kaspersky bring on the future

Data-Stealing Storm: Exploring the Dark Web Market for Compromised Credentials

What Businesses Need to Know About this Threat and How to Mitigate It

Kaspersky Digital Footprint Intelligence

Kaspersky
Digital Footprint
Intelligence

Introduction

The Kaspersky Digital Footprint Intelligence team has prepared a report that draws on data on millions of devices compromised by specific malware designed for stealing information, or infostealers.

Infostealer is a type of malware designed for collecting and stealing confidential information: accounts and credentials, cookies, bank card details, cryptowallets, and so on. The data stolen from millions of devices all over the world is forwarded to the malware operator's C&C (Command and Control) server and assembled into logs (a log file typically contains information from a single infected system), to then be distributed among the cybercrime community through darknet markets.

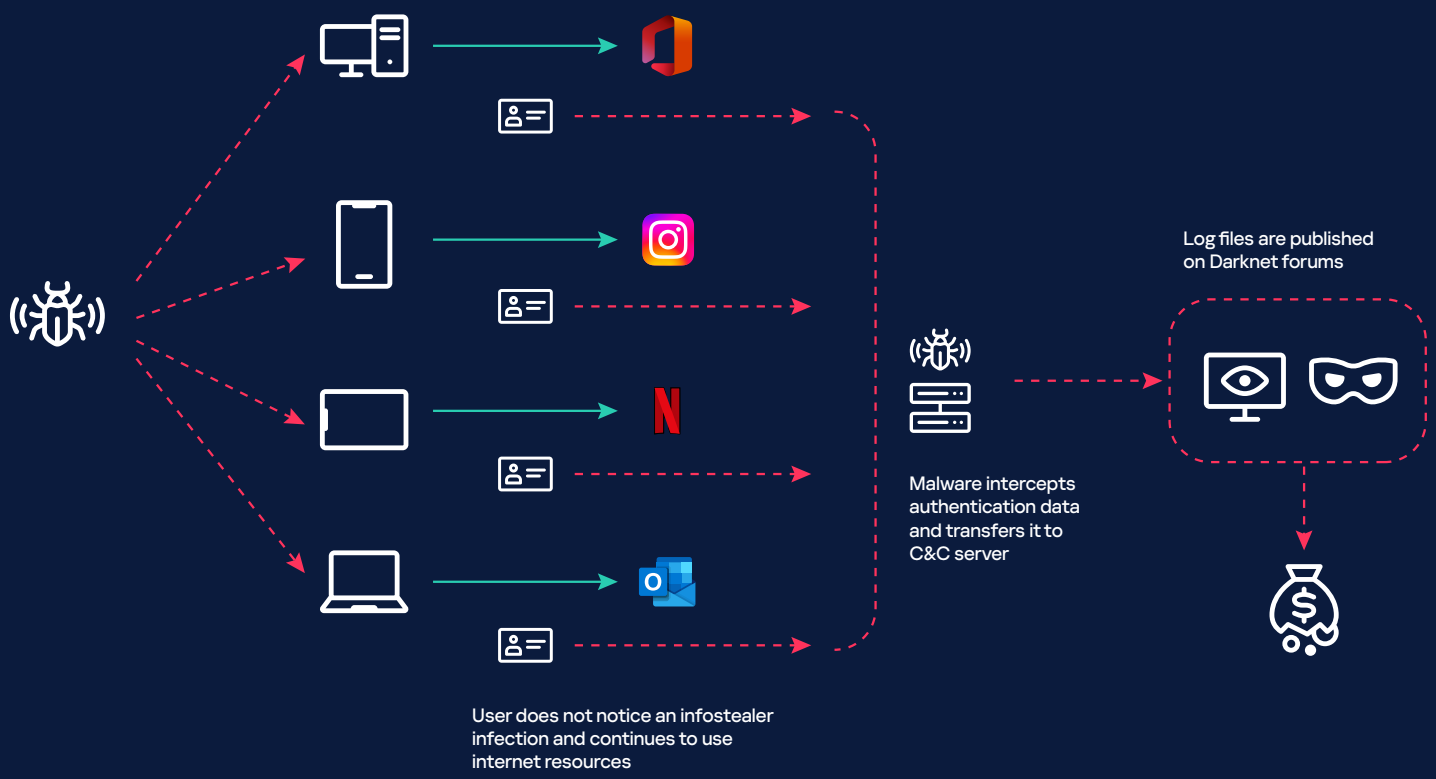
This report presents statistics and key takeaways from processing and analysis of infostealer logs collected from 2021 through 2023.

Sources of the analyzed information

Cybercriminals use private threads on underground forums to publish logs collected by infostealers from infected devices. These files contain users' accounts and other details, as well as information about the compromised device itself.

