ers.exe

Is DLL | Packer | Anti Debug | Anti VM | Signed | XOR

MalFamily: Xtremerat **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	1035.05 KB (1059888 bytes)
Compile time:	2018-06-26 16:23:21
MD5:	753b6e87f955dad98e36ce9a4dd3b6c7
SHA1:	ab1f773580464001ecc35fc02e28ab88e4d0f286
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-06-28 01:57:09

URL(s) file hosting

http://earthart.org/dev/ers.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-06-27 01:40:21	35/67	

Import library

mscoree.dll

23 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

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

- Spam: services.exe (484) called API GetSystemTimeAsFileTime 2659550 times

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\HKCU
- data: C:\Windows\InstallDir\Server.exe
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\HKLM
- data: C:\Windows\InstallDir\Server.exe
- key: HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{76253HHC-XA2V-2RX2-2O03-OUBJOR754AC4}
- data: unknown
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{76253HHC-XA2V-2RX2-2O03-OUBJOR754AC4}\StubPath
- data: C:\Windows\InstallDir\Server.exe restart

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\73qhmD3.cfg
- file: C:\Windows\InstallDir\Server.exe
- file: C:\Windows\InstallDir\
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\73qhmD3.dat
- file: C:\Users\Seven01\AppData\Roaming\E62877\73E4A9.exe
- file: C:\Users\Seven01\AppData\Roaming\E62877

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

Attempts to modify or disable Security Center warnings

Creates known XtremeRAT mutexes

Collects information to fingerprint the system

Queries information on disks, possibly for anti-virtualization

Sniffs keystrokes

- SetWindowsHookExW: Process: iexplore.exe(2932)

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

- Injection: ers.exe(2380) -> svhost.exe(2544)

Creates RWX memory

Possible date expiration check, exits too soon after checking local time

- process: server.exe, PID 2668

A process attempted to delay the analysis task.

- Process: 932build.exe tried to sleep 720 seconds, actually delayed analysis time by 0 seconds
- Process: svchost.exe tried to sleep 390 seconds, actually delayed analysis time by 0 seconds
- Process: sppsvc.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds

Reads data out of its own binary image

- self_read: process: ers.exe, pid: 2380, offset: 0x00000000, length: 0x00001000
- self_read: process: ers.exe, pid: 2380, offset: 0x00000080, length: 0x00000200

A process created a hidden window

- Process: server.exe -> C:\Users\Seven01\AppData\Local\Temp\297bin.exe
- Process: server.exe -> C:\Users\Seven01\AppData\Local\Temp\932build.exe

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Local\Temp\server.exe
- binary: C:\Users\Seven01\AppData\Local\Temp\svhost.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
- get_no_useragent: HTTP traffic contains a GET request with no user-agent header
- http_version_old: HTTP traffic uses version 1.0
- suspicious_request: http://aljesvin.com/app/Panel/five/fre.php

- suspicious_request: http://www.novaflashlight.com/h26/?4h=4vOPgv645ZjHKn5P6RaWoLmSB3CSxZeK1ix4fVLvQz24C28RHBvs+oSInXxh09Pxzcpw8gtk&wR=LJEpcJ_
- suspicious_request: http://www.xn--9t4bn3g84h.xn--mk1bu44c/h26/?4h=nN3yX7XqtabRP1oF6E4cRKIb3V+3dRO1pqhUfFJbqVw12KrOETe9UrErEU6bYsYtm+7BiQ/l&wR=LJEpcJ_
- suspicious_request: http://www.xn--9t4bn3g84h.xn--mk1bu44c/h26/
- suspicious_request: http://www.dstecco.com/h26/?4h=upB2b9aIcxU+d+QKRoFcgFCTQq8jGfTUTyPsJ5wkGAoIWg2SbMXBKvBumnCoOQbPk5X7UgVu&wR=LJEpcJ_
- suspicious_request: http://www.dstecco.com/h26/
- suspicious_request: http://www.criosaunas.com/h26/?4h=N/iXq/7ru3bhLUDPqHWoWW4x6s0AdqrAqPmX0Haz/TJzSlsjbSbD8z8YPlf8sQVbNdtnEGdX&wR=LJEpcJ_
- suspicious_request: http://www.criosaunas.com/h26/

