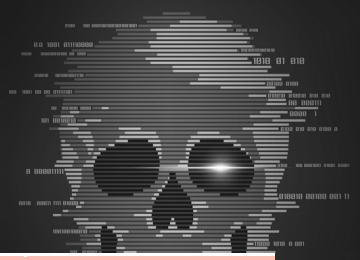
Antivirus Event Analysis Cheat Sheet

Version 1.12.0, 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 Chopper Cobalt COBEACON Cometer CRYPTES Cryptor Cryptor Destructor DumpCreds Exploit.Script.CVE Filecoder FRP. FastReverseProxy GrandCrab HackTool HKTL HTool Impacket IISExchgSpawnCMD JSP/BackDoor Keylogger Koadic Krypt Lazagne Locker Metasploit Meterpreter MeteTool Mimikatz Mpreter Nighthawk Packed.Generic.347 PentestPowerShell Phobos PHP/BackDoor Potato PowerSploit PowerSSH PshlSpy PSWTool PWCrack PWDump PWS. PWSX Ransom Razy Rozena Ryuk Ryzerlo Sbelt Seatbelt SecurityTool SharpDump Sliver Swrort Tescrypt TeslaCrypt Valyria Webshell
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:\PerfLogs \FrontEnd\HttpProxy\owa\auth\ \inetpub\wwwroot\aspnet_client\ *$ (execution on remote host) Other directories that are writable for Administrators only
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: .ASP .ASPX .BAT .CHM .HTA .JSP .JSPX .JAR .LNK .PHP .PS1 .SCF .TXT .VBS .WAR .WSF .WSH .XML .CS .JPG .JPEG .GIF .PNG .CS .CAB .ISO .JNLP .IMG .DIAGCAB .APPX .DMG .ONE
Time		Regular Work Hours	Outside Regular Work Hours, Public Holidays
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” **Tags >** trusted, known-distributor, zero-filled **File Size >** Less than 16 byte (most likely an empty file, error page etc.)	**Comments >** Negative user comments **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 **Suspicious combinations >** e.g. UPX, RARSFX and Microsoft Copyright	**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 **Comments>** THOR APT Scanner: “Hacktools”, “Threat Groups”, “Webshell”, “Cobalt Strike”, “Empire”, “Mimikatz”, “Veil”, “Privilege Escalation”, “Password Dumper”, “Koadic”, “Elevation”, “Winnti”