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

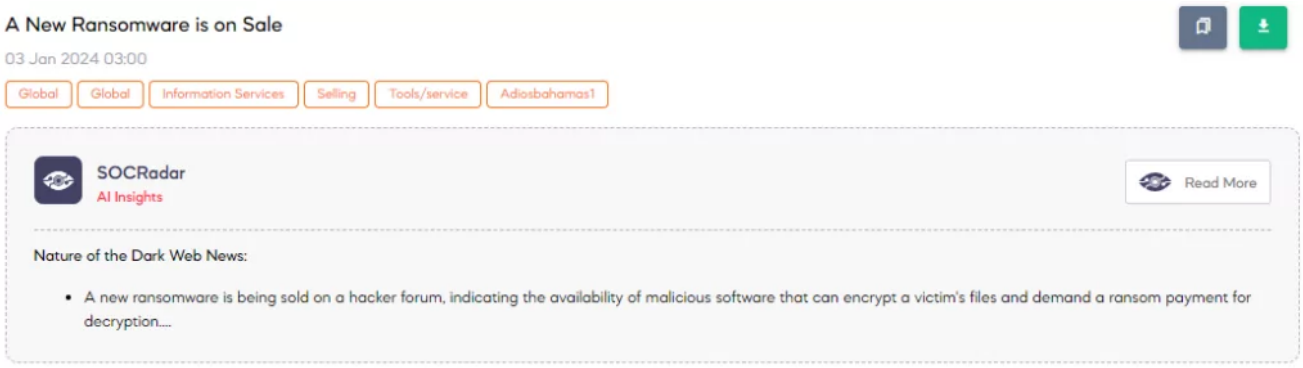
socradar.io/mastercard-data-leak-new-fully-undetectable-ransomware-elusive-stealer-source-code-leak-and-more/

January 8, 2024

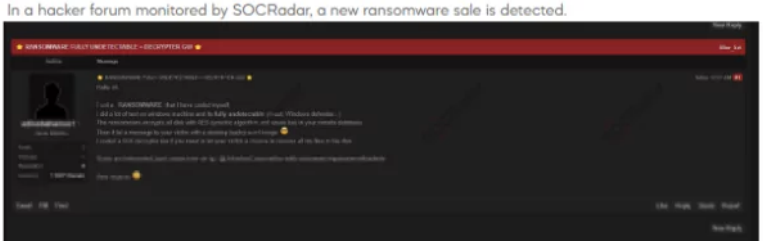
In recent discoveries across the cyber threat landscape, the SOCRadar Dark Web Team has identified various concerning developments, including an undetectable ransomware for sale claimed to be effective against major antivirus software, a Mastercard data leak asserted by the Toxcar Cyber Team on a Telegram 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.

Get your free Dark Web Report and find out if your data has been compromised.

