RED-N Managed Security
Weekly Update

Week ending July 1, 2022

*Headline **NEWS***

- **Microsoft** will fix Windows **RRAS**, **VPN** issues for all users in July
- **OpenSSL** issues a **bugfix** for the previous bugfix
- **AMD** investigates **RansomHouse hack** claims, theft of 450GB data
- **CISA** Warns of Active Exploitation of **'PwnKit' Linux** Vulnerability in the Wild
- Unrar Path Traversal **Vulnerability** affects **Zimbra Mail**
- Dozens of **cryptography libraries vulnerable** to private key theft
- **Microsoft Exchange** servers worldwide hit by **stealthy new backdoor** for past 15 months
- **CISA orders** agencies to **patch Windows LSA bug** exploited in the wild
- Critical **ManageEngine ADAudit Plus Vulnerability** Allows Network Takeover, Mass Data Exfiltration
- State Govt **unemployment**, **jobs services** down around the country after **cyberattack**

Other News Events of Note

- Clever **phishing** method **bypasses MFA** using Microsoft WebView2 apps
- New **Firefox** privacy feature **strips URLs of tracking** parameters
- Fake copyright infringement emails install **LockBit ransomware**
- **Ransomware** attacks **cost schools** more than **$3.5 billion** last year
- **Ransomware** attack caused ongoing **Napa Valley College** internet and phone system outage
- **BlackBasta** Ransomware group is a growing threat
- **Russian threat actors** may be **behind** June 8 **explosion** at a liquefied natural gas plant in Texas
- **US, Brazil seize 272 websites** used to illegally download music
- **Matanbuchus Loader Malware** Variant Delivering Cobalt Strike Beacons Via Spam Campaigns
- **LockBit 3.0** introduces the first ransomware **bug bounty** program
- **Millions** of free **VPN** user **records leaked**
- **Microsoft Exchange** bug abused to **hack building automation systems**
- Commonly existing **PLC Supply Chain Threats**: Multiple **critical vulnerabilities** in Codesys Runtime
- **Microsoft 365** now can prevent data leaks with **new session timeouts**
- **Raccoon Stealer** v2 – Part 1: The return of the dead
- **Gmail** gets **Material You web redesign** and 'Gmail-only' view without Chat, Meet
- **Microsoft Defender is hogging Intel CPUs** while AMD Ryzen remains unscathed
- A wide range of **routers** are **under attack** by **ZuoRAT** a new, unusually sophisticated malware
- **Microsoft 365** Users in US Face Raging Spate of **Attacks** via Voicemail Themed Email Phishing
- **Windows 10** KB5014666 update brings **new printing features**, **bug fixes**
- **YouTube** content creator **credentials** are **under siege** by **YTStealer** malware
- China reports: **US plants Trojan horse** programs in hundreds of important information systems
- **Microsoft**: **How** security leaders can **help** their teams **avoid burnout**
- **AMD hack** by **RansomHouse** due to some of its passwords being just 'password'
- **Norway** hit with **cyberattack**, temporarily suspending service
- **Amazon** fixes high-severity **vulnerability** in **Android Photos app**
- **Cyberattacks via Unpatched Systems** Cost Orgs More Than Phishing
- **FabricScape**: **Microsoft** warns of **vuln** in Service Fabric
- New in **Windows** version **22H2**: Windows Setup
- **Google Workspace** now **alerts** of critical changes to admin accounts
- Denial of Service **(DoS) Vulnerability** in **Apache httpd** "mod_sed" filter
- Publishing Giant **Macmillan** shuts down systems after **likely ransomware attack**
- **OpenSea** NFT Marketplace Suffers **Data Breach**, **warns of Phishing**
- **Google** TAG **blocked** dozens of domains used by **malactors**
- **AstraLocker 2.0** infects users with **ransomware** directly from **Word attachments**
- **XFiles** info-stealing **malware** adds support for **Follina** delivery
- **Google Docs** is getting native **eSignature support** for Workspace Individual
- **Jenkins** discloses **dozens of zero-day bugs** in multiple plugins
- A **Hive Ransomware recovery tool** from South Korea's KISA (Cyber Security Agency)