Mastercard Data Leak, New Fully Undetectable Ransomware, Elusive Stealer Source Code Leak, and More

Published: 2024-01-08 · Archived: 2026-04-05 14:19:08 UTC

In recent discoveries across the cyber threat landscape, the SOCRadar Dark Web Team has identified various concerning developments, including an undetectable ransomware for sale claimed to be effective against major antivirus software, a Mastercard data leak asserted by the Toxcar Cyber Team on a Telegram Channel, and the sharing of the source code of Elusive Stealer, a data theft malware. These findings underscore the evolving cyber threats, further emphasized by a recruitment post seeking a remote sales agent for a threat group offering fake hacking services.

A New Ransomware is on Sale

The SOCRadar Dark Web Team has come across a new ransomware being marketed on a hacker forum by a threat actor claiming to have personally developed it. The seller asserts that this ransomware is fully undetectable by significant antivirus software, including Avast and Windows Defender, thanks to extensive testing on Windows machines. It uses the AES symmetric algorithm to encrypt all disks, storing the decryption key in a remote database. Additionally, it changes the victim's desktop background to a message, indicating their system is compromised. The threat actor also mentions having developed a GUI decrypter, possibly for negotiations or ransom payments, allowing victims a chance to recover their encrypted files.

Data of Mastercard are Leaked by Toxcar Cyber Team

The SOCRadar Dark Web Team has reported a post on Garuda From Cyber's Telegram Channel, where the **Toxcar Cyber Team** claims they have leaked data from Mastercard. The threat actor asserts the attack targeted the United States site of Mastercard and categorizes it as a leak. The threat actor also shared 3 screenshots alleged to be from the Mastercard database, presenting what they purport to be evidence of the intrusion.

Source Code of Elusive Stealer is Shared

A SOCRadar Dark Web Analyst has detected a post on a hacker forum revealing the sharing of the **Elusive Stealer**'s source code. This stealer is a type of malware that specializes in stealing sensitive information from infected systems. The release of its source code is a significant cybersecurity concern, as it allows malicious actors to modify, improve, and spread the malware more widely, potentially leading to an increase in infections and data theft across various systems.

New Recruitment Post is Detected

A SOCRadar Dark Web Analyst has identified a recruitment post on a hacker forum for a threat group seeking a remote sales agent for fake hacking services. The threat group describes the position as full-time, remote, with a salary range of **$3000 – $5000**. The job entails selling pre-made scripts that defraud customers under the guise of hacking services, with over 80 daily inquiries. Responsibilities include lead generation, negotiation, and meeting sales targets while providing customer satisfaction.

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.
