# OOTW 11/21/2022

Monday, November 21, 2022 8:51 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 Nov 21th 2022!"

https://www.humanize.security/blog/news/144-cybersecurity-statistics-for-2022#thirth

**144 CYBERSECURITY STATISTICS FOR 2022**

Based on stats and data pulled and grouped from various sources

- Good to have data like this in your pocket when communicating importance of different capabilities, operational processes, program justification, and training initiatives

List

Statistics for C-Suite

Cybersecurity Insurance

Cybersecurity workforce

Human error statistics

Data Breach Statistics for 2022

DDoS statistics in 2022

DDoS statistics in 2022

Social engineering statistics in 2022

Phishing statistics in 2022

Zero Trust Statistics for 2022

Biggest Cyberattacks in 2022

Ransomware Statistics for 2022

Cybersecurity Predictions

Other

Few Stats of Interest:

- Insurance
  - Cyber insurance premiums increased by an average of 28% in the first quarter of 2022 compared with the fourth quarter of 2021
- Workforce
  - Cyber fatigue, or apathy to proactively defending against cyberattacks, affects as much as 42% of companies.
- Human Error
  - Only 53% of employees can correctly define phishing.
- Breaches
  - 192 days is the average number of days an organization takes to identify a breach.
- Ransomware
  - 14 US critical sectors have been subjected to intense ransomware attacks. (there are 16)
- Other
  - 54 % of companies say their IT departments are not sophisticated enough to handle advanced cyberattacks.

https://www.bleepingcomputer.com/news/security/us-charges-bec-suspects-with-targeting-federal-health-care-programs/

suspects with targeting federal health care programs/

## US charges BEC suspects with targeting federal health care programs

Business Email Compromise
Training I think is a big control for this
- Things that target changing current processes
- Asking for money in expedited timelines
- How to verify / Process for forms of verification

https://www.cisa.gov/uscert/ncas/alerts/aa22-320a

## Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester

What they did --
- used Log4Shell on vuln VMware Horizon
- Neutered Windows Defender with MpPreference -ExclusionPath
- Used PsExec, Mimikatz, Ngrok
- Where able to get DA creds to create a rogue DA account
- Used Powershell get-ad commands for discovery
- Changed local Admin accounts password as backup if lost DA

What was mentioned in mitigations -- which to me adds more context because based on actor behaviors
- Audit Kerberos (TGS) --- kerberoasting
- Ensure unique admin accounts for different tasks -- password reuse --- same local admin
- Ensure storage of clear text passwords in LSASS are disabled by default (in Registry)
- Separate user and admin accounts for different uses --- admin shouldn't be getting email and web browsing
- Disable inactive accounts

https://vulcanpost.com/809402/ftx-hacker-dumps-prices-of-eth-using-stolen-coins/

## FTX hacker dumps prices of ETH using stolen coins, revealing

## FTX hacker dumps prices of ETH using stolen coins, revealing another vulnerability of crypto

Cryptocurrency as a whole is all based on good faith and good math (decentralized) --- which everyone expresses how great there is no oversight --- but this shows that not everyone will act in good faith --- so thus rules and regulations become a thing

I attribute this behavior to ---- gosh if we didn't have people trying to perform cyber attacks then we wouldn't need security teams ----  things exist because of reasons and people should understand that

Since I don't play in the crypto currency realm --- if the market falls, might lead to reduce capabilities for some ransomware groups

https://thehackernews.com/2022/11/microsoft-warns-of-hackers-using-google.html

## Microsoft Warns of Hackers Using Google Ads to Distribute Royal Ransomware

Using SEO (Search Engine Optimization) to get users to download malware for free tools like TeamViwer, Visual Studios, Zoom --- leveraging Google's ads and search engine

Things that happened

- Free tool either installed BatLoader Or Atera Agent -> pre-conf scripts-> installs splahstop streamer ---
- Cmd to run powershell to disable and add exclusions for Defender
    - Add/Set-MpPreference
- Batloader
    - Use of mshta.exe --- used to run HTML Apps / Vbscript / Javascript
    - Targets AppResolver.dll
        - Embedded Vbscript
        - Polyglot --- PE+HTA

** interesting to look for mshta.exe executing on extensions other than .hta .vbs .js .txt

than .hta,vbs,js,txt
** allows for application whitelist bypass --- misdirected executions

"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 Nov 14th 2022!