

KELA



Inside the Infostealer Epidemic: Exposing the Risks to Corporate Security

April 2025

Table of contents

Executive Summary	3
The Cybercrime Ecosystem and Its Reliance on Corporate Credentials	4
<ul style="list-style-type: none">MotivationsBusiness ModelsCorporate credentials as commodityInfostealers as a tool to gain corporate credentials	
Evolution of compromised credentials sale	7
<ul style="list-style-type: none">Cybercrime forums and private salesAdoption of automated marketsAdoption of Subscription Model ('clouds of logs')Adoption of ULP Lists (url : login : pass)	
Insights on Infected employees	13
<ul style="list-style-type: none">Methodology and ScopeEmployees infected with infostealers<ul style="list-style-type: none">Top department affected - Project ManagementTop affected countries - BrazilTop Affected Sectors - TechnologyMachine (PC) Types and Usage BehaviorEmployment Status During Infection<ul style="list-style-type: none">Schneider Electric incident - Case StudySnowflake Incident - Case StudyTakeaways	
Ransomware groups and their use of valid accounts	27
<ul style="list-style-type: none">Methodology and ScopePlayAkiraRhysidaTakeaways	
Conclusion and Recommendations	34

Executive Summary

Infostealer malware and the resulting theft of corporate credentials are central to today's cybercrime landscape, driving both widespread credential trading and enabling devastating ransomware attacks. This report summarizes KELA's research on both of these critical areas, and key findings include:

- **Stolen credentials, particularly corporate ones, are high-value commodities facilitating various cyberattacks.** Infostealers, which automate credential theft, have become increasingly popular and are often sold as Malware-as-a-Service (MaaS). For context, KELA observed over 4.3 million machines infected globally by infostealer malware, accounting for more than 330 million compromised credentials over all in 2024. Additionally, almost 40% of infected machines in KELA's data lake included credentials for sensitive corporate systems, such as content management systems, email, Active Directory, Federation Services, and remote desktop.
- **Monetization methods for stolen credentials have evolved from traditional forums to automated markets and subscription-based models.** Automated markets allow for efficient querying and purchasing of credentials, while subscription models offer continuous access to stolen data. ULP (url:login:pass) lists provide a streamlined format for quick use in attacks.
- **Victim profiling, based on 300 victims of infostealers (employed by different organizations) showcased commonalities.** The analysis revealed that Project Management (28% of all), Consulting (12.7% of all), and Software Development (10.7% of all) roles were the most impacted victims. Brazil had the highest percentage of victims (9% of all). Personal computers (accounted for 64.7% of all) were more frequently infected than work computers, and most compromised accounts belonged to current employees.
- **Research into ransomware groups like Play, Akira, and Rhysida illustrated a concerning connection to infostealer compromises.** KELA identified compromised accounts associated with some of these ransomware groups' victims that had been shared up to 95 days prior to the attack being claimed, in one case just 5 days after infection. While it cannot be definitively stated that these attacks occurred as a direct result of these identified accounts, these groups are known to use valid accounts, among other methods, to gain initial access.

Infostealer-compromised accounts, available on sale in cybercrime underground, represent a significant avenue for ransomware actors to obtain these valid credentials. To mitigate the threat, KELA recommends active defense monitoring, proactive access management, robust antivirus solutions, and employee training.

The Cybercrime Ecosystem and Its Reliance on Corporate Credentials

The cybercrime ecosystem operates as a complex, interconnected network, mirroring many aspects of legitimate markets. Driven by financial, ideological, and strategic motivations, various threat actors specialize in different aspects of cybercrime, creating a marketplace for malicious goods and services. At the heart of this ecosystem lies the trade in corporate credentials, which have become a high-value commodity. These credentials grant cybercriminals access to sensitive organizational assets, facilitating a range of illicit activities and generating substantial profits. This section delves into the intricacies of the cybercrime ecosystem, exploring its motivations, business models, and the crucial role that corporate credentials play within it.

Motivations

The cybercrime ecosystem operates much like a legitimate market, driven by demand and supply, with threat actors of varying specialties providing goods and services. Threat actors typically fall into three main categories based on their motivations: ideological, financial, and strategic.

- **Ideological Motivation:** Such threat actors often engage in hacktivism, targeting individuals or organizations based on political or social beliefs.
- **Financial Motivation:** Focused on profit, these actors target entities with high-value assets—such as large companies or wealthy individuals—, or perform opportunistic attacks and seek to maximize their financial gain.
- **Strategic Motivation:** These threat actors, often associated with nation-states, target other nations or rival entities to gain sensitive information or intellectual property, commonly using proxy actors.

Financial motivation remains the most prevalent driver in the cybercrime landscape, where profit-focused threat actors dominate. Financially driven attacks tend to be less discerning about the specific target and instead aim to maximize returns by accessing high-revenue victims or targeting entities with monetizable data.

Business Models

Like in the legitimate economy, demand within the cybercrime ecosystem varies — threat actors seek different types of information and tools they can purchase to escalate and monetize their activities. For instance, the more sensitive a stolen database is (such as medical records of a private hospital) or the more confidential (such as strategic maps including plans stolen from a national intelligence agency), the more likely it is to command a higher price on cybercrime platforms. This is due to the greater willingness of interested buyers to pay for its potential monetization value and uniqueness. Another example is an initial access broker that may sell various remote access types (e.g., RDP, VPN, RMM) to ransomware operators at prices that reflect market demand (for example, access with domain admin privileges is valued higher), competing with other brokers in the process.

This financial ecosystem creates specializations, meaning that different types of actors conduct specific crime types: whether it's specializing in providing initial access, developing malware or creating social engineering tools (to name a few). For the last few years, a lot of actors have built their business model on selling corporate credentials to other actors, enabling access to high-value targets for less time and effort.

Corporate credentials as commodity

Corporate credentials are a high-value product in the cybercrime ecosystem, as they enable cybercriminals to gain access to sensitive assets of organizations and potentially receive higher profits than from targeting individuals. Credentials vary in access levels, from C-level resources to marketing CRMs etc. The major difference lies in access to different types of information, data and privileges.

Buyers can use these credentials for sophisticated attacks: a mailbox of a CEO for example, can be exploited to conduct a phishing campaign targeting the company. In other case, credentials of software used to manage all the human resources within a company, could allow a threat actor to access multiple individuals' personal information, which can be then sold on cybercrime forums for threat actors interested in buying databases. Another instance may be VPN credentials, stolen from an IT employee and then used to spread through the company's network and deploy ransomware or steal data.

These credentials can be stolen using various techniques, with sophistication levels varying: for instance, through brute forcing or password spraying attacks, as well as phishing methods. Infostealer malware, in particular, is becoming increasingly popular as threat actors use it to steal credentials on a large scale for monetization purposes. A single infostealer-infected machine can yield hundreds or even thousands of credentials, which can be sold by initial access brokers or any other threat actors, as they are treated as a commodity.

Infostealers as a tool to gain corporate credentials

Infostealer operations are a rapidly evolving segment of the cybercrime landscape, with attackers continuously refining their methods to capture and monetize sensitive information. Infostealing malware is designed to infiltrate systems and steal sensitive data, such as login credentials, financial details, personal details, system and network information. Once installed on a victim's system, they extract information from web browsers, password managers, and even clipboard data, with the type and scale of the data varying from one infostealer component to others.

Once acquiring the infostealer builds as MaaS, a threat actor willing to specialize on credentials selling needs to successfully set up an infrastructure and collecting compromised accounts on a wide scale, often using a team of traffers (related to the word traffic, referring to actors who have the means to infect multiple targets) to spread the infection. The following stage is monetization, highly utilizing the dedicated cybercrime platforms that have evolved over the last years.

Evolution of compromised credentials sale

After setting up infrastructure and collecting a stream of compromised credentials, threat actors are willing to monetize them. This chapter further explores the rise of subscription-based models and the emergence of ULP lists, revealing the increasing sophistication and commercialization of credential theft in today's cyber threat environment. This structure allows less-skilled threat actors to enter the trade; once they establish an effective infrastructure, infostealers can deliver a steady flow of infected devices, allowing actors to release credentials for sale to the market quickly.

```
=====
URL: https://[REDACTED].org/conta/
Username: [REDACTED]_CS
Password: [REDACTED]5

=====
URL: http://webmail.[REDACTED].net/zimbra/
Username: [REDACTED]@dombosco.net
Password: [REDACTED]901

=====
URL: https://[REDACTED].coop.br/
Username: [REDACTED]
Password: [REDACTED]55#

=====
```

Example of a "Passwords.txt" file included in a full bot, including URL, username and the passwords

Cybercrime forums and private sales

One of the common or traditional ways to monetize those compromised credentials would be to offer them on cybercrime forums to threat actors who may be interested in further exploitation for their own financial gain.

Below as can be seen is a screenshot reflecting that strategy — a threat actor listing for sale a bundle of 2.3 billion compromised credentials (in a form of `url:login:password`) collected from 2021 to 2024, at a price of USD259.

Selling 2.3kkk (billions) url:log:pass (high quality)

by erbesteratu - Monday August 26, 2024 at 06:23 PM

08-26-2024, 06:23 PM

erbesteratu



Breached

MEMBER

- My database is collected from logs for the period 2021-24 years
- There are more than 2,300,000,000 UNIQUE rows in the database
- 1. WITHOUT doubles
- 2. WITHOUT trash (without passwords \ localhost \ UNKNOWN etc.)
- 3. ONLY HIGH quality
- The database has already been uploaded to telegram group
- Price 259 usd
- Accept ANY Crypto (btc, eth, ltc, usdt etc.)
- Telegram - t.me/erbesteratu

Threat actor listing 2.3 million ULPs pack in price of USD259

While some actors prioritize volume, selling credentials in bulk with minimal filtering, as seen above, others take a more strategic approach, segmenting stolen data to cater to different buyers based on the value of specific accesses. This is possible due to the business model scalability—threat actors can infect an unlimited number of machines to meet demand in the stolen credentials market and succeed in capturing sensitive VPN credentials if they infect a large number of machines. Below is an example of an incident indicating demand for compromised credentials of organizations.

Transparent partnership, we will buy your access

📅 Publish date: Dec 13, 2024 👤 Author: BlackAPT in 🔗 Source: ExploitIn 📄 ID: 336173840

We are a professional team that is looking for access providers. Our team has achieved high success in monetization. Transparent cooperation, we offer direct access to chats for partners.

Access type: RDP, RDWeb, Citrix, VPN + RDP (Access via interface)

CA - 10kk+

UK - 10kk+

AU - 10kk+

TOP EU - 30kk+ (NL,IRE,GER)

Rest of the world - 50kk+

Minimum privilege: Domain Administrator

If possible, the company should be listed on a stock exchange.