A New Ransomware is on Sale

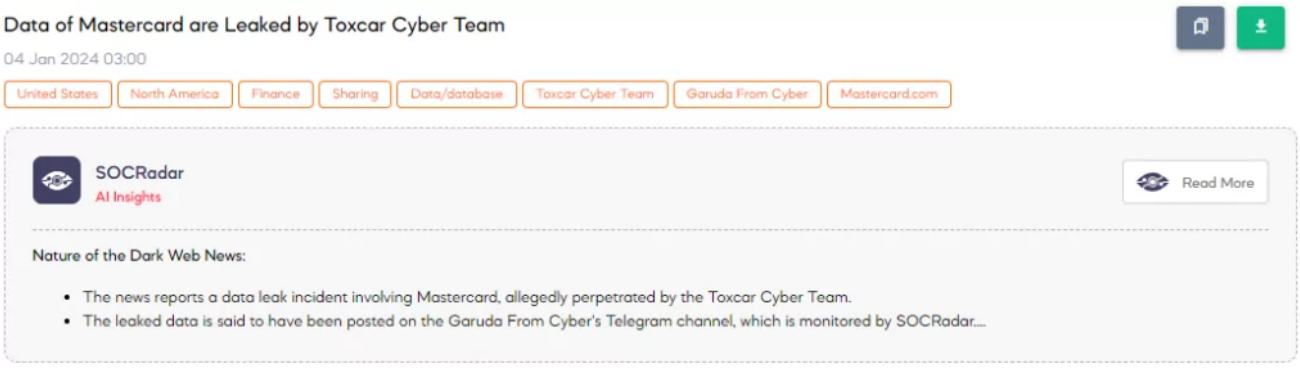


In a hacker forum monitored by SOCRadar, a new ransomware sale is detected.

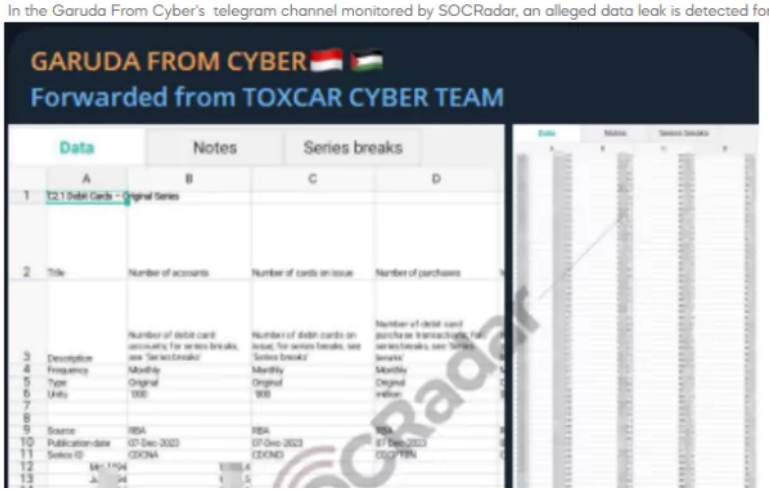


The SOCRadar Dark Web Team has come across a new ransomware being marketed on a hacker forum by a threat actor claiming to have personally developed it. The seller asserts that this ransomware is fully undetectable by significant antivirus software, including Avast and Windows Defender, thanks to extensive 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

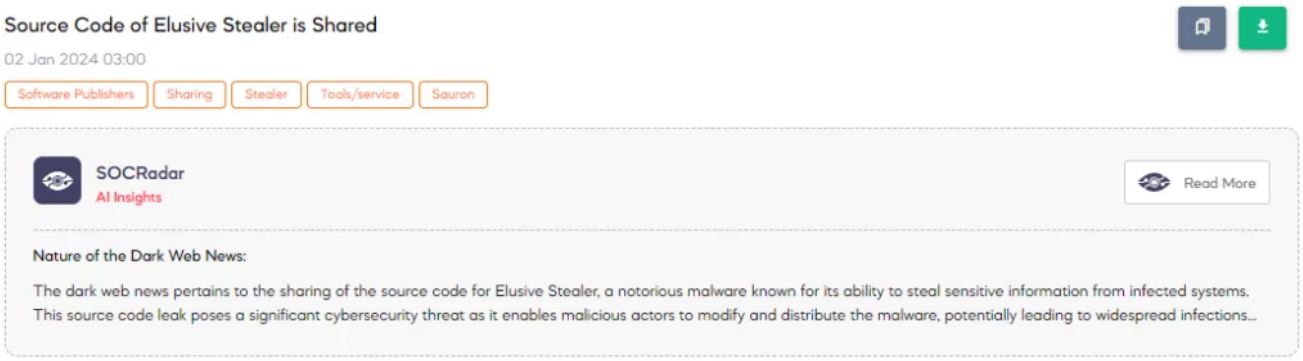


In the Garuda From Cyber's telegram channel monitored by SOCRadar, an alleged data leak is detected for Mastercard.

