Swascan
TINEXTA GROUP

Botnets and infostealers

Financial threat landscape 2023

www.swascan.com

Summary

Botnet and infostealer

Botnets pose a significant and insidious threat. Their resistant nature to mitigation efforts makes them particularly dangerous. Through analysis by Swascan's Cyber Security Team, not only have botnets that have directly affected Italian financial sector assets been identified, but also those that may have infected personal devices or those used by employees in remote work mode.

Connecting to business applications from infected devices can have devastating consequences. Malware such as InfoStealers can steal login credentials, financial information, personal data, credit card information, and confidential documents.

Subsection Extra #1 depicts the results of an analysis conducted on a sample of 30 Italian banks, equally divided between "significant" and "less significant" aimed at examining the presence of compromised devices and risks from data breaches considering the period between 2022 and 2023.

In detail, between 2022 and 2023 out of the 30 banks analyzed, a total of 48,565 devices were found to be infected by InfoStealer; specifically, it went from a total of 19,806 in 2022 to 28,759 credentials exfiltrated by InfoStealer in 2023 that stole current account login credentials but at the same time financial information, personal data, credit card information, and confidential documents, an increase of 45.2 percent.

One of the main observations, then, is the evident growth in the use of InfoStealer-type malware for credential exfiltration, involving both bank employees and end customers. Overall, an amount of 105,777 infected devices belonging to internal users, external users, end customers and devices from which cookies, autofills, history and documents were exfiltrated were found.

Contrary to this trend, the use of combolists is decreasing, highlighting a transition in attackers' tactics. In 2023, combolists totaled 1,148 compared to 9,486 in 2022, signaling a contraction in the approach to credential list publication. This translates into a significant percentage difference of 87.9 percent, indicating a significant decrease in the number of combolists published this year compared to the previous year.

In addition, subsection Extra #2 provides an overview of the main InfoStealers identified in the context of the analysis conducted.

Finally, in subsection Extra #3 an in-depth study was conducted regarding the main motivations behind the increasing use of InfoStealer-type malware through the examination of some underground forums where such malware is offered for sale.

---

[1] *The banks selected for analysis were classified as "significant" and "less-significant" according to the classification of the European Central Bank (ECB).*

[2] *Combolists are lists that contain previously compromised and publicly disclosed username and password combinations from data breaches on third-party websites. An attacker can benefit greatly from these combolists because they contain sensitive information from corporate accounts, including corporate email addresses and passwords.*

A dangerous synchronicity

Botnets and infostealers are often used in combination to conduct cyber attacks.

A botnet can be used to distribute and manage malware, including InfoStealers. Infected devices within the botnet can be exploited to spread malware on a massive scale, thereby increasing the number of vulnerable systems.

When InfoStealers have been installed on target devices they collect sensitive information and send it to the botnet command and control. The botmaster can then use this information for fraudulent purposes, such as identity theft or compromising access credentials by ensuring persistence within the target system.

This allows criminal hackers to obtain up-to-date information from affected devices even if new services and/or credentials get registered.

In the simplest terms, the botnet provides the control and distribution infrastructure, while infostealers collect sensitive information from the infected devices within this network. Integrating both these threats allows attackers to orchestrate sophisticated attacks and gain wider access to valuable data.

Subsection Extra #1 shows the results of an analysis of a sample of 30 Italian banks broken down equally into “significant” and “less significant”21 banks. The study examined the extent of compromised devices and the risks arising from data breaches in 2022 and 2023. Of the 30 banks analysed in the years 2022 and 2023, a total of 48,565 devices were found to be infected by InfoStealers. The figure for credentials exfiltrated by InfoStealer in 2022 was 19,806, rising by 45.2% to 28,759 in 2023. The thefts included not only current account access credentials, but also financial information, personal data, credit card information and confidential documents.

Subsection Extra #2 provides an overview of the main InfoStealers identified in the context of the analysis conducted.

Finally, subsection Extra #3 reports an in-depth study of the main reasons behind the ever-increasing use of InfoStealer-type malware. The investigation focused on some underground forums where such malware is offered for sale.

Notable Insights

Redline, Raccoon and Arkei were the top three most detected InfoStealers that compromised devices in the 30 banks surveyed.

The results of the analysis shown show clear growth in the use of InfoStealer-type malware, affecting both bank employees and external users. The results also show a significant increase in the number of compromised devices in 2023 compared to 2022. This rise could be attributed to the increased use of InfoStealer-type malware by attackers. This trend highlights the importance of adopting a multi-layered, proactive defence system to counter an ever-changing threat landscape.

Further confirmation of the trend comes from an investigation of the underground forums most frequented by cybercriminals. The growing number of threat actors developing and selling new InfoStealers with new features is evidence of an increasingly dynamic and sophisticated environment.

At the same time, a decrease in the use of combolists22 was noted, indicating a change in attackers' tactics. In 2023, the number of combolists totalled 1,148 compared to 9,468 in 2022, signalling a radical change in attitudes to publishing credential lists. The reduction in published combolists can be interpreted as a strategic change by attackers and appears to be backed by the increasing number of devices infected with InfoStealers.

In addition, the analyses show a marked decrease in data breaches in 2023 compared to the previous year.

Corporate emails appear in data breaches and combolists usually because corporate accounts have been used for third-party service memberships. This can lead to risk situations such as:

- Theft of social media accounts;
- Credential stuffing attacks;
- Targeted phishing attacks.

Combolists are highly valued because the attacker knows that an employee has used his or her corporate email on a third-party site that has suffered a data breach. This situation then leads the way to targeted phishing attacks where the attacker can try to persuade the employee to provide additional sensitive information or perform malicious actions within the corporate environment.

TIP The implications of the findings of this analysis are significant, drawing attention to the new challenges facing the banking industry in its efforts to protect sensitive information and critical assets. In view of this escalation of threats, it is imperative that financial institutions adopt advanced security measures; they must implement proactive strategies and cutting-

edge technology solutions to effectively prevent, detect, and mitigate botnets and security breaches.

EXTRA Analysis of compromised devices and data breaches Among “less-significant” and “significant” Italian Financial institutions

The main goal of the study is to carefully assess the cyber threats that can compromise the integrity and confidentiality of banks’ data, focusing specifically on three categories of botnet:

- Botnet-internal: this involves infected devices where credentials with corporate email addresses associated with scanned domains and domain credentials for access to internal portals have been exfiltrated.
- Botnet-external: focuses on infected devices outside the analysed banking organizations, which may include customers and bank users or outside visitors to the site.
- Botnet-other: includes cookies and autofills associated with the domains investigated. This categorisation aims to identify any traces of sensitive data or access to critical information through devices connected to or outside of the infrastructure.

