Kết quả phân tích mã độc

# Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | ExplorerEditor.dll |
| *MD5* | a42e212ee0cad5eb23da87e6fb9614ad |
| *SHA-1* | 846c0856f7b18c34cb786c75614c49ce10fbd612 |
| *SHA-256* | 8e398f0b5d98a231e544b4505ac7a873976e60093a54b7c3f5cecbab5796fd1b |
| *File type* | PE |
| *File size* | 27.0 KB |

# Kết luận chung

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

|  |  |
| --- | --- |
| *Loại mã độc* | Backdoor |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Export các hàm nghi ngờ độc hại tác động đến registry và gửi nhận dữ liệu đến host bobolili.dns-dns.com:8080 |

# Phân tích cơ bản

## Phân tích tĩnh cơ bản

### PE Header

*Target Machine*: x64

*Compilation Timestamp*: 27.0 KB

*Packer*: None

*PE Size*: 27.0 KB (27,648 bytes) - So sánh với filesize

*Các hàm import đặc trưng của mã độc*:

* 19 (send)
* 52 (gethostbyvalue)
* 16 (recv)
* 11 (inet\_addr)
* 18 (select)
* 13 (listen)
* 21 (setsockopt)
* 23 (socket)
* 115 (WSAStartup)
* 12 (inet\_ntoa)
* DuplicateTokenEx
* CreateProcessAsUserA
* RegDeleteValueA
* RegDeleteKeyA
* RegSetValueExA
* RtlLookupFunctionEntry
* CreateProcessA
* WriteFile
* FindFirstFileA
* TerminateProcess
* TerminateThread
* URLDownloadToFileA
* DeleteUrlCacheEntry

*Các hàm export nghi ngờ*:

* Install
* InstallService
* Remove
* RemoveService
* ServiceMain
* SetNew
* SetNewString

*Resource Language*: English

### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 8/71
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Undetected |
| Microsoft | Undetected |
| Symantec | Undetected |
| McAfee | Undetected |
| BitDefender | Undetected |

*Các kết quả tìm kiếm khác:*

* Dll thực hiện export các hàm nghi ngờ là thực hiện hành vi độc hại có tác động đến registry và gửi dữ liệu đến host *bobolili.dns-dns.com* port 8080 thông qua winsocket.
* Các hàm export của dll thực hiện nhận và trả về dữ liệu thông qua winsocket với từ host *bobolili.dns-dns.com:8080*

## Phân tích động cơ bản

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

Registry:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| RegCreateKeyExA | SOFTWARE\\Microsoft\\Internet Explorer\\ExplorerEditor\\ ServiceName | Tạo registry cho service |
| RegCreateKeyExA | SOFTWARE\\Microsoft\\Internet Explorer\\ExplorerEditor\\ ServiceDll | Tạo registry cho service |
| RegCreateKeyExA | SOFTWARE\\Microsoft\\Internet Explorer\\ExplorerEditor\\ ActiveString | Tạo registry cho service |
| RegCreateKeyExA | SOFTWARE\\Microsoft\\Internet Explorer\\ExplorerEditor\\ Password | Tạo registry cho service |
| RegQuerryValueA | SYSTEM\\CurrentControlSet\\Services\\ SENS\\ Parameters |  |
|  |  |  |

Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| TCPConnect | bobolili.dns-dns.com:8080 | Kết nối đến máy chủ dữ liệu. |

# 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>*

*<Vẽ hình minh họa >*

*<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>*

* Dll thực hiện export các hàm có hành vi bất thường
  + InstallService: thực hiện thêm các registry
    - SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\ServiceName
    - SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\ServiceDll
    - SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\ActiveString
    - SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\Password
  + RemoveService: thực hiện xóa registry
    - SOFTWARE\Microsoft\Internet Explorer\ServiceDll
    - SYSTEM\CurrentControlSet\Services\Parameters
  + ServiceMain:
    - Querry các giá trị registry:
      * SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\ServiceName: Sens
      * SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\ServiceDll: C:\\Winnt\\System32\\Sens.dll
      * SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\ActiveString: dargun
      * SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\Password: 158352692
    - Các giá trị được querry đúng thì thực hiện kết nối đến host: bobolili.dns-dns.com:8080 và nhận lệnh từ host này để gửi lại, các lệnh bao gồm:
      * Help: hiển thị danh sách và hướng dẫn các lệnh còn lại.
      * Exit: ngắt kết nối đến host.
      * Shell: lấy shell với quyền admin.
      * UserShell: lấy shell với quyền của user hiện tại.
      * Http://... + file: download file theo tham số.
  + SetNewString: thực hiện thêm các registry
    - SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\ActiveString
    - SOFTWARE\Microsoft\Internet Explorer\ExplorerEditor\Password

# Indicators of Compromise (IoC)

*<Danh sách các IoC của mã độc>*

Network IoC:

* bobolili.dns-dns.com:8080