Server.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:	23.50 KB (24064 bytes)
Compile time:	2018-04-21 16:15:52
MD5:	b9d0e59b693e28208c1ef2a8dbb820ee
SHA1:	4455ac7c246006212e8bf9dd35158e0f60d618d2
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-24 03:24:04

URL(s) file hosting

http://legalwatch.com/Files/Server.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-04-24 06:19:50	56/66	

Import library

mscoree.dll

4 Behaviors detected by system signatures

Sniffs keystrokes

- GetAsyncKeyState: Process: Server.exe(1976)

Installs itself for autorun at Windows startup

- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\3df0c4f09ba50ad55ae1a872404a9e64
- data: "C:\Users\Seven01\AppData\Local\Temp\Server.exe" ..
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\3df0c4f09ba50ad55ae1a872404a9e64
- data: "C:\Users\Seven01\AppData\Local\Temp\Server.exe" ..

Creates RWX memory

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

- IP: 60.48.39.240:1144 (Malaysia)

1 Host(s) detected

IP Address	Hostname	Reverse DNS
60.48.39.240		240.39.48.60.klj03-home.tm.net.my.

1 Countr(y|ies) detected

Hosts	Country
1	Malaysia