RED-N Managed Security
Weekly Update

Week ending December 17, 2022

*Headline **NEWS***

- Patch Tuesday - Windows 11 KB5021255 and KB5021234 cumulative updates released
- Patch Tuesday - Microsoft December 2022 Patch Tuesday fixes 2 zero-days, 49 flaws
- Microsoft December 2022 Patch Tuesday breakdown from SANS Institute
- Microsoft: December Windows Server updates break Hyper-V VM creation
- Microsoft fixes Windows Server issue causing freezes, restarts
- Microsoft fixes Windows taskbar bug causing Explorer, Office freezes
- Microsoft: Patch Tuesday KB5021233 causing hidparse blue screen on Windows 10 22H2
- VMware fixes critical ESXi and vRealize security flaws
- Critical Remote Code Execution Vulnerability in SPNEGO Extended Negotiation Security Mechanism
- Fortinet says SSL-VPN pre-auth RCE bug is exploited in attacks
- Hackers exploit critical Citrix ADC and Gateway zero day, patch now
- Samba Issues Security Updates to Patch Multiple High-Severity Vulnerabilities
- Uber suffers new data breach after attack on vendor, info leaked online
- Antivirus software can be hijacked to wipe data
- Apple fixes 'actively exploited' zero-day security vulnerability affecting most iPhones
- CISA Alert: Veeam Backup and Replication Vulnerabilities Being Exploited in Attacks – this was patched in March

Other News Events of Note

- Microsoft Alerts Cryptocurrency Industry of Targeted Cyber Attacks
- Log4J anniversary: A year on, a third of downloads are still vulnerable
- Turns out coffee also makes semiconductors work faster too
- TN blocks TikTok access on government networks, cites cybersecurity as primary concern
- You Can Now Protect Your Apple Account With Hardware Keys
- The mass extinction of UNIX workstations
- Xnspy stalkerware spied on thousands of iPhones and Android devices
- New Python malware backdoors VMware ESXi servers for remote access
- Effective, fast, and unrecoverable: Wiper malware is popping up everywhere
- China bans AI-generated media without watermarks
- FTX founder Sam Bankman-Fried arrested, set to be extradited to US
- Btrfs With Linux 6.2 Bringing Performance Improvements, Better RAID 5/6 Reliability
- ChatGPT and Our MSP – fascinating use for new tech
- Researchers smell a cryptomining Chaos RAT targeting Linux systems
- Pwn2Own Toronto: 54 hacks, 63 new bugs, $1 million in bounties
- Driving Through Defenses | Targeted Attacks Leverage Signed Malicious Microsoft Drivers
- Signed driver malware moves up the software trust chain – Sophos News
- I Solemnly Swear My Driver Is Up to No Good: Hunting for Attestation Signed Malware
- Precious Gemstones: The New Generation of Kerberos Attacks
- Rackspace ransomware attack highlights security comms' challenges
- LockBit claims attack on California's Department of Finance
- New GoTrim botnet brute forces WordPress site admin accounts
- The Albanian government IT workers arrested for not updating software
- FBI seized domains linked to 48 DDoS-for-hire service platforms
- Open-source repositories flooded by 144,000 phishing packages
- Attackers use SVG files to smuggle QBot malware onto Windows systems
- Hacker claims breach of FBI's critical-infrastructure portal
- NIST Retires SHA-1 Cryptographic Algorithm
- Microsoft discovers Windows/Linux botnet used in DDoS attacks
- Parsing LastPass' data breach notice
- GitHub to require all users to enable 2FA by the end of 2023
- Gemini Hit With Phishing Attack, 5.7M Customer Emails Leaked
- HR platform Sequoia says hackers accessed customer SSNs and COVID-19 data
- Minecraft: Newest choice for malware attacks among malactors that target gamers
- Scientists create living smartwatch powered by slime mold
- Microsoft updates Quick Assist on older Windows versions, promises to continue supporting it
- Number of command-and-control servers spiked in 2022
- Is nothing sacred? LEGO BrickLink bugs let hackers hijack accounts, breach servers