Cybercriminals typically sell logs to other cybercriminals, but they may share data for free. For example, they may share what is left after they have extracted all the information they need to boost their reputation with the community.

Infostealer infection scenario



One log file contains an average of

50.9 accounts

We analyze logs to isolate compromised accounts. If a user account is found in malware (Trojan, spyware bot, etc.) logs, this is a sign that the user's device was infected.

It is important to note that one log corresponds to one infection of a specific machine, while it can contain a large number of accounts for various websites or applications that were used on the device.

Infection trends we observed

The number of infections detected in 2023 represents a

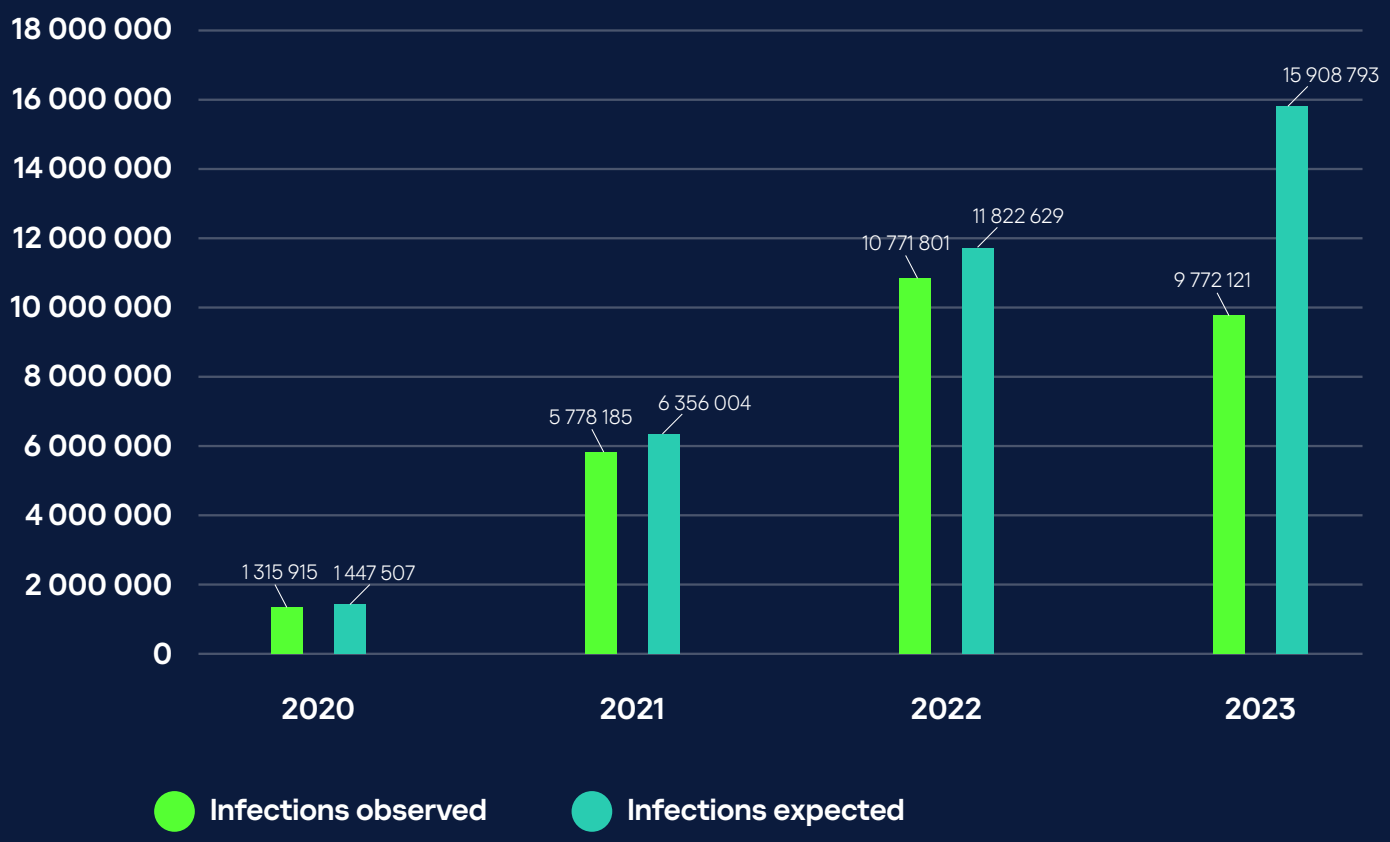
35%

increase on 2022 based on forecast data. The infection date is determined based on compromised device metadata contained in infostealer logs

Note that logs do not show up on the dark web immediately after a device is compromised. The account may have been hacked in 2022, but a corresponding log file might be published no earlier than 2023. Therefore, it is reasonable to expect 2023's actual infection figures to be adjusted upward if we consider predictions about the number of logs to be published in 2024.

