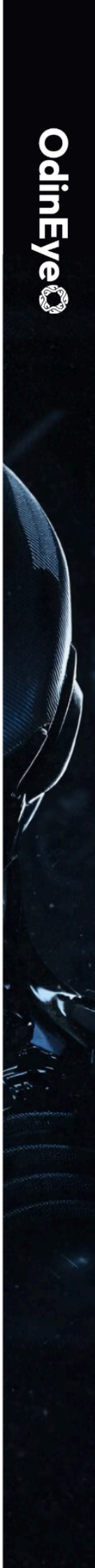
OdinEye

2025

BLACKSHRANTAC: RANSOMWARE THREAT ANALYSIS

Contents

Introduction	3
Executive Summary	4
Target and Victim Analysis	7
Technical Analysis	9
Case Studies	13
Technical Indicators (IOCs)	25
Conclusion & Mitigation	26
References	29



Introduction

The world of cyber threats is evolving from an era where traditional ransomware focused solely on file encryption to more complex and difficult-to-detect “data extortion” models. One of the most recent and aggressive examples of this transformation, **BlackShrantac**, emerged on the cyber threat scene in the last quarter of 2025 and has become a global risk factor targeting critical infrastructure, manufacturing, and technology sectors in particular. First detected on September 17, 2025, and responsible for 35 confirmed attacks worldwide in a short period, primarily in the United States, India, and Turkey, the group has drawn attention with its operational speed and effectiveness. Unlike classic ransomware groups, BlackShrantac largely bypasses the file encryption step in its operations, focusing its resources directly on exfiltrating terabytes of sensitive data from the network. This indicates that the group's primary motivation is not to render systems inoperable, but rather to compromise the confidentiality of corporate data and gain financial profit through extortion.

This report was prepared to provide actionable intelligence to corporate security teams (SOC/CSIRT) and senior executives (CISO) by comprehensively analyzing the BlackShrantac threat group's tactics, techniques, and procedures (TTP), target profiles, and operational capabilities. The methodology used in preparing the report is based on a multi-layered data verification process. The analyses were created by examining open-source intelligence (OSINT), technical analysis reports, and, most importantly, **primary data obtained from disclosure platforms (Dark Web)** belonging to threat actors. The fact that the group targets a wide geographical area, including the Russian Federation, without regard to geopolitical boundaries, and that Turkey is the third most attacked country globally, makes this report a vital defense resource for local organizations and critical infrastructure operators. This document aims not only to define the threat but also to provide concrete defense strategies based on identified malware signatures, network infrastructure, and attack vectors.

Executive Summary

BlackShrantac is a next-generation cybercriminal organization that emerged on the cyber threat scene on **September 17, 2025**, driven by financial motivations. The group pursued an aggressive growth strategy in the final quarter of 2025; elevating its operations that began in September to a peak in October, gaining global recognition in a short span of time.

As of December 2025, there are **35 confirmed successful attacks** carried out by the group. While BlackShrantac follows a path similar to the **"Big Game Hunting"** strategy in target selection, it does not limit its victim profile solely to Fortune 500 companies; it also targets SMEs with critical data, law firms, and manufacturing facilities through an opportunistic approach. The group's operational status is currently classified as **Active**.

When the group's victim profile is examined, it is evident that they focus on high-value-added sectors such as **Technology and Manufacturing** instead of random attacks. The following chart summarizes the sectoral density of these attacks:

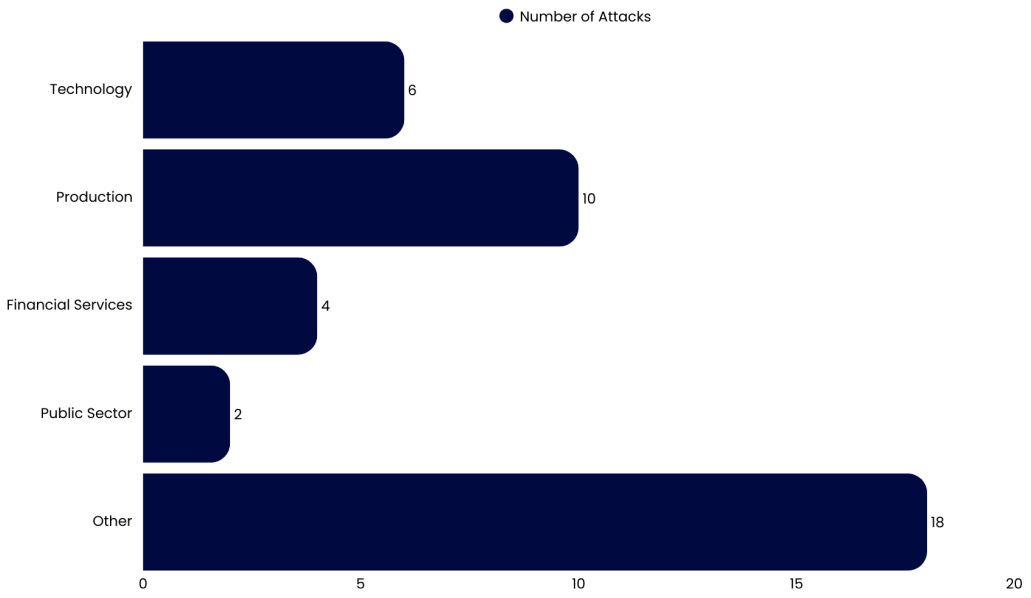


Figure 1: Verified Sectoral Distribution of BlackShrantac Attacks (2025)

1. Threat Profile and Motivation

BlackShrantac visualizes itself with a **"dark, hooded avatar"** to project an element of fear within the cyber underworld. Analysis of the group's target audience reveals that, unlike traditional ransomware groups (e.g., REvil, DarkSide), they lack political or geographic **"red lines"**.

Specifically, by violating the implicit rule against attacking Commonwealth of Independent States (CIS) countries and targeting institutions within the **Russian Federation**, the group demonstrates an independent, lawless **"mercenary"** structure focused purely on financial gain rather than being a state-sponsored entity. In terms of global attack traffic, the **United States (7 attacks)** and **India (6 attacks)** lead the list, while **Turkey (4 attacks)** stands as the third most targeted country.

2. Operational Model: Non-Encryption Extortion

The most critical feature distinguishing BlackShrantac in the current threat landscape is its tendency to skip the file encryption step in the **attack kill chain**. Instead of locking the victim's systems and halting operations, the group moves silently through the network (**Lateral Movement**), exfiltrates sensitive data reaching **Terabyte (TB)** scales, and conducts blackmail through **"Data Disclosure"**.

Evidence of this **"Pure Data Extortion"** model is clearly seen in attacks within Turkey:

- **Dem İlaç**: 1 TB of R&D and formula data was exfiltrated.
- **Rasen İnşaat**: 400 GB of strategic company data and employee information were compromised.
- **Şimşek A.Ş.**: 200 GB of logistics and distribution network data was leaked.

This method makes it difficult for security software (Antivirus/EDR) to detect traditional **"ransomware behaviors"** (such as file encryption) and significantly extends the attack's **dwell time**.

Analyst Note : "Pure Data Extortion" is a cybercrime tactic where threat actors, instead of blocking access by encrypting the victim's files, threaten to steal and expose the data. In this model, the primary risk is not "Data Loss," but a "Confidentiality Breach". Consequently, the traditional "Backup" strategies that organizations rely on cease to be a bargaining chip in this scenario, as the data is not locked but stolen.