Partnership for % or we will buy access if the network meets our requirements.

We do not accept critical infrastructure, hospitals, government or non-profit organizations. Commercial!

Countries not interested in China, CIS, USA and North Korea.

English speaking sellers welcome.

Example of operator of a group posting about their interest in initial access type for monetization

This post serves as a clear example of monetization strategies within the cybercrime ecosystem, specifically showcasing the collaboration between Initial Access Brokers (IABs) and other threat actors. The group, BlackAPT, explicitly seeks access providers offering high-value network entry points such as RDP, RDWeb, Citrix with administrative privileges in large, commercial organizations. By purchasing or profit-sharing with IABs, they establish footholds for advanced attacks, optimizing their operations for maximum financial gain. This post highlights the structured and professional nature of the cybercrime market, where specialized roles like IABs support large-scale monetization efforts while adhering to targeted criteria for profitability.

However, this relatively straightforward method of monetizing stolen credentials by listing them on the forums does not effectively support threat actors aiming for large-scale profits or running business models in highly competitive markets. Similar to legitimate business developments, the cybercrime ecosystem has adopted various monetization models in recent years, including the automated markets and subscription models.

Adoption of automated markets

Automated markets for selling compromised credentials, such as the 'Russian Market,' have emerged as a solution to the scalability issues faced by actors on cybercrime forums. These markets leverage automated functionality, allowing buyers to instantly query vast databases of stolen data and purchase specific credentials in a seamless, on-demand process. Users can filter searches by parameters such as email domains, services, geographic location or infostealer malware type, with the platform automating the retrieval and transaction steps. This efficiency eliminates the manual negotiation, catering to buyers seeking quick access to precise data. For instance, a buyer can search for credentials associated with "examplebank.com" and instantly acquire matching results for a fixed fee, such as \$5 per entry.

The screenshot displays the 'RUSSIAN MARKET' interface. On the left is a sidebar with navigation links: User, News, CVV, LOGS (with a 'pre-order' button), My orders, PROs, Checkers, Tools, My Purchases, and Support. The main area features search filters for Stealer, System, Country, State, City, Zip, ISP, Outlook, and Per page. A 'Links' section on the right includes search buttons for Links, Mask, Cookies, and Email, along with a 'ONLY WITH COOKIES' checkbox and a price slider. Below the filters is a table of search results.

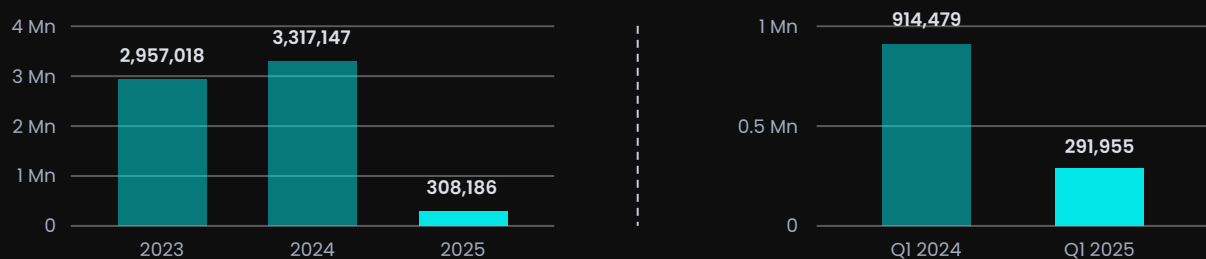
Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
lumma	Russia	valberry.com f5gint.net accounts.google.com digitalakara.school.venture.com accounts.google.com voltaga.com mvp.in flakart.com amartomatax.com mva.gov.in Show more...	-	-	archive.zip	2024.08.26 0.88Mb	MoFFFFyf [Diamond]	\$ 10.00	Buy
lumma	Russia	enlncbpc.bihar.gov.in examinationsservices.nic.in janganchay.menphchaon.gov.in eaps.amurline.ac.in examinationsservices.nic.in scholarships.gov.in tsabstst2024.com pmsonline.bih.nic.in nivergataonline.in udyamuster.bihar.gov.in Show more...	-	-	archive.zip	2024.08.26 4.22Mb	MoFFFFyf [Diamond]	\$ 10.00	Buy
lumma	Russia	client.msblox.com learning.tps.onhub.in online.cambridgeconnect.org sevthassa.oly.com studentlogin.amjaincollege.edu.in app.studobinder.com studentlogin.amjaincollege.edu.in studentlogin.amjaincollege.edu.in studentlogin.amjaincollege.edu.in studentlogin.amjaincollege.edu.in Show more...	-	-	archive.zip	2024.08.26 0.93Mb	MoFFFFyf [Diamond]	\$ 10.00	Buy

The interface of Russian Market showcasing advanced filtering options and streamlined purchase functionalities for compromised credentials

It is worth noting that log-oriented markets are dynamic and competitive. For instance, Genesis Market launched around 2018 and remained very popular until it was seized by law enforcement in April 2023. The launch of Exodus Market in January 2024, which introduced a paid subscription model, may be linked to the sale of Genesis's infrastructure on dark web forums after its shutdown—further highlighting the market's evolving nature. As for the scale, KELA collected above 360 million compromised accounts from the Russian Market since 2019. KELA's data reveals a significant increase in log listings on the Russian Market over the years, with compromised accounts counts rising to over 138 million in 2024. The most dramatic surge occurred between 2021 and 2023, peaking at 129 million in 2023. However, early 2025 data suggests a potential decline, with approximately 14 million accounts from 290,000 bots (a decline of over 50% compared to same time period in 2024), indicating a possible slowdown in the market's average monthly activity.



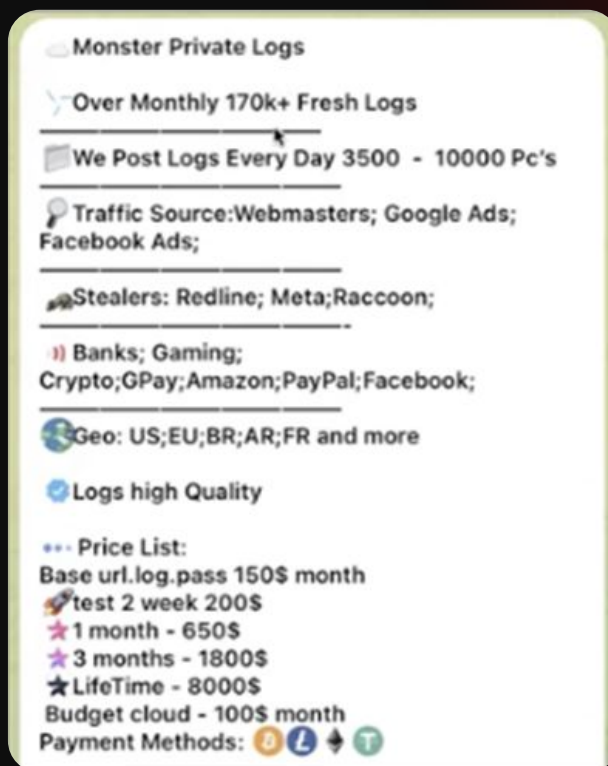
Compromised accounts



Bots

Adoption of Subscription Model ('clouds of logs')

The subscription model offers greater efficiency and sustainability compared to traditional one-off sales (as shown above). Threat actors have been increasingly monetizing credentials through subscriptions to their compromised credential service, allowing their clients to have continuous access to stolen data, without need to process each sale. The subscription model addresses the scalability issue mentioned earlier — for instance, if a threat actor operates infrastructure that continuously receives thousands of compromised credentials per day, manually selling them in batches would be inefficient. The subscription model enables threat actors to increase their number of recurring clients and manage larger volumes of data with ease.



Example of a subscription service on TG, where a threat actor is offering 170k logs for sale, meaning information stolen from 170k machines, for \$650 a month

This streamlined approach, mostly managed on Telegram channels, makes the subscription model especially appealing to threat actors focused on infostealer-stolen credentials monetization, as it supports their need for a reliable, easily manageable infrastructure. Such platforms provide essential infrastructure for these operations, including file hosting and APIs for easy management, which simplify the process and reduce costs for threat actors.

Adoption of ULP Lists (url : login : pass)

In parallel to the adoption of subscription models, ULP (url : login : pass) lists are also valuable for some cybercriminals. These lists represent a simplified and structured format of stolen credentials, where each entry contains the service URL, associated login username or email, and the password and do not include additional data on the infected machine itself.

ULP lists are believed to originate primarily from infostealers, which harvest credentials directly from infected machines. These credentials are then formatted into ULP structures for easier dissemination and monetization. These lists are typically shared on cybercrime forums and Telegram channels, rather than being sold in large, aggregated "clouds of logs." Unlike bulk data in the form of log files or archives often seen in earlier models, ULP lists are concise, easy to parse, and tailored for quick use by threat actors. Their separate distribution and streamlined structure make them particularly attractive for low-effort credential stuffing attacks, phishing campaigns, and targeted account takeovers.



Example of a subscription service, where “PLUTONIUM Team” offers a monthly-subscription menu to their ULP services

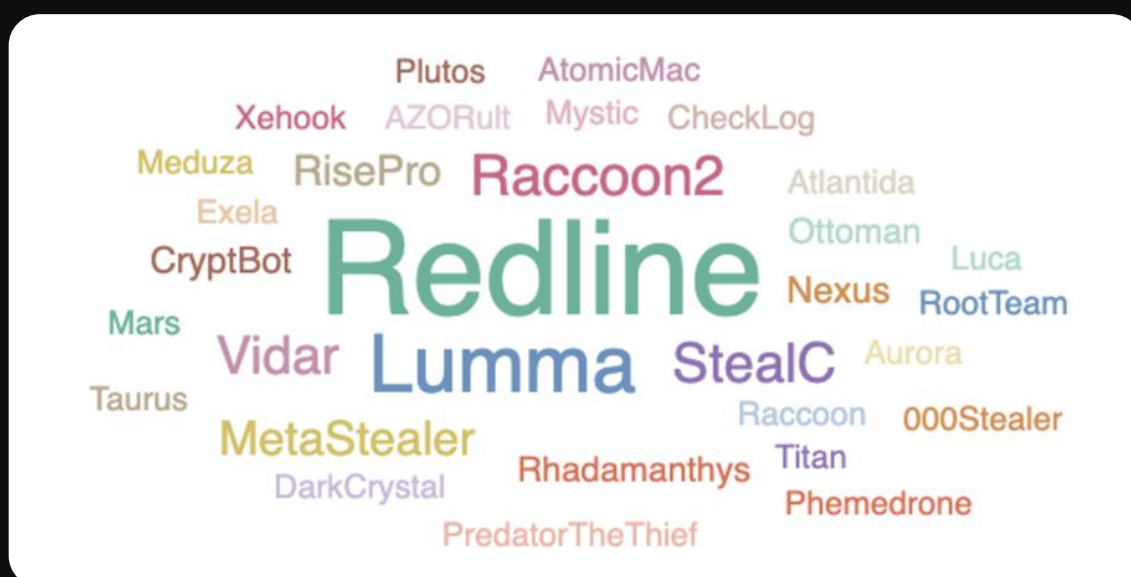
This shift demonstrates the continued evolution of the cybercrime economy, focusing on maximizing usability and efficiency for both sellers and buyers, while also catering to less sophisticated threat actors who seek immediate access to actionable data. As threat actors refine their tactics, the infostealers market will likely remain a significant vector in cybercrime, driving both individual and organized illicit activity across the globe. For context, KELA observed over 4.3 million machines infected globally by infostealer malware, accounting for more than 330 million compromised credentials over all in 2024. Additionally, almost 40% of infected machines in KELA’s data lake included credentials for sensitive corporate systems, such as content management systems, email, Active Directory, Federation Services, and remote desktop.

