RED-N Managed Security
Weekly Update

Week ending September 23, 2022

*Headline **NEWS***

- Critical Flaws in **Airplanes WiFi Access Point** Let Attackers Gain Root Access
- **Windows 11 22H2** is released, here are the new features
- Recent **Windows 11 update** apparently **causing various issues** due to Core Isolation (VBS)
- Critical **Vulnerability** in **Oracle Cloud Infrastructure** Allowed Unauthorized Access
- **LockBit ransomware builder leaked** online by "angry developer"
- Hackers Exploited **Zero-Day RCE** Vulnerability in **Sophos Firewall** — Patch Released
- Salesforce co-CEO Benioff says **there's 'no finish line when it comes to security'** after Uber hack
- British **teen arrested** in hacking case – likely linked to the **Uber** hack
- **Malicious OAuth applications** abuse cloud email services to spread spam
- **Microsoft Defender for Endpoint** will turn on **tamper protection** by default
- **Microsoft** Releases Out-of-Band **Security Update** for **Microsoft Endpoint Configuration Manager**
- **Python tarfile vulnerability** affects 350,000 open-source projects
- **Netgear**: Security Advisory for **Vulnerabilities** in FunJSQ on Some **Routers** and **Orbi WiFi** Systems

Other News Events of Note

- Record **DDoS Attack** with **25.3 Billion Requests** Abused HTTP/2 Multiplexing
- The Evolution of the **Chromeloader Malware** into delivery tool for others
- **Palo Alto Cortex XDR Agent**: Improper Link Resolution Vulnerability When Generating a Tech Support File
- **Microsoft Warns** of Large-Scale **Click Fraud** Campaign Targeting Gamers
- **Government of Lithuania** announces a breach investigation into **Revolut Bank**
- **LDAP Nom Nom** - Anonymously **bruteforce AD usernames** from DCs by abusing LDAP Ping requests (cLDAP)
- Credential **Phishing Targeting Government Contractors** Evolves Over Time
- **Active Directory and DNS**: Why you should not practice adding 8.8.8.8 in **DNS forwarder**?
- **American Airlines** discloses **data breach** after employee email compromise
- **Tech Companies** Continue to Embrace **Remote Work**
- Russia-**Nexus UAC-0113** Emulating Telecommunication Providers in Ukraine
- Microsoft **Teams' GIFShell Attack**: What Is It and How You Can Protect Yourself from It
- Clearwater cybersecurity firm **KnowBe4** weighing $4.2B private equity offer
- Exploiting **Azure AD Pass-Through Authentication (PTA) vulnerabilities**: Creating backdoor and harvesting credentials
- **Cobalt Strike 4.7.1** is now available. This is an out of band update to fix an issue with no workaround
- **New** unified **OneNote app** on the way to Windows this month
- New **Windows 11 security features** are designed for hybrid work
- **Domain Shadowing**: A Stealthy Use of **DNS Compromise** for Cybercrime
- **Hive ransomware** claims attack on New York Racing Association
- **Cyberattack** closes **Michigan school district** for 2 days
- **Exploiting** a Seagate **service** to create a SYSTEM shell
- **Malwarebytes** accidentally **blocks Google**, **YouTube** as malware
- **2-Step Email Attack** Uses Powtoon Video to Execute Payload
- Announcing: **Backblaze Computer Backup v8.5** for Windows and macOS
- **CISA** Alert: Iranian State Actors Conduct **Cyber Operations Against the Government of Albania** for 14 months
- **New Method** of **Volume Shadow Backup Deletion** Seen in Recent Ransomware
- IT Security Takeaways from the **Wiseasy Payment Terminal Hack**
- How to have fun **negotiating with a ransomware gang** – online chatbot game
- How to **Dodge New Ransomware Tactics**, Some Key Things to Watch for and Avoid
- Rewards plus: **Fake mobile banking rewards apps** lure users to install **info-stealing RAT** on Android devices
- Surge in **Magento 2** (e-commerce) template **attacks**
- **Noberus Ransomware**: **Darkside** and **BlackMatter** Successor Continues to Evolve its Tactics
- Researchers unearth **hacking group 'Mafalda'** that's been active, yet undetected for years
- **SMB authentication rate limiter** now on by default in Windows Insider, increasing difficulty for attackers
- **Windows 11 22H2** causing gaming **issues** for some **NVIDIA** users
- **Atlassian Confluence Vulnerability** CVE-2022-26134 Abused For Cryptocurrency Mining, Other Malware
- **NSA** shares **guidance** to help secure **OT/ICS critical infrastructure** – PDF link
- A Multimillion Dollar **Global Online Credit Card Scam** Uncovered
- Lessons from a Professional **Password Cracker**
- **Cyberattack Costs** for US Businesses **up** by **80%**