MALWARE HUNTING & THREAT HUNTER – OVERVIEW I

JOAS ANTONIO

DETAILS

- This pdf brings an overview about Malware Hunting and Threat Hunter, I hope it helps in your studies.
- https://www.linkedin.com/in/joas-antonio-dos-santos
- https://twitter.com/C0d3Cr4zy

MALWARE AND THREAT HUNTING

MALWARE HUNTING CONTENT

- https://nasbench.medium.com/hunting-malware-with-windows-sysinternals-process-explorer-2baec974bec9
- https://www.youtube.com/watch?v=vW8eAqZyWeo
- https://www.youtube.com/watch?v=A_TPZxuTzBU
- https://www.youtube.com/watch?v=owAOHsLyD3Y
- https://www.youtube.com/watch?v=Ljm6UPT0JkI
- http://index-of.co.uk/Malware/hta-t07r-license-to-kill-malware-hunting-with-the-sysinternals-tools_final.pdf
- https://securelist.com/how-to-hunt-for-rare-malware/77040/
- https://www.sentinelone.com/blog/malware-hunting-macos-practical-guide/
- https://malwarehunterteam.com/
- https://www.fireeye.com/blog/products-and-services/2021/03/hunt-and-detect-malware-with-advantage-yara-rules.html
- https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-find-ransomware?view=o365-worldwide
- https://www.cybered.io/webinars/proactive-malware-hunting-w-782
- http://download.microsoft.com/download/B/7/7/B7736788-7DEF-43F3-AC8A-C8521AD7354A/PDF/WIN-B306.pdf
- https://i.blackhat.com/USA-19/Wednesday/us-19-Amini-Worm-Charming-Harvesting-Malware-Lures-For-Fun-And-Profit.pdf

MALWARE HUNTING CONTENT

- https://www.semanticscholar.org/paper/Cryptocurrency-malware-hunting%3A-A-deep-Recurrent-Yazdinejad-Haddadpajouh/8ce52b6a580541e4f36cf44ba3ca59d1013e241c
- https://www.pluralsight.com/courses/detecting-analyzing-fileless-malware
- https://blog.reversinglabs.com/blog/hunting-for-ransomware
- https://www.malwarebytes.com/resources/files/2020/06/final_ebook_threat-hunting-made-easy_0518.pdf
- http://reconstructer.org/papers/Hunting%20malware%20with%20Volatility%20v2.0.pdf
- https://www.sans.org/reading-room/whitepapers/malicious/paper/38960
- https://www.blackhat.com/docs/webcast/08202015-big-game-hunting.pdf
- https://www.blackhat.com/docs/us-17/wednesday/us-17-Ruthven-Fighting-Targeted-Malware-In-The-Mobile-Ecosystem.pdf
- https://i.blackhat.com/eu-20/Thursday/eu-20-Cheng-The-Hunt-For-Major-League-IoT-ICS-Threats-A-Deep-Dive-Into-IoT-Threat-Terrain.pdf
- https://i.blackhat.com/eu-20/Thursday/eu-20-Cheng-The-Hunt-For-Major-League-IoT-ICS-Threats-A-Deep-Dive-Into-IoT-Threat-Terrain-wp.pdf
- https://i.blackhat.com/executive-interviews/2021/Black-Hat-20210225-Cisco_Threat-Hunting_v2.pdf
- https://www.blackhat.com/docs/eu-17/webcast/10052017-scaling-security-operations.pdf
- https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Rutkowska/BH-Fed-06-Rutkowska-up.pdf
- https://i.blackhat.com/asia-21/Thursday-Handouts/as-21-Khanna-Threat-Hunting-In-Active-Directory-Environment.pdf
- https://i.blackhat.com/USA-20/Thursday/us-20-Cureton-Heroku-Abuse-Operations-Hunting-Wolves-in-Sheeps-Clothing.pdf

