CRIF CYBER OBSERVATORY: CYBER ATTACKS IN 2023, 45% INCREASE IN DATA THEFT ON THE DARK WEB

- There are over 7.5 billion pieces of information circulating on the dark web at a global level, with a 15.9% increase in reports.
- The severity of alerts sent increased by 29% compared to the previous year
- The techniques used by cybercriminals are becoming increasingly sophisticated: with the malicious use of artificial intelligence, it is getting harder and harder to distinguish between genuine and bogus communications.

In 2023, there was an increase in compromised account credentials, combined with other data that is extremely valuable to hackers. In fact, it is estimated that more than 7.5 billion pieces of information are circulating on the dark web or are accessible on messaging platforms at a global level, up 44.8% from 2022. Moreover, there were 1,801,921 reports of data found on the dark web, with an increase of 15.9% compared to 2022.

These are some of the key findings from the CRIF Cyber Observatory, which analyzes the vulnerability of users and businesses to cyber-attacks, interpreting the key trends affecting data exchanged in both Open Web and Dark Web environments.

Cyber fraud types and dangers

In 2023, e-mail addresses became particularly valuable because they allow access to a number of different services. In fact, in the CRIF Observatory analysis, they were found in combination with passwords in 94.4% of cases, exposing the victim to more accurate and credible fraudulent messages, such as fake payments to be authorized or blocked accounts. These phishing messages contain malicious links that encourage victims to click and provide additional data to fraudsters.

Increasingly rich datasets of contact information supplement the victim's profile, making victims more vulnerable to fraud. The severity of alerts sent in 2023 increased by 29% overall compared to the previous year, confirming that the vulnerability to fraud per individual data exposure is increasing. In fact, in one in ten cases, as well as the victim's phone number, the e-mail address and the first and last name also appear.

CRIF CYBER OBSERVATORY: CYBER ATTACKS IN 2023, 45% INCREASE IN DATA THEFT ON THE DARK WEB

Lists of this type of personal data are a gold mine for fraudsters, who can perpetrate highly tailored fraud, including through the use of artificial intelligence, which is often mentioned in forums for exchanging phishing kits and malware. In 2023, this combination of multiple personal and contact data recorded a 45% increase compared to the previous year.

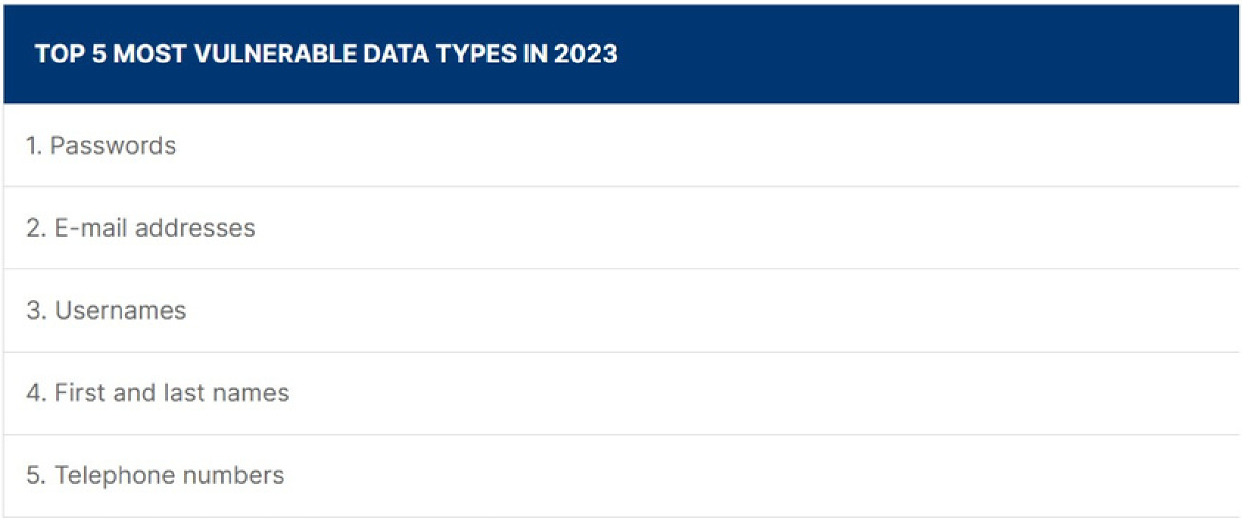
In addition, throughout 2023, there was a proliferation of ad-hoc tools available to the fraudster community. For example, phishing kits (such as Modlishka, Evilginx and many others) were widespread. These tools are ready to use, even by less experienced hackers, to target consumers with phishing campaigns. Due, among other things, to the malicious use of AI, fraudulent e-mails are becoming increasingly sophisticated, making it even more difficult for the recipient to distinguish between genuine and bogus communications. And the ability to quickly translate into multiple languages helps criminals increase phishing attacks at a global level.

