

# Antivirus Event Analysis Cheat Sheet

Version 1.9.0, Florian Roth @cyb3rops

Attribute	Less Relevant	Relevant	Highly Relevant
<b>Virus Type</b>	HTML Iframe Keygen Joke Adware Clickjacking Crypto FakeAV Tool-Nmap	Trojan Backdoor Agent Malware JS Creds PS PowerShell Exploit	PassView Tool-Netcat RemAdm NetTool Crypto Scan Clearlogs Miner HackTool HTool HKTL PWCrack SecurityTool PHP/BackDoor ASP/BackDoor JSP/BackDoor Backdoor.PHP Backdoor.ASP Backdoor.JSP Webshell DumpCreds MPreter Koadic Razy ATK/ Ransom Filecoder Packed.Generic.347 CobaltStr COBEACON Cometer Keylogger Meterpreter Metasploit PowerSSH Mimikatz PowerSploit PSWTool PWDump Swrort Rozena Backdoor.Cobalt PShISpy IISExchgSpawnCMD Exploit.Script.CVE Chopper
<b>Location</b>	Temp Internet Files Removable Drive (E:, F:, ...)	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
<b>User Context</b>		Standard User	Administrative Account Service Account
<b>System</b>	File Server Ticket System	Workstation Email Server Other Server Type	Domain Controller Print Server DMZ Server Jump Server Admin Workstation
<b>Form / Type</b>	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 .DAT .CS .CAB .ISO .JNLP
<b>Time</b>		Regular Work Hours	Outside Regular Work Hours
<b>Google Search (File Name)</b>		Well-known Malware (e.g., mssecsvc.exe) or no result at all	APT related file mentioned in report
<b>Virustotal (Requires Hash / Sample)</b>	<b>Notes &gt;</b> "Probably harmless", "Microsoft software catalogue" <b>File Size &gt;</b> Less than 16 byte (most likely an empty file, error page etc.) <b>ssdeep &gt;</b> 3:: means file is filled with zeros (likely caused by AV)	<b>Comments &gt;</b> Negative user comments <b>Additional Information &gt; Tags &gt;</b> CVE-* <b>Additional Information &gt;</b> File names: *.virus <b>Packers identified &gt;</b> Uncommon Packers like: PECompact, VMProtect, Telock, Petite, WinUnpack, ASProtect <b>Suspicious combinations &gt;</b> e.g. UPX, RARSFX, 7ZSFX and Microsoft Copyright	<b>File Detail &gt;</b> Revoked certificate <b>Packers identified &gt;</b> Rare Packers like: Themida, Enigma, ApLib, Tasm, ExeCryptor, MPRESS, ConfuserEx <b>Comments &gt;</b> THOR APT Scanner: "Hacktools", "Threat Groups", "Webshell", "Cobalt Strike", "Empire", "Mimikatz", "Veil", "Privilege Escalation", "Password Dumper", "Koadic", "Elevation", "Winnti"