RED-N Managed Security

Weekly Update

Week ending January 21, 2023

*Headline **NEWS***

- Researchers to release PoC exploit for critical Zoho RCE bug, patch now
- New Boldmove Linux malware used to backdoor Fortinet devices
- Norton LifeLock says thousands of customer accounts breached
- Unbelievably, there are still over 4,000 Sophos Firewall devices vulnerable to RCE attacks
- Hackers turn to Google search ads to push info-stealing malware
- 'Violated': NFT God Loses 'Life-Changing' Sum of Crypto After Clicking on Malware Link
- Git Users Urged to Update Software to Prevent Remote Code Execution Attacks
- Critical Security Vulnerabilities Discovered in Netcomm and TP-Link Routers
- Biden's new cybersecurity policy allows U.S. to preemptively hack criminals and foreign governments
- T-Mobile investigating data breach affecting 37 million accounts

Ransomware and Malware News

- Ransomware has now become a problem for everyone, and not just tech
- ChatGPT is enabling script kiddies to write functional malware
- Russian hackers are using ChatGPT to write malicious pieces of code
- Avast releases free BianLian ransomware decryptor
- Raccoon and Vidar Stealers Spreading via Massive Network of Fake Cracked Software
- Vice Society ransomware leaks University of Duisburg-Essen's data
- DNV Confirms Ransomware Attack Impacting 1,000 Ships
- Nissan North America data breach caused by vendor-exposed database
- Researchers Uncover 3 PyPI Packages Spreading Malware to Developer Systems
- Heads up! Xdr33, A Variant Of CIA's HIVE Attack Kit Emerges
- Derby, Kansas hit by computer network issues, billing impacted
- Mailchimp says it was hacked — again
- TurboTax, QuickBooks owner slammed for MailChimp data breach
- ChatGPT Creates Polymorphic Malware
- GCC hit hard with ransomware attacks, with Saudi and UAE organizations most affected
- Russian hacktivists NoName057 offer cash for DDoS attacks
- Ransomware Operators Continue to Aggressively Target US Healthcare Sector
- CISA Releases Four Industrial Control Systems Advisories
- Hacker group incorporates DNS hijacking into its malicious website campaign
- Social Security Numbers Stolen in PayPal Cyberattack
- Ransomware Payments 'Significantly Down' in 2022: Chainalysis
- New Microsoft Azure Vulnerability Uncovered — EmojiDeploy for RCE Attacks
- Adversaries' shift toward Shell Link (LNK) files - Following the LNK metadata trail
- Yum Brands says nearly 300 restaurants in UK impacted due to cyber attack
- The Evolution of Account Takeover Attacks: Initial Access Brokers for IoT
- Hackers now use Microsoft OneNote attachments to spread malware

Other News Events of Note

- Small business owners warned not to rely on Gen Z to handle cyber security
- Hacker group discloses ability to encrypt an RTU device using ransomware, industry reacts
- PoC exploits released for critical bugs in popular WordPress plugins
- ManageEngine CVE-2022-47966 IOCs to check if you use this product
- The big risk in the most-popular, and aging, big tech email programs

- Amazon's New Home Internet Service Is One Step Closer to Becoming a Reality
- Russia's largest hacking conference reflects isolated cyber ecosystem
- Meet Elizebeth Smith Friedman, The 'Mother Of Cryptology'
- Canada's largest alcohol retailer's site hacked to steal credit cards
- From phishing scams to propaganda: How Russia, rogue nations utilize cyber capabilities against the US
- Basecamp details 'obscene' $3.2 million bill that caused it to quit the cloud
- Cloudflare DDoS Report Finds Increase in Attack Volume and Duration
- MSI accidentally breaks Secure Boot for hundreds of motherboards
- Access to Nvidia's GeForce Experience, GeForce Now Blocked Due to Glitch
- Reviewer buys 16TB portable SSD for $70, proves it's a sham
- Hacktivists Leak 1.7TB of Cellebrite, 103GB of MSAB Data
- Google plans AirTag clone, will track devices with 3 billion Android phones
- Tape Storage Soars While HDD Sales Crash
- FCC Chair: 5G Expansion Creates 'Broader Attack Surface' for Cyberattacks
- Microsoft .NET 7 Brings Networking Improvements
- From Mozilla, Here's what's going on in the world of extensions
- IT Burnout may be Putting Your Organization at Risk
- AMD patches botched firmware that disabled cores on Ryzen 5 7600X
- Texas A&M University will block TikTok on its network and devices
- IBM: Quantum computing poses an 'existential threat' to data encryption
- FBI chief says he's 'deeply concerned' by China's AI program
- Authorities dismantle crypto exchange Bitzlato, allege it was cybercrime "haven"
- Sophos to lay off 450 employees globally
- China aims to grow local infosec industry by 30 percent a year, to $22 billion by 2025
- Microsoft investigates bug behind unresponsive Windows Start Menu
- Microsoft: Windows 11 apps might not start after system restore
- CISA 2022 Year in Review highlights effort, reduce risk to cyber, physical infrastructure
- CISA Reflects on Past Year, Upcoming Critical Infrastructure Security Priorities
- New tool: Introducing RPC Investigator
- Congress Gets Detailed Cybersecurity Advice From AAFP
- FTC Plan to Ban Noncompete Clauses Shifts Companies' Focus
- If your DNS queries LoOk liKE tHIs, it's not a ransom note, it's a security improvement
- Windows 10 KB5019275 preview update released with 14 fixes
- Veeam Research Finds IT Leaders Feel Increasingly Unprotected from Cyberattacks and Other Disasters
- Six years later, HPE and Oracle quietly shut door on Solaris lawsuit
- LastPass users should move their crypto funds, experts warn
- Over 19,000 end-of-life Cisco routers exposed to RCE attacks
- GAO reports difficulties in creating unified national cybersecurity strategy, performing oversight
- Hacker Gets Access To The FBI's No Fly List
- Pet fish commits credit card fraud on owner using a Nintendo Switch

Cyber Insurance News

- Skeptical Analysis of a Potential Federal Cyber Insurance Backstop
- At-Bay Launches New Admitted Cyber Insurance Product for Small Businesses
- Does Your Cyber Insurance Policy Cover a Ransomware Attack?