SOCRadar
Your Eyes Beyond

Identity
Threat Landscape Report 2026

Executive Summary

Identity is the New Attack Surface

Authentication systems are now exposed to the internet by design and infostealer malware have scaled credential theft to an industrial level. Together, these two forces produce a continuously refreshed pool of valid identities and attackers have learned to use them instead of attempting to bypass advanced security products.

THE STRUCTURAL SHIFT

Cloud adoption, SaaS sprawl, and remote work have repositioned identity as the primary boundary of enterprise security. The network perimeter no longer contains the threat surface.

At the same time, infostealer malware has made credential theft scalable, automated, and cheap. A single infection produces a structured log of usernames, passwords, session cookies, and device data.

01

The attack path has shifted

Instead of breaking systems, threat actors just log in. Valid credentials bypass advanced security products and endpoint controls without triggering alerts.

02

Advanced Security Tools Are Ineffective

When an attacker uses stolen credentials, their actions look indistinguishable from the real user. Detection becomes structurally harder.

OPERATIONAL IMPLICATIONS

Data exfiltration

A compromised identity with cloud access can exfiltrate bulk data silently, using native platform tools that generate no anomalous signatures.

Privilege escalation

Starting from a single compromised user account, attackers can escalate to administrative or domain-level control with minimal resistance.

Lateral movement

Valid credentials enable movement across systems, applications, and tenants without triggering security controls because each step looks like authorized access.

If an employee identity is compromised, the organization is effectively exposed even if they use state of the art security products. Identity must be treated as a critical security boundary. It should be governed, monitored, and defended with the same rigor as any network perimeter.

Strategic Priority

The Identity Threat Landscape

Digital identity has become a central element of modern enterprise security. Most corporate systems rely on identity-based access controls to manage authentication and authorization. As organizations expand their use of cloud services, SaaS platforms, and remote access technologies, identities increasingly function as the primary gateway to corporate infrastructure.

This shift has made identity a major target for threat actors. Instead of relying only on software exploitation, attackers often focus on obtaining valid credentials and authenticated sessions. Access obtained through legitimate identities allows threat actors to operate within environments with reduced detection risk. Once access is established, attackers can move laterally, escalate privileges, and reach sensitive systems.

Several developments have accelerated this trend. The widespread use of cloud identity providers concentrates access control in a small number of accounts. At the same time, infostealer malware campaigns collect large volumes of credentials, browser session tokens, and authentication data from infected devices. These stolen identities frequently appear in underground markets where they are purchased by ransomware operators, fraud networks, and other threat actors.

An organized underground ecosystem now supports the trade of compromised identities and system access. Stealer logs, corporate credentials, and remote access accounts are commonly sold or shared through dark web forums and closed communities. These assets provide a direct entry point into corporate environments and often serve as the starting stage of broader attacks such as ransomware operations, business email compromise, and data exfiltration.

As a result, identity compromise has become a key driver of modern cyber incidents. Understanding how identities are stolen, traded, and exploited is essential for assessing current cyber risk and developing effective defensive strategies.

Cloud Adoption and the Dissolution of the Perimeter

The concept of a fixed network perimeter no longer reflects how modern environments operate. As organizations moved to cloud services, the separation between internal and external systems has largely disappeared. Access is no longer tied to a defined boundary, but to user identities and cloud-based resources. As a result, many incidents now originate from compromised email and cloud accounts rather than direct network intrusion.

This change alters how attacks take place. Earlier models assumed that adversaries needed to penetrate a boundary. In current environments, valid credentials provide direct access without triggering traditional defenses.

WHY THE PERIMETER DISSOLVED

The Old Perimeter

A defined network edge separated "inside" from "outside." Firewalls and VPNs stood guard at the boundary.

THEN

Cloud Migration

Workloads moved to cloud infrastructure. Inside and outside of the enterprise collapsed into one another.

SHIFT

New Attack Surface

Incidents now begin with compromised accounts instead of traditional network breaches.

NOW

MODERN THREAT LANDSCAPE

SaaS Entry Points

Attackers most often break in through SaaS applications. No network breach required.

Identity is the New Perimeter

World class security products were built for hackers breaking in. Today's threat actors simply log in with stolen credentials.

Perimeter Defense is Obsolete

Traditional defenses assumed a boundary that no longer exists.

SaaS Proliferation and The Expansion of the Digital Identity Attack Surface

Each additional SaaS application increases the number of identities, permission sets, and trust links within an environment. Many of these elements are not reviewed with the same rigor as core systems. As a result, overly permissive integrations are becoming a key risk factor. When a single API connection is compromised, it can propagate access across multiple systems and, in some cases, across different organizations.

Governance gaps further amplify this risk. Untracked integrations and informal tooling reduce visibility and slow response efforts. Once access is established, containment depends on how quickly it can be identified and revoked. Identity artifacts such as tokens, OAuth grants, service principals, and federated links are often not managed as primary security controls. At the same time, external SaaS dashboards, CI/CD pipelines, and vendor-managed data stores now function as critical control layers, often without strong runtime protections.

KEY RISK FACTORS

SaaS Proliferation

Each new SaaS app an org adopts creates new identities, permissions, and trust relationships.

ORIGIN

Over-privileged Integrations

Third-party API links expand blast radius. One compromised API can cascade into hundreds of breached environments.

BLAST RADIUS

Governance Gap

Shadow infrastructure and unmanaged SaaS connections multiplies the risks.

RISK MULTIPLIER

KEY RISK FACTORS

Weak Control Planes

CI/CD platforms, vendor-hosted DBs, and third-party SaaS consoles are high-value targets with relatively lower resistance.

EXPOSURE

Identity Sprawl

Tokens, OAuth grants, service principals, and federated identity chains are rarely treated as core security posture.

SPRAWL

Non-Human Identity Problem

Service accounts, API keys, and OAuth tokens outlive their scope, accumulate permissions, and skip review cycles.

BLIND SPOT

KEY STATISTICS

PRIMARY ENTRY VECTOR

SaaS & OAuth apps & grants

The primary entry vector for modern identity-based attacks — enabling access without traditional network breach.

LEAST SCRUTINIZED

Non-human service accounts & keys

The least scrutinized credential type — service accounts and API keys are rarely rotated, monitored, or governed.

Credential Reuse: The Structural Vulnerability

Credential reuse is arguably the most consequential structural weakness in modern security, because it converts historical breaches into perpetual risk.

Most successful intrusions in the last few years didn't start with malware. Instead they started with valid credentials. Once inside, attackers used the victim's own tools to move laterally, blending into normal traffic and escalating privileges in minutes.

Beyond simple password reuse, attackers have matured their credential theft techniques. Information-stealing malware such as Raccoon Stealer and Redline steal credentials and session tokens from browsers, allowing attackers to authenticate.

Identity exposure is now permanent because you cannot "clean up" the fallout from large-scale credential breaches that have already seeded the dark web. This means any password that has ever appeared in a breach must be treated as compromised indefinitely.

Historical breaches become perpetual risk

Credential reuse is the most consequential structural weakness in modern security. Every past breach extends its reach indefinitely. A credential exposed once is a credential exposed forever.

WHY IT MATTERS

ENTRY METHOD

Valid credentials, not malware

Most successful intrusions in recent years started with valid credentials. The attacker authenticates and enters as a trusted user. They don't need any exploits anymore.

AUTHENTICATION ABUSE

INSIDE BEHAVIOUR

Lateral movement in minutes

Attackers use the victim's own tools to move laterally, blending into normal traffic and escalating privileges within minutes of access.

PRIVILEGE ESCALATION

DISTRIBUTION

Credentials seed the dark web

Large-scale breaches distribute credentials across dark web databases instantly and permanently, putting every reused password at ongoing risk.

PERMANENT EXPOSURE

STRUCTURAL IMPLICATIONS

REMEDIATION

Identity exposure cannot be undone

There is no mechanism to remove credentials already seeded across the dark web.

IMPLICATION

Any reused password is compromised

Any password that has ever appeared in a breach must be treated as compromised indefinitely. Regardless of when the breach occurred or whether the user is aware of it.

Infostealer Malware

CORE FUNCTION

Silent data exfiltration — no disruption, no noise

Unlike ransomware or wipers, infostealers are designed to be invisible. They collect stored credentials, session data, and files from an infected device and transmit them to attacker infrastructure without locking systems or alerting users. The infection may go undetected for days, weeks, or indefinitely.

DATA TARGETS

• **Browser credentials**	Saved usernames and passwords, autofill data, and stored payment card details from browsers.
• **Session cookies**	Active authentication tokens that allow account hijacking without needing a password.
• **Cryptocurrency wallets**	Wallet files, seed phrases, and private keys from desktop applications and browser extensions.
• **System fingerprint**	IP address, hardware details, OS version, installed software, and a desktop screenshot captured at time of infection.
• **Files of interest**	Documents matching operator-configured keywords or extensions. Threat actors can target terms like "password", "wallet", or "seed".

INFECTION VECTORS

Phishing emails · Malicious attachments · Cracked software & key generators · Malvertising · Fake software updates · Downloads from untrusted sites · SEO poisoning · ClickFix / fake CAPTCHAs

WHY THEY ARE EFFECTIVE

Bypasses traditional defences

Infostealers use valid credentials rather than exploits. Logging in with a stolen password looks identical to a legitimate login — triggering no alerts from most perimeter or endpoint controls.

Credentials remain valid over time

Stolen passwords and session tokens are often not rotated. A log from months or years ago may still provide working access — extending the operational window of every infection indefinitely.

Feeds the wider attack economy

Stealer logs are the primary upstream input for Initial Access Brokers, who package and resell access to ransomware groups. A single infection can enable multiple downstream attacks across different threat actors.

MALWARE-AS-A-SERVICE MODEL & OUTPUT

Malware-as-a-Service model

Many infostealers are sold by subscription on dark web forums. Operators receive the malware binary and a dashboard to view stolen logs — lowering the technical barrier for buyers with no malware development skills.

Output: stealer logs

Stolen data is packaged into structured records called logs. These are sold on dark web forums and Telegram channels, used for account takeover and fraud, or leveraged as initial access for ransomware operations.

Key Infostealer Families

MALWARE CLASSIFICATION

A malware "family" shares the same code lineage, development history, and operational identity

Infostealers are not one-off binaries. They are maintained software projects with versioned releases, feature updates, and identifiable code structures. Grouping them into families reflects how they are built, sold, tracked, and attributed.

01	**Code lineage and reuse**	Infostealers are maintained projects. Developers release versioned updates, fix bugs, and add features over time. Variants built from the same core codebase are grouped into one family even if they carry different names or have been forked by other actors.
02	**Malware-as-a-Service ecosystem**	Many families are sold as subscription services on underground forums. Each acts like a product line: buyers receive the binary, an admin panel, a log management dashboard, and sometimes customer support. This structure makes families stable, recurring, and distinctly identifiable.
03	**Detection and attribution**	Security analysts need consistent labels to track threats across time and organisations. Grouping malware into families allows teams to build detection rules from known behaviours, track campaigns across incidents, and attribute activity to specific threat actors or services operating that family.
04	**Feature differentiation**	Each family has technical differences that distinguish it from others: which browsers and applications are targeted, cookie and session theft capabilities, anti-analysis and evasion methods, and file grabbing rules. These differences matter for both attackers choosing a tool and defenders building countermeasures.
05	**Market branding in cybercrime**	Well-known families function like brands in underground markets. Reputation for high-quality logs, operational stability, and ease of use drives adoption.

