



2026 Quarterly Breach Report

Identity Risk in the Second Quarter



ATTACKERS ALREADY HAVE THE DATA: Why External Identity Exposure Demands Action

Most organizations have invested heavily in understanding what is happening inside their environments. They monitor networks, endpoints, identities, applications, and access attempts. Yet many of the signals that shape the next attack are already circulating beyond their control.

Exposed credentials, personal information, online identities, device information, and service data give cybercriminals a detailed view of employees, customers, and organizations. This information can be combined, enriched, and reused to support account takeover, impersonation, fraud, phishing, and other forms of social engineering.

Our Q2 2026 findings illustrate the scale of this external exposure. During the quarter, Constella identified more than 670,000 potential breaches containing more than 447 billion records across surface, deep, and dark web sources. After verification, deduplication, and quality review, more than 4,000 breaches containing 10.82 billion records and 57.64 billion attributes were ingested into the Constella Data Lake.

The identity signal within that data also became stronger. Email addresses appeared in 51.07% of curated Hacked Leaked and Combo records, while plaintext passwords appeared in 50.90%. These records do not exist in isolation. When credentials are connected with names, phone numbers, addresses, social identifiers, devices, and online services, attackers gain the context needed to create more convincing and targeted attacks.

Infostealer intelligence makes this challenge even more urgent. Constella registered 5.53 million devices with Q2 infection dates, nearly twice the Q1 total. The data recovered from infostealer activity shows how credentials can be connected with URLs, usernames, email addresses, and device identifiers. This gives attackers information about not only who a person is, but also which services and accounts may matter to them.

Organizations cannot protect what they cannot see. Identity risk management must extend beyond internal systems to include the data already exposed and available to adversaries.

Constella provides that external visibility. By connecting and validating fragmented identity data, we help organizations understand what attackers may already know, investigate the associated risk, and act before the information is weaponized against their employees, customers, or business.

Andres Andreu
CEO, Constella



HOW TO READ THIS REPORT

Understanding Constella's Data

This report analyzes breach and infostealer intelligence collected and processed by Constella Intelligence during Q2 2026, with comparisons to Q1 2026.

1

HUNTED DATA

Raw threat intelligence identified through automated scanning, intelligence partnerships, Telegram channels, and monitoring across surface, deep, and dark web sources. These findings have not yet been deduplicated or fully validated.

2

VERIFIED AND DEDUPLICATED

Collected data is curated, validated, and filtered to remove duplicate, recycled, and previously observed records.

3

INGESTED DATA

Verified intelligence is inserted into the Constella Data Lake after completing quality review and validation.

DATA LAKE TOTALS

Cumulative holdings at the close of the quarter. These totals should not be confused with the records processed during Q2 alone.

Executive Brief

WHAT IDENTITY EXPOSURE REVEALS

Most security tools help organizations monitor activity inside their environments. Constella provides visibility into exposed data already circulating outside those environments, including credentials, personal information, online identities, devices, and online services that attackers may use to plan their next move.

72.95B

records in the Data Lake
up 14.07% from Q1

51.07%

curated records with an email
address

5.53M

devices with Q2 infection dates
nearly twice the Q1 total

In Q2 2026, the volume and identity value of Constella's verified breach intelligence increased. The Data Lake closed the quarter with 72.95 billion records, up 14.07% from Q1, and ingested 10.82 billion verified records during the quarter.

The identity signal became stronger.

More than half of curated Hacked Leaked and Combo records contained an email address, up 11.19 percentage points from Q1. Plaintext passwords appeared in 50.90% of curated records, increasing the volume of credentials that can be immediately used for credential stuffing and account takeover.

Infostealer visibility also widened.

Constella registered 5.53 million devices with Q2 infection dates, nearly twice the Q1 total.

EXECUTIVE TAKEAWAY

Organizations cannot assess identity risk through incident counts alone. They need verified, deduplicated intelligence that connects exposed credentials, personal data, devices, online identities, and services so teams can understand what attackers may already know and act before the information is reused.

