

Identity Exposure Report

Secure the identities of your employees and customers in near real time.

Challenge

As enterprises rapidly adopt SaaS applications, the security landscape has fundamentally shifted. Now that up to 77% of web application breaches begin with stolen credentials (Verizon DBIR 2024), identity has overtaken infrastructure as the primary attack vector for modern threat actors.

Identity leaks can pose an immediate risk to organizational security, compliance, and operations. When threat actors obtain stolen credentials, it's a race against the clock to take action and prevent a breach from happening.

Solution

Using Identity data indexed by Recorded Future's Intelligence Graph®, this report details the number, recency, and criticality of compromised employee and customer credentials related to your organization. Understanding your exposure is a critical first step in preventing unauthorized access and protecting your cloud-based assets.

Identity Intelligence arms your organization with the freshest, broadest coverage of data leaks and credential harvesting across hacker, criminal, and invitation-only sites as well as extremist forums. Rather than just monitoring existing breaches, Recorded Future often has visibility into breached data before it reaches dark web markets, helping prevent impacts to your organization. Direct integration with security tools enables automated response, so you can proactively mitigate account takeovers and prevent business disruption.



Benefits

- Reduce operational and financial risk associated with stolen credentials.
- Better secure your attack surface, including the identities of employees and customers.
- Automate risk checks during critical events.

Key Capabilities

- Visibility across hacker, criminal, and invitation-only dark web sites.
- Automated lookups and remediation of exposed credentials with detailed context.
- Integrations with leading IAM and SOAR solutions.

"The timeliness is a big win with Identity Intelligence. Being able to automate the response after seeing an alert to our active directory allows us to feel confident that the account is secure."

Curtis Hartsell

Senior Cyber Threat Intelligence Manager,
Toyota Motors North America

"Thanks to the Recorded Future Managed Services team we caught on to our internal user's credentials leaking before anything could happen, and that helped us to prevent significant damage."

Security Analyst

Medium-sized enterprise internet software and services company

About the Report

FAQs:

What's the recommended response when credentials are detected?

We recommend a multi-step response. First, force a password reset for the affected accounts and enable multi-factor authentication if not already in place. Second, review the exposure details we provide, like malware type and system information, to understand the source and scope of the compromise. Third, monitor these accounts for any suspicious activity. And for maximum protection, consider integrating Recorded Future Identity Intelligence with your existing security tools to enable automated responses when credentials are exposed in the future.

Why didn't my report indicate any exposed identities?

A report showing no exposures means we haven't detected your domain's credentials across our indexed sources, which include dark web marketplaces, criminal forums, paste sites, and malware campaigns. Several factors could influence this, such as strong existing security measures, effective password policies, and/or successful security awareness training. While this is positive, it represents a point-in-time assessment. The threat landscape constantly evolves, and new exposures can occur at any time through data breaches or malware infections.

Also, keep in mind that your report analyzes only the specific corporate domain you submitted. Our intelligence indicates that most organizations have credential exposure across 5+ domains, including subsidiaries, acquisitions, and brand variations.

Do I still need to monitor leaked credentials if the report doesn't show any exposed credentials?

We still recommend regular monitoring as credential exposures can happen suddenly through new data breaches, social engineering attacks, or malware campaigns. Continuous monitoring will help ensure that you're alerted to new exposures identified by Recorded Future Identity Intelligence as quickly as possible and that you can respond rapidly before any malicious activity occurs.

Can I run reports for multiple domains if my company has several?

Currently, we can only provide results for the domain that appears in the email address submitted in the form.

How does this complement my organization's existing identity protection measures?

The Identity Exposure Assessment Report provides a valuable point-in-time snapshot of your credential exposure risk, but it's just the first step. Recorded Future Identity Intelligence builds on this by providing continuous monitoring and automated response capabilities that integrate directly with your existing security tools to stop account takeovers before they happen.

Executive Summary: [COMPANY] Identity Exposure Analysis

Key Findings

Between [DATE] and [DATE], Identity Intelligence found:

X

Credentials
Compromised

X

Authorization
URLs

X Days

Median Time to
Identification

X%

Credentials Identified
Within 24 Hours

Recommended Actions

Reduce operational and financial risk with Recorded Future's Identity Intelligence



Secure your attack surface,
including identities of
employees and customers



Prevent breaches with
automated risk checks at
critical access points



**Integrate with existing
security tools** to automate
and streamline remediation

Proprietary & Confidential

 Recorded Future®

Request Your [Identity Exposure Report](#)

[Request a demo](#) to see how you can pinpoint, prioritize, and take action on exposed credentials with Recorded Future.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,900 businesses and government organizations across more than 80 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com

© Recorded Future®, Inc. All rights reserved. All trademarks remain property of their respective owners.