ADDITIONAL CHARACTERISTICS

Families evolve continuously

A family does not stay static. New versions add evasion techniques, expand browser support, or target new data sources. Tracking version history is how analysts understand capability growth and anticipate what a family can now do that it previously could not.

One family, many operators

A single infostealer family can be actively used by hundreds of independent operators simultaneously. Each runs their own campaigns and targets, but all use the same underlying malware.

LummaC2 (Lumma Stealer)

OVERVIEW

MaaS used by multiple financially motivated groups including ransomware affiliates

Lumma Stealer (LummaC2) is a malware-as-a-service (MaaS) offering used by multiple financially motivated groups, including ransomware affiliates. The malware focuses on credential theft, browser data extraction, and cryptocurrency wallet harvesting, and it can also deploy secondary payloads. Distribution follows a multi-vector model that includes phishing, malvertising, trojanized software, and abuse of legitimate platforms. Microsoft-led disruption efforts targeted this ecosystem and resulted in the takedown of a large portion of its infrastructure.

EVASION TECHNIQUES

OBFUSCATION

Advanced obfuscation techniques

The malware applies advanced obfuscation methods to hinder analysis. These include control flow flattening and control flow obfuscation, custom stack decryption routines with large stack variables, and dead code insertion to disrupt static analysis tools.

LOW-LEVEL

Low-level execution techniques

Lumma uses low-level execution methods such as direct syscalls and Heaven's Gate. These techniques reduce visibility to user-mode security tools and complicate detection.

MASQUERADE

Process injection and masquerading

The malware performs process hollowing into legitimate binaries such as explorer.exe and executes under trusted process contexts. This allows it to blend with normal system activity and evade behavioral detection.

C2 EVASION

C2 evasion and resilience

Lumma relies on a multi-tier C2 architecture with fallback channels, including Telegram and Steam profiles. All traffic is encrypted over HTTPS and routed through services such as Cloudflare. C2 endpoints are further protected using ChaCha20 and custom encryption schemes.

NOTABLE DEPLOYMENT CAMPAIGNS

Canadian ClickFix Campaign

Thousands of phishing emails used fake invoice lures targeting Canadian organisations. Victims were routed through compromised sites to a ClickFix page that deployed Lumma alongside Xworm malware.

Manufacturing Sector Attacks

Lumma deployed in tandem with Amadey Bot against the manufacturing industry. Phishing emails and malicious downloads were used to exfiltrate sensitive network data from industrial environments.

Hamster Kombat Gamers

Lumma disguised as automation tools targeting players of the viral mobile game. Malicious payloads were hidden inside GitHub repositories promoted to the gaming community.

EtherHiding via Binance Smart Chain

Malicious code embedded in BSC smart contracts presented visitors with a fake CAPTCHA. The ClickFix technique silently loaded commands from the blockchain.

RedLine Stealer

OVERVIEW

Lua bytecode execution — GitHub repository abuse

A new variant of RedLine Stealer uses Lua bytecode to execute malicious logic, distributed through GitHub by abusing a trusted repository to host the payload. It is delivered via a compressed archive containing an installer, which executes the payload during installation. The malware compiles and runs the embedded bytecode at runtime, avoiding traditional script execution paths, and establishes persistence using scheduled tasks and fallback execution paths. It communicates with command and control servers over HTTP. Capabilities include system profiling, credential and data collection, screenshot capture and exfiltration. The malware has been observed globally across multiple regions.

EVASION TECHNIQUES

BYTECODE

Bytecode-based execution

Malicious logic is stored as compiled Lua bytecode rather than readable scripts, which reduces visibility for static detection tools.

LOLBAS

Living-off-the-Land techniques

The malware abuses native Windows components to trigger execution and uses error-handling mechanisms for stealth execution.

COMPONENTS

Use of modified legitimate components

The malware leverages altered versions of legitimate Lua tooling, helping it blend into normal software behavior.

RECON

Environment awareness

System and network context is collected before any further actions are taken.

NOTABLE DEPLOYMENT CAMPAIGNS

2020

Email Campaign Distributing RedLine Stealer

In early March 2020, researchers identified an email campaign delivering a then-new information stealer known as RedLine. The malware was promoted across underground channels and supported by a dedicated C2 panel. The campaign used pandemic-related themes to increase credibility and urgency. Emails encouraged recipients to support disease research efforts, leading to malicious payload delivery. Targeting focused on healthcare and manufacturing sectors in the United States.

2021

Malvertising Campaign Delivering RedLine Stealer

In early 2021, threat actors used malicious search ads to exploit increased demand for secure messaging applications. Users were redirected to cloned download pages that delivered RedLine Stealer instead of legitimate software. The campaign relied on social engineering and lookalike domains. Stolen data was later sold or used in further attacks.

Raccoon Stealer

Raccoon Stealer v2 is a malware-as-a-service (MaaS) infostealer built to steal browser credentials, cookies, credit card data, crypto-wallet data, Telegram Desktop data, local files, and host information. After the original operation paused in March 2022, the malware was rebuilt and relaunched as Raccoon Stealer 2.0 in May 2022.

EVASION & ANTI-ANALYSIS TECHNIQUES

String and configuration obfuscation

Raccoon v2 uses Base64 and RC4 to hide embedded strings and C2 configuration values. Separate RC4 keys can be used for internal strings and for the C2 list.

Dynamic linking at runtime

The malware resolves many API functions during execution instead of relying only on standard imports. It also downloads required third-party DLLs at runtime, which keeps the initial executable small.

Frequent network indicator changes

Operators changed unusual User-Agent strings over time, likely to weaken static network signatures.

NOTABLE DEPLOYMENT CAMPAIGNS

Cracked software distribution

The campaign relied on pirated software lures, where droppers were disguised as cracked installers to infect users. These installers delivered Raccoon Stealer alongside additional payloads, including malicious browser extensions, click-fraud bots, and Djvu/Stop ransomware. The stealer harvested browser-stored data such as passwords, cookies, autofill information, and cryptocurrency wallet details.

Vidar

OVERVIEW

MaaS derived from the Arkei family

Vidar is an information-stealing malware derived from the Arkei family and is operated as a malware-as-a-service (MaaS), allowing threat actors to configure campaigns and data collection. The infection chain typically follows a sequence of a malicious advertisement leading to a fake website, followed by a ZIP archive download containing an oversized executable. Once executed, the malware retrieves command-and-control infrastructure details via Telegram or fallback platforms such as Steam. Vidar is capable of exfiltrating a wide range of data, including browser credentials, cookies, cryptocurrency wallets, files, and application data.

EVASION & ANTI-ANALYSIS TECHNIQUES

SIZE EVASION

File size inflation (padding)

Executable artificially increased to ~684 MB using null bytes. Exceeds common scanning limits (e.g., VirusTotal upload cap). Padding inserted in the middle of the binary, preventing easy removal without breaking execution.

C2 RESILIENCE

Multi-channel C2 retrieval

The malware uses multiple channels to retrieve command-and-control information. Telegram serves as the primary source, while Steam profiles are used as a fallback. This design reduces reliance on a single infrastructure point and complicates disruption efforts.

BLENDING

Use of legitimate DLLs

The payload retrieves archives that contain benign libraries. These libraries are then abused for credential extraction, allowing malicious activity to blend with legitimate components and evade detection.

ANONYMITY

Infrastructure obfuscation

The operators use VPN gateways and are increasingly shifting toward Tor to maintain anonymity. Traffic is routed through proxy layers, and backend IP addresses are rotated frequently to avoid tracking and blocking.

NOTABLE DEPLOYMENT CAMPAIGNS

Google malvertising campaign

The campaign targeted users searching for widely used productivity and creative tools. Malicious ads redirect users to fake domains that closely imitate official download pages. Additional lures observed in the same campaign include OBS Studio, DaVinci Resolve, Rufus, and Krita.

Malware bundling campaigns

Vidar has been deployed alongside other malware families, including DJVU ransomware, IcedID, and RedLine stealer. This bundling approach increases monetization opportunities and expands the impact of a single infection.

SEO poisoning and cracked software

Some campaigns relied on SEO manipulation and YouTube-driven traffic to distribute malware. Victims were directed to fake download pages or cracked software sites, increasing exposure through organic search and social channels.

Stealc

OVERVIEW

Malware-as-a-Service first advertised January 2023

Stealc is an information stealer first advertised in January 2023 on Russian-speaking Dark Web forums by a threat actor known as Plymouth. It is positioned as a Malware-as-a-Service offering, with continuous development and regular feature updates. Observations show dozens of samples in the wild across more than 40 C2 servers. The ecosystem includes a fully featured admin panel for log parsing, filtering, and resale preparation, indicating strong alignment with underground log markets.

EVASION & ANTI-ANALYSIS MECHANICS

STATIC ANALYSIS

Dynamic API Resolution and No Import Table

StealC avoids using a standard Import Address Table entirely. Instead it traverses system memory at runtime to resolve Windows API functions dynamically, preventing static analysis tools from enumerating its capabilities from the binary alone.

BLENDING

Living off the Land with Legitimate DLLs

StealC retrieves legitimate DLLs at runtime and uses them to access stored data and perform decryption. By relying on trusted libraries, the malware blends its activity with normal system operations and reduces suspicion during analysis.

EXFILTRATION

Chunked Exfiltration — 256 KB / 512 KB

Large stolen files are split into 256 KB or 512 KB chunks and sent as multipart HTTP POST requests.

NOTABLE DEPLOYMENT CAMPAIGNS

Amadey Loader Campaign

A separate campaign involved delivery of Stealc via the Amadey loader, originating from a compromised self-hosted GitLab instance. The campaign abused legitimate infrastructure to evade detection, and established persistence through scheduled tasks and relocation of files to AppData. The primary payload targeted Chrome and Edge credentials via StealC, while a crypto clipper plugin was used for wallet hijacking. All exfiltrated data was sent to a dedicated Stealc C2 server.

Qilin StealC and ClickFix Campaign

In a notable 2025 campaign, initial access was achieved through a fake human verification prompt (ClickFix) hosted on a compromised website, leading the victim to execute a batch file. This resulted in the installation of NetSupport RAT with persistence established via registry Run keys. As a secondary payload, StealC V2 was deployed through DLL sideloading using mfpmp.exe alongside a malicious DLL. The outcome included credential theft, VPN access to a Fortinet device using those stolen credentials, and ultimately the deployment of Qilin ransomware.

Stealer Logs

A stealer log is a structured dataset produced by infostealer malware after infecting a system. It contains harvested data that can be directly used for account takeover and fraud. It is **the output artifact of an infostealer infection**. It is usually packaged as a folder or archive and stored locally before exfiltration to attacker infrastructure.

WHAT A STEALER LOG TYPICALLY CONTAINS

Browser credentials

Saved usernames and passwords, autofill data, and credit card numbers extracted from browsers.

Session cookies

Active authentication cookies that allow an attacker to hijack live sessions and bypass multi-factor authentication without needing the account password.

Crypto wallet data

Seed phrases, private keys, and wallet files from desktop applications and browser extensions can allow immediate and irreversible transfer of funds.

