RED-N Managed Security
Weekly Update

Week ending July 15, 2022

Headline ***NEWS***

- Microsoft **July 2022 Patch Tuesday** fixes exploited zero-day, 84 flaws
  - **CISA orders** agencies to **patch** new Windows **zero-day** used in attacks
  - A well presented listing of the **Patch Tuesday updates** from **Adobe** and **Microsoft**
- **Microsoft** investigates **July updates breaking Ac**cess applications
- Ongoing **phishing** campaign can **hack** you even when you're protected with **MFA**
- Microsoft releases **PoC exploit** for **macOS sandbox** escape vulnerability
- **Vulnerabilities** in **UEFI** that could allow undectable infections affect 70 **Lenovo laptop** models
- **AstraLocker ransomware decryptors** released by Emsisoft
- **VMware patches vCenter** Server flaw disclosed in November
- **OpenSSL** Releases **Fix** for High-Severity **Vulnerability**
- **Netwrix Auditor Bug** Could Lead to Active Directory Domain Compromise
- CISA pulls the fire alarm on **Juniper** Networks **bugs** – lots of affected products
- **Digium Phones Under Attack**: Insight Into the Web Shell Implant

Other News Events of Note

- **Microsoft** moves to **new Windows development cycle** with major release every three years, feature drops in between
- New working speculative execution **attack** sends **Intel** and **AMD** scrambling
- **Windows Autopatch** from Microsoft in general availability
- **Datto** founder Austin McChord blasts **Kaseya** for post acquisition changes: '**this sucks**'
- **Buggy** 'Log in With **Google' API** Implementation Opens **Crypto Wallets** to Account Takeover
- **OrBit**: New Undetected **Linux Threat** Uses Unique Hijack of Execution Flow
- **North Korean** threat actor targets small and midsize businesses with **H0lyGh0st ransomware**
- **Beware**: Your **CyberPower UPS** with yellow glue inside could burn up
- **French** virtual mobile telephone operator **La Poste Mobile** was hit by a **ransomware** attack
- **LockBit 3.0 ransomware** virus - removal and decryption options
- **Ransomware** gang now lets you **search their stolen data**
- **London** fails to retain **Atlassian** as it heads stateside in search of a 'broader set' of investors
- **Defense contractor pays $9m** to settle whistleblower's cybersecurity allegations
- Canadian **man pleads guilty** in Tampa to **ransomware** scheme that stole millions
- **RedAlert** aka **(N13V)**: A **Ransomware** that Targets Multiple OS Platforms
- **Bitcoin Miners** Shut as Texas Power Grid Nears Brink
- **Anubis** Networks is back with new **C2** server
- **Security** for **unmanaged devices** in the Enterprise network with **Microsoft Defender for IoT**
- **Google's tool** to turn old **laptops into Chromebooks** is now widely available
- **'Luna Moth'** Group Ransoms Data Without the **Ransomware**
- **Bandai Namco** has come under a **hacker attack**. A list of possible premiers of the publisher appeared
- **ChromeLoader**: New Stubborn **Malware** Campaign
- **Microsoft** warns that **Windows 20H2** will reach **EOS** on August 9, 2022
- **Ransomware** attacks against **education** are on the rise
- **RedAlert, LILITH,** and **0mega** Leading a Wave of **Ransomware** Campaigns
- Joshua Schulte: **Former CIA hacker convicted** of 'brazen' data leak
- South **Texas hospital data breach** puts 15,000 patients at risk
- **Virginia Commonwealth University Health** data **breach** exposes private information of thousands of patients
- 'Lives are at stake': **hacking of US hospitals** highlights **deadly** risk of **ransomware**
- The Long Tail of **Log4Shell Exploitation** – the **vulnerability** that will not die
- **Apetito**, **Exela** and **G4S** among seven alleged victims of **ransomware** gang **Hive**

Cyber Insurance News

- The **cyber insurance market** has an actuarial and critical infrastructure problem
- **Ransomware** Scourge Drives Price Hikes in **Cyber Insurance**
- **Travelers** Wants Out of Contract With **Insured** That Allegedly **Misrepresented MFA** Use
- How **War** Impacts **Cyber Insurance** – read the fine print