OOTW 04/03/2023

Monday, April 3, 2023 11:51 AM

"Hey everyone, welcome to a another addition to the Out of the Woods Threat Hunting podcast. This is Scott Poley, here with Mike Mitchell 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 Apr 3rd 2023!"

https://thedfirreport.com/2023/04/03/malicious-iso-file-leads-to-domain-wide-ransomware/

Malicious ISO File Leads to Domain Wide Ransomware

This DFIR report walks through a compromise that started with ISO phishing that led to IcedID payload and some cobalt strike beacons full domain takeover with, exfiltration and ransomware. There seemed to be a lot of hands on keyboard with this attack since parts didn't work at first and they had to manually make changes to get things working.

Some things to look at in terms of threat hunting:

- ISO payloads (execution of LNK -> cmd)
- ADFind discovery arguments
- Remote WMI execution
- DCSyncs
- Rclone arguments
- Cmd /c patterns (especially with with parent image exlorer.exe) or /c echo
- Powershell WebClient DownloadString
- Scheduled tasks --- seeing a lot of DLL runs with just the entry point markd as #1 to execute

- Powershell to uninstall Defender 'Uninstall-WindowsFeature'
- Procdump - lsass
- Dropped a number of open offensive tools --- no masquerading

https://www.fortinet.com/blog/threat-research/moobot-strikes-again-targeting-cacti-and-realtek-vulnerabilities

Moobot Strikes Again - Targeting Cacti And RealTek Vulnerabilities

Activity seen where Realtek Jungle, Cacti, IBM Aspera Faspex (file exchange application) vulns are being hit with MoonBot and Shell bot. These bots provide basic capabilities to scan, do DDoS, or download files (further payloads).

Some things to consider with hunting:

- Network Payload Headers - in both cases
    - Linux based commands are present with ';'
- Depending on you network visibility --- this data may be available to look for this behavior that could come up with possible other vulns that get discovered

https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability

This report tracks captures the activity of Winter Vivern using a known zimbra vulnerability in order to steal creds from a web mail by appending an arbitrary hexadecimal encoded or plaintext JavaScript snippet, which is executed as an error parameter when it is received in the initial web request. The JavaScript, once decoded, results in the download of a next stage bespoke JavaScript payload that conducts CSRF to capture usernames, passwords, and CSRF tokens from the user.

Cross-Site Request Forgery (CSRF) is an attack that forces authenticated users to submit a request to a Web application against which they are users to submit a request to a Web application against which they are currently authenticated. CSRF attacks exploit the trust a Web application has in an authenticated user.

Things to hunt for:

- I looked at activity for Winter Vivern across a few recent reports
  - SentinelOne - landing pages with malicious downloads (macros) or steal creds [early 2023]
    - https://www.sentinelone.com/labs/winter-vivern-uncovering-a-wave-of-global-espionage/
  - Lab52 - macros [9/2021]
    - https://lab52.io/blog/winter-vivern-all-summer/
- Big mention all other reports outside of proofpoint when looking at discovered infections -- powershell webclient downloadstrings

https://www.al.com/news/2023/04/jefferson-county-schools-victim-of-ransomware-attack.html

Jefferson County Schools victim of ransomware attack

Jefferson County Schools in AL were hit with ransomware over spring break.

To note Huntsville City Schools in AL were hit with ransomware end of 2020. Questions come if there is any lessons learned from previous attacks within the state to help with protecting or responding to those attacks.

https://www.darkreading.com/cloud/us-space-force-wants-700m-cybersecurity

US Space Force Requests $700M for Cybersecurity Blast Off

This report shows that there will be an increase of budget for US Space Force in cyber security. This is good awareness for those that are looking for future job opportunities. Other than potential clearances, it's good to get the required certifications to be allowed privileged access on those networks in order to be a good candidate for potential new positions. The list can be found here:

https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/

Top Cover 2 - Management

Apr 12th 12- 1pm EST

Live podcast Apr 20th 7-830pm EST

Fun interactive discord discussions and indepth experience based topics

Hunting for Impact Apr 26nd 12-1pm EST

Hands on hunting with Lee Archinal using real data and tools

"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 Apr 3rd 2023!