Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents

Whole Foods supplier making progress on restoration after cyberattack left shelves empty

therecord.media

United Natural Foods (UNFI) said it is now able to receive orders and deliver products to grocery stores across North America after a cyberattack limited its ability to operate last week.

Scattered Spider hackers targeting insurance industry following retail hits, Google warns

therecord.media

A group of hackers behind a recent string of attacks on retail stores in the U.K. and U.S. has shifted its focus to insurance firms in recent days, according to cybersecurity researchers.

Weekly Recap: iPhone Spyware, Microsoft 0-Day, TokenBreak Hack, AI Data Leaks and More

thehackernews.com

Some of the biggest security problems start quietly. No alerts. No warnings. Just small actions that seem normal but aren't. Attackers now know how to stay hidden by blending in, and that makes it hard to tell when something's wrong.

1,500+ Minecraft Players Infected by Java Malware Masquerading as Game Mods on GitHub

thehackernews.com

"The malware was impersonating Oringo and Taunahi, which are 'Scripts and macros tools' (aka cheats). Both the first and second stages are developed in Java and can only be executed if the Minecraft runtime is installed on the host machine."

BlueNoroff Deepfake Zoom Scam Hits Crypto Employee with macOS Backdoor Malware

thehackernews.com

The North Korea-aligned threat actor known as BlueNoroff has been observed targeting an employee in the Web3 sector with deceptive Zoom calls featuring deepfaked company executives to trick them into installing malware on their Apple macOS devices.

Industry Updates

Legislation, Business, Updates, Related Technologies

Bipartisan bill aims to create CISA-HHS liaison for hospital cyberattacks

therecord.media

Lawmakers want to create a liaison between the federal cybersecurity agency and the Department of Health and Human Services to allow for better coordination on cyberattacks and more robust threat information sharing.

Judge overturns Biden-era HHS rule on HIPAA protections for those seeking reproductive care

therecord.media

A federal judge on Wednesday overturned key aspects of a Biden-era Department of Health and Human Services (HHS) rule bolstering privacy protections for personal health information related to abortion and gender-affirming care.

Meta Starts Showing Ads on WhatsApp After 6-Year Delay From 2018 Announcement

thehackernews.com

The ads are expected to be displayed on the Updates tab through its Stories-like Status feature, which allows ephemeral sharing of photos, videos, voice notes, and text for 24 hours. These efforts are "rolling out gradually," per the company.

Backups Are Under Attack: How to Protect Your Backups

thehackernews.com

Ransomware has become a highly coordinated and pervasive threat, and traditional defenses are increasingly struggling to neutralize it. Today's ransomware attacks initially target your last line of defense — your backup infrastructure. Before locking up your production environment, cybercriminals go after your backups to cripple your ability to recover, increasing the odds of a ransom payout.
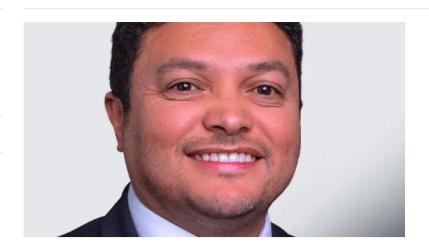
Proactive Approaches to Identify Cyberthreats

www.isaca.org

Waiting for an attack to occur before taking action is no longer a viable security strategy. Instead, a proactive stance is essential to identify potential threats early, minimize their impact and safeguard valuable assets. Embracing proactive measures empowers organizations to stay ahead of malicious actors and build a more resilient security posture.

DuckDuckGo beefs up scam defense to block fake stores, crypto sites - BleepingComputer

www.bleepingcomputer.com

The DuckDuckGo web browser has expanded its built-in Scam Blocker tool to protect against a broader range of online scams, including fake e-commerce, cryptocurrency exchanges, and "scareware" sites.

Fortifying the Operational Technology Sector: Battle-Tested Cyber Resilience Strategies - ISACA

www.isaca.org

Recent incidents highlight the severity of these threats. In May 2024, the NSA, FBI, and NCSC-UK issued an urgent warning to OT operators about rising hacktivist activity. These groups targeted insecure OT environments with simple yet effective tactics, exploiting outdated software lacking basic controls, such as multi-factor authentication (MFA).

ChatGPT will analyze Gmail emails, manage schedule on Google Calendar - BleepingComputer

www.bleepingcomputer.com

ChatGPT appears to be testing support for Gmail and Google Calendar integration. This will allow users to summarise emails and create events. ChatGPT already supports Gmail integration, but it's …

External Quick links

- AIScoop
- BleepingComputer
- Cisco Talos Intelligence Group
- CSO Online
- CyberScoop
- Cybersecurity Dive
- Cyware
- CyberWire
- FedScoop
- Government Executive
- Government Technology
- ISACA
- ISSA International
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- Schneier on Security
- SC Media
- StateScoop
- The Hacker News
- The Record