3. Operational Growth and Attack Speed

The group pursued an aggressive growth strategy in the final quarter of 2025. The initial wave of reconnaissance and attacks that began in September reached its peak in October and November. The following chart summarizes the group's increasing attack volume on a monthly basis:

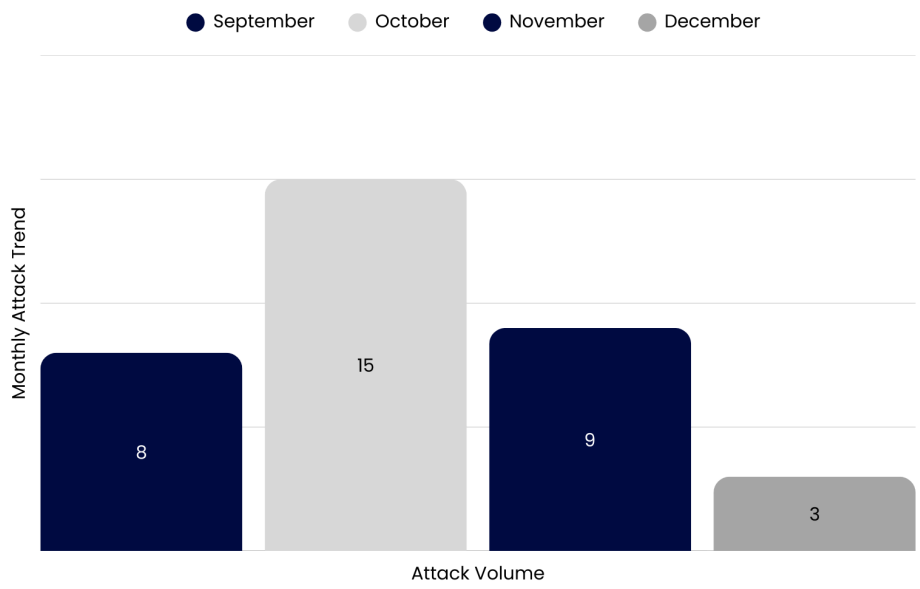


Figure 2: BlackShrantac Monthly Attack Trend (September - December 2025)

The sudden surge observed in October indicates that the group completed its infrastructure and transitioned to a **"mass exploitation"** phase. As of December 2025, there are a total of **35 confirmed victims**, and the group maintains an **"Active"** status.

Target and Victim Analysis

The operational data of the BlackShrantac group reveals not only its current victims but also its potential future target volume. This section analyzes the group's global reach and the true scale of the claims made on its leak platform.

1. Geopolitical Targeting and Global Reach

The group's geographic distribution proves that it possesses a structure that recognizes no geopolitical boundaries.

- **Critical Regions**: While the highest attack volume is concentrated in the **USA (7)** and **India (6)**, **Turkey (4)** stands as the third most targeted country by the group.
- **Broad Range**: The verified victim list includes strategic countries such as Mexico, Peru, Indonesia, South Korea, the UAE, Qatar, Malaysia, Egypt, and Australia.
- **Borderless Threat**: The group's inclusion of institutions in the **Russian Federation** on its target list demonstrates that it does not adhere to regional protection rules and is entirely financially motivated.

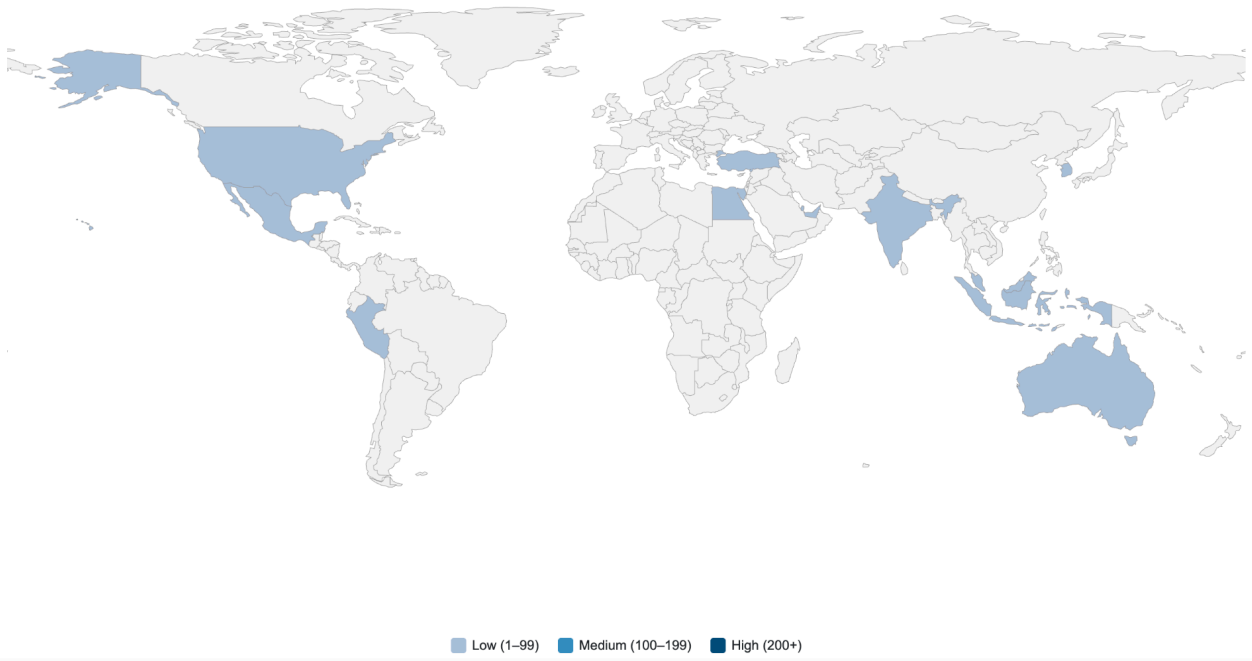


Figure 3: Global Impact Area of Black Shrantac Operations

2. Operational Scale: Verified vs. Alleged Attacks

Data from the group's leak panel reveals a significant disparity between confirmed operations and alleged volumes. This discrepancy indicates that the group creates **"threat inflation"** to exert psychological pressure on its victims.

- **Total Threat Volume**: While there are **38 verified attacks** confirmed to have been carried out by the group, their panels contain records of **621 unverified attacks** for which evidence has yet to be provided.
- **Verification Rate**: Only approximately **5.7%** of the total claims are currently verified.

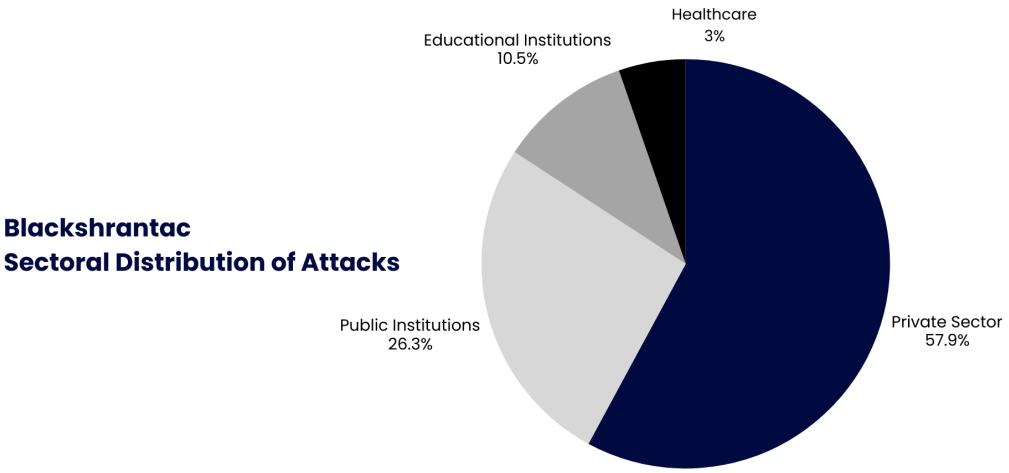


Figure 4: BlackShrantac Attacks by Industry

3. Sectoral Distribution and Real Percentages

The distribution of the **38 verified attacks** across institutional classes reflects the true nature of the group's targeting strategy:

- **Private Sector (Businesses)**: **57.9%** of verified attacks (22 attacks) directly target private companies.
- **Public Institutions**: **26.3%** of attacks (10 attacks) have targeted public administrations.
- **Educational Institutions**: Account for a total share of **10.5%** (4 attacks).
- **Healthcare Institutions**: Targeted at the lowest rate, representing **5.3%** (2 attacks) of total confirmed breaches.

