kaspersky bring on the future

The evolving threat landscape of infostealers:

trends, statistics, and mitigation strategies

Kaspersky
Digital Footprint
Intelligence

Kaspersky Digital Footprint Intelligence

Introduction

Infostealer malware has become one of the most pervasive cyber threats, targeting millions of devices worldwide and compromising sensitive personal and corporate data. These malicious programs are designed to extract credentials, cookies, financial details, and other valuable information, which is then aggregated into log files and circulated within the dark web underground community.

The Kaspersky Digital Footprint Intelligence team closely monitors infostealer activity to analyze emerging trends and assess the evolving tactics of cybercriminals. Last year, we released a report analyzing data from infostealer log files leaked on the dark web and dated between 2021 and 2023.

This report presents our latest findings for 2024, including updated statistics, insights into new and existing infostealer strains, and strategies for mitigating risks.

By understanding how infostealers operate and how their log files are distributed, organizations and individuals can take proactive measures to strengthen their cybersecurity posture. This report provides key data, actionable recommendations, and expert insights to help organizations detect, respond to, and prevent infostealer-related threats.

Check the 2024 report on infostealer threat landscape

The statistics for previous years may differ from earlier publications because older compromised credentials continue to surface on the dark web over time, and we adjust the figures for those years accordingly.

What's new in Kaspersky Digital Footprint Intelligence in 2024

Cybercriminal tools continue to advance, with malware evolving and acquiring new functionalities. However, defenders are also improving their capabilities. We have enhanced our approach to monitoring dark web resources, especially those where infostealer log files are frequently published.

The increase in analyzed data volumes necessitates updates to the analysis logic. We focused on verifying the uniqueness of added data, removing duplicates, and filtering out irrelevant information often found in log files.

In this research, a unique log file is considered to correspond to these infection of a single device.

A log file is an archive that contains stolen user data. It primarily consists of text files with account credentials, cookie parameters, and metadata. However, it may also include images, such as desktop screenshots or camera photos, as well as documents and other user files, like those stored on the desktop.

7.68%

Our ability to collect and process these log files has grown, with a 7.68% increase in the number of files gathered compared to last year.

Cybercriminals publish infostealer log files from infected devices in private sections of underground forums on the dark web. While attackers usually sell these logs, they may also share them for free after obtaining all the valuable information to boost their reputation within the cybercriminal community. We analyze these log files to identify compromised accounts. The presence of an account in these logs indicates that the user's device has been infected.

50.9

On average, a log file includes 50.9 compromised accounts. Storing passwords in text files — especially on the desktop — is highly unsafe. We strongly recommend using secure password management solutions.

How we overcome analysis challenges

Key challenge is identifying the log files' uniqueness. Log files are often reposted across multiple dark web platforms, sometimes with modifications:

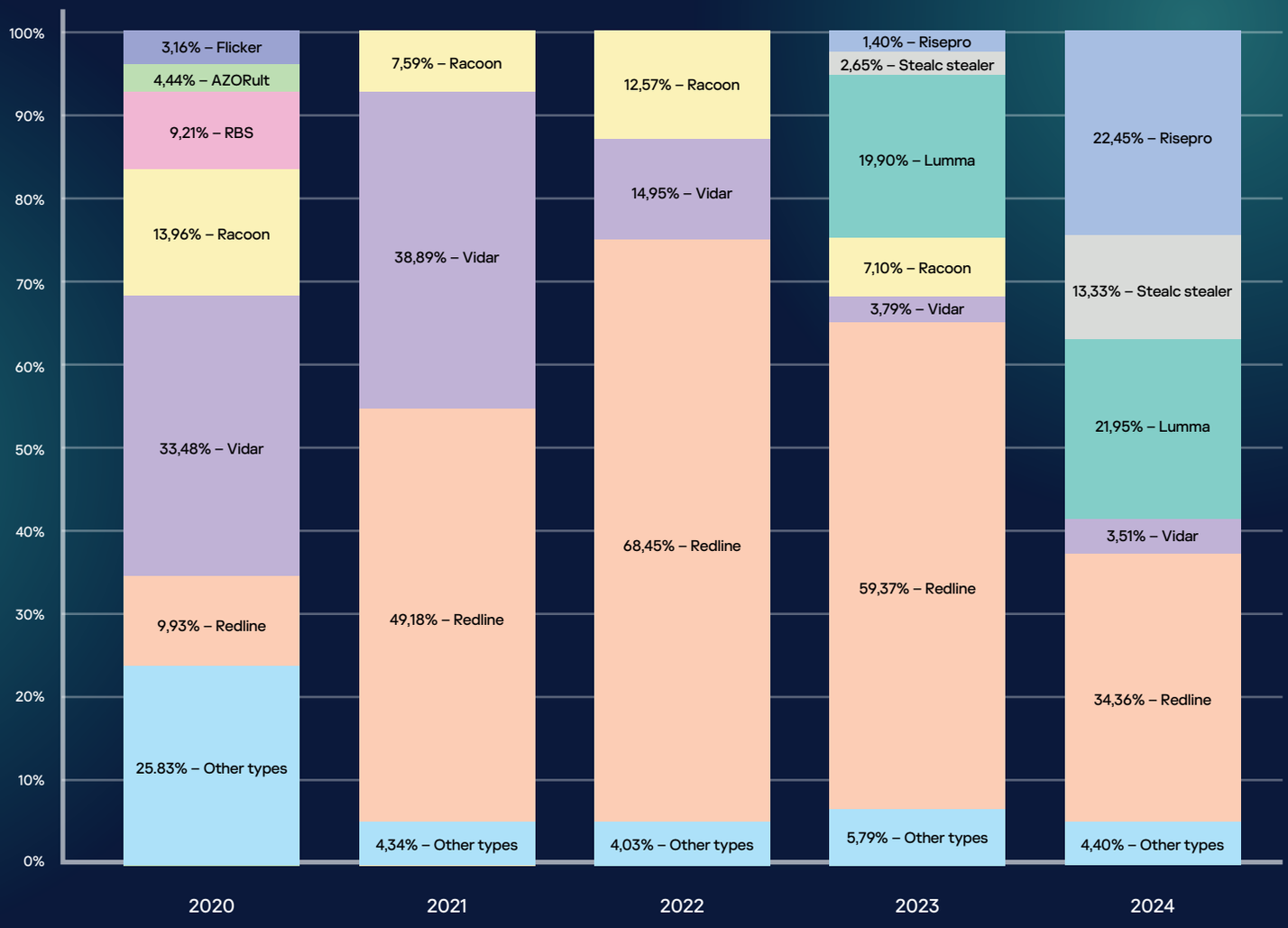
- **Added advertisements:** attackers may create separate promotional files or add links within files that have already been posted, usually in account or metadata files. Occasionally, advertisements are embedded in log file names.
- **Partial removals:** some files, such as desktop screenshots or camera images, may be deleted from the original file to reduce the log file size.
- Text file **format changes.**

These modifications affect the calculation of checksums, which can be used to determine whether a log file is unique or has already been processed before. While avoiding excessive duplicate entries is crucial, filtering too aggressively can lead to the exclusion of files that have already been considered but contain valuable new information. Moreover, excessive uniqueness checks may omit logs related to repeat infections, resulting in the loss of critical data.

Infection statistics by stealer type

A first insight from our analysis is the distribution of infections by infostealer type over the past five years (2020–2024). This data helps track the activity levels and popularity of different malware types year-on-year.

In 2024, the most infections were caused by Redline, followed by Risepro and Lumma.



Infections by stealer type, 2020-2024

Figures for 2023 have been slightly adjusted compared to last year's report. This is because more log files from 2023 were published on the dark web throughout 2024, requiring a statistical revision.

Cybercriminals often release stolen log files months or even years after the actual infection occurs. Because of this, we track both the date was published and the date the compromise actually happened. Toward the end of each year, we see more infections from previous years than we do at the start of the year. This happens because older compromised credentials continue to surface in the dark web over time.

