OOTW 2/21/2023

Tuesday, February 21, 2023 12:00 PM

"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 Feb 21st 2023!"

https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-1/

Stealc: a copycat of Vidar and Raccoon infostealers gaining in popularity – Part 1

An infostealer named Stealc pushed out as a Malware as a Service by Plymouth on Russian speaking forums emerged. The stealer seems to target most things infostealers look for but based on the criteria seems to target mass individuals vs organizations. Obviously it could be used for both, but was distributed by hijacking youtuber's accoutns and posting content that leads to a fake free software downloads.

Some characteristics to look at is some cmdline behaviour:

- Timeout /t 5
- Del /f /q "<path>"
- .php

Some characteristics of network behviours:

- Direct IP address callouts
- Url's ending with .dll (pulls down up to 7 different dlls)

https://threatmon.io/apt-sidecopy-targeting-indian-government-entities/

APT SideCopy Targeting Indian Government Entities

Group targeting Indian Government using Macro enabled documents that deployed a very versatile RAT (Remote Access Trojan)

Some interesting characteristics:

- Macro doesn't execute until document closes to help avoid defenses and sandboxes
- Eventually creates a .exe in the \Start Menu\Programs\Startup for persistence

https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

Fog of war: how the Ukraine conflict transformed the cyber threat landscape

This was a nicely put together timeline analysis with cyber activity in Ukraine prior and during the war with Russia.

I find this article interesting because it's the first real world case on the scale of the conflict to show what type of cyber activity leads to war and maybe with enough understanding could lead to good model of detecting war like efforts.

Made me think of thinthread in the documentary A Good American, which does touch on conspiracy but very good info on metadata and communications.

https://www.sentinelone.com/labs/wip26-espionage-threat-actors-abuse-cloud-infrastructure-in-targeted-telco-attacks/

WIP26 Espionage | Threat Actors Abuse Cloud Infrastructure in Targeted Telco Attacks

This article coverd how WIP26 used Microsoft Graph API to perform C2. This is a very intelligent way to bypass human and machine level analysis because it communicates with known trusted infrastructure.

Some interesting characteristics:

- It does create a schedule task for persistence
- It uses files with 'Update' and 'Launch' in the name so look for non protected directories with executable extensions with the names containing those strings.
    - They use cloud infrastructure to blend in to evade machine/human detections alike
    - They use naming conventions to help evade human detections

https://asec.ahnlab.com/en/48063/

HWP Malware Using the Steganography Technique: RedEyes (ScarCruft)

RedEye group targets individuals to collect info from them with a RAT. The Rat is embedded in a jpeg looking file that then runs powershell, mshta from a run reg keyand injects into explorer.exe.

Some interesting cmdline things:

- Ping -n -w args (a delayed execution mechanic to wait for response to ip that won't respond)
- Mshta <website>

Some interesting parent process things

- Explorer kicking off exe that require cmdline interaction
    - i.e. whoami --- if there is no cmdline terminal no data is returned so from a graphical exe like explorer ---- doesn't make sense

Live podcast March 16th 7-830pm EST

Fun interactive discord discussions and indepth experience based topics

Lateral Movement March 22nd 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 21st 2023!