newlog.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:	280.00 KB (286720 bytes)
Compile time:	2018-02-03 21:29:22
MD5:	f6c3700fecafc9a337a2d3610ca472c5
SHA1:	8fa1a70d9df6adf75f43565e90119808e241cd93
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-02-07 01:33:03

URL(s) file hosting

http://gg.usdipc.com/newlog.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-02-06 21:02:04	24/68	

Import library

mscoree.dll

20 Behaviors detected by system signatures

Collects information to fingerprint the system

Exhibits behavior characteristic of iSpy Keylogger

- C2: 192.168.56.1
- C2: poster.adexcel.co/WebPanel/api.php
- C2: poster.adexcel.co/WebPanel/api.php/WebPanel/api.php
- C2: poster.adexcel.co/WebPanel/api.php/WebPanel/api.php/WebPanel/api.php
- C2: poster.adexcel.co/WebPanel/api.php/WebPanel/api.php/WebPanel/api.php/WebPanel/api.php
- C2: poster.adexcel.co/WebPanel/api.php/WebPanel/api.php/WebPanel/api.php/WebPanel/api.php/WebPanel/api.php
- C2: poster.adexcel.co/WebPanel/api.php/WebPanel/api.php/WebPanel/api.php/WebPanel/api.php/WebPanel/api.php/WebPanel/api.php

Installs itself for autorun at Windows startup

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

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

Deletes its original binary from disk

Attempts to remove evidence of file being downloaded from the Internet

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

Sniffs keystrokes

- SetWindowsHookExW: Process: newlog.exe(2376)

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

- Injection: newlog.exe(2192) -> newlog.exe(2376)

Creates RWX memory

A process attempted to delay the analysis task.

- Process: newlog.exe tried to sleep 548 seconds, actually delayed analysis time by 0 seconds
- Process: WmiPrvSE.exe tried to sleep 361 seconds, actually delayed analysis time by 0 seconds

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://poster.adexcel.co/WebPanel/api.php

Performs some HTTP requests

- url: http://checkip.dyndns.org/
- url: http://poster.adexcel.co/WebPanel/api.php

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: 0x00040000, virtual_size: 0x0003fd94

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

30 HTTP Request(s) detected

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

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 25

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 11

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 1

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145

Port: 80
Count: 1

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 1

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 3

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 91

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 15

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 19

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80

Count: 2

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 10

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 3

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 8

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 9

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 2

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 1

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 1

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 1

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 1

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 15

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 28

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 5

http://poster.adexcel.co/WebPanel/api.php

Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 2

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 4

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 1

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 1

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 1

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co
IP Address: 198.54.114.145
Port: 80
Count: 1

http://poster.adexcel.co/WebPanel/api.php
Hostname: poster.adexcel.co

IP Address: 198.54.114.145
Port: 80
Count: 1