Performs some HTTP requests

- url: http://aljesvin.com/app/Panel/five/fre.php
- url: http://www.novaflashlight.com/h26/?4h=4vOPgv645ZjHKn5P6RaWoLmSB3CSxZeK1ix4fVLvQz24C28RHBvs+oSInXxh09Pxzcpw8gtk&wR=LJEpcJ_
- url: http://www.xn--9t4bn3g84h.xn--mk1bu44c/h26/?4h=nN3yX7XqtabRP1oF6E4cRKIb3V+3dRO1pqhUfFJbqVw12KrOETe9UrErEU6bYsYtm+7BiQ/l&wR=LJEpcJ_
- url: http://www.xn--9t4bn3g84h.xn--mk1bu44c/h26/
- url: http://www.dstecco.com/h26/?4h=upB2b9aIcxU+d+QKRoFcgFCTQq8jGfTUTyPsJ5wkGAoIWg2SbMXBKvBumnCoOQbPk5X7UgVu&wR=LJEpcJ_
- url: http://www.dstecco.com/h26/
- url: http://www.criosaunas.com/h26/?4h=N/iXq/7ru3bhLUDPqHWoWW4x6s0AdqrAqPmX0Haz/TJzSlsjbSbD8z8YPlf8sQVbNdtnEGdX&wR=LJEpcJ_
- url: http://www.criosaunas.com/h26/

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.86, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00101000, virtual_size: 0x00100ec4

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

- IP: 192.168.56.1:7728

12 HTTP Request(s) detected

http://aljesvin.com/app/Panel/five/fre.php
Hostname: aljesvin.com
IP Address: 103.14.121.81
Port: 80
Count: 2

http://aljesvin.com/app/Panel/five/fre.php
Hostname: aljesvin.com
IP Address: 103.14.121.81

Port: 80
Count: 13

http://www.novaflashlight.com/h26/?4h=4vOPgv645ZjHKn5P6RaWoLmSB3CSxZeK1ix4fVLvQz24C28RHBvs+oSInXxh09Pxzcpw8gtk&wR=LJEpcJ_
Hostname: www.novaflashlight.com
IP Address: 52.5.142.190
Port: 80
Count: 1

http://www.xn--9t4bn3g84h.xn--mk1bu44c/h26/?4h=nN3yX7XqtabRP1oF6E4cRKIb3V+3dRO1pqhUfFJbqVw12KrOETe9UrErEU6bYsYtm+7BiQ/l&wR=LJEpcJ_
Hostname: www.xn--9t4bn3g84h.xn--mk1bu44c
IP Address:
Port: 80
Count: 1

http://www.xn--9t4bn3g84h.xn--mk1bu44c/h26/
Hostname: www.xn--9t4bn3g84h.xn--mk1bu44c
IP Address:
Port: 80
Count: 1

http://www.xn--9t4bn3g84h.xn--mk1bu44c/h26/
Hostname: www.xn--9t4bn3g84h.xn--mk1bu44c
IP Address:
Port: 80
Count: 1

http://www.dstecco.com/h26/?4h=upB2b9aIcxU+d+QKRoFcgFCTQq8jGfTUTyPsJ5wkGAoIWg2SbMXBKvBumnCoOQbPk5X7UgVu&wR=LJEpcJ_
Hostname: www.dstecco.com
IP Address:
Port: 80
Count: 1

http://www.dstecco.com/h26/

Hostname: www.dstecco.com
IP Address:
Port: 80
Count: 1

http://www.dstecco.com/h26/
Hostname: www.dstecco.com
IP Address:
Port: 80
Count: 1

http://www.criosaunas.com/h26/?4h=N/iXq/7ru3bhLUDPqHWoWW4x6s0AdqrAqPmX0Haz/TJzSlsjbSbD8z8YPlf8sQVbNdtnEGdX&wR=LJEpcJ_
Hostname: www.criosaunas.com
IP Address: 184.168.221.96
Port: 80
Count: 1

http://www.criosaunas.com/h26/
Hostname: www.criosaunas.com
IP Address: 184.168.221.96
Port: 80
Count: 1

http://www.criosaunas.com/h26/
Hostname: www.criosaunas.com
IP Address: 184.168.221.96
Port: 80
Count: 1