The observable log dynamics suggest that in the first months of the year, the number of log files for the previous year is greater than in the last months of the year.

Yearly infection statistics



To build the forecast, we compared the number of compromised accounts from 2020 through 2023 by month. We used this data to identify a trend while augmenting our datasets from previous years with newly obtained data, which now allows us to predict expected numbers adjusted for the estimated amount of data to be added in the future[1]

[1] Cybercriminals may post log files containing compromised accounts on the darknet months or even years after infection. We track both posting dates and actual compromise dates. In 2024, we expect to see more data that was compromised in 2023 or earlier but leaked on the darknet some time after. Prior to 2022, the difference between observed and expected infections is smaller as most compromised login credentials have been leaked.

Infection statistics by operating system

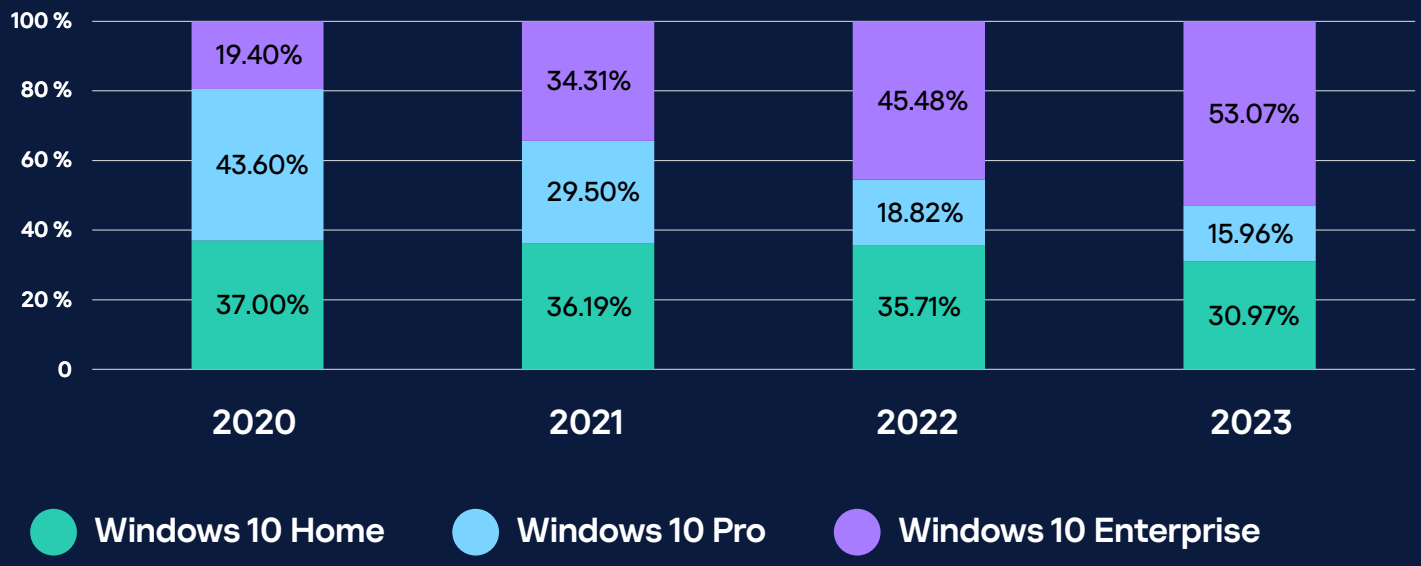
According to the metadata found in infostealer logs, the bulk of the compromised devices are powered by Windows. This can be attributed to the general popularity of this operating system, not security issues: Windows is one of the most widely used operating systems both in the home and corporate segments.

We have analyzed the infection statistics for various Windows versions: Home, Pro, and Enterprise. This data helps detect trends and split these between corporate and home users.

Windows 10 infection statistics

The diagram below shows the proportions of infections for various Windows 10 versions split by year from 2020 through 2023.

