wire.exe

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

MalFamily: Agenttesla **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	216.00 KB (221184 bytes)
Compile time:	2017-09-04 12:20:50
MD5:	30a76f7935aa35cb2a5e6b1bd4d6aa49
SHA1:	8f0b90f0b390e14c59b30a058ad0ab3f183c2cde
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-09-05 20:15:03

URL(s) file hosting

http://www.chrisan.com.br/plugins/js/wire.exe

http://191.96.249.212/post.php

Antivirus Report

Report date	Detection Ratio	Permalink
2017-09-05 17:02:52	32/64	

Import library

mscoree.dll

18 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN AgentTesla PWS HTTP CnC Checkin
- signature: Traffico Anomalo ? Start Traffico)

Collects information to fingerprint the system

Harvests information related to installed mail clients

- file: C:\Users\Seven01\AppData\Roaming\Thunderbird\profiles.ini
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password
- 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
- 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\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password
- 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\9375CFF0413111d3B88A00104B2A6676\00000003\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password
- 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\9375CFF0413111d3B88A00104B2A6676\00000003
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676

- key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676

Harvests information related to installed instant messenger clients

- file: C:\Users\Seven01\AppData\Roaming\.purple\accounts.xml
- key: HKEY_CURRENT_USER\Software\Paltalk

Harvests credentials from local FTP client softwares

- file: C:\Users\Seven01\AppData\Roaming\FileZilla\recentservers.xml
- file: C:\Users\Seven01\AppData\Roaming\SmartFTP\Client 2.0\Favorites\Quick Connect\
- file: C:\Users\Seven01\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini
- key: HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Local\Temp\Products\WinDecode.exe

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

Retrieves Windows ProductID, probably to fingerprint the sandbox

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Local\Temp\Products\WinDecode.exe
- file: C:\Users\Seven01\AppData\Roaming\ScreenShot

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Tregain
- data: C:\Users\Seven01\AppData\Local\Temp\Products\WinDecode.exe

Deletes its original binary from disk

Sniffs keystrokes

- SetWindowsHookExW: Process: wire.exe(2252)

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

- Injection: wire.exe(2092) -> wire.exe(2252)

Looks up the external IP address

- domain: checkip.dyndns.org

Performs some HTTP requests

- url: http://checkip.dyndns.org/
- url: http://191.96.249.212/post.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
- get_no_useragent: HTTP traffic contains a GET request with no user-agent header
- ip_hostname: HTTP connection was made to an IP address rather than domain name
- suspicious_request: http://checkip.dyndns.org/
- suspicious_request: http://191.96.249.212/post.php

A process attempted to delay the analysis task.

- Process: wire.exe tried to sleep 1675 seconds, actually delayed analysis time by 0 seconds
- Process: WmiPrvSE.exe tried to sleep 301 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

9 HTTP Request(s) detected

http://checkip.dyndns.org/
Hostname: checkip.dyndns.org
IP Address: 91.198.22.70
Port: 80
Count: 1

http://191.96.249.212/post.php
Hostname: 191.96.249.212
IP Address:
Port: 80
Count: 1

http://191.96.249.212/post.php
Hostname: 191.96.249.212
IP Address:
Port: 80
Count: 30

http://191.96.249.212/post.php
Hostname: 191.96.249.212
IP Address:
Port: 80
Count: 1

http://191.96.249.212/post.php
Hostname: 191.96.249.212
IP Address:
Port: 80
Count: 1

http://191.96.249.212/post.php
Hostname: 191.96.249.212
IP Address:
Port: 80
Count: 114

http://191.96.249.212/post.php
Hostname: 191.96.249.212
IP Address:
Port: 80
Count: 1

http://191.96.249.212/post.php
Hostname: 191.96.249.212
IP Address:
Port: 80
Count: 2

http://191.96.249.212/post.php
Hostname: 191.96.249.212
IP Address:
Port: 80
Count: 3

1 Host(s) detected

IP Address	Hostname	Reverse DNS
191.96.249.212 		

1 Countr(y|ies) detected

Hosts	Country
1	Russian Federation