At the same time, attention was given to the numbers of infected devices responsible for stealing access to corporate mail portals. They were considered separately from infected devices from which domain credentials were exfiltrated.

Significant institutions analysis

The total number of data breaches identified since 2016 for internal users is 38,174, of which 712 were compromised email accounts from InfoStealer and 37,462 combolisted email accounts. Itis important to note that this number includes both botnet-compromised corporate accounts and corporate emails occurring in combolists. Remember also in the total count, if a single account occurs in multiple combolists, it will be counted multiple times.

In the overall picture of identified data breaches, an interesting fact emerges. Regarding the last two years, we found 2,042 data breaches in 2023 and 10,166 in 2022. This is a significant 79.8% difference,

pointing to a marked decrease in data breaches during 2023 compared to 2022.

A closer look at the analysis shows that 1,062 emails belonging to internal users and/or external employees with corporate emails associated with analysed bank domains were identified in combolists in 2023, compared to a total of 8,945 in 2022. This is a significant 88.1% difference, indicating a significant decrease, from last year to this year, in the number of users associated with employees and collaborators occurring in published combolists. This suggests that the threat actors' attention is shifting to credentials exfiltrated by InfoStealers.

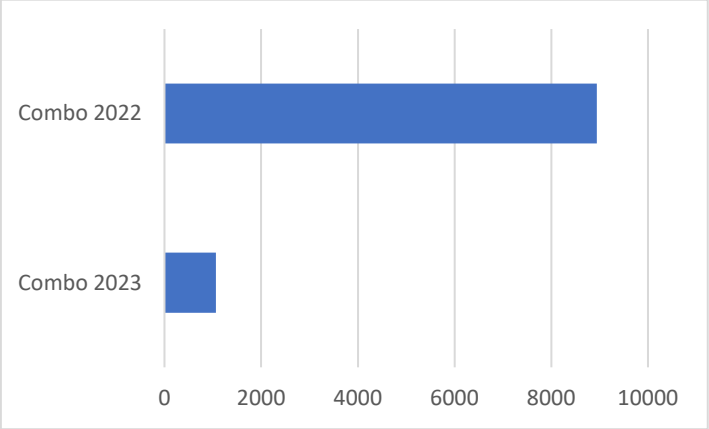

Figure 1: Comparison of the occurrence of corporate emails of Italian banks in combolists (2022-2023) - significant cluster

The reduction in published combolists can be interpreted as a strategic change by attackers and appears to be backed by the increasing number of devices infected with InfoStealers. In fact, the analysis that focused on the 15 "significant" banks identified a total of 51,971 devices (in this case, the figure refers to botnet-internal and botnet-external together, whereas previously the study covered internal users only) infected by botnets. It should be noted that this number indicates only infected devices from which credentials were exfiltrated, and voluntarily excludes devices from which cookies and autofills were exfiltrated. They number 39,622 (classified as botnet-other), making a total of 91,593 compromised devices.

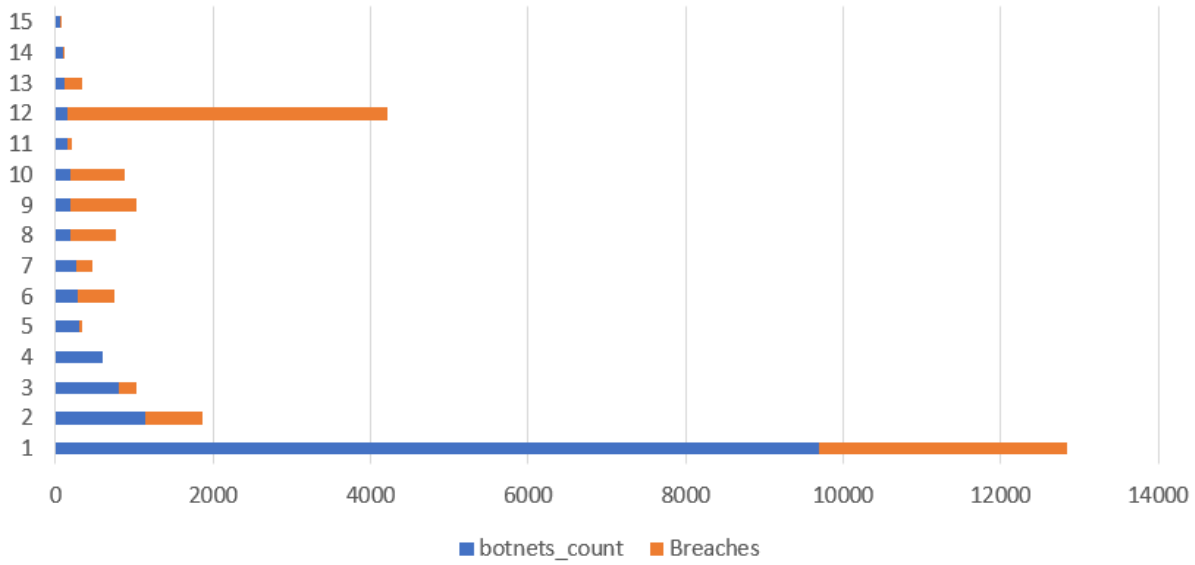

Figure 2: Compromised devices vs. data breaches - significant cluster

The analysis conducted in the 2022/2023 period revealed a significant increase in the overall number of infected devices, resulting in the exfiltration of credentials of both internal and external users of the banking organisations analysed.

As regards the 51,971 botnet-infected devices from which credentials were exfiltrated, in 2022 the total number of infected devices was 17,350, while in 2023 this figure rose to 26,308. This is an increase of 51.6%.