Collection and Verification Funnel

Constella expanded both its collection reach and verified intelligence in Q2 2026. The Data Lake closed the quarter with 1.43 million breaches, 72.95 billion records, and 544.16 billion attributes. These are cumulative totals across all breach data in the Data Lake, not Q2 additions alone.

CUMULATIVE BREACHES 1.43M up 1.48% from Q1	CUMULATIVE RECORDS 72.95B up 14.07% from Q1	CUMULATIVE ATTRIBUTES 544.16B up 11.85% from Q1
--	---	---

FROM COLLECTION TO VERIFIED INTELLIGENCE

Hunted data represents raw threat intelligence identified through automated scanning, intelligence partnerships, and monitoring across the surface, deep, and dark web. Ingested data is the verified, deduplicated subset that remains after curation, validation, and quality filtering.

The collection funnel expanded significantly while Constella continued applying its verification and quality standards.

	Hunted Data	Verified and Deduplicated	Ingested Data
Metric	Q1 2026	Q2 2026	Change
Breaches hunted	more than 229,000	more than 670,000	+192.73%
Records hunted	113.15B	447.27B	+295.31%
Breaches ingested	more than 3,600	more than 4,000	+10.12%
Records ingested	9.73B	10.82B	+11.18%
Attributes ingested	56.54B	57.64B	+1.96%

The hunted to ingested breach ratio widened from approximately 62 to 1 in Q1 to 166 to 1 in Q2. This reflects a broader collection funnel combined with consistent verification, deduplication, and quality standards.

What Q2 Breach Sources Reveal

Constella's verified breach intelligence comes from three distinct source types. Hacked Leaked breaches provide rich identity information from direct compromises. Combo breaches aggregate previously exposed credential pairs, while URL Logs connect stolen credentials with infected devices and online services.

