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

socradar.io/acuity-federal-breach-okta-leak-dcrat-exploit/

March 11, 2024

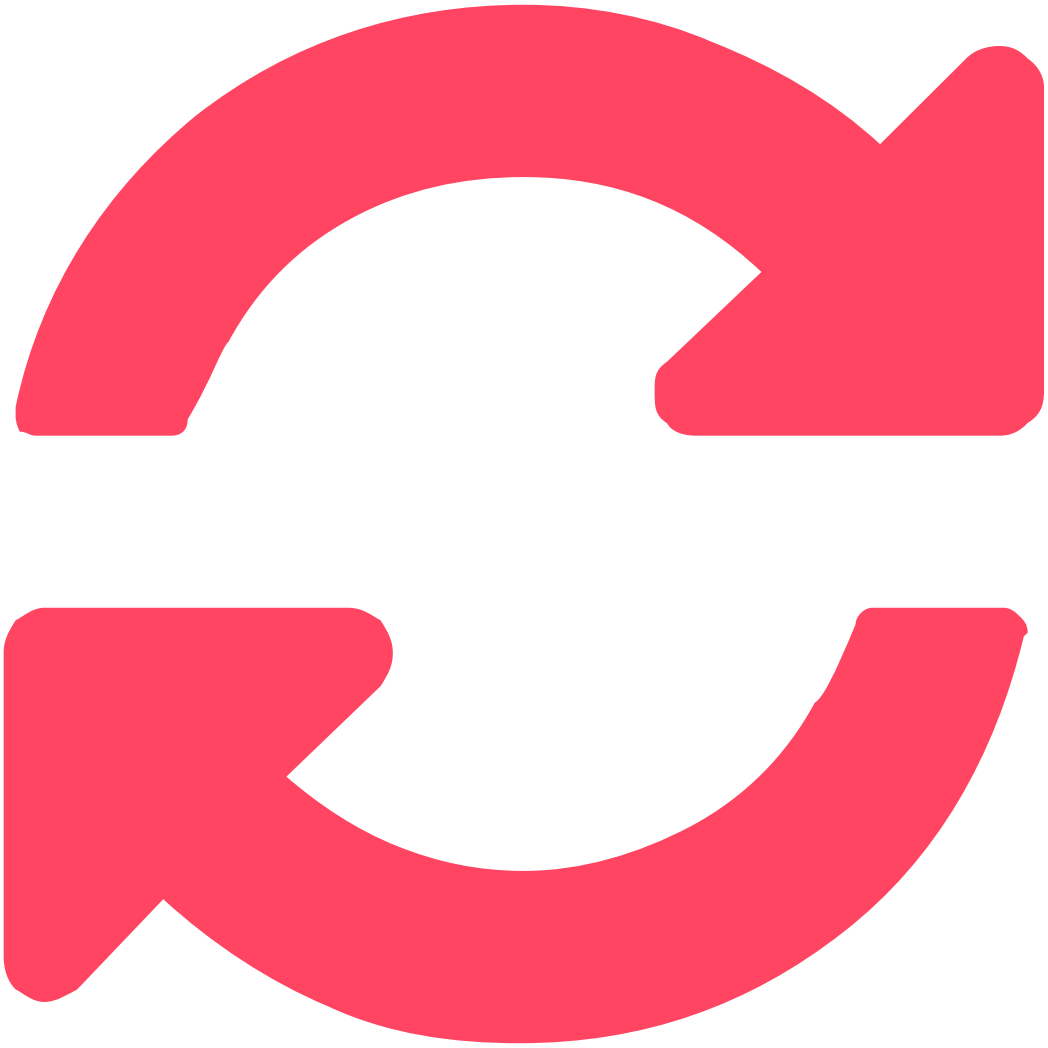
Home

Resources

Blog

Mar 11, 2024

7 Mins Read



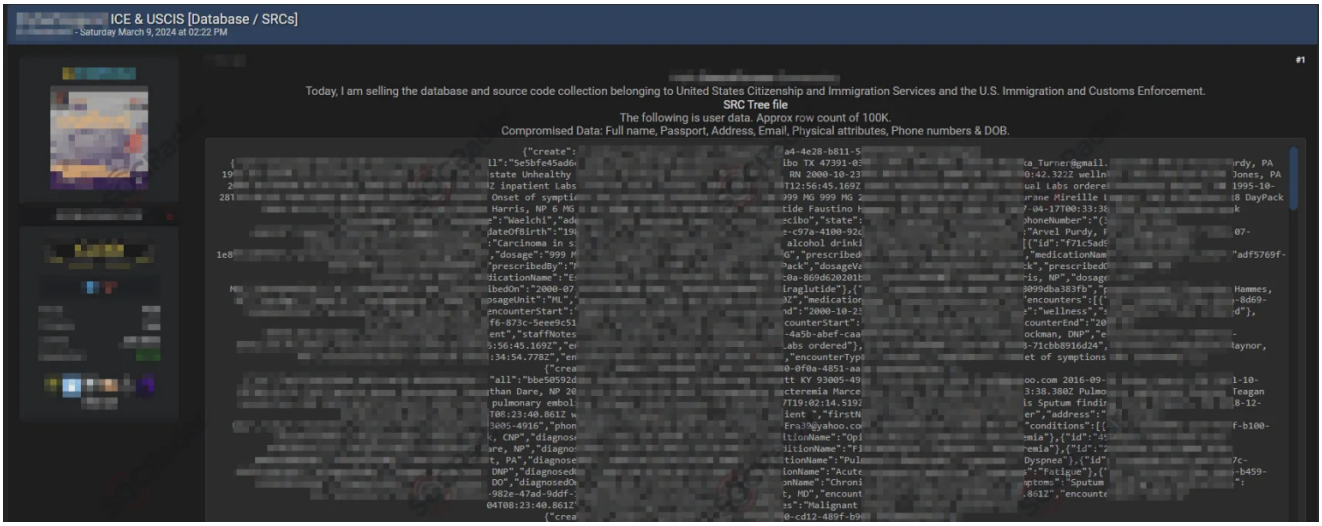
Mar 18, 2024

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.

Receive a Free Dark Web Report for Your Organization:

Alleged Breach of Federal Contractor Acuity Exposes ICE and USCIS Data



