polists.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:	1164.39 KB (1192340 bytes)
Compile time:	2018-02-07 22:51:36
MD5:	d6fb42edf3ecc65aec2431afe6cf2701
SHA1:	5d874d6b74eae8563292bcb9a23b7ca1b3637c53
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-02-14 14:51:10

URL(s) file hosting

http://whitedowell.com/polists.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-02-09 19:34:25	35/65	

Import library

mscoree.dll

18 Behaviors detected by system signatures

Anomalous binary characteristics

- anomaly: Unprintable characters found in section name

Checks the system manufacturer, likely for anti-virtualization

Likely virus infection of existing system binary

- file: c:\gmkhdqasmt\bin\loader.exe
- file: c:\gmkhdqasmt\bin\bqeaxyc.exe

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\prvjelbe.exe

Installs itself for autorun at Windows startup

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\prvjelbe.exe
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\prvjelbe.exe

Attempts to repeatedly call a single API many times in order to delay analysis time

- Spam: services.exe (488) called API GetSystemTimeAsFileTime 3859699 times
- Spam: lsass.exe (496) called API NtClose 487648 times

Tries to unhook or modify Windows functions monitored by Cuckoo

- unhook: function_name: WSASend, type: modification
- unhook: function_name: LdrLoadDll, type: modification
- unhook: function_name: WSASendTo, type: modification
- unhook: function_name: WSARecvFrom, type: modification
- unhook: function_name: NtQueryDirectoryFile, type: modification
- unhook: function_name: send, type: modification
- unhook: function_name: recv, type: modification
- unhook: function_name: recvfrom, type: modification
- unhook: function_name: closesocket, type: modification
- unhook: function_name: sendto, type: modification
- unhook: function_name: WSARecv, type: modification
- unhook: function_name: NtResumeThread, type: modification

Code injection with CreateRemoteThread in a remote process

- Injection: iexplore.exe(3044) -> None(264)

Tries to suspend Cuckoo threads to prevent logging of malicious activity

- Process: polistsmgr.exe (2816)

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

- Injection: polists.exe(2472) -> polists.exe(2672)

The binary likely contains encrypted or compressed data.

- section: name: \x1da0\x7fA\x0fdF, entropy: 8.00, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ|IMAGE_SCN_MEM_WRITE, raw_size: 0x00100a00, virtual_size: 0x00100834

Drops a binary and executes it

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

Expresses interest in specific running processes

- process: smss.exe

Starts servers listening on 0.0.0.0:21

A process attempted to delay the analysis task.

- Process: polists.exe tried to sleep 851 seconds, actually delayed analysis time by 0 seconds
- Process: svchost.exe tried to sleep 1629 seconds, actually delayed analysis time by 0 seconds
- Process: SearchFilterHost.exe tried to sleep 780 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

Attempts to connect to a dead IP:Port (2 unique times)

- IP: 192.168.56.1:80
- IP: 192.168.56.1:447

At least one process apparently crashed during execution