Antivirus Event Analysis Cheat Sheet v1.8.2

by Florian Roth | Aug 16, 2021

The analysis of Antivirus events can be a tedious task in big organizations with hundreds of events per day. Usually security teams fall back to a mode of operation in which they only analyze events in which a cleanup process has failed or something went wrong.

This is definitely the wrong approach for a security team. You should instead focus on highly relevant events.

This cheat sheet helps you select these highly relevant Antivirus alerts.

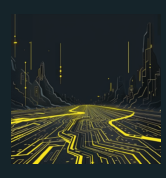
Download the Antivirus Event

Antivirus Event Analysis Cheat Sheet
Version 1.8.2, 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 Crypto Scan	HackTool HTool HKTL PWCrack SecurityTool Clearlogs PHP/BackDoor ASP/BackDoor JSP/BackDoor Backdoor.PHP Backdoor.ASP Backdoor.JSP Webshell DumpCreds MPreter Koadic Razy ATK/ CobaltStr COBEACON Cometer Keylogger MeteTool Meterpreter Metasploit PowerSSH Mimikatz PowerSploit PSWTool PWDump Swrort Rozena Backdoor.Cobalt PShlSpy Packed.Generic.347 IISExchgSpawnCMD
Location	Temp Internet Files Removable Drive (E:, F:, …)	C:\Temp $Recycle.bin C:\ProgramData C:\Users\Public AppData\Local\Temp AppData\Roaming\Temp C:\Windows\Temp	%SystemRoot% (e.g. C:\Windows) C:\ \\C\client\[A-Z]$ (remote session client drive) \\tsclient\<drive> C:\PerfLogs *$ (execution on remote host) Other directories that are writable for Administrators only
User Context		Standard User	Administrative Account 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 Extensions: .ASP .ASPX .BAT .CHM .HTA .JSP .JSPX .LNK .PHP .PS1 .SCF .TXT .VBS .WAR .WSF .WSH .XML .CS .JPG .JPEG .GIF .PNG .DAT .CS
Time		Regular Work Hours	Outside Regular Work Hours
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" **File Size >** Less than 16 byte (most likely an empty file, error page etc.) **ssdeep >** 3:: means file is filled with zeros (likely caused by AV)	**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 **Suspicious combinations >** e.g. UPX, RARSFX, 7ZSFX and Microsoft Copyright	**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", "Winnti"

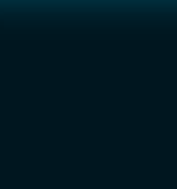
Recent Blog Posts

Introducing @NextronResearch: A New Channel for Threat Intelligence



October 31, 2024

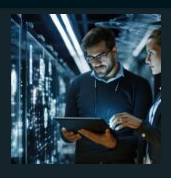
About the author:



Florian Roth

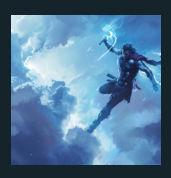
Florian Roth serves as the Head of Research and Development at Nextron Systems. With a background in IT security since 2000, he has delved deep into nation-state cyber attacks since 2012. Florian has developed the THOR Scanner and actively engages with the community via his Twitter handle @cyb3rops. He has contributed to open-source projects, including 'Sigma', a generic SIEM rule format, and 'LOKI', an open-source scanner. Additionally, he has shared valuable resources like a mapping of APT groups and operations and an Antivirus Event Analysis Cheat Sheet.

Important Announcement: Upcoming Migration of our Update Servers



August 14, 2024

Introducing THOR Cloud: Next-Level Automated Compromise Assessments



August 2, 2024

Antivirus Event Analysis Cheat Sheet v1.13.0

July 17, 2024

Top Blog Topics

THOR

Recommended Blog Posts

Introducing THOR Cloud: Next-Level Automated Compromise Assessments

Florian Roth
Aug 2, 2024

Read More

Cybersecurity is Not Just an IT Security Issue

Franziska Ploss
Jul 4, 2024

Read More

Announcing ASGARD Ana v4.1

Boris Deibel
Jun 21, 2024

Read More

Resources

Manuals

Fact Sheets

Customer Portal

Newsletter

Monthly news, tips and insights.

SUBSCRIBE

Company

About Us / Contact

Jobs