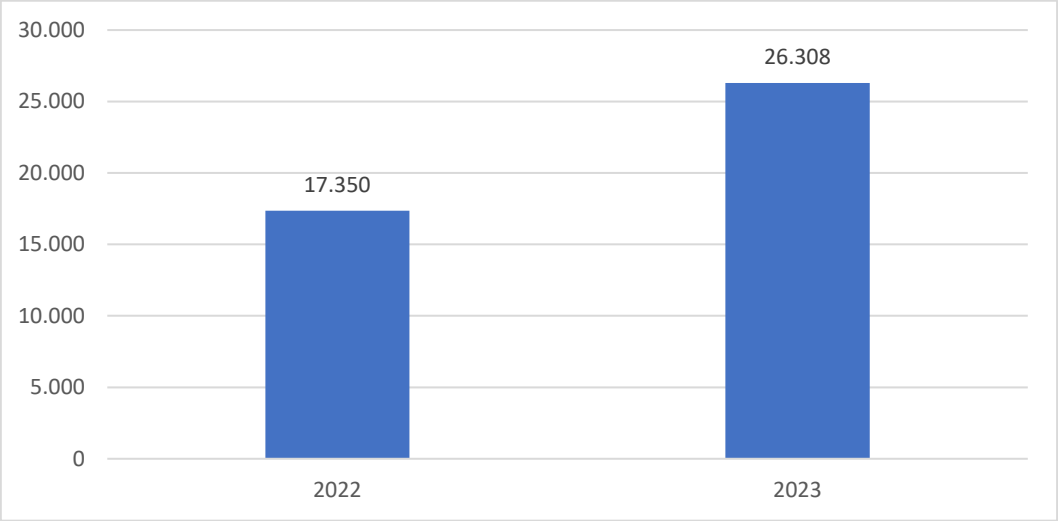

Figure 3: Infected devices from which credentials were exfiltrated (2022-2023) - significant cluster

Of the total number of infected devices, 1243 of them (botnet-internal) had internal credentials. Specifically, as stated above, credentials with corporate emails were exfiltrated in

712 cases, while Active Directory domain credentials were exfiltrated in the remaining 531 cases.

Looking at the 15 "Significant Institutions" (SI) analysed:

- One SI has no infected devices from which credentials including corporate email logins were exfiltrated;
- Six SIs have between 1 and 10 infected devices from which credentials including corporate email logins were exfiltrated;
- Five SIs have between 11 and 50 infected devices from which credentials including corporate email logins were exfiltrated;
- Three SIs have more than 50 infected devices from which credentials including corporate email logins were exfiltrated.

Additionally:

- Three SIs have no infected devices from which credentials including access with domain credentials were exfiltrated;
- Six SIs have between 1 and 10 devices from which credentials including access with domain credentials were exfiltrated;
- Four SIs have between 11 and 50 devices from which credentials including access with domain credentials were exfiltrated;
- Two SIs have more than 50 devices from which credentials including access with domain credentials were exfiltrated.

The following graph shows the distribution of credentials associated with various critical portal types:

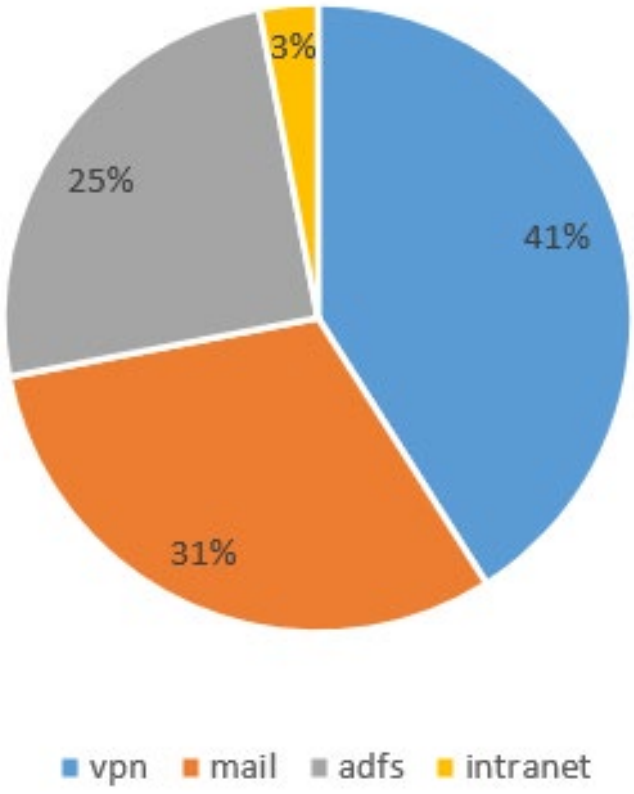

Figure 4: Distribution of stolen credentials on critical portals - significant cluster

Less-significant institutions analysis

The analysis of banks classified as less significant threw up some interesting dynamics. Again, the study showed a higher incidence of devices compromised by InfoStealer-type malware compared to the publication of combolists, which shows a decline.

For the 15 banks analysed, a total of 14,184 compromised devices were found, including, therefore, botnet-internal, botnet-external and botnet-other. A total of 11318 internal users included in data breaches, where corporate email was compromised, was detected from 2016 onwards. A more detailed analysis found a distinction between data from 2023 and 2022, revealing that 132 of these breaches were from 2023, while 710 were published in 2022.

Also noteworthy here is the change in the publication of combolists: in 2023, 86 internal users were found in combolists, compared to 541 in 2022. This is a significant 84.1% decrease in the occurrence of internal emails or corporate email collaborators of the analysed domains within the combolists for the analysed cluster.

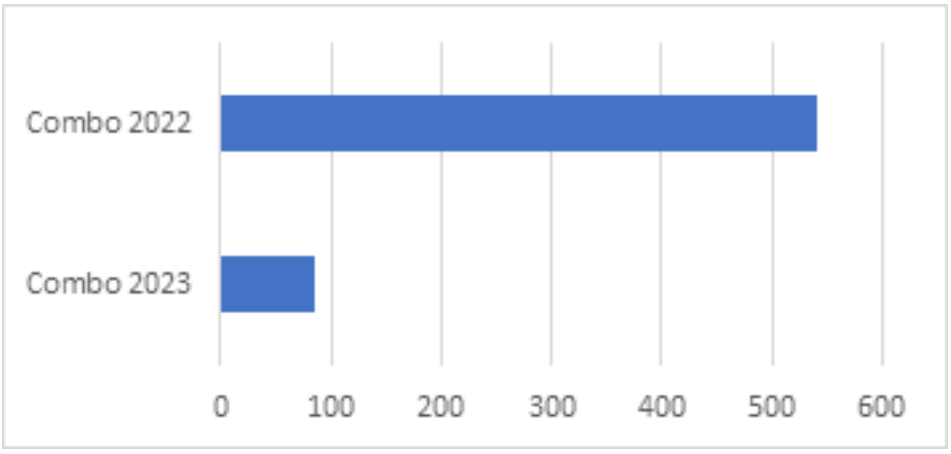

Figure 5: Comparison of the occurrence of corporate emails of Italian banks in combolists (2022-2023) - less significant cluster

The analysis reveals a total of 14,184 infected devices, taking into account both internal and external devices that accessed banking portals, as well as devices from which cookies and autofills were exfiltrated. By further refining the investigation and focusing exclusively on the devices from which credentials were exfiltrated, including employees and customers who accessed banking portals, the total number of infected devices is 6,539. Of these, 187 are internal (users with exfiltrated email addresses and domain users) and 6,352 are from external sources.

