adwcleaner%20last.exe

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

MalFamily: Bladabindi **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	63.51 KB (65031 bytes)
Compile time:	2017-05-31 19:39:25
MD5:	2d4e151f6f774efa90b3359a79baff27
SHA1:	4da63e5346883a8c42d7a9295dce09b1233ef6ea
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-07-16 08:18:02

URL(s) file hosting

http://extreme-alts.livehost.fr/download/adwcleaner%20last.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-07-15 18:53:43	43/63	

Import library

mscoree.dll

9 Behaviors detected by system signatures

Sniffs keystrokes

- GetAsyncKeyState: Process: Vape.exe(2796)

A process was set to shut the system down when terminated

- process: Vape.exe:2796

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\308bb7f0eb2fed41099e2ac197ff114b
- data: "C:\Users\Seven01\AppData\Local\Temp\Vape.exe" ..
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\308bb7f0eb2fed41099e2ac197ff114b
- data: "C:\Users\Seven01\AppData\Local\Temp\Vape.exe" ..

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\$Microsoft.NET

Anomalous binary characteristics

- anomaly: Actual checksum does not match that reported in PE header

Creates RWX memory

Reads data out of its own binary image

- self_read: process: adwcleaner20last.exe, pid: 2488, offset: 0x00000000, length: 0x0000fe07
- self_read: process: RegAsm.exe, pid: 2652, offset: 0x00000000, length: 0x0000a000

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Roaming\$Microsoft.NET\RegAsm.exe
- binary: C:\Users\Seven01\AppData\Local\Temp\Vape.exe

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

- IP: 88.190.115.10:5552 (France)

1 Host(s) detected

IP Address	Hostname	Reverse DNS
88.190.115.10		maz13-2-88-190-115-10.fbxo.proxad.net.

1 Countr(y|ies) detected

Hosts	Country
1	France