RED-N Managed Security
Weekly Update

Week ending September 16, 2022

*Headline **NEWS***

- **Microsoft** September 2022 **Patch Tuesday** fixes zero-day used in attacks, 63 flaws
  - **Windows 10 Update KB5017308 causes issues** when creating/copying files via **GPO**
- **Microsoft** issues **critical security updates** as PCs attacked through zero-day flaw
- **Microsoft issues patch** for serious security vulnerability affecting everything from **Windows 7** to Windows 11
- **Cisco** released a number of product advisories and patches
- **SAP Security Patch** Day – September2022, 8 new items, and 5 item updates
- **Adobe** released security updates for 7 different products
- **Trend Micro** released a critical update for an RCE and more for **Apex One**
- **CISA** launches incident, ransomware **reporting rulemaking RFI** related to **CIRCIA**
- **Apple** released zero-day fixes on Monday for the newly released **iOS 16** and older versions
- As reported last week, Thousands of **QNAP NAS** devices have been hit by **DeadBolt ransomware**
- **CISA**'s 5th Annual **National Cybersecurity Summit** coming to Atlanta, GA
- **Lenovo** released multiple **BIOS** Security Vulnerability updates
- Patch your **Mitel VoIP** systems, **Lorenz ransomware** gang is back on the prowl
- **Uber** confirmed reports of an **organization-wide cybersecurity breach** – as bad as it gets

Other News Events of Note

- **WordPress Zero-Day** Vulnerability in **WPGateway** Actively Exploited in the Wild
- Draft **EU** AI Act **regulations** could have a **chilling effect on open source** software
- Binarly Finds Six **High Severity Firmware Vulnerabilities** In **HP** Enterprise Devices
- There's a **New vCenter Converter** Beta out in limited release
- **Lorenz Ransomware** Group Cracks **Mitel MiVoice** And Calls Back For Free
- **Google** Completes Acquisition of **Mandiant**
- **Cisco Talos** shares insights related to recent **cyber attack on Cisco**
- **Montenegro** wrestles with **massive cyberattack**, Russia blamed
- **U-Haul** discloses **data breach** exposing customer driver licenses
- Eagle Mountain City, Utah falls victim to **BEC cybercrime**, loses nearly $1.13 million
- **VMware** released **ESXi 7.0U3g** – only bug fixes this time, so YMMV
- **SEC** charges **VMware** with misleading investors by obscuring financial performance
- **US** to 'choke off' **China**'s access to key **computer chips**
- **Steam** users warned of sophisticated **browser-in-the-browser** phishing **attack**
- **Twitter**'s Sacramento, CA **datacenter melted down** due to heat on Labor Day
- **FBI** warns of **vulnerabilities** in **medical devices** following several **CISA** alerts
- **Attackers** Can **Compromise** Most **Cloud Data** in Just 3 Steps
- Microsoft, Cloud Providers Move to **Ban Basic Authentication**
- Undermining **Microsoft Teams Security** by Mining Tokens
- **SparklingGoblin APT** Hackers Using New **Linux** Variant of **SideWalk Backdoor**
- **US Treasury Blacklists** Several More **Bitcoin Addresses** Allegedly Tied to Iran Ransomware Attacks
- DuckDuckGo, Proton, Mozilla throw weight behind **bill targeting Big Tech 'surveillance'**
- **PsExec** rewritten to use port 135 instead of 445 giving **hackers** more wiggle-room
- Researchers Detail **OriginLogger RAT** — Successor to Agent Tesla **Malware**
- **Daixin Ransomware** gang threatens 1m-plus medical record leak
- **Los Angeles CA, schools** chief **given** rare **emergency authority** to deal with cyberattack
- **Phishing** Campaign Targets Greek Banking Users
- **Browser-in-the-browser attacks** – watch out for windows that aren't! – good technical breakdown
- **VMware** announces **Ransomware Recovery as a Service** and Data Protection vision
- Implementing a Zero Trust strategy **after compromise recovery**
- **Microsoft 365 apps** will now **update** themselves as if by magic - a new way without disrupting your day
- Spyware, Ransomware, Cryptojacking **Malware** Increasingly Detected **on ICS Devices**
- **White House releases** post-SolarWinds federal software **security requirements**
- **Trojanized Putty app** put out by North Korea, delivered via WhatsApp as a job offer
- **Akamai** stopped new **record-breaking** 704.8 Mbps **DDoS attack** in Europe
- **Malvertising on Microsoft Edge's News Feed** pushes tech support scams
- **YouTube gaming videos** are spreading malware