RED-N Managed Security
Weekly Update

Week ending August 26, 2022

*Headline **NEWS***

- **Microsoft** shares workarounds for **broken audio on Windows 10** after KB5015878
- **Cookie theft** threat: When multi-factor authentication (**MFA**) is **not enough**
- **CISA** is **warning** of **high-severity PAN-OS DDoS flaw** used in attacks
- **LastPass** source **code, blueprints stolen** by **intruder** – no passwords stolen according to LastPass
- Latest **Windows security update** is **locking users out** of their PCs – Bitlocker issues
- **Atlassian Bitbucket Server** and **Data Center** - Command injection vulnerability - CVE-2022-36804
- The **online scammer** targeting you could be **trapped in a South-East Asian fraud factory**
- **Plex breach** exposes usernames, emails, and encrypted passwords
- **VMware LPE Bug** Allows Cyberattackers to Feast on **Virtual Machine Data** - update VMware tools to patch
  - **VMware Tools update** addresses a local privilege escalation vulnerability (CVE-2022-31676)

Other News Events of Note

- Losses from **business email compromise (BEC)** scams are about **50 times greater than** those caused by **ransomware**
- Uncovering a **ChromeOS remote memory corruption vulnerability**
- **Microsoft** shakes up **Teams Rooms** subscriptions, **slashing prices** and altering plans
- **Ukraine** and **Poland** have signed a memorandum of understanding on **cooperation** in the field of **cyber security**
- **FDIC Issues** Crypto-Related **Cease and Desist Orders** to 5 Companies Including FTX US Exchange
- **Cyber Signals**: Defend against the new **ransomware** landscape – **insights** from **Microsoft**
- **SEC** plotting **to fine** major **Wall Street banks $1 billion** over use of banned messaging apps
- Ten key facts about **callback phishing attacks**
- **RTLS** Systems Found **Vulnerable** to **MiTM Attacks** and **Location Tampering**
- Reservations Requested: **TA558 Targets Hospitality and Travel** – Proofpoint report
- **FBI warns** of **residential proxies** used in **credential stuffing** attacks – PDF link
- **Fremont County**, CO **cyberattack**
- Microsoft finds **critical hole in operating system** that for once isn't Windows – it is in **ChromeOS**
- Over 80,000 **exploitable Hikvision cameras** exposed online
- **ETHERLED**: Air-gapped systems **leak** data **via** network card **LEDs**
- **French Hospital Ransomware** attack, they sent patients to other hospitals as a result
- Texas, **Mansfield Independent School District** Investigating **Ransomware** Attack
- The **Rise of Data Exfiltration** and Why It Is a **Greater Risk Than Ransomware**
- Legitimate **SaaS Platforms** Being Used to **Host Phishing Attacks**
- **Google researchers expose** Iranian **hackers' tool to steal emails** from Gmail, Yahoo and Outlook
- **Apple Updates Boot Camp** for Intel Macs with WiFi **Improvements and Bug Fixes**
- Before **Portland lost $1.4 million** in **BEC**, city treasurer raised red flag
- VMware **Carbon Black causing BSOD** crashes on Windows Worldwide – fixed within a few hours
- Researchers Warn of **AiTM Attack Targeting Google G-Suite** Enterprise Users – ALWAYS check the URL in the browser
- **Microsoft Defender** stomps even harder **against ransomware** in AV-TEST's **latest ranking**
- **SolarWinds CISO** Shares 3 **Lessons From** the Infamous **Attack**
- **Bug in CrowdStrike Falcon** Allows Removal of Security Agent
- Key **Findings from** the **1H 2022** FortiGuard Labs **Threat Report**
- The **Full FortiGuard Labs Report** in PDF format is here – excellent insights
- Looking for the '**Sliver**' lining: **Hunting for emerging command-and-control frameworks** – from Microsoft
- MagicWeb: **NOBELIUM's** post-compromise **trick to authenticate as anyone** – from Microsoft
- **Oracle** Faces Class-Action Lawsuit Over **Tracking 5 Billion People**
- Hackers ransomware the **Dominican Agrarian Institute**; ask for $600 thousand to return data
- **Zoom patches** make-me-root security flaw, **patches the patch**
- Major airline technology provider **Accelya attacked by ransomware** group
- **GitLab 'strongly recommends' patching** critical RCE vulnerability
- **Ransomware** updates & **1-day exploits** – report from Kaspersky
- **Phishers** who **hit Twilio** and **Cloudflare stole 10k credentials** from 136 other companies
- **Chips for America** - programs seek to restore U.S. leadership in **semiconductor manufacturing**
- Kimsuky's **GoldDragon** cluster and its **C2 operations**
- **Microsoft Security** highlights from **Black Hat USA 2022**
- **LockBit gang hit by DDoS attack** after threatening to leak Entrust ransomware data
- An **interview with initial access broker** Wazawaka
- The **O.MG Elite Cable** is a Scarily Stealthy **Hacker Tool**