Distribution of infections across affected Windows 10 versions, 2020–2023

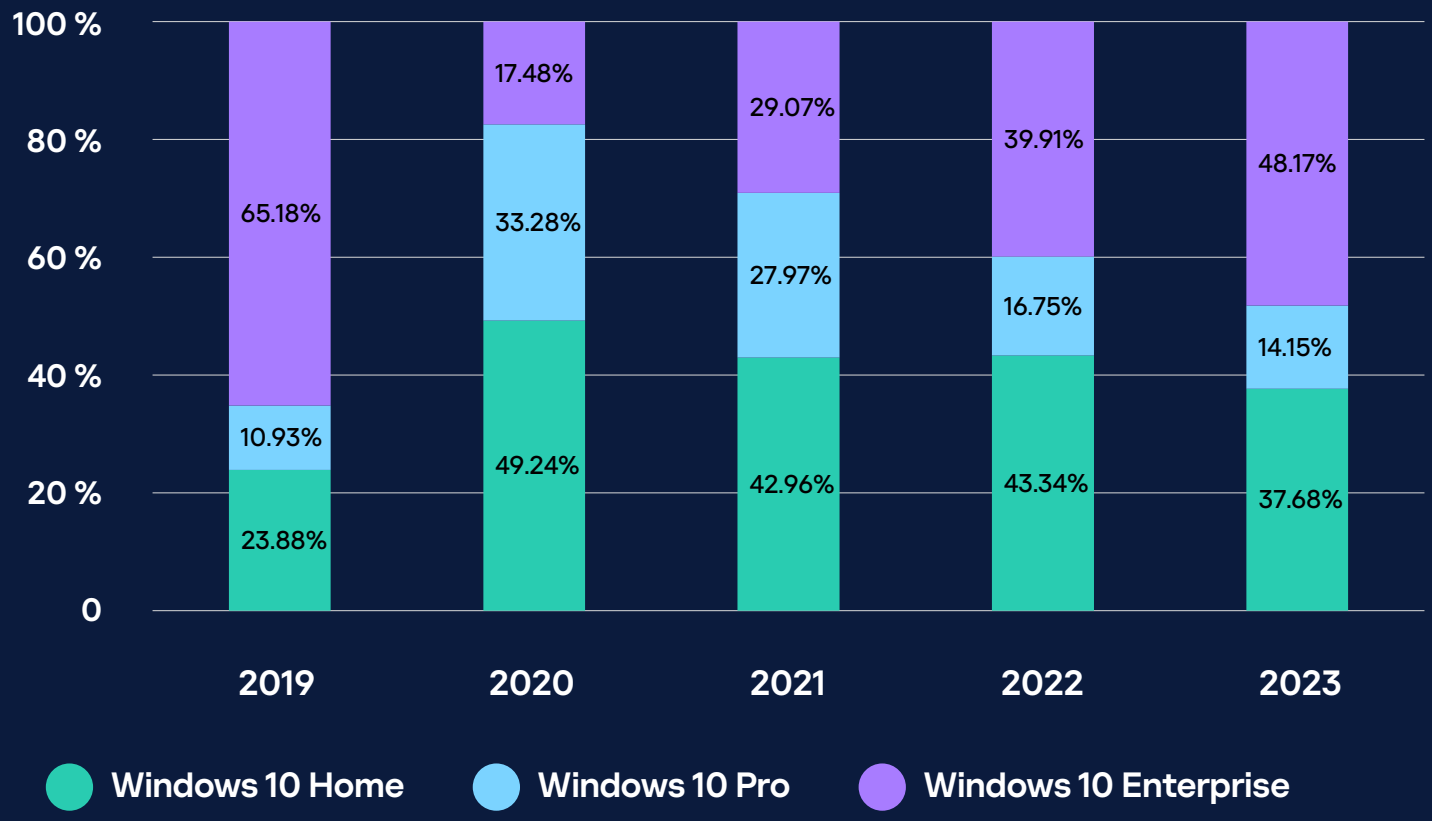


It can be seen from the diagram that the relative numbers of compromised corporate users have increased from year to year.

Corporate access availability statistics by Windows 10 version

Another trend is one associated with compromise of accounts in various Windows 10 versions that have access to corporate resources.

Compromised corporate Windows 10 accounts



A malicious actor can gather information about an employee's credentials with a corporate email as a login to an average of **1.85 web applications** from a log file.

The diagram shows that the number of accounts found in infostealer logs associated with the Home version started shrinking after 2020, the year when it also peaked.

We attribute this trend to the COVID-19 pandemic, which started in March 2020 and led to a mass transition to remote working, with employees often using their personal devices.

The latter often lack the robust security controls used in corporate environments, such as protective solutions, and corporate and password policies. This factor increases the likelihood of the device being infected, as it lacks the added security layer that prevents malware from being downloaded and run. Therefore, compromising the employee's personal device that was used to log in to work resources may lead to leakage of corporate accounts and access information.

