Farah Alhamzawi

Mr. Green

Independent Study & Mentorship

12 January 2023

Analysis of Cybercrimes in 2023

Sharks, Tim, and David DiMolfetta. “The Largest Cyberattack of Its Kind Recently Happened. Here’s How ...” The Largest Cyberattack of Its Kind Recently Happened. Here’s How., 2023, www.washingtonpost.com/politics/2023/10/11/largest-cyberattack-its-kind-recently-happened-heres-how/.

Tim Sharks, the author of "The Largest Cyberattacks of Its Kind Recently Happened," measures the most crucial and dangerous cyberattacks that have taken place in 2023 through his research as well as David Dimolfette discusses the ever-growing world of cybercrime and how elaborate the crimes get as technology evolves. In the aftermath of the most significant cyberattack of its kind, a comprehensive research analysis unveils the intricacies of the incident. The assault, recognized as HTTP/2 "Rapid Reset," was a distributed denial-of-service (DDoS) attack targeting internet giants Cloudflare, Google, and Amazon Web Services (AWS). Leveraging a previously undisclosed vulnerability in the HTTP/2 protocol, the attackers overwhelmed web servers with an unprecedented volume of illegitimate requests. The sheer scale of the attack is staggering, surpassing all previous records. In just two minutes, it generated more requests than Wikipedia's total article views for September 2023. The method employed, a botnet consisting of 20,000 machines, raises concerns about the potential impact, considering the existence of much larger botnets. The vulnerability in the HTTP/2 protocol extended its reach to every modern web server, making it a universal threat. Notably, the document refrains from attributing the attack to any specific entity, leaving the perpetrators unidentified.

Throughout the article, Sharks reveals vulnerabilities in open-source tools, mainly the curl tool. The Cybersecurity and Infrastructure Security Agency (CISA), FBI, and Treasury Department responded with guidance on securing open-source software, emphasizing its relevance to operational technology (OT) and industrial control systems (ICS). However, it all unfolds in the case of U.S. Navy Petty Officer Wenheng "Thomas" Zhao, who pleaded guilty to accepting bribes from a Chinese intelligence officer. Zhao “admitted sending his Chinese handler plans for U.S. military exercises in the Indo-Pacific region, operational orders and electrical diagrams and blueprints for a radar system on a U.S. military base in Okinawa, Japan, according to court documents and U.S. officials,” and was arrested in August of 2023 facing up to and 20 years in prison.

Shifting the focus to the cybersecurity dynamics of the Israel-Hamas conflict, the analysis underscores the prevalence of disinformation over direct hacking activities. Elon Musk's platform, X (formerly Twitter), faces scrutiny for potential violations of disinformation rules related to the conflict. Through this, we can see that Google has taken a strategic move towards enhancing cybersecurity by announcing the adoption of "passkeys" as the default login method. Passkeys, designed as a password replacement functionality, aim to bolster security by relying on encrypted code stored on users' devices, mitigating the risks associated with traditional passwords. The research analysis also touches on broader cybersecurity developments, including the FBI's initiative to build a diverse workforce, the SEC's investigation into a Twitter security lapse, and the surge of U.S. cyber support to Israel. This comprehensive overview provides a deeper understanding of the multifaceted cyber landscape depicted in the document.

Overall, this article analyzed major cyberattacks throughout 2023 in the United States. Through these attacks, it would be assumed that even the smallest attack could cause significant damage to both information and knowledge.