System fingerprint

Hardware profile, OS version, IP address, installed software, running processes.

Application tokens

Session tokens and credentials from messaging apps, gaming platforms, VPN clients, and email clients.

Files of interest

Documents matching operator-configured keywords or extensions — text files, PDFs, and anything containing terms like "password", "wallet", or "seed".

LOG LIFECYCLE

Packaged and exfiltrated

The collected data is compressed into a ZIP archive or structured folder on the victim's machine, then sent to the attacker's command and control server.

Sold on dark web marketplaces

Logs are traded individually or in bulk on criminal marketplaces. Buyers include Initial Access Brokers, fraud operators, and ransomware groups who use them to gain footholds in corporate environments.

Case Study 1: The Snowflake Campaign

WHAT HAPPENED

Large-scale campaign — compromised customer credentials, not platform vulnerability

In 2024, a large-scale campaign targeted customers of Snowflake, with initial activity observed in mid-April and public disclosure following in late May. Multiple high-profile victims were impacted, including Santander Bank and Ticketmaster. Threat actors such as "whitewarlock" and clusters tracked as UNC5537 monetized the access via data sales and extortion. Notably, the campaign was not attributed to a platform vulnerability but was instead driven by compromised customer credentials.

STRUCTURAL CONDITIONS THAT ENABLED THE CAMPAIGN

Credential-centric access model

Snowflake environments rely on valid credentials for access, and the lack of enforced MFA across some accounts increased overall exposure.

Reuse of credentials from stealer logs

Attackers leveraged previously stolen credentials at scale, aligning with the well-known "hackers don't hack, they log in" pattern.

Decentralized customer responsibility

Security configurations such as MFA and IP restrictions were customer-managed, and inconsistent security posture across tenants created uneven protection.

HOW CREDENTIALS WERE OBTAINED

Commodity infostealer infections

A Snowflake employee device was reportedly infected with Lumma Stealer, which harvested credentials, session data, and system information.

Stealer log ecosystems

Compromised credentials were likely aggregated and distributed via dark web markets, with over 500 Snowflake-related instances observed in stealer logs.

CONSEQUENCES

Personal data exposure

Customer PII, communications metadata, and employee records were exfiltrated across multiple victim organisations and advertised for sale on criminal forums.

Regulatory & legal exposure

Public-company disclosure obligations were triggered. Incidents created regulatory notification requirements, litigation risk, and reputational damage across affected organisations.

Extortion & ransom collection

The federal indictment described successful ransom collection from victims. Stolen data was leveraged as extortion pressure, with some organisations making payments to prevent publication.

Case Study 2: Telefónica Intrusion

WHAT HAPPENED

Sustained campaign — multiple incidents across the first half of 2025

A series of intrusions targeted Telefónica across the first half of 2025, beginning with an initial breach of an internal Jira ticketing system. The attackers were linked to the Hellcat ransomware group, and multiple incidents followed, indicating a sustained campaign rather than a single event. Data was leaked on a dark web forum, in some cases without prior extortion, while later stages shifted toward staged leaks and ransom pressure.

STRUCTURAL CONDITIONS THAT ENABLED THE CAMPAIGN

High infostealer infection footprint

Over 500 employee devices had been infected in a prior period, exposing credentials for both internal systems and third-party platforms used by the organization.

Weak identity security controls

The absence of strong password policies, combined with evidence that brute-force attacks were feasible on some systems, left identity controls critically underdeveloped.

HOW CREDENTIALS WERE OBTAINED

Infostealer malware

A stealer malware was used to compromise the credentials of more than 15 employees, harvesting browser-stored credentials and session data in the process.

Credential aggregation

Access to a large internal dataset containing approximately 24,000 employee records and many other files from the company enabled further targeting and escalation beyond the initial foothold.

CONSEQUENCES

Data exposure

The initial leak comprised approximately 2.3 GB of internal data, while a second breach saw up to 106 GB exfiltrated. The exposed material included internal tickets and issue summaries, employee data and communications, network diagrams and operational logs, and customer-related records.

Identity risk expansion

Compromised employee credentials extended the threat beyond Telefónica's own perimeter, with third-party accounts including cloud and enterprise tools also affected as a result.

Reputational and regulatory impact

Public leaks and ransom threats drew significant attention, placing the organization under ongoing scrutiny from regulators and eroding public trust.

Case Study 3: Orange Spain Attack

WHAT HAPPENED

Orange Spain experienced a multi-hour internet outage after unauthorized access to its RIPE account

Orange Spain experienced a multi-hour internet outage after unauthorized access to its RIPE account. The attacker, known as "Snow," altered BGP routing and RPKI records, which disrupted route announcements and led to significant traffic loss, estimated at around 50%. The incident affected customer connectivity but did not involve data exfiltration. Services were restored after Orange regained control of the RIPE account.

STRUCTURAL CONDITIONS THAT ENABLED THE CAMPAIGN

Exposure in stealer ecosystems

Credentials for RIPE accounts are widely available in infostealer marketplaces.

Weak account security controls

There was no enforced multi-factor authentication (MFA) on RIPE accounts, compounded by a lack of strong password policies.

Centralized control plane risk

A single RIPE account had authority over large IP ranges, creating a high-impact single point of failure.

HOW CREDENTIALS WERE OBTAINED

EMPLOYEE'S DEVICE WAS INFECTED

Raccoon Stealer infection in September 2023

An Orange Spain employee's device was infected with Raccoon infostealer malware in September 2023. The malware harvested stored credentials, including access to the RIPE account (access.ripe.net). The compromised account used a weak password "ripeadmin" and had no MFA enabled, allowing direct account takeover. The credentials were later discovered in publicly available stealer logs and reused by the attacker.

CONSEQUENCES

Service disruption

Customers experienced internet connectivity issues for several hours due to a large-scale routing failure caused by invalid BGP announcements.

Traffic impact

Network traffic dropped by approximately **50%** during the incident window.

Operational risk exposure

The incident demonstrated how identity compromise can disrupt core network infrastructure.

Access Brokers

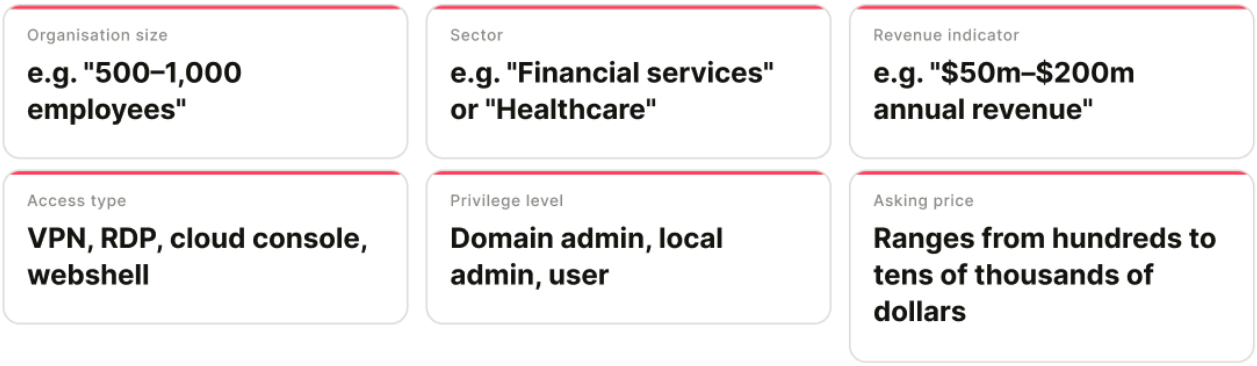
Access brokers, commonly referred to as Initial Access Brokers (IABs), are specialized threat actors who focus on obtaining unauthorized access to corporate environments and monetizing that access. They operate as intermediaries within the cybercrime economy. Their role is limited to gaining and validating access, after which they sell it to other actors who conduct follow-on activities such as ransomware deployment, data exfiltration, or financial fraud.

OPERATIONAL MODEL

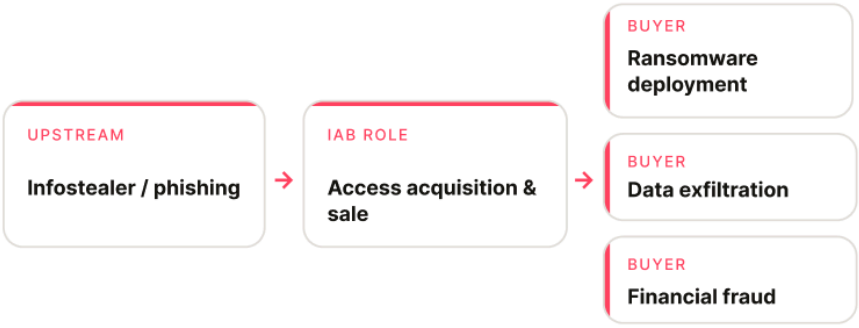
Types of Access Sold

Access brokers offer a range of entry points into corporate environments. Common examples include corporate VPN and RDP access, cloud service accounts such as Microsoft 365 or AWS, privileged credentials including domain administrator accounts, and session tokens or cookies obtained through infostealer logs. The latter has become increasingly important, as it enables bypass of certain authentication controls.

WHAT A DARK WEB LISTING TYPICALLY INCLUDES



ROLE IN THE MODERN ATTACK CHAIN



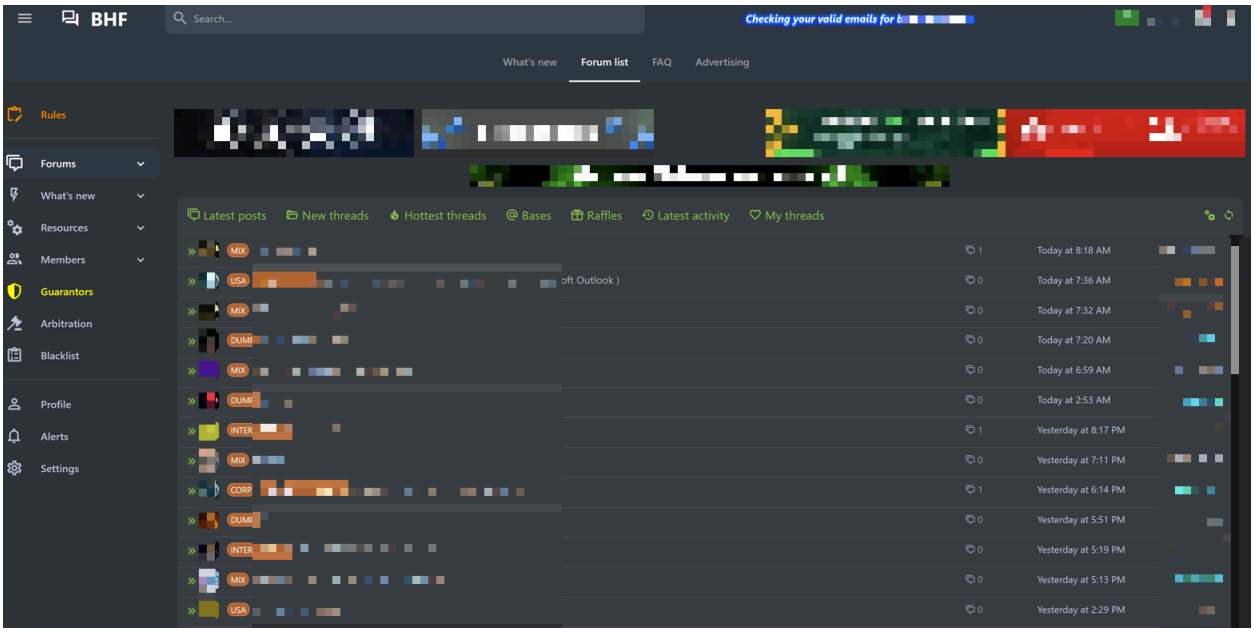
Dark Web Markets

Dark web forums play a central role in the identity threat ecosystem. They function as structured marketplaces where threat actors exchange credentials, access, and tooling.

