RED-N Managed Security

Weekly Update

Week ending March 11, 2023

*Headline **NEWS***

- Fortinet warns of new critical unauthenticated RCE vulnerability
- Suspected Chinese Campaign to Persist on SonicWall Devices
- Veeam fixes bug that lets hackers breach backup infrastructure
- CISA warns of critical VMware RCE flaw exploited in attacks
- Google Chrome 111 Patches 40 Vulnerabilities
- Google removing Chrome Cleanup Tool on Windows
- Medusa Ransomware gang posts video of data stolen from Minneapolis schools

Ransomware, Malware, and Vulnerabilities News

- 2022 Year in Review - The DFIR Report
- Rethinking Tactics: Annual Cybersecurity Roundup 2022 - Security Roundup
- Cyber-Threat Detections Surge 55% in 2022
- Intel CPU vulnerabilities fixed. But should you update?
- Apple Releases Safari Technology Preview 165 With Bug Fixes and Performance Improvements
- Emotet malware attacks return after three-month break
- Google Cloud Platform allows data exfiltration without a (forensic) trace
- Tips for Investigating Cybercrime Infrastructure
- How to prevent Microsoft OneNote files from infecting Windows with malware
- 10 dark web monitoring tools
- Core Members of DoppelPaymer Ransomware Gang Targeted in Germany and Ukraine
- PoC exploit for recently patched Microsoft Word RCE is public (CVE-2023-21716)
- DrayTek VPN routers hacked with new malware to steal data, evade detection
- Critical Vulnerabilities Allow Hackers to Take Full Control of Wago PLCs
- Old Windows ‘Mock Folders’ UAC bypass used to drop malware
- Data breach exposed millions of Verizon customers' account info
- Almost Half of Industrial Sector Computers Affected By Malware in 2022
- Industrial sector threats on the rise: an annual overview by Kaspersky
- DBatLoader and Remcos RAT Sweep Eastern Europe
- Cyberattack hits major hospital in Spanish city of Barcelona
- Acer confirms breach after 160GB of data for sale on hacking forum
- New HiatusRAT router malware covertly spies on victims
- Transparent Tribe Hackers Distribute CapraRAT via Trojanized Messaging Apps
- Brazilian Conglomerate Suffers 3TB Data Breach
- Hackers are quickly learning how to target cloud systems
- New malware variant has “radio silence” mode to evade detection
- Stealthy UEFI malware bypassing Secure Boot enabled by unpatchable Windows flaw
- Remote Code Execution as a Service
- Vulnerability in DJI drones may reveal pilot's location
- Attack campaign uses PHP-based infostealer to target Facebook business accounts
- Vulnerability in Toyota Management Platform Provided Access to Customer Data
- AI-Powered 'BlackMamba' Keylogging Attack Evades Modern EDR Security
- CISA's KEV Catalog Updated with 3 New Flaws Threatening IT Management Systems
- 557 CVEs Added to CISA's Known Exploited Vulnerabilities Catalog in 2022
- Exploitation of Critical Vulnerability in End-of-Life VMware Product Ongoing

- Jenkins Security Alert: New Security Flaws Could Allow Code Execution Attacks
- New ScrubCrypt Crypter Used in Cryptojacking Attacks Targeting Oracle WebLogic
- WP Statistics WordPress Plugin Patches CSRF Vulnerability
- Indigo still grappling with fallout one month after ransomware attack
- Akamai mitigates record-breaking 900Gbps DDoS attack in Asia
- Elementor WordPress Contact Form Plugin Vulnerability Exposes Up To 200,000 Sites
- IceFire Ransomware Returns | Now Targeting Linux Enterprise Networks
- Microsoft: Business email compromise attacks can take just hours
- Hackers Exploiting Remote Desktop Software Flaws to Deploy PlugX Malware
- Old Cyber Gang Uses New Crypter – ScrubCrypt
- Attackers exploit APIs faster than ever before
- Cyber attack shuts down Wilkes-Barre Area school
- Hackers Compromised Two Large Data Centers in Asia and Leaked Major Tech Giants' Login Credentials
- LastPass Hack: Engineer's Failure to Update Plex Software Led to Massive Data Breach
- AT&T alerts 9 million customers of data breach after vendor hack
- New GoBruteforcer malware targets phpMyAdmin, MySQL, FTP, Postgres
- New Version of Prometei Botnet Infects Over 10,000 Systems Worldwide
- GSA misled customer agencies over Login.gov privacy standard compliance, watchdog alleges
- Security researchers targeted with new malware via job offers on LinkedIn
- Acronis downplays intrusion after 12GB trove leaks online
- SEC charges Blackbaud for failing to disclose 'full impact' of ransomware attack
- Our Daily Bread Hack Shows Nonprofits Vulnerable to Cyberattacks
- Microsoft OneNote to get enhanced security after recent malware abuse
- City of Ottawa and contractor victims of "phishing" scam

Other News Events of Note and Interest

- Outlook for Mac now free, Microsoft 365 subscription not needed
- Where the New National Cybersecurity Strategy Differs From Past Practice
- Backblaze Annual Failure Rates for SSDs in 2022: Less Than One Percent
- NIST launches cybersecurity community of interest for small businesses
- Removing Local Active Directory the Easy Way
- Take Google Docs Offline to Access Your Files Anywhere
- Microsoft Updates Teams PowerShell Module to Version 5.0
- Migrating to Authentication Methods Policies - Happy days!
- Nvidia Driver Bug Increases CPU Usage
- How to roll back Nvidia driver to fix problems on Windows 11
- Microsoft Unveils Its Own Version of Nvidia's RTX Super Resolution
- Microsoft PowerToys 0.68.0: A breakdown of two new applications
- Why the Floppy Disk Just Won't Die
- Akamai releases new threat hunting tool backed by Guardicore capabilities
- Cobalt Strike 4.8: (System) Call Me Maybe
- Sued by Meta, Freenom Halts Domain Registrations
- Azure AD System-Preferred Authentication
- Microsoft shares fix for Outlook login errors in Exchange environments
- Microsoft 365 Apps admin center: Remote Office configuration
- AMD fixes a driver timeout issue that led to BSOD, system freeze on Windows 10, Windows 11

- Raising the bar for software security: GitHub 2FA begins March 13
- Encrypt Email in Microsoft Outlook to Safeguard your Sensitive Information
- Enable Report Suspicious Activity in Azure AD to Stay Alerted on Suspicious MFA Requests
- AmigaOS 3.2.2 released for those feeling nostalgic
- ECB tells banks to run cyber stress tests after rise in hacker attacks
- Belgium bans TikTok from government phones after U.S. and E.U.

Cyber Insurance News

- As cyber attacks on health care soar, so does the cost of cyber insurance
- 'Skinny' Cyber-Insurance Policies Create Compliance Path
- French Cyber Insurance Law Provokes Uncertainty