RED-N Managed Security
Weekly Update

Week ending August 19, 2022

*Headline **NEWS***

- **Microsoft's Secure Boot fix** sends some PCs into BitLocker Recovery
- New **macOS 12.5.1** and **iOS 15.6.1** updates **patch "actively exploited" vulnerabilities**
- **Microsoft** will turn off **TLS 1.0 and 1.1** in Internet Explorer and EdgeHTML on September 13
- **Exploit** out for **critical Realtek flaw** affecting many networking devices – **Zero-Click**
  - For a list of **affected devices** that use the **Realtek** chip in question see this github link
- CVE-2022-30216 - Authentication coercion of the **Windows "Server" service**
- Snyk finds **PyPi malware** that **steals Discord** and **Roblox credential** and **payment** info
- Protect against **AiTM/ MFA phishing attacks** using Microsoft technology
- **Chrome browser** gets **11 security fixes** with **1 zero-day – update now!**
- **CISA** added **7 new vulnerabilities** to their **known exploits** catalog
- Users of **Zoom** on **Macs** told to **update app** as company issues **security fix**

Other News Events of Note

- **Novant** warns patients of **data breach**; 1.3 million notification letters mailed
- Disrupting **SEABORGIUM**'s ongoing **phishing** operations
- Senior Care Giant **Avamere** Suffers **Cybersecurity Breach**
- **Black Hat** and **DEF CON** visitors differ on physical risk management
- **CISA Director** Praises Congress and International Cybersecurity Cooperation
- **Callback phishing** attacks see **massive 625% growth** since Q1 2021
- **Argentina**'s Judiciary of Córdoba **hit by PLAY ransomware** attack
- **Credential phishing** attacks **skyrocketing**, 265 brands impersonated in H1 2022
- **CISA** breaks down **Zeppelin Ransomware**
- **Test antivirus software** for Windows 10 - June 2022 Report
- **Hackers** Took Over a **Commercial Satellite** to Broadcast Hacker Movies
- **Scam email** claims to be from **Microsoft**, warning of unusual activity
- **Threat** in your **browser**: what dangers innocent-looking **extensions** hold for users
- Detecting a **Rogue Domain Controller** - **DCShadow Attack**
- **Torch.AI** wins **Pentagon** 'insider threat' cybersecurity **contract**
- The new **USB Rubber Ducky** is more dangerous than ever
- Configure **attack surface reduction** in **Microsoft Defender** using **Group Policy** or **PowerShell**
- White Hat **Hacker** at DefCon **Jaikbreaks Tractor** to Play Doom
- **US** announces **export ban** on **advanced semiconductor manufacturing** tech
- Nozomi Networks Researchers Reveal **Zero-Day RTLS Vulnerabilities**
- **CohnReznick** data breach **class action settlement**
- **Microsoft's macOS Tamper Protection** hits general availability
- **Microsoft** and **Canonical** announce **native .NET availability** in Ubuntu 22.04 hosts and containers
- **Pentagon** put **microgrid technology** to the test at **DEF CON**, drawing on **hackers'** ingenuity
- Is the **drop in ransomware numbers** an illusion? Experts divided
- **TechCrunch** launches **TheTruthSpy spyware lookup tool**
- Criminals posting **counterfeit Microsoft products** to get **access** to victims' **computers**
- **BlackByte ransomware** gang is back with **new extortion tactics**
- **Iran-linked hacking group** is targeting Israeli shipping
- **Janet Jackson** had the power to **crash laptop computers**
- **Google blocked largest DDoS** to date – 46 million RPS
- **LibreOffice 7.4 released** with MS Office compatibility improvements
- How **US Teen Rickrolled** His **High School District** in Illinois
- **UK Water Supplier** Hit by 'Extremely Concerning' **Cyberattack**
- **Apex Capital** blames **malware attack** for 'unplanned system outage' – **BlackByte** claims responsibility
- **LockBit** claims **ransomware** attack on security giant **Entrust**, leaks data
- **APT29** Continues Targeting **Microsoft 365**, deactivates logging
- A Deep Dive Into **Black Basta Ransomware**
- **Bumblebee Loader** – The High Road to Enterprise Domain Control
- **Amazon** fixes **Ring Android app flaw** exposing camera recordings
- **US** deployed **cyber 'hunt forward' team** to Croatia
- **Hackers** steal crypto from **Bitcoin ATMs** by exploiting zero-day bug

> "The vast majority of cybercrime today is successful because it exploits the people behind the keyboard"
>
> Crane Hassold, director of threat intelligence, Abnormal Security