HACKED LEAKED

~3,000

73.80% of Q2 ingested breaches

up 12.76% in breach count from Q1

PII WITHIN HACKED LEAKED

~2,850

95.13% of Hacked Leaked breaches

up 12.21% in breach count from Q1

COMBO BREACHES

~270

6.63% of Q2 ingested breaches

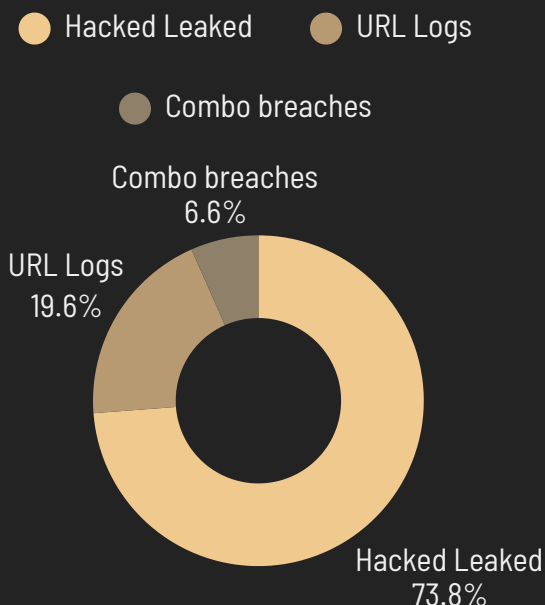
down 8.19% in breach count from Q1

URL LOGS

~790

19.57% of Q2 ingested breaches

up 7.88% in breach count from Q1



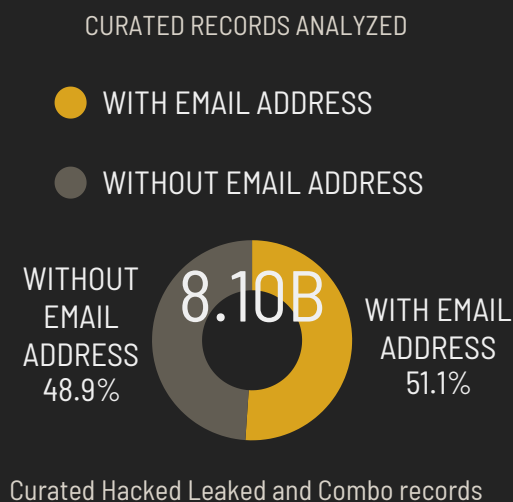
PII remains central to the exposure

More than 95% of Q2 Hacked Leaked breaches contained personal information beyond credentials. Names, phone numbers, addresses, identifiers, and financial information give attackers the context needed to support impersonation, fraud, phishing, and targeted social engineering.

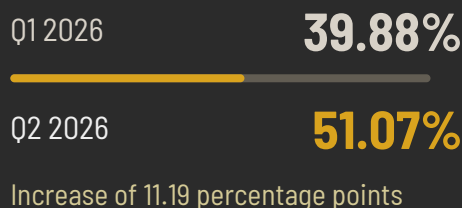
Although the number of Combo breaches declined, their record volume increased 250.22% in records. This indicates that credential compilations are becoming larger, not that detection coverage has decreased.

Email Addresses Strengthen the Identity Signal

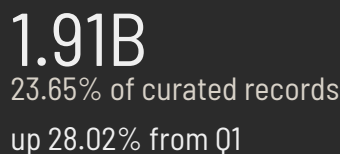
Email addresses are a primary connection point between exposed credentials, personal information, online accounts, and organizations. In Q2, email addresses appeared in 51.07% of curated Hacked Leaked and Combo records, up 11.19 percentage points from Q1. This strengthens the ability to connect fragmented exposure and understand how attackers may reuse it.



EMAIL ADDRESS PRESENCE



UNIQUE EMAIL ADDRESSES



RECORDS WITH EMAIL ADDRESS

51.07%

4.13B

up 34.43% from Q1

RECORDS WITHOUT EMAIL ADDRESS

48.93%

3.96B

down 14.57% from Q1

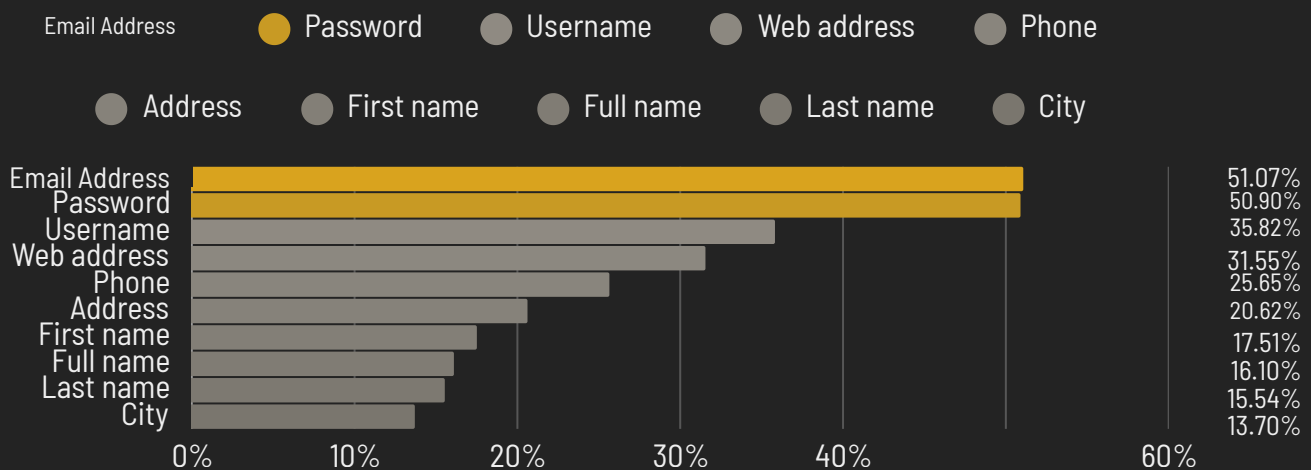
Email addresses connect the exposure.

