Antivirus Event Analysis Cheat Sheet

Version 1.14.0, Florian Roth @cyb3rops

Attribute	Less Relevant	Relevant	Highly Relevant
Virus Type	Adware Clickjacking Crypto FakeAV HTML Iframe Joke Keygen Tool-Nmap	Agent Backdoor Clearlogs Creds Crypto Exploit JS LNK Malware Miner NetTool PassView PowerShell PS RemAdm Scan Stealer Tool-Netcat Trojan Wacatac	Adfind ASP/BackDoor ATK/ Backdoor.ASP Backdoor.Cobalt Backdoor.JSP Backdoor.PHP Blackworm Brutel BruteR Certify Chaos Chopper Cobalt COBEACON Cobra Cometer ContiCrypt CRYPTES Cryptor CylanCrypt DelShad Destructor DumpCreds DumpPert Exploit.Script.CVE Filecoder FRP. FastReverseProxy GrandCrab HackTool Haperlockl Havoc HiddenTear HKTL HTool HydraCrypt Impacket IISExchgSpawnCMD JSP/BackDoor Keylogger Koadic Krypt Lazagne Locker Lockbit Mallox Metasploit Meterpreter MeteTool Mimikatz Mpreter MsfShell MultiDump NanoDump NativeDump Nighthawk Packed.Generic.347 PentestPowerShell Phobos PHP/BackDoor Potato PowerSploit PowerSSH PshlSpy PSWTool PWCrack PWDump PWS. PWSX pypykatz Ransom Razy Rozena Rusthound Ryuk Ryzerlo SafetyKatz Sbelt Seatbelt SecurityTool SharpChrome SharpDAPI SharpDump SharpHound SharpKatz SharpS. ShpKatz Shellcode Sliver Snaffler SOAPHound Splinter Stopcrypt Swrort Tescrypt TeslaCrypt TrickDump TurtleLoader Valyria WannyCry Webshell Xorist
Location	Temp Internet Files Removable Drive (E:, F:, …) All other folders	C:\Temp $Recycle.bin C:\ProgramData C:\Users\Public C:\Users\All Users AppData\Local\Temp AppData\Roaming\Temp C:\Windows\Temp	C:\Windows\System32 C:\Windows C:\ \\Client\[A-Z]$ (remote session client drive) \\tsclient\<drive> C:\Program Files\Microsoft Azure AD Sync\ C:\Program Files\AzureAppProxy\ C:\Windows\System32\Tasks\ C:\Windows\System32\spool\ C:\Perflogs AppData\Local\Microsoft\Terminal Server Client\Cache\ \FrontEnd\HttpProxy\owa\auth\ \inetpub\wwwroot\aspnet_client\ \*$ (execution on remote host)
User Context		Standard User	Administrative Account Service Account
System	File Server Ticket System	Workstation Email Server Other Server Type	Domain Controller Print Server DMZ Server Jump Server Admin Workstation Application Proxy Connector
Form / Type	Common Archive (ZIP)	Not Archived / Extracted, Uncommon Archive (RAR, 7z, encrypted Archive)	File Extensions: APPX .ASP .ASPX .BAT .CAB .CHM .CS .DIAGCAB .DMG .GIF .HTA .ICS .IMG .ISO .JAR .JNLP .JPG .JPEG .JSP .JSPX .LNK .MSC .ONE .PHP .PNG .PS1 .RDP .SCF .TXT .VBE .VBS .VHD .VHDX .WAR .WBK .WLL .WSF .WSH .XLL .XML
Time		Regular Work Hours	Outside Regular Work Hours, Public Holidays
Virustotal (Requires Hash / Sample)	**Tags >** trusted, known-distributor, zero-filled **File Size >** Less than 16 byte (most likely an empty file, error page etc.)	**Tags >** url-pattern, auto-open, obfuscated, via-tor, lnk, invalid-signature **File names >** *.virus **Packers identified >** Uncommon Packers like: PECompact, VMProtect, Telock, Petite, WinUnpack, ASProtect	**File Detail >** Revoked certificate **Tags >** spreader, dropper, cve-20*, exploit, revoked-cert, trojan, yoda*, hiding-window **Packers identified >** Rare Packers like: Themida, Enigma, ApLib, Tasm, ExeCryptor, MPRESS, ConfuserEx