RED-N Managed Security
Weekly Update

Week ending October 29, 2022

*Headline **NEWS***

- **ConnectWise** patched a **critical RCE vulnerability** in Recover and R1Soft Server Backup Manager
- **Google** fixes seventh **Chrome zero-day** exploited in attacks this year
- **Atlassian Jira Align**, Version 10.107.4 **Vulnerability** Advisory
- **Apple** fixes **new zero-day** used in attacks against iPhones, iPads, and iPods – check here for your particular version
- Stranger Strings: An **exploitable** flaw in **SQLite** the world's most widely used database software
- Researchers Detail **Windows Event Log Vulnerabilities**: LogCrusher and OverLog
- **Cisco** warns admins to **patch AnyConnect** flaws exploited in attacks
- Windows **Mark of the Web Zero-Days** Remain Patchless, Under Exploit
- **Mark of the Web Windows Zero-Day Vulnerability** Lets JavaScript Files Bypass Security Warnings
- **VMware** fixes critical **Cloud Foundation** remote code execution bug and **backports to EOL systems** too
- Incoming **OpenSSL critical fix**: Organizations, users, get ready!
- Microsoft fixes **Windows vulnerable driver blocklist** sync issue
- **Thomson Reuters** leaked at least **3TB** of sensitive **data**, including **server passwords**
- In a disturbing move, **PayPal** quietly reintroduces **$2,500 "misinformation" fine**
- **Microsoft** shares workaround for **ongoing Outlook** login **issues**
- **Microsoft OneDrive crashes** because of recent Windows 10 updates – not fixed yet

Other News Events of Note

- **DHS** rolls out **new cybersecurity performance goals** for private sector
- Just in time for **Cybersecurity Awareness Month** - Cybersecurity **Risks & Stats** This Spooky Season
- An **interview** with **cyber threat hunter** Hiep Hinh
- "**Dormant Colors**": Live Campaign With Over 1M **Data Stealing Extensions** Installed
- **Microsoft fixes printing issue** blocking Windows 11 22H2 upgrades
- **Typosquat campaign** mimics 27 brands to **push** Windows, Android **malware**
- **CodeXTF2/ScreenshotBOF**: An alternative **screenshot** capability **for Cobalt Strike** that uses WinAPI
- **Multiple RCE Vulnerabilities** Discovered in **Veeam Backup & Replication** App
- **Microsoft** Technical Takeoff session on the **new Local Administrator Password Solution (LAPS)**
- **Microsoft Technical Takeoff sessions** on many more topics than just LAPS
- Soon **Google** will stop supporting **Chrome** on **Windows 7** and **8.1**
- When would a **cyberattack** trigger a **NATO response based on Article 5's verbiage**? It's a mystery
- **Hive Ransomware** Hackers Begin **Leaking Data** Stolen from **Tata Power** Energy Company
- How the **"pizza123" password** could take down an organization -The importance of **password hygiene**
- How Teams of **Volunteer Techies Hunt** Down **Ransomware Gangs**
- **Windows Event Log Analysis** - Incident Response Guide
- **Steps to follow** in event of **Cyber attack** – Reddit discussion
- **Cybersecurity teams** are **reaching** their **breaking point**. We should all be worried
- **SentinelOne** Launches **WatchTower** Vital Signs
- How **Kerberos Golden Ticket Attacks** Are Signaling a Greater Need for Identity-Based Security
- Ukrainian to be extradited is charged for operating **Raccoon Stealer malware service**
- **Windows 11 22H2** KB5018496 update brings **better MSA** experience, **right click Task Manager**
- **DEV-0832 (Vice Society)** opportunistic **ransomware** campaigns **impacting US education** sector
- **Ransomware down** this year – but there's a catch
- **Data Breaches Rise** By 70% Globally in Q3 2022
- **Ransomware** Gangs **Ramp Up** Industrial Attacks in US
- **Server Manager** disk resets can lead to data loss
- **Microsoft** gives an early brief glimpse of **Windows 11 22H2 Moment 2** update
- Use **additional context in Microsoft Authenticator notifications** - Azure Active Directory
- Daniel Kaye Charged With Operating **Real Deal Dark Web Market**
- Massive **cryptomining campaign** abuses **free-tier cloud** dev **resources**
- **Apple** Exec Confirms iPhones Will Get **USB-C Ports**
- **Microsoft** delists the **OneNote UWP** app from the Microsoft Store
- One of the world's biggest **ticket websites (See Tickets)** suffered a **multi-year data breach**
- Hackers use **Microsoft IIS web server logs** to control malware
- **Passwordless authentication market** to reach $6.6B by 2025
- **Windows servers** that have been **fueling massive DDoSes** for months
- Where is the Origin? **QAKBOT Uses Valid Code Signing Certificates**