The most significant surge in 2024 was in infection by the Risepro stealer, whose share of all infections grew from 1.4% in 2023 to 22.45% in 2024, and Stealc, which first appeared in 2023 and increased its share from 2.65% to 13.33%. In 2024, Redline remained the most prevalent infostealer, accounting for 34.36% of infections

Yearly infection trends

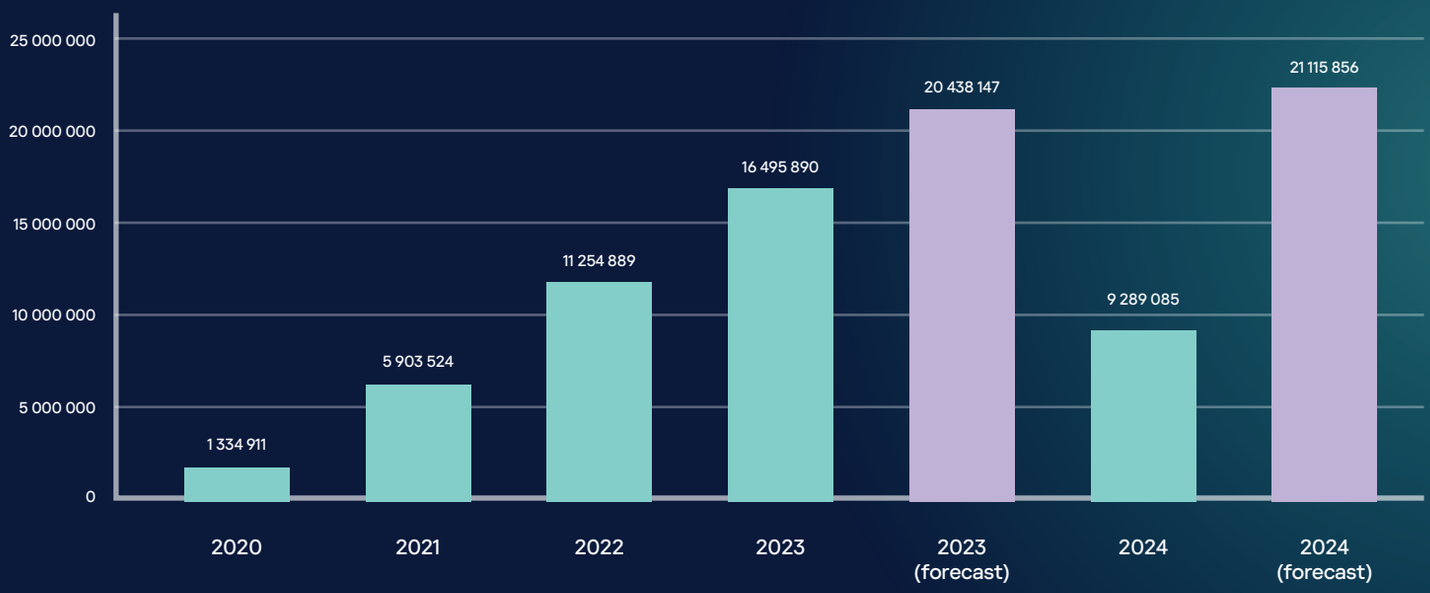
In August 2024, we projected that 15,908,793 devices had been infected with infostealers in 2023, with the logs subsequently leaked on the dark web.

2023 forecast review. In 2024, we made a forecast for the number of infections in 2023, as some log files dated 2023 had not yet been published on dark web resources. As explained in the "Context" section under "Infection statistics by stealer type", there is a time lag between the date of infection and the publication of the log file on a dark web platform.

In August 2024, we projected that 15,908,793 devices had been infected with infostealers in 2023, with the logs subsequently leaked on the dark web. As of March 2025, the number of processed log files (equivalent to infections) dated 2023 reached 16,495,890, exceeding our forecast by 3.69%.

At the beginning of 2025, we observe new log files from 2023 are still being published, indicating the total number of 2023 infections was even higher.

2024 infection trends and forecast. We estimate 2024's total infections will exceed 2023's level but remain within a comparable range. As of March 2025, 9,289,085 infections from 2024 have been observed.