Around 100

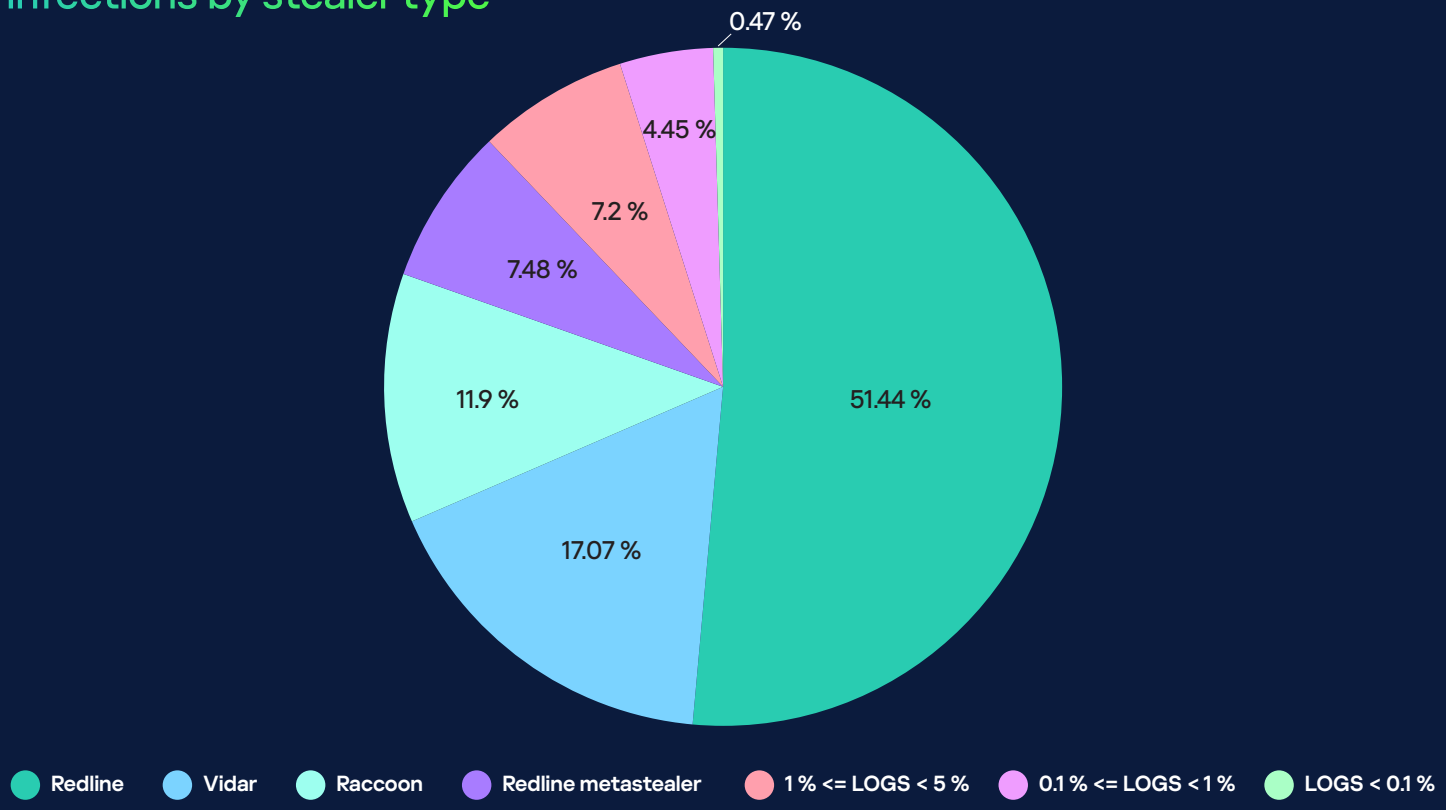
different infostealer types were found in logs[1].

