Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | virus-ransomware-6e080aa085293bb9fbdcc9015337d309.exe.exe |
| *MD5* | 6e080aa085293bb9fbdcc9015337d309 |
| *SHA-1* | 51b4ef5dc9d26b7a26e214cee90598631e2eaa67 |
| *SHA-256* | 9b462800f1bef019d7ec00098682d3ea7fc60e6721555f616399228e4e3ad122 |
| *File type* | PE32 |
| *File size* | 257 KB |

# Kết luận chung

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

|  |  |
| --- | --- |
| *Loại mã độc* | Ransomware |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Mã độc tống tiền thực hiện mã hóa các file document, ảnh,.. đổi tên file bị mã hóa thành đuôi .ecc |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x86

*Compilation Timestamp*: 1969-12-31 16:00:00

*Packer*: None

*PE Size*: 257 KB (263,680 bytes)

*Các hàm import đặc trưng của mã độc*:

* ZwUnmapViewOfSection
* VirtualAllocEx
* WriteProcessMemory
* ResumeThread
* ShellExecuteExW
* InternetOpenUrlW
* InternetReadFile
* InternetSetCookieW
* GetEnvironmentVariableW
* PathFindFileNameW
* OpenClipboard
* SetClipboardData
* GetVolumeInformationW
* TerminateProcess
* DeleteFileW

*Resource Language*: English

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 59/68
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Trojan-Ransom.Win32.Bitman.acta |
| Microsoft | Ransom:Win32/Tescrypt.B |
| Symantec | Trojan.Gen.2 |
| McAfee | Ransom-TeslaCrypt.a |
| BitDefender | Gen:Variant.Ransom.TeslaCrypt.24 |

*Các kết quả tìm kiếm khác:*

* Mã độc sử dụng kỹ thuật hollowing process để đẩy stage2 vào process. Code của stage2 được encrypt trong resource.

## Phân tích động cơ bản

Registry:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| RegSetValue | Software\Microsoft\Windows\CurrentVersion\Run\msconfig | Tạo key autoruns |
|  | Software\Microsoft\Windows\CurrentVersion\Run\svcav\_module |  |

Process:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| CreateProcess | C:\Windows\a.exe | Thực thi mã độc sau khi cài đặt |
| TerminateProcess | Taskmgr  Procexp  Regedit  Msconfig  cmd.exe | Terminate các process trên, không cho phép thực thi. |

Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| TCPConnect | http://3kxwjihmkgibht2s.wh47f2as19.com | Kết nối về máy chủ điều khiển |
|  | <http://34r6hq26q2h4jkzj.7hwr34n18.com>  http://34r6hq26q2h4jkzj.onion |  |
|  | https://3kxwjihmkgibht2s.s5.tor-gateways.de/ |  |