OOTW 10-31-2022

Monday, October 31, 2022 9:07 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 October 31st 2022!"

https://www.bleepingcomputer.com/news/security/new-azov-data-wiper-tries-to-frame-researchers-and-bleepingcomputer/

New Azov data wiper tries to frame researchers and BleepingComputer

Cyberops + Psyops

Couple Data Points

Notice Theme: Ukrainian retaliating against Western Coutries for not doing enough in the war effort	Related to Russia Ukraine War
Wiper named "Azov" derived from the *Ukrainian Azov Regiment*	Past Ukrainian neo-Nazi association --- Russia War Propaganda Theme
Claimed to be BleepingComputer, MalwareHunterTeam, targetted Security Researchers	Media/information outlets commonly reporting on Russia's Cyber Activity in the war
Not real ransomware --- no way to recover data	Historically similar to that of NotPetya --- looked like ransomware, with no recovery

Supports Russian Agenda --- could it be psyops + cyberops

By affecting a wide number of unaffiliated targets with misinformation streams is at it's core misinformation/propaganda strategies
**More sources contributing to information greater than creditable sources

Interestingly enough --- Autorun keys were used for persistence --- even though system was being wiped

***Hunter covers this and more
Uses Registry Run keys **Autorun or ASEP Registry Key Modification**

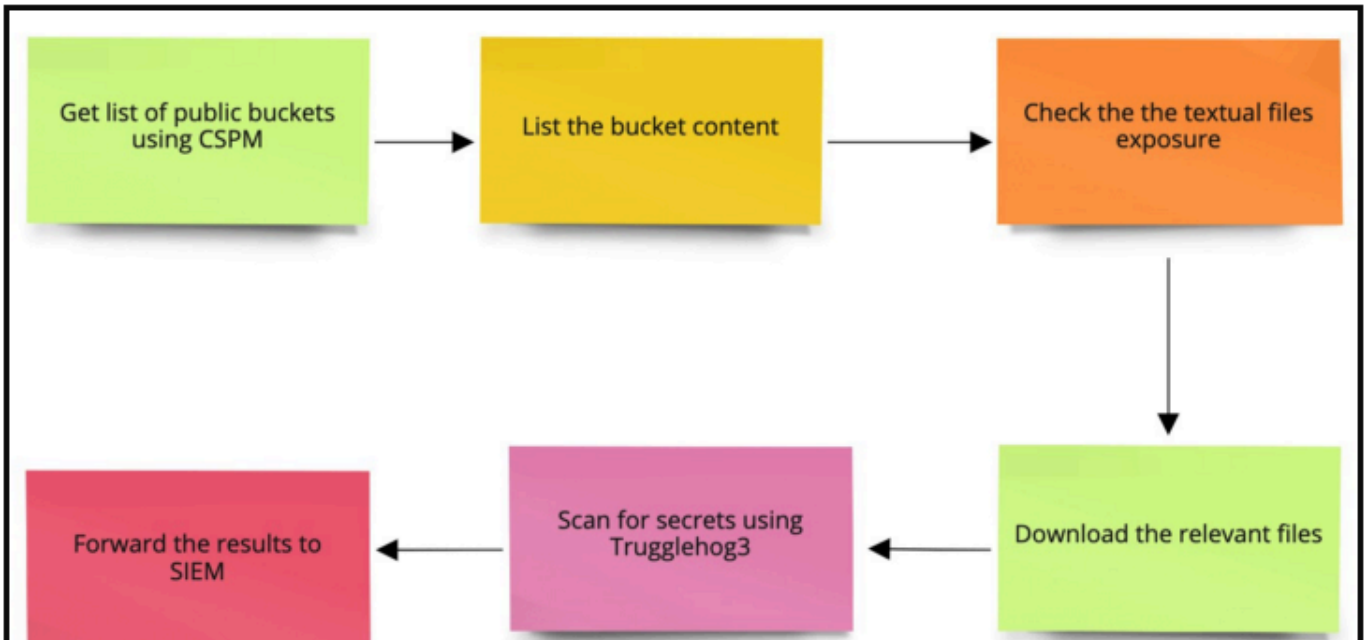
- 11 run key locations and 7 values to exclude

https://www.bleepingcomputer.com/news/security/new-open-source-tool-scans-public-aws-s3-buckets-for-secrets/

New open-source tool scans public AWS S3 buckets for secrets

Common cloud breaches are associated to misconfig and poor key management --- common for people in the past to crawl github for AWS keys because people would create a solution and leave the key in the code

Tying this into alerting was an interesting and logical way to monitor kind of your security posture for this sort of thing --- putting data and alerts into the SIEM



Actions performed by the S3crets Scanner

Highlights something people don't often turn attention to in cyber security --- that is recon -- typically they have public facing servers to the internet and the tax and value to respond/monitor for activity is not usually practical ---- but it's always good to identify information that you weren't planning on sharing and it does sound like a good response to take similar info gathering tools and run them periodically against yourself --- almost like a counter-intel hunting --- hunts that I frankly haven't been thinking about but might have it's own category worth investing time in

https://thehackernews.com/2022/10/twilio-reveals-another-breach-from-same.html

Twilio Reveals Another Breach from the Same Hackers Behind the August Hack

Twilio seeing activity similar to that of during a breach/incident August in June following year

Attack originated with Social Engineering for creds with some SMS trickery too

This makes me think of after actions --- from a hunting perspective --- I would want to put together activities seen in the initial breach and look for those across the network --- I also would want to flag the machines affected and scrutinize those a little more for some period of time --- especially if the compromise is credential related and machines weren't all rebuilt as a response

