# *RED-N* Managed Security

## Weekly Update

*Week ending March 4, 2023*

### *Headline* ***NEWS***

- BlackLotus Becomes First UEFI Bootkit Malware to Bypass Secure Boot on Windows 11
- Microsoft releases Windows security updates for Intel CPU flaws
- Cisco patches critical Web UI RCE flaw in multiple IP phones
- Aruba Networks fixes six critical vulnerabilities in ArubaOS
- Booking.com's OAuth Implementation Allows Full Account Takeover
- CISA director urges tech sector to stop shipping unsafe products
- CISA Issues Warning on Active Exploitation of ZK Java Web Framework Vulnerability
- More Cybercriminals Ditching Ransomware To Focus On Data Extortion
- 2023 CrowdStrike Global Threat Report
- Vulnerabilities Being Exploited Faster Than Ever
- CISA releases free 'Decider' tool to help with MITRE ATT&CK mapping

### Ransomware, Malware, and Vulnerabilities News

- Dish Network still reeling from week-old ransomware attack
- U.S. Cybersecurity Agency Raises Alarm Over Royal Ransomware's Deadly Capabilities
- Highlights from the New U.S. Cybersecurity Strategy
- Survey shows most people don't rely on SMS-based 2FA, they use apps
- Security Defects in TPM 2.0 Spec Raise Alarm
- 'Major' U.S. Marshals Service hack compromises sensitive info
- Microsoft Introduces Suspicious Activities Reporting in Azure AD
- Dark web market BidenCash leaks info on two million payment cards
- Hatch Bank discloses data breach after GoAnywhere MFT hack
- From CVE-2022-33679 to Unauthenticated Kerberoasting
- PureCrypter Malware Targets Governments Through Discord
- WannaCry Hero & Kronos Malware Author Named Cybrary Fellow
- New cyberattack tactics rise up as ransomware payouts increase
- Canadian Telecom Firm Telus Reportedly Investigating Breach
- Canada banning TikTok from government mobile devices over concerns about cyberattacks
- Ransomware Attack Forces Produce Giant Dole to Shut Down Plants
- ChromeLoader campaign lures with malicious VHDs for popular games
- 'Ethical hacker' among ransomware suspects cuffed by Dutch cops
- RIG Exploit Kit still infects enterprise users via Internet Explorer
- Wiper malware goes global, destructive attacks surge
- When Low-Tech Hacks Cause High-Impact Breaches
- PlugX Trojan Disguised as Legitimate Windows Debugger Tool in Latest Attacks
- PureCrypter Malware Targets Government Entities in Asia-Pacific and North America
- QNAP Launches Security Bounty Program
- Microsoft Defender for Office 365 named best email security service of 2023
- Crypto-mining malware attacking Apple Mac with pirated software
- Cyberattack on Boston union results in $6.4M loss
- LastPass Says DevOps Engineer Home Computer
- Middlebury College temporarily suspends online ticket sales following third-party data breach
- Critical flaws in WordPress Houzez theme exploited to hijack websites
- Boston union loses $6.4M in cyberattack
- Beware rogue 2FA apps in App Store and Google Play – don't get hacked!

- New Exfiltrator-22 post-exploitation kit linked to LockBit ransomware
- Russian Darknet Markets, Ransomware Groups Thrive Despite Sanctions, Report
- Record Number of Mobile Phishing Attacks in 2022
- OneNote Embedded file abuse
- All CVEs Are Not Created Equal
- Attacker Floods PyPI With 1000s of Malicious Packages That Drop Windows Trojan via Dropbox
- Threat intelligence: Why Attributing Cyber-Attacks Matters
- Computer Security Incident Response Teams: CSIRT Models, Skills & Best Practices
- Bitdefender Releases Free Decryptor for MortalKombat Ransomware Strain
- Snatch ransom gang claims Ingenico scalp
- Attackers publish Beeline's Jira database, exposing customers
- Hackers Claim They Breached T-Mobile More Than 100 Times in 2022
- CISA Tells Agencies What to Prioritize to Meet Cybersecurity Log Mandate
- Minneapolis Public Schools still investigating what caused 'encryption event'
- Pierce Transit, city of Lakewood victim of ransomware attack
- China Is Relentlessly Hacking Its Neighbors
- Ransomware attack on chip supplier causes delays for semiconductor groups
- All In One SEO WordPress Plugin Vulnerability Affects Up To 3+ Million
- Experts Identify Fully-Featured Info Stealer and Trojan in Python Package on PyPI
- Chick-fil-A confirms accounts hacked in months-long "automated" attack
- Play ransomware claims disruptive attack on City of Oakland
- EPA issues water cybersecurity mandates, concerning industry and experts
- Rapid7 finds cyber personnel can't patch vulnerabilities fast enough
- Several Law Firms Targeted in Malware Attacks
- Scammers use fake QR codes to put malware on phones
- Unpatched old vulnerabilities continue to be exploited
- Sun Pharma Reports IT Security Incident
- Warning on SolarWinds-like supply-chain attacks: 'They're just getting bigger'
- Belgium's cyber security agency links China to spear phishing attack on MP
- EV Charging Infrastructure Offers an Electric Cyberattack Opportunity
- Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards
- Attackers increasingly using transfer.sh to host malicious code

## Other News Events of Note and Interest

- Tenable 2022 Threat Landscape Report
- Without FIDO2, MFA Falls Short
- How to use a YubiKey with Fedora Linux
- How to set up two-factor authentication on your online services
- System-preferred multifactor authentication in Azure AD
- How to enable two-factor authentication on your Google account
- Wireshark 4.0.4 Released
- CISA Shares Advice to Improve Networks' Monitoring and Hardening
- Top US cybersecurity official calls on Microsoft and Twitter to match Apple's commitment to user security
- A tale of Phobos - how we almost cracked a ransomware using CUDA
- Microsoft Defender may soon get installed on your Windows PC automatically
- Dashlane is the latest password manager to dash toward a password-less future

- Cybersecurity Label for U.S. Coming as Early as April - EE Times
- Cisco to acquire startup Valtix to beef up its multi-cloud network security
- Australia plans to reform cyber security rules, set up agency
- Work-From-Home Regulations Are Coming. Companies Aren't Ready
- Intel releases new Bluetooth drivers to improve connection between your phone and PC
- The importance of cyber security in the horticultural sector
- Economic pressures are increasing cybersecurity risks; a recession would amp them up more
- Well-funded security systems fail to prevent cyberattacks in US and Europe: Report
- New Microsoft Intune Suite launches to help teams improve their endpoint security
- Microsoft somehow brings iMessage to Windows, will it last?
- Intel Patches Stuttering Ethernet Issues, but It's Just a Workaround for Now
- CISA red team shares key findings to improve network monitoring and hardening
- FTX Confirms $9 Billion in Customer Funds Vanished
- After killing MSDT, Microsoft looks to add VBScript removal in Windows 11 23H2 (Moment 4)

**Cyber Insurance News**

- CISA Leader Tells MSPs Cyber Insurance Market 'Fueled Rise In Ransomware'
- Cyber Insurance Back From the Brink After Ransomware Onslaught
- Traditional underwriting won't cut it in "chaotic" cyber market – Corvus