OOTW 01/23/2023

Monday, January 23, 2023 11:17 AM

"Hey everyone, welcome to a another addition to the Out of the Woods Threat Hunting podcast. This is Scott Poley, here with Mike Mitchel and This weekly segment features the top 5 stories that threat hunters need to be thinking about, as well as our thoughts on the subject and hunting strategies.

With that, let's dive into the Top 5 Threat Hunting Headlines for the week of Jan 23rd 2023!"

Are you new to threat hunting?

Are you looking to sharpen your threat hunting skills?

Do you want some social media cred to PROVE that you are a real threat hunter?

Join Cyborg Security's senior threat hunter, Lee Archinal, in our latest fully interactive threat hunting workshop covering credential access! The workshop will dive into the area of credential access including:

* the mechanics of credential access
* what the adversaries are looking for
* tricks of the trade AND
* most importantly how threat hunters and organizations can hunt for signs and traces of credential access in their environment.

When you join, you will get free access to a suite of threat hunting tools you can take home with you, along with real world hunt data you can hone your skills on!

And, if you can complete the final challenge, you'll get your "Credential Access Level 1" certification that you can share on social media to prove that YOU have mastered hunting for credential access.

Join up at the link in the description or check out the event on our LinkedIn page!

https://www.dailydot.com/debug/no-fly-list-us-tsa-unprotected-server-commuteair/

EXCLUSIVE: U.S. airline accidentally exposes ‘No Fly List’ on unsecured server

CommuteAir exposed 'no fly list' that had 1.9 million records of people, as well as, some company personnel and 40 AWS bucket credentials. This happened through a publicly exposed Jenkins server discovered via Shodan.

- Use attack tools to audit yourself --- like Shodan or other tools
- 3rd party services to perform these audits are not frequent enough typically
- Important to 'know thy self'

https://thedfirreport.com/2023/01/23/sharefinder-how-threat-actors-discover-file-shares/

ShareFinder: How Threat Actors Discover File Shares

DFIR report that focused entirely on a technique for finding shares seen in multiple malware campaigns. The tool is ShareFinder which is part of PowerView / module of PowerSploit Framework (powershell post exploitation tool)

- Cmdlet is Invoke-ShareFinder
- Default action is to look for default shares
    - C$, ADMIN$, IPC$
- Can change some of the default behavior

Largest take away, be able to detect or hunt for one-to-many relationships as far as network connections go.

- Some services this is standard behavior
- Look at your vuln scan service --- it will behave this way, but you can use the data to model/emulate
- Also a good behavior credential access techniques, lateral movements,

brute force

https://media.defense.gov/2023/Jan/18/2003145994/-1/-1/0/CSI_IPV6_SECURITY_GUIDANCE.PDF

IPv6 Security Guidance

NSA's released guidelines for IPv6. Really good points and references to dig deeper into concerns, configurations, and risk.

Implementing IPv6 can have some security gotchas. This is a great opportunity to make sure to have good threat hunting processes in case there is a configuration or architecture lapse that adversaries can take advantage of.

- Focus on post exploitation routine hunts
    - Persistence
    - Execution
    - Discovery

https://gizmodo.com/chatgpt-ai-polymorphic-malware-computer-virus-cyber-1850012195

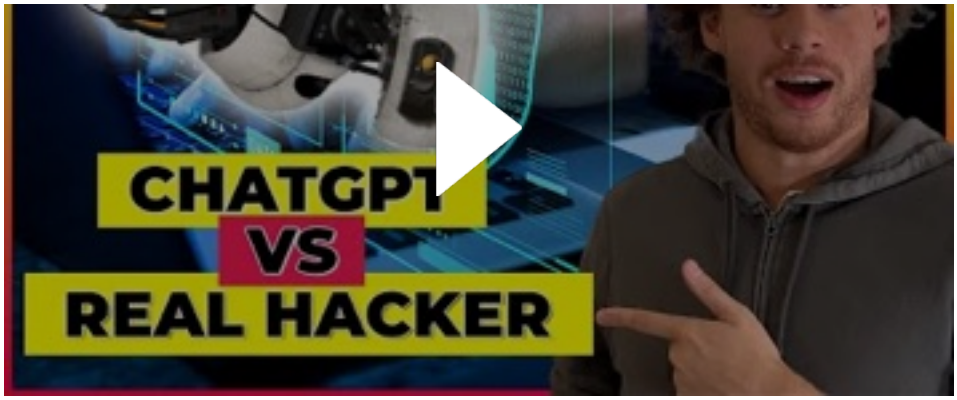
ChatGPT Is Pretty Good at Writing Malware, It Turns Out

Doom and gloom article about chatGPT making advanced malware. ChatGPT can definitely help make malware but it still takes a savy or educated individual to be able to fully construct and leverage it. Great counter reference in the you tube video provided below

- It doesn't understand the native context of environments that malware has to execute in
- No concept of fully integrated c2 infrastructure and malware management

- But since chatGPT understands language really well --- I would still say in can give a leg up on Social Engineering

    Can ChatGPT Write Malware Better Than Me?



https://thehackernews.com/2023/01/gamaredon-group-launches-cyberattacks.html

Gamaredon Group Launches Cyberattacks Against Ukraine Using Telegram

Russian-state sponsored attack on Ukraine using telegram as the c2 for payload delivery. Hard to analyze malware because the ip address would change frequently and it only targeted the ip space of Ukraine.

- **Constantly change IP infrastructure shouldn't stop threat hunting for identification**
    - **Malware used vbscript to launch powershell to pull down execute php file**
    - **Easy to detect behavior --- especially if you look at normal execution of powershell**
- **Thoughts on ideas for war/conflict driven targeted cyber attacks**
    - **Proxying data through other countries to mask techniques to identify yourself as a target**
    - **Might make sense for some businesses or situations**

"Thanks Everyone for joining our Out of the Woods Threat Hunting Podcast. Looking forward to syncing back up next week.
With that, that closes out our Top 5 Threat Hunting Headlines for the week of Jan 23th 2023!

Happy Hunting