These platforms support different stages of the attack chain, from initial access brokerage to large scale data distribution. Forums also enable reputation systems, escrow services, and vendor specialization, which increases efficiency and trust among criminal actors. **Stealer logs** are one of the main data sources fueling this ecosystem.

The combination of dark web distribution channels and automated credential harvesting has shifted identity into a primary attack surface. In many cases, attackers no longer need to exploit technical vulnerabilities. Access is obtained through valid credentials, making expensive security solutions obsolete.

BHF



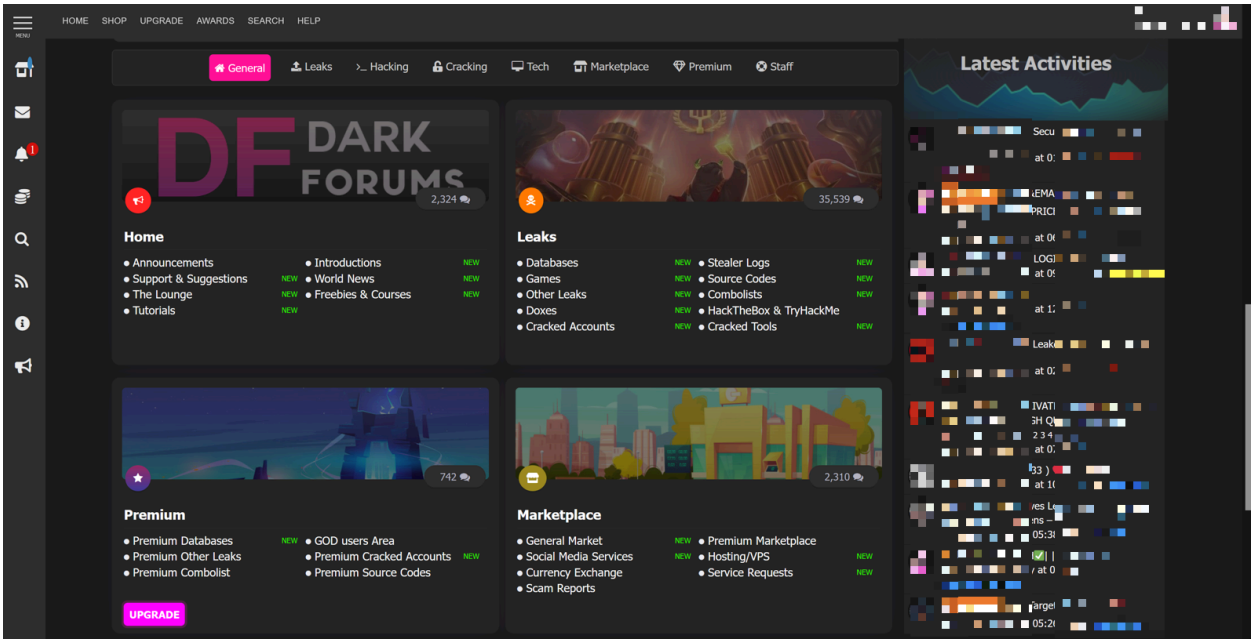
Main screen of BHF hacker forum

BHF (Best Hack Forum) is a Russian-language cybercrime forum that has been active since at least 2012. It is accessible via both the surface web and the Tor network and serves as a platform for threat actors involved in a wide range of illicit activities.

The forum is organized into categories such as software cracking, social engineering, access sales, vulnerability exploitation, combo list distribution, stealer logs, spam tools, and hacking tutorials.

To support transactions, BHF provides an escrow (guarantor) service aimed at reducing fraud between participants. Due to its longevity, technical scope, and large user base, it remains a significant component of the Russian-speaking underground ecosystem.

DarkForums



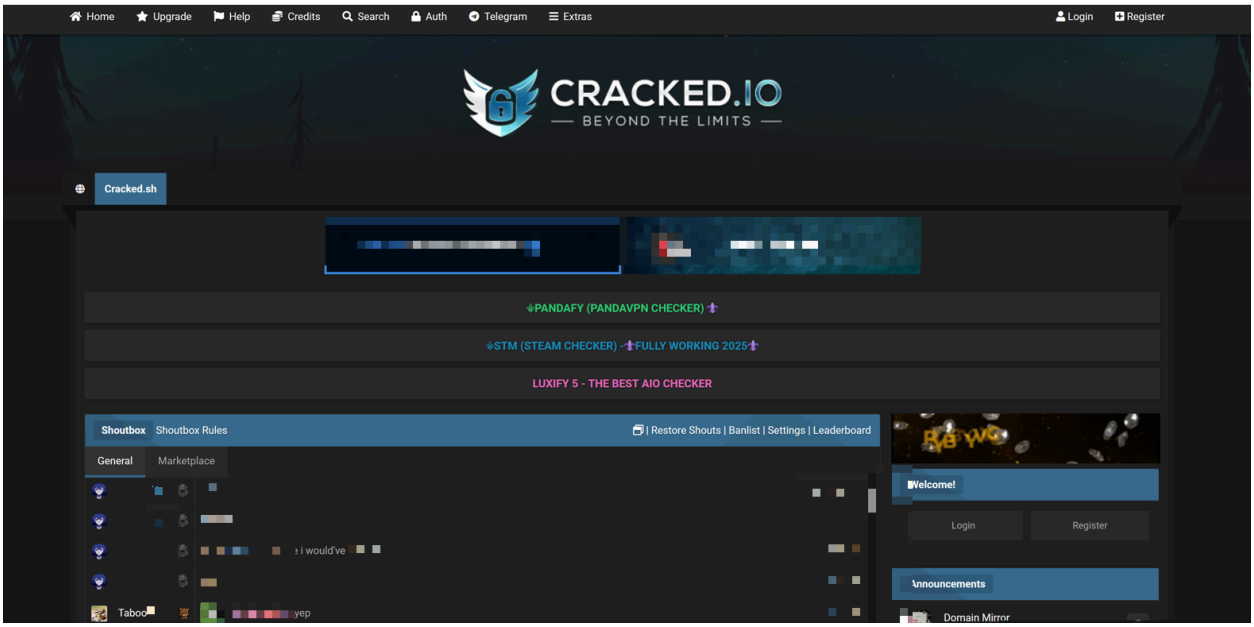
DarkForums hacker forums' home page

Following the takedown of BreachForums, threat actors redistributed across multiple underground platforms. One such platform was DarkForums, which emerged in 2023 after the shutdown of BreachForums operated by pompompurin. The forum gained increased traction in 2025, particularly after the disappearance of BreachForums in April.

DarkForums function as a typical Dark Web forum, facilitating the exchange of leaked databases, stealer logs, combo lists, leads, malware, account checkers, and compromised accounts. It also includes dedicated sections for premium content and sales.

The platform implements a tiered membership structure similar to BreachForums, with paid roles such as VIP, MVP, and GOD. Higher-tier members are granted access to restricted Telegram channels, including exclusive data leak feeds not available to standard users.

Cracked



Cracked forum

Cracked was an English-language cybercrime forum operating on the surface web, known for its large and active user base. The platform hosted discussions on combo lists, compromised credentials, stealer logs, hacking tools, and software vulnerabilities. It also included multiple language-specific subforums, with the French section identified as one of the most active.

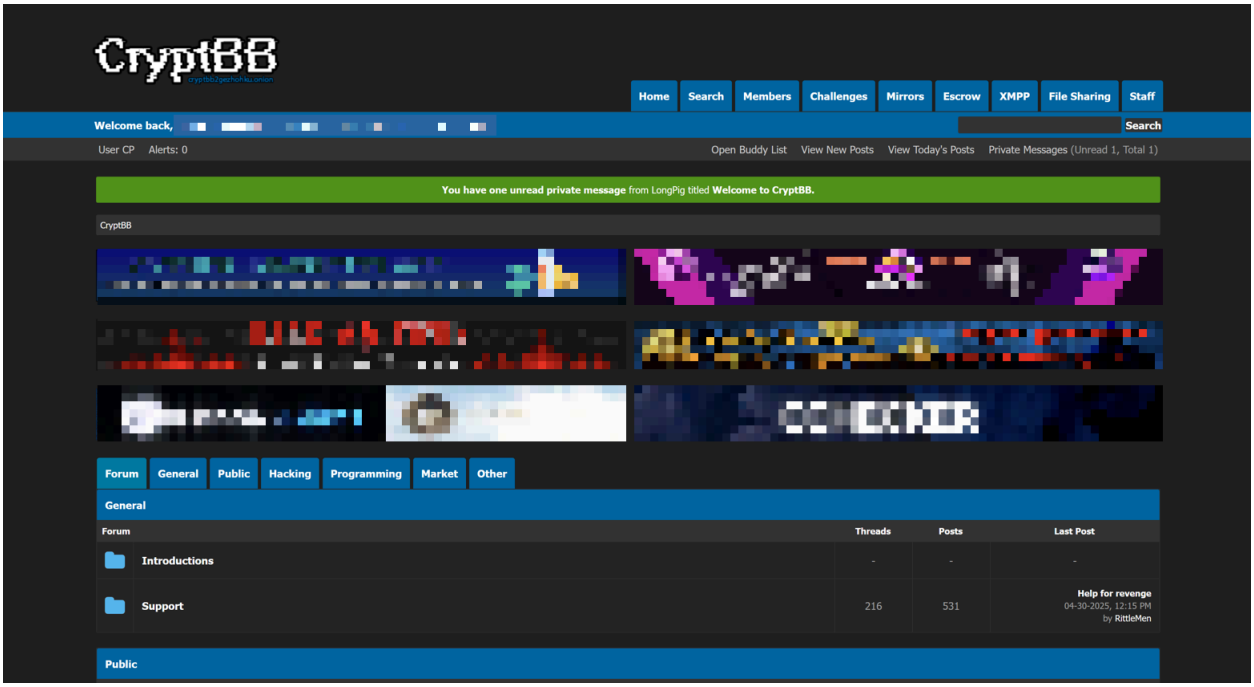
On 29 January 2025, Cracked.io was targeted as part of Operation Talent, a coordinated law enforcement effort led by the FBI with international partners. The operation resulted in the seizure of domains associated with both Cracked.io and Nulled.to, two major platforms involved in the distribution of stolen data, credential leaks, and illicit software.

Prior to the disruption, the two forums functioned as central hubs within the cybercrime ecosystem. They served both as discussion platforms and as marketplaces offering cybercrime-as-a-service, including stolen data, malware, and hacking tools. Investigators assessed that the involved actors generated approximately EUR 1 million in criminal profits.