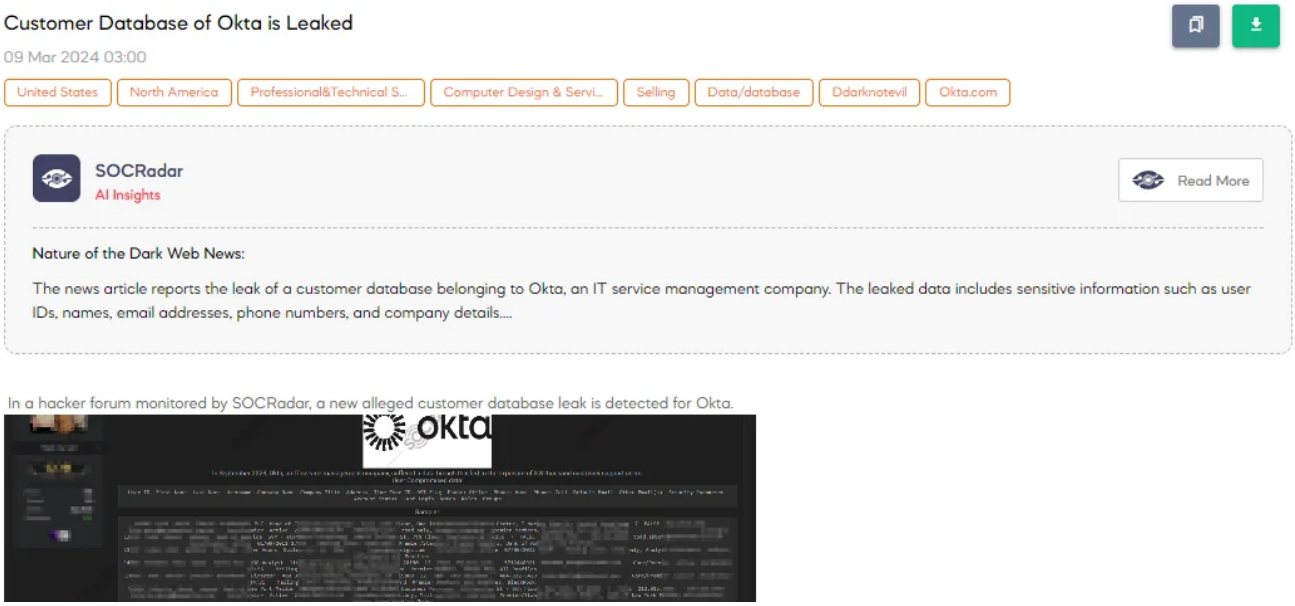
In a recent cybersecurity incident, SOCRadar Dark Web Team detected a post on a hacker forum where a member of the group known as CyberNiggers claimed to have breached Acuity, a United States federal contractor, and is now purportedly selling data associated with the U.S. Immigration and Customs Enforcement (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.

