọi hàm ***main*** với password admin của firefox.



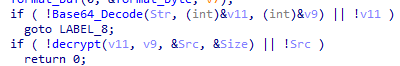


Nếu đúng thực hiện đọc các file ***“signons.txt”*** để lấy tất cả các user và password của người dùng. 

Đọc lần lượt các file “signons.txt”, “signons2.txt”, “signons3.txt” chứa user và mật khẩu đã được mã hóa bằng Base64.



Thực hiện decrypt mã độc sẽ lấy được user và mật khẩu người dùng.



## Hành vi hoạt động của loại mã độc:

### Stealer:

Mã độc lấy thông tin của người dùng từ file ***signons.txt*** của trình duyệt firefox.

# Indicators of Compromise (IoC)

Hashes:

* 18576950eb9eb965cb49bcde31ce4bcc7f2803b1f42cc7ff6a4354800748d711