RED-N Managed Security

Weekly Update

Week ending January 14, 2023

*Headline **NEWS***

- Microsoft ASR and Defender issue create ASRmageddon for admins worldwide on Friday the 13th
- Latest Defender Update KB2267602 Bug Deletes Shortcuts
- Microsoft Patch Tuesday, January 2023 Edition
- Windows 11 KB5022303 and KB5022287 cumulative updates released
- Microsoft fixes issue causing 0xc000021a blue screen crashes
- Microsoft fixes Windows 11 22H2 broken OOBE but app installs are now failing
- Auth0 fixes RCE flaw in JsonWebToken library used by 22,000 projects
- JsonWebToken Security Bug Opens Servers to RCE
- Cisco warns of auth bypass bug with public exploit in EoL routers
- AMD Quietly Lists 31 New CPU Vulnerabilities, Issues Patch Guidance
- Fortinet: Hackers Exploit Zero-Day Vulnerability In VPN
- Hackers Actively Exploiting Critical "Control Web Panel" RCE Vulnerability

Ransomware and Malware News

- DNV's Fleet Management Software Hit By Cyber Attack
- SCATTERED SPIDER Attempts to Avoid Detection with Bring-Your-Own-Driver Tactic
- CISA orders agencies to patch Exchange bug abused by ransomware gang
- Over 1,300 fake AnyDesk sites push Vidar info-stealing malware
- Russian Turla Hackers Hijack Decade-Old Malware Infrastructure to Deploy New Backdoors
- Hackers Distributing Malicious Visual Studio Extensions to Attack Developers
- Hackers push fake Pokemon NFT game to take over Windows devices
- US Supremes deny Pegasus spyware maker's immunity claim
- Lorenz ransomware gang plants backdoors to use months later
- Dark Pink: New APT group targets governmental, military organizations in APAC, Europe
- Raspberry Robin's botnet second life
- StrongPity espionage campaign targeting Android users
- Hackers leak sensitive files after attack on San Francisco transit police
- Hackers hit websites of Danish central bank, other banks
- 22,000 orders, most for $12.71, in a weekend? Powell brothers lacrosse company hit by cyber attack
- Hundreds of SugarCRM servers infected with critical in-the-wild exploit
- Royal Mail halts international services after cyberattack
- Global Cyber-Attack Volume Surges 38% in 2022
- Guardian confirms it was hit by ransomware attack
- Cyberattack takes down land-records management system used by many Vermont towns
- RAT malware campaign tries to evade detection using polyglot files
- IcedID Malware Strikes Again: Active Directory Domain Compromised in Under 24 Hours
- IcedID botnet operators exploit Google ads in their campaign
- Why are there so many cyberattacks lately? An explainer on the rising trend
- Ransomware gangs ditch encryption, embrace data extortion
- Dozens of clerk of court offices in Louisiana offline following Cott Software cyber attack

Other News Events of Note

- ChatGPT is making it much easier for script kiddies to create malware
- Microsoft is adding OpenAI writing tech to Office
- New Study Uncovers Text-to-SQL Model Vulnerabilities Allowing Data Theft and DoS Attacks

- Rufus gets updated Fido script to fix broken Windows ISO downloads
- Microsoft's VALL-E can imitate any voice with just a three-second sample
- Researchers Hacked California's New Digital License Plates
- Identity Thieves Bypassed Experian Security to View Credit Reports
- The dark web's criminal minds see IoT as the next big hacking prize
- Unwrapping Ursnifs Gifts - The DFIR Report
- German regulator warns of new banking and crypto malware 'Godfather'
- InfoSec Handlers Diary Blog - SANS Internet Storm Center
- A Siemens S7-1500 Logic Controller Flaw Raises the Specter of Stuxnet
- Threat Intelligence Report - Check Point Research
- Palantir Announces Strategic Partnership with Cloudflare Focused on Cloud Cost Optimization
- Microsoft 365 Basic gives you 100GB of OneDrive space (but no Office) for $2
- Corrupted file to blame for FAA aviation stoppage that delayed thousands of flights
- Google Chrome 109 now available, last version to support Windows 7 and 8.1
- 7 Reasons Global Attacks Will Rise Significantly in 2023
- Fake job offers trick applicants and steal information
- Microsoft: Exchange Server 2013 reaches end of support in 90 days
- How to Enable Memory Saver in Google Chrome to Reduce RAM/CPU Usage
- Zoom fixed several LPEs
- Fake AMD Radeon drivers reveal a deeper Google problem
- Microsoft fixes Windows database connections it broke in November
- Rufus alternative Ventoy fixes Windows 11 bypass related bug, VHDX booting issue, and more
- "Security Vulnerability" In CLEAR Leads To Calls For Members To Have IDs Checked At Security
- Windows 11 Pro will soon disable insecure SMB guest authentication by default
- Microsoft fumbles zero trust upgrade for some Asian customers
- China's new quantum code-breaking algorithm raises concerns in the US
- Chuck E. Cheese still uses floppy disks in 2023, but not for long
- A fifth of passwords used by federal agency cracked in security audit

Cyber Insurance News

- Companies warned to step up cyber security to become 'insurable'
- Cyber Insurance Market to Generate USD 48,328.4 Million Revenue in 2030
- Is your cyber coverage ready? Cyber insurance uptake is rising, but coverage questions remain
- Cowbell advises SMEs on cyber catastrophe preparation