



Week ending August 5, 2022

### Headline NEWS

- [VMware urges admins to patch critical auth bypass bug](#) immediately
- [Cisco fixes critical remote code execution bug](#) in VPN routers
- Millions of [Arris routers](#) are [vulnerable](#) to path traversal attacks
- [Critical RCE Bug Could Let Hackers Remotely Take Over DrayTek Vigor Routers](#)
- [Microsoft releases Winget 1.3](#) with portable apps, documentation, and install notes support
- Almost two years after [Apple's M1](#) launch, [Microsoft Teams goes native](#)
- [Microsoft warns Windows 10 KB5015878 \(July\) could break notification area](#)
- [Twitter confirms zero-day](#) used to expose data of [5.4 million accounts](#)

### Other News Events of Note

- [Large-Scale AiTM Attack](#) targeting enterprise users of [Microsoft email services](#)
- [Ransomware Bill](#) Passes House
- [Chromium Browsers](#) Allow [Data Exfiltration](#) via Bookmark Syncing
- [Microsoft Defender Experts for Hunting](#) now generally available
- [Ransomware](#) affects 1 in 40 – Are you at risk?
- [BlackCat ransomware](#) claims attack on European gas pipeline
- [Microsoft Outlook](#) is [crashing](#) when [reading Uber](#) receipt emails
- [Gootkit Loader](#) Resurfaces with Updated Tactic to Compromise Targeted Computers
- [Australian Hacker Charged](#) with Creating, Selling Spyware to Cyber Criminals
- Publicly Reported [Ransomware Incidents](#) are only the [tip of the iceberg](#)
- [Hackers](#) stole passwords for accessing [140,000 payment terminals](#)
- [Nomad](#) token bridge [drained of \\$190M](#) in funds in security exploit
- [Malicious browser extension](#) targets Gmail and AOL users
- [Hackers](#) have found a new way to [hijack](#) your [Discord account](#)
- [Microsoft](#) announces [new](#) external attack surface audit [tool](#)
- [EU missile maker MBDA](#) confirms [data theft extortion](#), denies breach
- [If using, update now!](#) [GnuTLS](#) patches [memory mismanagement bug](#)
- [How Leaked Twitter API Keys](#) Can be Used to Build a Bot Army
- [Chinese Hackers](#) Using New [Manjusaka Hacking Framework](#) Similar to Cobalt Strike
- [North Koreans](#) Steal [LinkedIn Resumes](#) in Crypto Job Search Scam
- [NVIDIA 515.65.01 Linux Driver](#) Released With Fixes
- Thousands of [Solana wallets](#) drained in multimillion-dollar exploit
- [Backblaze Drive Stats](#) for Q2 2022 – If you're shopping for a drive, check here
- [New Linux malware "RapperBot"](#) brute-forces [SSH servers](#) to breach networks
- German semiconductor giant [Semikron](#) says [hackers encrypted](#) its [network](#)
- [Woody RAT](#): A new feature-rich [malware](#) spotted in the wild
- [Cloned Atomic Wallet](#) website is pushing [Mars Stealer malware](#)
- [Hackers Exploited Atlassian Confluence Bug](#) to Deploy [LJI Backdoor](#) for Espionage
- [American Express, Snapchat](#) Open-Redirect [Vulnerabilities Exploited](#) in Phishing Scheme
- [Cybersecurity agencies](#) reveal last year's [top malware](#) strains
- [Bumblebee Malware Email Lures](#) and [File Sharing Services](#) Lead to [Malware](#)
- [New York](#) Becomes First State to [Mandate CLE in Cybersecurity, Privacy and Data Protection](#)
- [Spanish research agency](#) still recovering after [ransomware](#) attack
- [Rufus 3.20](#) is out with automatic local account creation, and more for [Windows 11](#)
- ["Huge flaw"](#) threatens [US emergency alert system](#), DHS researcher warns
- [Attackers](#) leveraging [Dark Utilities "C2aaS"](#) platform in malware campaigns
- [Hackers](#) try to [extort survey firm QuestionPro](#) after alleged data theft
- [UK regulator](#) makes U-turn on [Avast-Norton cyber security deal](#), clearing way for acquisition
- [CyRC Vulnerability Advisory](#): Local privilege escalation in [Kaspersky VPN](#)
- [Threat Actors](#) Pivot to [Abusing Explorer](#) and Other [LOLBins](#) via [Windows Shortcuts](#)
- [Slack](#) resets passwords after exposing hashes in invitation links

