RED-N Managed Security

Weekly Update

Week ending January 28, 2023

Headline ***NEWS***

- ISC Releases Security Patches for New BIND DNS Software Vulnerabilities
- Apple fixes actively exploited iOS zero-day on older iPhones, iPads
- iOS 16.3 fixes multiple security vulnerabilities
- VMware fixes critical security bugs in vRealize log analysis tool
- Ransomware access brokers use Google ads to breach your network
- CISA: Protecting Against Malicious Use of Remote Monitoring and Management Software
- Exploiting a Critical Spoofing Vulnerability in Windows CryptoAPI
- GoTo's LastPass breach keeps getting worse – more stolen
- Realtek SDK Vulnerability Attacks Highlight IoT Supply Chain Threats
- Lexmark warns of RCE bug affecting 100 printer models, PoC released
- Hive Ransomware Infrastructure Seized in Joint International Law Enforcement Effort
- AMD fixes major Windows 11 22H2 bug that led to launch failures with 23.1.2 driver
- Microsoft urges admins to patch on-premises Exchange servers
- Microsoft fixes Windows 11 issue behind Remote Desktop freezes

Ransomware, Malware, and Vulnerabilities News

- The Chilling Potential of ChatGPT for Criminal Activities
- Electronic health record giant NextGen dealing with cyberattack
- Sliver C2 Leveraged by Many Threat Actors
- Microsoft plans to kill malware delivery via Excel XLL add-ins
- Microsoft took its macros and went home, so miscreants turned to Windows LNK files
- Google Ads invites being abused to push spam, adult sites
- ShareFinder: How Threat Actors Discover File Shares
- FanDuels warns of data breach after customer info stolen in vendor hack
- Why PayPal Users Need to Check Their Accounts (Right Now)
- Hackers demand millions in ransom from Arnold Clark, threaten massive upload of customer information
- FBI Says North Korea Responsible for $100 Million Harmony Protocol Crypto Hack
- Administrator of RSOCKS Proxy Botnet Pleads Guilty
- DragonSpark | Attacks Evade Detection with SparkRAT and Golang Source Code Interpretation
- Emotet Malware Makes a Comeback with New Evasion Techniques
- Kaspersky Releases 2023 Predictions
- Attackers Exploit Fortinet Zero-Day CVE-2022-42475 with BoldMove Malware
- Contractor 'mistakenly' opened email starting Baltimore County school cyberattack
- Federal agencies hacked using legitimate remote desktop tools
- New stealthy Python RAT malware targets Windows in attacks
- Chinese Hackers Utilize Golang Malware in DragonSpark Attacks to Evade Detection
- The Unrelenting Menace of the LockBit Ransomware Gang
- Over 4,500 WordPress Sites Hacked to Redirect Visitors to Sketchy Ad Pages
- Lessons Learned from the Windows Remote Desktop Honeypot Report
- Hilton Hotels Loyalty Program Data Breached, Info of 3.7 Million Users for Sale
- Security Navigator Research: Some Vulnerabilities Date Back to the Last Millennium
- Zacks Investment Research data breach affects 820,000 clients
- Bitwarden password vaults targeted in Google ads phishing attack
- Blank Image Attack: Blank Images Used to Evade Anti-Malware Checks
- New Mimic Ransomware Abuses Everything APIs for its Encryption Process

- Indiana, Wawasee Community Schools Responds To Ransomware Attack
- Kelowna, Canada – Vice Society claims responsibility for Okanagan College ransomware
- One Brooklyn Health Confirms Cyberattack, BlackCat Ransomware Claims Attack On NextGen
- New Wave of Cyberattacks Targeting MS Exchange Servers
- SaaS RootKit Exploits Hidden Rules in Microsoft 365
- Uncle Sam slaps $10m bounty on Hive while Russia ban-hammers FBI, CIA
- ChatGPT is a bigger threat to cybersecurity than most realize
- Welcome to Goot Camp: Tracking the Evolution of GOOTLOADER Operations
- Seven Insights From a Ransomware Negotiator
- New 'Hook' malware allows hijacking, real-time spying on Android devices
- Dutch hacker arrested for trying to sell the personal information of nearly every Austrian citizen
- PlugX malware hides on USB devices to infect new Windows hosts

Other News Events of Note and Interest

- AI Passes U.S. Medical Licensing Exam
- ChatGPT passed an MBA exam and one professor is sounding the alarm
- Microsoft moves a step closer to replacing Windows 11 stock Mail app with the new "One Outlook"
- The University of Florida hints at a likely TikTok ban, and other campuses may follow
- XenServer, split from Citrix, promises per-core prices 'unlike certain other hypervisors'
- Introducing the GitHub Bug Bounty swag store
- Chromium's WebRTC Zero-Day was Just the Tip of the Iceberg
- 75k WordPress sites impacted by critical online course plugin flaws
- Massive Ad Fraud Scheme Targeted Over 11 Million Devices with 1,700 Spoofed Apps
- We're just shouting into the void, says US watchdog offering cybersecurity advice
- It may be time to move on from NTFS as Microsoft is quietly enabling Windows 11 ReFS support
- The Importance of Standardizing Azure AD Account Creation
- Shutterstock Has Launched Its Generative AI Image Tool
- Singularity: Here's When Humanity Will Reach It, New Data Shows
- Vice Society Ransomware Group Targets Manufacturing Companies
- IPv6 for Dummies: NSA pushes security manual on DoD admins
- If your Start menu or apps are freezing up on Windows, Microsoft has a suggestion
- Microsoft 365 outage took down Teams, Exchange Online, Outlook - globally
- Bitwarden responds to encryption design flaw criticism
- NIST Risk Management Framework Aims to Improve Trustworthiness of Artificial Intelligence
- CISA publishes long-awaited K-12 cybersecurity roadmap
- Smart ovens do really dumb stuff to check for Wi-Fi, like call Russia and China
- Unmasking VENOM SPIDER the threat actor behind Golden Chickens MaaS

Cyber Insurance News

- Cyber Reinsurance Rates Still Growing, But Not as Fast
- Regulator Stress Test Highlights Cyber Insurance Concerns
- Bermuda Insurance Leader Dan Rance Joins Resilience to Accelerate Move Upmarket
- Cyber insurance won't save your company if it has a breach
- What to Expect from Cyber Insurance in 2023 and Beyond
- Beazley's New $45m "Cyber Catastrophe Bond" May Be Sign of Things to Come
- Cyber insurance provider Coalition approved Lloyd's coverholder in the UK