GenAI Threat Landscape

Digital Threat Report

Company: ACME

Domain: acme.com

Authorized By: john.doe@acme.com | Requested On: 09/09/2024

VYDAR
powered by Zenox

Media
contact@zenox.ai
www.zenox.ai

ZenoX AI
Av. Dr. Chucri Zaidan, 1550
BR - São Paulo - SP, 04711-130

Summary

On September 4, 2024, ACME faces a concerning threat landscape that demands immediate attention. A significant volume of 8,432 stolen user credentials circulating, combined with the exposure of 72 employee credentials, poses a substantial risk of intrusion and data breaches. The presence of 8 suspicious websites related to the company's brand or domain expands the attack surface, making ACME vulnerable to phishing attacks and malware distribution. The 12 mentions in messages, possibly originating from clandestine forums, suggest that malicious actors might be discussing vulnerabilities and planning fraudulent activities against the company. The TECHNOLOGY sector in which ACME operates is frequently targeted by cybercriminals due to the large volume of sensitive data it manages, such as customer information and financial data. The combination of these factors indicates a vulnerable cybersecurity posture, requiring robust measures to mitigate risks and protect its assets and reputation. It is crucial to investigate the validity of the exposed credentials, implement stricter security measures, and strengthen employee awareness regarding cybersecurity best practices.

Summary Generated by Tellyu AI

This summary was generated by our proprietary generative artificial intelligence Tellyu, customized in real-time to analyze the threats found in your company.

Results

CREDENTIALS	EMPLOYEE CREDENTIALS
8432	72

CREDENTIALS FOR SALE	DARKWEB MENTIONS
428	312

FRAUD MENTIONS	SUSPICIOUS WEBSITES
12	8

LAST EXPOSURE

5 Days Ago

On this page, we present a summary of the main results detected by Vydar, our advanced Threat Intelligence solution. Here, you will find crucial information about compromised credentials, data for sale, mentions on the dark web, and suspicious websites related to your domain and organization. This data is collected and analyzed continuously to offer a clear and detailed view of the cyber threats that may impact your company.

We recommend that you take advantage of our **14-day free trial** to experience the full power of **Vydar** and protect your company against the most advanced cyber threats.

VYDAR
powered by ZenoX

Infected Machines Credentials

Credentials found through infected machines, for example, through "stealers", are confidential information, such as usernames and passwords, that are stolen by malware installed on compromised devices. These malicious programs monitor and record the victim's activities, capturing sensitive data directly from the browser or other applications, and sending this information to the attackers.

8432
Credentials

URL	Username	Password	Infection Date	Country	IP Address
acme.com/login	user*****name	p@$$*****rd	09/04/2024	-	-
mail.acme.com	john.*****doe	Em@1l*****rd	09/02/2024	-	-
shop.acme.com/checkout	jane.*****smith	Sh0pping*****rd	08/30/2024	-	-
support.acme.com/login	david.*****wilson	Supp0rt*****rd	08/26/2024	-	-
forum.acme.com/login	emily.*****brown	F0rum*****rd	08/22/2024	-	-

See All

VYDAR powered by ZenoX

Employee Credentials

Obtained employee credentials refer to usernames and passwords for corporate accounts, especially those associated with the company's domain, that were stolen by malware installed on compromised devices. This malware captures the credentials used by employees when accessing their emails and other corporate systems.

72
Credentials

URL	Username	Password	Infection Date	Country	IP Address
app.monday.com/login	john.d*****@acme.com	pa$$****rd	09/03/2024	-	-
zoom.us/signin	jane.s*****@acme.com	Sec****rd!@#.	08/29/2024	-	-
github.com/login	david.m*****@acme.com	G1thub****rd	08/25/2024	-	-
slack.com/signin	emily.b*****@acme.com	Slac****rd	08/18/2024	-	-
sso.acme.com/login	michael.w*****@acme.com	Acme****rd	08/11/2024	-	-
mail.google.com/mail	sarah.c*****@acme.com	G00gle****rd	08/05/2024	-	-
jira.acme.com/login	robert.h*****@acme.com	J1ra****rd	07/29/2024	-	-
confluence.acme.com/login	linda.p*****@acme.com	C0nflu****rd	07/22/2024	-	-
bitbucket.org/login	james.t*****@acme.com	B1tbu****rd	07/15/2024	-	-
trello.com/login	mary.k*****@acme.com	Tr3llo****rd	07/08/2024	-	-

See All

VYDAR powered by ZenoX

Suspicious Websites

URLs identified that mention, in whole or in part, the name of a company and that may be associated with malicious activities, such as phishing campaigns, are considered suspicious. These websites are often created by cybercriminals to deceive users into believing they are accessing a legitimate company website when, in fact, they are entering their credentials or other sensitive information in an environment controlled by the attackers.

8
Websites

Date	URL
08/25/2024	http://acme-pr*****otions.com/
08/18/2024	https://get-ac*****e-deals.net/
08/11/2024	https://acme-su*****pport-desk.org/
08/04/2024	https://acme-lo*****gin-page.com/
07/28/2024	http://www.ac*****me-rewards.com/
07/21/2024	https://secure-ac*****me.net/
07/14/2024	https://acme-onli*****ne-banking.info/
07/07/2024	https://acme-cust*****omer-service.xyz/
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

See All

VYDAR
powered by ZenoX

Credentials For Sale On The Darkweb

Credentials sold on the dark web are stolen usernames and passwords that are traded in clandestine online marketplaces. These credentials may belong to email accounts, social networks, banking services, or even corporate systems, and are offered to cybercriminals to carry out fraud, identity theft, or targeted attacks.

428
Credentials

URL	Price ($)	Infection Date	Country	Source
acme.com	15	08/28/2024	US	Stealer
shop.acme.com	12	08/16/2024	CA	Stealer
support.acme.com	18	08/04/2024	AU	Stealer
acme.com	14	07/20/2024	GB	Stealer
forum.acme.com	16	07/08/2024	DE	Stealer
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

See All

VYDAR powered by ZenoX

Mentions on the Darkweb

Refers to any mention of a company or organization found in clandestine forums, marketplaces, or shared files in this hidden part of the internet. These mentions may include discussions about vulnerabilities, stolen data, attack plans, or even the sale of sensitive information linked to the company.

312
Mentions

Date	Name	Source
09/01/2024	ACME customer database leak	DarkWeb
08/27/2024	Leaked ACME employee credentials	DarkWeb
08/23/2024	ACME website vulnerabilities	DarkWeb
08/19/2024	ACME payment card data dump	DarkWeb
08/15/2024	ACME internal documents exposed	DarkWeb
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

See All

VYDAR powered by ZenoX

Mentions in Fraud Channels

Refers to mentions of a company or organization identified in groups and channels of encrypted messaging applications, such as Telegram, where cybercriminals share fraud techniques and market illicit products or services. In these communities, there may be discussions about how to circumvent the company's security systems, the sale of stolen data, or even the organization of targeted attacks.

12
Mentions

Date	Message	Source
09/03/2024	Anyone have ACME credentials for sale?	Forum
08/29/2024	Selling ACME database dump, PM for details.	DarkWeb
08/25/2024	Found some ACME vulnerabilities, might be exploitable.	Hacker Chat
08/21/2024	ACME website is down, possible DDoS attack?	Social Media
08/17/2024	ACME security breach, thousands of accounts compromised.	News Website
08/13/2024	Looking for ACME employee login credentials.	Cybercrime Forum
08/09/2024	ACME website defaced, hackers claim responsibility.	Security Blog
08/05/2024	ACME credit card data leaked online.	Pastebin
08/01/2024	ACME data breach confirmed, investigation underway.	Company Statement
07/27/2024	ACME network infiltrated, sensitive data stolen.	Whistleblower Report

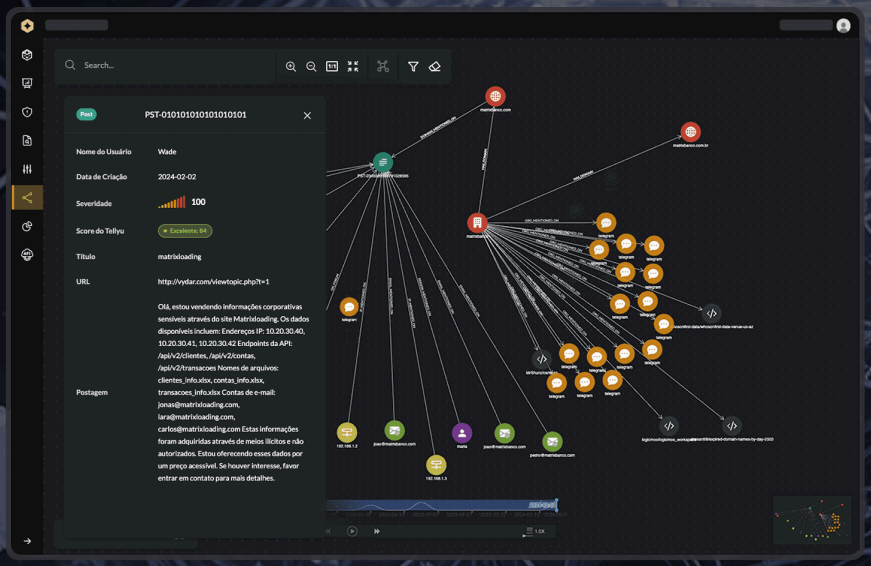
See All

AROUND THE WORLD

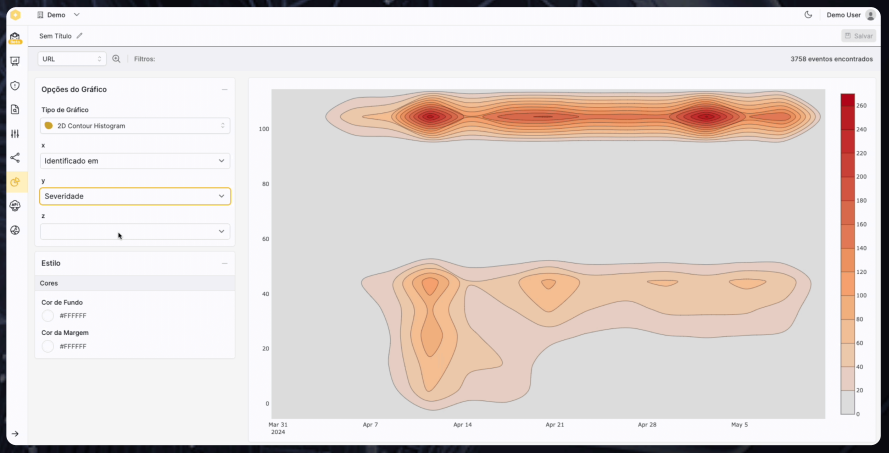
Global Threats

The Around the World page offers a global view of detected threats, allowing you to identify the geographical origin of these malicious activities. The locations highlighted on the map represent areas where mentions of the company, compromised credentials, or other suspicious cyber activities were found. This geographical analysis is crucial to understanding where the greatest risks are concentrated and how these threats are distributed around the world. With this information, it is possible to adopt more targeted and effective defense strategies, ensuring a quick and precise response to global threats that may impact your company's security.

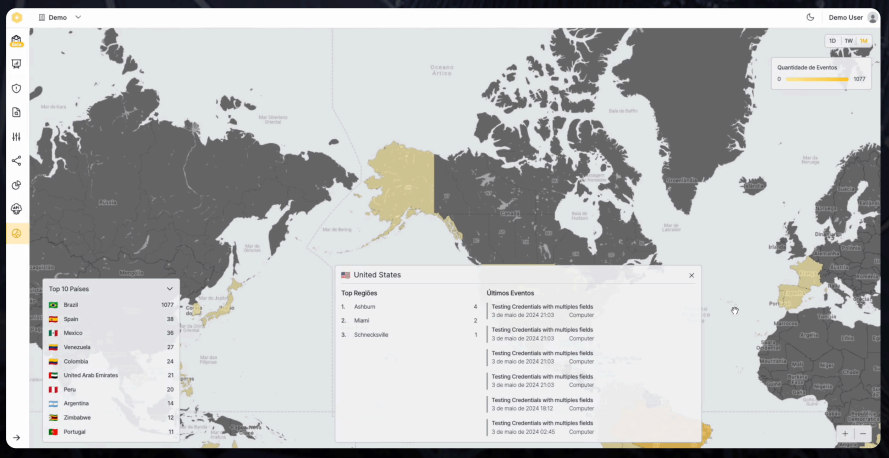
Country	Threat
United States of America	612 Credentials
Canada	84 Credentials
United Kingdom	56 Credentials
Australia	48 Credentials
Other Countries	32 Credentials



Custom Dashboards



Investigation Platform



Real-Time Map

VYDAR
powered by ZenoX

FREE TRIAL AT WWW.VYDAR.AI

Media
contact@zenox.ai
www.zenox.ai

ZenoX AI
Av. Dr. Chucri Zaidan, 1550
BR - São Paulo - SP, 04711-130