Of these 187 cases, 106 corporate email credentials were exfiltrated for the purpose of accessing the internal and external portals of the organisations analysed, together with 81 Active Directory domain users.

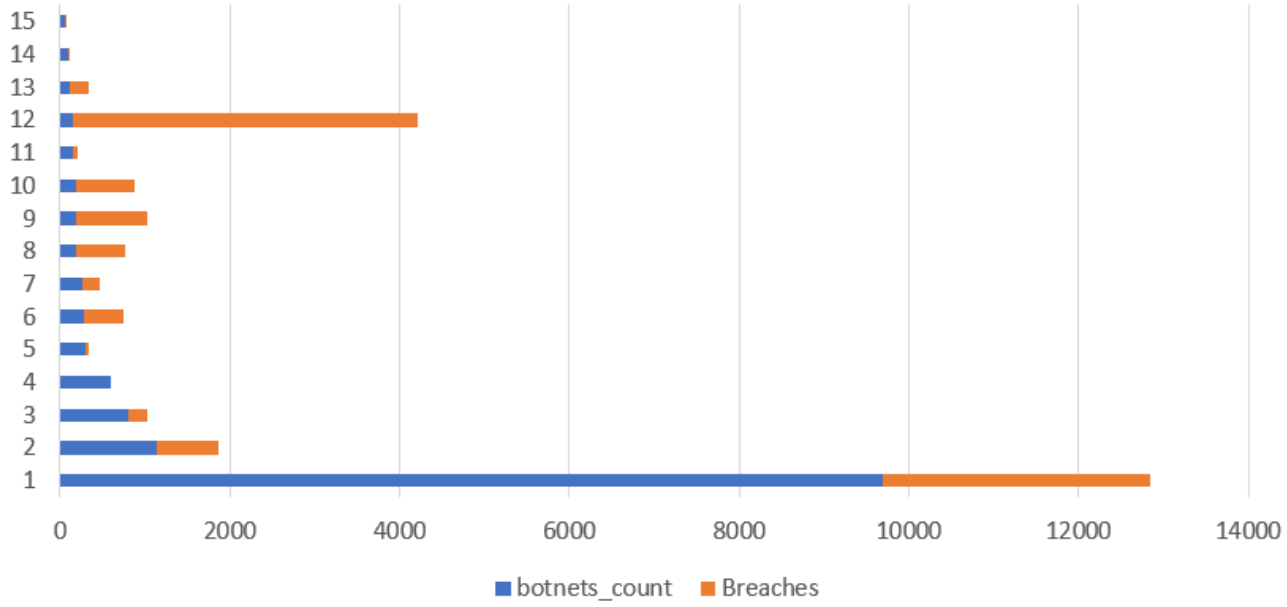

Figure 6: Compromised devices vs. data breaches - less significant cluster

As regards the 6539 total infected devices (taking botnet-internal and botnet external together) from which credentials were exfiltrated, the total number of exfiltrated credentials in the last two years is 4907; of these, 2456 credentials were exfiltrated by InfoStealers in 2022, whereas the number was 2451 in 2023.

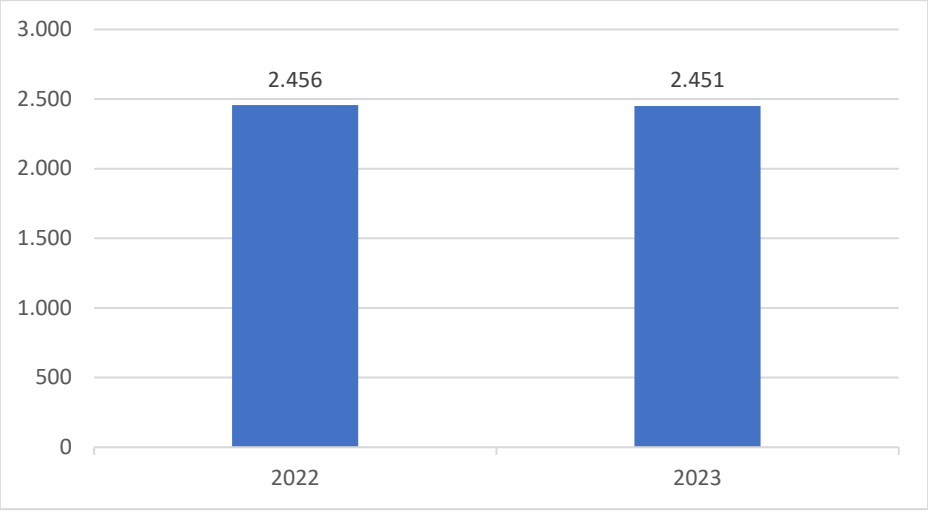

Figure 7: Infected devices from which credentials were exfiltrated (2022-2023) - less significant cluster

Looking at the 15 "Less- significant institutions" banks (LSI) analysed:

- One LSI has no infected devices from which credentials including corporate email logins were exfiltrated.
- Eleven LSIs have between 1 and 10 devices from which credentials including corporate email logins were exfiltrated.
- Three LSIs have between 11 and 50 devices from which credentials including corporate email logins were exfiltrated.
- No LSIs have more than 50 devices from which credentials including corporate email logins were exfiltrated.

Additionally:

- Four LSIs have no infected devices from which credentials including access with domain credentials were exfiltrated.
- Eight LSIs have between 1 and 10 devices from which credentials including access with domain redentials were exfiltrated.
- Three LSIs have between 11 and 50 devices from which credentials including access with domain credentials were exfiltrated.
- No LSIs have more than 50 devices from which credentials including access with domain credentials were exfiltrated.

