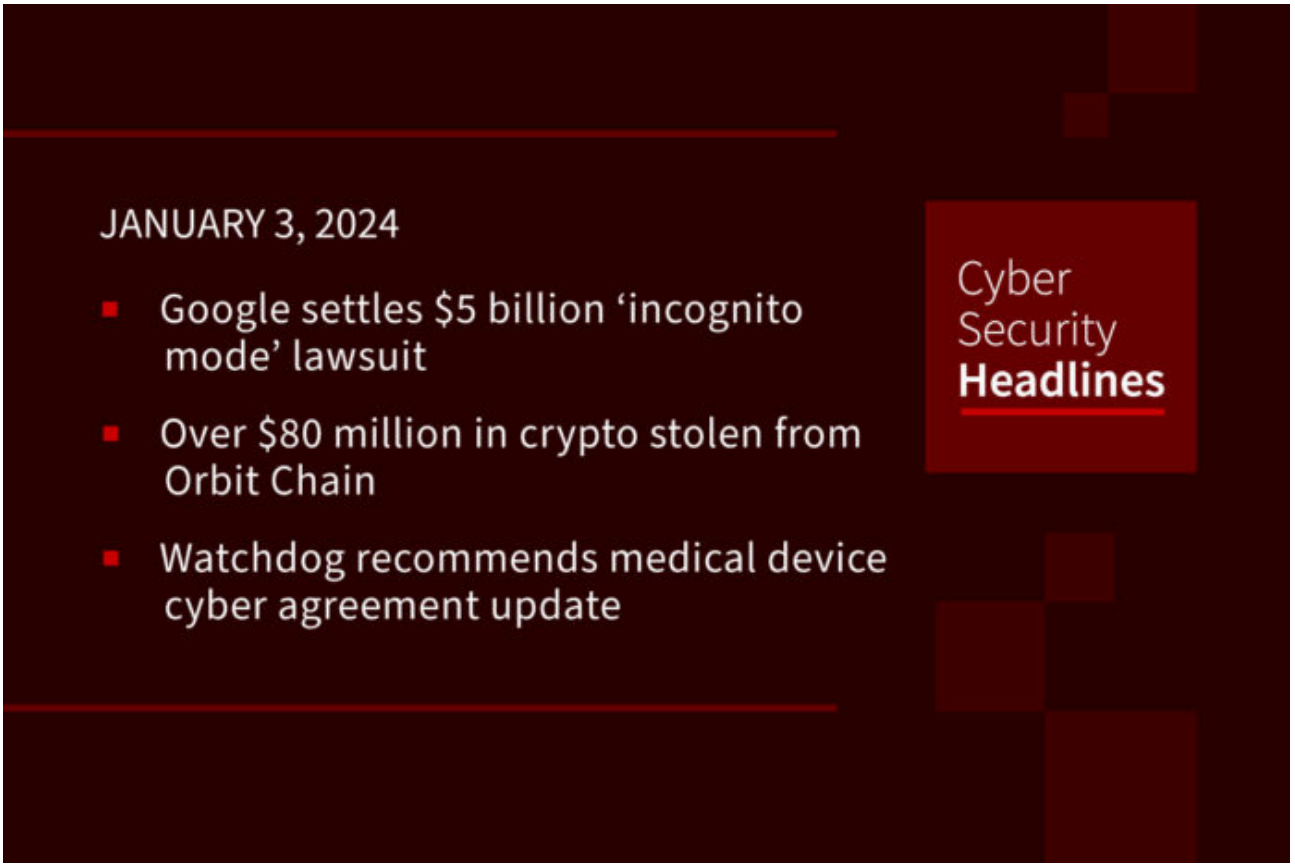
Cybersecurity News: Google $5B suit settled, Orbit Chain loses $80M, FDA cyber agreement

By Sean Kelly

Published: 2024-01-03 · Archived: 2026-05-01 02:11:55 UTC



Google settles $5 billion 'incognito mode' lawsuit

Google has agreed to settle a class-action lawsuit filed in June 2020 that alleged the company misled users by tracking their internet usage even when their browsers were in "incognito" or "private" mode. The plaintiffs alleged that Google violated federal wiretap laws by using Google Analytics to track user activity. Google attempted to get the lawsuit dismissed by pointing to a message it displays informing users that their activity might still be visible to websites they visit, their organization, or their ISP. The class-action lawsuit originally sought roughly $5 billion in damages, however, the final settlement terms have yet to be disclosed.

