U.S. Faces Cyber Onslaught: Fico Breach, ID, CC, Military Data Sale

Published: 2024-04-01 · Archived: 2026-04-05 16:32:55 UTC

Explore the latest dark web threats uncovered by SOCRadar's Dark Web Team. From breaches affecting major corporations such as Fico to the sale of sensitive data, the digital underworld continues to pose significant risks.

Receive a Free Dark Web Report for Your Organization:

JustEvil Claims to Have Obtained Sensitive Data from BAE Systems

The SOCRadar Dark Web Team has identified a concerning development involving the threat group/actor JustEvil aka KillMilk. According to reports, JustEvil claims to have successfully accessed sensitive personal data belonging to UK defense personnel from **BAE** Systems. This data allegedly includes resumes, professional certifications, and job roles, potentially exposing individuals to identity theft, phishing attacks, and other cyber threats.

Identity Documents of American Citizens are on Sale

In another alarming discovery, our team observed the sale of identity documents of American citizens on a hacker forum. This data, which includes names, addresses, Social Security numbers, and phone numbers, poses a high risk of identity theft, financial fraud, and reputational damage for affected individuals.

Credit Cards Belonging to the United States are on Sale

Further exacerbating the situation, stolen credit cards belonging to individuals in the United States have been spotted for sale on the dark web. With over **100 cards** in stock and priced at $13 per card, this development signals a potential data breach at financial institutions or payment processors, highlighting the urgent need for enhanced security measures and vigilance.

USDoD Exposes Fico.com Database

A major threat surfaced, idle for a long time; USDoD came back to the cybercrime arena. An alleged data breach involving **FICO**, a major analytics software company was shared by the threat actor on a hacker forum. The leaked database reportedly contains personal and professional information of individuals associated with FICO, raising serious concerns about data security and privacy.

Cyber Niggers' Alleged US Military Files

Lastly, the threat group CyberNiggers has purportedly released US military files, including precompiled **JARs** and certificate files belonging to the Air Force and Navy. This breach underscores the ongoing risks of insider threats

and unauthorized access to sensitive military data, necessitating comprehensive security measures and collaboration among stakeholders.

These developments highlight the dynamic and evolving nature of cyber threats on the dark web. Organizations must remain vigilant, implement robust security protocols, and leverage threat intelligence solutions like SOCRadar to detect and mitigate risks effectively.

Powered by DarkMirror™

Gaining visibility into deep and dark web threats can be extremely useful from an actionable threat intelligence and digital risk protection perspective. However, monitoring all sources is simply not feasible, which can be time-consuming and challenging. One click-by-mistake can result in malware bot infection. To tackle these challenges, SOCRadar's DarkMirror™ screen empowers your SOC team to follow up with the latest posts of threat actors and groups filtered by the targeted country or industry.
