RED-N Managed Security

Weekly Update

Week ending February 3, 2023

Headline ***NEWS***

- QNAP fixes critical bug letting hackers inject malicious code
- Microsoft releases emergency updates to fix XPS display issues
- Samsung Issues Fix for Dying 980 Pro SSDs
- Exploit released for critical VMware vRealize RCE vulnerability
- Researcher drops Lexmark RCE zero-day rather than sell vuln ‘for peanuts’
- High impact vulnerabilities fixed in latest Firefox release
- Cybercrime is world’s third-largest economy thanks to booming black market
- Microsoft OneNote, Evernote Phishing Attacks Are Threat To MSPs
- New High-Severity Vulnerabilities Discovered in Cisco IOx and F5 BIG-IP Products
- CISA Alert: Oracle E-Business Suite and SugarCRM Vulnerabilities Under Attack
- Atlassian's Jira Software Found Vulnerable to Critical Authentication Vulnerability
- GoAnywhere MFT Users Warned of Zero-Day Exploit
- High-Severity Privilege Escalation Vulnerability Patched in VMware Workstation

Ransomware, Malware, and Vulnerabilities News

- New DDoS-as-a-Service platform used in recent attacks on hospitals
- City of London on High Alert After Ransomware Attack
- US, Middle Eastern allies include cyber collaboration in Abraham Accords
- Discrepancies Discovered in Vulnerability Severity Ratings
- Mon Dieu! Suspected French ShinyHunters gang member in the dock
- Hacker finds bug that allowed anyone to bypass Facebook 2FA
- GitHub says hackers cloned code-signing certificates in breached repository
- Realtek Vulnerability Under Attack: Over 134 Million Attempts to Hack IoT Devices
- 8x8 Incident/Compromise?
- Anker finally comes clean about its Eufy security cameras
- Microsoft disables verified partner accounts used for OAuth phishing
- Microsoft: Over 100 threat actors deploy ransomware in attacks
- Russian-backed hackers actively targeting US health care sector, HHS warns
- Atlantic General Hospital, MD experiences ransomware event
- Small Business Cyberattack Analysis: Most-Targeted SMBs
- Southern Arizona’s largest school district hit by cyber attack
- Central Okanagan School District, Canada: Everybody at risk of cyber attacks
- Firms fear software stack breach as attack surface widens
- Circle K US spills partial credit card details, among other sensitive data
- PoS malware can block contactless payments to steal credit cards
- Firmware Flaws Could Spell 'Lights Out' for Servers
- New Nevada Ransomware targets Windows and VMware ESXi systems
- Options trading desks 'flying blind' after derivatives platform hit by ransomware attack
- ‘Backdoor’ to Attack Satellites: CSO Sees Cyber Risks in Space Force Ground Systems
- LockBit has released a new variant: LockBit Green
- Researchers Uncover New Bugs in Popular ImageMagick Image Processing Utility
- Additional Supply Chain Vulnerabilities Uncovered in AMI MegaRAC BMC Software
- Cyber Insights 2023: Criminal Gangs
- OneNote documents spread malware in several countries
- No Macro? No Worries. VSTO Being Weaponized by Threat Actors

- North Korean hackers stole research data in two-month-long breach
- Cisco fixes bug allowing backdoor persistence between reboots
- MalVirt .NET Virtualization Thrives in Malvertising Attacks
- Google sponsored ads malvertising targets password manager
- ‘0ktapus’ hackers are back and targeting tech and gaming companies, says leaked report
- Rising ‘Firebrick Ostrich’ BEC Group Launches Industrial-Scale Cyberattacks
- Iranian OilRig Hackers Using New Backdoor to Exfiltrate Data from Govt. Organizations
- Threat Actors Use ClickFunnels to Bypass Security Services
- The Dangerous Consequences of Threat Actors Abusing Microsoft’s “Verified Publisher” Status
- Ransomware targeting VMware ESXi
- Steps to Surviving a Ransomware Attack
- Florida hospital takes IT systems offline after cyberattack
- Serious security hole plugged in infosec tool binwalk
- CVE-2023-25136: Pre-Auth Double Free Vulnerability in OpenSSH Server 9.1
- Feds say cyberattack caused suicide helpline's outage
- JD Sports warns data of 10mn customers put at risk in cyber attack

Other News Events of Note and Interest

- Datto’s Rob Rae Jumps To Pax8: ‘Their Passion For MSP Growth Is Second To None’
- Until further notice, think twice before using Google to download software
- Microsoft Unveils VALL-E, A Game-Changing TTS Language Model
- Inside the grim world of office spyware
- Microsoft Security Best Practice: Clean Up Active Directory Accounts with PowerShell
- Panama’s Supreme Court to rule on cryptocurrency legislation
- Windows Package Manager is so good I won't use anything else now
- WAN router IP address change blamed for global Microsoft 365 outage
- Facebook drains users' cellphone batteries intentionally says ex-employee
- Students and professors protest TikTok bans at state schools
- What can you do if your Facebook or Instagram account gets hacked?
- ChatGPT just got an update that makes its responses more accurate
- Microsoft Defender can now isolate compromised Linux endpoints
- Internet Archive Adds Calculator Emulators
- Backblaze Drive Stats for 2022
- Microsoft's DirectStorage tech signals the sunset of SATA SSDs
- ‘Cryptoqueen’ Wanted by FBI for Role in $4,000,000,000 Pyramid Scheme Sells Luxury Apartment in UK
- Microsoft rolls out ChatGPT-powered Teams Premium
- Microsoft 365 trial offer blocks access to Windows 10 desktops
- TikTok opens transparency center as lawmakers weigh US ban
- LibreOffice, the Free Office Suite, Has a Fresh New Look
- Introducing ChatGPT Plus – a paid service
- De-Bloated Windows 11 Build Runs on 2GB of RAM

Cyber Insurance News

- Cyber Insights 2023 – massive changes coming
- The corporate world is losing its grip on cyber risk