



Week ending July 29, 2022

Headline NEWS

- [Oakbot Resurfaces With New Playbook](#)
- [Beware New Windows Vulnerability With Remote Search Window Access](#)
- [Critical Filewave MDM Vulnerabilities Allow Attackers Full Mobile Device Control](#)
- [Critical security vulnerability in Grails could lead to remote code execution](#)
- [Update Google Chrome now! New version includes 11 important security patches](#)
- [LibreOffice Releases Software Update to Patch 3 New Vulnerabilities](#)
- [Critical Samba bug could let anyone become Domain Admin – patch now!](#)
- [Serious OAuth vulnerability In Grafana Could Allow Account Takeover](#)
- [US govt warns Americans of escalating “Robotext” SMS phishing attacks](#)

Other News Events of Note

- [Hackers scan for vulnerabilities within 15 minutes of disclosure – and other insights from over 600 IR cases](#)
- [Hackers exploited PrestaShop zero-day to breach online stores](#)
- [CosmicStrand: the discovery of a sophisticated UEFI firmware rootkit](#)
- [Computer glitches harmed 'nearly 150' patients after Oracle Cerner system go-live](#)
- [Source code for Rust-based info-stealer released on hacker forums](#)
- [Raccoon Stealer v2 – Part 1: The return of the dead - information stealer](#)
- [BlackCat attacks SRM Technologies then taunts victim on LinkedIn](#)
- [iCloud Passwords for Windows now supports 2FA code generator](#)
- [Volusion e-commerce platform data breach \\$4.3M class action settlement](#)
- [VR Malware Lets Hackers Into Your Headset](#)
- [Amadey Bot Being Distributed Through SmokeLoader](#)
- [Discord, Telegram Services Hijacked to Launch Array of Cyberattacks](#)
- [LockBit Ransomware Group Augments Its Latest Variant, LockBit 3.0, With BlackMatter Capabilities](#)
- [Google Chrome is blocking all downloads from Portable Apps – says they are “dangerous”](#)
- [Larry Ellison \(Oracle\) and Satya Nadella \(Microsoft\) Create the Multi-Cloud Future](#)
- [Microsoft: Malicious IIS extensions quietly open persistent backdoors into servers](#)
- [LinkedIn phishing target employees managing Facebook Ad Accounts](#)
- [AMD 22.7.1 driver has major OpenGL optimizations and Windows 11 22H2 support](#)
- [Microsoft: Windows, Adobe zero-days used to deploy KNOTWEED's Subzero malware](#)
- [Risk-Based Approach to Vulnerability Patching - Vulnerability Management 10x faster](#)
- [Kansas MSP NetStandard shut down cloud services to fend off cyberattack](#)
- [Apple network traffic takes mysterious detour through Russia for 12 hours](#)
- [Gmail's Material Redesign is Officially Rolling Out to Everyone](#)
- [EU found evidence employee phones compromised with Pegasus](#)
- [DDoS Attack Trends in 2022: Ultrashort, Powerful, Multivector Attacks](#)
- [New 'Robin Banks' phishing service targets banks: BofA, Citi, and Wells Fargo](#)
- [U.S. doubles reward for tips on North Korean-backed hackers](#)
- [Phishing Attacks Skyrocket with Microsoft and Facebook as Most Abused Brands](#)
- [Average Data Breach Costs Soar to \\$4.4M in 2022](#)
- [Phishing Attacks Blast Off from InterPlanetary File System](#)
- [SharpTongue aka Kimsuky Deploys Clever Mail-Stealing Browser Extension “SHARPEXT”](#)
- [APT-Like Phishing Threat Dynamically Mirrors Landing Pages to harvest credentials and tokens](#)
- [Breach Exposes Users of Microleaves Proxy Service](#)
 - [Proxy Service Permanently Shuts Down Operations after Breach](#)
- [Mozilla has released Firefox 103, jam-packed with new features](#)
- [Who's Behind the Keyboard doxes cyber-criminals](#)
- [Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022](#)
- [LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Defender Security Tool](#)
- [Dahua IP Camera Vulnerability Could Let Attackers Take Full Control Over Devices](#)
- [Linux malware soars to an all-time high in the first half of 2022, although Windows still leads the pack](#)

