nd.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:	1133.00 KB (1160192 bytes)
Compile time:	2018-06-02 10:28:07
MD5:	91efed7bb6493d373d8fda375bc8338c
SHA1:	acd933c41dbc01698f5fe1d200f494887a4318c4
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-06-03 10:00:02

URL(s) file hosting

http://srathardforlife.com/wp-admin/us/nd.exe

Antivirus Report

Report date	Detection Ratio	Permalink
No report available		

Import library

mscoree.dll

16 Behaviors detected by system signatures

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\Googledocs.exe

- copy: C:\Users\Seven01\AppData\Roaming\cvdd.exe
- copy: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\954d1751ffef0cb2d74e585c2d0733cb.exe

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\Googledocs.exe
- file: C:\Users\Seven01\AppData\Roaming\cvdd.exe

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\954d1751ffef0cb2d74e585c2d0733cb
- data: "C:\Users\Seven01\AppData\Roaming\cvdd.exe" ..
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\954d1751ffef0cb2d74e585c2d0733cb
- data: "C:\Users\Seven01\AppData\Roaming\cvdd.exe" ..
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\954d1751ffef0cb2d74e585c2d0733cb.exe
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\954d1751ffef0cb2d74e585c2d0733cb.exe
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job

A process was set to shut the system down when terminated

- process: cvdd.exe:2896

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

- Spam: services.exe (484) called API GetSystemTimeAsFileTime 1924909 times

Queries information on disks, possibly for anti-virtualization

Sniffs keystrokes

- GetAsyncKeyState: Process: cvdd.exe(2896)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.98, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00026400, virtual_size: 0x00026234
- section: name: .rsrc, entropy: 8.00, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ, raw_size: 0x000f4c00, virtual_size: 0x000f4acc

Performs some HTTP requests

- url: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Roaming\Googledocs.exe
- binary: C:\Users\Seven01\AppData\Roaming\cvdd.exe

A process created a hidden window

- Process: nd.exe -> "cmd"
- Process: Googledocs.exe -> "cmd"
- Process: Googledocs.exe -> "cmd"
- Process: cvdd.exe -> "cmd"
- Process: cvdd.exe -> "cmd"

Reads data out of its own binary image

- self_read: process: Googledocs.exe, pid: 2828, offset: 0x00000000, length: 0x0011b400

At least one IP Address, Domain, or File Name was found in a crypto call

- ioc: inetsim.org0

A process attempted to delay the analysis task.

- Process: sppsvc.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds
- Process: cvdd.exe tried to sleep 573 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

Attempts to connect to a dead IP:Port (3 unique times)

- IP: 192.168.56.1:443
- IP: 212.83.167.116:766 (France)
- IP: 192.168.56.1:80

1 HTTP Request(s) detected

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 95.101.34.82
Port: 80
Count: 1

1 Host(s) detected

IP Address	Hostname	Reverse DNS
212.83.167.116		212-83-167-116.rev.poneytelecom.eu.

1 Countr(y|ies) detected

Hosts	Country
1	France