Acuity Federal Contractor Breach, Okta Customers Leak, DCRat Exploit and Access Sales

Published: 2024-03-11 · Archived: 2026-04-05 12:50:27 UTC

In the Dark Web, a world of illicit activities and cyber threats, the SOCRadar Dark Web Team has uncovered a series of alarming findings. From a breach of a federal contractor exposing sensitive data to the sale of unauthorized access and leaked databases, the implications of these discoveries are far-reaching.

Join us as we delve into the dark underbelly of the internet, exploring the potential impact on national security, personal privacy, and the need for robust cybersecurity measures.

Alleged Breach of Federal Contractor Acuity Exposes ICE and USCIS Data

In a recent cybersecurity incident, SOCRadar Dark Web Team detected a post on a hacker forum where a member of the group known as CyberNiggers claimed to have breached Acuity, a United States federal contractor, and is now purportedly selling data associated with the U.S. Immigration and Customs Enforcement (ICE) and the United States Citizenship and Immigration Services (USCIS). This breach allegedly compromises sensitive and personally identifiable information (PII) of over **100,000 victims**, potentially impacting a vast number of people.

The alleged stolen data includes full names, passport details, dates of birth, phone numbers, email addresses, physical addresses, and physical attributes.

Further details from Hackread revealed that the breach extends to more sensitive layers, including source code, user manuals, and confidential communications between ICE agents and contractors. These documents encompass discussions on investigative techniques, insights into the Ukraine and Russia conflict, and information on global terrorism-related seminars, illustrating the breach's potential impact on national security and intelligence operations.

One of the most alarming aspects of this incident is the method of the alleged breach. The threat actor claimed to have exploited a critical zero-day vulnerability in GitHub, allowing them to steal GitHub tokens and further their malicious activities. This points to the importance of robust cybersecurity measures and the need for constant vigilance against emerging threats and vulnerabilities.

Customer Database of Okta is Leaked

The SOCRadar Dark Web Team discovered a post on a hacker forum where a threat actor claims to have leaked the Okta customer database, following a data breach in September 2023. This breach reportedly compromised the

personal and professional information of 3.8 thousand customer support users, including sensitive details like User IDs, names, contact information, and security parameters.

Further investigation by using SOCRadar's Threat Hunting module revealed that the dataset shared by the threat actor matches a database previously alleged to belong to the National Defense Information Sharing and Analysis Center, which was published by a member of CyberNiggers in March 2023.

DCRat Exploit Are on Sale

The SOCRadar Dark Web Team uncovered a post on a hacker forum indicating that a threat actor is offering a new alleged exploit for **DCRat (also known as Dark Crystal)** for sale. DCRat is a Remote Access Tool (RAT) that can be used for malicious purposes, such as unauthorized access to victims' computers, data theft, and deploying malware. The exploit being sold purportedly allows an attacker to gain access to the host system merely by using a link to the host, simplifying the process of infiltrating systems for malicious actors.

Unauthorized VPN Access Sale is Detected for a French Software Company

The SOCRadar Dark Web Team detected a post on a hacker forum where a threat actor is advertising the sale of unauthorized VPN access. This access is purported to belong to a French software company with an annual revenue of approximately **$49.2 million**. The details provided in the post suggest a significant security breach, emphasizing the type of access being sold is through a VPN, along with domain user credentials.

Databases of Many Sectors in India are Leaked

The SOCRadar Dark Web Team detected a post on a hacker forum where a threat actor has announced a significant data leak impacting multiple sectors in India. According to the claim, the leaked databases collectively amount to a substantial **10 gigabytes** of data. This announcement has evidently attracted considerable attention within the cybercriminal community, as evidenced by the volume and tone of the comments under the post. These comments reflect a high level of interest from other threat actors, though some express skepticism regarding the freshness of the data, suspecting it might be outdated.

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.