[1] Data available within our field of view

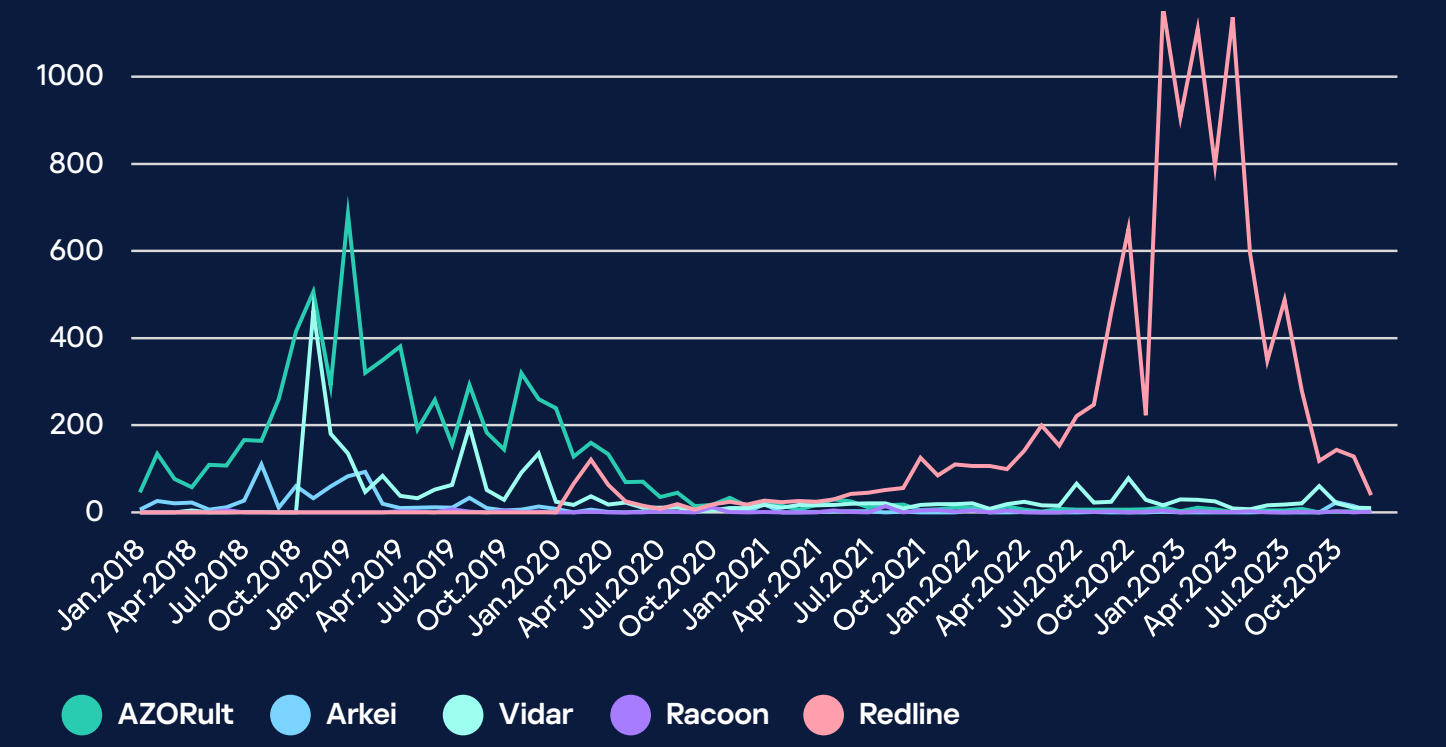
Infection statistics by stealer type

The diagram below reflects the percentages of the types that we detected in 2020–2023.