CYBER KILL CHAIN

- https://i.blackhat.com/executive-interviews/us-20/black-hat-webcast-summary_how-attackers-confuse-investigators-with-cyber-false-flag-attacks_extrahop.pdf
- https://www.blackhat.com/docs/webcast/10212014-webcast-controlling-your-own-battlespace.pdf
- https://www.blackhat.com/docs/us-16/materials/us-16-Malone-Using-An-Expanded-Cyber-Kill-Chain-Model-To-Increase-Attack-Resiliency.pdf
- https://www.blackhat.com/docs/us-16/materials/us-16-Beery-The-Remote-Malicious-Butler-Did-It-wp.pdf
- https://www.blackhat.com/docs/webcast/10222015-battlefield-network.pdf
- https://www.blackhat.com/docs/webcast/02182016-a-community-attack-model-sager.pdf
- https://i.blackhat.com/USA-19/Thursday/us-19-Conti-Operational-Templates-for-State-Level-Attack-and-Collective-Defense-of-Countries.pdf
- https://www.blackhat.com/docs/webcast/10202016-investigating-ddos-arbor.pdf
- https://www.blackhat.com/docs/us-15/materials/us-15-Hovor-UTIP-Unstructured-Threat-Intelligence-Processing.pdf
- https://i.blackhat.com/USA-19/Wednesday/us-19-Jablonski-Attacking-Electric-Motors-For-Fun-And-Profit.pdf
- https://www.proof.com.br/blog/o-que-e-cyber-kill-chain/
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://computerworld.com.br/seguranca/voce-conhece-o-conceito-de-cyber-kill-chain/
- https://www.4security.com.br/wp-content/uploads/2020/02/4Security-Cyber-Kill-Chain.pdf

MITRE ATT&CK

- https://attack.mitre.org/
- https://realprotect.net/o-que-e-o-mitre-attck-e-como-ele-pode-melhorar-sua-cybersecurity/
- https://www.anomali.com/pt/resources/what-mitre-attck-is-and-how-it-is-useful
- https://www.mcafee.com/enterprise/pt-br/security-awareness/cybersecurity/what-is-mitre-attack-framework.html
- https://www.welivesecurity.com/br/2019/06/07/como-usar-mitre-attck-uma-lista-de-tecnicas-e-procedimentos-de-ataques-e-defesas/
- https://www.rapid7.com/fundamentals/mitre-attack/
- https://www.threatq.com/mitre-attack/
- https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf
- https://attack.mitre.org/docs/MITRE_ATTACK_Enterprise_11x17.pdf
- https://attack.mitre.org/docs/training-cti/CTI%20Workshop%20Full%20Slides.pdf
- https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
- https://www.cybereason.com/hubfs/dam/collateral/1-pagers/cr-mitre-one-pager.pdf

THREAT HUNTING

- https://docs.broadcom.com/doc/threat-hunting-with-mitre-attack
- https://www.threathunting.net/files/hunt-evil-practical-guide-threat-hunting.pdf
- https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CyberDrill-2020/Cyber%20Threat%20Hunting%20Workshop%20-%20ITU%20191120 20.pdf
- https://docs.broadcom.com/doc/play-offense-advanced-threat-hunting-en
- https://www.betaalvereniging.nl/wp-content/uploads/TaHiTI-Threat-Hunting-Methodology-whitepaper.pdf
- https://media.kaspersky.com/en/business-security/enterprise/Kaspersky_Threat_Hunting_Services.pdf
- https://media.kaspersky.com/en/business-security/enterprise/threat-hunting-services-datasheet.pdf
- https://www.sans.org/reading-room/whitepapers/threathunting/paper/38710
- https://www.mitre.org/sites/default/files/publications/pr-19-3892-ttp-based-hunting.pdf
- http://ceur-ws.org/Vol-2833/Paper_10.pdf
- https://www.blackhat.com/docs/webcast/11172016-building-a-threat-hunting-program.pdf
- https://www.group-ib.com/brochures/Group-IB_Threat%20Hunting%20Framework_Leaflet_ENG_.pdf

THREAT HUNTING

- https://www.blackhat.com/docs/us-17/thursday/us-17-Bianco-Go-To-Hunt-Then-Sleep.pdf
- https://i.blackhat.com/executive-interviews/us-20/black-hat-webcast-summary_understanding-and-disrupting-offensive-innovations.pdf
- https://www.blackhat.com/docs/webcast/2018-08-23-intelligent-security-automation-by-ty-miller.pdf
- https://i.blackhat.com/webcasts/2019/BlackhatWebinar-Leveraging-Red-for-Defense-by-David-Kennedy.pdf
- https://www.blackhat.com/docs/webcast/04142016-arbor-spectrum.pdf
- https://www.blackhat.com/docs/us-17/wednesday/us-17-Kacer-SS7-Attacker-Heaven-Turns-Into-Riot-How-To-Make-Nation-State-And-Intelligence-Attackers-Lives-Much-Harder-On-Mobile-Networks.pdf
- https://www.blackhat.com/docs/webcast/09172015-leveraging-proactive-defense.pdf
- https://www.blackhat.com/docs/webcast/2018-12-13-virustotal-enterprise-by-evan-derheim.pdf
- https://www.blackhat.com/docs/eu-17/materials/eu-17-Thompson-Red-Team-Techniques-For-Evading-Bypassing-And-Disabling-MS-Advanced-Threat-Protection-And-Advanced-Threat-Analytics.pdf
- https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors-wp.pdf
- https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors.pdf

