

# Uncover, investigate, and block threats on the deep & dark web

Malicious actors · #9176491 TLP: Amber

**Guuh NVi** 89

Also known as 5511987654321 Shen456 Guardians of Peace

First seen on 05/11/2022 at 15:47 · Last seen on 08/25/2023 at 15:19

**Top groups and channels**

- 📍 GG ELITE 📍
- 📍 SUPPORT WORLDPREMIUM-CHKS 💎
- 🗣️ Seven Reborn
- 🔗 TUTORIAL BRASIL OFC 📄 (Courses & System) 📄
- 📍 Closed Deal! 📄 Coupons & Promos 🏆

[View more](#) ▾

**Activity**

Month	Activity
Mar	602
Apr	513
May	428
Jun	539
Jul	627
Aug	829

Messages and posts

45.2k >

Tickets

198 >

The channels and forums of the Deep & Dark Web conceal a variety of dangers and threats that put your company at risk. This includes the marketplaces of access credentials, cards, and samples of databases, or even the orchestration of attacks. Malicious actors use these channels to disseminate new modus operandi, bypass security, and deceive your customers. You need an External Cybersecurity platform with full visibility to find these risks and act quickly to prevent attacks and losses.

Multimedia detection with computer vision

Open search for terms on the Deep & Dark Web

Generative AI for threat summarization

## Deep & dark web alerts

Monitor key groups, forums, marketplaces, and Darknet sites to anticipate attacks and discover new schemes

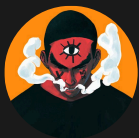


New frauds emerge first on the Deep & Dark Web. Be embedded to uncover schemes involving your company, sector, and competitors.

Receive alerts when terms related to your company, sector, or any keyword of interest are mentioned by malicious actors.

Intercept conversations and be the first to know about attack orchestration, vulnerability exploitation, and even insider recruitment for collaboration with cybercrime.

- Exposure of samples and databases
- Disclosure of frauds or schemes
- Sale of cards and credentials
- Exploitation of vulnerabilities and bugs
- Ransomware alerts



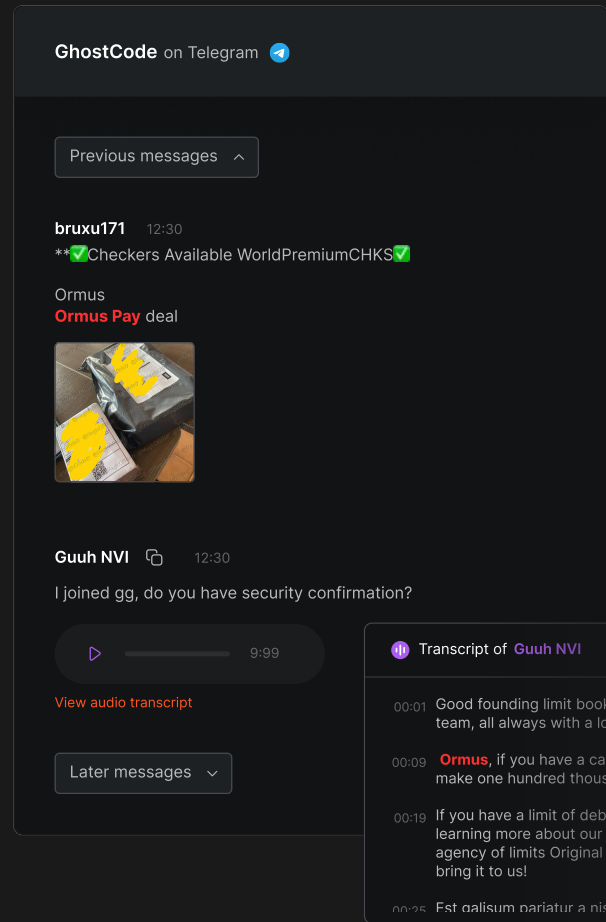
Guuh NVi 🔥 89

5511987654321

Shen456

## Threat actor profile and scoring to enrich your investigations

- Evaluate the risk level of malicious actors
- Access interaction history on other channels
- See the most targeted industries
- Check other actors with whom the profile interacts



## Multimedia detection with computer vision

This unique feature allows you to detect threats on the Deep & Dark Web in audio, video, and images, uncovering and responding to attacks involving complex schemes against organizations. Automatic transcription for audio and video turns multimedia content into actionable intelligence, protecting your organization with the most advanced technology.

