RED-N Managed Security

Weekly Update

Week ending November 26, 2022

Headline ***NEWS***

- **Google** pushes **emergency Chrome update** to fix 8th zero-day in 2022, patch now
- **New Windows Server updates cause domain controller freezes, restarts**
- Microsoft Confirms **Critical Bugs In Windows 11 22H2 Update**
- Microsoft warns of **Remote Desktop freezes** on **Windows 11 22H2**
- **AMD** releases **new chipset driver** to **fix blue screens of death** on **Windows 11 22H2** and more
- Upgrade to **Apache Commons Text 1.10** to Avoid New Exploit
- Action required: **Upgrade** Windows clients to v1.32.3 · **Tailscale VPN**
- **Pentagon releases zero trust strategy** to guide DoD cybersecurity priorities
- **WhatsApp data leak**: 500 million user records for sale
- **Windows zero-day** vulnerability allows **JS files** to **bypass security messages**, exploited by hackers

Other News Events of Note

- **Aggressive Qakbot Campaign** and the **Black Basta Ransomware** Group Targeting U.S. Companies
- **ESF** Partners, **NSA**, and **CISA** Release **Software Supply Chain Guidance** for Customers
- **Microsoft** makes a **game** of **Team** building, with benefits
- You Can Finally **Spot Internet Coverage Gaps** on FCC's **Broadband Maps**
- **Windows 11** Release Preview (KB5020044) **fixes high CPU usage** in File Explorer and more
- Microsoft Warns of **Hackers Using Google Ads** to Distribute **Royal Ransomware**
- Keeping Up With **Ransomware News**
- **Meta** keeps **booting small-business** owners for being hacked on **Facebook**
- **AXLocker**, **Octocrypt**, and **Alice**: Leading a **new** wave of **Ransomware** Campaigns
- **Google** releases **165 YARA rules to detect Cobalt Strike** attacks
- How **social media scammers** buy time to **steal your 2FA codes**
- **Attackers bypass** Coinbase and MetaMask **2FA** via TeamViewer, **fake support chat**
- Microsoft Warns of **Rise in Stolen Cloud Tokens** Used to **Bypass MFA**
- **Token tactics**: How to prevent, detect, and **respond to cloud token theft**
- **Emotet** is back and delivers **payloads** like **IcedID** and **Bumblebee**
- **AirAsia ransomware** attack? **Daixin** Team **'leaks five million records'**
- Information on **DMARC** analytic vendors, **email authentication**, and **email security tools**
- **5 free resources from** the Cybersecurity and Infrastructure Security Agency (**CISA**)
- **Microsoft** set to "**hard block**" OneDrive and SharePoint on **Internet Explorer 11** in **January 2023**
- **Donut extortion group** also targets victims with **ransomware**
- **Google won** a **lawsuit** against the **Glupteba botnet** operators
- **Windows 10 22H2** now in broad deployment, **available to everyone**
- **Android file manager apps** infect thousands with **Sharkbot malware**
- Threat Assessment: **Luna Moth Callback Phishing** Campaign
- Adversarial **AI Attacks Highlight** Fundamental **Security Issues**
- **Hackers breach** energy orgs **via** bugs in **discontinued web server**
- **ViperSoftX**: Hiding in System Logs and **Spreading VenomSoftX**
- **Cybercrooks to ditch BTC** as regulation and tracking improves
- **Windows Subsystem for Linux** now packaged as a **Microsoft Store app**
- **Mastodon vulnerable** to multiple system configuration problems
- Study shows **50% of repair shops snooped** on **customer devices**
- **University** orders investigation into **Oracle finance disaster**
- **Professional** stealers: **opportunistic scammers targeting** users of **Steam**, **Roblox**, and **Amazon** in 111 countries
- **US offshore oil and gas rigs at 'significant' risk of cyberattacks**, warns government watchdog
- **Ducktail Hacker Group** Evolves, **Targets Facebook Business** Accounts
- **Microsoft SQL Server** license **prices rise ten percent** as version 2022 debuts
- Ouch! **Ransomware gang** says it won't attack **AirAsia** again due to the "chaotic organization" and sloppy network
- **RDP** from Windows 10 to Windows 10 **by workstation** name suddenly saying "incorrect password" but **RDP by IP works**?
- Beware of **fake MSI Afterburner** that **installs cryptojacking** and information-stealing malware
- **Docker Hub repositories** hide over **1,650 malicious containers**
- Massive **INTERPOL** takedown **seized $130 million** from cybercriminals worldwide
- **U.S. Navy Forced to Pay** Software Company **for Licensing Breach**
- Founder ran **FTX** as "**personal fiefdom**"; many **assets stolen or missing**, court hears
- **Massive Twitter data breach** reported earlier in the year **worse than reported**; multiple hacks