RED-N Managed Security
Weekly Update

Week ending October 8, 2022

Headline ***NEWS***

- **Fortinet** warns admins to **patch critical** auth bypass **bug immediately**
- **Updated** information: Customer **Guidance** for Reported **Zero-day Vulnerabilities in Microsoft Exchange Server**
- Steam Gaming **Phish** Showcases **Browser-in-Browser Threat**
- **'IT security issue'** impacts **multiple hospitals** across several states
- Microsoft investigates **Windows 11 22H2 Remote Desktop issues**
- **Lloyd's of London** investigates and responds to **possible cyber attack**
- **Ransomware Group BlackByte** Bypasses "Enormous" Range of EDR Tools using trusted drivers
- **Lazarus hackers** target Dell drivers with new rootkit
- **Cisco Patches** High-Severity **Vulnerabilities** in Communications, Networking Products

Other News Events of Note

- **Microsoft** Shares Its **Experience** of Migrating Data in Times of Cyber Warfare
- **How to protect** your **Mac** against ransomware and other cyberthreats
- This could become big, fast - **Phishing** with **Chromium's Application Mode**
- The Russians didn't appreciate **Ferrari** sanctions - hit by **ransomware**, hackers leak 7 GB of data
- **BlackCat ransomware** gang claims to have hacked **US defense contractor NJVC**
- Now that **Basic Authentication is Turned Off** in Exchange Online, What Happens Next?
- Researchers Link **Cheerscrypt Linux-Based Ransomware** to Chinese Hackers
- CrowdStrike Falcon Platform Identifies **Supply Chain Attack via a Trojanized Comm100** Chat Installer
- Between ransomware and month-long engagements, **IR teams need a hug – and a nap**
- Excellent article - **Ransomware hunters**: the self-taught tech geniuses **fighting cybercrime**
- This is why we can't have nice things - **Overwatch 2 Hit By DDoS** Attacks on Launch Day
- You thought you bought software – **all you bought was a lie**
- **October is Cybersecurity Awareness Month** - Microsoft's offering
- Back to Basics: **Cybersecurity's Weakest Link** – Cybersecurity month article
- **Cybersecurity awareness tips** from Microsoft to empower your team to #BeCyberSmart
- **Virginia Mason Franciscan Health** parent company responding to 'IT security incident'
- **Hackers** maintained deep access **inside military organization's network**, U.S. officials reveal
- **Bumblebee Malware** Loader's Payloads Significantly Vary by Victim System
- How **Ransomware** Is **Causing Chaos** in American Schools
- The Majority of **PostgreSQL Servers** on the Internet are **Insecure**
- Hundreds of **Microsoft SQL servers** backdoored with new **malware**
- **Microsoft Edge 106** arrives on the Stable Channel with **more reliable web defenses**
- Nebraska - **Douglas County**'s 911 impacted by **ransomware** cryptovirus
- **Ransomware** groups operate like legitimate businesses
- Canadian **Netwalker ransomware hacker sentenced to 20 years** in U.S. prison
- **NetScaler** reclaims identity after **Citrix**, **Tibco** merge as **'Cloud Software Group'**
- **Canonical** Launches **Free Ubuntu Pro** Subscriptions for Everyone
- Delivery of Malware: **A Look at Phishing Campaigns** in Q3 2022
- Email Defenses Under Siege: **Phishing Attacks Dramatically Improve**
- **Millions** in Cryptocurrency **Vanished** as Agents Watched Helplessly
- Detecting and preventing **LSASS credential dumping attacks** – by Microsoft Security
- **TikTok**'s "secret operation" **tracks you** even if you don't use it
- **First 72 Hours of Incident Response** Critical to Taming Cyberattack Chaos
- **Avast** releases **free decryptor** for **MafiaWare666 ransomware** variants
- New **cryptojacking campaign** exploits **OneDrive vulnerability**
- The **City of Dunedin, FL** says it's dealing with a "**cybersecurity incident**"
- **Wireshark 4.0** Network Protocol Analyzer **Released**
- **Over 70%** of Taiwan businesses **report ransomware attacks in supply chain**
- EU to Make **USB-C the Standard Charging Port** Starting in 2024
- **Splunk** alleges **source code theft** by former employee who started rival biz
- Russian **Hackers** Shut Down **US State Government Websites**
- **Eternity Group** Hackers Offering New **LilithBot Malware-as-a-Service** to Cybercriminals
- IT pros suffer from serious **misconceptions** about **Microsoft 365 security**
- **Multi-Factor Authentication Fatigue** Key Factor in **Uber** Breach
- Study shows that **Google Chrome** is by far the **most vulnerable browser** in 2022