The following graph shows the distribution of credentials associated with various critical portal types:

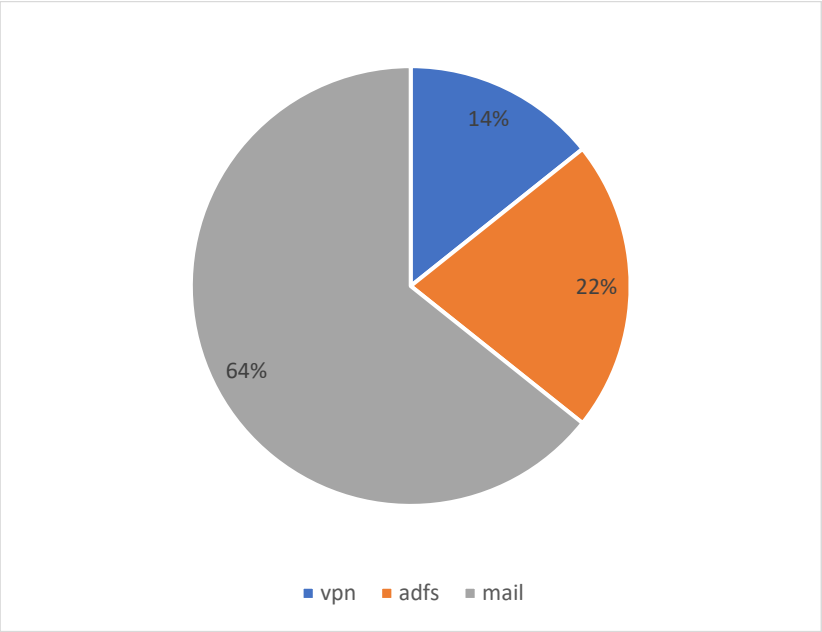

Figure 8: Distribution of stolen credentials on critical portals - less significant cluster

Top 15 infostealer families

The following analysis provides an overview of the main InfoStealers identified during the analysis. The top 15 malware apps identified during the analysis are:

Anubis	Arkei	Azorult	DarkCrystal	Ficker
Krot	LummaC	Nexus	Oski	Predator
Raccoon	RedLine	StealC	Taurus	Vikro

For the 30 banks surveyed, a total of 58,510 exfiltrated credentials linked to banking activities emerged. (The sample took into account botnet-internals and botnet-externals relating to "significant institutions" and botnet-internals and botnet-externals relating to "less significant institutions"). Of these, the 15 InfoStealers identified were responsible for the exfiltration of 52,326 internal and external credentials (27,405 in 2023 alone). The remaining credentials were exfiltrated by InfoStealers from unidentified families, listed in the chart below as "other".

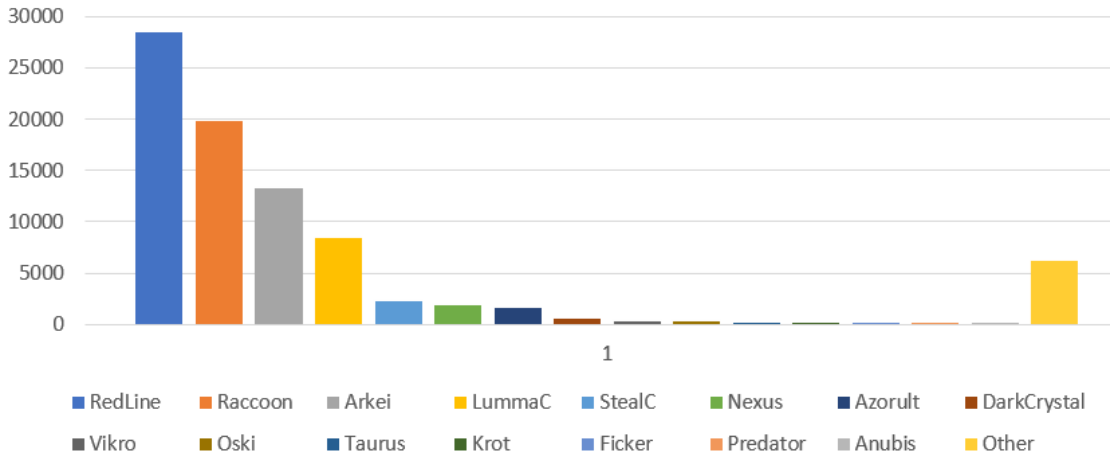

Figure 9: Top 15 identified InfoStealers found in the 30 banks surveyed

Focusing on the cluster of 15 "significant" banks, a detailed picture emerges of data exfiltrations caused by 15 specific InfoStealers. Altogether, these malware were responsible for 46,692 data compromises, 25,054 of which occurred in the year 2023 alone.

Redline comes out on top with a total of 17,257 compromises, 9,160 of which occurred in 2023. In second place is Raccoon, with 11,463 total compromises, 7,128 of which were detected in 2023. In third place was Arkei, with a total of 9,537 compromises, including 2,367 in 2023.

One interesting element is LummaC's fourth place in the overall ranking of significant banks, having taken third place in 2023. It is a malware app that appeared this year and totalled 4,060 exfiltrations for the cluster under examination. This suggests a rapid spread and significant impact in the short survey period.