Operational activity between 28 and 30 January led to the arrest of two suspects, the search of seven properties, and the seizure of 17 servers and more than 50 electronic devices. Authorities also confiscated approximately EUR 300,000 in cash and cryptocurrency.

Following the initial takedown, Cracked temporarily continued operations by migrating to a new domain, maintaining its role in the underground ecosystem until subsequent enforcement actions disrupted its presence.

CryptBB



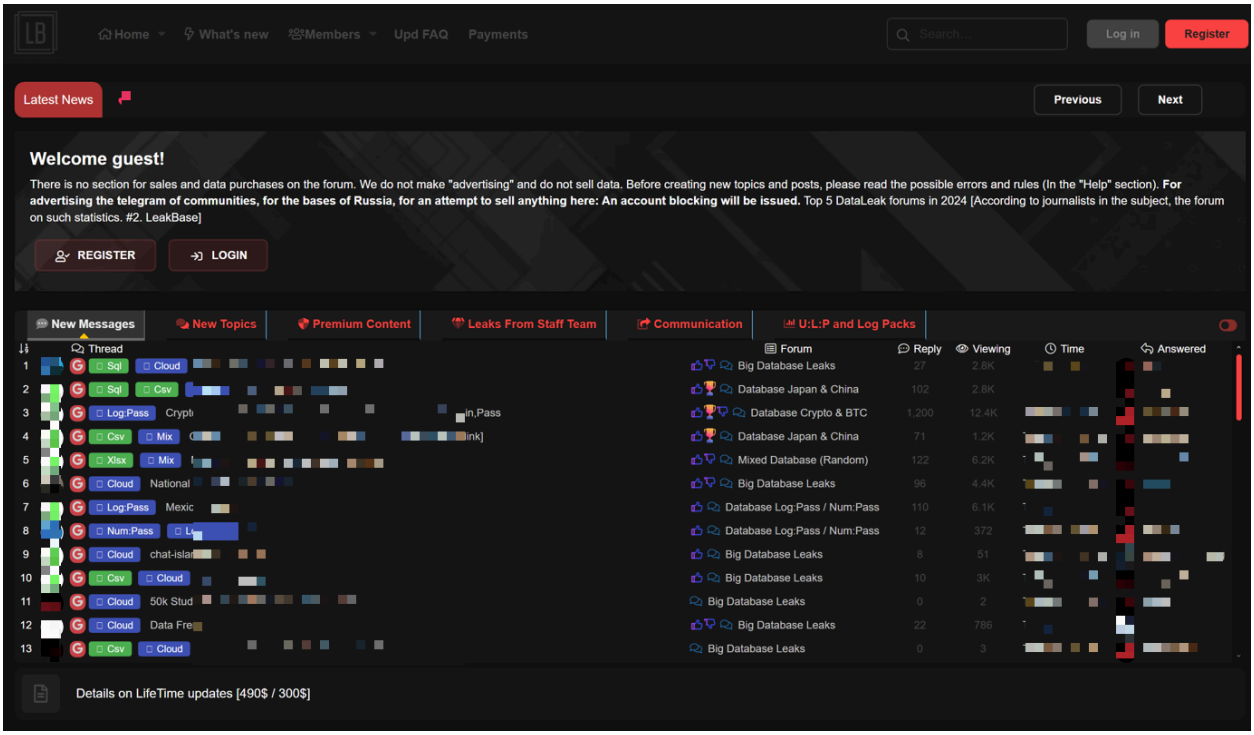
Mainpage of CryptBB

CryptBB is a Tor-based forum that has maintained a consistent but low-visibility presence on the Dark Web since 2017. It was initially established by actors known as LongPig and Power and gained recognition for its strong operational security practices and strict user vetting, including interview-based onboarding. While registration has become more accessible over time, the community remains selective.

The forum focuses on cybercrime, offensive security, and anonymity. It serves as a controlled environment for the exchange of stealer logs, malware tooling, and exploitation techniques. Its minimal interface and emphasis on user-managed privacy settings differentiate it from larger, more exposed platforms.

CryptBB follows a limited exposure model, avoiding large-scale recruitment and public visibility. Access to the platform is typically distributed through trusted networks or invite-based channels, reinforcing its appeal among experienced and security-conscious threat actors.

LeakBase



Main Page of LeakBase

LeakBase was a prominent Dark Web forum with a strong focus on data leaks and stealer logs. It maintained a large and regularly updated archive of compromised databases, including both historical breaches and newly exposed data.

The platform was accessible via the surface web and operated in English. It functioned as both a marketplace and a discussion forum where threat actors exchanged compromised information. A significant volume of stealer log data was hosted on the platform, including credential pairs, combo lists, and other forms of access data. The forum had a credit-based economy and featured structured sections covering malware, vulnerabilities, legal tools, and leak-related content. This structure supported a reputation-driven and active user base. The forum also enforced a ban on Russia-related data, likely to reduce geopolitical risk.

On 3 March, law enforcement agencies conducted coordinated international operations involving arrests, property searches, and knock-and-talk interventions. Approximately 100 enforcement actions targeted 37 high-activity users.

On 4 March, authorities advanced to the technical disruption phase by seizing the forum's domain and replacing it with an official notice.

Following the takedown, the forum migrated to a .bz domain. This domain was later seized by the cybercrime unit of Russia's Ministry of Internal Affairs (BSTM).

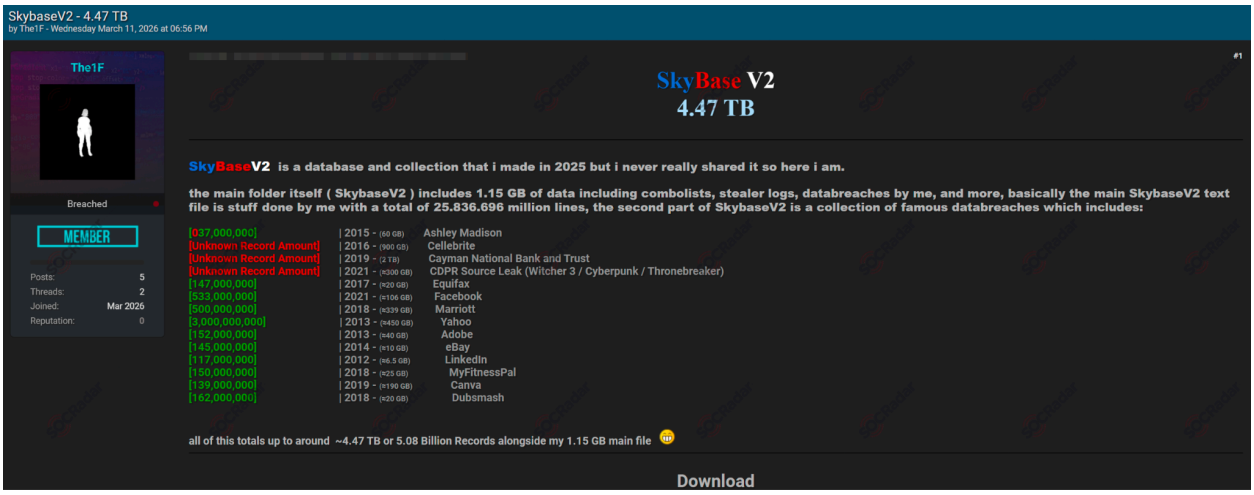
Dark Web Findings

This section presents selected findings from Dark Web forums monitored by SOCRadar. The examples included here represent a small subset of a much larger ecosystem. Similar services, datasets, and tools are continuously shared, updated, and commercialized across multiple platforms.

The volume and accessibility of stealer logs, credential databases, and ready-to-use tooling indicate a mature and scalable underground economy.

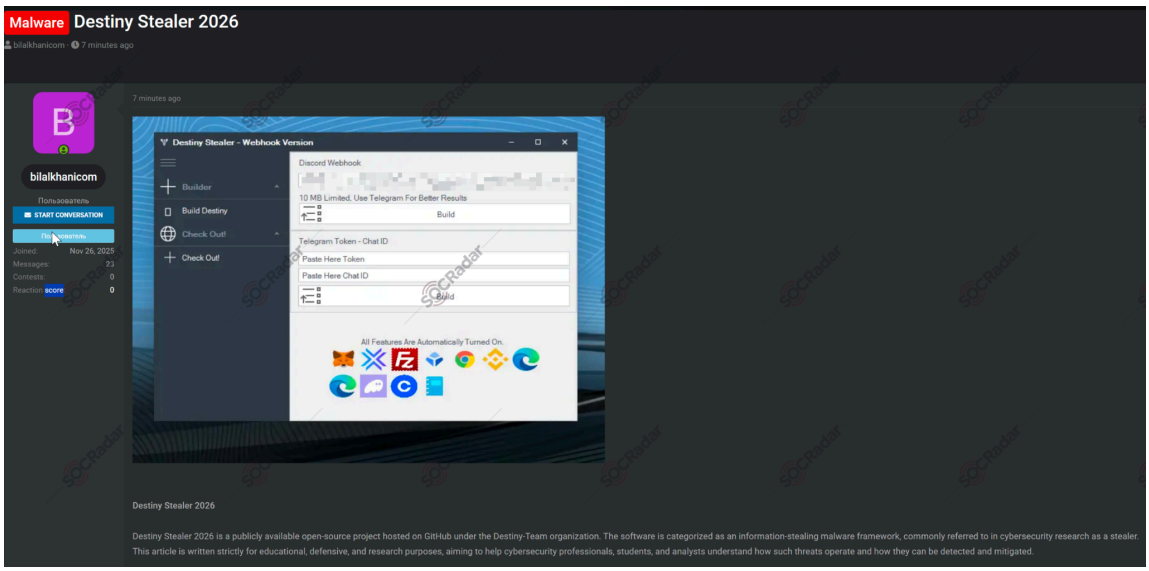
These observations highlight a key risk. Organizations should assume that compromised identities will be exploited over time and adopt controls that reduce reliance on static credentials since those exposed credentials and personal data can circulate for long periods and be reused across campaigns.

