RED-N Managed Security

Weekly Update

Week ending February 24, 2023

Headline ***NEWS***

- VMware warns admins of critical Carbon Black App Control flaw
- Hackers now exploit critical Fortinet bug to backdoor servers
- Researcher publishes Ava Labs Avalanche zero-day vulnerability, says 'entire protocol compromised'
- Windows Server 2022 Feb. 2023 Patchday: Secure Boot issues also on bare metal systems!
- Windows Server 2022: VMware ESXi 7.0 U3k Patch for Secure Boot Issue (Update KB5022842, Feb. 2023)
- Sensitive US military emails spill online
- Inbound Connector Restricted Imposed by Exchange Online
- Microsoft urges Exchange admins to remove some antivirus exclusions
- Dish Network suffers multi-day customer service and website outage

Ransomware, Malware, and Vulnerabilities News

- Royal Ransomware Expands Attacks by Targeting Linux ESXi Servers
- Ransomware Gang Conti Has Re-Surfaced and Now Operates as Three Groups
- News Corp says state hackers were on its network for two years
- New WhiskerSpy malware delivered via trojanized codec installer
- Indigo admits cyber attack was ransomware, employee data accessed
- 87% of Container Images in Production Have Critical or High-Severity Vulnerabilities
- CISA Adds Three New Vulnerabilities in KEV Catalog
- City of Oakland declares state of emergency after ransomware attack
- Researchers unearth Windows backdoor that’s unusually stealthy
- Semiconductor industry giant says ransomware attack on supplier will cost it $250 million
- IBM Report: Ransomware Persisted Despite Improved Detection in 2022
- Coinbase cyber-attack
- A world of hurt for Fortinet and Zoho after users fail to install patches
- Hackers obtain personal data from 200K+ in southern Nevada casino data breach
- Hydrochasma: New Threat Actor Targets Shipping Companies and Medical Labs in Asia
- Indian Ticketing Platform RailYatri Hacked - 31 Million Impacted
- Samsung Introduces New Feature to Protect Users from Zero-Click Malware Attacks
- Sobeys admits to data breach in November 2022
- How to Detect New Threats via Suspicious Activities
- Highmark notifies members of data breach related to malicious email phishing campaign
- Activision Data Breach Contains Employee Details, Call of Duty's Future, and More
- Aker Solutions Provides Update on Cyber Attack
- More vulnerabilities in industrial systems raise fresh concerns about critical infrastructure hacks
- Microsoft grows automated assault disruption to cover BEC, ransomware campaigns
- 'Stealc' information-stealing malware emerges from the dark web
- DNA testing biz vows to improve infosec after criminals break into database it forgot it had
- Hackers Scored Corporate Giants' Logins for Asian Data Centers
- BD finds hacking risk in infusion pump software
- Fortinet FortiNAC CVE-2022-39952 Deep-Dive and IOCs
- Multilingual skimmer fingerprints 'secret shoppers' via Cloudflare endpoint API
- Hackers Exploit Privilege Escalation Flaw on Windows Backup Service
- MyloBot Botnet Spreading Rapidly Worldwide: Infecting Over 50,000 Devices Daily
- Chip company loses $250m after ransomware hits supply chain

- Bookstore chain Indigo partially restores website after cyber incident
- A New Kind of Bug Spells Trouble for iOS and macOS Security
- LockBit gang takes credit for attack on water utility in Portugal
- Lehigh Valley Health Network says it was target of cyberattack by ransomware gang with ties to Russia
- An Overview of the Global Impact of Ransomware Attacks
- A Deep Dive into the Evolution of Ransomware Part 1
- Attackers Flood NPM Repository with Over 15,000 Spam Packages Containing Phishing Links
- S1deload Stealer – Exploring the Economics of Social Network Account Hijacking
- GoAnywhere zero-day opened door to Clop ransomware
- ‘Nevada Group’ hackers target thousands of computer networks
- Threat Actors Adopt Havoc Framework for Post-Exploitation in Targeted Attacks
- Various Threat Actors Targeting ManageEngine Exploit CVE-2022-47966
- Researchers Create an AI Cyber Defender That Reacts to Attackers
- Key Findings from the 2H 2022 FortiGuard Labs Threat Report

Other News Events of Note and Interest

- NIST plots biggest ever reform of Cybersecurity Framework
- Signal CEO: We “1,000% won’t participate” in UK law to weaken encryption
- 10 dark web monitoring tools
- Google paid $12 million in bug bounties to security researchers
- Intel Paid Out Over $4.1 Million via Bug Bounty Program Since 2017
- NSA shares guidance on how to secure your home network
- Sneaky legit way to score free virtual tech support
- Crypto investors under attack by two new malware, reveals Cisco Talos
- Supreme Court to Hear Section 230 Cases: Here's What to Know
- Munich Security Attendees Microsoft, Google, Apple, Amazon, Microsoft, Meta
- Microsoft admits cloud cash grab is over as it pushes more cost-effective Azure VMs
- Microsoft brings Split Screen to all Edge users in the Stable channel
- Norway Seizes $5.84 Million in Cryptocurrency Stolen by Lazarus Hackers
- Microsoft pushes February 2023 firmware update to Surface Duo and Duo 2
- Outlook spam filters aren't working for many; maybe disable alerts
- Why privileged access management should be critical to your security strategy
- Instead of SMS 2FA, Use Your iPhone's Built-In Two-Factor Authentication
- Oracle is targeting users on Java compliance after new licensing terms
- Veeam bundles backup products into Veeam Data Platform
- Windows 11 debloater app renamed again, gets new setup page, mods marketplace, and more
- Microsoft is now injecting full-size ads on Chrome website to make you stay on Edge
- WD SN850X NVMe SSD that beat Samsung, Seagate, and Hynix is BSODing and freezing Windows 11
- Chrome 110 will automatically discard background tabs. Here’s how to stop it
- CVSS system criticized for failure to address real-world impact
- Cyberthreats, Regulations Mount for Financial Industry

Cyber Insurance News

- HardBit ransomware wants insurance details to set the perfect price
- Seven reasons to avoid investing in cyber insurance
- Coalition cyber protection now available to large enterprise businesses in US