RED-N Managed Security

Weekly Update

Week ending October 15, 2022

*Headline **NEWS***

- **Microsoft** October 2022 **Patch Tuesday** fixes **two zero-days**, 1 used in attacks, **84 flaws, 13** of which are **critical**
- The October 2022 **Exchange SUs do not contain fixes for the zero-day vulnerabilities** reported publicly on September 29, 2022
- **Windows 11** KB5018427 update released with **30 bug fixes**, improvements
- **Aruba** fixes **critical RCE** and **auth bypass** flaws in **EdgeConnect**
- **VMware** fixed a **high-severity bug** in **vCenter** Server
- Pro-Russian **hackers** claim responsibility for **knocking U.S. airport websites offline**
- **Critical vm2 sandbox** escape **flaw** uncovered, patch ASAP!
- Say Goodbye to **Microsoft Office** and Hello to **Microsoft 365**

Other News Events of Note

- **Phishing-Resistant MFA** to Implement Stronger MFA Authentication
- **Phishing** attack spoofs **Zoom** to steal **Microsoft** user credentials
- **NSA, CISA, FBI** issue **alert** on custom exfiltration tools being used against Defense Industrial Base
- **Resource Public Key Infrastructure** (RPKI), intended to safeguard the routing of data traffic, can be **broken**
- **Windows 11 22H2** breaks **provisioning** with 0x800700b7 **errors**
- **Intel** confirms **Alder Lake BIOS** Source Code **leak** is authentic
- **Protect** Your Organization **from** Outlook **Phishing** Attack using External Email Tagging
- **PayPal apologizes** for policy notice saying users could face $2,500 fines for misinformation
- Behind the Scenes of the **Caffeine Phishing-as-a-Service Platform**
- **Windows 11** Now Offers Automatic **Phishing Protection**
- **OAuth 2** and why **Microsoft** is finally forcing you into it
- Florida firm's **webcam surveillance violates human rights**, Dutch court says
- **VirtualBox 7.0.0** Final is now available
- **2FA** is over. Long live **3FA**!
- Researchers extract **master encryption key** from **Siemens PLCs**
- **BazarCall Call Back Phishing** Attacks Constantly Evolving Its Social Engineering Tactics
- **All Windows versions** can now block admin brute-force attacks with **Admin lockouts**
- Rising premiums, more restricted **cyber insurance coverage** poses big **risk** for companies
- **Toyota** dev left **key to customer info** on **public** GitHub page for five years
- In-Depth Look into Data-Driven Science Behind **Qualys TruRisk**
- The Latest **Funding News** and What it Means for **Cyber Security in 2023**
- Microsoft **Exchange** servers hacked to **deploy LockBit ransomware**
- **Windows 11 22H2 blocked** due to Windows Hello issues **on some systems**
- **VMware** vSphere 8, now available for download
- **Black Basta Ransomware** Gang Infiltrates networks via **QAKBOT**, **Brute Ratel**, and **Cobalt Strike**
- The **forensic analysis** of a **ransomware attack** [Q&A]
- **Alchimist**: A **new attack framework** in Chinese for **Mac**, **Linux** and **Windows**
- **Google** Rolling Out **Passkey Passwordless Login** Support to Android and Chrome
- AI-generated imagery is the new clip art as **Microsoft adds DALL-E to its Office suite**
- What the **Uber Breach Verdict** Means for **CISOs** in the US
- **Microsoft** accidentally **revealed** design prototype of **next-gen Windows** version
- **Microsoft** Unveils **New Audio Dock** and Microsoft **Presenter+ Remote**
- **Magniber Ransomware** Adopts **JavaScript** to Attack Individual Users
- **Chinese**-linked **hackers** targeted **U.S. state legislature**
- **Microsoft Teams Premium,** a new offering with more features
- Happy Sweet **16 Birthday** to the **pfSense Firewall**
- Over **80,000 DJI drone IDs exposed** in data leak
- **Microsoft 365 Defender** now automatically **disrupts ransomware** attacks – only for businesses
- **Zeek** is Now a Component of Microsoft Windows
- **China's** Cyberattack **Strategy** Explained
- **Russian DDoS attack project 'DDOSIA'** pays contributors for more firepower
- Researchers Reveal **Detail for Windows Zero-Day Vulnerability** Patched Last Month
- **Zimbra** servers are still being **exploited** by the **zero-day** from last month
- New PHP Version of **Ducktail Malware Hijacking Facebook** Business Accounts
- Over 45,000 **VMware ESXi** servers just reached **end-of-life**
- **Google Translate** is being **hijacked** by phishers **to steal your data**