4. Critical Sectoral Vertical Targets

Within these broad categories, the group specifically focuses on the following vertical sectors:

- **Industry and Technology**: Technology (6 attacks), Manufacturing (5 attacks), and Computer Systems Design Services.
- **Critical Infrastructure and Services**: Energy, Construction, Textile Production, and Law Firms.
- **Agriculture**: Crop Production and general Agriculture/Forestry activities.

Technical Analysis

This section covers the operational infrastructure, attack cycle, and the execution of the **"Pure Data Extortion"** model by the Black Shrantac group in technical detail. Our analysis includes critical information for the detection and neutralization of the methods employed by the actor.

1. Operational History and Activity Analysis

The first technical findings regarding the Black Shrantac group were observed in early 2025. The group's activity graph shows distinct fluctuations, unlike standard ransomware groups:

- **Early Period Activities**: The group emerged in **January 2025** with **7 verified attacks** and reached its first major peak in **February** by increasing the attack volume to **15**.
- **Restructuring and Second Wave**: Although the attack volume showed a decrease between **March and August**, the group reactivated as of **September**.
- **Current Status**: Classified as **"Active"** as of **September 17, 2025**, the group proved its operational capacity by reaching another peak of **15 attacks** in **October 2025**.

2. Black Shrantac Attack Kill Chain

The group's technical operations consist of a multi-stage process aimed at violating data confidentiality.

- **Reconnaissance and Initial Access**: Attackers perform the initial breach by identifying vulnerabilities in target networks.
- **Data Collection and Preparation**: Following the breach, critical data such as financial documents, HR records, R&D data, and internal correspondence are gathered in **"staging"** areas.
- **High-Volume Data Exfiltration**: The most concrete evidence of the group's technical skill is its capacity to exfiltrate TB-scale data (e.g., **Dem İlaç - 1 TB**, **Rasen İnşaat - 400 GB**) from the network.
- **Dwell Time**: Skipping or delaying the encryption step prevents security software (EDR/AV) from triggering **"ransomware"** alarms, allowing attackers to remain in the network for a longer duration.

Figure 5: Black Shrantac Attack Kill Chain

3. Data Extortion and Blackmail Methodology

Black Shrantac technically emphasizes the **"encryptionless ransomware"** tactic.

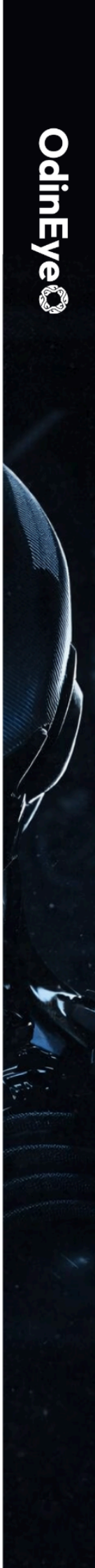
- **Victim Shaming**: Black Shrantac utilizes stolen data published on leak platforms to apply social pressure and tactical leverage, forcing victims into payment.
- **Extended Blackmail**: The group goes beyond threatening to release data; they also contact business partners via email to draw attention to the breach and undermine corporate reputation.
- **Disclosed Data Types**: Technical reviews indicate that the group targets passports, insurance documents, financial balance sheets, product R&D data, and strategic internal communications.

> **Analyst Note: Victim Shaming** is a tactical social pressure method used to coerce victim organizations into meeting ransom demands. Black Shrantac's aggressive deployment of this tactic demonstrates that defense teams must move beyond "availability" and prioritize **"data confidentiality"** in their security frameworks.

4. Infrastructure and Panel Management

The group utilizes a decentralized and anonymous infrastructure to coordinate its attacks and manage victim data.

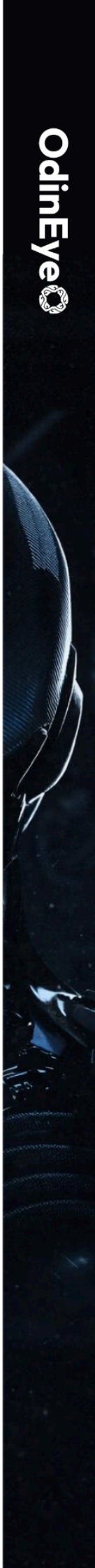
- **Management Portals:** Operators and affiliates gain access to specially designed **TOR-based management panels** to conduct negotiations with victims and update leak lists.
- **Operational Security (OPSEC):** Attackers utilize multiple layers hosted deep within the TOR network to mask their real IP addresses and evade tracking.



5. Operational Strategy and Tactics (TTPs)

Black Shrantac executes the **"Pure Data Extortion"** model with technical mastery, distinguishing itself from traditional ransomware groups. The primary MITRE ATT&CK techniques utilized by the group are as follows:

Initial Access (T1566- Phishing):	The group often gains entry into target networks through sophisticated spear-phishing campaigns.
Lateral Movement (T1021 - Remote Services):	Following the infiltration, attackers spread through the network (**Lateral Movement**) to identify financial data, HR records, and R&D documents, subsequently gathering them in a central location (**staging**).
Data Exfiltration (T1041):	The group's most prominent signature is the transfer of identified data to servers under its control before proceeding to the encryption phase. The cases of **Dem İlaç (1 TB)** and **Rasen İnşaat (400 GB)** prove the group's technical capability to exfiltrate massive volumes of data without detection.



Case Studies

The disclosures made by the Black Shrantac group on its leak site prove that the group has accessed the most sensitive data of its target institutions. The following cases demonstrate the devastating impact of the group's **"Pure Data Extortion"** model.

1. Dem İlaç (demilac, Inc) – Turkey

Operating in the pharmaceutical sector, Dem İlaç represents one of the group's largest-scale data theft cases.

