OOTW 12/12/2022

Monday, December 12, 2022 11:16 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 Dec 12th 2022!"

https://www.bleepingcomputer.com/news/security/rackspace-warns-of-phishing-risks-following-ransomware-attack/

Rackspace warns of phishing risks following ransomware attack

Phishing emails seem to be hitting people that are customers of rackspace following the ransomware attack against rackspace's exchange environment.

From the complaints the phishing emails seem to be associated with RackSpace directly. There are a lot of assumptions being made by people with out data to support their claims --- one associated with "its obvious that customer data was stolen" --- I feel like that if your MX record was in the RackSpace IP address space --- that would suggest you as one of their customers --- so doesn't tie to that.

But from last weeks mention of ProxyNotShell vuln being present --- typical practice seen was for adversaries to pivot to company email access and dump. Something people should be considering because those line up better social engineering attempts / wire frauds.

https://www.deepinstinct.com/blog/new-muddywater-threat-old-kitten-new-tricks

New MuddyWater Threat: Old Kitten; New Tricks

Iranian actors installing remote administration software, Snycro --- free 21-day trial --- cloud file hosting and download of msi file contained in a zip.

These remote admin tools are being seen more and more by attackers because it gives easy to use access and can easily bypass EDR tools. It is important to know what is running in your environment and to identify these tools when they get installed. Might be a good approach to focus on ones that allow free trials because attackers seem to lean on those so there is no payment trail back to them.

https://thehackernews.com/2022/12/researchers-detail-new-attack-method-to.html

Researchers Detail New Attack Method to Bypass Popular Web Application Firewalls

Technique seen to circumvent web application firewalls (WAFS) --- involves appending JSON syntax to SQL injection Payloads

Because WAFS can't parse the data correctly --- it can't read and alert/block properly

This is always interesting based on how we as defenders and IT folk build things based on how things should work or be utilized --- Typically attacking protocols is really focused on the 'should' and 'may' requirements in the RFC. Those requirements often either confuse developers or get ignored and allow attackers to create novel attacks.

https://www.volexity.com/blog/2022/12/01/buyer-beware-fake-cryptocurrency-applications-serving-as-front-for-applejeus-malware/

฿uyer ฿eware: Fake Cryptocurrency Applications Serving as Front for AppleJeus Malware

North Korea's Lazarus Group seen using the AppkleJeus malware. This malware uses a Novel DLL side-loading technique called chained DLL Side-Loading

Typical DLL side-loading, EXE looks for:

- Path to DLL hardcoded in EXE
- DLL in the same directory as the EXE
- DLL in default System directory

In this case the malicious DLL was one loaded by the first legitimate DLL --- so DLL side-loading in later step.

https://thehackernews.com/2022/12/hack-for-hire-group-targets-travel-and.html

Hack-for-Hire Group Targets Travel and Financial Entities with New Janicab Malware Variant

The group Evilnum know for being "mercenary" hackers has been targeting companies to steal what seems to be business related data and intellectual property. They use Janicab backdoor.

Typical steps in the process:

- LNK dropper ---- content can be found in HUNTER
- Once file decrypted --- has a startup VBS script

"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 Dec 12th 2022!