Constella Intelligence Quarterly Report Finds Infostealer Infections Nearly Doubled in Q2 2026

Increased infostealer infections signal broader identity exposure, giving criminals details about victims' online services and context for personalized scams.

LOS ALTOS, CA, UNITED STATES, September 24, 2026 /EINPresswire.com/ -- Constella Intelligence, a leader in Identity Risk Intelligence, today announced the release of its latest Quarterly Identity Breach Report, revealing a significant expansion in external identity exposure and infostealer activity during the second quarter of 2026.

> By connecting and validating fragmented identity data, organizations can better understand what attackers may already know and act before that information is weaponized."
>
> *Andres Andreu, CEO of Constella*

Constella registered 5.53 million devices with Q2 infostealer infection dates, a 99.53% increase from Q1. During the quarter, Constella also identified more than 670,000 potential breaches containing more than 447 billion records. Following 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 findings highlight a growing security challenge: identity exposure can originate on personal or unmanaged devices outside the reach of traditional corporate security controls. Infostealers can capture credentials, browser activity, device information, and details about the online services a victim uses, giving criminals a head start on potential attacks and providing the context needed to create highly personalized scams.

Nearly every Q2 infostealer record analyzed contained a URL associated with an online service accessed from the infected device, while 94.97% contained passwords, 46.95% contained usernames, and 46.05% contained email addresses. Together, these artifacts can reveal which services victims use and provide attackers with greater context about where stolen access may be valuable.

"Organizations cannot protect what they cannot see," said Andres Andreu, CEO of Constella Intelligence. "Identity risk management must extend beyond internal systems to include the data

already exposed and available to adversaries. By connecting and validating fragmented identity data, organizations can better understand what attackers may already know and act before that information is weaponized."

Constella's Data Lake closed the quarter with 72.95 billion records, up 14.07% from Q1, and 544.16 billion attributes. Email addresses appeared in 51.07% of curated Hacked Leaked and Combo records, an increase of 11.19 percentage points from Q1, while plaintext passwords appeared in 50.90%.

More than 95% of Q2 Hacked Leaked breaches contained personally identifiable information beyond credentials. Names, phone numbers, addresses, identifiers, and financial information can add context that may enable highly personalized scams, impersonation, fraud, phishing, and targeted social engineering.

The report also examines risks associated with browser cookies and session tokens captured by infostealers. When a stolen session remains valid, an attacker may potentially reuse an already authenticated session without completing the normal login process again. The actual risk depends on factors including token validity, platform controls, and whether compromised sessions are detected and revoked.

Key Findings From the Quarterly Report:

• 5.53 million devices were registered with Q2 infostealer infection dates, up 99.53% from Q1.

• The Constella Data Lake reached 72.95 billion records, an increase of 14.07% from Q1.

• 51.07% of curated Hacked Leaked and Combo records contained an email address, up 11.19 percentage points from Q1.

• 50.90% contained plaintext passwords.

• Constella observed 64.72 million social media attributes across six tracked platforms, with Telegram and Facebook accounting for 95.81% of that exposure.

• The five largest verified Q2 breaches associated with specific companies or domains contained a combined 1.05 billion records.

Read more about the evolving infostealer threat.

To accompany the report, Constella CEO Andres Andreu and Chief Technology Officer Alberto Casares discuss the evolving infostealer landscape and what these exposures mean for organizations protecting employees, customers, and digital identities.

Their discussion examines why organizations need visibility beyond traditional credential monitoring and how the broader identity context exposed by infostealers can help security teams better understand potential risk.

What Security Teams Can Do:

The report recommends that organizations expand identity risk management beyond internal systems. Actions include correlating external exposure across identities, treating confirmed plaintext credentials as immediately actionable, investigating infostealer infections beyond password resets, strengthening authentication controls, and continuously monitoring external identity exposure.

Download the Quarterly Identity Breach Report

The complete Constella Intelligence Quarterly Identity Breach Report provides analysis of breach and infostealer intelligence collected and processed during Q2 2026, including trends in identity exposure, infostealer activity, breach sources, geographic and industry concentration, and recommended actions for security teams.

About Constella Intelligence

Constella Intelligence provides organizations with visibility into exposed identity data already in the hands of cybercriminals, helping them understand how that information could be weaponized against employees, customers, and their 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.

Constella Intelligence, Inc
Constella Intelligence
marketing@constellaintelligence.com

This press release can be viewed online at: https://www.einpresswire.com/article/944892177

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.