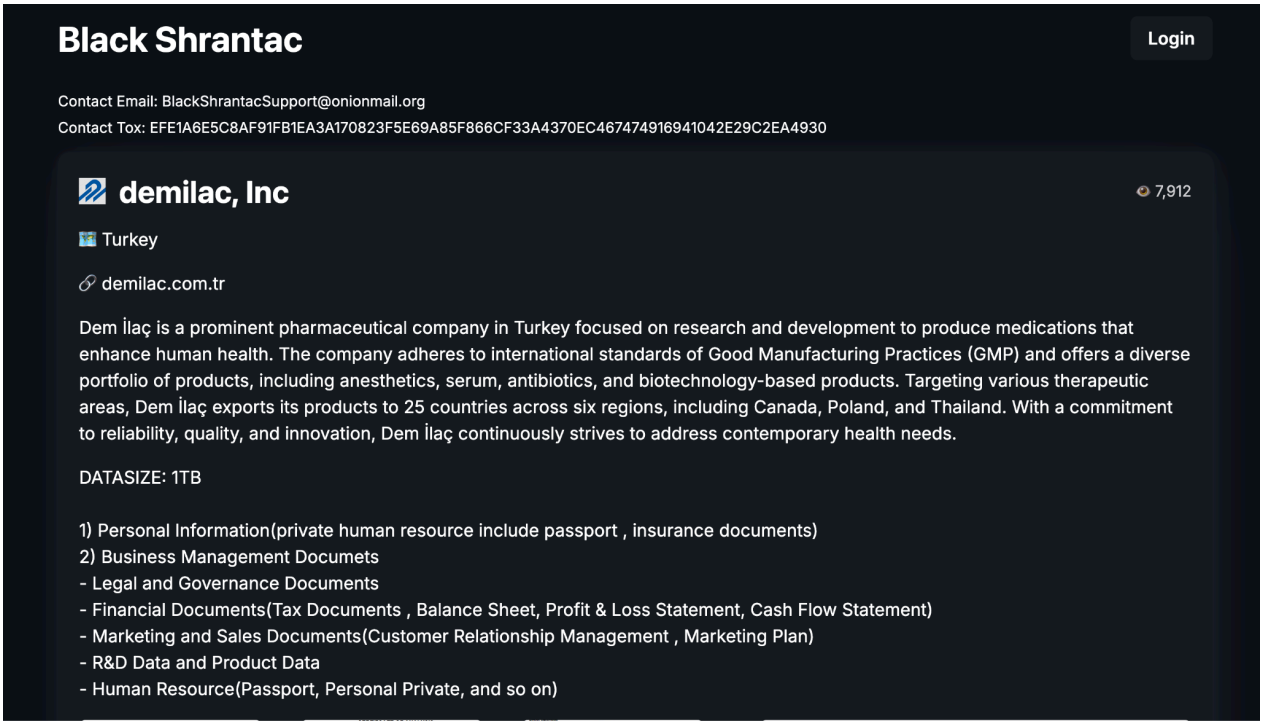


Figure 6: Evidence Documents Belonging to the Dem İlaç Data Leak

Figure 7: Sensitive Personal Data Belonging to Dem İlaç Employees

2. Rasen İnşaat ve Yatırım Ticaret A.Ş. – Turkey

This case in the construction sector demonstrates the significant depth to which the group penetrates internal corporate operations.

- **Leak Size:** 400 GB of data exfiltrated.
- **Critical Findings:**
    - **Internal Communication Database:** In-company email traffic and strategy discussions were compromised.
    - **Employee Data:** Salary information, bonus structures, visa application forms, and severance/compensation records were leaked.
    - **Business Partners:** Access was gained to third-party information, including customer contracts and investor details.
- **Status:** The group's panel currently displays a warning stating **"Company data will be Publish soon,"** indicating that the full dataset is scheduled for imminent public release.

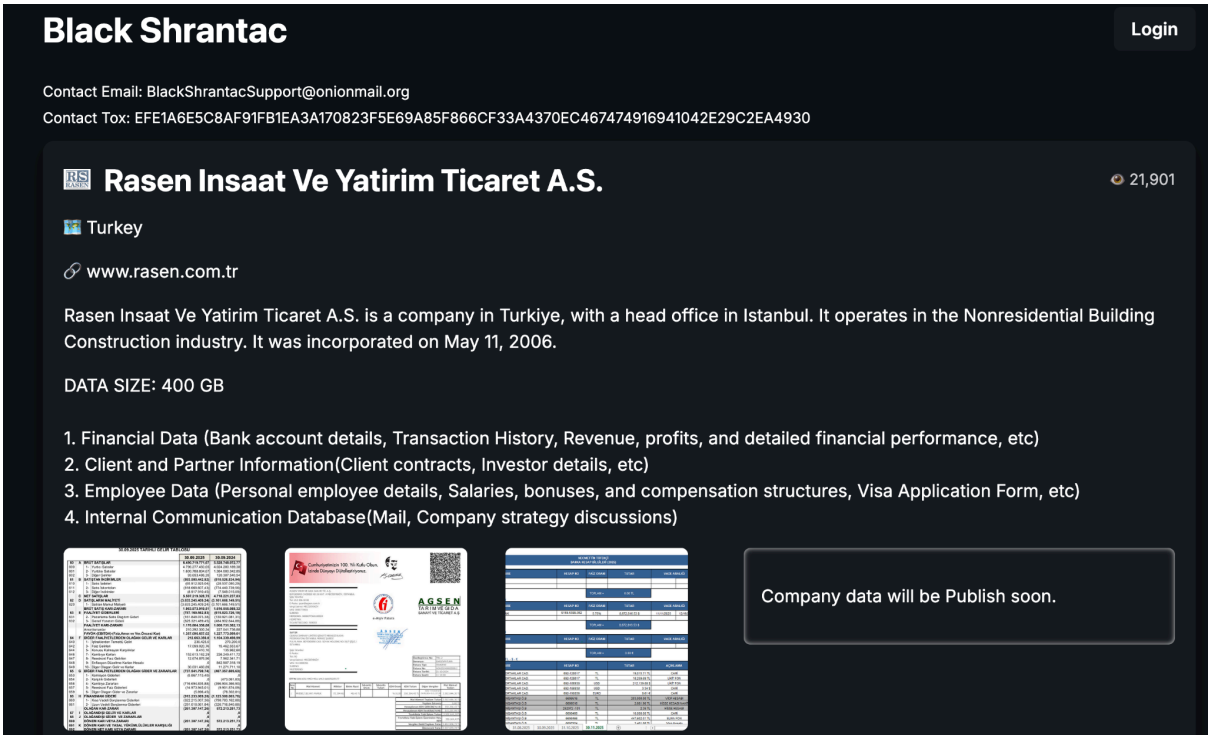
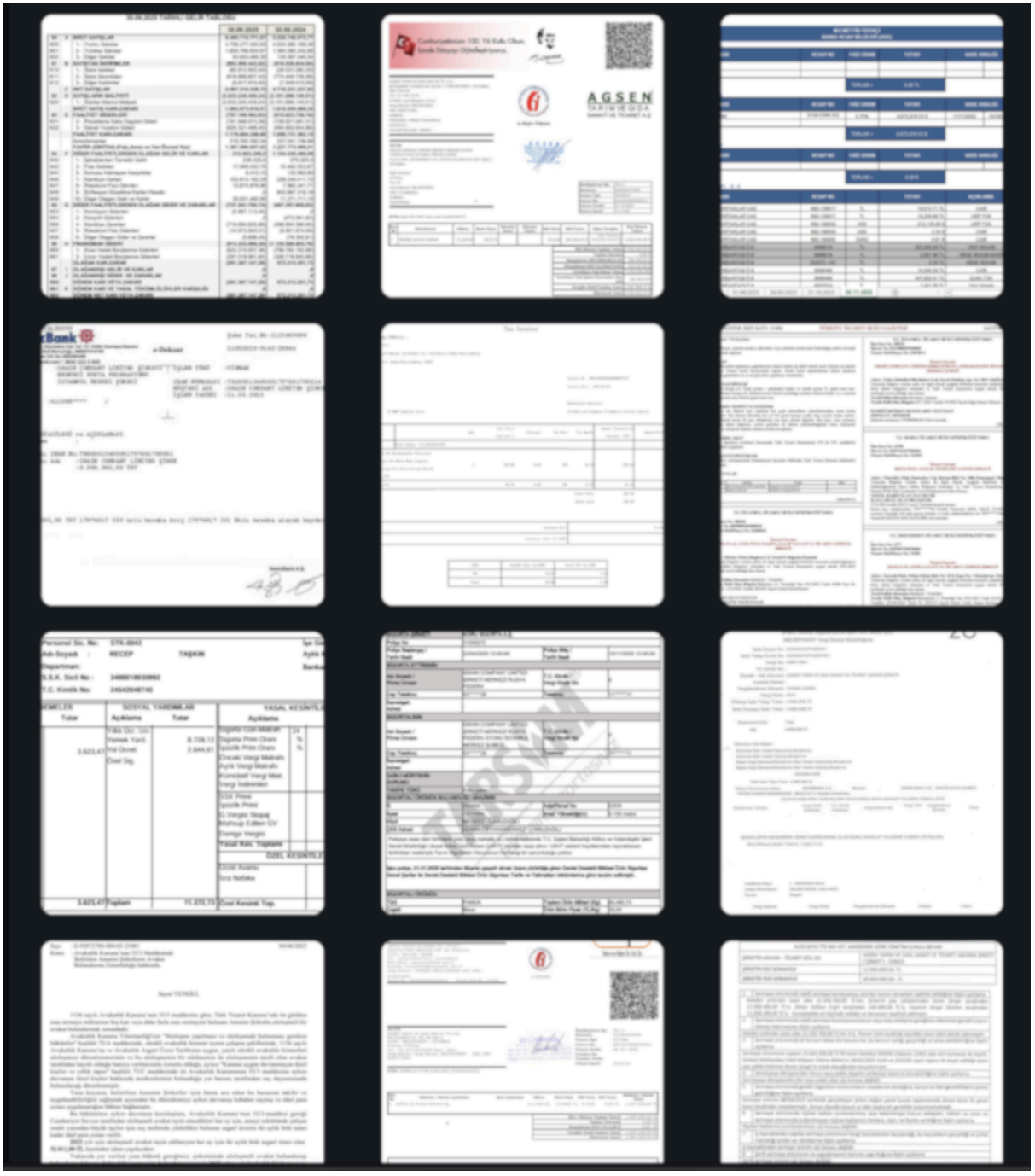


