Antivirus Event Analysis Cheat Sheet

Version 1.8.1, Florian Roth @cyb3rops

Attribute	Less Relevant	Relevant	Highly Relevant
Virus Type	HTML Iframe Keygen Joke Adware Clickjacking Crypto FakeAV	Trojan Backdoor Agent Malware JS Creds PS PowerShell Exploit Ransom PassView Tool-Netcat Tool-Nmap RemAdm NetTool Crypto Scan	HackTool HTool HKTL PWCrack SecurityTool Clearlogs PHP/BackDoor ASP/BackDoor JSP/BackDoor Backdoor.PHP Backdoor.ASP Backdoor.JSP Webshell DumpCreds MPreter Koadic Razy CobaltStr COBEACON Cometer Keylogger MeteTool Meterpreter Metasploit PowerSSH Mimikatz PowerSploit PSWTool PWDump Swrort Rozena Backdoor.Cobalt PShlSpy Packed.Generic.347 IISExchgSpawnCMD
Location	Temp Internet Files Removable Drive (E:, F:, …)	C:\Temp $Recycle.bin C:\ProgramData C:\Users\Public AppData\Local\Temp AppData\Roaming\Temp C:\Windows\Temp	%SystemRoot% (e.g. C:\Windows) C:\ \\Client\[A-Z]$ (remote session client drive) \\tsclient\<drive> C:\PerfLogs \*$ (execution on remote host) Other directories that are writable for Administrators only
User Context		Standard User	Administrative Account Service Account
System	File Server Email Server Ticket System	Workstation Other Server Type	Domain Controller Print Server DMZ Server Jump Server Admin Workstation
Form / Type	Common Archive (ZIP)	Not Archived / Extracted, Uncommon Archive (RAR, 7z, encrypted Archive)	File Extensions: .ASP .ASPX .BAT .CHM .HTA .JSP .JSPX .LNK .PHP .PS1 .SCF .TXT .VBS .WAR .WSF .WSH .XML .CS .JPG .JPEG .GIF .PNG .DAT
Time		Regular Work Hours	Outside Regular Work Hours
Google Search (File Name)		Well-known Malware (e.g. mssecsvc.exe) or no result at all	APT related file mentioned in report
Virustotal (Requires Hash / Sample)	**Notes >** "Probably harmless", "Microsoft software catalogue" **File Size >** Less than 16 byte (most likely an empty file, error page etc.) **ssdeep >** 3:: means file is filled with zeros (likely caused by AV)	**Comments >** Negative user comments **Additional Information > Tags >** CVE-* **Additional Information >** File names: *.virus **Additional Information >** File names: hash value as file name **Packers identified >** Uncommon Packers like: PECompact, VMProtect, Telock, Petite, WinUnpack, ASProtect **Suspicious combinations >** e.g. UPX, RARSFX, 7ZSFX and Microsoft Copyright	**File Detail >** Revoked certificate **Packers identified >** Rare Packers like: Themida, Enigma, ApLib, Tasm, ExeCryptor, MPRESS, ConfuserEx **Comments>** THOR APT Scanner: “Hacktools”, “Threat Groups”, “Webshell”, “Cobalt Strike”, “Empire”, “Mimikatz”, “Veil”, “Privilege Escalation”, “Password Dumper”, “Koadic”, “Elevation”, “Winnti”