figx.exe

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

MalFamily: Ispy **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	240.00 KB (245760 bytes)
Compile time:	2018-04-13 00:20:47
MD5:	1dd59b46c55d33af810deb7379d8a75f
SHA1:	fc5fa83211e5ab3f899928b71081e0ce4ce3fada
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-04-16 19:51:03

URL(s) file hosting

http://lalecitinadesoja.com/imagenesdeunasdisenos.com/files/figx.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-04-16 09:59:56	41/66	

Import library

mscoree.dll

22 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: Traffico Anomalo ? Start Traffico)

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Paychex Inc
- data: C:\Users\Seven01\AppData\Roaming\Paychex Inc\Paychex Inc.exe

Creates a hidden or system file

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

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\Paychex Inc\Paychex Inc.exe

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

Harvests information related to installed instant messenger clients

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

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

Collects information to fingerprint the system

Exhibits behavior characteristic of iSpy Keylogger

- C2: 192.168.56.1
- C2: figure.agrillcs.com/api.php
- C2: figure.agrillcs.com/api.php/api.php
- C2: figure.agrillcs.com/api.php/api.php/api.php
- C2: figure.agrillcs.com/api.php/api.php/api.php/api.php

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

- Process: figx.exe tried to sleep 2654 seconds, actually delayed analysis time by 0 seconds
- Process: WmiPrvSE.exe tried to sleep 421 seconds, actually delayed analysis time by 0 seconds

Sniffs keystrokes

- SetWindowsHookExW: Process: figx.exe(2652)

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Roaming\Paychex Inc\Paychex Inc.exe:Zone.Identifier

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

- Injection: figx.exe(2480) -> figx.exe(2652)

Creates RWX memory

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
- suspicious_request: http://checkip.dyndns.org/
- suspicious_request: http://figure.agrillcs.com/api.php

Performs some HTTP requests

- url: http://checkip.dyndns.org/
- url: http://figure.agrillcs.com/api.php

Unconventionial language used in binary resources: Kashmiri

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.25, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00036000, virtual_size: 0x00035204

Looks up the external IP address

- domain: checkip.dyndns.org

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

- IP: 192.168.56.1:80

16 HTTP Request(s) detected

http://checkip.dyndns.org/
Hostname: checkip.dyndns.org
IP Address: 216.146.43.70
Port: 80
Count: 1

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 10

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 26

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 1

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58

Port: 80
Count: 1

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 1

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 94

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 5

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 1

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 1

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80

Count: 1

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 2

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 2

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 2

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 1

http://figure.agrillcs.com/api.php
Hostname: figure.agrillcs.com
IP Address: 108.170.51.58
Port: 80
Count: 1