More than 25% of incidents on the deep & dark web are detected in images, audio, and videos.

# Explore

Search for anything in Axur's infiltrated message groups



## Summary by Generative AI BETA

Activities related to your company in the last 7 days



There have been several scams being discussed involving Ormus, including:

- Activation of accounts with low values, such as R\$10, and misuse of these accounts in different banks.
- Use of personal information, such as SSN and identification data, to create fake accounts.
- Sharing and selling credit card information, including card numbers, BINs (Bank Identification Numbers) and limits.

## Explore

Search anything in our vast integrated Data Lake. Conduct personalized searches in a completely secure environment and rely on generative AI to summarize the most relevant threats. Search for exposed personal information, such as emails, identity documents, and addresses within monitored sources.

➔ Filter results by relevance, date, or custom preset, triggering alerts for new detections;

➔ Navigate past and future messages to gain real-time conversation context;

➔ Create actionable tickets for the most critical cases, enabling immediate investigation;

➔ Optimize efficiency by grouping identical messages posted across multiple channels.

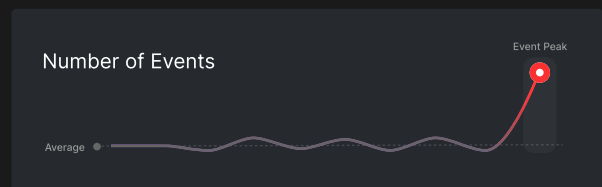
## DeepChat

Our proprietary generative AI model

You don't need to delve into every event on the Deep & Dark Web to gain an objective view of ongoing activities. Start your day with a briefing on the most pertinent mentions related to your brand using DeepChat, our patented generative AI model fluent in the language of cybercrime. Get accurate insights to optimize threat management and have an executive report at your disposal whenever needed.

## Anomaly alerts

Stay tuned to what matters most



Set up anomaly alerts for above-average mentions in specific channels or using keywords of your choice. Whenever an anomaly is detected, an alert is sent to promptly draw your attention to what's most important. Act quickly and avoid surprises.

**High** 8 identical messages

\*BRUXU\* Schemes and methods 2024\*  
✔ Ormus Scheme ✔ Job Iara Ormus PAY 🏆 ALL UPDATED!  
+55 79 9927-0779 📄 LIL OLUAP CHKS LOGINS 📄  
📱 WhatsApp 📍 Detected in audio

---

**Medium**

✔ #Cheker to order ✔ I make all types of Checkers, depending on the Customer's preference ✔ NODE/ADB/PYTHON™ I HAVE VARIOUS APIS  
hacker22 Family of 7 📄  
📱 Telegram 📍 Detected in image

---

**Medium**

darkw022@gmail.com:Dark-3657 | Plan = Ertan | Purchase Date = 6/13/2022 10:18:26 PM | Subscription Type = PAID | Renewal Date = 4/5/2024 7:14:44 PM  
📄 📄

## Ransomware alerts to monitor attacks

Receive immediate notifications about emerging threats, with screenshots for visual context.

### Victim identification

Understand which companies are targeted, and identify patterns within the same market or region.

### Track groups

Identify and monitor the activities of specific ransomware groups.

### Third-party risks

Evaluate the risk of data exposure related to vendors.

### TTPs Identification

Strengthen defenses against the evolution of ransomware tactics, techniques, and procedures.

## Infrastructure alerts

Monitor devices directly accessible via IP addresses. Receive alerts about open ports, CVEs, and vulnerabilities.

File repository \* Ransomware attack alert / Open

## Ormus Group is a victim of a ransomware attack

ShadowByte

+

VICTIM

### Ormus Group

Website	<a href="https://OrmusGroup.com">https://OrmusGroup.com</a>
Estimated Attack Date	04/07/2024 at 05:19 PM
Country	Brazil
Description	Is a leading manufacturer of screen advertising since 197... well as digital advertising solution.

RANSOMWARE GROUP

### ShadowByte

Post URL <https://ransomwarefeedx.br/874238237483y2823y>

High risk level

SOURCE

Ransomware feed

### Events history

Threat detected  
01/01/2022 at 09:30 AM

Ticket created

### Notes

Add here any  
Axur does not

# Protect your company from deep & dark web threats.

Get a demo

Discover all our solutions at [axur.com](https://axur.com)

**AXUR**