OOTW 01/30/2023

Monday, January 30, 2023 9:20 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 30th 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://threatpost.com/watering-hole-attacks-push-scanbox-keylogger/180490/

Watering Hole Attacks Push ScanBox Keylogger

Watering hole attacks hosting ScanBox

ScanBox
- Javascript based --- meaning loaded in browser
- Controlled by "plugin IDs"
    - Keylogger
    - Victim browser plugin identification
    - Browser fingerprinting
    - Peer Connection plugin
    - Security check plugin

STUN protocol
- NAT traversal --- typical used for p2p comms
- Used for c2 interaction

Takeaways:
- Stealthy way to use malicious tools without installing anything.
- Look for STUN protocol
    - Everything inside can be encrypted --- so focus on the header
    - https://www.rfc-editor.org/rfc/rfc5389
    - https://en.wikipedia.org/wiki/STUN
    - STUN can be used as C2 for different future attacks
- Depending on Security Tool infrastructure --- may be able to look at javascript payload detections

https://cybernews.com/news/german-tank-support-spurs-russian-cyberattacks/

Germany's tank support met with Russian cyberattacks

Germany supporting Ukraine with tanks, promotes Cyber response from Russia/Russia supporting actors

Type of behavior:

- Looked like mass scanning for infrastructure and vulns
- Some follow on activity based on seen vulns --- but more DDoS like attemps
- Comments on infrastructure being used from NATO/Ukraine supporting countries
    - But that is kind of to be expected, DDoS is botnet driven --- and Russia isn't suppose to attack itself in that case (kind of their rules of engagement

Takeaways:

- Just highlighting geopolitical ties to cyber
- Important intel --- what is your country/company going to be doing --- and who does that effect

https://cybernews.com/security/russians-use-western-networks-attack-ukraine/

Russian hackers use western networks to attack Ukraine

Cyber Security Firm Lupoivs spread decoys/honeytokens to gather intel on adversaries.

Primarily targeting Russia/Russian supported adversaries by using Ukrainian themed decoys

Decoys:

- HoneyFiles --- contains critical info to be used for follow on attacks and beaconed
- WebPortals -- vulnerable
- High interaction /ssh services --- using same creds as webportal

Bait interaction:

- Opportunistic adversary - scan and run CVEs/Exploits
- Third-Party - adversary discovers on their own --- or from someone sharing the collected info --- (thoughts here are these adversaries could

have opened docs in a secure way as to protect from this type of counter intel)
- Bait - adversaries that opened decoys and proceeded to attack --- more manual

Discoveries:
- Attacks seemed to originate from global orgs that were compromised in countries around the world (15 healthcare orgs)
- 50-60 attackers on decoys within minutes
- Wide range of attacks deployed --
    - SQL injection
    - Remote file inclusion
    - Docker exploitation
    - Use of leaked creds
    - Known CVEs
    - DDoS
    - Custom scripts

Takeaways:
- Fantastic work
- Shows how quickly information disclosure could ramp up to cyber attack if there is intent
- Also a great way to answer --- who are my threats --- what are their capabilities

https://www.theguardian.com/business/2023/jan/30/jd-sports-cyber-attack-customers-data-jd-size-millets-blacks

JD Sports hit by cyber-attack that leaked 10m customers' data

JD Sports appeared to be breached --- not much technical data around the breach other that customer identifying data was exposed (supposedly not passwords or credit cards)

https://thehackernews.com/2023/01/realtek-vulnerability-under-attack-134.html

Realtek Vulnerability Under Attack: Over 134 Million

Attempts to Hack IoT Devices

Realtek vulnerability affects UDPServer in their RealtekJjungle SDK. Affects a large number of IoT devices as well as network devices. Hard to know what chipset is present in devices so look for port 9034 open. Basically running a stripped-down linux system from RealTek, which is why a bash script is run to pull down and run malware.

Takeaways:

- **Good example of supply chain effects on defense**
- **Hard for the consumers --- but orgs really need to assess all devices they put on the network for open services ports/etc.**

More details:
https://unit42.paloaltonetworks.com/realtek-sdk-vulnerability/

https://onekey.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/

"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 30th 2023!

Happy Hunting