

stub.exe

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

MalFamily: Lokibot


MalScore: 100

| | |
|----------------------|--|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| File size: | 512.00 KB (524288 bytes) |
| Compile time: | 2018-07-02 05:48:41 |
| MD5: | 6c73fa61d98f5063f60cc712fc4ebe69 |
| SHA1: | ac850e54aa627a2ff41505994b7898dd10a25f1f |
| Import hash: | f34d5f2d4577ed6d9ceec516c1f5a744 |
| Submitted: | 2018-07-04 11:51:09 |

URL(s) file hosting

<http://meta-mim.in/stub.exe>

Antivirus Report

| Report date | Detection Ratio | Permalink |
|---------------------|-----------------|---|
| 2018-07-03 13:19:51 | 44/68 |  |

Import library

mscoree.dll

21

Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN LokiBot User-Agent (Charon/Inferno)



- signature: ET TROJAN LokiBot Checkin
- signature: ET TROJAN LokiBot Request for C2 Commands Detected M2
- signature: ET TROJAN LokiBot Request for C2 Commands Detected M1
- signature: ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1
- signature: ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2

Installs itself for autorun at Windows startup

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\filename.exe
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\filename.exe

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\E62877\73E4A9.exe
- file: C:\Users\Seven01\AppData\Roaming\E62877

Checks the system manufacturer, likely for anti-virtualization

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\filename.exe

Harvests credentials from local FTP client softwares

- file: C:\Users\Seven01\AppData\Roaming\FileZilla\sitemanager.xml
- file: C:\Users\Seven01\AppData\Roaming\FileZilla\recentservers.xml
- file: C:\Users\Seven01\AppData\Roaming\Far Manager\Profile\PluginsData\42E4AEB1-A230-44F4-B33C-F195BB654931.db
- file: C:\Program Files (x86)\FTPGetter\Profile\servers.xml
- file: C:\Users\Seven01\AppData\Roaming\FTPGetter\servers.xml
- file: C:\Users\Seven01\AppData\Roaming\Estsoft\ALFTP\ESTdb2.dat
- key: HKEY_CURRENT_USER\Software\Far\Plugins\FTP\Hosts
- key: HKEY_CURRENT_USER\Software\Far2\Plugins\FTP\Hosts
- key: HKEY_CURRENT_USER\Software\Ghisler\Total Commander
- key: HKEY_CURRENT_USER\Software\LinasFTP\Site Manager

Harvests information related to installed instant messenger clients

- file: C:\Users\Seven01\AppData\Roaming\purple\accounts.xml

Harvests information related to installed mail clients

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c0000000000046\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7d19c9e894f20d4780a31c9a9f17da11
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\00471e98b7a362469ed97e3915fd411
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\10b0e4d6eb1de34dabd532a0806a0fec\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\192e64c97bf3a54488a039619c763627\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\12b0e4d6eb1de34dabd532a0806a0fec\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\192e64c97bf3a54488a039619c763627\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\32a3dc9c400a4b448b60ab7fe553a392\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\32a3dc9c400a4b448b60ab7fe553a392\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\8503020000000000c0000000000046\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\43e0bb79f0f2d84db98ff4f730d23d24\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\7760e21103136b47946c9c80fa097f15\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\0a0d020000000000c0000000000046\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\6a50d9bd87f9a8478751861a1591a6c2\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\6a50d9bd87f9a8478751861a1591a6c2\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\192e64c97bf3a54488a039619c763627\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\10b0e4d6eb1de34dabd532a0806a0fec\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\0a0d020000000000c0000000000046\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\7d19c9e894f20d4780a31c9a9f17da11\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\7760e21103136b47946c9c80fa097f15\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\43e0bb79f0f2d84db98ff4f730d23d24\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\00471e98b7a362469ed97e3915fd4111\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook
- key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook

Collects information to fingerprint the system

Attempts to repeatedly call a single API many times in order to delay analysis time

- Spam: services.exe (484) called API GetSystemTimeAsFileTime 2593867 times

Queries information on disks, possibly for anti-virtualization

Executed a process and injected code into it, probably while unpacking

- Injection: stub.exe(2548) -> RegAsm.exe(2792)

Creates RWX memory

A process attempted to delay the analysis task.

- Process: build.exe tried to sleep 720 seconds, actually delayed analysis time by 0 seconds
- Process: sppsvc.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds
- Process: Host.exe tried to sleep 1050 seconds, actually delayed analysis time by 0 seconds

Reads data out of its own binary image

- self_read: process: Host.exe, pid: 3040, offset: 0x00000000, length: 0x00020000

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Roaming\Install\Host.exe
- binary: C:\Users\Seven01\AppData\Local\Temp\Host.exe

HTTP traffic contains suspicious features which may be indicative of malware related traffic

- post_no_referer: HTTP traffic contains a POST request with no referer header
- http_version_old: HTTP traffic uses version 1.0
- suspicious_request: http://valdepian.com/proba/valdepian/Panel/five/fre.php

Performs some HTTP requests

- url: http://valdepian.com/proba/valdepian/Panel/five/fre.php

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.71, characteristics:
IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size:
0x00023000, virtual_size: 0x00022220

Attempts to connect to a dead IP:Port (1 unique times)

- IP: 192.168.56.1:1199

At least one process apparently crashed during execution

2

HTTP Request(s) detected

<http://valdepian.com/proba/valdepian/Panel/five/fre.php>



| |
|----------------------------|
| Hostname: valdepian.com |
| IP Address: 178.218.172.18 |
| Port: 80 |
| Count: 2 |

| |
|---|
| http://valdepian.com/proba/valdepian/Panel/five/fre.php |
| Hostname: valdepian.com |
| IP Address: 178.218.172.18 |
| Port: 80 |
| Count: 12 |