An email address does more than identify an account. It can connect exposed passwords, names, phone numbers, addresses, devices, and online services, giving attackers the context needed to target individuals and organizations more effectively.

Exposed Data Builds a More Complete Identity

Credentials remain prominent, but Q2 exposure extended well beyond usernames and passwords. Names, phone numbers, addresses, locations, and other personal information provide additional context that attackers can use to identify targets, impersonate individuals, and create more convincing attacks.

Percentages are based on 8.10 billion curated Hacked Leaked and Combo records.



NOTABLE QUARTERLY CHANGES IN PERCENTAGE POINTS

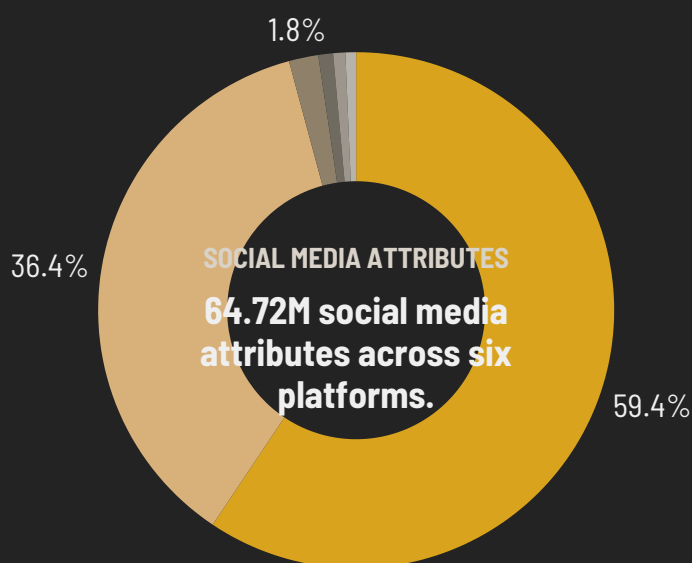
Email Address +11.19 points | Password +8.61 points | Phone down 20.14 points | Full name down 11.41 points

Credentials are only part of the exposure

Credentials are only one part of the exposure. Names, phone numbers, addresses, web activity, and other personal information provide additional context that can make exposed identities more useful for impersonation, fraud, phishing, and targeted social engineering.

Social Identifiers Connect Digital Identities

Social media identifiers help connect usernames, aliases, phone numbers, and other exposed attributes across platforms. In Q2, Constella observed 64.72 million social media attributes across six tracked platforms. Telegram and Facebook accounted for 95.81% of that exposure, providing valuable context for identity resolution, investigation, phishing, and impersonation.



PLATFORM DISTRIBUTION

● Telegram	38,431,801	59.39%
● Facebook	23,568,362	36.42%
● Instagram	1,193,257	1.84%
● LinkedIn	597,728	0.92%
● Twitter	492,147	0.76%
● Skype	431,897	0.67%

Telegram remains the leading social identity signal

Telegram represented 59.39% of Q2 social media exposure. When Telegram profiles are connected with phone numbers, usernames, names, and other identifiers, investigators can gain valuable context for resolving digital identities and understanding potential threat actor activity.

Percentages represent the composition of social media attributes observed in Constella's Q2 breach intelligence. They do not represent breaches of the platforms themselves.

INFOSTEALERS REVEAL MORE THAN PASSWORDS

Infostealers capture information directly from compromised devices, giving attackers visibility into credentials, online services, identities, and devices. The resulting data can reveal not only who a victim may be, but also which accounts and services may be valuable to target.

5.53M

DEVICES WITH Q2 INFECTION DATES

up 99.53% from Q1

14.13M

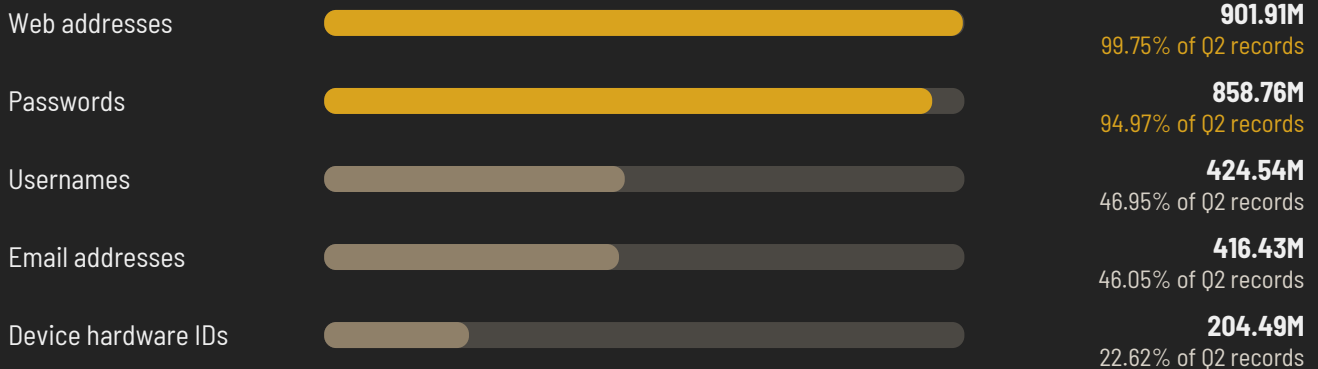
**INFOSTEALER PACKAGES
INSERTED**

904.21M

**INFOSTEALER RECORDS
INSERTED**

processed and deduplicated

WHAT INFOSTEALER RECORDS CONTAIN



ATTACKERS CAN SEE THE SERVICES THAT MATTER

Web addresses appeared in nearly every Q2 infostealer record, while passwords appeared in 94.97%. When URLs are connected with usernames, email addresses, and device identifiers, attackers gain a detailed view of which services a victim uses and where stolen access may be most valuable.

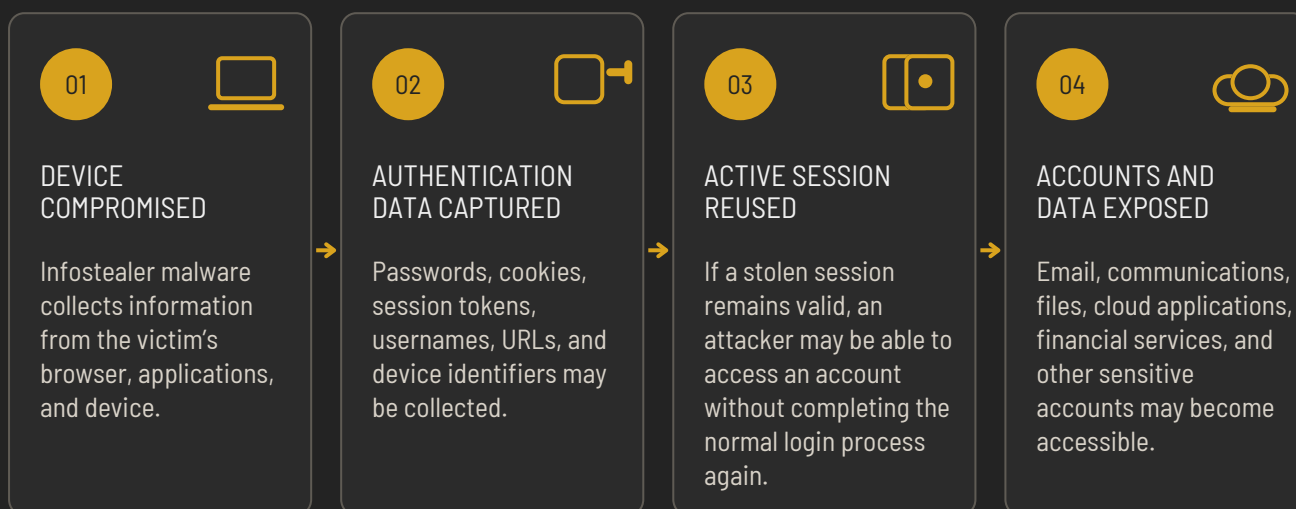
WHY THE TOTALS MOVED DIFFERENTLY

Device totals are organized by infection date. Package and record totals are organized by ingestion date, so the measures may move in different directions.

STOLEN SESSIONS CAN BYPASS THE LOGIN

Infostealers do not stop at passwords. They can also capture browser cookies, session tokens, browsing data, cached credentials, and device information. This gives attackers potential access to accounts and services that a victim has already authenticated.

FROM DEVICE INFECTION TO ACCOUNT ACCESS



Passwords | Cookies | Session Tokens | URLs | Usernames | Device IDs

WHY A VALID SESSION CAN BYPASS A NEW LOGIN.

Multifactor authentication helps protect the initial login. It may not prevent access when an attacker reuses a valid session that has already completed authentication. The risk depends on token validity, platform controls, and whether the compromised session is detected and revoked.

AI ACCOUNTS CREATE A NEW EXPOSURE POINT

As employees use AI services for work, compromised sessions could expose conversation history, prompts, uploaded files, corporate information, and connected applications. This makes visibility into infected devices and exposed sessions increasingly important.

SEE WHAT ATTACKERS MAY ALREADY POSSESS

Constella helps organizations identify exposed identity and infostealer data circulating outside their environments. By connecting people, devices, credentials, and online services, teams can investigate potential risk and act before stolen information is reused.

Note: The Q2 dataset does not quantify the prevalence of cookie theft, session-token exposure, authenticated session reuse, or AI account exposure. These examples illustrate potential risks associated with infostealer-compromised devices.

What the Largest Verified Q2 Breaches Reveal

The five largest verified Q2 breaches in Constella's dataset associated with a specific company or domain contained a combined 1.05 billion records. Generic country datasets and credential compilations are excluded so the ranking remains focused on attributable incidents.

1

USPS

Postal and logistics · United States

737.74M records

Largest verified Q2 breach in Constella's dataset associated with a specific company or domain.

2

Truecaller

Telecommunications and caller identification · India

123.48M records

3

addi.com

Financial services and buy now, pay later · Colombia

78.86M records

4

icfes.gov.co

Government and education · Colombia

55.48M records

5

zenbusiness.com

Business services · United States

54.82M records

Identity exposure crosses industries and borders

The largest Q2 incidents span postal services, telecommunications, financial services, government, education, and business services across three countries. This range demonstrates that exposed identity information is not limited to one industry or type of organization.

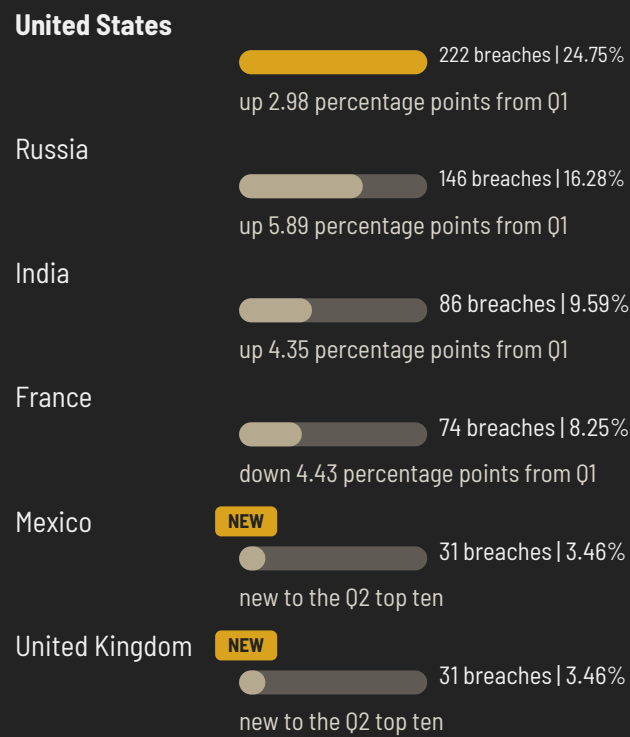
Executive takeaway

The size of a breach is only one measure of risk. Organizations must also understand which employees, customers, domains, and identity attributes appear within exposed data and how that information could be combined with other sources.

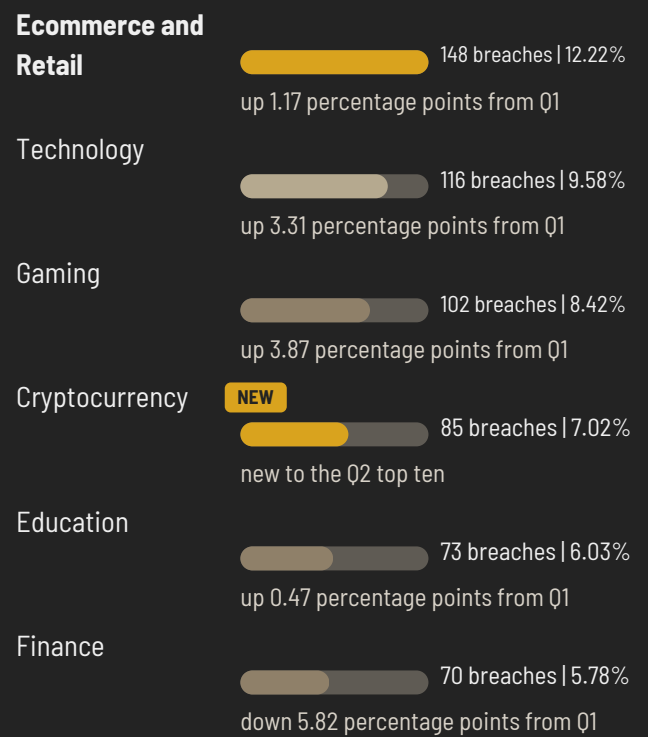
WHERE Q2 EXPOSURE WAS CONCENTRATED

Q2 Hacked Leaked breach intelligence shows that external identity exposure crosses both geographic and industry boundaries. The United States led geographically attributed breaches, while ecommerce and retail led industry-attributed breaches. Technology, gaming, and cryptocurrency also represented a growing share of attributed Q2 activity.

GEOGRAPHIC CONCENTRATION



INDUSTRY CONCENTRATION



EXPOSURE FOLLOWS IDENTITY RICH ECOSYSTEMS

The leading industries include consumer platforms, digital services, financial accounts, and institutions that maintain extensive identity and account information. Their presence reinforces the need to understand which employee and customer identities have already been exposed outside an organization’s environment.

Country percentages are based on approximately 900 Hacked Leaked breaches with geographic attribution. Industry percentages are based on approximately 1,200 Hacked Leaked breaches with sector attribution. Records without reliable attribution are excluded.

WHAT SECURITY TEAMS SHOULD DO NEXT

Start with external visibility. The question is no longer whether attackers possess exposed data. It is whether an organization can identify that exposure, understand how it connects to its people and systems, and act before it is weaponized.



01

CORRELATE EXPOSURE ACROSS IDENTITIES

Match employee, executive, and customer domains against verified breach data. Use email, username, phone, social profile, and device context to connect fragmented records and prioritize investigation.



02

TREAT PLAINTEXT CREDENTIALS AS IMMEDIATELY ACTIONABLE

Require password resets where current exposure is confirmed, check for reuse across applications, and monitor authentication activity for credential stuffing and anomalous access.



03

RESPOND TO INFOTEALERS BEYOND PASSWORD RESETS

Investigate the affected endpoint, rotate exposed credentials and secrets, examine the services connected with captured URLs, and review active sessions or other authentication artifacts when the available intelligence supports it.



04

STRENGTHEN AUTHENTICATION AND STORAGE

Prioritize phishing resistant multifactor authentication for executives and high value accounts. Review password storage practices and migrate weak or legacy hashing implementations to appropriately configured modern alternatives.



05

MONITOR EXTERNAL EXPOSURE CONTINUOUSLY

Quarterly reports show how the exposure landscape changes, but identity risk develops continuously. Integrate verified breach and infostealer intelligence into ongoing investigation and response workflows.

SEE WHAT ATTACKERS MAY ALREADY KNOW

Learn how Constella can help your team identify exposed identity data, investigate potential risk, and act before the information is reused.

METHODOLOGY AND LIMITATIONS

This report analyzes breach and infostealer intelligence collected and processed by Constella Intelligence during Q2 2026, with comparisons to Q1 2026.

1 COLLECTION

Constella collects intelligence from infostealer logs, underground forums and communities, dark web repositories, automated discovery, intelligence partnerships, and other surface, deep, and dark web sources.

2 VERIFICATION AND DEDUPLICATION

Automated processing removes duplicate, recycled, and previously observed records. Automated triage flags sensitive information and supports domain validation. Subject matter experts verify attribution and breach details before ingestion into the Constella Data Lake.

3 SCOPE AND DENOMINATORS

Breach statistics reflect data collected or processed during the stated period. Data Lake totals are cumulative holdings at quarter end.

Email, password, and personal information prevalence figures are based on 8,095,846,352 curated Hacked Leaked and Combo records. Social media percentages represent the distribution across the six platforms tracked since Q1.

4 INFOSTEALER TIMING

Device counts are organized by infection date. Package and record counts are organized by ingestion date. Processing timing can therefore cause these measures to move in different directions.

Cookies, session tokens, authenticated access, and AI account exposure are discussed as potential risks associated with infostealers. The Q2 dataset presented in this report does not quantify their prevalence.

5 ATTRIBUTION

Geographic and industry distributions include only Hacked Leaked breaches with reliable attribution. Geographic classifications are based on breached entity headquarters or available data provenance. Records without sufficient attribution are excluded.

6 COMPARABILITY AND INTERPRETATION

Quarterly changes can reflect collection coverage, breach composition, processing timing, and detector coverage. They should not be interpreted as a complete measure of global incident frequency or overall platform security.

Percentages may not total exactly 100% because of rounding and differences in category scope.

SEE WHAT ATTACKERS MAY ALREADY KNOW

Constella Intelligence gives organizations visibility into exposed data already in the hands of cybercriminals and helps them understand how that information could be weaponized against employees, customers, and the business.

Enterprises, managed service providers, technology platforms, and investigative teams use Constella intelligence to enrich investigations, monitor exposed identities, and strengthen protection for employees, customers, and digital populations.



UNDERSTAND YOUR EXTERNAL
IDENTITY EXPOSURE

[REQUEST A DEMO](#)



About Constella Intelligence

Constella is a global leader in Identity Risk Intelligence. Through its extensive breach and infostealer intelligence, Constella helps organizations identify exposed credentials, personal information, devices, online identities, and services circulating outside their environments. Enterprises, managed service providers, technology platforms, investigative teams, and law enforcement agencies use Constella intelligence to enrich investigations, monitor exposed identities, and strengthen protection against digital risk.



Where Data & Identity Intersect

Powered by

**THE WORLD'S LARGEST VERIFIED
IDENTITY DATA LAKE**

