RED-N Managed Security
Weekly Update

Week ending September 9, 2022

*Headline **NEWS***

- **QNAP** patches **zero-day** used in new Deadbolt **ransomware attacks**
- **Interpol** and local Police **dismantled** an Asian **Sextortion ring**
- **Zyxel** has released **patches** for **NAS products** affected by a format string vulnerability
- **HP** fixes **severe Privilege Escalation bug** in pre-installed **HP Support Assistant** tool
- **Cisco** RV110W, RV130, RV130W, and RV215W **Routers** IPSec VPN **Server Authentication Bypass Vulnerability**
- **Wt1Shop seized by authorities –** marketplace for 5.85 million PII stolen records
- **US condemns** 'unprecedented' **Iranian cyberattack** against Albania
- **Microsoft** investigates **Iranian attacks** against the Albanian government
- **Google Cloud Backup and DR** are now publicly available
- **US citizenship systems vulnerable** to 'major' malicious cyberattacks, Homeland Security watchdog finds

Other News Events of Note

- Mozilla **Firefox** 104.0.1 fixes **YouTube** playback issues
- **Kaspersky** Securelist report on **the nature of cyber incidents**
- **EvilProxy Phishing-As-A-Service** With MFA Bypass Emerged In Dark Web
- **American Express**: This is a Secure Message from your **Attacker - phishing**
- China News reports **U.S. hacked China 10,000 times, stole 140GB** of critical data
- **PaloAlto**'s Unit 42 released **IAM-Deescalate**: Open Source Tool to Help **Reduce** the Risk of **Privilege Escalation**
- **AT&T Alien Labs** reports on **Shikitega -** New stealthy **malware** targeting **Linux**
- **InterContinental Hotels Group** PLC suffered a **ransomware** attack
- French security firm **Orange Cyberdefense** investigating claims of **compromise**
- European Commission to introduce **cyber requirements for Internet of Things (IoT)** products
- **PaloAlto**'s Unit 42 reports: **Mirai** Variant **MooBot** Targeting **D-Link Devices**
- TA505 Group's **TeslaGun** and **ServHelper** In-Depth **Analysis**
- **US bars** 'advanced tech' firms from **building China factories** for 10 years
- **China**'s great leap forward in chips **faces US pushback**
- **Windows File History** review: Free, **effective** continuous data protection - **backup**
- Second largest **U.S. school district** (Los Angeles United School District) hit by **ransomware**
- **Mandiant** report on **APT42**: Crooked Charms, Cons, and Compromises
- Ransomware gang's **Cobalt Strike servers DDoSed** with anti-Russia messages
- **Sliver** is gaining favor as an alternative to **Cobalt Strike**
- 200,000 **North Face accounts hacked** in credential stuffing attack
- Microsoft Security Profiling **DEV-0270: PHOSPHORUS' (aka Nemesis Kitten) ransomware** operations
- **Cisco Talos** report on **MagicRAT: Lazarus'** latest gateway into victim networks
- **CISO**'s say **stress and burnout**, not job loss as a result of a breach, are their **top personal risks**
- **GIFShell attack** creates reverse shell using **Microsoft Teams GIFs**
- **Microsoft** offers **SQL Server 2022** release candidate to **Linux** world
- What to Do Right Away **If You Click** a **Phishing Link**
- **Gmail** ditches **icon labels** in its navigation bar
- **CISA** orders agencies to **patch Chrome**, **D-Link flaws** used in attacks
- **Vulnerability Exploits**, Not Phishing, Are the **Top Cyberattack Vector** for Initial Compromise
- **$30 Million Seized**: How the Cryptocurrency Community Is **Making It Difficult for North Korean Hackers** To Profit
- **US state of Virginia** has more **datacenter capacity** than Europe or China
- **Patreon security** team **layoffs** cause backlash in creator community
- **Wordfence** Blocked Nearly 5 Million Attacks Targeting 0-Day in **BackupBuddy Plugin**
- **VMware**: **ESXi VM Performance** Tanks Up To 70% Due To Intel **Retbleed Mitigation in Linux 5.19**
- **Ligado network** will jam Iridium's receivers used by DoD: National Academies
- The **Top Cyberattacks** Against Businesses
- **Lampion malware** returns in **phishing** attacks abusing **WeTransfer**
- **SentinelLabs -** Crimeware Trends | **Ransomware** Developers Turn to **Intermittent Encryption** to Evade Detection
- **NortonLifeLock** - 8 in 10 **Websites leak** your **search terms** to 3rd parties, often advertisers