Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | RasTls.dll |
| *MD5* | ad5529370ae4c328efca74090acbce4e |
| *SHA-1* | 6d6ed63e7ace329a3467181ece2529c4cfe1a565 |
| *SHA-256* | 0f421253dfc0d696626b9923a8472ed741cbebae208314b7e9dbc722a6ec0d38 |
| *File type* | Win32 DLL |
| *File size* | 169.50 KB |

# Kết luận chung

|  |  |
| --- | --- |
| *Loại mã độc* | Remote access trojan |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | DLL Hijacking |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x86

*Compilation Timestamp*: 2015-08-14 01:53:03

*Packer*: None

*PE Size*: 169.50 KB (173,568 bytes) - So sánh với filesize

*Các hàm import đặc trưng của mã độc*:

* RegOpenKeyExA
* RegSetValueExW
* RegCloseKey
* VirtualAllocEX
* CreateToolhelp32Snapshot
* OpenProcess
* TerminateProcess

*Các hàm export nghi ngờ*:

* RasEapFreeMemory
* RasEapGetIdentity
* RasEapInvokeInteractiveUI

*Resource Language*: English

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 47/71
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | UDS:DangerousObject.Multi.Generic |
| Microsoft | Trojan:Win32/Skeeyah.A!bit |
| Symantec | ML.Attribute.HighConfidence |
| McAfee | GenericRXAA-AA!AD5529370AE4 |
| BitDefender | Trojan.GenericKD.42974116 |

*Các kết quả tìm kiếm khác:*

https://www.upguard.com/blog/dll-hijacking

rastlsc.exe là một phần mềm hợp pháp được cung cấp bởi Symantec. Hành vi độc hại được giấu ở trong dll RasTls.dll để tránh bị detect. Kết thúc thực thi, binary thực hiện start dllhost.exe làm persistent connect đến một domain máy chủ điều khiển, tạo reg key autostart cùng window. Terminate tiến trình gốc.

## Phân tích động cơ bản

Registry:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| RegSetValue | SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Userinit | Tạo key autoruns |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| CreateProcess | C:\Windows\SysWOW64\dllhost.exe | Tạo process dllhost.exe connect với  domain *hou.phimnoi.org* |
| TerminateProcess | C:\Windows \rundll32.exe | Terminate dll được hijack vào tiến trình gốc, từ đó terminate tiến trình gốc |

Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Domain** | **Mô tả** |
| TCPConnect | hou.phimnoi.org | Kết nối đến domain |