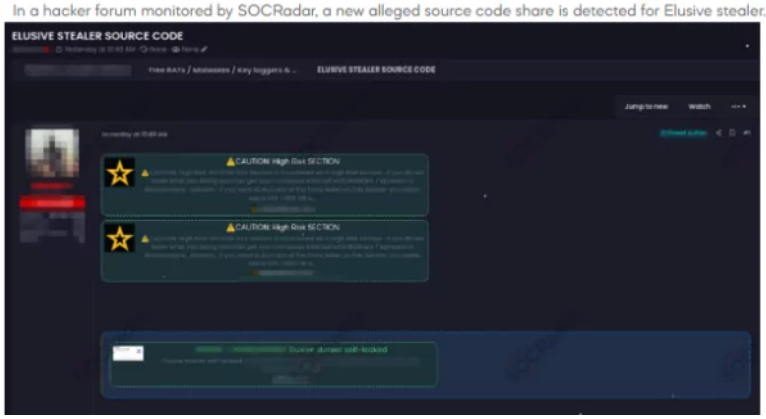


The SOCRadar Dark Web Team has reported a post on Garuda From Cyber's Telegram Channel, where the **Toxcar Cyber Team** claims they have leaked data from Mastercard. The threat actor asserts the attack targeted the United States site of Mastercard and categorizes it as a leak. The threat actor also shared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

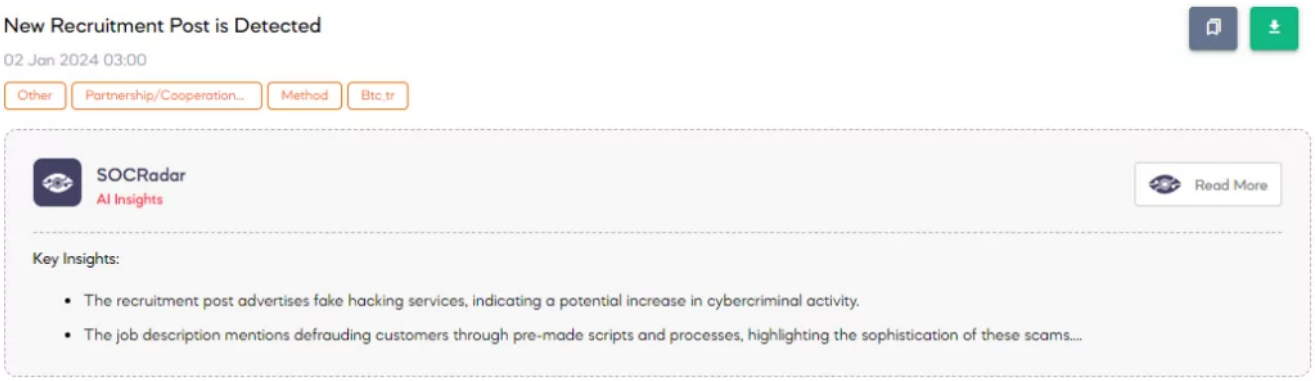


In a hacker forum monitored by SOCRadar, a new alleged source code share is detected for Elusive stealer.



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.

PROTECTION OF PERSONAL DATA COOKIE POLICY FOR THE INTERNET SITE

Protecting your personal data is one of the core principles of our organization, SOCRadar, which operates the internet site (www.socradar.com). This Cookie Usage Policy ("Policy") explains the types of cookies used and the conditions under which they are used to all website visitors and users.

Cookies are small text files stored on your computer or mobile device by the websites you visit.

Cookies are commonly used to provide you with a personalized experience while using a website, enhance the services offered, and improve your overall browsing experience, contributing to ease of use while navigating a website. If you prefer not to use cookies, you can delete or block them through your browser settings. However, please be aware that this may affect your usage of our website. Unless you change your cookie settings in your browser, we will assume that you accept the use of cookies on this site.

1. WHAT KIND OF DATA IS PROCESSED IN COOKIES?

Cookies on websites collect data related to your browsing and usage preferences on the device you use to visit the site, depending on their type. This data includes information about the pages you access, the services and products you explore, your preferred language choice, and other preferences.

