RED-N Managed Security

Weekly Update

Week ending August 12, 2022

*Headline **NEWS***

- **August 2022 Patch Tuesday** | Microsoft Releases 121 Vulnerabilities with 17 Critical
- Microsoft August **Patch Tuesday** fixes **critical Secure Boot GRUB** vulnerability
    - Microsoft **blocks UEFI bootloaders** enabling Windows Secure Boot bypass
    - Microsoft warns about **Windows update fails**, UEFI update might be necessary to fix
- Microsoft: **Exchange 'Extended Protection' needed** to fully patch new bugs
- Microsoft 365 **version 2206** update pulled due to **apps crashing**
- **Microsoft Edge's** new "**Enhanced Security**" feature now available to everyone
- **Twitter** confirms **zero-day** used to expose data of 5.4 million accounts
- **US sanctions crypto mixer Tornado Cash** used by North Korean hackers
- The **SEC's cyberattack reporting rules** are seeing fierce opposition
- **Cisco hacked by Yanluowang ransomware** gang, 2.8GB allegedly stolen
- **Palo Alto** Networks: New **PAN-OS DDoS** flaw exploited in attacks
- Researchers Find **Vulnerability** in Software Underlying **Discord, Microsoft Teams**, and Other Apps
- **Ukraine's cyber chief** comes to **Black Hat** in surprise visit

Other News Events of Note

- **Hackers** are actively exploiting **password-stealing** flaw in **Zimbra**
    - **Zimbra** auth bypass bug exploited to **breach over 1,000 servers**
- **DuckDuckGo** rolls out new Microsoft blockers after backlash
- Top cybersecurity **products unveiled at Black Hat 2022**
- **Rufus**: **Microsoft is blocking** Windows **ISO** downloads
- Seven Common **Active Directory attacks** and recommended prevention tactics
- **Chromium** site **isolation bypass** allows wide range of attacks on browsers
- New **GwisinLocker ransomware** encrypts Windows and Linux ESXi servers
- **Gmail** Cross Site Scripting **(XSS) hack** earns researcher $5,000
- **North Korean hackers** target crypto experts with fake Coinbase job offers
- **Chinese hackers** use new Windows malware to **backdoor govt, defense orgs**
- **7-Eleven** stores in Denmark closed due to a **cyberattack**
- **Twilio hacked** by **phishing** campaign targeting internet companies
- Higher risks and premiums are creating **critical gap in cyber insurance**
- A Single **Flaw Broke** Every Layer of **Security in MacOS**
- **Targeted attack** on industrial enterprises and public institutions
- Over 9,000 **VNC servers exposed online** without a password
- **Google** hit with **lawsuit** for dropping **free Workspace** apps
- **SOVA malware** adds ransomware feature to **encrypt Android** devices
- Your next **Phishing** email may come straight **from PayPal**
- Change the level of **protection** in the **Microsoft Junk Email Filter**
- **Malware-packed Chinese apps** found on **Mac App Store**
- **China** could be **reviewing security bugs** before tech companies issue patches
- **UAE** reports 3.4 million **phishing attacks** in quarter two
- **Chinese New Backdoor** Deployed For Cyberespionage
- **Linux** kernel **privilege escalation** vulnerability CVE-2022-2590
- **Multiple Vulnerabilities** Discovered in **Device42** Asset Management Appliance
- **LogoKit** update – The **phishing kit** leveraging Open Redirect Vulnerabilities
- What to watch for as **'Hacker Summer Camp'** gets underway in Las Vegas
- **Meta** Takes Action Against **Cyber Espionage** Operations Targeting **Facebook**
- **Maui ransomware** operation linked to **North Korean 'Andariel'** hackers
- **Cyberattack** forces **Ski-Doo maker BRP** to suspend operations
- VMware Report Warns of **Deepfake Attacks and Cyber Extortion**
- **Kali Linux 2022.3** adds 5 new tools, updates Linux kernel

- How **older security vulnerabilities** continue to pose a threat
- **Intel 'Sunny Cove'** SGX **Vulnerability** Discovered
- **Microsoft 365 outage** triggered by **Meraki** firewall false positive
- **Windows 11 Encryption** May Damage Data, Microsoft Says
- **FBI** helps **stop cyberattack** targeting Nebraska hospital
- **Google** now **blocks** Workspace account **hijacking** attempts **automatically**
- Automotive supplier breached by **3 ransomware gangs in 2 weeks**
- **Stegomalware** Surge - Attackers Using File, **Video, Image to Hide Malware**
- Hacker uses **new RAT malware in Cuba Ransomware** attacks
- **Conti** extortion gangs behind surge of **BazarCall phishing attacks**
- **Ransomware** gangs move away from exploiting **Microsoft Office macros**
- Jacksonville FL **Sheriff's Office** attacked by **ransomware**
- The **US Offers** a **$10M Bounty** for Intel on **Conti Ransomware** Gang
- Many **ZTNA, MFA** Tools Offer **Little Protection** Against Cookie Session Hijacking Attacks
- **BlueSky Ransomware**: Fast Encryption via Multithreading
- **Zeppelin ransomware** may encrypt devices multiple times in attacks
- **Starlink** Successfully **Hacked** Using $25 Modchip
- **Google** wants to remind you that using **2FA doesn't have to be a... drag**
- **PyPI Package** 'secretslib' Drops **Fileless Linux Malware** to Mine Monero
- Ex-CIA security boss predicts **coming crackdown on spyware**
- **Zoom** Is Great for Remote Work and **Remote Code Execution**
- **Cedar Rapids, IA schools** make **ransom payment** in regard to cyber security incident
- Threat Group **APT-C-35**: New Windows Framework Revealed
- **Google fined $60 million** over Android location data collection
- **Linux** Gets New Patch To Fix AMD **Retbleed Mitigation**
- **Ransomware** attack cripples **HanesBrands** sales in $100 million blow
- **Microsoft Outlook** to roll out controversial **change** to where it places apps
- How to Attack and **Remediate Excessive Network Share Permissions** in AD Environments
- Don't be surprised if your organization suffers **multiple cyberattacks**
- Four **Flaws**, Other **Weaknesses** Undermine **Cisco ASA Firewalls**