Figure 8: Technical Summary of Rasen İnşaat Data Breach



Figurel 9: Sensitive Corporate Data Belonging to Rasen İnşaat

3. Şimşek A.Ş. (simsekas, Inc) – Turkey

The case of **Şimşek A.Ş.**, a Coca-Cola distributor, demonstrates the group's command over logistics and distribution network data.

- **Leak Size:** 200 GB of data has been compromised.
- **Targeted Content:** Business continuity plans, non-disclosure agreements (NDAs), corporate correspondence (Business Letters), and marketing-sales strategies.
- **Analysis:** The disclosure of this data has the potential to directly damage the company's commercial competitiveness and its supply chain security.

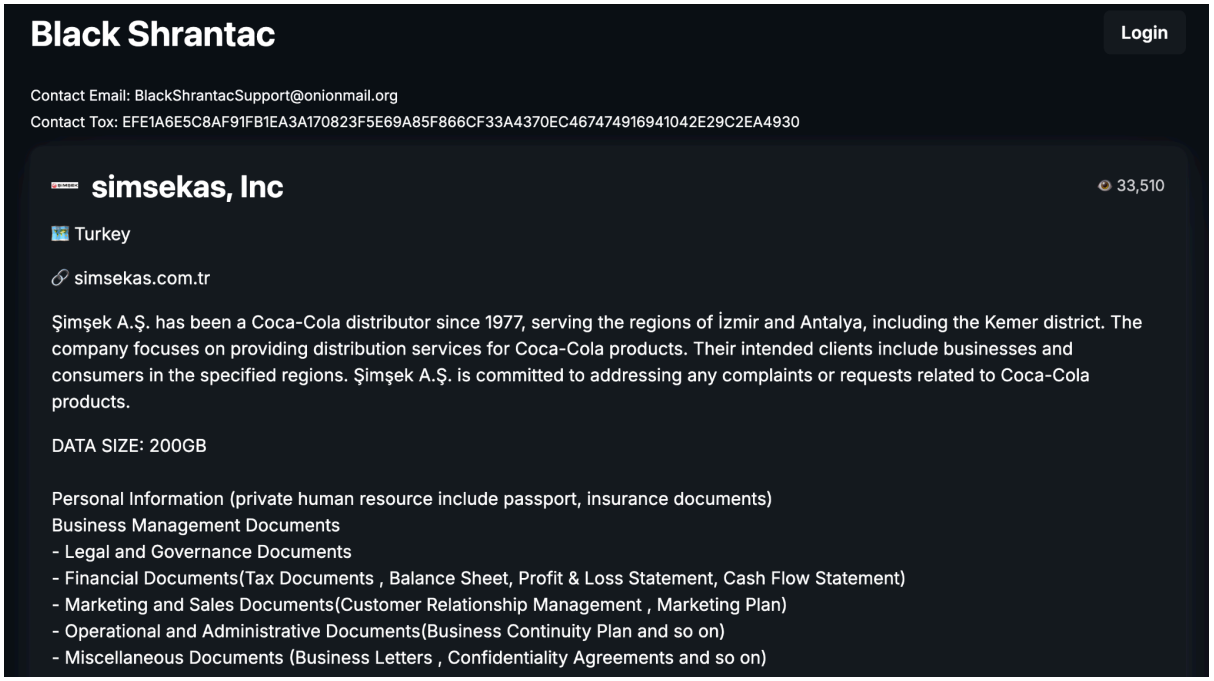


Figure 10: Technical Summary of Şimşek A.Ş. Data Breach

Figure 11: Sensitive Corporate Data Belonging to Şimşek A.Ş.

Figure 12: Sensitive Personal Data Belonging to Şimşek A.Ş. Employees

4. Altaş Temizlik – Turkey

Identified as one of Turkey's leading organizations in urban cleaning and solid waste management, Altaş Temizlik is one of the most prominent victims on Black Shrantac's leak platform. According to data from the group's panel, this case reached significant disclosure traffic with over **52,440 views**.

Leaked Sensitive Data Categories

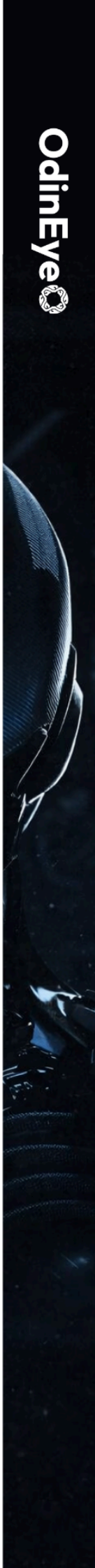
The group disclosed two primary datasets containing both the institution's operational costs and the most private information of its employees:

1. Financial Data (Finance Info):

- Company production costs and detailed invoice records.
- Bank statements, payment lists, and corporate tax declarations.
- The leak images, which specifically feature the **"August 2023 Payment Plan"** and **"Commercial Loans"** breakdowns, indicate that the company's cash flow and debt structure have been completely exposed.
- Employee payrolls and detailed benefit breakdowns.

2. Human Resources Data (HR Information):

- Employment contracts and personnel files.
- Photocopies of driver's licenses (DL).
- The most critical finding includes the **Social Security Numbers (SSN)** and personal identification details of the employees.