In this context, open source messaging applications – such as Telegram – are increasingly becoming the ideal place to exchange stolen data, but also to provide instructions for creating off-the-shelf malware or to buy and sell hackers' tools. Infostealers (malware designed to steal personal data) are a further threat to consumers: spread via harmful links, malicious e-mails or compromised websites, they pose a threat to users' security, operating covertly and capturing information and credentials during browsing.

CRIF CYBER OBSERVATORY: CYBER ATTACKS IN 2023, 45% INCREASE IN DATA THEFT ON THE DARK WEB

The most desirable and vulnerable data in cyberspace

Once again in 2023, the main categories of data under attack were passwords, e-mail addresses, usernames, first and last names, and telephone numbers. This information circulates mostly on the dark web and is therefore more vulnerable. Compared to 2022, passwords overtook e-mail addresses to take top spot, while usernames rose to third place, overtaking first and last names and telephone numbers among the most vulnerable data.



TOP 5 MOST VULNERABLE DATA TYPES IN 2023
1. Passwords
2. E-mail addresses
3. Usernames
4. First and last names
5. Telephone numbers

Source: CRIF Cyber Observatory

Very often e-mail addresses are associated with a password, occurring in 94.4% of cases (up 4.4% from 2022); usernames (65.6%) also often appear with passwords. Telephone numbers play a key role in these cases and, when combined with passwords (16.6%), increase the vulnerability of victims. This combination is up 25.6% compared to the previous year.

CRIF CYBER OBSERVATORY: CYBER ATTACKS IN 2023, 45% INCREASE IN DATA THEFT ON THE DARK WEB

Most hacked account types

Most hacked accounts are related to entertainment sites (56.6%), followed by e-commerce (16.4%) and social media (11.9%). The risk of theft of such data can have direct financial consequences for victims. Fourth and fifth place are the theft of accounts related to payment service (6.2%) and financial (4.8%) websites and forums, such as banking sites.

Stolen credit card information

As for credit cards, in addition to the card number, the cvv and expiry date are very frequently present on the dark web, in 96.9% of cases.

Businesses increasingly targeted by cybercrime

Through a qualitative analysis of the domains, the CRIF Cyber Observatory investigated whether the e-mail accounts found on the dark web refer to personal or business accounts. In 91.1% of cases they are personal e-mail accounts, while the remaining 8.9% of cases are business accounts, up 2.1% compared to 2022.

Switzerland

Looking at the most common passwords found on the dark web, in Switzerland we find at the top combinations of simple numbers such as "123456", "123456789" and first names such as "andrea", "daniel" and “sandra”, but also simple terms such as "newsletter", "password", “sunshine”, and “snoopy”.

CRIF Cyber Observatory

CRIF Cyber Observatory investigates the vulnerability of individuals and businesses to cyber attacks on the open and dark webs; it also indicates which items of information are most exposed, what details can be found on the internet and where the traffic in data is most concentrated. This survey was carried out with reference to 2022.

CRIF
Together to the next level