RED-N Managed Security

Weekly Update

Week ending February 18, 2023

Headline ***NEWS***

- February Patch Tuesday Updates Fix 75 Windows Vulnerabilities
- Microsoft Patch Tuesday, February 2023 Edition
- Apple fixes new WebKit zero-day exploited to hack iPhones, Macs
- Apple fixes zero-day spyware implant bug – patch now!
- Apple releases macOS Ventura 13.2.1 with bug fixes
- CISA warns of Windows and iOS bugs exploited as zero-days
- VMware, Windows 11 shafted by Windows Server 2022
- Palo Alto - CVE-2023-0001 Cortex XDR Agent: Cleartext Exposure of Agent Admin Password
- Citrix Patches High-Severity Vulnerabilities in Windows, Linux Apps
- Critical Vulnerability Patched in Cisco Security Products
- Fortinet fixes critical RCE flaws in FortiNAC and FortiWeb
- Adsense abused: 11,000 sites hacked in a backdoor attack
- Git security vulnerabilities announced
- February 2023 Patchday: EWS problems after Exchange Server security update

Ransomware, Malware, and Vulnerabilities News

- Social security numbers exposed in N.J. school district data breach
- Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities
- DPRK hackers steal at least $630m in cryptocurrency during the year
- LocalPotato vulnerabilities - When Swapping The Context Leads You To SYSTEM
- Pepsi Bottling Ventures suffers data breach after malware attack
- Technion University hacked and locked; previously unknown attackers demand 80 BTC
- Top background check services hit by data breach
- Four misconceptions about data exfiltration
- With local schools increasingly under cyberattack, a new resource can help bolster defenses
- Cloudflare blocks record-breaking 71 million RPS DDoS attack
- Honeypot-Factory: The Use of Deception in ICS/OT Environments
- 451 PyPI packages install Chrome extensions to steal crypto
- Chinese phones from OnePlus, Xiaomi, and Oppo are laced with spyware
- Employee of Pa.-based health insurer gets phished, resulting in data breach
- Plan now to avoid a communications failure after a cyberattack
- Spain, U.S. dismantle phishing gang that stole $5 million in a year
- Serious Security: GnuTLS follows OpenSSL, fixes timing attack bug
- Pig Butchering Scams Are Evolving Fast
- Fool's Gold: dissecting a fake gold market pig-butchering scam
- Healthcare giant CHS reports first data breach in GoAnywhere hacks
- Kaspersky's 2022 spam and phishing report
- Beepin' Out of the Sandbox: Analyzing a New, Extremely Evasive Malware
- Embattled VMware ESXi Hypervisor Flaw Exploitable in Myriad Ways
- How to Disable/Enable the SLP service on VMware ESXi
- EU countries told to step up defence against state hackers
- Ransomware attacks surge against US manufacturing plants
- Airline SAS network hit by hackers, says app was compromised
- RedEyes hackers use new malware to steal data from Windows, phones
- OT Network Security Myths Busted in a Pair of Hacks

- Researchers Uncover 700+ Malicious Open Source Packages
- Threat actors are using fake Emsisoft code-signing certificates to disguise their attacks
- 13 Years Later, the Bad Bugs of DNS Linger on
- Attacks on industrial infrastructure on the rise, defenses struggle to keep up
- Boulder County recovers money accidentally sent to hackers
- Hackers hit US Windows systems with "Mortal Kombat" ransomware
- LockBit spree hits three large companies
- Havoc Command and Control Across the Cyberspace
- ESXiArgs ransomware fights off Team America's data recovery script
- The return of ICEFALL: Two critical bugs revealed in Schneider Electric tech
- Hyundai and Kia issue software upgrades to thwart killer TikTok car theft hack
- Phishing as a Service threat research
- After apparent hack, data from Australian tech giant Atlassian dumped online
- Hackers backdoor Microsoft IIS servers with new Frebniis malware
- ProxyShellMiner Campaign Creating Dangerous Backdoors
- Ransomware attackers finding new ways to weaponize old vulnerabilities
- Experts Warn of Surge in Multipurpose Malware
- Burton Snowboards cancels online orders after 'cyber incident'
- Medusa Claims PetroChina Ransomware Attack
- Russian hacker convicted of $90 million hack-to-trade charges
- Des Moines Public Schools says data exposed in ransomware attack
- GoDaddy: Hackers stole source code, installed malware in multi-year breach
- Hacker Uncovers How to Turn Traffic Lights Green With Flipper Zero
- FBI is investigating a cybersecurity incident on its network
- Malware delivery through Microsoft OneNote files is growing in a post-macro world
- Vulnerabilities open Korenix JetWave industrial networking devices to attack
- How Attackers Bypass Two-factor Authentication (2FA)
- New WhiskerSpy malware delivered via trojanized codec installer
- City of Oakland declares state of emergency after ransomware attack
- Researchers unearth Windows backdoor that’s unusually stealthy

Other News Events of Note and Interest

- Windows 11 22H2 driver updates are failing left and right with 0x80070103 error
- IPv6 is coming to Azure AD
- Bad Firmware Update Bricks Over 30k T-Mobile Home Internet Modems
- Microsoft is making DCOM hardening mandatory on Windows 10, 11, and Server soon
- MFA number matching is coming is coming to Microsoft logins on February 27, 2023
- Microsoft WinGet package manager failing from expired SSL certificate
- Zoom, Slack Holdouts Make Office Life Miserable for Others
- Farewell to Subversion: GitHub Sunsets Support After 13 Years
- The best printers in 2023 | Tom's Guide
- Opera is adding ChatGPT to its sidebar
- Crypto Firm Paxos Faces SEC Lawsuit Over Binance USD Token
- SEC Chief Gensler Warns Crypto Firms to Comply With Rules After Kraken Shutters US Staking Program
- Windows 11 "System requirements not met" watermark apparently begins haunting 22H2 users now
- Performing File-Level Backups from the Command Line

- Samsung 990 Pro SSD firmware update should halt—but not reverse—rapid wear-out
- Mandiant: 79 Percent Of Cybersecurity Decisions Ignore Threat Intelligence
- X.Org Drivers Updated For Old Trident & S3 Graphics
- Eurostar forces 'password resets' — then fails and locks users out
- Report Reveals How US Has 'Not Advanced the Ball' on Top Cyber Risks
- What to expect from the upcoming national cyber strategy
- Cybersecurity High-Risk Series: Challenges in Protecting Privacy and Sensitive Data
- 2022 ICS/OT Cybersecurity Year in Review Is Now Available
- Microsoft: Some WSUS servers might not offer Windows 11 22H2 updates
- Here's another good reason to keep your GeForce Experience software up to date
- NIST's New Crypto Standard a Step Forward in IoT Security
- You.com challenges Google, Microsoft with launch of 'multimodal conversational AI' in search
- Latest WinGet 1.5 preview from Microsoft brings PowerShell module improvements, and more
- Microsoft's Bing AI Is Leaking Maniac Alternate Personalities Named "Venom" and "Fury"
- AMD drivers are bricking Windows 11 systems...again
- New and Improved Message Recall Feature for Exchange Online
- Twitter Limits SMS-Based 2-Factor Authentication to Blue Subscribers Only
- Researchers Hijack Popular NPM Package with Millions of Downloads

Cyber Insurance News

- Ransomware attacks creating repercussions for the insurance industry
- CFC introduces policy encryption for cyber insurance
- Brit Renews and Expands Flagship Cyber Consortium
- Cloud outage risk primed for parametric cyber ILS risk transfer
- CloudCover announces the strategic partnership with Hylant Global Captive Solutions