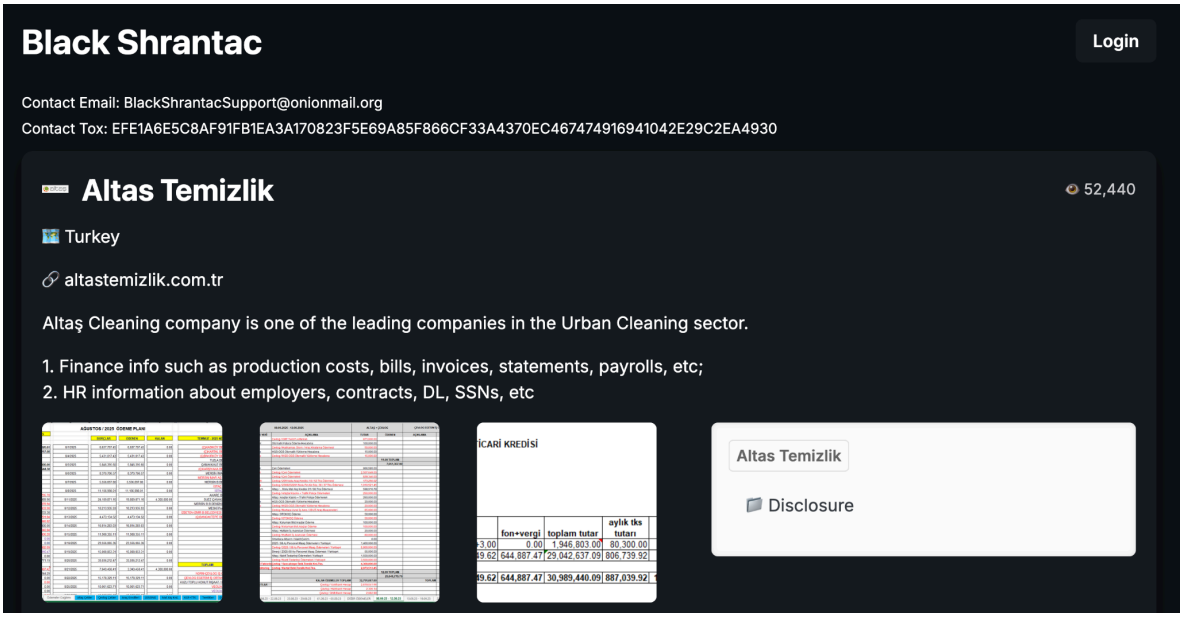


Figure 13: Altas Temizlik Sensitive Corporate Data Leak

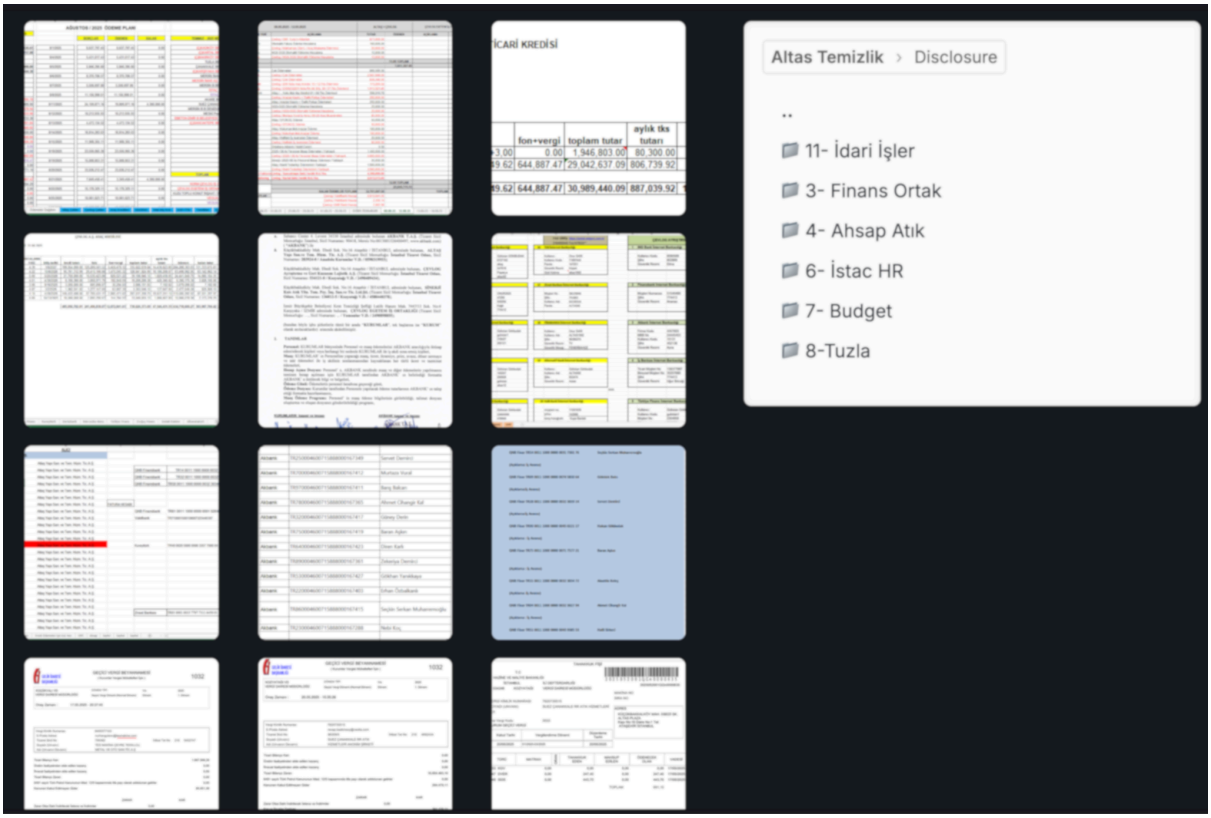


Figure 14: Sensitive Corporate Data Belonging to Altas Cleaning

5. Global Perspective

The operational range of the Black Shrantac group extends far beyond Turkey's borders, spanning five different continents. An examination of the group's leak platform reveals that it has successfully implemented the **"Pure Data Extortion"** model across a wide geographic area, ranging from the Western world to the Asia-Pacific region.

Below is a detailed analysis of the most critical data breaches carried out by the group on a global scale:

A. Oceania and Asia Operations

- **Netstar Australia PTY Ltd:** One of the group's most significant global victims. As a provider of technology and navigation solutions, Netstar suffered a massive **800 GB data breach**. The exfiltrated data is assessed to include core corporate systems and extensive customer databases, posing long-term risks to client privacy and proprietary technology.
- **VFM Systems & Services (P) Ltd (India):** India currently ranks as the second most targeted country by the group. In the VFM Systems case, **70 GB of data** was exfiltrated, focusing heavily on internal IT infrastructure and system integration documentation.
- **Badan Pengelola Keuangan Haji (BPKH - Indonesia):** This attack on a critical public financial institution responsible for Hajj fund management involved the theft of **200 GB of data**. This case underscores that the group does not differentiate between private enterprises and state-backed financial entities, often choosing targets with high social and political sensitivity to maximize extortion pressure.

