



RED-N Managed Security

Weekly Update

Week ending December 10, 2022

Headline NEWS

- [Rackspace confirms Ransomware Attack across some of its servers](#)
- [Cole & Van Note Announces Filing of Rackspace Ransomware/Data Breach Class Action](#)
- [Cisco discloses high-severity IP phone bug with exploit code and no patch – workaround may break your phone system](#)
- [Microsoft: November updates break ODBC database connections](#)
- [Ping bug potentially allows remote takeover of FreeBSD systems](#)
- [Severe AMI MegaRAC flaws impact servers from AMD, ARM, HPE, Dell, others](#)
- [WordPress Hit With Multiple Vulnerabilities In Versions Prior To 6.0.3](#)
- [Amnesty International Canada says it was hacked by Beijing](#)
- [Researchers found security holes in IBM's cloud infrastructure](#)
- [Internet Explorer 0-day including bits left in Edge exploited by North Korean actor APT37](#)
- [LastPass Security Breach Worse Than Initially Reported](#)
- [VMware vCenter Server 7.0 Update 3i Release Notes – several CVEs have been patched](#)
- [Heads Up – VMware ESXi 8.0 Host Client unable to attach existing virtual disk to VM](#)

Other News Events of Note

- [RIP Passwords? Passkey support rolls out to Chrome stable](#)
- [Malicious Actors Exploit TikTok 'Invisible Challenge' to Steal Users' Info](#)
- [U.S. again delays deadline for Real IDs, until May 2025](#)
- [Sneaky hackers reverse defense mitigations when detected continue to acquire persistence](#)
- [Infostealer Malware popularity spikes on the Dark Web](#)
- [Preparing for a Russian cyber offensive against Ukraine this winter - Microsoft On the Issues](#)
- [Nobody should be surprised that Exposed RDP Servers Actively Targeted By Hackers](#)
- [Ransomware attack forces French hospital to cancel operations and transfer patients](#)
- [Ransomware attackers say AllMS 'deadline' has ended and they will publish](#)
- [Want to detect Cobalt Strike on the network? Look to process memory](#)
- [Ventoy Tool Can Boot Multiple OSes From a Single USB Drive](#)
- [The Story of a Ransomware Turning into an Accidental Wiper](#)
- [Kali Linux 2022.4 adds 6 new tools, Azure images, and desktop updates](#)
- [SpaceX Unveils Starshield, an Encrypted Starlink Service for Governments](#)
- [The Rise of the Machines: AI A Dangerous New Attack Vector](#)
- [Bitwarden adopts passwordless authentication for its web vault](#)
- [Largest mobile malware marketplace identified by Resecurity in the Dark Web](#)
- [Austin, TX - Ransomware attack limiting some Travis Central Appraisal District services](#)
- [Microsoft plots superpowered Bing app to break the dominance of Apple and Google](#)
- [Poetic injustice - Scammers Are Scamming Other Scammers Out of Millions of Dollars](#)
- [SentinelOne \(S\) Reports Q3 Loss, Tops Revenue Estimates](#)
- [Vice Society Ransomware Attackers Targeted Dozens of Schools in 2022](#)
- [Zerobot – New Go-Based Botnet Campaign Targets Multiple Vulnerabilities](#)
- [CloudSEK claims it was hacked by another cybersecurity firm](#)
- [For Cyberattackers, Popular EDR Tools Can Turn into Destructive Data Wipers](#)
- [Ransomware gangs targeted U.S. companies the most in first half of 2022](#)
- [Excellent List - Windows CMD Commands: Basic CMD Prompt Commands List](#)
- [New Ransom Payment Schemes Target Executives, Telemedicine](#)
- [The FBI isn't happy with new iCloud end-to-end encryption](#)
- [Understanding NIST CSF to assess your organization's Ransomware readiness](#)
- [Hackers use new Fantasy data wiper in coordinated supply chain attack](#)
- [US government to spend \\$1.5 billion on alternative to Huawei and ZTE 5G telecom gear](#)
- [Huntress - Threat Advisory: Qakbot Activity Is Rising](#)
- [Excellent CISA info graphic on phishing](#)
- [The Average Person's Corporate Email Account is Worth about \\$2 on Automated Dark Web Markets](#)
- [Antwerp Belgium's city services down after hackers attack digital partner](#)
- [Microsoft Edge 109 is the last version to support Windows 7/8.1](#)
- [MuddyWater Hackers use corporate email accounts used to send MSP remote access tool](#)
- [TikTok Banned on Govt. Devices; Will Private Sector Follow Suit?](#)
- [Breaking the silence - Recent Truebot Malware activity – by Cisco Talos](#)
- [Microsoft Alerts Cryptocurrency Industry of Targeted Cyber Attacks](#)