THREAT HUNTING

- https://i.blackhat.com/executive-interviews/2020/20201001_Trend_Micro_Heroku_AbuseOps_v3.pdf
- https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors.pdf
- https://i.blackhat.com/briefings/asia/2018/asia-18-Zhu-and-Li-Death-Profile-wp.pdf
- https://www.blackhat.com/docs/webcast/08252016-pay-no-attention.pdf
- https://www.blackhat.com/docs/webcast/07202017-mitigating-and-responding.pdf
- https://i.blackhat.com/USA-19/Wednesday/us-19-Joly-Hunting-For-Bugs-Catching-Dragons.pdf
- https://i.blackhat.com/USA-19/Wednesday/us-19-Nickels-MITRE-ATTACK-The-Play-At-Home-Edition.pdf
- https://i.blackhat.com/USA-19/Thursday/us-19-Smith-Fantastic-Red-Team-Attacks-And-How-To-Find-Them.pdf
- https://www.blackhat.com/docs/us-15/bhus15-schedule.pdf
- https://i.blackhat.com/briefings/asia/2018/asia-18-bohannon-invoke_dosfuscation_techniques_for_fin_style_dos_level_cmd_obfuscation-wp.pdf
- https://i.blackhat.com/webcasts/2019/2019-03-21-deception-through-history-by-david-balcar.pdf
- https://i.blackhat.com/us-18/Thu-August-9/us-18-Haken-Automated-Discovery-of-Deserialization-Gadget-Chains-wp.pdf
- https://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-dodge.pdf
- https://www.blackhat.com/presentations/bh-jp-05/bh-jp-05-geers.pdf
- https://www.blackhat.com/presentations/bh-dc-07/Heasman/Paper/bh-dc-07-Heasman-WP.pdf

THREAT HUNTING

- https://media.defcon.org/DEF%20CON%2028/DEF%20CON%20Safe%20Mode%20villages/DEF%20CON%20Safe%20Mode%20-%20Recon%20Village%20-%20Ladislav%20Baco%20-%20unting%20for%20Blue%20Mockingbird%20Coinminers.pdf
- https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-DimitrySnezhkov-Zombie-Ant-Farm-Practical-Tips.pdf
- https://media.defcon.org/DEF%20CON%20China%201/DEF%20CON%20China%201%20presentations/DEF%20CON%20China%201.0%20-%20Presentations/DEF%20CON%20China%201.0%20-%20Aden-Wee-Jing-Chung-You-are-not-hiding-from-me-Updated-.NET.pdf
- https://media.defcon.org/DEF%20CON%2028/DEF%20CON%20Safe%20Mode%20presentations/DEF%20CON%20Safe%20Mode%20-%20Cooper%20Quintin%20-%20Detecting%20Fake%204G%20Base%20Stations%20in%20Real%20Time.pdf
- https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20workshops/DEFCON-27-Workshop-Guillaume-Ross-Defending-environments-and-hunting-malware-with-osquery.pdf
- https://media.defcon.org/DEF%20CON%20Conference%20Programs/DEF%20CON%2025%20program.pdf
- https://media.defcon.org/DEF%20CON%2011/DEF%20CON%2011%20program.pdf
- https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEF%20CON%2024%20-%20Brad-Woodberg-Malware-Command-And-Control-Channels-A-Journey-Into-Darkness-UPDATED.pdf

MALWARE ANALYSIS

- https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1070&context=creativecomponents#:~:text=The%203%20most%20common%20we,properties%20analysis%2C%20and%20automated%20analysis.
- https://www.blackhat.com/presentations/bh-dc-07/Kendall_McMillan/Presentation/bh-dc-07-Kendall_McMillan.pdf
- https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/web-and-network-security/content-analysis/2-4/generated-pdfs/Malware_Analysis_Guide_v24.pdf
- https://iopscience.iop.org/article/10.1088/1742-6596/1140/1/012042/pdf
- https://docs.broadcom.com/doc/malware-analysis-service-en
- http://stalukder.cs.edinboro.edu/publications/Malware_Survey.pdf
- https://cnsatuva.github.io/files/Intro_Reverse_Malware_Analysis.pdf
- https://www.passus.com/files/FireEye_AX_ds.pdf
- https://media.kaspersky.com/en/enterprise-security/Kaspersky-Lab-Whitepaper-Machine-Learning.pdf