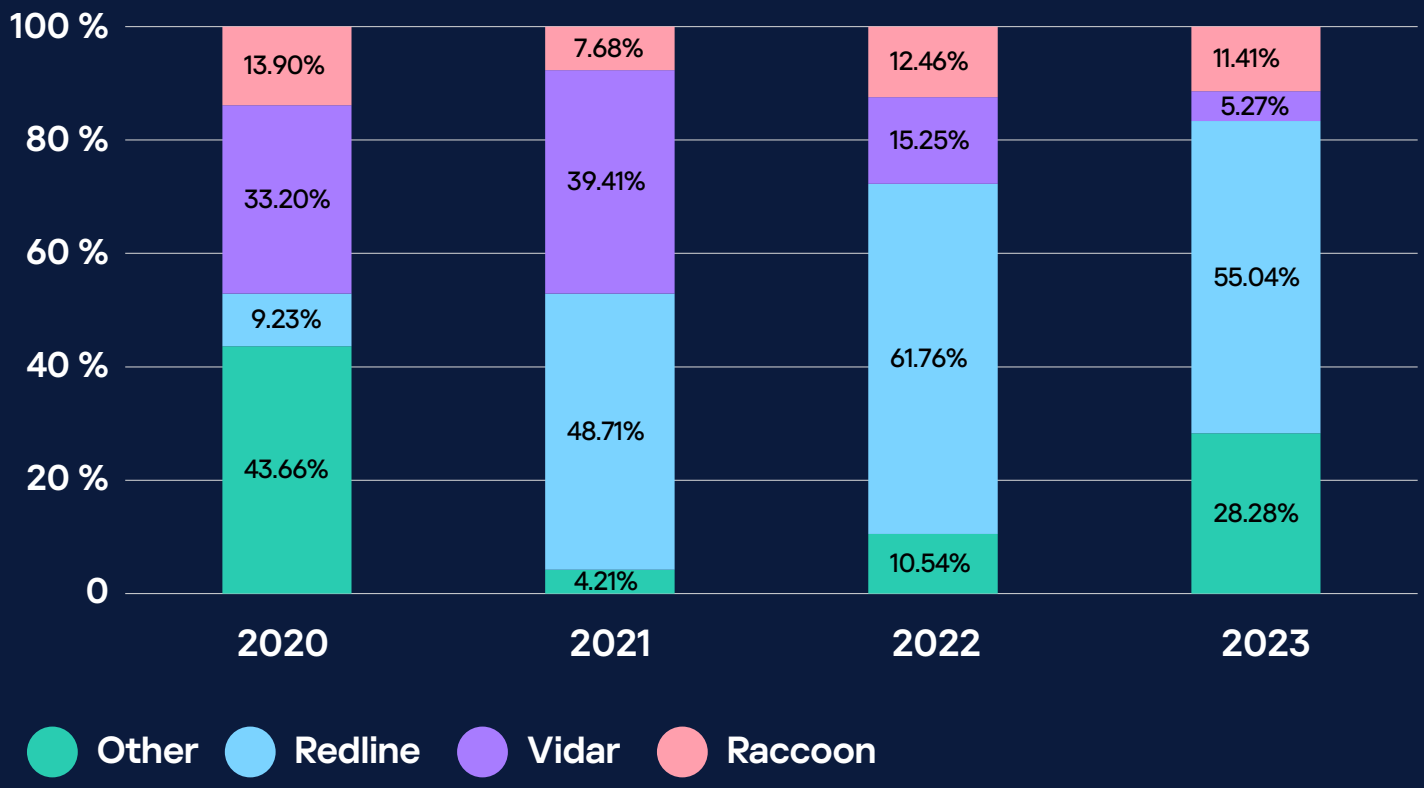
Infections by stealer type



Mentions of the different stealers on dark web forums



The changes in the popularity of the three most widespread stealers during the period looked as follows:



The share of infections attributed to new stealers increased from

4.21% to **28.28%**

in 2021–2023.

This trend is evidence of activity on the infostealer development market.

The new lumma stealer accounted for

6.38%

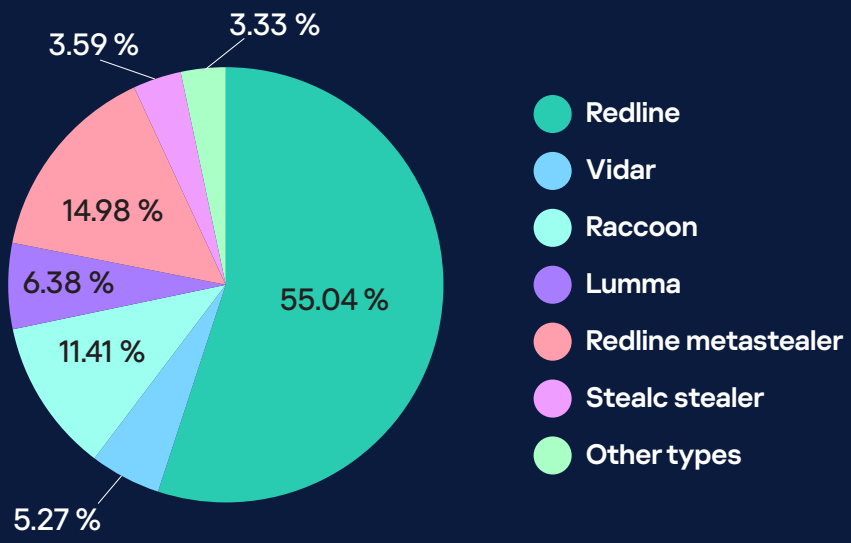
of total infections in 2023.

Redline gained popularity in 2021 and has accounted for half of all infections since then. Vidar peaked in 2020–2021, but then declined significantly in the years that followed.

Written in C, lumma emerged in 2022 and started gaining popularity in 2023 on the back of a MaaS (malware-as-a-service) distribution model. It is mostly a regular infostealer, but with an added focus on cryptowallets. It spread via sweeping email, YouTube, and Discord spam campaigns.

Among the new stealers, Stealc also stands out as it accounted for 3.59% of infections in 2023.

Infections by stealer type, 2023



Compromised credentials statistics by top-level domain

We have analyzed the number of compromised accounts with websites hosted in various regional domains. The data sample represents Latin character and generic top-level domains.

Below, you can find a list of the 30 domains with the largest number of compromised accounts in 2023. These domains experienced an average increase of 230% in the number of compromises compared to 2021.

It is important to emphasize that some domains are not only utilized for hosting local websites but also for popular international services.

For instance, streaming platform Twitch operates on the domain .tv while being international and not associated with any particular country. This fact may largely impact the frequency of compromises for the domain .tv, but, in fact, it does not necessarily correlate with the infostealer threat level in a particular country. Additional examples encompass websites such as linked.in, telegra.ph, etc. Indeed, any domain may host popular international websites, rendering them relevant targets for cybercriminals. It's essential to recognize that while the existence of such websites within the domain zone may impact the frequency of compromised accounts, it does not necessarily correlate directly with the infostealer threat level in a country linked to this domain.