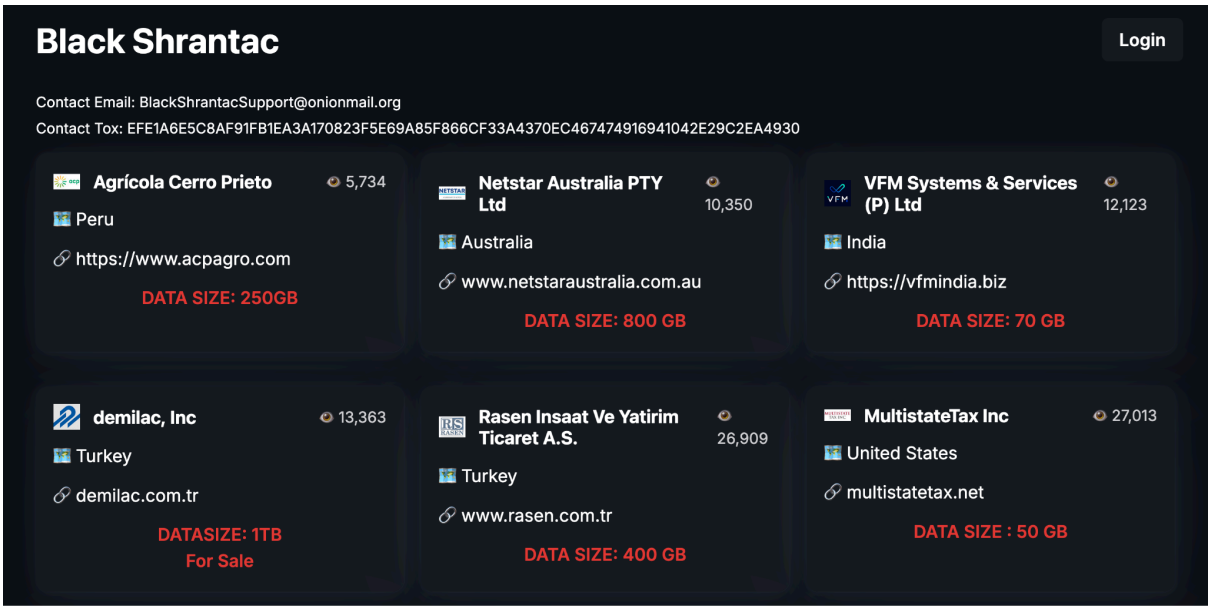
B. North and South America Targets

- **MultistateTax Inc (United States):** The United States remains the most frequently targeted country, with **7 confirmed attacks** by this actor. This specific breach involved **50 GB** of highly sensitive tax and financial consulting data. The exposure of tax records represents a severe risk of secondary fraud and identity theft for the firm's clients.

- **Cabinets 2000, LLC (United States):** This case exemplifies the group's "Business-centric" strategy, where they target mid-to-large scale private enterprises that may hold valuable proprietary data but lack the massive defensive budgets of global conglomerates.
- **Superintendencia Nacional de Fiscalización Laboral (SUNAFIL - Peru):** Representing the group's expansion into the South American market, this attack targeted a regulatory public body. By disclosing official government documents, the group demonstrated a clear intent to disrupt state regulatory functions and compromise institutional trust.

C. Europe and Other Regions

- **M&BM, Inc (Bulgaria):** Operating as a key logistics and service provider in Eastern Europe, M&BM represents the group's foothold in the European market. The breach demonstrates that no region is exempt from their "Pure Data Extortion" campaigns, particularly those with complex supply chain links.
- **Wide Geographical Range:** Verified victim lists and technical analysis confirm that organizations across **Mexico, the Russian Federation, South Korea, the United Arab Emirates, Qatar, Malaysia, and Egypt** are being actively monitored, infiltrated, and extorted by Black Shrantac.



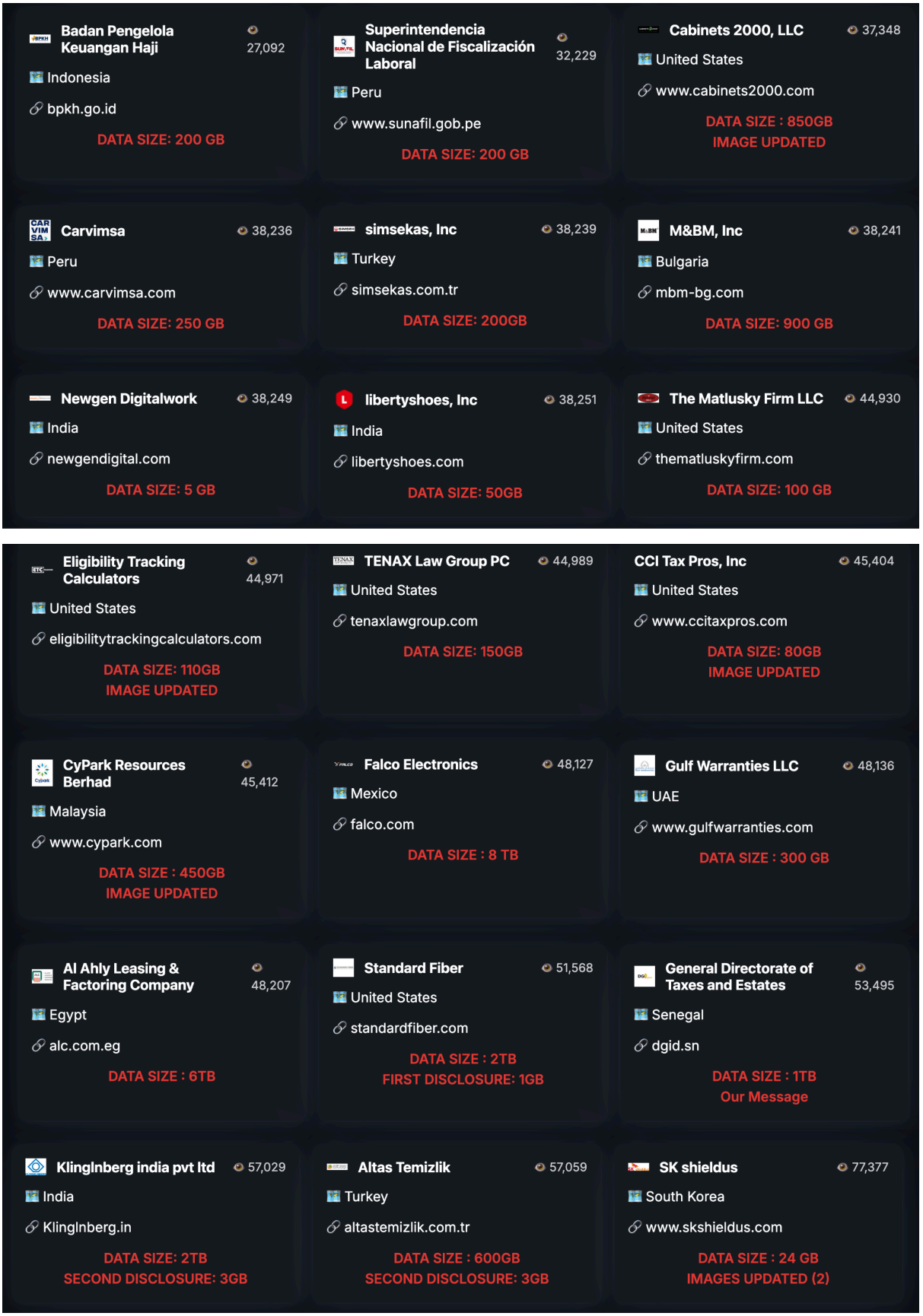


Figure 15: Sensitive Information Exfiltrated by Black Shrantac

Technical Indicators (IOCs)

This section contains the technical data required for security operations centers (**SOC**) and incident response (**IR**) teams to detect, mitigate, and perform retroactive threat hunting for Black Shrantac attacks. The indicators listed below pertain to the group's operational infrastructure and the malware samples utilized during their campaigns. Black Shrantac threat actors leverage anonymous communication channels and hidden services as their primary operational base to evade detection.

