OOTW 5/08/2023

Monday, May 8, 2023 8:25 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 May 8th 2023!"

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/deconstructing-amadeys-latest-multi-stage-attack-and-malware-distribution/

Deconstructing Amadey's Latest Multi-Stage Attack and Malware Distribution

Legitimate Windows executable file wextract.exe, used for extracting files from cabinet (.cab) archives, is being exploited by malicious actors. Typically found in the System32 folder, this file can be vulnerable to misuse when replaced or modified by fake versions. Cybercriminals have employed such fake wextract.exe files for malware distribution, information theft, remote access, and ransomware delivery. McAfee Labs has analyzed malicious wextract.exe samples found in the wild, shedding light on the potential threats associated with this new form of cyberattack. Stay vigilant and ensure you protect your systems against such disguised malware.

A lot of extraction of exes to the temp directory

- Looking at the characteristics of the unpacking they are all 4 character names and written in the temp directory with in a short window of time
    - File creates >1 and name == 4 char in temp directory in 5 min

window
- Multiple registery values being set for the HKLM*Windows Defender settings
    - Reg contains HKLM*Windows Defender and value set events > 2 time window 5 mins
- Web downloaded exes
    - File creates >1 and name == 4-5 char in temp directory in 5 min window
- Schedule task being created from the temp directory
- Cacls.exe changing file permissions
    - Cacls.exe >5 min time window by host

https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/

Kimsuky Evolves Reconnaissance Capabilities in New Global Campaign

SentinelLabs has identified ongoing cyberattacks by Kimsuky, a North Korean state-sponsored APT group with a history of targeting organizations worldwide. These campaigns use a new malware component called ReconShark, which is delivered through spear-phishing emails, OneDrive links, and malicious macros. ReconShark acts as a reconnaissance tool with unique execution instructions and server communication methods, and its recent activity has been confidently attributed to North Korea. The group, active since at least 2012, is known for its intelligence collection and espionage operations, and has evolved its BabyShark malware to include an expanded reconnaissance capability in the form of ReconShark.

Hunts-
- User Agent contains 'curl'
- Browsers and outlook LNK modifications --- tougher but possible recent modify timestamps that differ from others
- New dotm file creations in "Microsoft\Templates"
- Cmd /c >4 in 5 min time windows by host

https://www.bleepingcomputer.com/news/security/alphv-gang-claims-ransomware-attack-on-constellation-software/

ALPHV gang claims ransomware attack on Constellation Software

Constellation Software, a Canadian diversified software company, has confirmed a breach in some of its systems by threat actors, resulting in the theft of personal information and business data. The incident was limited to a small number of systems related to internal financial reporting and data storage, with no impact on independent IT systems of Constellation's operating groups and businesses. The company has contained the attack and restored the affected IT infrastructure systems. The ALPHV ransomware gang, also known as BlackCat, has claimed responsibility for the attack and threatens to leak over 1 TB of stolen data if Constellation refuses to negotiate. The gang has already leaked some documents online as proof of the breach.

More a talking piece that I think about ---

- First we worry about supply chain attacks
- Ransomware groups get access to all sorts of various networks
- Russia has been behind some of the most known supply chain attacks
- Ransomware groups are "protected"/operate from russia in a numer of instances
- Ransomware groups goal is to make money
- Nation State sponsors cyber ops have lots of money

So wonder when Ransomware groups start to merge into access brokers for cash if they haven't already

https://securityaffairs.com/145892/cyber-crime/san-bernardino-county-sheriff-paid-ransom.html

San Bernardino County Sheriff's Department paid a $1.1M ransom

The San Bernardino County Sheriff's Department confirmed that it paid a $1.1-million ransom following a ransomware attack in April. The attack impacted various systems, including email, in-car computers, and some law enforcement databases, forcing the department to temporarily shut down some systems. The ransom was paid to restore system functionality and secure breached data. While law enforcement agencies typically recommend not paying ransoms, the department likely felt they had no other option to recover the encrypted systems or prevent sensitive data disclosure. The ransomware gang behind the attack is suspected to be from Eastern Europe and has previously targeted US entities. Cities, hospitals, and school districts are often targeted by cybercriminals due to their weak defenses and the sensitive data they hold.

Food for though:
Ransomware groups typically make money from data recovery and extortion --- and interestingly enough it is common for law enforcement to recommend not paying, but I feel the extortion piece can really force their hand because of the risk of their data going public from case work to protecting people in general --- so unique problem from some business/sector-verticals

https://www.reversinglabs.com/blog/secure-software-blogwatch-solarwinds

SolarWinds hack: Did DOJ know 6 months earlier?

An investigative reporter has found that the US Department of Justice (DOJ) knew about the SolarWinds breach six months earlier than initially reported. The DOJ detected unusual traffic from a server running SolarWinds' Orion software suite and reached out to the company for help. However, SolarWinds engineers couldn't identify a vulnerability in their code. The attack impacted at least nine US federal agencies and several tech and security firms. Although the DOJ informed the US Cybersecurity and Infrastructure Agency about the breach, the National Security Agency wasn't notified, causing frustration within the agency.

Food for though:
Communication is key especially when different groups, people, entities

offer different value/solutions to a problem

- If history has proven --- when there is a break down in sharing information amongst interested parties/vested parties --- real threats become major issues
- Makes me think of why we want to set up ISACs --- or other sharing groups --- but for most groups to function well I feel like it's hard for everyone to have an equal role in the process --- almost like you need a master group that determines who gets and sees what --- but it should be made up of members from the distributed groups

Live Podcast May 18th 7-8:30pm EST
outofthewoods@cyborgsecurity.com
Questions to be answered or topics to be discussed

TOP Cover 3 - Reporting and Communication May 24th 12-12:30

Threat Hunting Workshop - Exfil May 31st 12-1pm EST

"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 May 8th 2023!