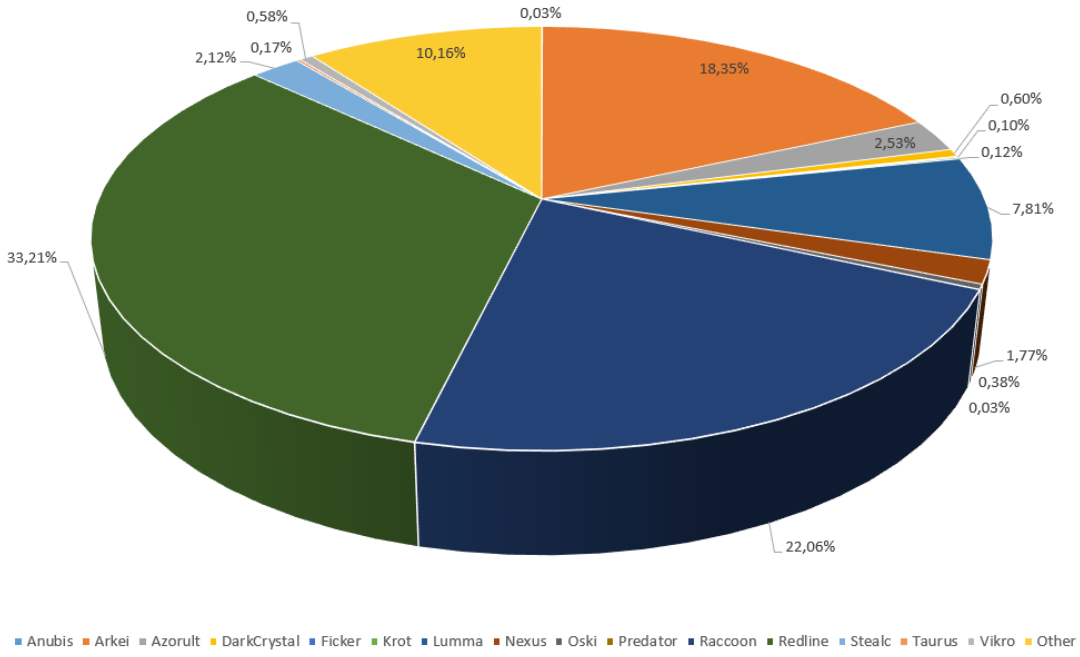

Figure 10: Top 15 identified InfoStealers - significant clustert

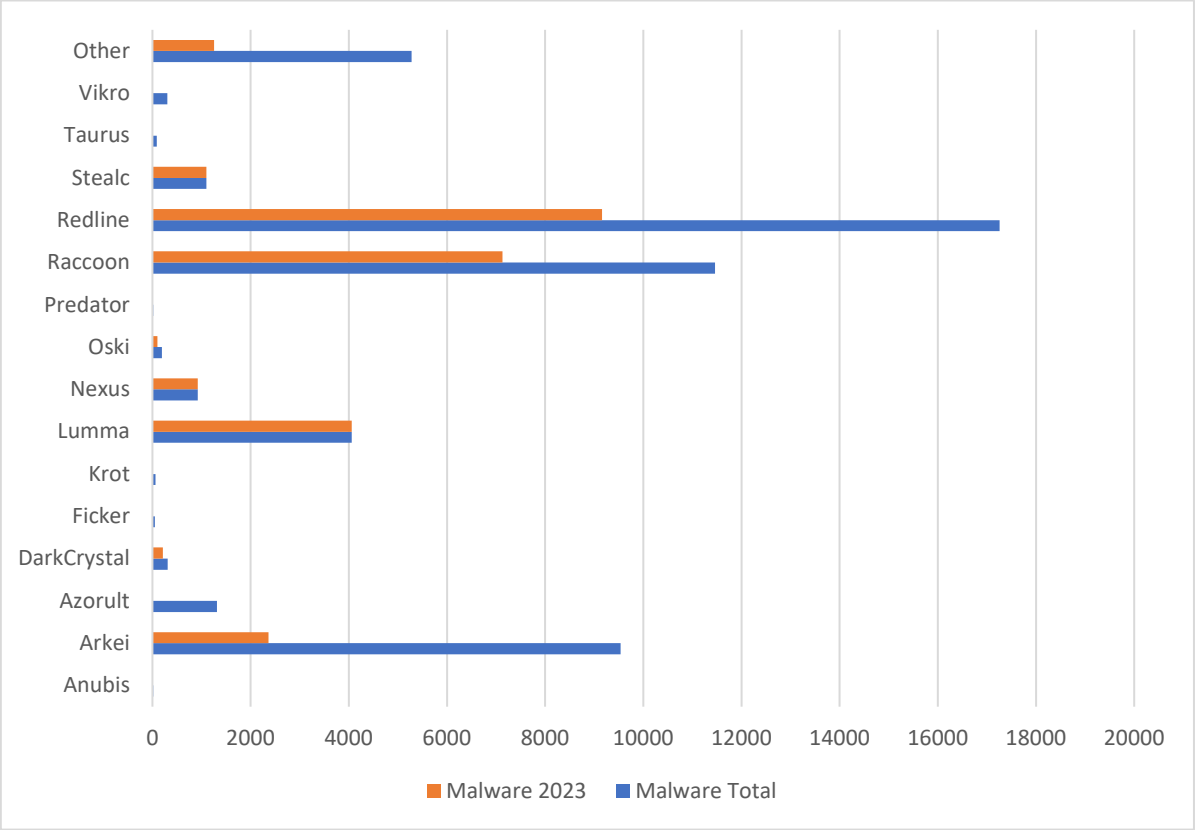

Figure 11: InfoStealer total vs 2023 - cluster significant

Extending the analysis to the cluster of 15 "less significant" banks, a similar picture emerges with regard to the 15 malware in question. Redline remains dominant in the top spot, accounting for 37% of total exfiltrations. Redline was responsible for a total of 2,089 exfiltrations, 1,025 of which occurred in 2023.

In second and third place in the overall ranking are Arkei (24%) and Raccoon (23%) respectively. Looking at 2023 only, the podium is occupied by Redline, Raccoon, and LummaC, with a total of 327 exfiltrations.

Overall, the 15 malware programmes analysed in the reference cluster were responsible for 5634 compromises, 2,351 of which occurred in 2023 (excluding botnet-other), confirming a significant frequency of threats over the last year.