Yearly infection statistics, 2020-2024

Our projected infection count:

- **2023: Between 18 million and 22 million infections.**
- **2024: Between 20 million and 25 million infections.**

Corporate email use on third-party platforms

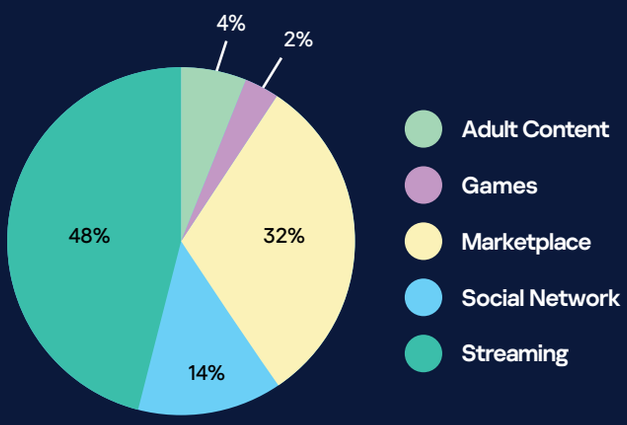
Corporate email refers to work email addresses provided by employers for professional tasks and access to company resources. Using corporate email on third-party platforms poses a cybersecurity risk, as it can lead to employee account theft. This is especially relevant if the password for a third-party resource matches the one used for corporate resources or follows a predictable pattern across different services (for example, a user might create passwords like Word2025!, where “2025” is a recurring suffix in all their passwords). Additionally, it facilitates social engineering attacks.

While some security policies allow corporate emails for work-related services (e.g., HR platforms, hosting providers), most prohibit their use for personal accounts. However, some corporate email users do use them for personal purposes, although it is challenging to assess the exact proportion.

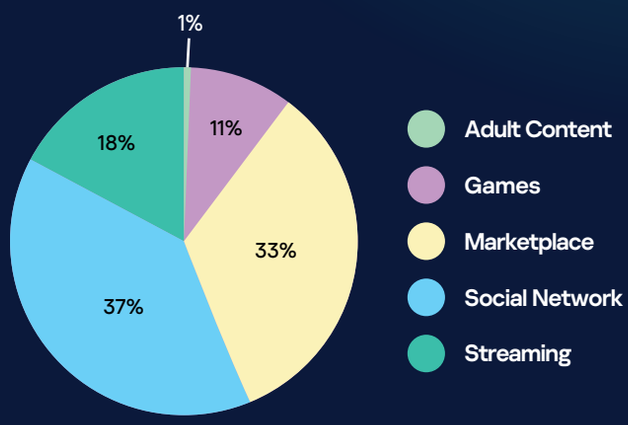
We aimed to estimate the percentage of users who registered on three popular platforms — Roblox, Discord, and Netflix — using corporate email addresses. To do this, we analyzed compromised accounts from these services where the login was in email format. Our analysis revealed that, on average, **7% of users whose accounts were leaked on the dark web had registered on these platforms with a corporate email.**

To study the issue further, we compiled a sample of 50 banking sector companies to evaluate the types of entertainment services where users register with corporate email addresses. We examined compromised credentials leaked on the dark web, linked to the corporate domains of these companies, across five to ten popular platforms in five categories: adult content, social media, gaming, marketplaces, and streaming.

Our findings revealed that employees most commonly used their work email addresses to register on streaming services, marketplaces, and social networks. In a few cases, corporate emails were also found to be used as logins on gaming platforms and adult content websites.



Corporate email usage on entertainment platforms: statistics from a sample of 50 banking sector companies



Student email usage on entertainment platforms

To approach the topic from another angle, we also explored how frequently .edu domain emails are used to register on third-party services. These domains are primarily associated with educational institutions and should be used for study-related activities. However, as our research shows, people sometimes use these domains for other purposes. Most commonly, compromised .edu emails were used to register on social media platforms and marketplaces.