Due to the rapidly evolving and spreading of the infostealers attacks, KELA conducted a deep dive into infostealer-infected machines of corporate employees, analyzing the profile of those victims in order to define the threat, and suggest recommendations to combat it.

Infected employees insights

In response to the rise of infostealers and the rapid growth of compromised credentials being sold on cybercrime platforms, KELA conducted in-depth research using its in-house collection of infected machines including compromised credentials. This study aims to highlight the profiles of individuals most at risk, as well as provide actionable insights and strategic recommendations to address the threat of infostealers and the increasing volume of compromised credentials.

Below is a map presenting the prominent infostealer malware families identified by KELA, such as Redline, Lumma, Raccoon2 (now defunct),¹ StealC, MetaStealer, and Vidar, among others. They operate as Malware-as-a-Service (MaaS) — meaning that different cybercriminals gain access to the malware for a fee. In this research sample, StealC accounts for the largest share at 40.07%, followed by Lumma at 26.82% and Redline at 12.58%. Other notable malware families include Vidar (6.62%), MetaStealer (5.63%), and an aggregated Other category, which makes up 8.28% of the sample.



Prominent infostealer malware types identified by KELA

¹ [Source](#)

Methodology and Scope

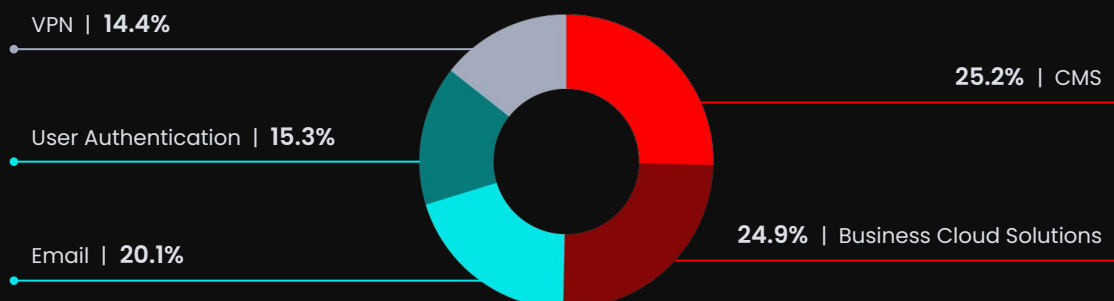
The main goal of this research was to identify a profile of a typical employee infected by infostealers, including job department and job title, as well as other relevant details. The main challenge was to identify machines of employees, since commodity infostealers' attacks are usually opportunistic and do not target specific individuals, therefore taking a random set of machines would prove inefficient.

To address this, KELA compiled a dataset of machines compromised through information stealing malware and containing credentials to corporate VPN services, as they are more likely to capture employee-related compromises. The dataset consists of 300 machines collected by KELA, containing more than 100,000 compromised credentials, infected with various types of infostealer malware, with infection dates ranging from July 19, 2024, to August 19, 2024. For each machine, KELA identified an affected individual who was using this computer, based on information contained in the stolen bot. KELA's analysis showed that key attributes documented in the dataset in addition to infected machines' metadata included:

- The victim's role within an organization (job title)
- Employment status at the time of compromise
- An affected company's sector and jurisdiction
- Indicators of shared or non-shared PC usage (if there were credentials related to few individuals in one bot)
- Indicators of work or personal PC (whether the machine is likely personally owned or provided by the company)

By focusing on these parameters, KELA gained a clear view of the departments, job titles, and industries that are most susceptible to infostealer compromises. This analysis allowed KELA to explore how certain job positions may inherently carry higher risk due to factors such as access levels, regular use of certain sensitive services, or device sharing practices.

































It is worth mentioning that each infected machine/bot, in addition to corporate VPN credentials used to define the research scope, included other types of sensitive services, all of which can be of interest to threat actors. In the researched dataset, the most frequent type is CMS (all WordPress), accounting for 25.2% of all instances, followed by Business Cloud Solutions with 24.9%, Email at 20.1%, User Authentication (with Okta being the most common) with 15.3%, and VPN (with F5 being the most common) with 14.4%.



Primary service types targeted (based on 300 infected machines)

Employees infected with infostealers

This chapter outlines the findings of this research, highlighting the most common workplace departments, sectors, jurisdictions, and characteristics of computer ownership and usage observed in the study.

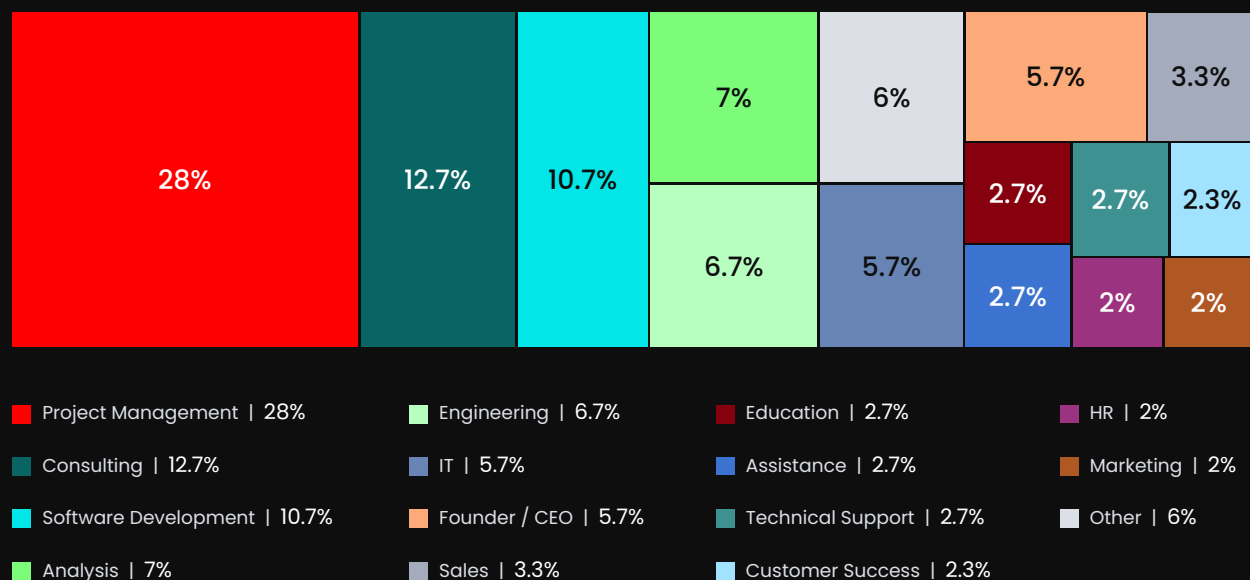
 https://vpn2[REDACTED]/global-protect/login.esp	(C) 1st Critical
 [REDACTED]	 Ransomware +1
 [REDACTED]	
 [REDACTED]  VPN  Infected Bots • Source Date: Sep 26, 2024	
 Unresolved	
 https://vpn2[REDACTED]/global-protect/login.esp	(C) Recurring Critical
 [REDACTED]	 Ransomware +1
 [REDACTED]	
 [REDACTED]  VPN  Infected Bots • Source Date: Sep 02, 2024	
 Unresolved	
 https://vpn2[REDACTED]/global-protect/login.esp	(C) 1st Critical
 [REDACTED]	 Ransomware +1
 [REDACTED]	
 [REDACTED]  VPN  Infected Bots • Source Date: Sep 02, 2024	
 Unresolved	
 https://vpn.[REDACTED]/remote/login	(C) 1st Critical
 [REDACTED]	 Ransomware +1
 [REDACTED]	
 [REDACTED]  VPN  Infected Bots • Source Date: Jul 26, 2024	
 Unresolved	

Compromised VPN accounts as seen in KELA's platform

Top department affected: Project Management

As can be seen in the graph below, the analysis revealed that the most frequently compromised department was Project Management, accounting for 28% of all departments where affected employees were working. This was followed by Consulting (12.7%) and Software Development (10.7%). Other areas include Data Analysis (7%), Engineering (6.7%), IT and Founder/CEO, each (5.7%), and sales (3.3%). Additionally, 6% of victims were included into an "Other" category, with miscellaneous positions such as Education Assistance, Technical Support, Customer Success, HR, Marketing, and others. These findings underscore the effect of Project Management roles and highlight the diversity of positions affected by infostealer campaigns.