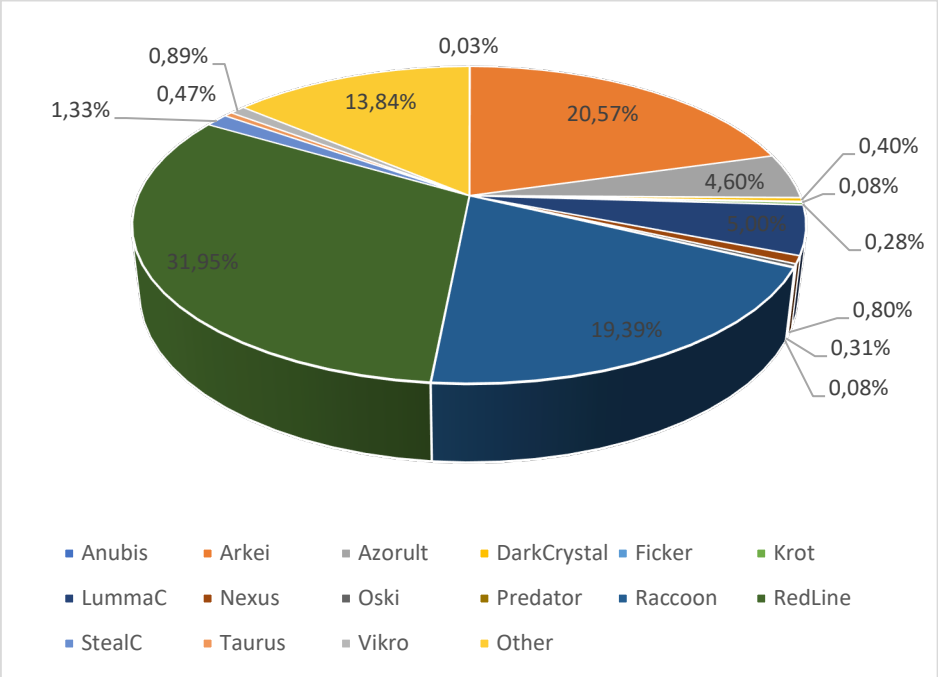

Figure 12: Top 15 identified InfoStealers - less significant cluster

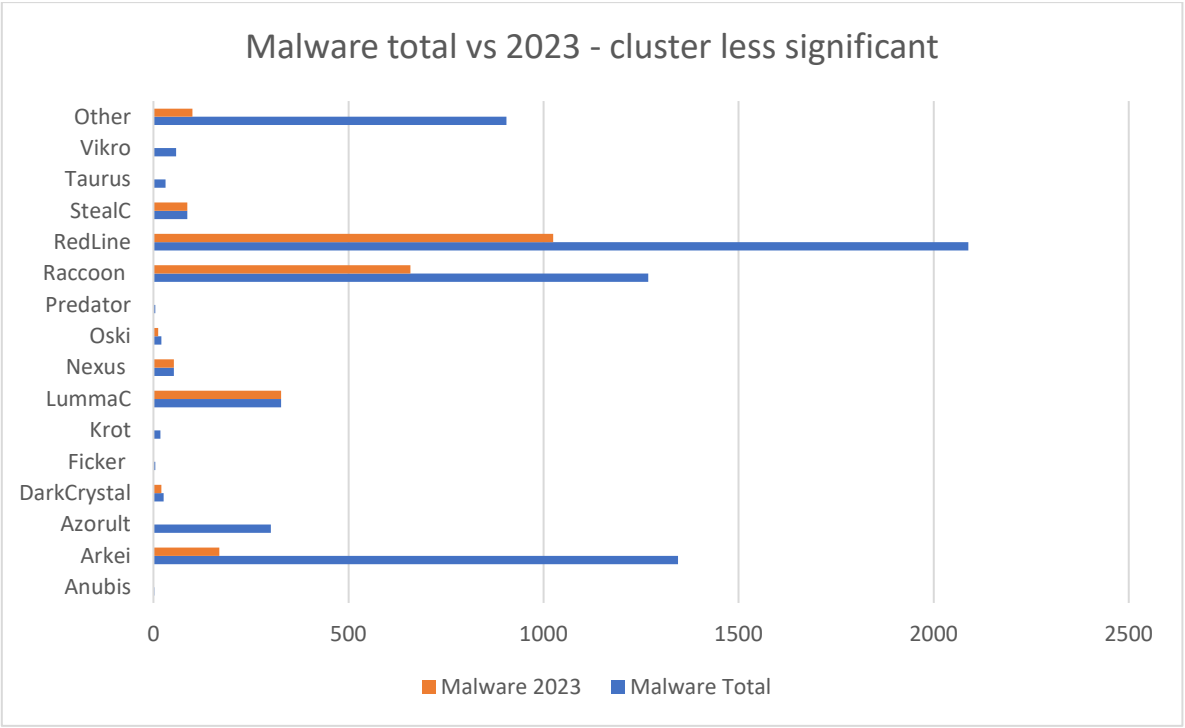

Figure 13: InfoStealer total vs 2023 - cluster less-significant

EXTRA Infostealer presence in the underground ecosystem

Underground forums have become a thriving hub for the distribution of malware, especially Infostealers. These forums are often frequented by cybercriminals seeking to buy or sell malware and/or Initial Access Brokers. In fact, a veritable criminal ecosystem has developed in recent years, based on the sharing of knowledge, skills and information.

There are several factors contributing to the growing popularity of InfoStealers. One of them is the ease of finding these ready-to-use products. Another important factor is the sophistication of the malware. It can in fact totally evade the most common AntiVirus systems installable on personal devices, which effectively increases the number of infected devices globally. There are also many experienced programmers who offer their skills in developing custom InfoStealers to meet threat actors' needs. At the same time, there are people who can assist with everything related to the installation, maintenance and provision of virtual infrastructures on so-called "Bulletproof" Hosting Providers.

Research on the various underground forums suggest that InfoStealers are typically sold as subscriptions and constitute an actual business model called "Malware-as-a-Service" (MaaS). For example, LummaStealer, one of the most widely used InfoStealers in 2023, has different types of subscriptions depending on user needs:

- Experienced: $250 per month;
- Professional: $500 per month;
- Corporate: $1000 per month.

The threat actor behind the Lumma project points out that the malware is "fully undetectable" and that it runs on both ARM and Intel architectures, thus also putting new MacOS running Windows on virtual environments at risk.

The threads related to the sale of these malware are constantly renewed, as product updates are posted regularly with new features announced (see Figure 20) (e.g., Windows Defender evasion feature, exfiltration of Google account cookies). This grade of professionalism and level of service can be seen as comparable to that of a legitimate vendor of commercial or legal products.

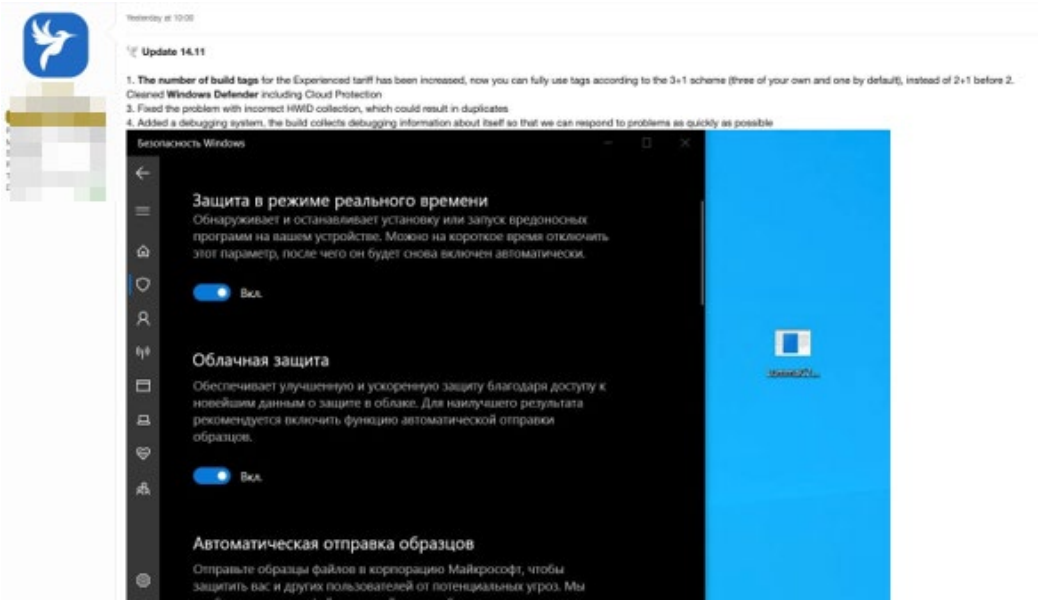

Figure 14: Example of LummaStealer's Windows Defender evasion feature

LummaStealer is not the only InfoStealer of note in 2023, however; there are numerous malware families circulating in the various forums frequented by cybercriminals, such as StealC, Meduza Stealer, DanaBot, Silver RAT, Continental Stealer, Se7en, Scarlet Project, and Rhadamanthys.

