

log.exe

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

**MalFamily: Lokibot**


**MalScore: 100**

<b>File type:</b>	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
<b>File size:</b>	272.00 KB (278528 bytes)
<b>Compile time:</b>	2018-04-27 00:36:39
<b>MD5:</b>	7689084a60f4481351bbbe4ef36b08a1
<b>SHA1:</b>	e65f3af07cceac08fe5f9124e51c19f8984c94c8
<b>Import hash:</b>	f34d5f2d4577ed6d9ceec516c1f5a744
<b>Submitted:</b>	2018-05-07 02:18:02

### URL(s) file hosting

<http://dhm-mhn.com/floyd/log.exe>

### Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-06 20:54:00	39/66	

### Import library

mscoree.dll

**16**

## 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

Collects information to fingerprint the system

Attempts to modify or disable Security Center warnings

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\8503020000000000c00000000000046\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\00471e98b7a362469ed97e3915fd4111
- 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\86ed2903a4a11cfb57e524153480001\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\818ecc2f310b344f807e8af5dc013189\Email
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\192e64c97bf3a54488a039619c763627
- 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
- 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
- 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
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189
- 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\8503020000000000c00000000000046
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\43e0bb79f0f2d84db98ff4f730d23d24
- 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  
- 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\0a0d020000000000c00000000000046\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb00aa002fc45a  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\6a50d9bd87f9a8478751861a1591a6c2  
- 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  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\0a0d020000000000c00000000000046  
- 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  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\86ed2903a4a11cfb57e524153480001  
- 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\13dbb0c8aa05101a9bb00aa002fc45a\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

Harvests information related to installed instant messenger clients

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

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

Creates a hidden or system file

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

- file: C:\Users\Seven01\AppData\Roaming\E62877

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

- Spam: services.exe (488) called API GetSystemTimeAsFileTime 4019420 times

Queries information on disks, possibly for anti-virtualization

Deletes its original binary from disk

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

- Injection: log.exe(2356) -> log.exe(2628)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.77, characteristics:  
IMAGE\_SCN\_CNT\_CODE|IMAGE\_SCN\_MEM\_EXECUTE|IMAGE\_SCN\_MEM\_READ, raw\_size:  
0x0002b600, virtual\_size: 0x0002b424

Performs some HTTP requests

- url: http://vopspyder.website/log/five/fre.php

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://vopspyder.website/log/five/fre.php

A process attempted to delay the analysis task.

- Process: log.exe tried to sleep 840 seconds, actually delayed analysis time by 0 seconds  
- Process: svchost.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds  
- Process: sppsvc.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

## 2 HTTP Request(s) detected

<http://vopspyder.website/log/five/fre.php>

Hostname: vopspyder.website

IP Address: 185.6.242.251

Port: 80

Count: 2

<http://vopspyder.website/log/five/fre.php>

Hostname: vopspyder.website

IP Address: 185.6.242.251

Port: 80

Count: 15