Large Aggregated Breach Dataset Advertised on Dark Web Forum



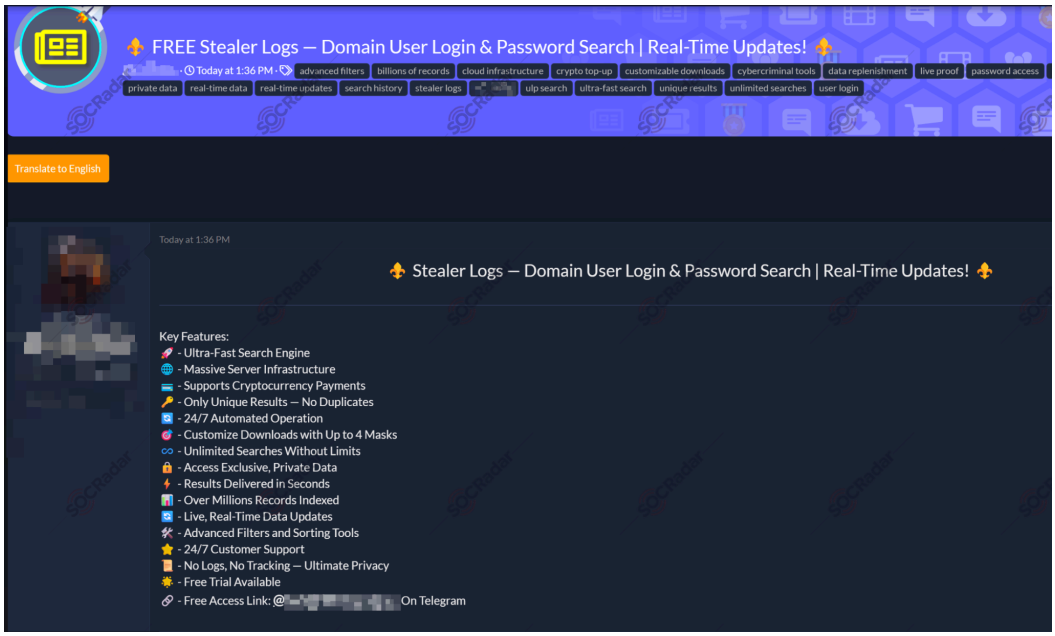
A threat actor advertised a large database collection named “SkyBase V2” on a Dark Web forum monitored by SOCRadar. The dataset is claimed to reach 4.47 TB and includes combolists, stealer logs, and aggregated data from multiple historic breaches. The actor states the collection contains over 5 billion records, combining older breach data with newly compiled credential sets.

“Destiny Stealer 2026” Tool Shared on Dark Web Forum



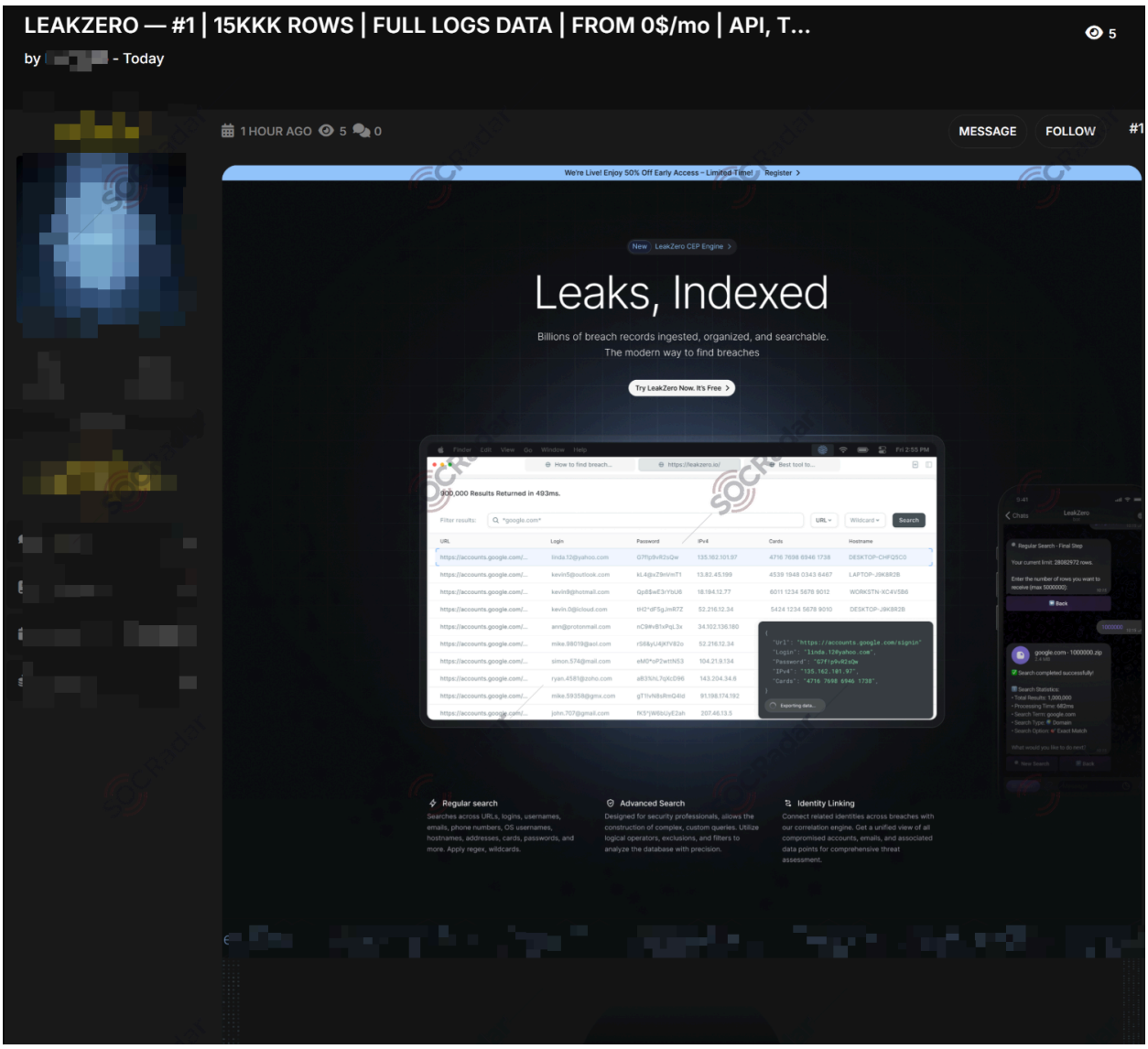
A stealer tool named “Destiny Stealer 2026” has been shared on a Dark Web forum monitored by SOCRadar. The tool is described as an information-stealing malware framework capable of extracting browser credentials, cookies, session data, and system information. Its modular structure and data collection features indicate ongoing development in commodity infostealer tooling, reinforcing the risk of scalable credential theft and account compromise.

Stealer Log Search Service Promoted on Dark Web Forum



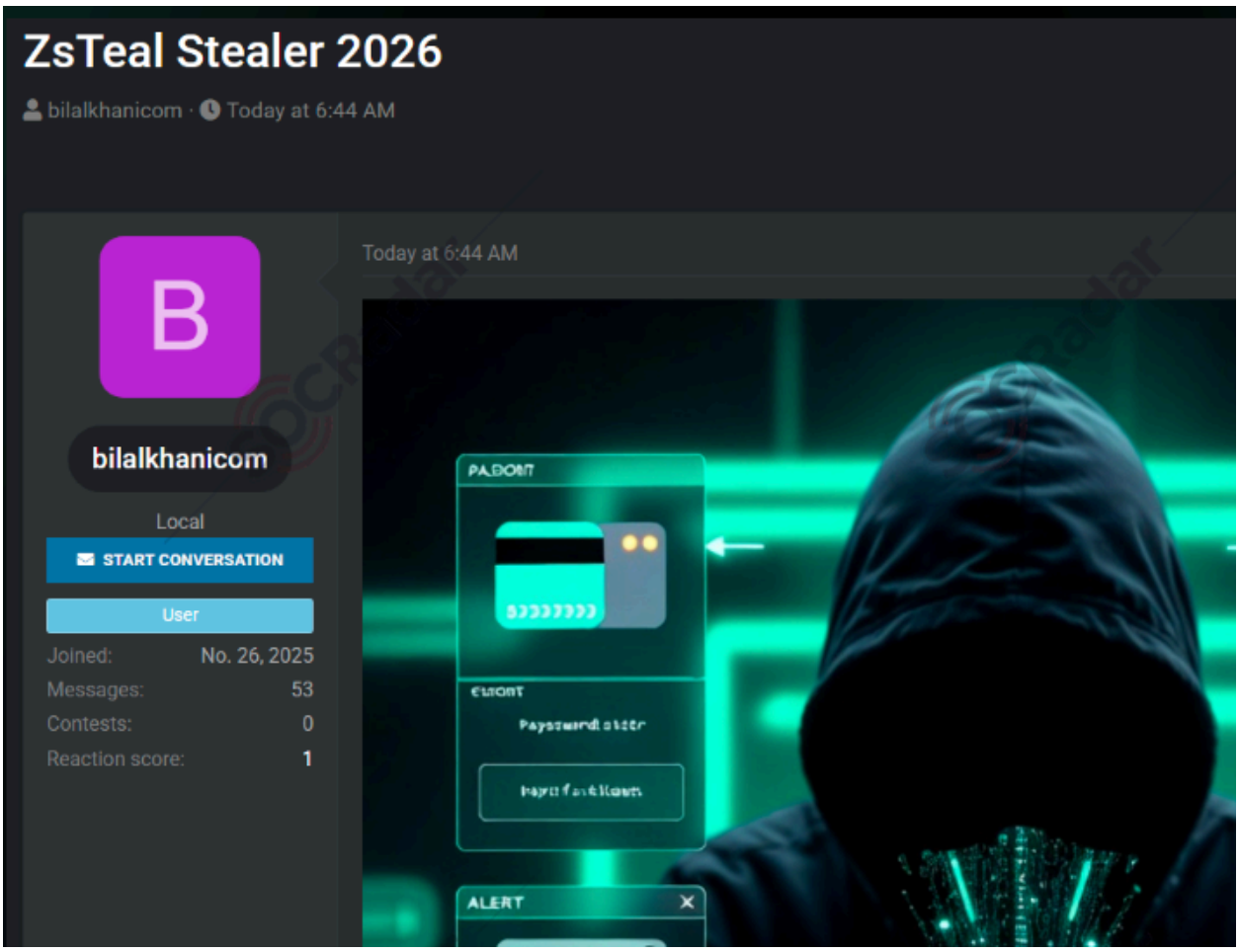
A new stealer log search service has been identified on a Dark Web forum monitored by SOCRadar. The platform claims to provide real-time access to millions of indexed credentials through a fast search engine. It supports cryptocurrency payments and offers advanced filtering, unlimited queries, and automated updates. The service is promoted with privacy-focused features and a free trial.

“LeakZero” Stealer Log Service Advertised on Dark Web Forum



A new stealer log service named “LeakZero” has been promoted on a Dark Web forum monitored by SOCRadar. The platform claims to provide access to over 15 billion records and positions itself as a professional solution for breach data analysis. It advertises low-cost access plans, including a free tier, along with supporting documentation and customer support.