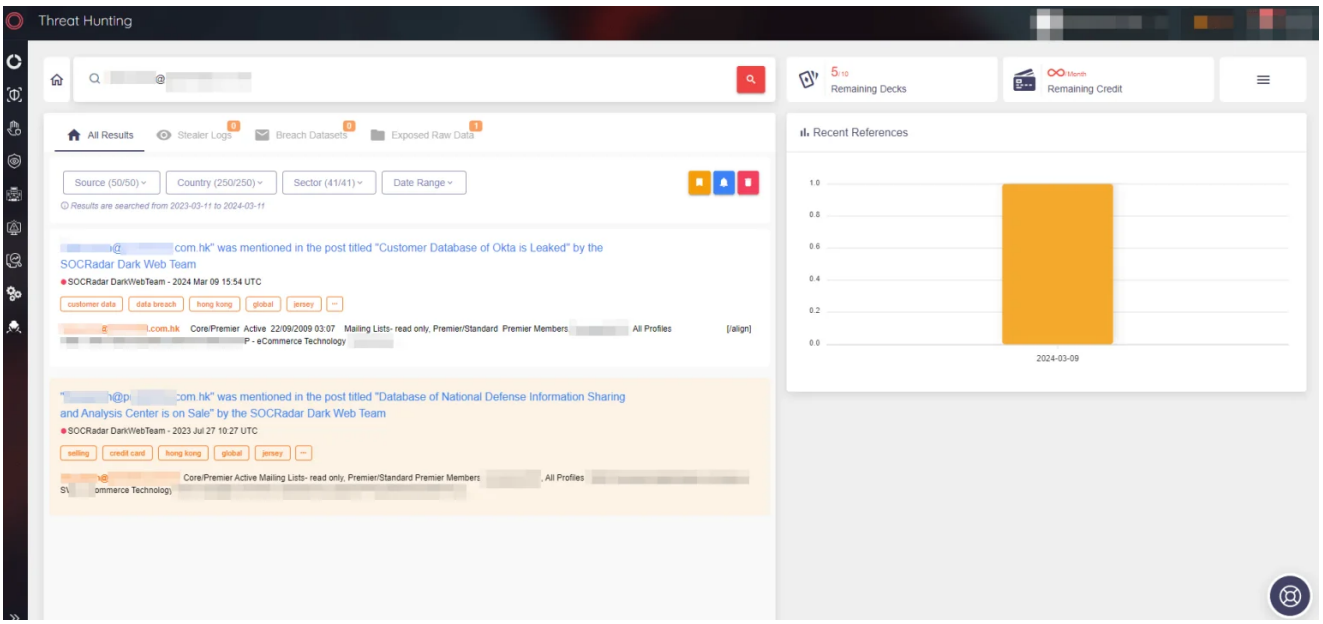
Further details from Hackread revealed that the breach extends to more sensitive layers, including source code, user manuals, and confidential communications between ICE agents and contractors. These documents encompass discussions on investigative techniques, insights into the Ukraine and Russia conflict, 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



