RED-N Managed Security

Weekly Update

Week ending February 11, 2023

*Headline **NEWS***

- High-Severity Privilege Escalation Vulnerability Patched in VMware Workstation
- CVE-2023-25136: Pre-Auth Double Free Vulnerability in OpenSSH Server 9.1
- Qakbot mechanizes distribution of malicious OneNote notebooks
- CISA releases recovery script for ESXiArgs ransomware victims
- Google released Chrome 110, which Patches 15 Vulnerabilities, no longer runs on Win 7 or 2008
- The forecast from Davos: a catastrophic cyber event
- Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day

Ransomware, Malware, and Vulnerabilities News

- Florida state court system, US, EU universities hit by ransomware outbreak
- N.J. hospital admits patient data was stolen in cyberattack that paralyzed facility
- Linux version of Royal Ransomware targets VMware ESXi servers
- RSAWeb hit by ransomware attack
- Threat group targets over 1,000 companies with screenshotting and infostealing malware
- Michigan AG warns of cybersecurity risks after data breach of gaming sites
- Until further notice, think twice before using Google to download software
- Serious security hole plugged in infosec tool binwalk
- Feds say cyberattack caused suicide helpline's outage
- Over 30k Internet-Exposed QNAP NAS Hosts Impacted By CVE-2022-27596 Flaw
- ESXiArgs Ransomware Attack Targets VMware Servers Worldwide
- VMware Security Response Center (vSRC) Response to 'ESXiArgs' Ransomware Attacks
- 'Phishing-as-a-service' kits drive uptick in theft: One business owner's story
- Hacking into Toyota’s global supplier management network
- You may not care where you download software from, but malware does
- Hackers backdoor Windows devices in Sliver and BYOVD attacks
- Here's a list of proxy IPs to help block KillNet's DDoS bots
- Collect, Exfiltrate, Sleep, Repeat - The DFIR Report
- GuLoader Malware Using Malicious NSIS Executables to Target E-Commerce Industry
- Chip equipment maker MKS Instruments says it is investigating ransomware attack
- Five Guys allegedly hit by ransomware
- Linux Variant of Clop Ransomware Spotted, But Uses Faulty Encryption Algorithm
- Medusa botnet returns as a Mirai-based variant with ransomware sting
- ION brings clients back online after ransomware attack
- Cybersecurity Incident Under Investigation in Berkeley County Schools - 19,000 Students Have Day Off
- Over 12% of analyzed online stores expose private data, backups
- Unpatched Security Flaws Disclosed in Multiple Document Management Systems
- CVE-2022-21587: Rapid7 Observed Exploitation of Oracle E-Business Suite Vulnerability
- The Rise of Script Kiddies: Where Inexperience Meets Opportunity
- Lessons Learned on Ransomware Prevention from the Rackspace Attack
- US online grocery delivery platform leaks 11m user records
- Arkansas DMV renewal slowdown caused by third-party data breach
- Drug distributor AmerisourceBergen confirms security breach
- Mysterious leak of Booking.com reservation data is being used to scam customers
- Critical Infrastructure at Risk from New Vulnerabilities Found in Wireless IIoT Devices

- Cloud Credentials Phishing | Malicious Google Ads Target AWS Logins
- Valve waited 15 months to patch high-severity flaw. A hacker pounced
- Reddit Breached With Stolen Employee Credentials
- U.S. and U.K. sanction TrickBot and Conti ransomware operation members
- Modesto police computers targeted in ransomware attack
- Cybersecurity Incident Shuts Down Biglaw Network
- Largest Canadian bookstore Indigo shuts down site after cyberattack
- Cybercriminals Bypass ChatGPT Restrictions to Generate Malicious Content
- Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure
- Singapore hit by growing cybercrimes, clocks $501M in losses from scams
- Satellite hack: BAE Systems forecasts major attack within 2023
- Highmark data breach exposes private information of about 300k customers
- If You Use LastPass, You Need to Change All of Your Passwords ASAP
- A10 Networks confirms data breach after Play ransomware attack
- BEC Attacks Surge 81% in 2022
- Experts warn Auto Industry OEMs and dealerships both at risk for cyberattacks

Other News Events of Note and Interest

- Remember Bing? With ChatGPT's Help, Microsoft Is Coming for Google Search
- Microsoft's new Bing and Edge hands-on: Surprisingly well-integrated AI
- How to try out the new Microsoft Edge with ChatGPT
- Google to release ChatGPT-like bot named Bard
- Ars Archivum: Top cloud backup services worth your money
- US stalkerware developer fined $410,000 and ordered to modify apps so they reveal spying
- Warning: Microsoft Teams Free (classic) will be gone in 2 months
- Users discover iCloud Backup issues following iOS 16.3 update
- Microsoft releases OOB update for Windows 10, 11, and Server to fix .NET issue
- Surprise! China's top Android phones collect way more info
- The U.S. secretly passed a medical cybersecurity law
- Is Windows 11 spying on you? New report details eye-opening levels of telemetry
- Treasury Says Cloud Computing Poses Risks to Financial Sector
- SonicWall warns web content filtering is broken on Windows 11 22H2
- Microsoft confirms Windows 11 and 10 Patch Tuesday broke DirectX apps on Intel hardware
- A Hackers Pot of Gold: Your MSP's Data
- Adobe and Microsoft Bring Industry-Leading Acrobat PDF to Microsoft Edge
- Dark Web Market Revenues Sink 50% in 2022
- Samsung Confirms 990 Pro SSD Firmware Fix Coming Soon

Cyber Insurance News

- Tackling the New Cyber Insurance Requirements: Can Your Organization Comply?
- Cyber insurance predictions, British steel supplier cyber attack
- Cyber Insurance, A Must-Have for Small Businesses
- Munich Re announces cyber risk management program
- Cyber Liability Insurance: Why Your Business Needs It According to AI