It was nice to see that they were adopting a more robust 2FA solution

https://thehackernews.com/2022/10/researchers-uncover-stealthy-techniques.html

Researchers Uncover Stealthy Techniques Used by Cranefly Espionage Hackers

New backdoor Danfuan written C# in combination with reGeorg webshell seen hitting targets

Seems to target network equipment, like Wireless Acess Points, and loadbalancers --- endpoints that are less likely to have endpoint protection or monitoring

There was an emphasis on targets set more closely related to corporate transactions --- maybe a precursor to gained third party affiliates and or customers for intended target access

18 month dwell time with no data exfil --- long game which lends more towards a different target in mind

https://www.infosecurity-magazine.com/news/ransomware-precursor-to-physical/

Ransomware is Being Used As a Precursor to Physical War: Ivanti

Ransomware is Being Used As a Precursor to Physical War: Ivanti

Interesting --- Not surprised by this --- I remember an exercises where special operatives were practicing with cyber operatives to see how well each team can work together --- RC drone extra eyes --- to killing lights in facility rooms before room breaches --- disabling alarms --- like the spy stuff in movies --- forgot the University that was hosting the exercise/range to test/experiment with this concept

This being said --- part of identifying threats is determining if you are a target compared to geopolitical positions --- and the scale of the attack say if a nation state vs cyber crime were to target you -- knowing that ranwomware/datawipers are capabilities of these nation states --- validate your criticality to infrastructure and strategically prepare for these types of engagements

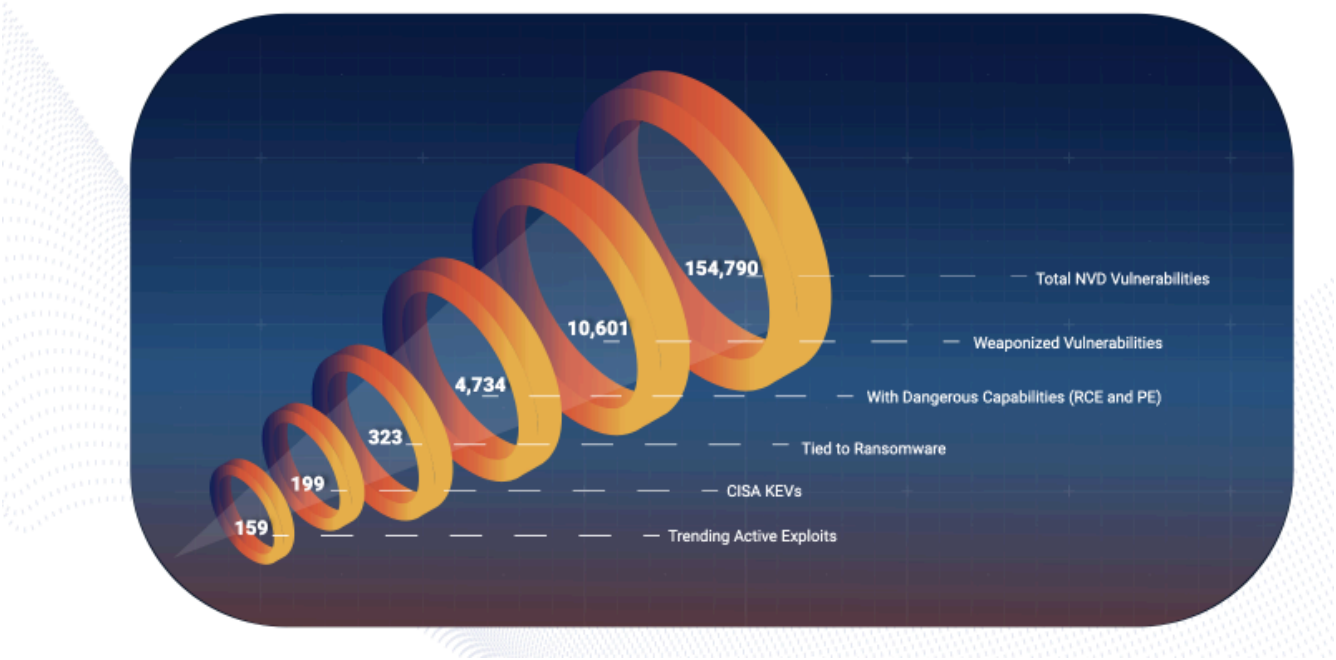
When the question of war comes up --- if you sit somewhere in the critical infrastructure space --- you become a target based on adjacency to higher priority targets

But I wish it was that cut and dry cause now as mentioned before psyops is a big part now --- so are there certain services or resources that if cut off or disrupted for the public --- can that affect public opinions and engagement in case of a longer term war

Great infographic on Ransomware ties to vulnerabilities --- take into account what vulnerabilities are being targeted --- system/software types and categories, vulnerability characteristics --- RCE, escalation, initial access --- and adjust criticality assignments to get those things patched sooner than later --- priority driven patch management

https://www.ivanti.com/resources/v/doc/pr-survey-report/ransomware-quarterly-indexreport_q2-q3

Ransomware vulnerabilities funnel



"Thanks Everyone for joining our Out of the Woods Threat Hunting Podcast. Looking forward to syncing back up next week.
With that, let's dive into the Top 5 Threat Hunting Headlines for the week of October 31st 2022!"

31st 2022.