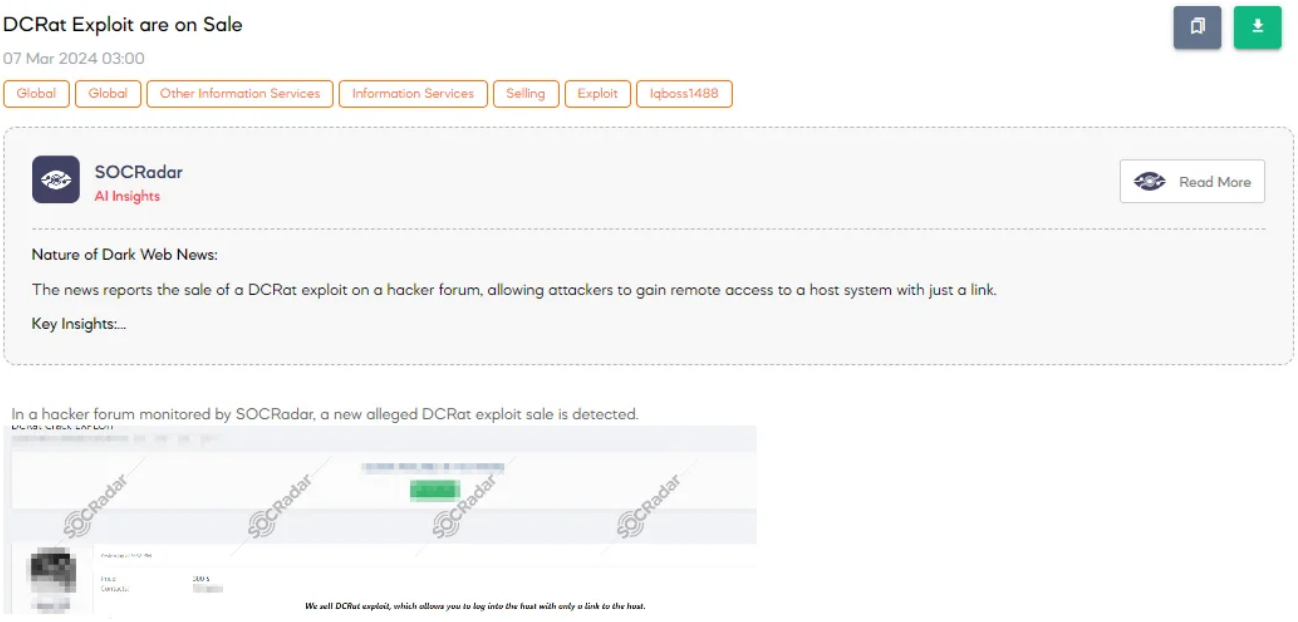
The SOCRadar Dark Web Team discovered a post on a hacker forum where a threat actor claims to have leaked the Okta customer database, following a data breach in September 2023. This breach reportedly compromised the personal and professional information of 3.8 thousand customer support users, including sensitive details like User IDs, names, contact information, and security parameters.



SOCRadar Threat Hunting

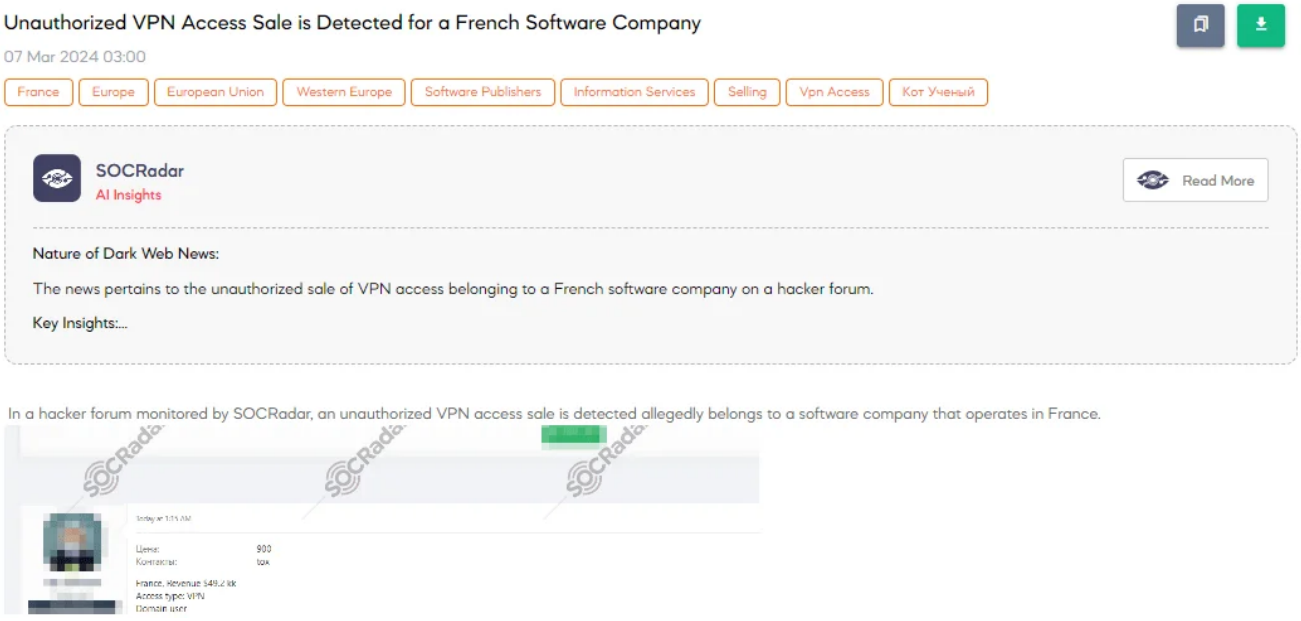
Further investigation by using SOCRadar's Threat Hunting module revealed that the dataset shared by the threat actor matches a database previously alleged to belong to the National Defense Information Sharing and Analysis Center, which was published by a member of CyberNiggers in March 2023.

