OOTW 11/28/2022

Monday, November 28, 2022 9:14 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 Nov 28th 2022!"

https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/

Emotet Strikes Again – LNK File Leads to Domain Wide Ransomware

Data Analysis of an Emotet Breach --- Key Findings

- Phishing LNK to download Emotet
- Outbound SMTP spam emails
- Tactical RMM (domain registered close to incident timeline)
- Cobalt Strike Enumeration
    - Net command & nltest
- Remote Service Creation (failed)
- Remote copy and execute via WMI
- Enumerate SMB Shares
- Additional Cobalt Strike Enumeration
    - Noisier
- ZeroLogon Exploit (failed)
- Remote Service Creation Domain Controller
- DC enumeration
    - Bat files
    - Adfind
- Rclone Exfil

- Rclone Exfil
  - FileServer
  - MailServer
- AnyDesk install
- NetScan
- Don't Sleep
- Ransomware Deployment

https://cybernews.com/editorial/opzero-exploit-hunter-kremlin/

OpZero's modus operandi: opportunity hunter, front for Kremlin, or both?

> ***OpZero, a Russian company, is a fairly new player in the market of zero-day exploits, but it raised some eyebrows with unusually high prices for certain vulnerabilities.***
>
> ***Seems to be more a broker than a researcher creator***
>
> ***Put up 1.5 million for Signal RCE exploit on Android phones specifically --- suspect to be able to break into Ukranian communications (both highly used) --- (might be stretch to just rely on that --- but insightful) as well as US government and CyberSecurity Professionals***
>
> ***Why the RCE --- Typically the best way to break encrypted phone communications is to be present on the end device***

https://thehackernews.com/2022/11/russia-based-ransomboggs-ransomware.html

Russia-based RansomBoggs Ransomware Targeted Several Ukrainian Organizations

Ukraine Ransomware attack called RansomBoggs

- Written in .NET
- Deployment similar to Sandworm (Russian GRU)

    - Relating more to Indeustroyer2 which was activity in April
    - Powershell Script
    - POWERGAP --- similar code structure and programmer preferences --- i.e. -foregroundcolor RED, same variable names

https://www.bleepingcomputer.com/news/security/vice-society-ransomware-claims-attack-on-cincinnati-state-college/

Vice Society ransomware claims attack on Cincinnati State college

Vice Society targets educational institutions --- weird target set ---- but possible that the victim selection is oppurtunistic because of budgets and staffing and/or value of research institutions where the data stolen may have follow on value

Vice Society picked a GTA themed site --- thus the name, really interested the skill / maturity of this group

Historically educational institutions were a great target to pivot from and hop through because of the internet speed and reliability.

https://www.yahoo.com/news/millions-twitter-users-hacked-colossal-130736003.html

Millions of Twitter users hacked in ‘colossal’ security breach

API attack that was able to expose phone numbers and emails for Twitters user base --- Around 5.4 million records --- Fixed in Jan 2022

This type of information disclosure isn't critical but note worthy

- This type of information is more and more widely availble
- This can't be used directly against you, but is used to expose personal weaknesses based on how connected people are to their technology
- This is where awareness training is valuable --- be smart with how you use tech --- personal protection strategies should be covered in business Cyber Awareness programs

"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 Nov 28th 2022!