Windows OS infections statistics

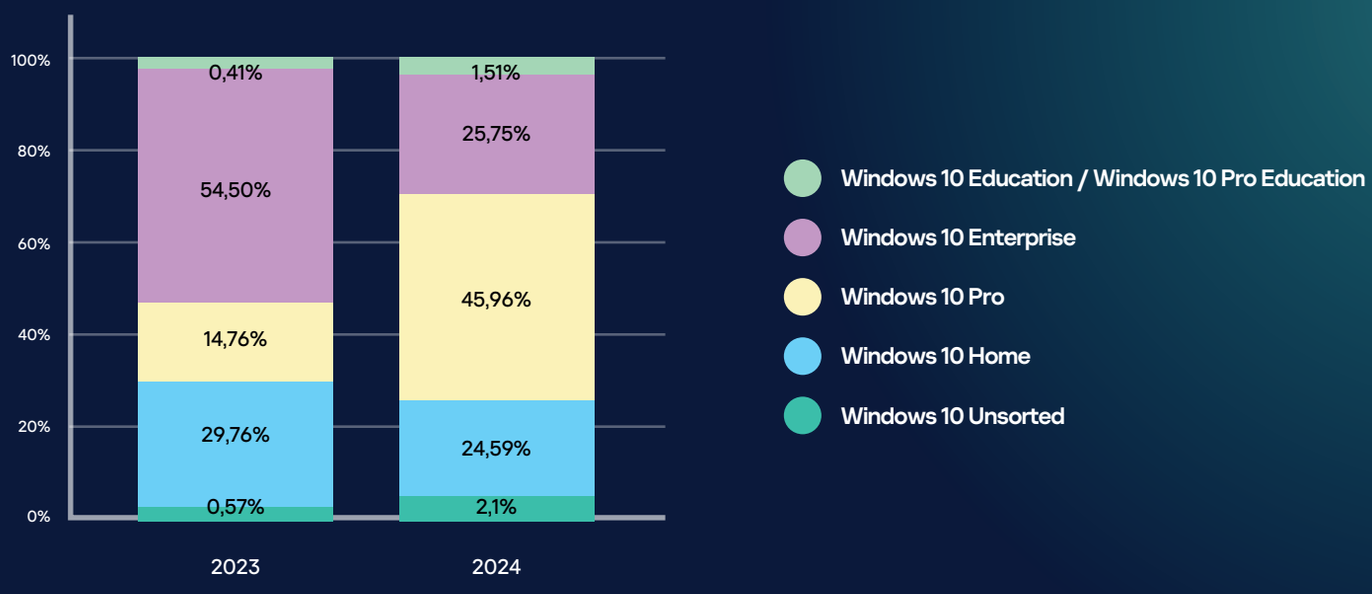
Metadata from infostealer logs indicates that most compromised desktop devices run on Windows. This is primarily due to the widespread use of the operating system rather than security flaws. Windows remains one of the most commonly used operating systems in both home and corporate environments.

To identify trends and distinguish between corporate and home users, we analyzed stealer infection statistics across different Windows versions. As mentioned above, they reveal OS popularity trends over time.

	2020	2021	2022	2023	2024
Windows 7	14,78%	8,42%	5,62%	3,67%	3,89%
Windows XP	0,02%	0,01%	0,04%	0,01%	0,00%
Windows 8.1	4,36%	2,88%	2,49%	1,96%	1,31%
Windows 8	0,62%	0,32%	0,28%	0,28%	0,17%
Windows 10	80,17%	88,41%	91,19%	92,63%	82,71%
Windows 11	0,10%	0,06%	0,21%	0,56%	↑ 11,81%
Windows Server 2012	0,08%	0,04%	0,04%	0,15%	0,01%
Windows Server 2016	0,02%	0,04%	0,05%	0,08%	0,01%
Windows Server 2019	0,10%	0,06%	0,05%	0,09%	0,03%
Windows Vista	0,03%	0,02%	0,04%	0,12%	0,00%
Windows Server	0,21%	0,14%	0,29%	0,63%	0,09%

Infected devices by Windows OS version, 2020-2024

In 2024, we observed the start of a migration from Windows 10 to Windows 11, with Windows 11 infections increasing from 0,56% in 2023 to 11,81% in 2024.



Windows 10 Versions: infostealer infection statistics (2023–2024)

In 2023, we found that every second device (55%) infected with infostealers was corporate. This conclusion was based on data showing that the highest number of infections occurred on Windows 10 Enterprise. In 2024, the share of infections in the Windows 10 Enterprise declined, possibly indicating that companies are accelerating their migration to a newer operating system as part of their cybersecurity efforts.

Insights into other Windows versions show that although the share of infections on the unlicensed version of Windows 7 remains below 1%, there has been a slight increase in infections on this platform, likely due to weaker or absent security mechanisms in unlicensed versions.