The Project Management department included various job positions based on employees' self-descriptions, such as Technical Project Manager, SAP Operation Team Lead, Digital and Innovation and Head of IoT Services, among others. These roles often involve managing cross-functional teams, coordinating tasks, and accessing sensitive organizational systems. These employees' responsibilities, which frequently combine technical and managerial elements, make them attractive targets for infostealer campaigns due to their broad system access and reliance on digital tools for collaboration and communication. For example, one of the affected employees was working at a big software development company for 13 years, starting as a sales consultant and now being director of strategy & business development, with access to VPN, Jira credentials and other sensitive info on their infected machine.²



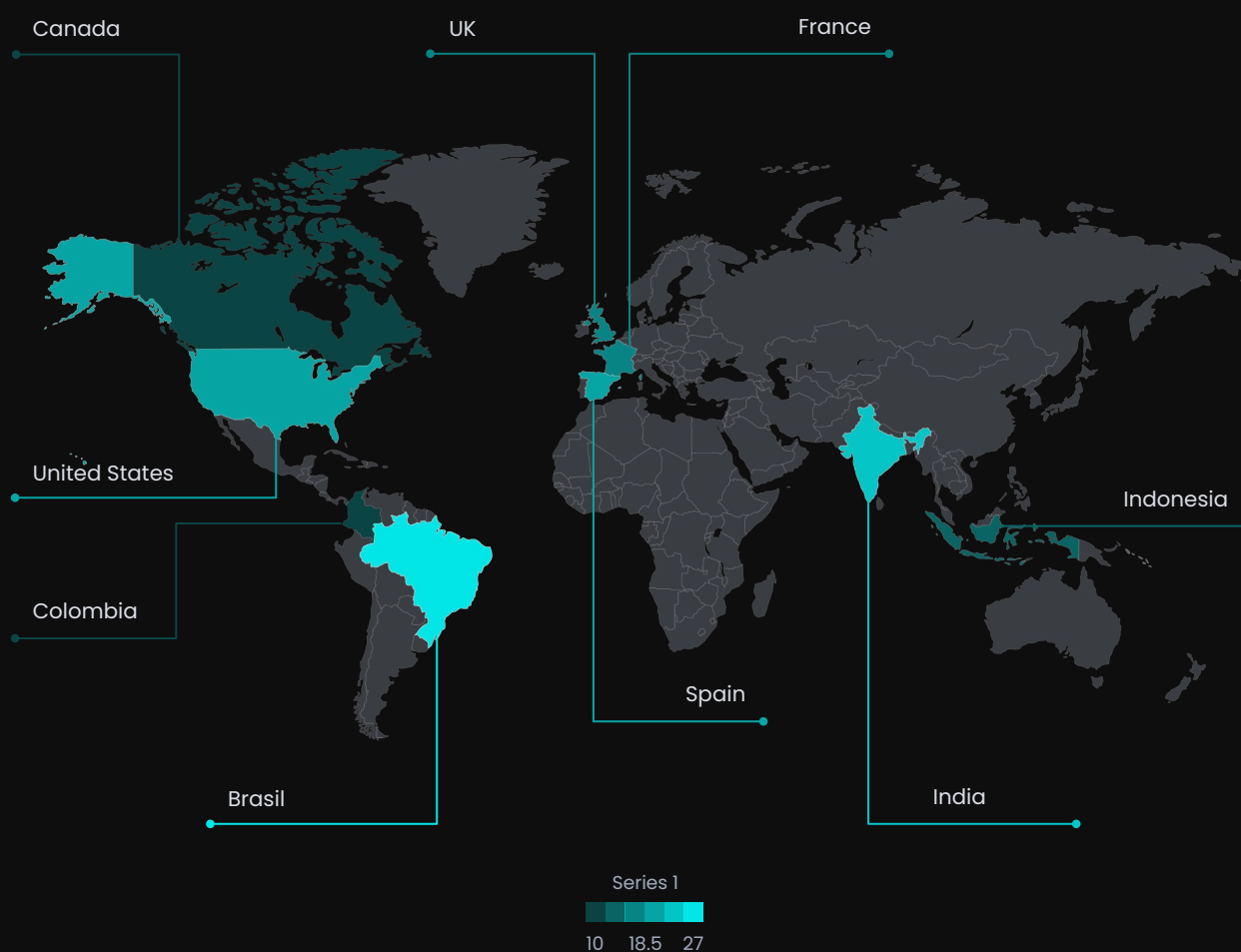
Infected employees' departments

² In these and other departments KELA has created clusters based on the most relevant grouping for our results that can be wider than traditional definition of roles.

Top affected countries: Brazil

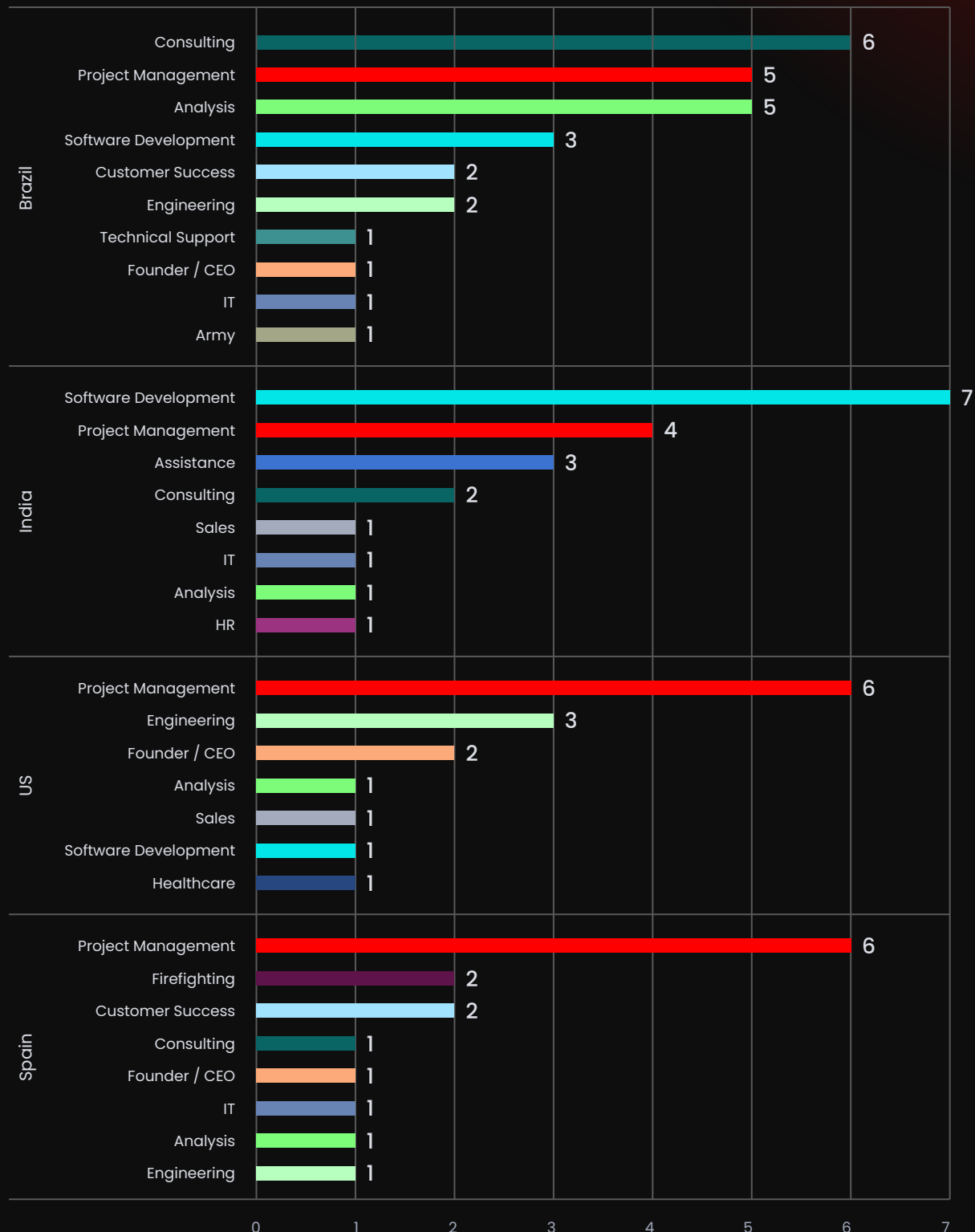
Brazil had the highest percentage of victims, with 9% affected, followed by India with 6.7%, while the United States and Spain each accounted for 5%. It is worth mentioning that, according to KELA's data lake, accounting for millions of bots collected in 2024, Brazil and India are also the most affected countries, with India accounting for 7.67%, followed by Brazil at 7.29%.

France recorded 4.3%, and the United Kingdom and Indonesia each had 4%. Additionally, Canada and Colombia both reported 3.3%. All other countries in the dataset had a lower percentage of victims, highlighting the concentration of cases in these top regions.



Frequency of Targeted Countries

As shown in the graph below, the analysis of job positions affected by infostealers across the most impacted countries reveals that in Brazil, the most common roles were in Consulting, Project Management, and Analysis, followed by Software Development. In India, Software Development was the leading area, followed by Project Management and Assistance. The United States, Spain, significant representation in Project Management, consistent with observations across all countries, remaining the most vulnerable.



The number of machines/individuals showing the top targeted countries and their corresponding departments

Top Affected Sectors: Technology

The analysis of the sectors, to which the companies of affected employees pertain, revealed that Technology was the most frequently represented, accounting for 14% of the cases, followed by IT Services and IT Consulting with 11%, and Manufacturing with 9%. Other prominent sectors included Professional Services (9%), Government Administration (7%), Telecommunications (6%), and Education (6%).



The Technology and IT Services sectors in this dataset spans a variety of technology-related fields, including software development, IT services, computer and network security, cloud services and fintech (financial technology). The affected organizations include software firms, enterprise software developers, providers of computer hardware, printing and network security services and web design companies. Although infostealer campaigns are not necessarily targeted, the concentration of victims in technology-oriented companies likely reflects the high digital footprint of employees in these industries.