2. WHAT ARE COOKIES AND WHAT ARE THEIR PURPOSES?

Cookies are small text files stored on your device or web server by the websites you visit through your browsers. These small text files, containing your preferred language and other settings, help us remember your preferences on your next visit and assist us in making improvements to our services to enhance your experience on the site. This way, you can have a better and more personalized user experience on your next visit.

The main purposes of using cookies on our Internet Site are as follows:

- Improve the functionality and performance of the website to enhance the services provided to you,

- Enhance and introduce new features to the Internet Site and customize the provided features based on your preferences,
- Ensure legal and commercial security for the Internet Site, yourself, and the Organization, and prevent fraudulent transactions through the Site,
- Fulfill legal and contractual obligations, including those arising from Law No. 5651 on the Regulation of Publications on the Internet and the Fight Against Crimes Committed Through These Publications, as well as the Regulation on the Procedures and Principles Regarding the Regulation of Publications on the Internet.

3. TYPES OF COOKIES USED ON OUR INTERNET SITE 3.1. Session Cookies

Session cookies ensure the smooth operation of the internet site during your visit. They are used for purposes such as ensuring the security and continuity of our sites and your visits. Session cookies are temporary cookies and are deleted when you close your browser; they are not permanent.

3.2. Persistent Cookies

These cookies are used to remember your preferences and are stored on your device through browsers. Persistent cookies remain stored on your device even after you close your browser or restart your computer. These cookies are stored in your browser's subfolders until deleted from your browser's settings. Some types of persistent cookies can be used to provide personalized recommendations based on your usage purposes.

With persistent cookies, when you revisit our website with the same device, the website checks if a cookie created by our website exists on your device. If so, it is understood that you have visited the site before, and the content to be presented to you is determined accordingly, offering you a better service.

3.3. Mandatory/Technical Cookies

Mandatory cookies are essential for the proper functioning of the visited internet site. The purpose of these cookies is to provide necessary services by ensuring the operation of the site. For example, they allow access to secure sections of the internet site, use of its features, and navigation.

3.4. Analytical Cookies

These cookies gather information about how the website is used, the frequency and number of visits, and show how visitors navigate to the site. The purpose of using these cookies is to improve the operation of the site, increase its performance, and determine general trend directions. They do not contain data that can identify visitors. For example, they show the number of error messages displayed or the most visited pages.

3.5. Functional Cookies

Functional cookies remember the choices made by visitors within the site and recall them during the next visit. The purpose of these cookies is to provide ease of use to visitors. For example, they prevent the need to re-enter the user's password on each page visited by the site user.

3.6. Targeting/Advertising Cookies

They measure the effectiveness of advertisements shown to visitors and calculate how many times ads are displayed. The purpose of these cookies is to present personalized advertisements to visitors based on their interests.

Similarly, they determine the specific interests of visitors' navigation and present appropriate content. For example, they prevent the same advertisement from being shown again to the visitor in a short period.

4. HOW TO MANAGE COOKIE PREFERENCES?

To change your preferences regarding the use of cookies, block or delete cookies, you only need to change your browser settings.

Many browsers offer options to accept or reject cookies, only accept certain types of cookies, or receive notifications from the browser when a website requests to store cookies on your device.

Also, it is possible to delete previously saved cookies from your browser.

If you disable or reject cookies, you may need to manually adjust some preferences, and certain features and services on the website may not work properly as we will not be able to recognize and associate with your account. You can change your browser settings by clicking on the relevant link from the table below.

5. EFFECTIVE DATE OF THE INTERNET SITE PRIVACY POLICY

The Internet Site Privacy Policy is dated The effective date of the Policy will be updated if the entire Policy or specific sections are renewed. The Privacy Policy is published on the Organization's website (www.socradar.com) and made accessible to relevant individuals upon request.

SOCRadar
Address: 651 N Broad St, Suite 205 Middletown, DE 19709 USA
Phone: +1 (571) 249-4598
Email:
Website: www.socradar.com