Antivirus Event Analysis - Cheat Sheet

Version 1.2, 12.05.2018, 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 Keylogger Ransom	HackTool (HTool) HKTL PWCrack Scan SecurityTool Clearlogs PHP/BackDoor ASP/BackDoor JSP/BackDoor Backdoor.PHP Backdoor.ASP Backdoor.JSP Webshell NetTool DumpCreds CobaltStrike
Location	Temporary Internet Files Removable Drive (E:, F:, …)	AppData $Recycle.bin User Temp (e.g. %AppData%\Temp)	%SystemRoot% (e.g. C:\Windows) C:\ (non-recursive) C:\Temp C:\Windows\Temp \\Client\[A-Z]$ (remote session client drive) C:\PerfLogs Other dirs writable for Administrators only
User Context		Standard User	Administrator Service Account
System	File Server Email Server	Workstation Other Server Type	Domain Controller Print Server DMZ Server Jump Server
Form / Type	Common Archive (ZIP)	Not Archived / Extracted Uncommon Archive (RAR, 7z, encrypted Archive)	File Types: .PS1 .RTF .VBS .BAT
Time		Regular Work Hours	Outside Regular Work Hours
Virustotal Check (Requires Hash / Sample)	**Notes >** "Probably harmless" "Microsoft software catalogue"	**Comments >** Negative user comments **Additional Information > Tags >** CVE-* **FileVersionInfo properties >** empty or non-existent **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	**File Detail >** Revoked certificate **Additional Information >** Many different file names **Packers identified >** Rare Packers like: Themida, Enigma, ApLib, Tasm, ExeCryptor, MPRESS **Comments>** THOR APT Scanner: “Hacktools”, “Threat Groups”, “Webshell”, “Cobalt Strike”, “Empire”, “Mimikatz”, “Veil”, “Privilege Escalation”, “Password Dumper”, “Password Tools”, “Koadic”, “Elevation”