




2600 South 1st Street Austin, Tx


7/17-21/2023

This week in Cyber Security

- Monday: For most of the tech world, new technology can be a scary thing. Generative AI is no exception. Despite safeguards being put in place with software like ChatGPT, developers were able to create an even more open-source AI, calling it WormGPT. It can assist in creating extremely good spam/phishing as well as successful malware. Threat group TeamTNT appears to be making a comeback and expanding past the crypto mining tactics of the past. Anonymous Sudan targets PayPal in a brief DOS attack lasting 30 seconds as a demonstration of the ability to disrupt the UAE and USA markets.
- Tuesday: A possible privilege escalation within Google Cloud has been discovered enabling supply chain attacks. Security group Orca refers to the build as Bad.Bunny, which Google has since patched. Ben Yelin continues to push a privacy campaign in Massachusetts. If this is passed, it could open the door for further legislation around privacy nationwide. Jump Cloud releases a breach by a APT actor. It is suspected that they are state backed. Jump cloud also releases the July 2023 Incident Indicators of Compromise (IoCs).
- Wednesday: CISA warns about threats in Adobe, Microsoft and Citrix. After high-risk vulnerabilities were discovered on the three platforms, CISA puts out a warning as they can have major consequences if exploited. WhatsApp remote deactivation campaign is discovered. The campaign targets 2 billion users. A look back at the Log4J exploit. Although the exploit was corrected quickly, the



look back into ensuring backup resiliency is brought to light. As backups were pushed back into production, many of these were missing the patch to correct for the Log4J vulnerability.

- Thursday: Sophos analyzes the malvertising exploits. The threat actors are using SEO to move the malicious ads to the top of the search results which leads to a higher click and infection rate. Research has shown rapid remediation for the MoveIT vulnerability which is promising. Guidepost security releases the GRIT ransomware report.
 - Friday: A very sophisticated Malware going by BundleBot has been discovered. The software is being disguised as Google AI Chatbot and other utilities. A look back through the year as local governments are targeted for ransomware attacks. These attacks can be detrimental for small governments and have the potential to be life threatening as emergency services can become affected. Zyxel devices are becoming compromised and used for DDoS attacks leading to devastating results against targets.
- 



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://thehackernews.com/2023/07/wormgpt-new-ai-tool-allows.html>

<https://thehackernews.com/2023/07/teamtnts-cloud-credential-stealing.html>

https://www.techtarget.com/searchsecurity/news/366544710/Orca-Google-Cloud-design-flaw-enables-supply-chain-attacks?Offer=abt_pubpro_AI-Insider

https://mgaleg.maryland.gov/cmte_testimony/2021/ehe/1rcAOg9F9D6ANs7ee2-J86wNsEj62WQg8.pdf

<https://www.bleepingcomputer.com/news/security/jumpcloud-discloses-breach-by-state-backed-apt-hacking-group/>

<https://jumpcloud.com/support/july-2023-iocs>

<https://therecord.media/cisa-warnings-adobe-microsoft-citrix-vulnerabilities>

<https://arstechnica.com/security/2023/07/vulnerabilities-in-adobe-coldfusion-and-citrix-netscaler-are-under-active-exploitation/>

<https://www.forbes.com/sites/daveywinder/2023/07/18/all-whatsapp-users-warned-accounts-can-be-deactivated-by-anyone-with-1-email/?sh=6c8362fb20ae>

<https://news.sophos.com/en-us/2023/07/20/bad-ad-fad-leads-to-icedid-gozi-infections/>

<https://www.bitsight.com/blog/new-research-reveals-rapid-remediation-moveit-transfer-vulnerabilities>

<https://www.guidepointsecurity.com/resources/grit-ransomware-report-2023-2024>



<https://thehackernews.com/2023/07/sophisticated-bundlebot-malware.html>

<https://thehackernews.com/2023/07/local-governments-targeted-for.html>

<https://thehackernews.com/2023/07/ddos-botnets-hijacking-zyxel-devices-to.html>

