p?id=e0c199b36b383f2b59adb0823f6e2135a668762a1250e0b4a63f68b3e

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

MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	260.00 KB (266240 bytes)
Compile time:	2018-04-10 17:30:12
MD5:	ddb2fe695edb5ded29389ad905cbe749
SHA1:	0a52fa3ceecd90d2b224a76827acfc3c5cdab19a
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-04-13 09:15:04

URL(s) file hosting

http://37.59.117.243/index.php?id=e0c199b36b383f2b59adb0823f6e2135a668762a1250e0b4a63f68b3ec3f37b4

Antivirus Report

Report date	Detection Ratio	Permalink
2018-04-12 23:44:32	46/68	

Import library

mscoree.dll

17 Behaviors detected by system signatures

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\Roaming\ONEOK Inc\ONEOK Inc.exe

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

Retrieves Windows ProductID, probably to fingerprint the sandbox

Installs itself for autorun at Windows startup

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

Sniffs keystrokes

- SetWindowsHookExW: Process: index.phpide0c199b36b383f2b59adb0823f6e2135a668762a1250e0b4a63f68b3ec3f37b4(2544)

Attempts to remove evidence of file being downloaded from the Internet

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

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

- Injection: index.phpide0c199b36b383f2b59adb0823f6e2135a668762a1250e0b4a63f68b3ec3f37b4(2312) -> index.phpide0c199b36b383f2b59adb0823f6e2135a668762a1250e0b4a63f68b3ec3f37b4(2544)

Looks up the external IP address

- domain: checkip.dyndns.org

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 6.99, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00036000, virtual_size: 0x00035774

Performs some HTTP requests

- url: http://checkip.dyndns.org/

HTTP traffic contains suspicious features which may be indicative of malware related traffic

- get_no_useragent: HTTP traffic contains a GET request with no user-agent header
- suspicious_request: http://checkip.dyndns.org/

A process attempted to delay the analysis task.

- Process: index.phpide0c199b36b383f2b59adb0823f6e2135a668762a1250e0b4a63f68b3ec3f37b4 tried to sleep 1798 seconds, actually delayed analysis time by 0 seconds
- Process: WmiPrvSE.exe tried to sleep 361 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

1 HTTP Request(s) detected

http://checkip.dyndns.org/

Hostname: checkip.dyndns.org
IP Address: 216.146.43.71
Port: 80
Count: 1