Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | MSRSAAP.EXE |
| *MD5* | 08174d88b1ab8d5c46a86ec40620afb5 |
| *SHA-1* | eadc13f3a9afb4b2229fe60f2550c3e4c129115c |
| *SHA-256* | ddff9a6a442b85be442f9ea366206a77ae95c64216daca2c401d65a861741ff0 |
| *File type* | PE32 |
| *File size* | 658 KB |

# Kết luận chung

|  |  |
| --- | --- |
| *Loại mã độc* | RAT, Keylogger |
| *Dòng mã độc* | DarkComet |
| *Đặc điểm chính* | Resource lưu code độc hại được mã hóa. Mã độc giải mã resource lưu thông tin config. Dựa vào thông tin config để thực thi lưu keylog và clipboard của máy. |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x86

*Compilation Timestamp*: 2012-06-07 08:59:53

*Packer*: None

*PE Size*: 658 KB (674,304 bytes) - So sánh với filesize

*Các hàm import đặc trưng của mã độc*:

* InternetReadFile
* InternetOpenUrlA
* InternetOpenA
* InternetConnectA
* InternetCloseHandle
* GetKeyboardType
* GetCurrentThreadId
* FindFirstFileA
* WriteFile
* RaiseException
* WSACleanup
* WSAStartup
* WSAGetLastError
* gethostname
* getservbyname
* gethostbyname
* gethostbyaddr
* socket
* shutdown
* sendto
* send
* select
* recv
* ntohs
* listen
* ioctlsocket
* inet\_ntoa
* inet\_addr
* htons
* getsockname
* connect
* closesocket
* bind
* accept
* ShellExecuteExA
* ShellExecuteA
* SHGetFileInfoA
* SHFileOperationA
* URLDownloadToFileA
* HttpQueryInfoA
* FtpPutFileA
* Netbios

*Resource Language*: English

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 61/67
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Backdoor.Win32.DarkKomet.xyk |
| Microsoft | Backdoor:Win32/Fynloski.PA!MTB |
| Symantec | Backdoor.Graybird |
| McAfee | Generic BackDoor.xa |

*Các kết quả tìm kiếm khác:*

* Mã độc thuộc dark commet thu thập thông tin người dùng vào file.dc trong %AppData%. Khởi chạy một Process IExplorer thông qua notepad.exe để liên lạc đến host *botnet.no-ip.inf* , nếu thực thi binary qua cmd thì mã độc sẽ copy bản thân vào thư mục %Document% để kết nối đến host *botnet.no-ip.info*.

## Phân tích động cơ bản

File System:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| WriteFile | C:\Users\%username%\Documents\msdcsc.exe | Di chuyển vào Document |

Registry:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| RegSetValue | Software\Microsoft\Windows\CurrentVersion\Run\MicroUpdate  Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit | Tạo key autoruns – persistent |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Name** | **Mô tả** |
| CreateProcess | notepad | Thực thi mã độc sau khi cài đặt |

Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **IP** | **Mô tả** |
| TCPConnect | botnet.no-ip.info:4129 | Kết nối về máy chủ điều khiển |