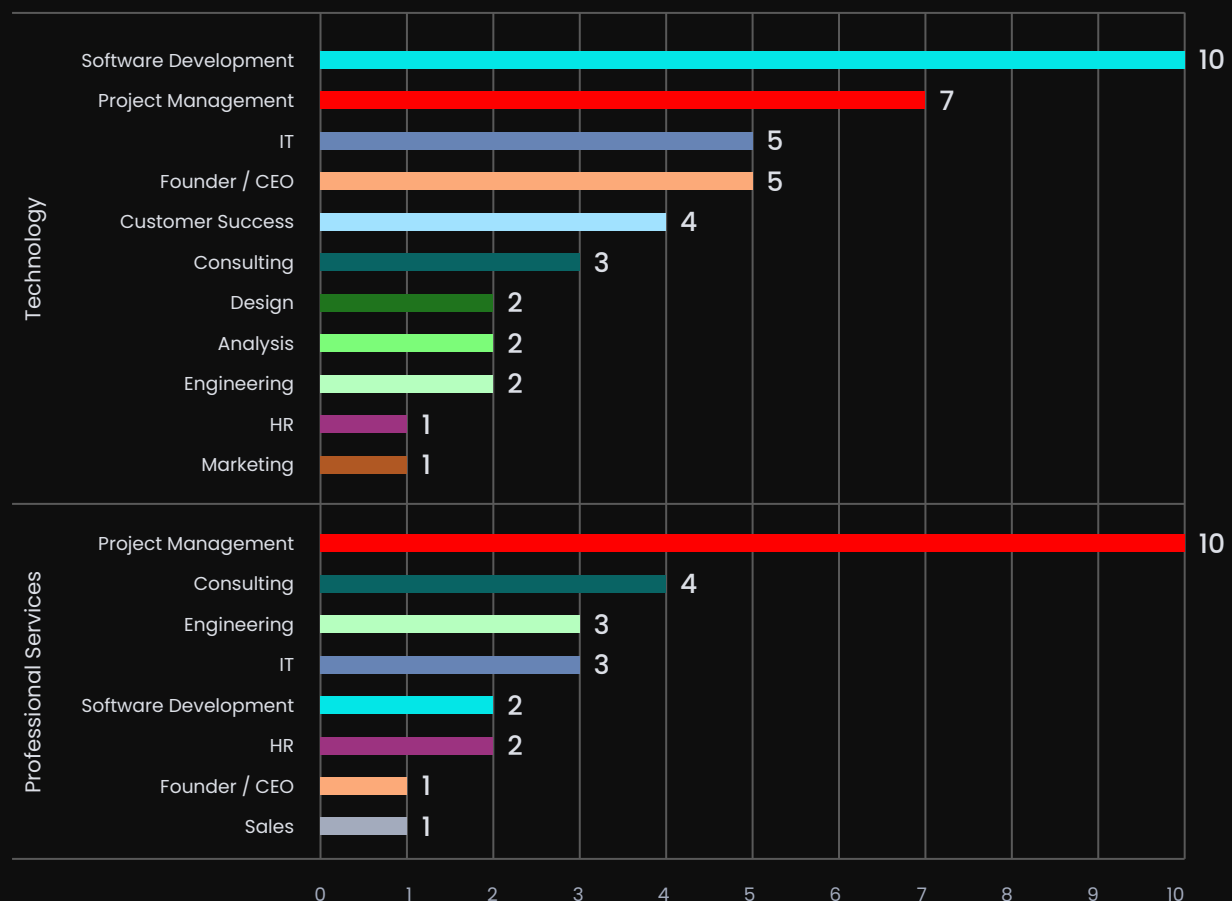
Employees in these companies often work with a wide array of digital tools, platforms, and systems, making them frequent users of the internet and software applications—prime environments for infostealer delivery mechanisms like phishing, malicious advertisements, and compromised websites. Additionally, the potential access to sensitive data, intellectual property, and critical organizational systems makes technology sector employees attractive, albeit unintended, targets for cybercriminals.

The analysis of the top five affected sectors highlights which departments in these companies were more vulnerable to infostealers, with Software Development and Project Management leading across all sectors.

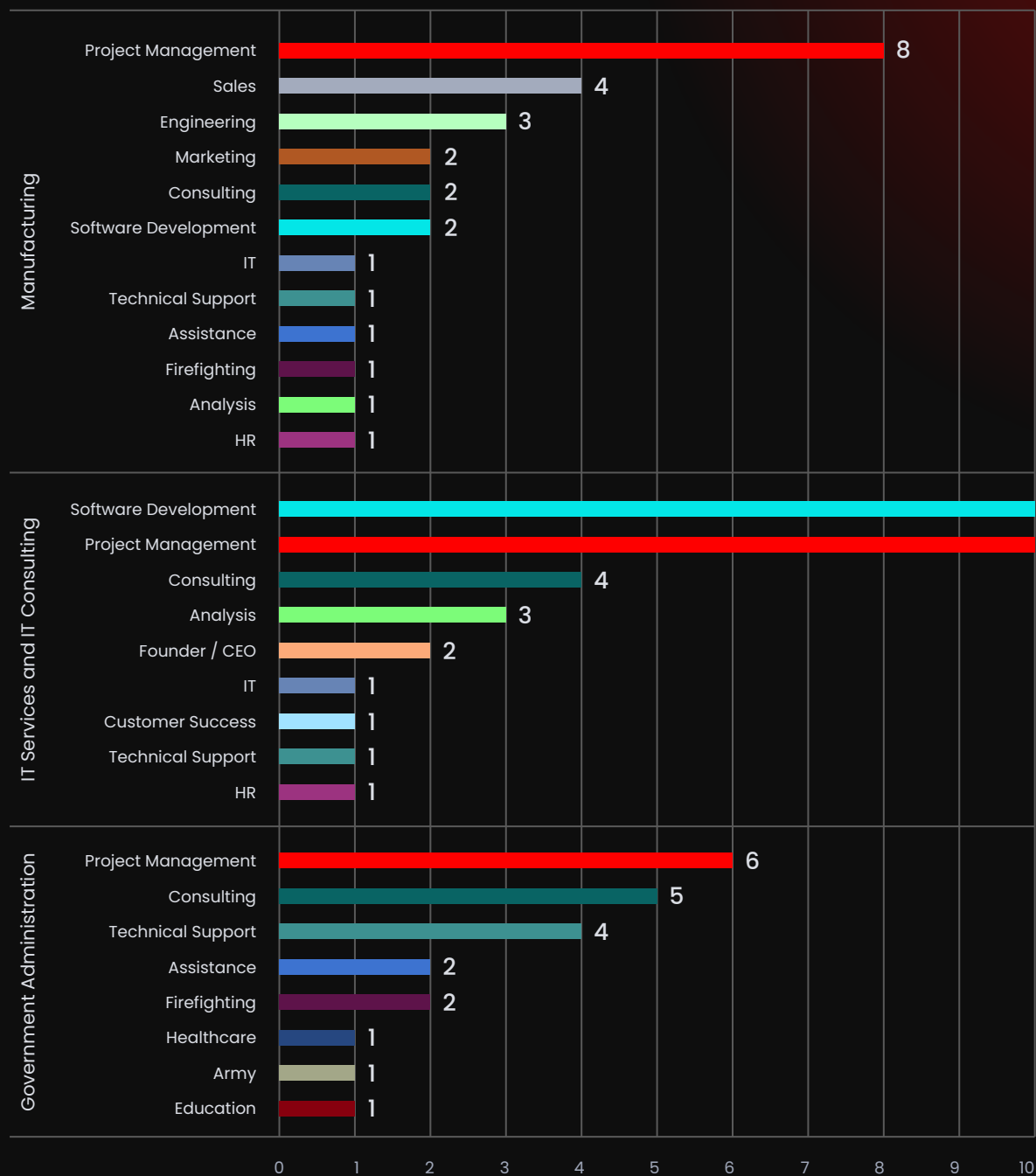
The prevalence of software development roles, especially in Technology and IT Services and IT Consulting, aligns with the nature of these industries and their positions. Employees in these sectors frequently interact with advanced digital systems, tools, and networks, increasing their likelihood of exposure to infostealer campaigns, which are often disseminated through widespread phishing attacks or malicious websites.

Project Management positions were consistently observed across the top affected sectors. As noted above, the nature of these roles involves overseeing workflows, managing employees, and working across numerous systems and tools, which creates multiple points of exposure. Moreover, management roles are diverse and not always requiring a high level of technological understanding or security awareness. This lack of technical expertise, combined with the variety of individuals in these roles, may contribute to their higher prevalence in the set, making them more susceptible to infostealer mechanisms.

Finally, Consulting roles were also among the areas frequently impacted. The work of consultants often involves conducting extensive online research, interacting with numerous platforms, and navigating diverse digital environments. This high level of online activity inadvertently increases their risk of falling victim to infostealer mechanisms, as it exposes them to a greater number of potential phishing or malware attacks.



The number of machines showing the most targeted departments in top targeted sectors



The number of machines/individuals showing the most targeted departments in top targeted sectors

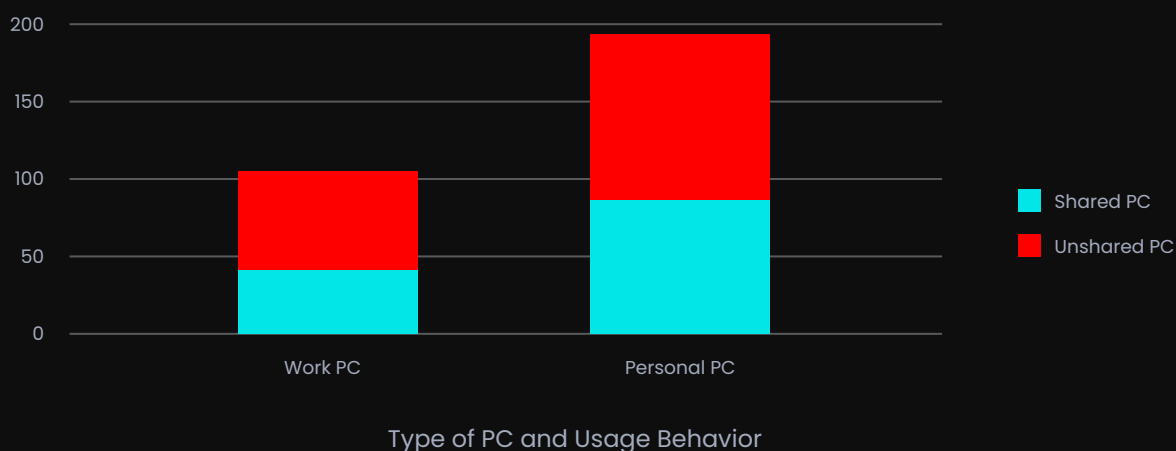
In summary, while infostealer campaigns are opportunistic in nature, the analysis shows that roles with frequent digital interaction, whether technical, managerial, or research-focused, are inherently more likely to fall victim.

Machine (PC) Types and Usage Behavior

In this part of the research, KELA documented the type of infected machines, focusing on two use cases: personal/work and shared/non-shared. In this context, it means whether the machine is likely personally owned or provided by the company, based on the amount of work-related credentials present on the machine³, and if one or few individuals appeared to use the machine based on compromised credentials. The analysis of 300 infected machines showed that 64.7% were personal computers, while 35.3% were work computers.

Among the personal computers, 44.8% were used at least by one other individual and 55.2% were unshared: the results are most likely related to the common use by a family's members or friends. For work computers, 39.6% were shared, probably when using the computer for non-work purposes or when using colleagues' credentials, and 60.4% were unshared.

These results indicate that personal, unshared computers were the most frequently infected category, representing 35.7% of all cases, followed by personal, shared computers at 29%.



The findings suggest that personal computers are generally more likely to fall victim to infostealers than work computers, which may reflect differences in security protocols and user behavior. Personal devices often lack the robust cybersecurity measures commonly implemented on work computers, such as enterprise-level firewalls, endpoint protections, and regular monitoring. Additionally, users of personal devices may be more likely to engage in risky online behavior or download unverified content, which increases the likelihood of exposure to infostealers.

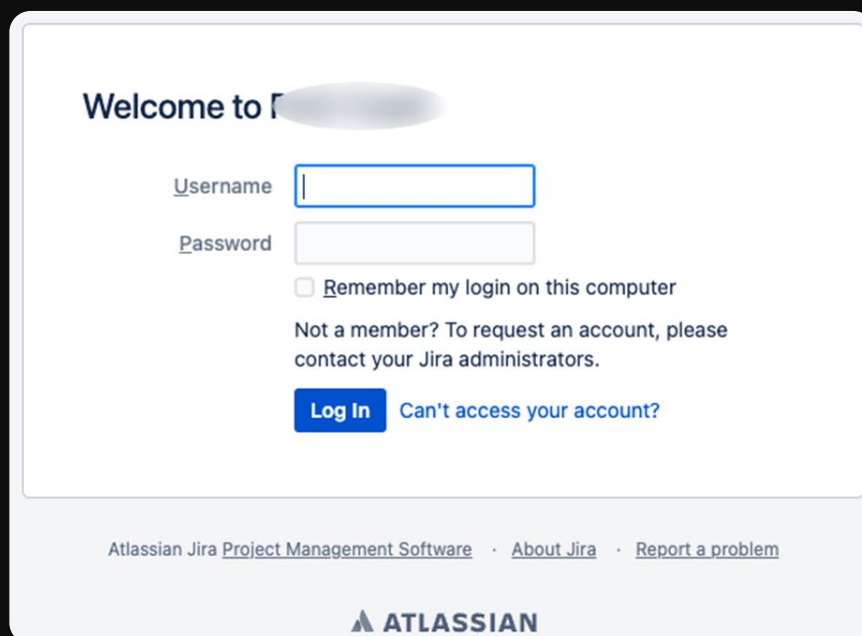
However, these personal computers appeared in the dataset because they stored work credentials, posing a critical security risk. This indicates that employees working on personal devices are inadvertently putting their organizations at greater risk. This practice increases the organization's attack surface, making these devices an attractive target for infostealers and heightening the risk of credential theft, unauthorized access, and data breaches.

³ Since many people use the same machine both for work and personal purposes, this classification is not absolute but rather a way to categorize machines based on their observed usage.

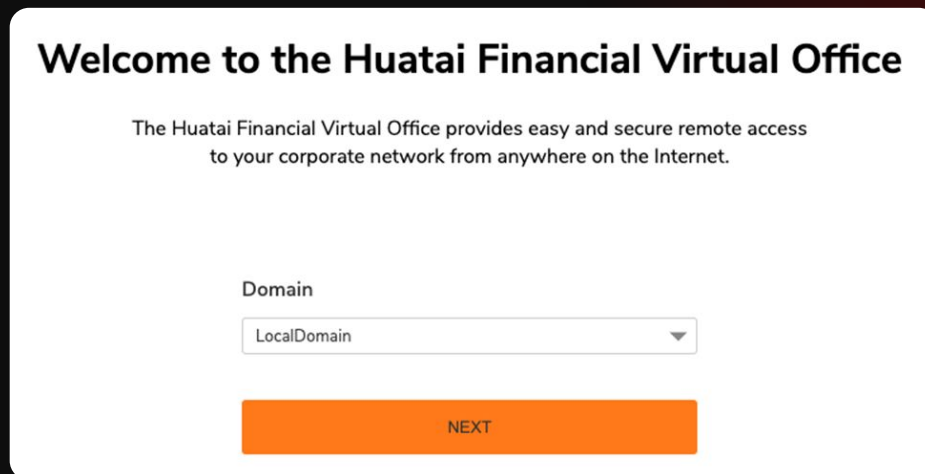
Employment Status During Infection

KELA also reviewed the sample dataset to determine whether compromised accounts were associated with current or past employees of affected companies at the time of infection. KELA found that the majority of infected machines included credentials for current employment.

One such instance involved a victim whose machine was infected with an infostealer in July 2024, compromising their work-related credentials while they were still employed at the company. The organization, a global accounting firm with billions in revenue, employs the victim as a senior associate. Among the compromised credentials, KELA identified their full access credentials for sensitive work environments, including a Jira account, multiple remote computers, and remote access credentials for a financial management service.

A screenshot of the Atlassian Jira login interface. The page has a white background with a light gray border. At the top, it says "Welcome to" followed by a blurred area. Below this are two input fields: "Username" and "Password". The "Username" field has a blue border and a cursor. Below the "Password" field is a checkbox labeled "Remember my login on this computer". Underneath the checkbox is the text "Not a member? To request an account, please contact your Jira administrators." At the bottom of the login area are two buttons: a blue "Log In" button and a blue link "Can't access your account?". At the very bottom of the page, there is a footer with the text "Atlassian Jira Project Management Software" followed by links "About Jira" and "Report a problem". The Atlassian logo is centered at the bottom.

Screenshot of the employee's compromised Jira account log-in panel



Screenshot of the employee's compromised credentials for financial remote management environment log-in panel

This potential threat lies in the ability of threat actors to exploit those employees' compromised credentials to access sensitive systems, perform unauthorized financial operations, exfiltrate critical data, or use the access for further attacks, making it particularly sensitive due to the direct impact on organizational operations, security, and reputation.

Interestingly, 13% of the machines had credentials related to the past employees of the company. It is worth mentioning that different infostealers vary in terms of their credential harvesting techniques — some based on active usage recording, while others — on saved passwords on the machine. Therefore, the presence of credentials associated with past employment does not necessarily reflect active usage at the time of infection.

KELA notes that this underlines the importance that organizations implement account management procedures including revoking access at the time an employee departs the organization, as unrevoked accounts represent a security risk if an unauthorized actor were to gain access.

Schneider Electric incident | Case Study

KELA observed and analysed an infected machine from the sample of this research including credentials to a VPN that had been compromised through infostealing malware to Schneider Electric, a company from the automation machinery manufacturing sector. KELA later observed that Schneider Electric was claimed victim to ransomware attacks by Clop ransomware (on June 27, 2023) and later by Cactus ransomware (on January 17, 2024) and by Hellcat ransomware (on November 2, 2024). KELA highlights that this may not be the confirmed initial access vector used for any of those ransomware attacks, however such compromised accounts could potentially be used by threat actors to conduct such attacks. In regards to the attack by Hellcat, it was later confirmed by one of their operators that they obtained access to Schneider Electric's Jira server using exposed credentials and then scraped 400,000 rows of user data using MiniOrange REST API. It is speculated that the breach may be related to a Schneider Electric employee infected by the Lumma infostealer in October 2024.

Snowflake Incident | Case Study

In mid-April 2024, a threat actor dubbed UNC5537 exploited stolen credentials to access customer accounts on Snowflake, a multi-cloud data warehousing platform. This attack, which affected at least 165 companies, was traced back to credentials obtained through infostealer malware. The threat actors bypassed accounts without multi-factor authentication (MFA) using various methods, including the web-based UI, command-line tools, and a custom utility named "rapeflake" to exfiltrate data. By late May, data belonging to victims like Santander Bank and Ticketmaster surfaced on cybercrime forums, leading to public disclosure and further investigations.

As part of its investigation, Snowflake later revealed⁴ that the threat actor also accessed a demo account belonging to a former employee using stolen personal credentials. According to Snowflake's official statement on May 30, 2024, this demo account, which was not protected by Okta or MFA, was isolated from Snowflake's production and corporate systems and did not contain sensitive data. However, the incident demonstrates how even a non-sensitive demo account access can be exploited by threat actors to escalate their activities and target more critical systems. This underscores the importance of awareness to access management and to revoking former employees' access to systems and ensuring the widespread adoption of MFA to mitigate potential attack vectors.

⁴ [Source](#)

Takeaways

The analysis of 300 infostealer victims, confirmed employees with access to corporate resources, highlighted several notable trends. Project management roles emerged as the most frequently affected, followed by consulting and software development. Personal computers, particularly unshared ones, were commonly infected, and credentials from current employment were compromised more often than those from past roles. These findings underscore the diverse vulnerabilities that infostealer campaigns exploit, emphasizing the need for enhanced cybersecurity awareness, robust device security, and proactive access management across all industries and roles.

Importantly, these compromised employees can inadvertently serve as the entry point for devastating ransomware attacks, as threat actors leverage stolen credentials to gain initial access to sensitive systems. The following chapter will delve deeper into how ransomware groups exploit valid accounts, including those compromised by infostealers, to carry out their attacks.

Ransomware groups and their use of valid accounts

The use of valid accounts is a common initial access vector used in cyberattacks.⁵ There are a number of methods in which threat actors can obtain these valid accounts, including password spraying attacks, brute force attacks, phishing, and the use of infostealer-compromised accounts that are being shared or sold in cybercrime sources. Among the actors that are known to use valid accounts as an initial access vector are ransomware groups, including Play, Akira and Rhysida.

Methodology and Scope

KELA reviewed victims of the above three ransomware groups that were claimed on their blogs between October 1, 2023 and October 1, 2024. KELA compared these victims against its data lake of compromised accounts to identify instances in which these victims had had accounts compromised through infostealing malware that were posted in cybercrime sources between 5 and 95 days before they were claimed as victims by the ransomware group.

KELA specifically looked for compromised accounts related to virtual private networks (VPN), remote desktop, remote monitoring and management (RMM), and Active Directory, as these are among the types of accounts that ransomware groups could use when gaining initial access.

KELA identified compromised accounts associated with some of the groups' victims that had been posted between 5 and 95 days prior to the attack being announced on the groups' blogs. Whilst it cannot be stated that these attacks occurred as a result of the use of these identified accounts, or even any infostealer-compromised account, these groups are known to use valid accounts, among other methods, to gain initial access. One of the means in which they could obtain valid accounts is through infostealer-compromised accounts, available on sale in cybercrime underground, like the ones described below.

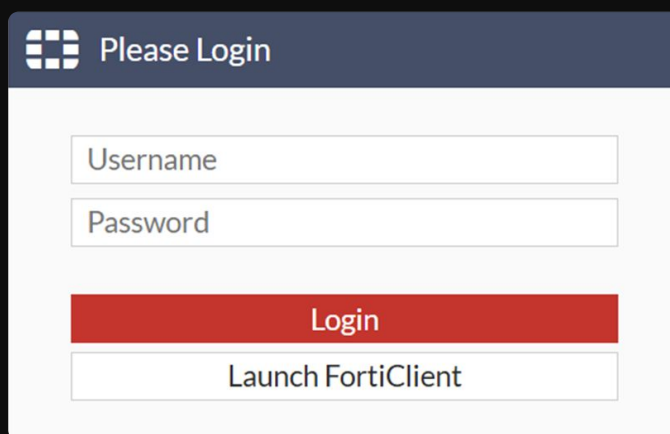
⁵ [Source](#); [source](#); [source](#)

Play

The Play ransomware group (also known as Playcrypt) has been active since at least June 2022. The Play ransomware group is believed to operate as a closed organization, without affiliate programs.⁶ Among the initial access vectors used by the group is through the abuse of valid accounts, including VPN accounts. Access to these accounts could be achieved through accounts that have been reused across different platforms, were previously exposed, or that were obtained through illegal means.⁷ Play ransomware actors have been observed using external-facing services such as Remote Desktop Protocol (RDP) and VPN for initial access.^{8,9}

KELA identified several victims of Play that were claimed between October 1, 2023 and October 1, 2024, that had compromised accounts shared between 5 and 95 days prior to the attack being claimed.

For instance, a Canadian steel manufacturer was claimed by Play on April 30, 2024 after the company detected unusual activity on April 17, 2024. KELA identified a compromised VPN account, associated with the victim company, that was posted on March 30, 2024 as part of a bot that was shared on a Telegram channel. KELA notes that the login page for the VPN is publicly accessible. In addition to the VPN account, KELA identified other services associated with the company which were also included in the same bot. These services mainly relate to what could be a development server.



The image shows a web-based login interface. At the top, there is a dark blue header with a white grid icon and the text 'Please Login'. Below the header, there are two white input fields with grey borders, labeled 'Username' and 'Password'. Underneath these fields is a prominent red button with the word 'Login' in white text. At the bottom of the form is a white button with the text 'Launch FortiClient'.

VPN login page

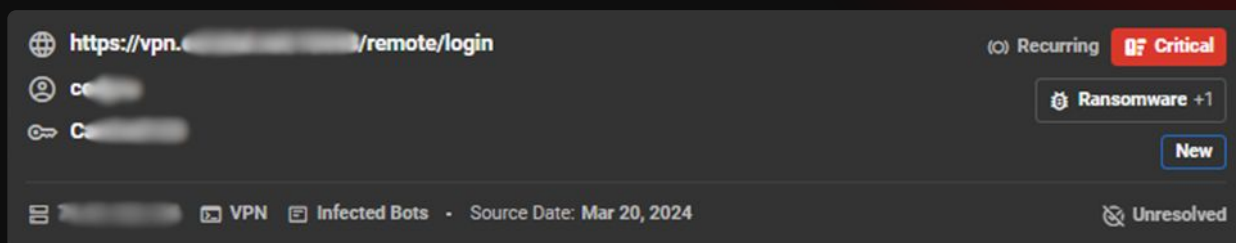
⁶ [Source](#)

⁷ [Source](#); [source](#)

⁸ [Source](#)

⁹ KELA notes that Play has also been observed using other initial access vectors in their attacks. Another infection vector used by the group is the exploitation of public-facing applications, particularly through known FortiOS (CVE-2018-13379 and CVE-2020-12812) and Microsoft Exchange (CVE-2022-41040 and CVE-2022-41082, also known as ProxyNotShell) vulnerabilities, [source](#)

Moreover, KELA identified a VPN account for a US-based construction company that was claimed as a victim of Play on March 27, 2024.¹⁰ The compromised account was included as part of a bot that was shared to a Telegram channel, in January 2024, and was again shared in February 2024 on Telegram as part of a ULP file.



Compromised VPN account as seen on KELA's platform

Finally, on February 5, 2024, a waste management company was claimed as a victim of Play. KELA identified a compromised account for a remote desktop service that was posted approximately 40 days before the attack was claimed by Play.¹¹

¹⁰ KELA was unable to access the service and was redirected to a Microsoft login page, however, prior to redirection a Citrix gateway page was displayed potentially indicating that this is being used as the authentication gateway.

¹¹ KELA was unable to access the site.

Akira

Akira was identified in March 2023, and initially targeted exclusively Windows environments.¹² However, the following month the group expanded their capabilities to target Linux machines, specifically VMware ESXI virtual machines.¹³

One of the initial access vectors that Akira has been observed using to gain initial access to their victims is using valid credentials. KELA notes that Akira's operators claim in their negotiations with victims that they purchased the initial access to the victim's system "on the dark web".¹⁴ Akira has also been observed gaining initial access to their victims through VPN services without multifactor authentication (MFA) enabled, mostly using known Cisco vulnerabilities (CVE-2020-3259 and CVE-2023-20269).^{15 16}

KELA identified numerous accounts that, based on the service URL, use Active Directory Federation Services (AD FS) for authentication, as well as VPN and remote desktop-related accounts of Akira's victims that were shared between 5 and 95 days prior to the victim being claimed on Akira's blog.

For example, KELA identified a compromised account associated with a machinery company that was claimed as a victim of Akira in August 2024. Among the accounts were Fortinet VPN login credentials. KELA also identified a compromised account for another service, which appears to use AD FS, that belonged to an employee that based on their LinkedIn page is still working at the organization.¹⁷ The account was posted 3 days before the company experienced disruption as a result of a cyberattack.

Furthermore, KELA identified accounts associated with victims of Akira that belonged to previous employees which highlights the importance that organizations implement the required user access management processes to ensure that the necessary accesses are revoked when employees leave. Among these accounts was an account related to a Canadian hospital that was claimed as a victim of Akira in November 2023. The organization stated in an update posted to their website that they experienced a data security incident on October 23, 2023. The compromised account, identified by KELA, was posted on September 23, 2023 as part of a bot shared on Telegram. KELA notes that the service is publicly available and appears to be a login portal to access various sites. KELA was able to identify the employee that the account belonged to. KELA notes that, based on the employee's LinkedIn, the employee left the hospital in March 2023. Other accounts of the employee, associated with the hospital, were also included in the bot such as Salesforce and Microsoft accounts.

¹² [Source](#)

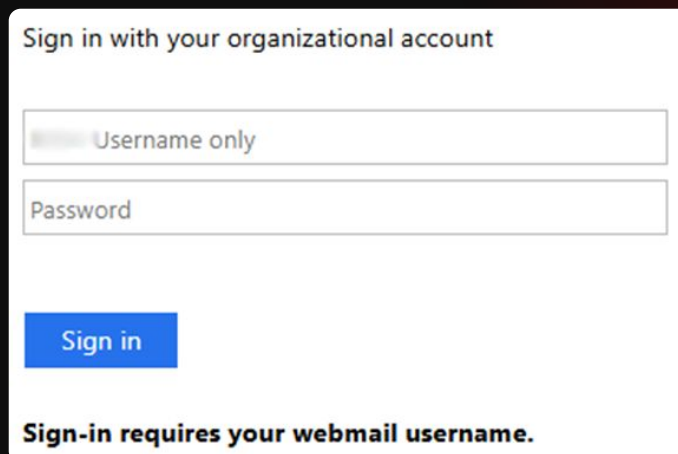
¹³ [Source](#)

¹⁴ [Source](#)

¹⁵ [Source](#)

¹⁶ Additional methods of initial access include the use of external-facing services such as RDP and spearphishing ([source](#))

¹⁷ KELA notes that this service could not be found (Error 404).



Sign in with your organizational account

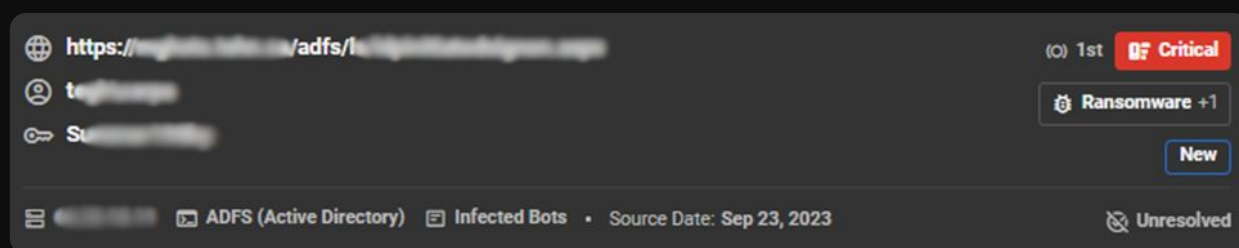
Username only

Password

Sign in

Sign-in requires your webmail username.

Hospital login page



Compromised VPN account as seen on KELA's platform

Furthermore, various accounts were detected by KELA that appear to belong to an individual who previously worked for an IT service provider company that likely provided IT services to a victim of Akira that was claimed in December 2023. Among the accounts were accounts for what appears to be an AD FS authentication portal for the victim organization.¹⁸

Finally, KELA identified two compromised remote access accounts for a transportation company that were shared in June 2024.¹⁹ The organization was claimed as a victim of Akira in August 2024 after the company detected the attack on July 7, 2024. KELA notes that the compromised accounts were shared around a week before the company reportedly detected the attack. One of the accounts belonged to an individual that worked as an administrative assistant at the company until November 2023.

¹⁸ KELA could not access the service and received a service unavailable HTTP Error 503 message.

¹⁹ KELA could not access the login portal.

Rhysida

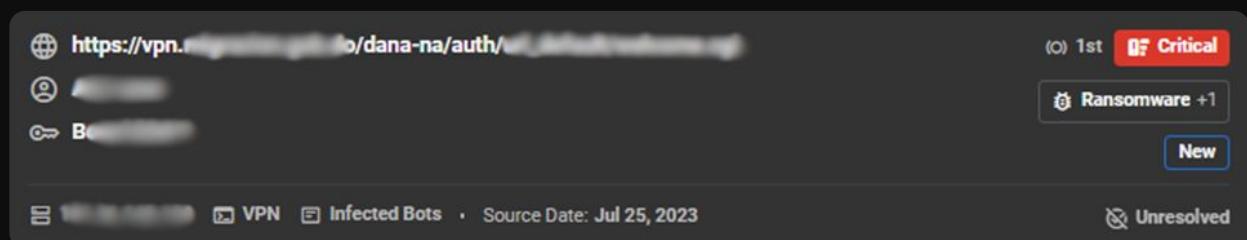
The Rhysida ransomware group claimed its first victims in June 2023. There have been indications that Rhysida is connected to another ransomware group that was active from 2021, called Vice Society.²⁰

The Rhysida group has been observed using compromised valid VPN credentials to gain initial access to their victims, notably due to accounts lacking MFA.²¹ There are also reports that Rhysida uses compromised RDP and VPN accounts that they have acquired from cybercrime sources.^{22 23}

KELA identified numerous accounts associated with Rhysida victims that were shared between 5 and 95 days before the victim was claimed. For example, Rhysida claimed a hospital based in Jordan on its blog in December 2023. KELA identified a compromised account for what appears to be a remote access account, for this hospital, that was posted in November 2023. KELA notes that the login page is accessible.

Moreover, KELA identified three compromised VPN accounts for another victim.²⁴ The victim, which is a utilities company, was claimed by Rhysida in September 2023. Among the accounts was an account which, based on KELA's research, belongs to an existing employee of the organization.

