Kết quả phân tích mã độc

## Thông tin mẫu

|  |  |
| --- | --- |
| *Filename* | Monitor-4.exe |
| *MD5* | c04fd8d9198095192e7d55345966da2e |
| *SHA-1* | 86ee262230cbf6f099b6086089da9eb9075b4521 |
| *SHA-256* | 0c98769e42b364711c478226ef199bfbba90db80175eb1b8cd565aa694c09852 |
| *File type* | PE32 |
| *File size* | 24.00 KB |

## Kết **luận chu**ng

|  |  |
| --- | --- |
| *Loại mã độc* | BOT |
| *Dòng mã độc* |  |
| *Đặc điểm chính* | Mã độc thực hiện kết nối với host [*http://www.malwareanalysisbook.com*](http://www.malwareanalysisbook.com) liên tục vô thời hạn sử dụng useragent Internet Explorer 8.0 (string: Internet Explorer 8.0) |

## **Phân tích cơ** bản

### Phân tích tĩnh cơ bản

#### PE Header

*Target Machine*: x86

*Compilation Timestamp*: 2011-10-01 02:49:12

*Packer*: None

*PE Size*: 24.00 KB (24,576 bytes)

*Các hàm import đặc trưng của mã độc*:

* StartServiceCtrlDispatcherA
* CreateMutex
* OpenMutex
* InternetOpenA
* InternetOpenUrlA
* CreateServiceA

*Resource Language*: English

#### Kết quả tìm kiếm online

*VirusTotal:*

* Tỉ lệ nhận diện: 38/68
* Dòng mã độc:

|  |  |
| --- | --- |
| Kaspersky | Undetected |
| Microsoft | VirTool:MSIL/CryptInject |
| Symantec | ML.Attribute.HighConfidence |
| McAfee | GenericRXJJ-TY!C04FD8D91980 |
| BitDefender | Clean |

*Các kết quả tìm kiếm khác:*

Bài lab 07 của practical malware analysis

### Phân tích động cơ bản

Process*:*

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| OpenMutexA | HGL345 | Kiểm tra nếu open thành công có nghĩa là máy tính đã bị lây nhiễm rồi, không cần chạy lại lây nhiễm nữa. |

Registry:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| RegSetValue | HKLM\System\CurrentControlSet\Services\Malservice | Tạo key autoruns |

Network:

|  |  |  |
| --- | --- | --- |
| **Hành vi** | **Path** | **Mô tả** |
| TCPConnect | [*http://www.malwareanalysisbook.com*](http://www.malwareanalysisbook.com) |  |