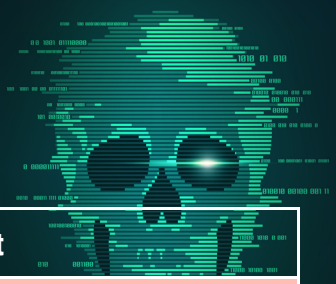
Antivirus Event Analysis Cheat Sheet

Version 1.5
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 Crypt Scan	HackTool HTool HKTL PWCrack SecurityTool Clearlogs PHP/BackDoor ASP/BackDoor JSP/BackDoor Backdoor.PHP Backdoor.ASP Backdoor.JSP Webshell DumpCreds CobaltStrike Keylogger MeteTool Meterpreter Metasploit PowerSSH Mimikatz PowerSploit PSWTool PWDump
Location	Temporary Internet Files Removable Drive (E:, F:, …)	AppData $Recycle.bin User's %Temp% (e.g. %AppData%\Temp)	%SystemRoot% (e.g. C:\Windows) C:\ C:\Temp C:\Windows\Temp \\Client\[A-Z]$ (remote session client drive) C:\PerfLogs C:\Users\Public Other dirs writable for Administrators only
User Context		Standard User	Administrator, 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 Types: .PS1 .RTF .VBS .BAT .CHM .XML .TXT .JSP .JSPX .ASP .ASPX .PHP .WAR
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-* **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 **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"

Highly Relevant Events by Vendor	
McAfee	HTooL-Mimikatz*, *Chopper*, *CCProxy*, Tool-Xscan, HTool-WCE, ASP/BackDoor.gen, PortScan-ScanLine, BackDoor-BKX, Trojan-Cleaver, BackDoor-FAJ, Generic-FAHD*, PWS-Spyeye*, *SecurityTool*, HTool-GSECDump, Clearlogs, PWCrack-*, Tool-Sbd, ASP/BackDoor.gen, HTool-nts6, PHP/BackDoor.gen, *JSP/Webshell, *PHP/Webshell, Tool-TCPScan, RDN/Generic PUP*, Tool-NtCmd, Clearlogs
Symantec	Infostealer.Derusbi, Hacktool.Mimikatz, SecurityRisk.WinCredEd, Hacktool.PTHToolkit, NetCat, Backdoor.Hadmad, Backdoor.Korplug*, Hacktool.Scan, Pwdump, SuperScan, PasswordRevealer, XScan, PHP.Backdoor*, JSP.Backdoor*, Trojan.Explod*, Backdoor.Korplug*, Backdoor.Graybird, Trojan.Malscript, Hacktool.*
Sophos	Clearlog, Generic PUA IC, Troj/Aspdoor*, Troj/Bckdr-RSM, Troj/Plugx*, Troj/ASPXSpy*, Troj/Chopper*
Kaspersky	VBS.WmiExec, HackTool.*, Backdoor.ASP*, Backdoor.JSP*, Backdoor.PHP*, Trojan.Win32.StartServ, *NetTool.Win32.Agent*, Backdoor.Win32.Gulpix*, HEUR:NetTool.Win32.Generic, *NetTool.Win32.Portscan*, UDS:DangerousObject.Multi.Generic, HackTool.Win32.XScan*, Backdoor.Win32.Liondoor*, *Clearlog*, NetTool.Win32.ZXProxy*