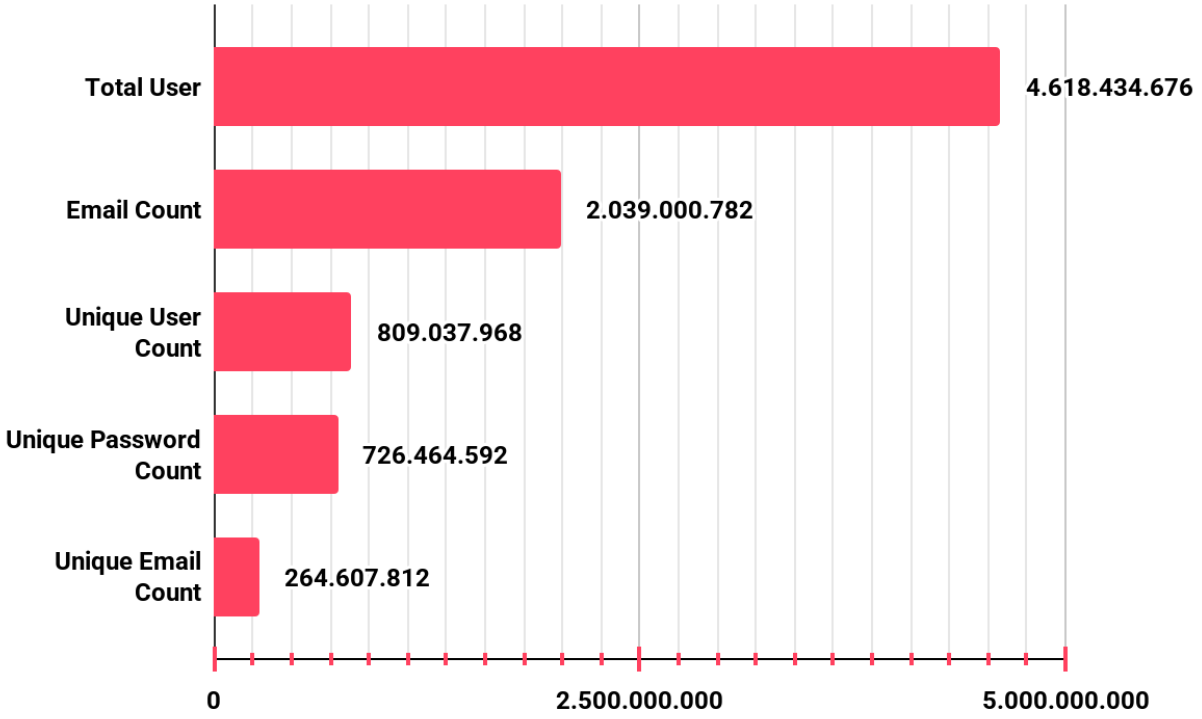
“ZsTeal Stealer 2026” Tool Shared on Dark Web Forum



A new infostealer tool named “ZsTeal Stealer 2026” has been shared on a Dark Web forum monitored by SOCRadar. The malware targets browser credentials, cryptocurrency wallets, gaming accounts, and communication platforms. It also collects system information and uses evasion techniques such as sandbox detection.

Stealer Log Trends

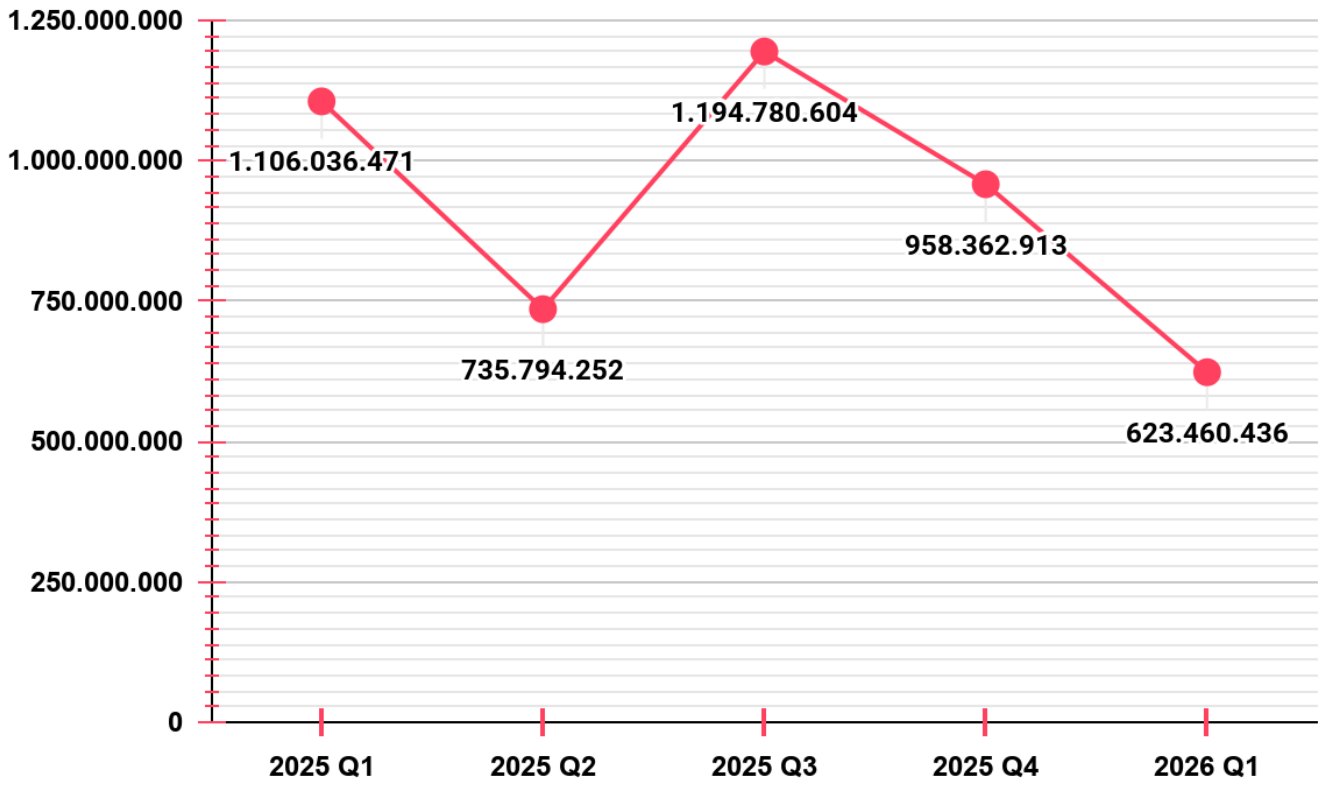
General Patterns in Stealer Log Data



The dataset shows a very large exposure surface, with over 4.6 billion total records. However, the number of unique users is around 809 million, which shows that the dataset includes similar emails and usernames from various services. When a stealer malware collects data, they collect everything they are designed to. That's why credential reuse is one of the most fundamental mistakes.

Email count exceeds 2 billion, while unique emails remain limited to 264 million. A similar pattern appears in passwords. There are 726 million unique passwords, which is relatively close to the number of unique users. This may indicate password reuse across different accounts or limited password diversity.

Quarterly Distribution of Stealer Log Activity

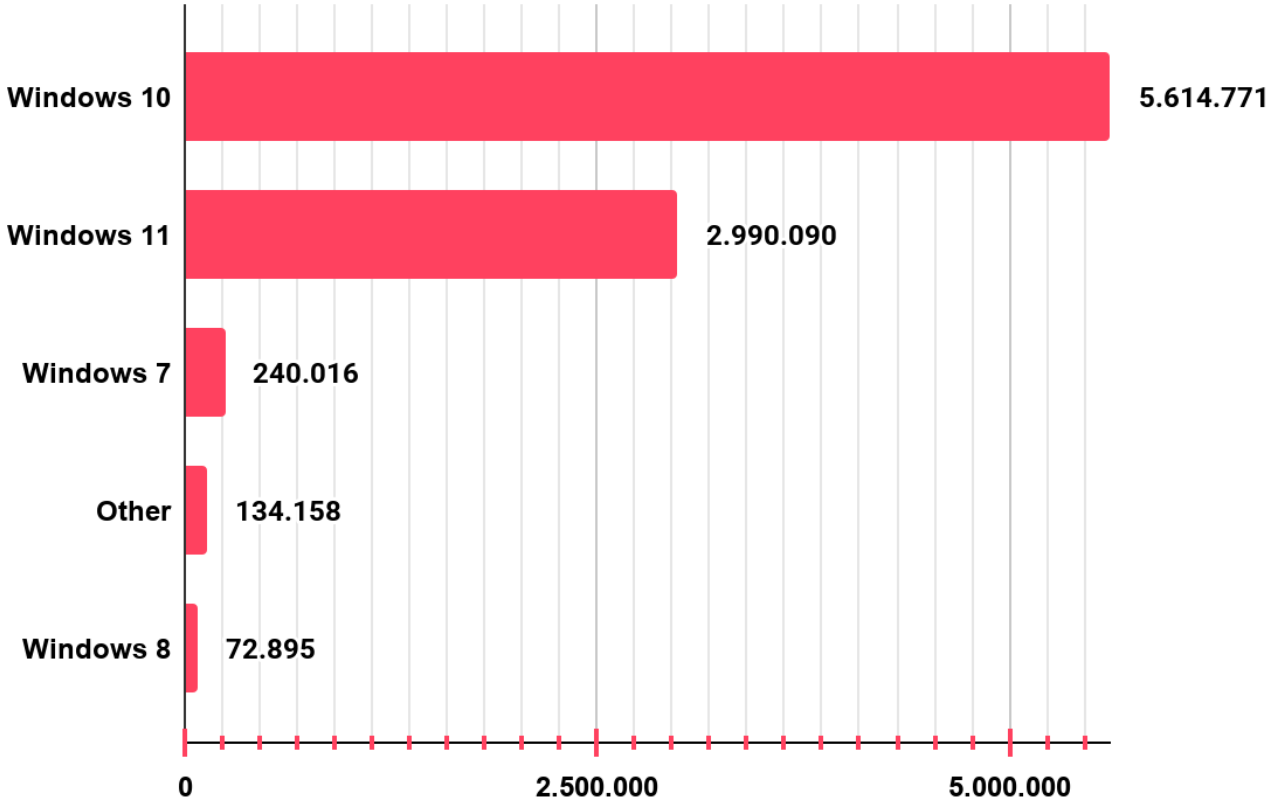


The data shows fluctuating activity across quarters, with clear peaks and declines. 2025 Q3 stands out as the highest point, exceeding 1.19 billion records. This suggests a period of intensified stealer campaigns or increased distribution efficiency. 2025 Q1 also shows elevated activity, while Q2 drops significantly. This decline may indicate temporary disruption in operations or reduced infection spread.

Activity rises again in Q4, though it does not reach Q3 levels. This pattern suggests that threat actors can quickly recover after slow periods with new campaigns. The decline observed in 2026 Q1 reflects partial data coverage rather than a decrease in activity, as the dataset only includes the period up to the time the report was prepared.

Overall, the distribution does not follow a stable trend. Instead, it reflects campaign-driven behavior.

