decx.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:	236.00 KB (241664 bytes)
Compile time:	2018-03-21 22:49:47
MD5:	89c04063f2fbb061d30cd978e7a9d46f
SHA1:	ae54ac003d5b081096c7c187e78ef434aa7b660e
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-03-23 17:30:03

URL(s) file hosting

http://lashawnbarber.com/images/files/decx.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-03-23 12:52:13	18/67	

Import library

mscoree.dll

20 Behaviors detected by system signatures

Collects information to fingerprint the system

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Gentek Inc
- data: C:\Users\Seven01\AppData\Local\Temp\Gentek Inc\Gentek 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\Local\Temp\Gentek Inc\Gentek 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

Exhibits behavior characteristic of iSpy Keylogger

- C2: 192.168.56.1
- C2: declan.ziraat-helpdesk.com/api.php
- C2: declan.ziraat-helpdesk.com/api.php/api.php
- C2: declan.ziraat-helpdesk.com/api.php/api.php/api.php
- C2: declan.ziraat-helpdesk.com/api.php/api.php/api.php/api.php

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

- Process: decx.exe tried to sleep 2427 seconds, actually delayed analysis time by 0 seconds

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Local\Temp\Gentek Inc\Gentek Inc.exe:Zone.Identifier

Sniffs keystrokes

- SetWindowsHookExW: Process: decx.exe(2380)

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

- Injection: decx.exe(2260) -> decx.exe(2380)

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://declan.ziraat-helpdesk.com/api.php

Performs some HTTP requests

- url: http://checkip.dyndns.org/
- url: http://declan.ziraat-helpdesk.com/api.php

Unconventionial language used in binary resources: Divehi

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.06, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00035000, virtual_size: 0x00034dd4

Looks up the external IP address

- domain: checkip.dyndns.org

Creates RWX memory

9 HTTP Request(s) detected

http://checkip.dyndns.org/
Hostname: checkip.dyndns.org
IP Address: 216.146.38.70
Port: 80
Count: 1

http://declan.ziraat-helpdesk.com/api.php
Hostname: declan.ziraat-helpdesk.com
IP Address:
Port: 80
Count: 1

http://declan.ziraat-helpdesk.com/api.php
Hostname: declan.ziraat-helpdesk.com
IP Address:
Port: 80
Count: 22

http://declan.ziraat-helpdesk.com/api.php
Hostname: declan.ziraat-helpdesk.com
IP Address:
Port: 80
Count: 1

http://declan.ziraat-helpdesk.com/api.php
Hostname: declan.ziraat-helpdesk.com
IP Address:
Port: 80
Count: 1

http://declan.ziraat-helpdesk.com/api.php
Hostname: declan.ziraat-helpdesk.com

IP Address:
Port: 80
Count: 92

http://declan.ziraat-helpdesk.com/api.php
Hostname: declan.ziraat-helpdesk.com
IP Address:
Port: 80
Count: 1

http://declan.ziraat-helpdesk.com/api.php
Hostname: declan.ziraat-helpdesk.com
IP Address:
Port: 80
Count: 2

http://declan.ziraat-helpdesk.com/api.php
Hostname: declan.ziraat-helpdesk.com
IP Address:
Port: 80
Count: 3