ROBO6K

2600 South 1St Street Austin, Tx

7/10-14/2023

This week in Cyber Security

- Monday 7/10 Reports of a major phishing campaign targeted at Microsoft and Adobe. A new ransomware family has emerged called Big Head with at least two of its variants being documented.
- Tuesday 7/11 NATO has proposed adding Cyberspace to Article 5. This article states that an attack against a member is an attack against all members. Amazon Prime day is becoming a hug attack surface for threat actors. Razer data breach results in loss of data with a 100k demand for the data.
- Wednesday 7/12 July patch Tuesday breakdown includes fixes for 132 new flaws with 6 being actively used in the wild. Chinese threat actor tracked as Storm-0558 gained access to at least 25 US organizations through Microsoft cloud. Barracuda releases a spotlight on extortion email attacks. These are ones demanding small amounts that may otherwise go unnoticed.
- Thursday 7/13 CISA and the FBI release a joint advisory on the Chinese Cyberespionage campaign.
- Friday 7/14 Takes a look at AI and its potential use in disinformation. The DOD continues to push its CMMC for third party providers to government contractors. This will require MSPs to have certain requirements. This is like the requirement for the contractors to use the $500 hammer. This may cause fallout as the cost will go up exponentially and could push business out of the government contract space.

Closing Notes:

Remember that this is not everything and that the threat landscape is forever changing. It takes everyone working together to help our clients protect themselves and prevent an attack. Stay vigilant and for any questions or if you would like more news on the happenings in Cyber Security, please do not hesitate to contact me.

Caleb Leggett

cleggett@robo.net

Your ROBO Technician

Article links:

https://www.vadesecure.com/en/blog/m365-phishing-email-analysis-eevilcorp

https://www.trendmicro.com/en_us/research/23/g/tailing-big-head-ransomware-variants-tactics-and-impact.html

https://therecord.media/christian-marc-liflander-on-nato-cyber-defense

https://veriti.ai/blog/amazon-prime-day-a-buyers-guide-to-avoiding-phishing-campaigns/

https://www.hackread.com/razer-data-breach-database-backend-access-sold/

https://blog.barracuda.com/2023/07/12/threat-spotlight-extortion-attacks/

https://thecyberwire.com/newsletters/daily-briefing/12/131

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-193a

https://thecyberwire.com/newsletters/disinformation-briefing/5/28

https://www.cpomagazine.com/cyber-security/an-msps-perspective-on-the-defence-departments-cmmc-compliance-standards/