(The Hacker News)

Over $80 million in crypto stolen from Orbit Chain

On New Year's Eve, hackers stole over 26,000 Ethereum (ETH) from South Korean blockchain bridge project, Orbit Chain. Orbit Chain confirmed the incident in which attackers transferred the crypto to five wallet addresses and over 15 million stablecoin. Orbit Chain is working with law enforcement and cyber experts to track down and freeze the stolen assets. Users have also been warned that reimbursement scams are now circulating and that they should refer to Orbit Chain's official page for updates.

(Infosecurity Magazine)

Watchdog calls for updated medical device cyber agreement

A new report from the Government Accountability Office (GAO) has highlighted that the FDA's medical device cybersecurity agreement is in need of an update. Although incident data has not shown that medical device exploitation is common, the reports says medical devices pose a significant cybersecurity threat to hospitals. The FDAs authority over medical devices has increased in recent years and medical device manufacturers can be penalized under federal law for failing to fix cyber vulnerabilities. The GAO recommended the FDA and CISA update their medical device cyber agreement to reflect organizational and procedural changes.

(FedScoop)

Ukraine says Russia hacked web cameras to spy on targets

Ukraine security officers say Russians hacked two online surveillance cameras in Kyiv. The cameras were installed on residential buildings and used by residents to monitor the surrounding area and parking lot. Russian intelligence allegedly gained remote access to the cameras, changed their viewing angles, and connected them to YouTube to stream sensitive footage. Ukraine's security service (SBU) said the hacked cameras likely helped Russians direct drones and missiles toward Kyiv during a large-scale missile strike against Ukraine on Tuesday.

(The Record)

Huge thanks to our sponsor, NetSPI

Hackers breach Australian court hearing database

Australia's Court Services Victoria (CSV) has warned that court hearing videos were exposed after suffering a ransomware attack. CSV said the attack disrupted its in-court audio/visual technology network, video and audio recordings, and transcription services. The leaked recordings contain a mix of public and confidential information from court proceedings between November 1 to December 21. CSV's disclosure did not identify the responsible threat actor however sources report that the Qilin ransomware gang may be behind the attack.

(Bleeping Computer)

Mysterious hacker attacked industry-leading Iranian companies

On December 20, a hacker called 'irleaks' announced the sale of over 160,000,000 records allegedly stolen from 23 leading insurance companies in Iran. The hacker is seeking $60,000 for the stolen data which they claim includes names, birth dates, father's names, phone numbers, mobile numbers, and national codes. Researchers say the data appears legit but it is not clear how the hackers targeted so many insurance companies at the same time. On December 30, irleaks also say they hacked Iran's largest delivery platform, SnappFood, and stole 3 Terabytes of data.

(Security Affairs)

Google password resets not enough to stop info-stealing malware

On October 23, a cybercriminal known as "PRISMA" boasted of a hacking technique that could continue accessing a victim's Google account even after the password is changed. Security researchers have confirmed the malware exfiltrates session tokens to allow the malware operator to hijack the victim's accounts. The exploit takes advantage of Google's MultiLogin feature which synchronizes Google accounts across different services. Users who suspect they have been infected should log out entirely, and thus invalidate their session tokens, to prevent exploitation. There are six known malware families abusing the vulnerability, most of which target Windows systems.

(The Register)

Steam drops support for Windows 7 and 8.1 to boost security

As of January 1, Steam will no longer receive software and security updates on Windows 7, Windows 8, and Windows 8.1. While Steam still technically works on these older OS, the gaming company said they cannot "guarantee continued functionality." They also said using older versions of Steam could cause systems to be vulnerable to new security flaws and the rise of information-stealing malware. Steam recommends users upgrade to Windows 10 or 11. Windows 10 reaches end of support in October 2025, which may make Windows 11 a better option for users who do not wish to keep upgrading their operating system.

(Bleeping Computer)
