PGDOUOUT.exe

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:	539.28 KB (552224 bytes)
Compile time:	2018-05-30 12:28:07
MD5:	00bce26e2a1013c5acf40519f3fa9db4
SHA1:	948f9987ebb057c9f6a942324f34be29437eb838
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-06-01 23:24:08

URL(s) file hosting

http://www.paulocamarao.com/server-log/PGDOUOUT.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-06-01 04:42:36	21/66	

Import library

mscoree.dll

22 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 NT\CurrentVersion\Windows\Load
- data: C:\Users\Seven01\AppData\Roaming\FolderN\name.exe.lnk

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\FolderN
- 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\FolderN\name.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

The sample wrote data to the system hosts file.

 - added: 127.0.0.1

Sniffs keystrokes

 - SetWindowsHookExW: Process: svhost.exe(2904)

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

 - Injection: PGDOUOUT.exe(2576) -> svhost.exe(2904)

Creates RWX memory

A process attempted to delay the analysis task.

 - Process: svhost.exe tried to sleep 599 seconds, actually delayed analysis time by 0 seconds

Reads data out of its own binary image

 - self_read: process: PGDOUOUT.exe, pid: 2576, offset: 0x00000000, length: 0x00001000
 - self_read: process: PGDOUOUT.exe, pid: 2576, offset: 0x00000080, length: 0x00000200

A process created a hidden window

 - Process: PGDOUOUT.exe -> "cmd.exe"

Drops a binary and executes it

 - binary: C:\Users\Seven01\AppData\Local\Temp\svhost.exe
 - binary: C:\Users\Seven01\AppData\Local\Temp\PGNANOOUT.exe

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/
 - suspicious_request: http://www.paulocamarao.com/server-log/PGNANOOUT.exe

Performs some HTTP requests

 - url: http://checkip.dyndns.org/
 - url: http://www.paulocamarao.com/server-log/PGNANOOUT.exe

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: 0x00048600, virtual_size: 0x00048410

Looks up the external IP address

- domain: checkip.dyndns.org

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

- IP: 192.168.56.1:587

2 HTTP Request(s) detected

http://checkip.dyndns.org/
Hostname: checkip.dyndns.org
IP Address: 131.186.113.135
Port: 80
Count: 1

http://www.paulocamarao.com/server-log/PGNANOOUT.exe
Hostname: www.paulocamarao.com
IP Address: 64.90.50.213
Port: 80
Count: 1