OOTW 02/06/2023

Monday, February 6, 2023 10:28 AM

"Hey everyone, welcome to a another addition to the Out of the Woods Threat Hunting podcast. This is Scott Poley, here with Lee Archinal 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 Feb 6th 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://thedfirreport.com/2023/02/06/collect-exfiltrate-sleep-repeat/

Collect, Exfiltrate, Sleep, Repeat

Iranian

- Powershell for everything
  - Basic commands
  - Custom scripts
- Autohotkey keylogging
  - Saved key strokes in regkey
  - Readkey ps1 to access

- Word creating files

Take Aways:

- Look at Office programs creating non standard file types
- Great example of how PowerShell can be used in all Phases of an attack

https://www.trendmicro.com/en_us/research/23/b/new-apt34-malware-targets-the-middle-east.html

New APT34 Malware Targets The Middle East

Iranian malware used for stealing creds

Dropped:

1. %System%\psgfilter.dll: The password filter dynamic link library (DLL) used to provide a way to implement the password policy and change notification
2. %ProgramData%\WindowsSoftwareDevices\DevicesSrv.exe: The main .Net responsible for exfiltrating and leaking specific files dropped into the root path of this backdoor execution. This backdoor requires the .Net library implementing Microsoft Exchange webservices to authenticate with the victim mail server and exfiltrate through it.
3. %ProgramData%\WindowsSoftwareDevices\Microsoft.Exchange.WebServices.dll: The library to support the second component's capability.
4. %ProgramData%\WindowsSoftwareDevices\DevicesSrv.exe.config: An app configuration

4. %ProgramData%\WindowsSoftwareDevices\DevicesSrv.exe.config: An app configuration file for runtimes of the .Net execution environment. This allows the option of falling back to .Net 2.0.

   Modified Reg Key:

   HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa
   Notification Packages = scecli, psgfilter

   Type of behavior:
   - Emailed sent data collected for different passwords using proton mail

   Takeaways:
   - Look at/control outbound email to common email providers
   - Look for Reg Key mods for the password filter implementation
   - 2 different attacks discussed about Iran but very different attacks and techniques
   - Similar techniques here go back to Operation Clever over a decade ago --- some behaviors still persist
     - https://scadahacker.com/library/Documents/Cyber_Events/Cylance%20-%20Operation%20Cleaver%20Report.pdf

https://opalsec.substack.com/p/the-defenders-guide-to-onenote-maldocs

The Defender's Guide to OneNote MalDocs

Common social engineering technique is using OneNote to get clicks

- OneNote files are not affected by Protected View/Mark-of-the-web
- Can embed a number of files commonly used to attack with

Takeaway
- Look at ONENOTE.EXE launching mshta.exe
  - May need a few other interesting launching behaviors
- Some tools listed to help analyze these types of attacks
  1. One-Extract by Volexity
  2. OneNoteAnalyzer by knight0x07
  3. OneDump.py by Didier Stevens

https://www.reliaquest.com/i/blog/socgholish-fakeupdates/

SocGholish: A Tale of FakeUpdates

SocGholish attacks (fake updates) seen still being seen in the wild.

Interesting behaviors:
- Attack pulled Event ID 4776 DC validating creds to perform discovery actions
- Attacker enabled restricted admin mode to enable pash the hash for RDP
    - 'cmd /c reg add hklm\\System\\CurrentControlSet\\Control\\LSA /f /v disablerestrictedadmin /t REG_DWORD /d 0'

Takeaways:
- Protect data on you DC --- looing for someone pulling log data from the DC should be considered sensitive
    - Think of how many times you have put your password in the username field and then successfully logged in after once you realized your mistake
    - All of that is logged in plain text

https://analyst1.com/north-korea-intelligence-assessment-2022/

North Korea: Intelligence Assessment 2022

Breakdown of how North Korea Intelligence services and Cyber Ops work -- Very detailed and informative

Takeaways:
- **Good way to understand North Korea as a potential threat**
- **Lot of emphasis on making money**
    - **Shell companies to move supply chains through**
    - **Dedicated offices to stealing money**
    - **Dedicated offices to laundry the money**

Similar sources for Russia operations and structure:
https://www.valisluureamet.ee/doc/raport/2022-en.pdf

https://nsarchive.gwu.edu/sites/default/files/documents/4378262/Estonian-

https://nsarchive.gwu.edu/sites/default/files/documents/4378262/Estonian-Foreign-Intelligence-Service.pdf

Live Podcast Feb 16th - Cyber Sentinel (whiskey sour) --- interact with us on discord and or listen

"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 Feb 6th 2023!

Happy Hunting