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.

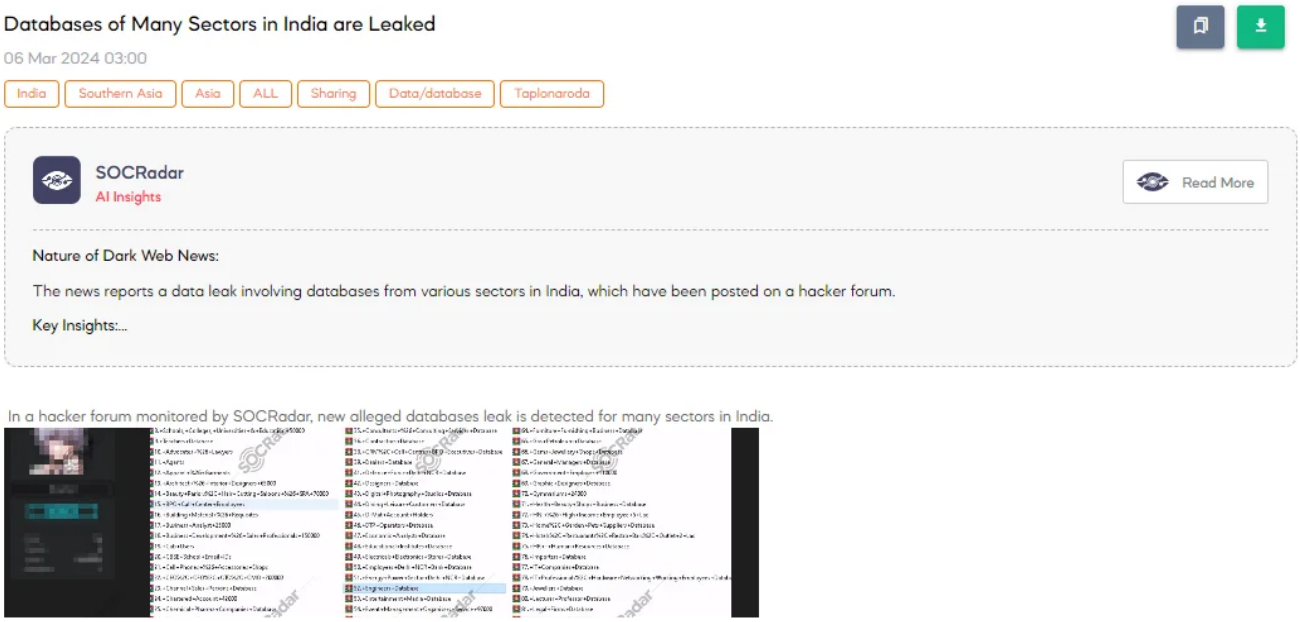
Unauthorized VPN Access Sale is Detected for a French Software Company



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.

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