This kind of malware is also distributed in free and/or cracked versions. There are, of course, many risks in such cases. The cracked malware may contain additional malware or backdoors, which would infect the devices of the threat actors using it; moreover, the availability of these free programmes puts a dangerous tool in the hands of possibly quite experienced users, thus increasing the scale of malware distribution.

Just like legitimate companies, these cybercriminal groups publish posts for new recruits and indicate the skills required; the reverse also happens. In fact, there are many developers who are prepared to offer their skills and services to threat actors who want custom malware.

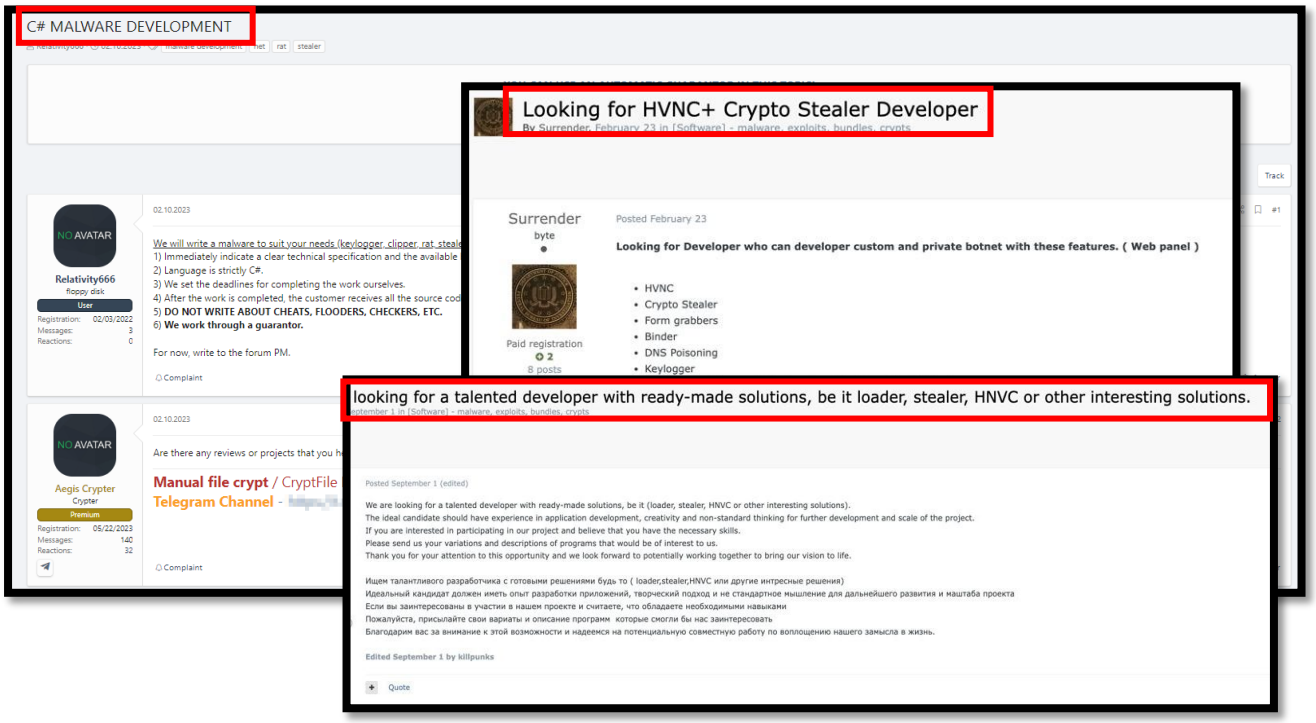

Figure 15: Examples of posts published on a well-known underground forum where developers advertise their skills for malware development

Next steps

Analysis of the cyber crime landscape reveals a significant transformation, in which it is increasingly becoming a "commodity." This phenomenon can be attributed to its increasing democratization, made possible through facilitated access to new vertical codes and skills. In particular, the dramatic increase in "InfoStealers as a service" is an obvious manifestation of this trend. This democratization is also reflected in its accessibility, with a variety of actors, including less experienced ones, able to exploit these cyber criminal resources.

In this context, a possible surge in the use of InfoStealers alongside phishing campaigns can be expected. The combination of techniques such as social engineering and simplified access to sophisticated tools will foster an increase in the effectiveness of targeted attacks, threatening the security of sensitive information.

In summary, the analysis envisions a future in which Information Stealer type malware will continue to proliferate, with a focus on 2024.

The outlook is definitely worrisome, especially when we look at what has passed with the ransomware phenomenon.

Indeed, as could be observed, it is not only InfoStealers as a service that are distributed, the preserve of Criminal Hackers with significantly lower skills, but also the infrastructural code itself of the malware itself.

Making the code available, as mentioned, was one of the triggers for the ransomware epidemic in the 2020/2023 triennium.

A hydra effect, allowing the most experienced and skilled threat actors to modify at will infrastructures that are already in place and for sale, creating custom variants that are more effective and especially difficult to track.

There will be an increase in products for sale, most likely, and consequently an increase in attacks via this type of malware.

This will be accompanied by increased expertise in the Deep and Dark Web, further fueling the spread of malware. The transition from combolist publishing to the spread of InfoStealer logs indicates a shift in attacker strategies, requiring organizations to strengthen their defenses. The growing InfoStealer infections highlighted in the analysis underscore the urgency of advanced security measures.

Consequently, only through a holistic approach to cybersecurity will it be possible to mitigate the potentially devastating impacts of emerging cyber threats.

Credits

Analysis by:

Martina Fonzo

Riccardo Michetti

Technical Contributors:

Soc Team Swascan

Editing & Graphics:

Federico Giberti

Melissa Keysomi

Contact Info

Milano

+39 0278620700

www.swascan.com

info@swascan.com

Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI