GenAI Threat Landscape

Digital Threat Report

Company: ACME Corp

Domain: acme.com

Authorized By: jose@acme.com | Requested On: 08/08/2025

INTELLI WAY

Media
contato@intelliway.com.br
intelliway.com.br

Intelliway
R. Roberto da Silva, 20, Sala 310, Ed. Premium Office – Mata da Praia, Vitória – ES, 29066-091

Summary

A ACME, em 18 de Setembro de 2024, enfrenta um cenário de ameaças preocupante que exige atenção imediata. Um volume alto de credenciais de funcionários expostas (1328) combinadas com um número significativo de credenciais encontradas em mercados da dark web (450) sugerem um possível vazamento de dados ou campanha de phishing direcionada. A presença de domínios suspeitos (436) relacionados à marca acme Media levanta preocupações adicionais sobre potenciais ataques de phishing ou tentativas de manchar a reputação da empresa.

Embora não haja menções diretas em mensagens de fóruns da dark web ou plataformas similares, o vazamento de credenciais em si já coloca a empresa em risco. A acme Media, atuando nos setores de Serviços e Entretenimento, frequentemente lida com dados confidenciais de clientes, tornando-se um alvo atrativo para cibercriminosos.

A ausência de menções em mensagens não deve ser interpretada como um sinal de segurança, mas sim um alerta para fortalecer os mecanismos de detecção e resposta a ameaças, considerando que ataques podem estar em estágios iniciais de planejamento. Recomenda-se uma investigação completa sobre a origem das credenciais vazadas, fortalecer as políticas de senhas e implementar medidas robustas de segurança para proteger os ativos da empresa e a confiança do cliente.

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

450

EMPLOYEE CREDENTIALS

1328

CREDENTIALS FOR SALE

19

DARKWEB MENTIONS

1384

SUSPICIOUS WEBSITES

436

LAST EXPOSURE

A Year 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.

450
Credentials

URL	Username	Password	Infection Date	Country	IP Address
rhopen.acme.com/acme/index.html	dani*******eida	Nath******1010	09/10/2024	-	-
nadika.dushan@acme.com	201*@may	P******e	09/09/2024	-	-
fts.acme.com	l*****a	l******i	09/04/2024	-	-
fts.acme.com/login	z******2	8271******qw...	09/04/2024	-	-
fts.acme.com/register	rog************@gmail.com	Ro*****50	09/04/2024	-	-
es.acme.com/s%c4%adguenos/	vid*********@gmail.com	9600******Savs	09/04/2024	-	-
es.acme.com/s%c3%adguenos/	vi********ga	8500******Savs	09/04/2024	-	-
es.acme.com/s%c3%adguenos	vid*********@gmail.com	8500******Savs	08/14/2024	-	-
appreciateprogram.acme.com	7******8	di********co	08/13/2024	-	-
rhopen.acme.com/	hi********es	P*****5	08/13/2024	-	-

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.

1328
Credentials

URL	Username	Password	Infection Date	Country	IP Address
www.netflix.com/in/login	mat**********@acme.com	Ka******14	09/17/2024	-	-
www.linkedin.com/uas/login-submit	gem**********@acme.com	Be******26	09/17/2024	-	-
www.insights-metrics.com/dev/acmeop...	bre**********@acme.com	B******0	09/16/2024	-	-
www.facebook.com/	nec**********@acme.com	Te********06	09/16/2024	-	-
wppit.service-now.com	pla**********@acme.cc	6t*****i3	09/14/2024	-	-
wppit.service-now.com/selfservice/incid...	nat**********@acme.com	Pa******87	09/14/2024	-	-
wppit.service-now.com/service	jef**********@acme.com	Ka*******21	09/14/2024	-	-
wppit.service-now.com/welcome.do	vin**********@acme.c	P******9	09/14/2024	-	-
oxygene	jul**********@acme.com	Sa******51	09/09/2024	-	-
login.microsoftonline.com/common/oaut...	vin**********@acme.com	Ka******23	09/07/2024	-	-

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.

436
Websites

Date	URL
09/17/2024	https://panel**********/acmeweb/otpPage?homeNo=b376e675...
09/17/2024	https://resea**********/
09/17/2024	https://admin**********/
09/17/2024	https://newsi**********/
09/17/2024	https://repor**********/
09/17/2024	https://ftp.g**********/
09/17/2024	https://www.i**********/
09/17/2024	https://vpn.m**********/
09/16/2024	https://www.b**********/
09/16/2024	https://ek.sa**********/
[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.

19
Credentials

URL	Price ($)	Infection Date	Country	Source
acme.com	10	08/31/2024	PH	Stealer
acme.com	10	09/04/2024	PH	Stealer
acme.com	10	08/05/2024	KE	Stealer
acme.com	10	05/27/2024	FR	Stealer
acme.com	10	03/28/2024	IN	Stealer
acme.com	10	03/28/2024	MX	Stealer
acme.com	10	02/09/2024	IN	Stealer
panel.acme.com.ua	10	02/13/2024	UA	Stealer
panel.acme.com.ua	10	01/26/2024	UA	Stealer
panel.acme.com.ua	10	01/05/2024	FI	Stealer
[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 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.

1384
Mentions

Date	Name	Source
11/01/2020	acme.com	DarkWeb
05/24/2020	www.acme.com	DarkWeb
09/18/2024	TH_115.87.238.232_2024_09_04_17_42_51 - @OmegaCloud_FreeLogs.rar/...	DarkWeb
09/18/2024	PH_158.62.17.27_2024_09_04_10_15_11.rar/passwords.txt	DarkWeb
09/18/2024	PH_158.62.17.27_2024_09_04_10_15_11.rar/autofill/Microsoft Edge_Profile 1...	DarkWeb
09/18/2024	PE[e51a819f6fe3a387a78e01c70d7b4063][38.253.189.76].rar/Cookies/O...	DarkWeb
09/18/2024	PE[C09B250792716849AD1C9DCBB9C228FF] [2024-08-18T18_13_12.35...	DarkWeb
09/18/2024	PE[C09B250792716849AD1C9DCBB9C228FF] [2024-08-18T18_13_12.35...	DarkWeb
09/18/2024	NG_102.88.33.246_2024_08_28_22_36_48 - @OmegaCloud_FreeLogs.ra...	DarkWeb
09/18/2024	KE_197.232.143.33_2024_08_16_10_11_48 - @OmegaCloud_FreeLogs.rar/K...	DarkWeb

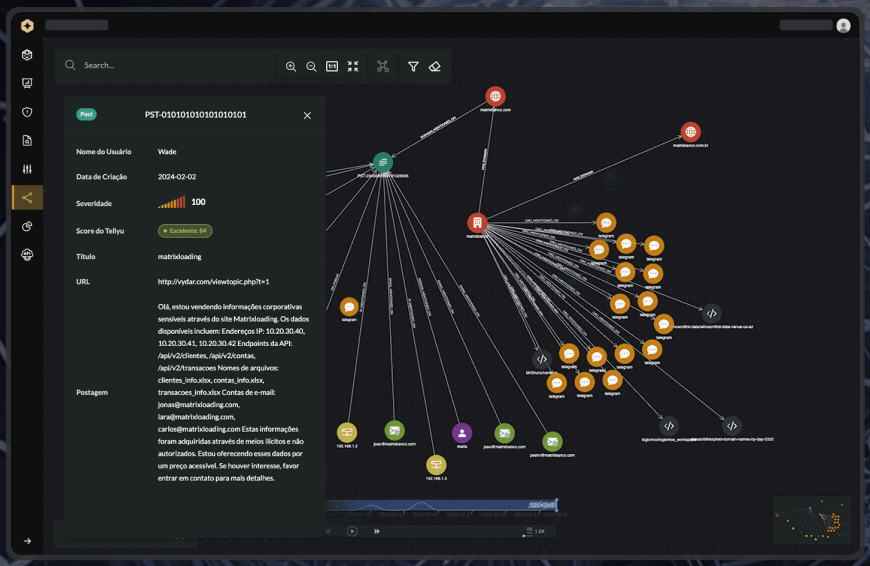
See All

AROUND THE WORLD

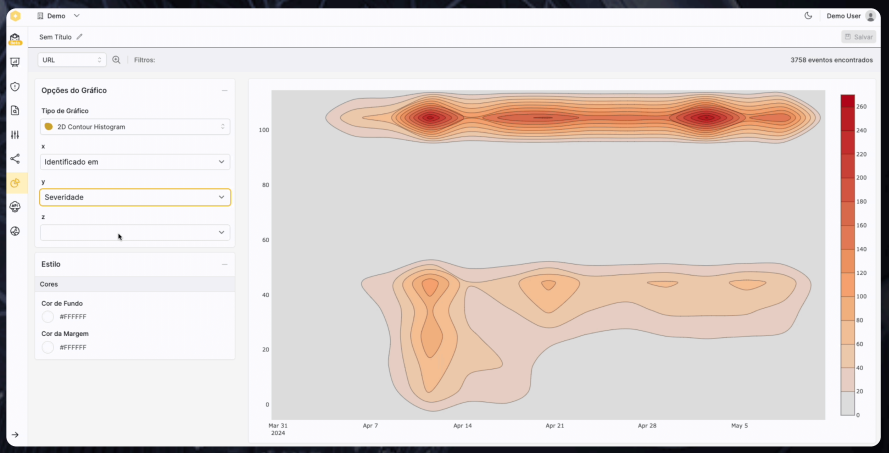
Global Threats

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.

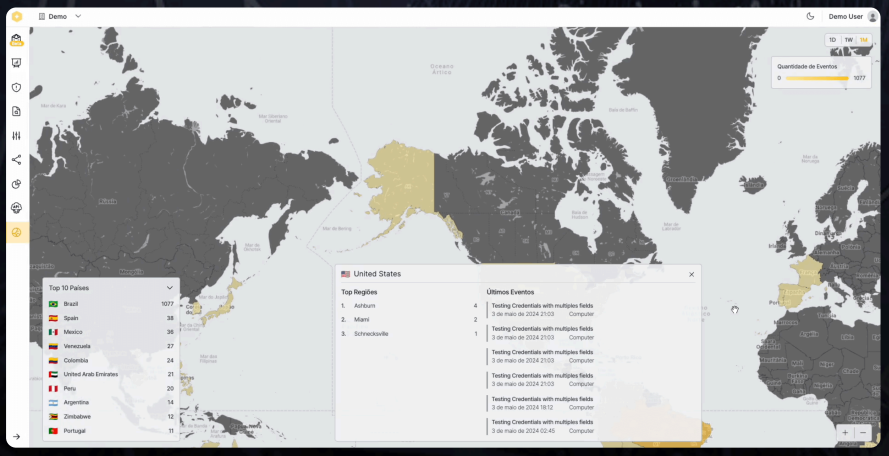
Country	Threat
Spain	23 Credentials
Romania	15 Credentials
India	8 Credentials
Brazil	7 Credentials
Other Countries	31 Credentials



Investigation Platform



Custom Dashboards



Real-Time Map

VYDAR
powered by Zenox

FREE TRIAL AT WWW.VYDAR.AI

Media
contato@intelliway.com.br
intelliway.com.br

Intelliway
R. Roberto da Silva, 20,
Sala 310, Ed. Premium
Office – Mata da Praia,
Vitória – ES, 29066-091