	2020	2021	2022	2023	2024
Windows Seven Black Edition	0,09%	0,09%	0,07%	0,08%	0,20%
Windows 7	99,91%	99,91%	99,93%	99,92%	99,80%

Windows 7 Versions: infostealer infection statistics (2020–2024)

Compromise of financial data statistics

95%

of the bank card numbers contained in the log files leaked on the dark web appear technically valid.

For 44% of the log files collected in 2023 and 2024, we were able to analyze data on compromised bank cards. While the share of leaked cards is far less than 1% of the cards in circulation worldwide as of 2024, we found that 95% of the bank card numbers contained in the log files leaked on the dark web appear technically valid.

The analysis also revealed that, on average, each log file contains 0.071 cards, or roughly one card in every 14 log file.

Every 14th infostealer infection leads to a stolen credit card.

Conclusion

The evolving threat landscape of infostealers highlights the importance of proactive cybersecurity measures. Our findings indicate that cybercriminals continue refining their methods, while defenders must stay ahead through improved detection and response strategies.

What to do if your company was mentioned on the Dark Web?

If data leak by infostealer is detected, the following steps should be taken immediately:

- **Change compromised account passwords** and monitor for suspicious activity associated with those accounts.
- **Notify affected users** and instruct them to run full security scans on all devices, removing any detected malware.
- **Monitor darkweb markets** proactively to detect compromised accounts before they pose risks to customers or employees. A detailed guide on setting up monitoring can be found here.
- **Leverage Kaspersky Digital Footprint Intelligence** to track what cybercriminals know about your company's assets, identify potential attack vectors, and implement protective measures in a timely manner.

To enhance protection and mitigate the risks of infostealer infections, we recommend:

- **Implementing a security awareness program** for employees, including regular training and performance assessments.
- **Enforcing a strict password policy** for all corporate resources to reduce credential-related vulnerabilities.

By adopting these measures, to reduce the risks of encountering credential-related cyber threats organizations can strengthen their defenses against infostealers and minimize the impact of potential breach

Your Step-by-Step Guide: What to Do If Corporate Accounts Are Compromised

Type of account	Recommendations

Active Directory domain account
 	
Administrative account
 	
Account for a corporate system
	• Verify the presence of a user with specified login name.
	• Initiate investigation and response procedures, if login's presence was verified. Make sure to include the following steps:
	  ◦ Perform a full antivirus scan on affected user devices and corporate machines and remove any detected malware.
	  ◦ Enforce a password reset for the compromised account.
	  ◦ Analyze log events for unusual activities such as failed logins, attempts of privilege escalation, etc.
	• Enable MFA (Multi-factor authentication) for all corporate systems, if not already implemented.
	• Strengthen password policy according to security best practices, where applicable.
	• Enhance employee awareness regarding cybersecurity to mitigate risks posed by malware infections.
	• Ensure that current Endpoint Protection Platform (EPP) is capable of detecting, mitigating, and removing infostealer malware.

Type of account	Recommendations
Employee account for third-party resource	• Verify the presence of a user with specified login name. • Inform affected employee about discovered account - an indicator of compromise. • Recommend affected employee to perform a full antivirus scan on affected user devices and corporate machines and remove any detected malware. Advise them to reset their passwords afterwards. • Enhance employee awareness regarding cybersecurity to mitigate risks posed by malware infections. • Restrict employees from use of corporate email addresses for authentication on external resources. • Ensure that current Endpoint Protection Platform (EPP) is capable of detecting, mitigating, and removing infostealer malware.

Client account	• Verify if mentioned account exists. Determine whether the account belongs to a client or to an employee.
	• Inform the affected user about the compromise.
	• Initiate investigation and response procedures:
	  ◦ Force a password reset for affected user.
	  ◦ Check event/application logs for any unauthorized access or unusual activity.
	  ◦ If the account is confirmed to belong to a client, ask them to perform full antivirus check of their devices.
	  ◦ If the account belongs to an employee, perform a full antivirus scan on affected user devices and corporate machines, and remove any detected malware.
	• Enable MFA (Multi-factor authentication) for affected application, if not already implemented.
	• Strengthen password policy according to security best practices, where applicable.
	• Enhance employee and client awareness regarding cybersecurity to mitigate risks posed by malware infections.

www.kaspersky.com

https://dfi.kaspersky.com/