	Top-level domain extension	Number of compromised credentials per domain, 2023[1]
1	.com	325,900,000
2	.br	28,800,000
3	.in	8,200,000
4	.co	6,000,000
5	.vn	5,500,000
6	.io	4,800,000
7	.tv	4,700,000
8	.mx	4,600,000
9	.fr	4,500,000
10	.es	4,400,000
11	.id	4,400,000
12	.it	4,200,000
13	.ar	4,200,000
14	.tr	3,800,000
15	.pe	3,400,000
16	.cl	2,900,000
17	.pl	2,700,000
18	.eg	2,700,000
19	.de	2,700,000
20	.sa	2,600,000
21	.ru	2,500,000
22	.uk	2,500,000
23	.pk	2,400,000
24	.nz	2,300,000
25	.th	2,200,000
26	.me	2,100,000
27	.us	2,100,000
28	.hu	2,000,000
29	.bd	1,600,000
30	.eu	1,600,000

[1] The table displays rounded numbers

Analysis of corporate systems

We used the data that we gathered to collect statistics on re-infections of corporate users.

We selected 50 banking organizations in various regions to analyze compromised employee accounts[1]. Our analysis focused on larger organizations (with 1,000 or more on the payroll), excluding those that saw only isolated infection cases.

We defined three categories of re-infection:

1

Short-term: less than three days between re-infections[2]

2

Long-term: more than three days between re-infections

3

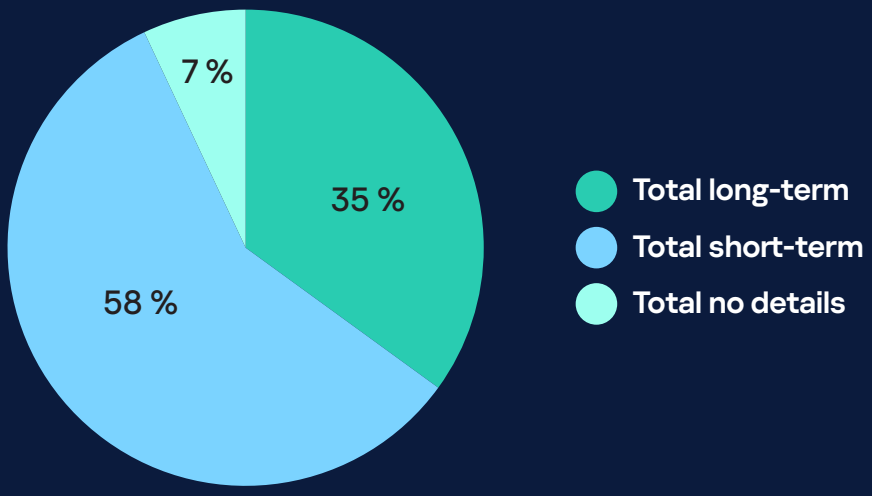
Other: the interval between infections cannot be determined from available metadata

1 The study used email addresses from log files that were found on the dark web and thought to be associated with a specific company in a sample. The compromised data was not verified in order to prevent unauthorized access to any company's infrastructure.

2 The benchmark was based on the average period within which a critical incident could be detected, taking into account weekends, holidays, and possible employee absence

According to our data presented in the diagram below, most of the re-infections fell in the short-term category, and 35%, in the long-term category.

Re-infections



Also, we can make the following conclusions:

21.07%

of all employees in review whose devices were infected ran malware again.

8.94%

of infected employees ran malware again in three or more days after getting infected for the first time.

Conclusion and advice

In the last three years, we have observed a steady increase in infostealer infections that appear within our field of vision. Windows 10 Enterprise accounts for an increasing number of compromised devices, which suggests an increase in the number of infected corporate devices.

Malicious actors are actively developing new stealers and using these in their attacks. The share of devices compromised with malware that was not present among the three most popular types rose by more than 20% in 2021–2023.

We have observed re-infection trends. Long-term re-infections may be symptomatic of several issues:

Insufficient employee awareness

Ineffective incident detection and response measures

Confidence that it is enough to change the password if the account has been compromised

Refusal to investigate the incident

Compromise of service accounts is a direct threat to the security of user and other data, but the very fact that the device has been infected suggests that data stored on it may have been leaked. Besides, in some cases, malicious actors may retain access to the infected machine for a long time.

Hence, the following are steps that must be taken if a data leak through logs has been detected:

- Immediately change the passwords for accounts that are presumed to be compromised and look for suspicious events associated with those accounts.
- Notify the users whose devices may be infected of the need to run full antivirus scans of all their devices and delete any malware they find.
- Start proactively monitoring darknet markets to detect compromised accounts before they affect the cybersecurity of customers or employees. A detailed guide on setting up monitoring can be found here;
- Use Kaspersky Digital Footprint Intelligence to stay on top of what malicious actors know about the company's resources, promptly detect potential attack vectors, and configure protection or take steps to eliminate cyberthreats in a timely manner.

To ensure efficient protection and reduce the risks associated with infostealer infection, we recommend doing the following:

- Design an employee information security awareness program, and provide regular training and performance assessments.
- Introduce a strict password policy for all corporate resources.

www.kaspersky.com