MALWARE ANALYSIS

- https://github.com/rshipp/awesome-malware-analysis
- https://github.com/Apress/malware-analysis-detection-engineering
- https://github.com/PacktPublishing/Mastering-Malware-Analysis
- https://github.com/ytisf/theZoo
- https://github.com/SpiderLabs/malware-analysis
- https://github.com/hasherezade/malware_training_vol1
- https://github.com/nheijmans/malzoo
- https://github.com/intezer/ELF-Malware-Analysis-101
- https://www.mentebinaria.com.br/treinamentos/an%C3%A1lise-de-malware-online-amo-r11/

MALWARE ANALYSIS

- https://github.com/rshipp/awesome-malware-analysis
- https://github.com/Apress/malware-analysis-detection-engineering
- https://github.com/PacktPublishing/Mastering-Malware-Analysis
- https://github.com/ytisf/theZoo
- https://github.com/SpiderLabs/malware-analysis
- https://github.com/hasherezade/malware_training_vol1
- https://github.com/nheijmans/malzoo
- https://github.com/intezer/ELF-Malware-Analysis-101
- https://www.mentebinaria.com.br/treinamentos/an%C3%A1lise-de-malware-online-amo-r11/
- http://www.blackstormsecurity.com/bs/treinamento.html
- https://github.com/filipi86

ROOTKIT AND BOOTKITS

- http://diatinf.ifrn.edu.br/prof/lib/exe/fetch.php?media=user:1379492:pericia_forense_computacional:7-analise-de-maquinas-comprometidas.pdf
- ftp://ftp.registro.br/pub/gts/gts0205/10-rootkit-drm.pdf
- https://www.lume.ufrgs.br/bitstream/handle/10183/26345/000757798.pdf?sequence=1
- https://i.blackhat.com/USA-20/Wednesday/us-20-Demirkapi-Demystifying-Modern-Windows-Rootkits.pdf
- https://tcxsproject.com.br/dev/Biblioteca%20Livros%20Hacker%20Gorpo%20Orko/Rootkits_and_Bootkits__Reversing.pdf
- https://scholar.afit.edu/cgi/viewcontent.cgi?article=4107&context=etd
- https://www.tandfonline.com/doi/abs/10.1080/10658980701402049?journalCode=uiss19
- https://pablo-bravo.com/files/survey.pdf
- https://www.usenix.org/system/files/login/articles/1061-spyware.pdf
- https://blackhat.com/docs/us-14/materials/us-14-Haukli-Exposing-Bootkits-With-BIOS-Emulation-WP.pdf
- https://www.blackhat.com/presentations/bh-usa-09/KLEISSNER/BHUSA09-Kleissner-StonedBootkit-SLIDES.pdf

BUFFER OVERFLOW AND EXPLOIT WRITER

- https://github.com/gh0x0st/Buffer_Overflow
- https://github.com/johnjhacking/Buffer-Overflow-Guide
- https://github.com/justinsteven/dostackbufferoverflowgood
- https://github.com/Tib3rius/Pentest-Cheatsheets/blob/master/exploits/buffer-overflows.rst
- https://github.com/V1n1v131r4/OSCP-Buffer-Overflow
- https://github.com/helviojunior/live_bufferoverflow
- https://github.com/FabioBaroni/awesome-exploit-development
- https://github.com/midnightslacker/exploit_training
- https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/
- https://techilive.in/puzzlemaker-attacks-exploit-windows-zero-day-chrome-vulnerabilities-zdnet/

AWESOMES RED TEAM AND BLUE TEAM

- https://github.com/threat-hunting/awesome_Threat-Hunting
- https://threat-hunting.github.io/awesome_Threat-Hunting/Training,%20Documents%20and%20Instructions/
- https://threat-hunting.github.io/awesome_Threat-Hunting/Tools,Dataset,Framework/
- https://github.com/hslatman/awesome-threat-intelligence
- https://github.com/tylerha97/awesome-reversing
- https://githubmemory.com/repo/saad-eddine/reverse-engineering
- https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://github.com/marcosValle/awesome-windows-red-team
- https://github.com/mantvydasb/RedTeam-Tactics-and-Techniques
- https://github.com/CyberSecurityUP/Awesome-Malware-Analysis-Reverse-Engineering
- https://github.com/CyberSecurityUP/Awesome-Red-Team-Operations
- https://github.com/CyberSecurityUP/Awesome-PenTest-Practice
- https://github.com/CyberSecurityUP/Adversary-Emulation-Matrix
- https://github.com/fabacab/awesome-cybersecurity-blueteam
- https://securityblue.team/
- https://www.tefter.io/~awesome/lists/awesome-cybersecurity-blueteam
- https://github.com/CyberSecurityUP/Awesome-Blue-Team-Operations
- **My ebooks:** https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU