

## Essential Guide

# Protecting Your Assets and Identities Against

# The Rising Threat of Infostealers

```
011001000
01001000000111001
001110100011001010111100
101110011001100100000011011
010011001010010000001100110011
1011010001110100011010010111001
0010100100000011000100110100101101
0001110100110000101101000110101011
00110001000000110100101101000010111
01100100000011010010110011001000000
100000011100100110000101101100110010
000110010101110000111010000100000011
0110010000001101110110110001000001
0010000 1100110 00100010
10001 0111001 00000
0110 0010110 00101
00010 11101010 110011
01101001 01000 101110 101000110
001011100110010 0011100110110111
0000101101101 100011011101101
11101000010 11001110110111
111100010000001101
0111001000100000
0100100000011101
00000101110001
```



# Executive Summary

In 2023, **infostealer activity increased by 266%**. Infostealers are malicious programs designed by threat actors to steal sensitive information, which once stolen can lead to identity theft, fraud, network breaches and significant business disruption.

Any organization has its crown jewel assets, whether it's a central database holding PII, an application that drives operations, or something else entirely that holds significant value to the company. To access these assets, attackers can choose to target either the technology or the people. While technology can be targeted by finding vulnerabilities, misconfigurations and exposures, people are targeted by phishing, malicious websites, and malware. Infostealers are **a critical part of how attackers target the people side of this equation, in order to gain access to valuable credentials** that can help them with a wide range of malicious activities.

Understanding infostealers and their business impact is a crucial part of securing any modern organization. In this eBook, we will take a holistic look at the infostealer landscape, discussing top infostealers and how they work, how infostealers evade modern cybersecurity tools, and how you can protect your assets and identities against this increasing risk.

---

<sup>1</sup>IBM [X-Force Threat Intelligence Index 2023](#)

# Table of contents

|                                                                       |           |
|-----------------------------------------------------------------------|-----------|
| Chapter #1 . . . . .                                                  | 4         |
| <b>What are Infostealers?</b>                                         |           |
| Chapter #2 . . . . .                                                  | 7         |
| <b>The Role of Infostealers in the Modern Cybercrime Ecosystem</b>    |           |
| Chapter #3 . . . . .                                                  | 10        |
| <b>How Do People Get Infected by Infostealers?</b>                    |           |
| <b>Top Infostealers in the Cybercrime Ecosystem . . . . .</b>         | <b>14</b> |
| RedLine Stealer . . . . .                                             | 15        |
| Lumma Stealer . . . . .                                               | 16        |
| Stealc . . . . .                                                      | 17        |
| Raccoon Stealer . . . . .                                             | 18        |
| Vidar . . . . .                                                       | 19        |
| Chapter #4 . . . . .                                                  | 20        |
| <b>Identity Protection as the First Line of Defense</b>               |           |
| <b>Staying One Step Ahead of Infostealers at Every Turn . . . . .</b> | <b>22</b> |

## Chapter #1

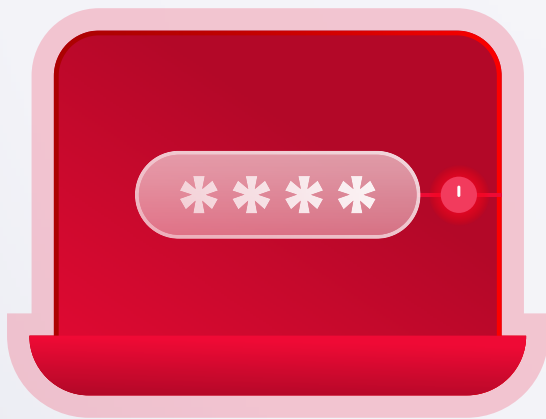
# What are Infostealers?

Infostealers are a category of malware that specialize in silently gathering sensitive information from an infected device. They are sometimes known as infostealing malware.

Unlike other types of threat, like a ransomware attack which grabs attention by locking down a system or encrypting data and demanding payment to return access or unencrypt the data, infostealers have a more insidious arrival. Infostealers focus on quietly extracting data like login credentials, financial information, and other private data without the user's knowledge. In this way, **infostealers can easily fly under the radar for long periods of time**, and the first time an organization may realize they are a victim could be when an attack takes place using the stolen information as an entry point. Complicating the situation further, often **infostealers may infect an employee's personal computer**, which can result in credentials to organizational assets being stolen entirely outside of their network.



# Infostealers typically aim to harvest:



**Login credentials for websites and services**

**Payment information such as credit card numbers**

**Browser session cookies to hijack authenticated sessions**

**Cryptocurrency wallets including private keys and wallet files**

**Autofill data such as addresses and other saved personal details**

**System details such as network, hardware and OS specifications**

**Logs and event data, to gain insight into behavior, security incidents or system issues**

Once harvested by infostealers, the attacker exfiltrates data to their infrastructure, where it can be used for a wide range of use cases, including launching a further attack such as identity theft, or directly sold to other threat actors on cybercrime marketplaces, mainly in the Dark Web.

# What do Infostealers do?

Infostealers have various capabilities and use an assortment of techniques to harvest data from infected systems. Some examples include:



## Keylogging

When this occurs, the infostealer can record every keystroke which a user inputs, allowing attackers to filter for passwords, financial data, and other PII.



## Form grabbing

Forms are often used to enter login credentials and payment information, so it's highly effective for infostealers to intercept this data on web pages.



## Clipboard hijacking

When clipboard content is targeted by infostealers, it can be monitored and even altered, giving attackers access to account numbers or passwords.



## Screen capture

In some cases, an infostealer takes sporadic snapshots of the screen, bypassing text extraction limitations by harvesting a full screenshot of any activity.



## Session hijacking

Cookies and session tokens can be stolen which allow attackers to impersonate the victim's session, gaining immediate access to online accounts.



## Credential dumps

When login credentials are saved to web browsers or software, infostealers extract the stored system data, and then attempt to crack any encryption.



## Email harvesting

In this situation, the infostealer searches emails and additional files on the machine, which can then be used for phishing material or spam.



## Crypto-wallet harvesting

Certain strains of malware can search for common crypto-wallet software, in the hopes of stealing private keys to crypto accounts.

## Chapter #2

# The Role of Infostealers in the Modern Cybercrime Ecosystem

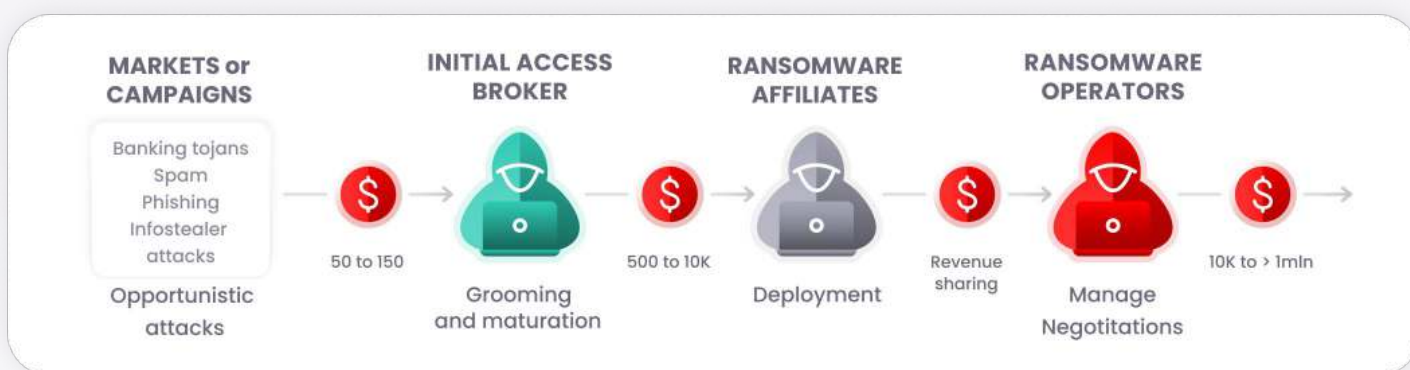
Why are infostealers such a hot topic right now?

In 2023, for the first time, and continuing now in 2024, the use of valid accounts has become the most common entry point into victim environments, alongside phishing — which can also be a method used to launch an infostealer attack. In IBM's X-Force Threat Index, these together represented 60% of all incidents and a 71% increase year over year was presented for infostealers alone.

Protecting valid accounts and identities from infostealers should be a priority on any security agenda.

# Hackers Don't Break In, They Log In

For threat actors, there are a number of reasons why **infostealers have become so popular as a weapon of choice**. Credentials are an easy way to access an organization's infrastructure without drawing attention to the attacker or setting off security solutions, and infostealers are one of the best ways to get those credentials in the first place — less time consuming than attempting to brute force by guessing passwords, and more effective than credential stuffing, where threat actors buy or uncover username/password combinations for one service, and then attempt to use the same combinations to gain access to another.



In comparison, infostealers are a relatively cheap and easy way to gain a foothold into organizations in order to launch a further attack such as ransomware, financial fraud or Business Email Compromise, or to obtain data that can then be sold on for a quick pay-day on botnet markets, and through Telegram channels or clouds of logs.

Credentials are then acquired by various **cybercriminal groups**, including ransomware operators, who use them as a foothold to infiltrate networks and deploy malicious software. **This ecosystem is designed with a clear division of labor:** IABs handle the acquisition and sale of access, while ransomware groups and other attackers focus on exploiting the compromised systems for their own goals, such as encrypting data for ransom or launching further attacks.

The growth in tools such as **anti-detect browsers** has also reduced the chance of detection for threat actors, making it easier than ever for cybercriminals to hide their identity and leverage infostealer harvested data.

# What are Anti-detect Browsers?

Anti-detect browsers are designed to help users mask or alter their digital fingerprints to avoid detection by online tracking systems, anti-fraud mechanisms, or website verification processes. They do this by simulating different user environments and providing features to obscure or spoof the information websites typically collect from users,

While there are legitimate purposes for anti-detect browsers, cybercriminals can use these browsers to mimic victim environments to bypass fraud detection and log in undetected, manage multiple stolen accounts simultaneously using isolated browser sessions, spoof locations and devices to evade detection, bypass MFA using session cookies or stolen tokens, bypass browser-based detection techniques such as captchas, and even to conduct fraudulent transactions using stolen financial information.

In addition to ransomware, stolen credentials can be used for credential stuffing attacks (where attackers try to gain access to multiple accounts using the same credentials), business email compromise scams, and espionage activities. Often, threat actors specialize in one of these functions, streamlining the process and increasing their efficiency within this illicit market. This coordinated system enables rapid turnover, as credentials flow from one set of actors to the next, each with specialized roles that maximize the profitability of stolen data and ensure continual exploitation of compromised networks.

Through this chain, cybercriminal marketplaces serve as central hubs where infostealer-harvested credentials and other stolen data is bought, sold, and traded, sustaining a vast underground economy.



## Chapter #3

# How Do People Get Infected by Infostealers?

There are various methods that cybercriminals use in order to infect a machine or an organization with an infostealer.

In many cases, Traffickers collaborate with infostealer developers or IABs, and earn commissions for successful infections. They employ techniques such as social engineering and SEO poisoning to lure users into downloading software that has hidden malware, or visiting compromised websites. Traffickers may disguise downloads as legitimate programs, offer game cheats, or software cracks, which then execute malware when clicked on or installed.



# Whether by using Traffickers or directly targeting users, some techniques in more detail include:



## Phishing Emails

Infostealers are often distributed via phishing attacks, where malware arrives by email attachment or via links to malicious websites. These emails appear legitimate, and can often leverage fear or excitement to convince the recipient to open an infected attachment or visit a compromised webpage.



## Drive-by Downloads

Even without a user directly interacting with a malicious link or attachment, in some cases, merely visiting a compromised or malicious website can result in an infostealer being installed on a device. This is known as a drive-by download, which exploits vulnerabilities in browsers or plugins to trigger the install.



## Malvertising

A portmanteau of malicious advertising, threat actors can inject malicious code into advertisements, pop-ups or website banners, which then infect machines when users click on the advert or even just visit the website. These can be hosted on scam websites, or even on legitimate websites by leveraging vulnerabilities.



## Trojanized Software

Another method used to inject infostealers is through pirated or cracked software, which is disguised as a legitimate application. When users download these programs, they may inadvertently install the infostealer, which activates when the software is run for the first time.



# Leaked Credentials vs. Compromised Accounts: Understanding the Difference



**Leaked Credentials:** These are login details—usernames and passwords—that have been exposed in data breaches or shared publicly online. While concerning, they're often inactive or outdated and can usually be addressed with measures like password resets or MFA implementation.



**Compromised Accounts:** These are far more dangerous. They represent active, unauthorized access into accounts, often obtained through infostealers from an actively compromised machine or browser, or phishing attacks. Compromised accounts allow attackers to bypass security measures and exploit corporate systems, posing a significant threat to your organization.

## Top Infostealers in the Cybercrime Ecosystem

Over the years, a range of infostealers have emerged, each with different capabilities and methods of distribution. Here are some of the most prominent examples:



**RedLine Stealer**



**StealC**



**Vidar**



**Lumma Stealer**



**Raccoon Stealer**

# RedLine Stealer



## RedLine Stealer

⚠ Type: Cybercrime ⏸ Status: Inactive



One of the most widespread infostealers, RedLine targets browser credentials, cryptocurrency wallets, and session cookies. It is frequently sold on underground forums and updated regularly to evade detection.

In November 2024, RedLine was disrupted by law enforcement, and KELA can confirm that there has been a lack of new bots infected by RedLine since this time<sup>2</sup>. However, as with all Malware-as-a-Service, it is always possible that they will return, or their affiliates will switch to other operations.

### Five facts about RedLine Stealer:



#### Cost

This infostealer can be bought by subscription for \$100–600 per month.



#### Capabilities

As well as steal data, RedLine Stealer can upload and download files, execute commands, and send back information about the infected device.



#### Spread

RedLine has been known to be spread via phishing emails, malvertising, cracked software, fake downloads, and malicious websites.



#### Targets

While RedLine Stealer has been used in attacks around the world, it appears to avoid systems in the Commonwealth of Independent States (CIS), including Russia.



#### Detection

This infostealer can be customized so that attackers can choose what to steal, and it also uses obfuscation techniques to avoid being discovered.

<sup>2</sup>Redline infostealer disrupted by law enforcement, Security Week, November 2024

# Lumma Stealer



## Lumma Stealer

ⓘ Type: Cybercrime ⓘ Status: Active



Lumma Stealer, also known as LummaC2 Stealer has been seen in the wild since 2022, and is known for targeting browser credentials, cryptocurrency wallets, and system information. Popular among cybercriminals for its affordability and modular design, Lumma Stealer is often marketed on underground forums and designed to evade traditional detection methods.

### Five facts about Lumma Stealer:



#### Cost

Lumma Stealer is typically sold for around \$250-1000 for monthly subscription, with optional updates and support packages as add-ons.



#### Capabilities

Besides credential theft, Lumma Stealer can upload and download files, execute remote commands, and exfiltrate system details.



#### Spread

This malware is commonly distributed through phishing campaigns, malicious websites, cracked software, and browser extensions.



#### Targets

Lumma avoids infecting machines in the Commonwealth of Independent States (CIS) region, with built-in geofencing to exclude certain locales, including Russia.



#### Detection

Lumma Stealer uses sophisticated code obfuscation techniques to evade detection, with attackers often customizing it for specific targets.

# Stealc

The logo for StealC, featuring the word "StealC" in white text on a red rectangular background.

## Stealc

! Type: Cybercrime    ○ Status: Active

A large red circular logo with the word "StealC" in white text, surrounded by concentric blue circles and small blue dots.

Often considered to be a copycat infostealer of Raccoon and Vidar, StealC is a credential-stealing malware with the presumed developer Plymouth, readily available on Russian-speaking cybercrime markets.

### Five facts about Stealc:



#### Cost

The product is offered for \$300 for monthly subscription, \$700 for 3 months, and \$1000 for 6 months.



#### Capabilities

StealC can execute commands and download and upload files. With an admin panel, attackers do not need technical proficiency to launch an attack.



#### Spread

This infostealer is frequently distributed through phishing emails, fake software downloads, malvertising, and infected browser extensions.



#### Targets

While customizable, StealC's configuration typically includes a geofencing option to avoid infecting systems in the Commonwealth of Independent States (CIS).



#### Detection

StealC uses multiple evasion techniques, including code obfuscation and in-memory execution, to avoid detection by antivirus tools.

# Raccoon Stealer



## Raccoon Stealer

ⓘ Type: Cybercrime ⏸ Status: Active



A notorious infostealer known for its ability to steal data from browsers, system files, and cryptocurrency wallets — Raccoon Stealer is favored for its ease of use and is widely distributed via phishing campaigns. The Ukrainian developer was extradited to the US, where he faces criminal charges related to his role in the infostealing malware<sup>3</sup>.

### Five facts about Raccoon Stealer:



#### Cost

A subscription to Raccoon Stealer can be obtained on cybercrime markets for \$200 per month.



#### Capabilities

This infostealer harvests data from over 60 applications, including login credentials, credit card information, cookies, and cryptocurrency wallet accounts.



#### Spread

Often delivered via exploit kits, Raccoon can mimic the legitimate application ESET Live Installer to help trick users into downloading the malware.



#### Targets

The FBI has warned that more than 100,000 devices have been infected by Raccoon Stealer, and set up a website for victims<sup>4</sup>.



#### Detection

The latest version of Raccoon includes a reporting system that detects and blocks IPs used by crawlers and bots from cyber-intelligence firms.

<sup>3</sup>Ukrainian developer behind Raccoon Stealer extradited to the U.S., Bank Info Security, February 2024

<sup>4</sup>[Raccon.ic3.gov](https://raccon.ic3.gov)

# Vidar



## Vidar

ⓘ Type: Cybercrime ⏸ Status: Active



A sophisticated infostealer with the ability to exfiltrate sensitive browser data, system information, and stored files. In 2023, Vidar hit the headlines after one of the malware users successfully infected Booking.com, gaining access via a phishing email<sup>5</sup>.

From: [redacted] <[redacted]@email.com>  
Sent: 10 October 2023  
To: [redacted]  
Subject: Re: LOST ID

Good afternoon! I am writing again about a lost passport. Despite thoroughly searching our car, including under the seats and in the trunk, we were unable to locate my passport. Moreover, we have checked all the luggage and clothes. We strongly believe that we left it at your hotel. To assist you in identifying it, I have attached photos of the passport along with all necessary details. In addition I have provided our check-in details, including the quest number.

[https://drive.google.com/uc?export=download&confirm=antivirus&id=\[redacted\]](https://drive.google.com/uc?export=download&confirm=antivirus&id=[redacted])  
Password 123456

Please assist us in finding the document, as we have another trip planned for next week and will need it again.  
Best wishes!

## Five facts about Vidar:



### Cost

Subscriptions start from \$130 for one week to \$750 for 90 days.



### Capabilities

As well as steal information Vidar can be a downloader for additional malware, such as ransomware or banking trojans.



### Spread

There are many ways that Vidar spreads, including via phishing campaigns, malvertising, cracked software, and bundled alongside ransomware.



### Targets

Vidar has a special interest in cryptocurrency wallets, so attracts threat actors looking to steal from Exodus, Electrum, and more.



### Detection

Vidar often uses encrypted communication channels to evade detection, as well as anti-analysis measures to bypass antivirus tools.

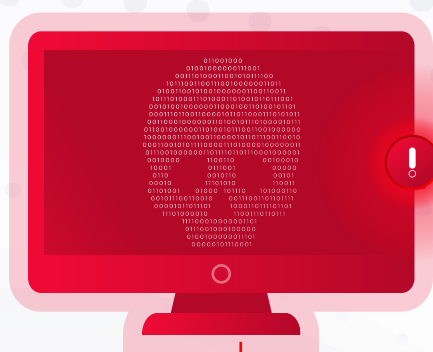
<sup>5</sup>Secure Works, [Booking.com attack 2023](#)

# Why Aren't Infostealers Being Detected by EDR?

Despite the growing sophistication of Endpoint Detection and Response (EDR) solutions, many infostealers continue to evade detection.

One reason for this is **fileless malware techniques**, where malware runs directly in memory instead of writing files to disk. Lumma uses multi-stage fileless techniques to deliver its final payload and other infostealers, for example part of the execution of some versions of Agent Tesla and Mekotio also function this way. EDR solutions rely on scanning files, so it's much more of a challenge for them to detect these kinds of attacks.

In other cases, infostealers launch **Living Off the Land (LotL) attacks**, where they abuse legitimate system tools including PowerShell, Windows Management Instrumentation, and other trusted processes. Malware blends in with normal system activity, making it harder to detect. One example is RedLine, that often uses PowerShell or cmd.exe and in 2023 spread its malware via malicious Microsoft OneNote files, or Azorult, that while it has been quiet in recent years, has been known to use legitimate Windows processes such as explorer.exe to execute payloads.





**Advanced obfuscation techniques** are also part of what makes infostealers hard to detect by traditional antivirus and EDR tools. When attackers are purposely encrypting or scrambling code, it's challenging to detect their infostealers in action.



Although it is rare, in some cases infostealers will exploit zero-day vulnerabilities, which are unknown to software vendors and therefore cannot be patched. As EDR solutions often rely on signatures or detection rules, these become **EDR blind spots**, and fall through the cracks. Additionally, any EDR is only as good as its configuration, which means it can't cover all attack vectors or be immune to **human error**. It's important to remember that even with perfect configuration in place, in some cases, your users will turn off EDR settings or alerts if they interfere with their user experience. For example, users may wish to install a game, cracked software, or shadow IT, and fall back on insecure practices to make that happen.

As a result of all of these factors and more, Endpoint Detection and Response is not enough to protect against the risk of infostealers.



## Chapter #4

# Identity Protection as the First Line of Defense

In an era where personal and corporate data is under constant threat, **proactive identity protection** has become crucial.

During a two-day research study of one botnet market by Verizon, 65% of infostealer logs were posted for sale less than one day after being collected<sup>6</sup>. By focusing on securing digital identities and assets at the earliest stages, organizations and individuals can significantly reduce the risks resulting from infostealer infections, and effectively shield themselves from the rising threat of infostealers and compromised assets and credentials.

Remember, cyber attacks aren't being designed and implemented overnight. In reality, infostealers are one part of a complex cybercrime ecosystem, where different attackers with various specialties coordinate and liaise on known channels and with specific TTPs to launch both opportunistic and targeted attacks over long periods of time. With the right vantage point, you can stay ahead of the threat.

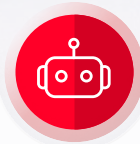
<sup>6</sup>Verizon, [2024 Data Investigations Report](#)

To catch these activities ahead of time, identity security tools monitor illicit Dark Web marketplaces, cybercrime forums, and messaging and bot marketplaces, intercepting compromised credentials in real-time, and offering access to a deep and wide range of insights, including infostealer and bot-related information, associated threats, and compromised service categories. Acting preventatively, identity security can also help enforce best practices such as account reset, password rotation and multi-factor authentication. Your organization gains access to prioritized alerts, organized by severity and business context.

## ● Key Capabilities for Identity Protection Solutions



**Interception** of compromised assets and accounts by monitoring botnet markets, Telegram channels, and other Dark Web sources.



**Automation** of specific pre-emptive measures such as quarantining infected machines, enforcing MFA, or resetting passwords for compromised accounts.



**Take-down** services that remove stolen credentials from markets and Dark Web channels before they can be purchased by bad actors.



**Monitoring** of the TTPs of known threat actors, to learn the plans, processes and methodologies for current and future attacks



**Insights** into the evolving infostealer landscape, including Malware-as-a-Service offerings, new infostealers, and new tools and techniques.

# Staying One Step Ahead of Infostealers at Every Turn

The evolving threat landscape calls for constant vigilance. Infostealers are increasingly sophisticated, employing advanced evasion techniques to bypass security measures.

However, with a combination of strong identity protection alongside best practices such as regular software updates and a layered security approach, you can reduce your exposure to these threats. The key is to be proactive and ensure that security measures are continuously adapting to the changing tactics of cybercriminals.

## The Cybercrime Underground Chaos



# In the past year, KELA has tracked:

**5000+**

Ransomware Victims

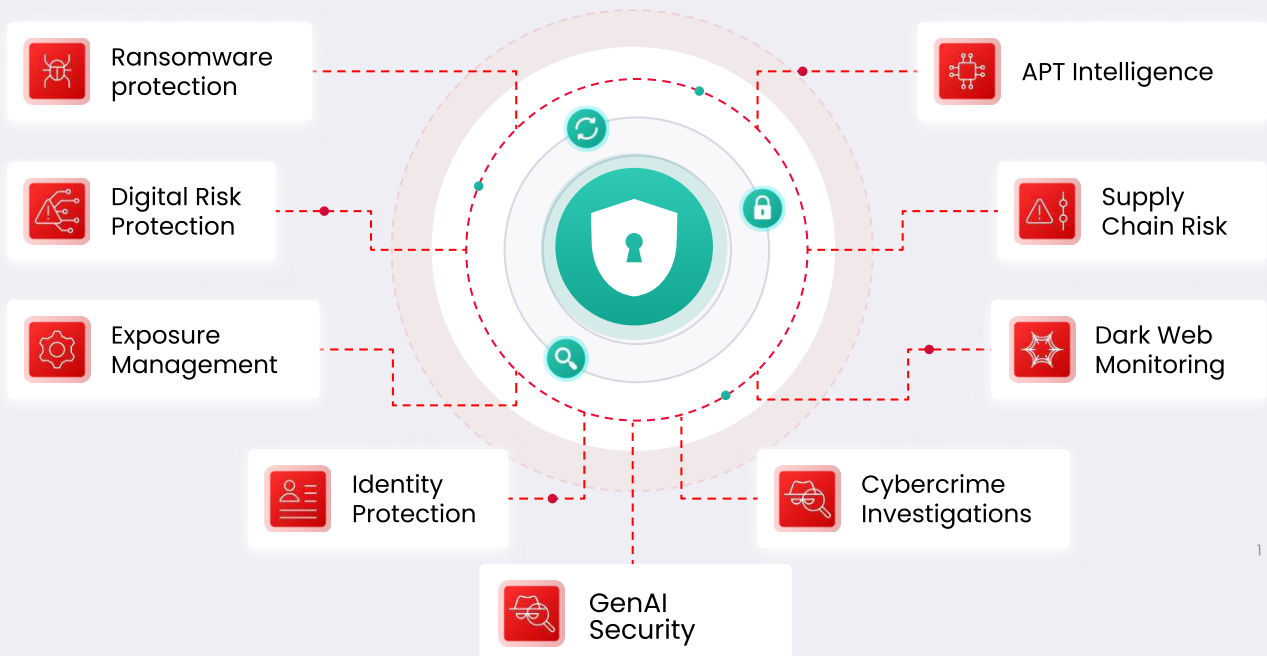
**52 Million+**

Infostealer Logs

**3 Billion +**

Compromised Credentials

## Proactive Threat Exposure Reduction:



## Who Are Our Clients?



Businesses



Enterprises



Law Enforcement



Government



GenAI Developers



# What Makes Our Customers Happy

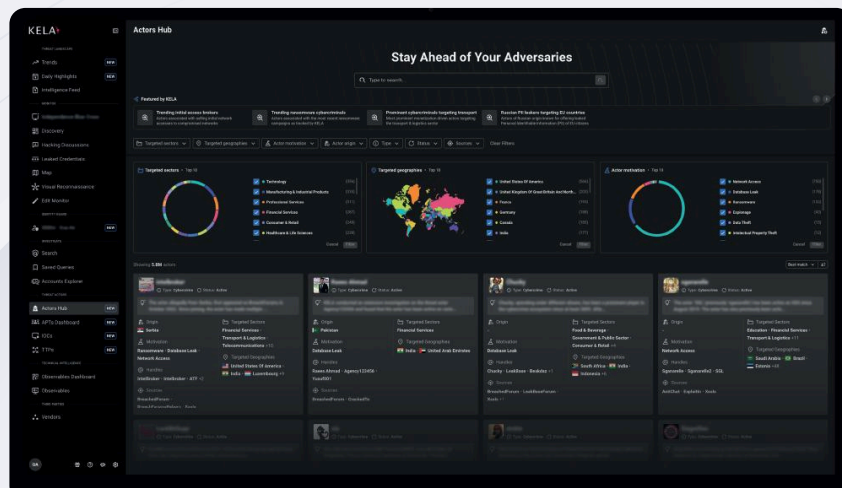
KELA holds a strong rating of 4.8 on Gartner Peer Reviews, exceeding Recorded Future. This high rating underscores KELA's dedication to quality, relevance, and the delivery of high-impact intelligence that integrates seamlessly into your security strategy.

4.8 ★★★★★

36 Ratings on Gartner Peer Insights

As of 28 Aug 2024

- ✓ 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!