r8OSpd.jpg

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:	684.00 KB (700416 bytes)
Compile time:	2018-07-04 23:22:40
MD5:	8dac3bd23e46d8a73acc093e17678e2d
SHA1:	98bf4f02dca876e11d0d1a6abef6c4faa82319a2
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-07-08 17:42:02

URL(s) file hosting

https://a.coka.la/r8OSpd.jpg

Antivirus Report

Report date	Detection Ratio	Permalink
2018-07-06 09:55:43	43/68	

Import library

mscoree.dll

25 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\NzoHrh.url
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\NwctLW.url
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\NzoHrh.url
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\NwctLW.url

Creates a hidden or system file

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

Retrieves Windows ProductID, probably to fingerprint the sandbox

Checks the CPU name from registry, possibly for anti-virtualization

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\r8OSpd.jpg

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\8503020000000000c000000000000046\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\f86ed2903a4a11cfb57e524153480001\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\8503020000000000c000000000000046
- 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\0a0d020000000000c000000000000046\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a
- 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\0a0d020000000000c000000000000046
- 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\f86ed2903a4a11cfb57e524153480001
- 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

Anomalous binary characteristics

- anomaly: Actual checksum does not match that reported in PE header

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

- Spam: services.exe (484) called API GetSystemTimeAsFileTime 2127913 times

A process attempted to delay the analysis task by a long amount of time.

- Process: WmiPrvSE.exe tried to sleep 421 seconds, actually delayed analysis time by 0 seconds
- Process: RegAsm.exe tried to sleep 3347 seconds, actually delayed analysis time by 0 seconds
- Process: sppsvc.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds
- Process: vbc.exe tried to sleep 720 seconds, actually delayed analysis time by 0 seconds

Queries information on disks, possibly for anti-virtualization

Sniffs keystrokes

- SetWindowsHookExA: Process: RegAsm.exe(2168)

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

- Injection: r8OSpd.jpg(2376) -> vbc.exe(2136)

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Roaming\r8OSpd.jpg:Zone.Identifier

Creates RWX memory

At least one IP Address, Domain, or File Name was found in a crypto call

- ioc: 1.911642F
- ioc: 43220.17F
- ioc: 3.192541E-09
- ioc: -0.002891566
- ioc: -2.859661E-29
- ioc: -3.868554E-13
- ioc: -2.330965E-35
- ioc: -9.578219E-05
- ioc: -28.88809
- ioc: 9.68435E
- ioc: 1.0.0.0
- ioc: pplication.app
- ioc: asm.v2
- ioc: -7.838439E-29
- ioc: 5.21489E
- ioc: 4.226392E-08
- ioc: 5.468407E
- ioc: 3214.484F

- ioc: 1.037437E-15
- ioc: 1.251374E-38
- ioc: 4.10815E-17
- ioc: -3.603012E
- ioc: -1.585127E

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Roaming\BqCLgNwDkNQH.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://replaxed.ru/amb-1/fred.php

Performs some HTTP requests

- url: http://replaxed.ru/amb-1/fred.php

The binary likely contains encrypted or compressed data.

- section: name: .rsrc, entropy: 7.98, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ, raw_size: 0x00092000, virtual_size: 0x00091fb8

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

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

- IP: 192.168.56.1:333

2 HTTP Request(s) detected

http://replaxed.ru/amb-1/fred.php
Hostname: replaxed.ru
IP Address: 159.148.186.6
Port: 80
Count: 2

http://replaxed.ru/amb-1/fred.php
Hostname: replaxed.ru
IP Address: 159.148.186.6
Port: 80
Count: 12