Operating System Exposure



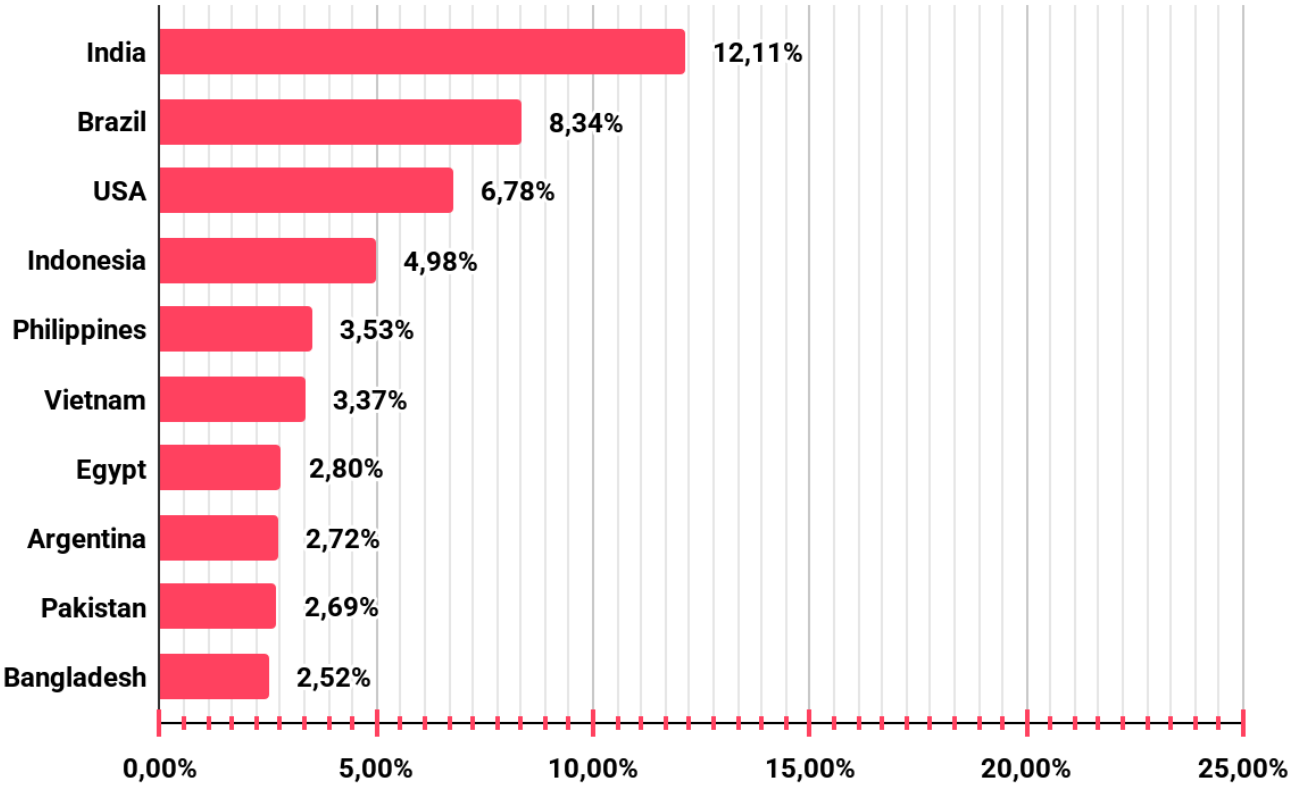
The distribution shows a strong concentration on modern Windows systems. Windows 10 leads with more than 5.6 million records, followed by Windows 11 with close to 3 million. This indicates that most infections occur on actively used and supported systems. Attackers are not limited to outdated environments. They successfully target current user bases.

Legacy systems such as Windows 7 and Windows 8 appear with much lower volumes. Their presence still matters, but they are not the main driver of exposure. The “Other” category remains minimal, which suggests limited activity outside the Windows ecosystem.

The gap between Windows 10 and Windows 11 is notable. Windows 10 still holds a larger share, likely due to its broader global adoption. This makes it a primary target for stealer operators.

Overall, the data confirms that identity theft risks are centered on mainstream Windows platforms, where user density and credential value are highest.

Geographic Concentration of Stealer Log Infections



The distribution shows a clear concentration in emerging and high-population regions. India leads with over 12 percent, followed by Brazil and the United States. This indicates that both population size and digital adoption play a role in exposure. Large user bases increase the probability of infection at scale.

Southeast Asia is strongly represented. Indonesia, the Philippines, and Vietnam together form a significant share. This suggests active targeting or widespread infection vectors in these regions. Similar patterns appear in South Asia, with Pakistan and Bangladesh contributing notable volumes.

The presence of the United States within the top three is important. It shows that high-value targets are still heavily affected, even if their percentage share is lower than more populous countries.

Overall, the data points to a mix of scale-driven exposure and opportunistic targeting. Regions with large and growing internet populations appear more frequently, but developed markets remain critical due to the higher value of stolen credentials.

Defensive Strategies

Understanding how identity-based attacks work is only half of the picture. The other half is building the right defenses.

Identity Attack Vectors

Phishing and Social Engineering

Phishing remains a leading initial access method. Attackers use emails, messages, or calls to trick users into entering credentials on fake login pages or approving fraudulent MFA requests. Techniques such as business email compromise (BEC), adversary-in-the-middle phishing kits, and MFA fatigue attacks increase the success rate even in environments with MFA.

Defense requires layered controls. Organizations should enforce SPF, DKIM, and DMARC, deploy phishing-resistant MFA such as FIDO2 passkeys or hardware security keys, and run regular phishing simulations. Service desks also need strict identity verification procedures before performing account resets.

Infostealer Malware

Infostealer malware collects credentials, session cookies, browser passwords, and cryptocurrency wallets from infected endpoints. Families such as RedLine, Raccoon, Lumma, and Vidar are widely distributed examples. Once deployed, they exfiltrate data within seconds and logs are quickly sold on dark web markets.

Organizations should deploy EDR tools that detect suspicious access to browser credential stores or unusual processes. Enterprise browser policies should disable local password storage and require password managers. Employees should avoid installing untrusted software and using personal devices for corporate access.

Credential Stuffing

Credential stuffing uses large datasets of leaked usernames and passwords from previous breaches. Automated tools test these combinations across many services. Because users often reuse passwords, attackers can gain valid access without phishing or cracking credentials.

Defense focuses on eliminating password reuse. Organizations should enforce unique passwords and provide password managers. Additional controls include CAPTCHA, rate limiting, and anomaly-based login detection. Monitoring for logins from unusual devices or locations can help detect compromised accounts quickly.

Session Hijacking and Cookie Theft

Web applications use session cookies to maintain authenticated sessions. If an attacker steals a cookie, they can impersonate the user without needing credentials or MFA. Infostealer malware commonly collects these cookies, and they may remain valid for hours or days.

Applications should enforce Secure and HttpOnly cookie attributes and limit session lifetimes. Sensitive actions should require re-authentication. Device binding and continuous session monitoring can reduce the usability of stolen cookies and detect suspicious activity.

Token Theft and OAuth Abuse

Cloud services rely on authentication tokens such as OAuth access tokens, refresh tokens, and JWTs. If attackers obtain these tokens, they can access services without triggering standard login alerts. OAuth consent phishing is a common technique where users unknowingly grant access to malicious applications.

Organizations should restrict OAuth permissions to approved applications and prevent users from granting consent to unknown apps. Conditional access policies should evaluate token usage context, including device and location. Unusual token activity should trigger additional authentication or token revocation.

Defensive Controls

Identity Threat Intelligence and Dark Web Monitoring

Threat intelligence specifically focused on identity gives organizations early warning of credential exposure. Stealer log markets, paste sites, breach databases, and criminal forums are monitored by CTI teams and commercial platforms to detect when corporate credentials, session tokens, or employee data appear for sale or free distribution. Organizations with large workforces need automated systems that continuously check whether employee credentials appear in known breach datasets or stealer logs.

Multi-Factor Authentication: Deployment and Uplift

MFA remains one of the highest-impact controls for reducing account takeover risk. However, not all MFA is equal. SMS-based one-time passcodes (OTPs) are vulnerable to SIM swapping and real-time phishing interception. Authenticator app-based OTPs are stronger but still susceptible to AiTM attacks. Phishing-resistant MFA, specifically FIDO2 hardware security keys and passkeys, is the gold standard because authentication is cryptographically bound to the legitimate origin.

Session Security and Cookie Management

Session security is frequently overlooked relative to authentication security, but it is equally important. A stolen session bypasses authentication entirely. Organizations should establish clear policies for session lifetime, requiring re-authentication for sensitive operations and automatically terminating sessions after inactivity periods.

Privileged Access Management and Least Privilege

Privileged accounts are high-value targets. If an administrator's credentials are compromised, the blast radius is far greater than for a standard user account. Privileged access management (PAM) solutions enforce the principle of least privilege by granting elevated permissions only when needed and only for specific tasks, through time-limited, audited sessions.

Infostealer Detection and Post-Infection Remediation

Detecting an infostealer infection quickly is important, but the work does not stop at remediation of the endpoint. Even after malware is removed, any credentials or session tokens present on the device during infection must be considered compromised. All passwords accessible from the infected device should be reset, all active sessions invalidated, and any OAuth tokens revoked.

Identity Security Awareness

Technology controls alone are not sufficient. Human factors remain a significant vulnerability. Employees need regular, practical training on how phishing attacks work, what MFA fatigue attacks look like, and why they should never approve an unexpected authentication request. Training should be scenario-based and updated as attack techniques evolve.

Future Outlook: Identity Threats in 2026 and Beyond

The identity threat landscape continues to shift. Attack techniques are becoming more automated, more sophisticated, and harder to detect with conventional controls. At the same time, new technologies are expanding the attack surface in ways that many organizations are not yet prepared to address.

AI-Powered Phishing and Social Engineering at Scale

Generative AI has dramatically lowered the cost and effort required to produce convincing phishing content. Attackers can now generate highly personalized, grammatically correct phishing emails at scale, using publicly available information from LinkedIn, company websites, and social media. AI voice cloning is already being used in vishing attacks to impersonate executives and request urgent wire transfers or credential disclosures.

Deepfake video technology is advancing rapidly and is expected to be used more broadly in identity fraud, particularly in remote identity verification scenarios such as onboarding, account recovery, and KYC processes. Organizations that rely on video-based verification should begin evaluating deepfake detection tools. More broadly, the assumption that human-reviewed content is inherently trustworthy is becoming less safe to rely on.

Machine Identity Explosion

The growth of cloud-native architectures, microservices, and automation has led to a dramatic increase in the number of non-human identities in enterprise environments. Service accounts, API keys, CI/CD pipeline tokens, and cloud role assignments now vastly outnumber human user accounts in many organizations, yet they often receive far less governance attention.

These machine identities are attractive targets because they frequently have broad permissions and are not subject to the same MFA controls as human users. Where API keys and tokens are embedded in code repositories, configuration files, or build logs, is a systemic problem. Organizations should invest in solutions that address this problem. Implementing automated scanning for exposed credentials in code repositories, and establishing lifecycle management policies for all non-human identities can decrease the risks associated with this vector. This area of identity security is expected to receive increasing regulatory and vendor attention through 2026 and beyond, as AI-supported development becomes more common and leads to rapid growth in machine identities.

Identity-First Security Architecture

This approach means that access decisions are made based on who the user is, the health and trust level of their device, the sensitivity of the resource being accessed, and the context of the request, rather than whether the request comes from inside or outside a corporate network. Zero trust architecture principles formalize this model. Adoption of identity-first security requires investment in strong identity governance, continuous authentication, and contextual access policy enforcement. Organizations that do not make this shift remain exposed to attacks that exploit trust within their environments.

Passwordless Authentication and Passkey Adoption

Password-based authentication is increasingly recognized as a structural weakness. Passwords are stolen through phishing, credential stuffing, and malware, and they place a significant burden on users and helpdesks alike.

Major platform vendors including Apple, Google, and Microsoft have integrated passkey support, and consumer adoption is growing.

Enterprise adoption is following, though at a slower pace due to integration complexity and dependencies. By 2026, passwordless authentication is expected to become the standard for new application deployments, and organizations that have not begun their transition will face increasing pressure from both security and usability perspectives.

CTI teams should monitor for attacker techniques designed to circumvent passkey adoption, as adversaries will adapt their methods in response.

Who is SOCRadar?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in 150+ countries

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.