RED-N Managed Security
Weekly Update

Week ending September 30, 2022

*Headline **NEWS***

- Two **Zero-Day Microsoft Exchange vulnerabilities** without patch are being exploited – **mitigation steps** published
- **Microsoft Customer Guidance** for Reported Zero-day **Vulnerabilities in Microsoft Exchange Server**
- Critical Remote Hack Flaws Found in **Dataprobe's Power Distribution Units**
- **WhatsApp 0-Day Bug** Let Hackers Execute a Code & Take **Full** App **Control** Remotely
- **Don't Buy a PC With 8GB of RAM** (Unless You Plan to Upgrade It)
- Time's up: **Microsoft Exchange Online Basic Authentication deprecation** start was Saturday
- **Microsoft** confirms **Windows 11 Printer issue** after the 22H2 update

Other News Events of Note

- **Ransomware** operators might be dropping file encryption in favor of **corrupting files**
- **Microsoft** to retire **Exchange Online client access rules** in a year
- **Australia** flags **privacy** overhaul after huge cyber attack on **Optus**
- Mozilla **Firefox celebrates its 20th anniversary**, will continue to support current content blockers
- **Facebook** sued for allegedly **spying on users** via in-app web browser
- The Mystery of **Metador** | An **Unattributed Threat** Hiding in Telcos, ISPs, and Universities
- **NVIDIA** update to fix lower performance after upgrading to **Microsoft Windows 11** 2022
- **Cyberattack** on **InterContinental Hotels** Disrupts Business at Franchisees and Supply Chain
- The Ukrainian military intelligence warns that **Russia** is planning to **escalate cyberattacks**
- **Cloudflare** launches an **eSIM** to secure mobile devices
- **Pure VPN** joins forces with **Samsung** to build a safer online world, integrated into Samsung's secure Wi-Fi
- **North Korea's Lazarus Hackers** Targeting macOS Users Interested in Crypto Jobs
- **Pass-the-Hash Attacks** and How to Prevent them in Windows Domains
- **Kaspersky** report on **NullMixer**: oodles of **Trojans** in a single dropper
- **Paloalto's Unit42** report on Hunting for **Unsigned DLLs to Find APTs**
- **Wall Street Journal** report Why **Even Big Tech Companies Keep Getting Hacked**—and What They Plan to Do About It
- **FCC** takes long-delayed step against **spam text** surge
- **IRS reports** significant **increase in texting scams**; warns taxpayers to remain vigilant
- **Microsoft** Security Report Highlights **OAuth Compromise** of Exchange Online
- **Facebook** report on Removing **Coordinated Inauthentic Behavior** from China and Russia
- **Cloudflare** justifiably tooted their own horn - Cloudflare named a **Leader in WAF** by Forrester
- US arm of **Israeli defense giant Elbit Systems** says it was **hacked**
- 20-year-old **Linux workaround** is still **slowing down AMD** systems (not Intel)
- **Oracle** to pay $23 million **to settle SEC charges** related to Foreign Corrupt Practices Act
- **L2 network security controls** can be **bypassed** using VLAN 0 stacking and/or 802.3 headers
- Good read from The New York Intelligencer - **Inside the Ransomware Gangs That Extort Hospitals**
- **Never-before-seen malware** has infected hundreds of **Linux** and **Windows** devices
- In a bit of scary news - **Most attackers need less than 10 hours** to find weaknesses
- **Agent Tesla RAT** delivered by **Quantum Builder** with new TTPs
- **Hacked Fast Company** sends **'obscene and racist' alerts** via Apple News
- Sophisticated Covert **Cyberattack Campaign, STEEP#MAVERICK**, Targets Military Contractors
- **Hackers** now sharing cracked **Brute Ratel** post-exploitation kit online
- **Chaos** is a Go-Based **Swiss Army Knife Of Malware**
- **Mandiant** report on Bad VIB(E)s Part One: Investigating Novel **Malware Persistence Within ESXi Hypervisors**
- New **Royal Ransomware** emerges in multi-million dollar attacks
- **Microsoft** report on **ZINC** Threat Actor weaponizing open-source software
- **Brave browser** to start blocking annoying **cookie consent** banners
- **Microsoft** guidance on **Top 10 ways to secure your data** - Best practices for small and medium sized businesses
- **Microsoft Edge** can now make **desktop web apps** feel more native
- **M365 Backup**: Why is it imperative to protect Microsoft Office 365?
- **Microsoft Edge** and **Microsoft Defender Smartscreen,** adding more Phishing and Threat Intelligence sensors
- **Microsoft** to let Office 365 users report **Teams phishing** messages
- Amazon-themed campaigns of **Lazarus APT** (aka **Hidden Cobra**) in the Netherlands and Belgium
- **Los Angeles Unified School District** rejects paying ransom to **Vice Society**, which then published the stolen data