Furthermore, KELA identified a remote desktop account that was shared for a government entity that was later claimed as a victim of Rhysida.²⁵ Furthermore, a VPN account for another government entity was shared approximately 50 days before the victim detected unusual activity and about 70 days before the victim was claimed by Rhysida.²⁶



Compromised VPN account as seen on KELA's platform

²⁰ [Source](#); [source](#); [source](#)

²¹ [Source](#)

²² [Source](#); [source](#)

²³ They have also successfully conducted phishing campaigns to acquire credentials. In other cases, the group exploited vulnerabilities such as Zerologon, a privilege escalation flaw in Netlogon Remote Protocol (CVE-2020-1472) ([source](#))

²⁴ KELA could not access the site.

²⁵ KELA could not access the site.

²⁶ KELA could not access the site.

Takeaways

Valid accounts are a common initial access vector used by threat actors, including ransomware actors. There are multiple ways in which threat actors can obtain these accounts, including through infostealer-compromised accounts that are being circulated in cybercrime sources.

Play, Akira and Rhysida are all ransomware groups that are known to use valid accounts as an initial access vector. KELA identified compromised accounts associated with a number of these groups' victims that had been shared between 5 and 95 days before the attacks were claimed by the ransomware groups. KELA cannot confirm whether these accounts were used by the ransomware groups in their attacks, however, such accounts represent a significant threat to organizations as they can be abused by threat actors to gain access to an organization which they then use to conduct their attacks, like ransomware attacks.

Conclusion and Recommendations

Infostealers have become a prevalent tool in the cybercrime ecosystem, enabling the widespread theft of corporate credentials. This research by KELA delved into two critical aspects of this issue: the profile of employees infected by infostealers and the exploitation of compromised accounts by ransomware groups.

The analysis of 300 victims of infostealers highlighted several trends. Project management roles emerged as the most frequently affected (28%), followed by consulting and software development. Geographically, Brazil recorded the highest percentage of victims. The Technology sector was the most targeted. Personal computers, especially unshared ones (35.7%), were most commonly infected. Additionally, credentials from current employment were compromised more frequently than those from past roles. These findings underscore the diverse vulnerabilities that infostealer campaigns exploit, reinforcing the need for enhanced cybersecurity awareness, device security, and access management across industries.

Further research into ransomware groups like Play, Akira, and Rhysida revealed a concerning connection to these infostealer compromises. KELA identified certain compromised accounts associated with some of these ransomware groups' victims that had been shared between 5 and 95 days prior to the attack being claimed. While it cannot be definitively stated that these attacks occurred as a direct result of these identified accounts, these groups are known to use valid accounts, among other methods, to gain initial access.

Infostealer-compromised accounts, available on sale in cybercrime underground, represent a significant avenue for ransomware actors to obtain these valid credentials. This link between infostealer infections and potential ransomware attacks underscores the severity of credential compromise and the cascading risks it poses to organizations.

To address these growing threats, KELA recommends:

1. **Active Defense Monitoring:** Continuously monitor credential exposure to identify sensitive work-related credentials at the earliest stages of compromise. Early detection allows organizations to block potential security threats by promptly changing passwords, revoking access to compromised accounts, and implementing other protective measures. Leveraging a cyber exposure management platform can help organizations effectively monitor exposed credentials and address vulnerabilities before they escalate into significant security breaches. This applies to all employees and particularly those in high-risk roles like project management and software development.

2. **Ensure Proactive Access Management and Rights Revocation:** Organizations must actively manage access levels and authorized privileges for employees during their tenure, adjusting them as responsibilities change. Special emphasis should be placed on promptly revoking access for former employees to prevent unauthorized use of lingering credentials. Regular audits of access rights and privileges can strengthen security and minimize risks associated with outdated or inappropriate permissions. This is crucial for all employees, especially in sectors with high employee turnover or those handling sensitive data, and also includes demo or testing accounts.
3. **Implement Robust Antivirus Solutions:** Deploy comprehensive antivirus software with real-time scanning and behavioral analysis to minimize the risk of falling victim to cyber threats. Antivirus protections provide an essential layer of defense against malicious mechanisms, such as phishing campaigns, malicious downloads, and drive-by attacks. Regular updates and advanced features enhance the effectiveness of these solutions, providing critical protection against evolving cyber threats. This is especially important on personal devices where employees might handle corporate data.
4. **Invest in Employee Training and Awareness:** Prioritize training programs that enhance employees' understanding of cyber threats and their associated risks. This is particularly critical for organizations where employees access sensitive work-related environments from personal computers. Training sessions should be as practical as possible, focusing on the organization's unique identifiers, specific asset types, and tailored scenarios. This approach empowers employees to independently recognize and respond to potential threats while fostering a cybersecurity-aware culture. Specific training should be given regarding credential security, multi-factor authentication (MFA) best practices, and recognizing phishing attempts.
5. **Implement and Enforce Multi-Factor Authentication (MFA):** Enforce MFA on all accounts, especially those with access to sensitive data or critical systems, such as VPNs, remote desktop services, and administrative accounts. MFA significantly reduces the risk of unauthorized access, even if credentials are stolen or compromised. Regularly review and update MFA configurations to ensure they remain effective against evolving threats.
6. **Regularly Audit and Review Access Logs:** Implement a system for regularly auditing and reviewing access logs for suspicious activity. This can help identify unauthorized access attempts or compromised accounts early, allowing for prompt action to mitigate potential damage. Automate log analysis and anomaly detection where possible to improve efficiency and effectiveness.
7. **Incident Response Plan:** Develop and maintain a comprehensive incident response plan specifically addressing credential compromise and potential ransomware attacks. Regularly test and update the plan to ensure it remains effective and aligned with current threats.

Fight AI with AI

5000+

Ransomware
Victims

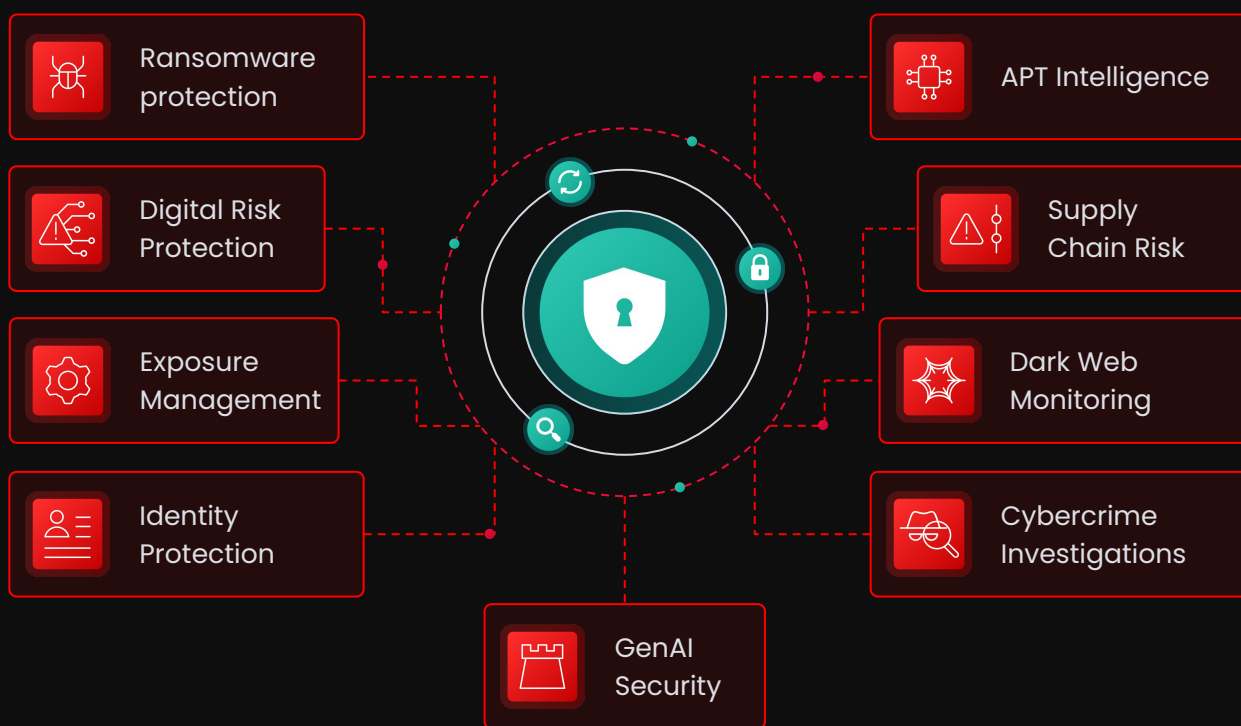
4.3 Million+

Infected
Machines

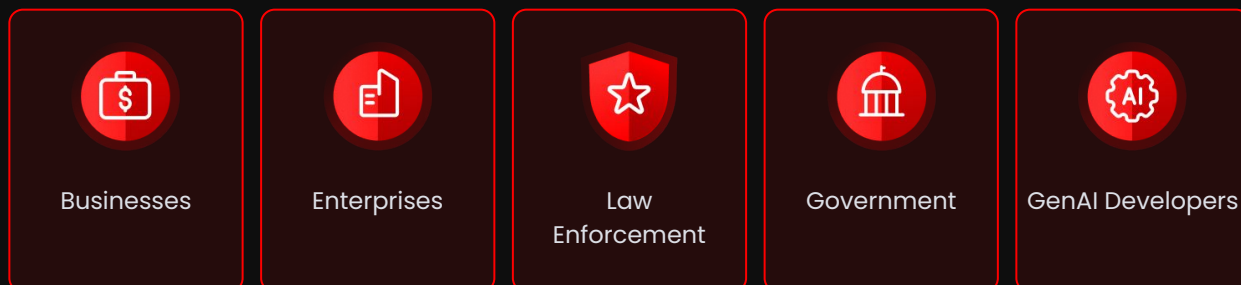
4 Billion

Compromised
Credentials

Proactive Threat Exposure Reduction



Who Are Our Clients?



What Makes Our Customers Happy

KELA holds a strong rating of 4.8 on Gartner Peer Reviews, exceeding Recorded Future. This high rating underscores KELA's dedication to quality, relevance, and the delivery of high-impact intelligence that integrates seamlessly into your security strategy.

4.9 ★★★★★

47 Ratings on Gartner Peer Insights

As of April 16, 2025

- ✓ Stop Real Attacks Before They Happen
- ✓ Exposure-Centric with Actionable Intelligence
- ✓ Automated and Easy to Use



Empowering Diverse Industries:

From retail to finance, healthcare to government, KELA's platform ensures that every sector can safeguard against financial loss, compliance violations, operational disruptions, and more.

[Book a demo](#)

Choose KELA for 100% real, actionable intelligence!