



RED-N Managed Security

Weekly Update

Week ending November 5, 2022

Headline NEWS

- [You Need to Update Google Chrome, Windows, and Zoom Right Now, and Apple, VMware, Cisco, Zimbra, SAP and Oracle](#)
- [Cisco addressed several high-severity flaws in its products](#)
- [Hundreds of U.S. news sites push malware in supply-chain attack](#)
- [Fortinet FortiGuard Labs has patched a number of vulnerabilities, see the PSIRT advisories](#)
- [OPENSLL Vulnerability – the sky isn't quite falling – evaluation by Tenable](#)
- [Europe prepares to rewrite the rules of the Internet, starting November 1, 2022](#)
- [Cyber officials from 37 countries, 13 companies to meet on ransomware in Washington](#)
- [Microsoft Authenticator gains feature to thwart spam attacks on MFA](#)
- [Dropbox discloses breach after hacker stole 130 GitHub repositories](#)
- [CISA Publishes Multi-Factor Authentication Guidelines to Tackle Phishing](#)
- [Apple macOS Ventura bug disables security software](#)
- [Emotet is back from vacation](#)
- [TikTok admits China staff can access European user data as FCC commissioner urges app be banned](#)

Other News Events of Note

- [AMD fixes infamous black screen issue on Windows 11 22H2 with latest driver](#)
- [Thousands of GitHub repositories deliver fake PoC exploits with malware](#)
- [New Azov data wiper tries to frame researchers and BleepingComputer](#)
- [Can a new form of cryptography solve the internet's privacy problem?](#)
- [2022 Cyber Threat Report Details Growing Trends](#)
- [Online age-verification system could create 'honeypot' of personal data and viewing habits, privacy groups warn](#)
- [What is a Proxy Server? How does it work?](#)
- [Hackers selling access to 576 corporate networks for \\$4 million – PDF file](#)
- [Hacking group abuses antivirus software to launch LODEINFO malware](#)
- [Mozilla Firefox fixes freezes caused by new Windows 11 feature](#)
- [Ransomware remains top cyber risk for organizations globally, says Allianz](#)
- [Follina Exploit Leads to Domain Compromise via Qbot](#)
- [Aurubis plant in Buffalo lays off employees following cyber attack](#)
- [Bed, Bath & Beyond confirms data breach following employee phishing attack](#)
- [CosMiss: Azure Cosmos DB Vulnerability](#)
- [Charter raises base Internet to \\$80 a month; price hikes to hit 9.5M users](#)
- [Google ad for GIMP.org served info-stealing malware via lookalike site](#)
- [Backblaze Q3 2022 HDD Report, Balancing Price and Reliability](#)
- [Chegg sued by FTC after suffering four data breaches within 3 years](#)
- [Nucleus Security Releases Free CISA KEV Enrichment Dashboard and Research, Providing Vulnerability Prioritization](#)
- [CVE-2022-31692: Authorization rules can be bypassed via forward or include in Spring Security](#)
- [NVIDIA GeForce 526.47 WHQL driver is available for download](#)
- [SHA-3 code execution bug patched in PHP – check your version](#)
- [New SandStrike spyware infects Android devices via malicious VPN app](#)
- [New Windows 'LockSmith' PowerToy lets you free locked files](#)
- [LockBit 3.0 gang claims to have stolen data from Thales](#)
- [TeamViewer 15.35.7, incoming connections completely broken on specific computers](#)
- [Checkmk monitoring: Remote Code Execution by Chaining Multiple Bugs](#)
- [Transforming your organization to cloud-only: Migrating Active Directory identities to cloud identities](#)
- [Hackers steal \\$420K from Port of Louisiana; the Mississippi River port is beefing up security](#)
- [Despicable Scumbag Waste-of-Flesh Hacker Charged with Extorting Online Psychotherapy Service](#)
- [Oreo Giant Mondelez Settles NotPetya 'Act of War' Insurance Suit](#)
- [Microsoft is killing custom domain names in Outlook.com for Microsoft 365 Individual and Family](#)
- [ALMA Observatory shuts down operations due to a cyberattack](#)
- [Cybercrime Buys Security Software in Bear Market](#)
- [Windows 11 22H2: network printing switched to RPC over TCP](#)
- [Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor](#)
- [Volatile Geopolitics Shake the Trends of the 2022 Cybersecurity Threat Landscape](#)
- [British govt is scanning all Internet devices hosted in UK](#)
- [Z-Library eBook site domains seized by U.S. Dept of Justice](#)
- [Microsoft Warns on Zero-Day Spike as Nation-State Groups Shift Tactics](#)