URL:	http://b2ykcy2gcug4gnccm6hnrb5xapnresmyjjqgvhafaypppwgo4feixwyd.onion/login
	http://jvkpexgkuaw5toiph7fbgucycvnafaqmfvakymfh5pdxepvahw3xryqd.onion/login
E-POSTA:	BlackShrantacSupport@onionmail.org
TOX ID:	EFE1A6E5C8AF91FB1EA3A170823F5E69A85F866CF33A4370EC467474916941042E29C2EA4930
MD5:	f89aab69e01d21b2c8ce2b8ee9909d25
	42b9f136abd20cfe07cd08a9b1631ea8
	e46f155df70c8a8c4506a2a42425c1a6
	17794ab9e93297365519f0db1c6a8a6d97b7a2c449ee51c4ae4723cf1d18a71e
	b5f90df776e6f57a7fec03f9e325ccf9debe4ddbcc8c385f0bb3edd91ef71927

> **Analyst Note:** Black Shrantac's global case profile indicates that the group employs a **"Sector Agnostic"** (independent of industry) yet **"Data-Centric"** approach. Their focus on navigation data in Australia, public funds in Indonesia, and pharmaceutical R&D data in Turkey demonstrates the threat actor's technical expertise in identifying and exfiltrating the **"crown jewels"**—the most valuable data sets—to inflict maximum damage or coerce the victim into paying a ransom within any compromised network.

Conclusion & Mitigation

Throughout 2025 and into early 2026, **Black Shrantac** has proven to be a sophisticated threat actor capable of bypassing traditional ransomware defense mechanisms through its coordinated operations in Turkey and across the globe. By pivoting from traditional file encryption to directly targeting **"Data Confidentiality"** and aggressively employing **"Victim Shaming"** tactics, the group has demonstrated that organizations require more than just robust backup strategies; they need a comprehensive, data-centric protection architecture.

1. General Assessment

The analyzed cases (**Dem İlaç**, **Rasen İnşaat**, **Şimşek A.Ş.**, **Altaş Temizlik**) reveal that the threat actor has specialized in identifying **"critical data sets"** (such as R&D formulas, financial balance sheets, and passports) capable of extracting the highest possible ransom from every network they infiltrate.

Black Shrantac's ability to exfiltrate **TB-scale data**, particularly from industrial and technology sector victims in Turkey, serves as clear evidence that they are successfully exploiting deficiencies in **internal network visibility** and **Data Loss Prevention (DLP)** protocols.

2. Strategic and Tactical Recommendations

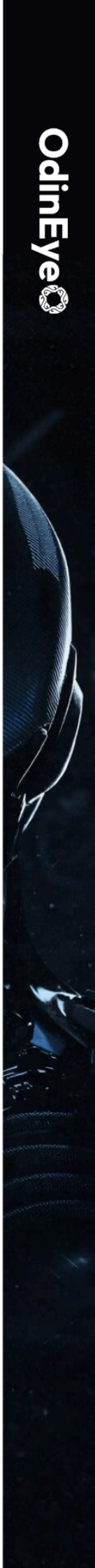
To gain resilience against Black Shrantac and similar "Pure Data Extortion" groups, it is recommended that organizations take the following steps:

Tactical Measures (For SOC and IT Teams):

- **IOC Blocking:** The MD5 hashes, email addresses, and **.onion** domains specified in Section 6 must be immediately blocked across all firewalls and Endpoint Detection and Response (**EDR**) systems.
- **Network Traffic Analysis:** High-volume outbound data transfers—specifically upload activities occurring outside of standard business hours—should be configured to trigger real-time, high-priority alerts.
- **Privileged Account Audit:** Since the group heavily utilizes compromised credentials for **Lateral Movement**, the implementation of Multi-Factor Authentication (**MFA**) must be mandatory for all administrative accounts. Additionally, continuous monitoring for suspicious login patterns and unusual source IPs is essential.

Strategic Measures (For Management and Security Leaders):

- **DLP Integration:** Implement and enforce rigorous Data Loss Prevention (DLP) rules designed to detect and block the exfiltration of sensitive assets, including Personally Identifiable Information (PII), proprietary R&D documents, and scanned passports/ID documents. Policies should be "block-first" for high-sensitivity data classes.
- **Supply Chain Security:** As evidenced by the Şimşek A.Ş. case, attackers often leverage vulnerabilities in the distribution and partner network. Organizations must increase the frequency and depth of third-party security audits, ensuring that vendors and distributors meet the same cybersecurity standards as the parent organization.
- **Employee Awareness & Simulation:** Since spear-phishing remains a primary initial access vector, regular, high-fidelity training and phishing simulations are essential. Staff should be trained specifically to recognize the sophisticated social engineering tactics used to target high-value personnel (HR, Finance, and R&D).



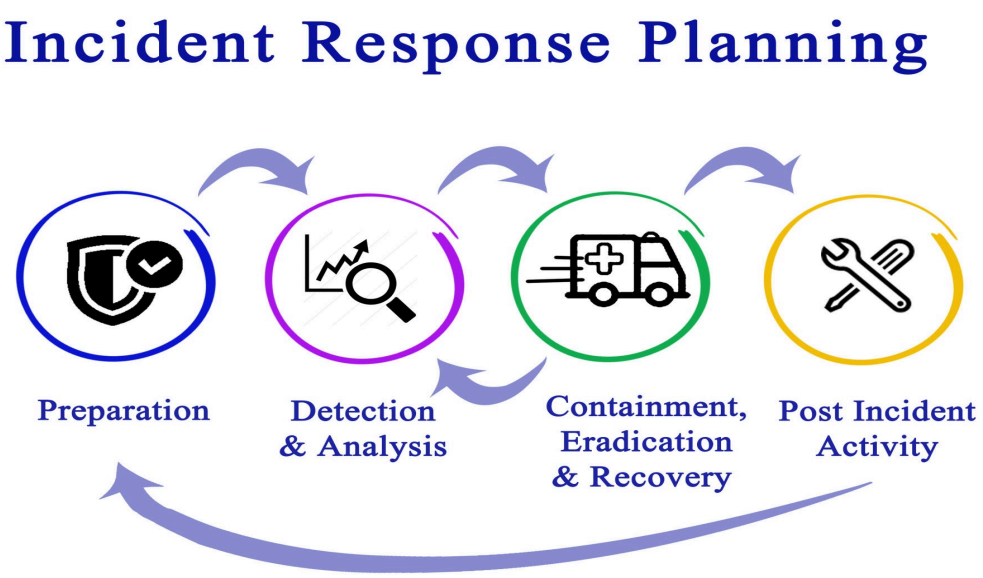


Figure 16: Recommended Incident Response (IR) Planning Cycle Against the Black Shrantac Threat

Black Shrantac is poised to remain a **disruptive force** within the cybercrime ecosystem, leveraging aggressive **"Victim Shaming"** social pressure and the credible threat of selling exfiltrated data to commercial competitors. It is imperative that defense teams adopt a **proactive posture**—informed by the findings and technical indicators in this report—to effectively mitigate risk and minimize the operational impact of potential data breaches.

References

[1] Ransomlook.io. *BlackShrantac Ransomware Group Profile and Monitoring.* url: https://www.ransomlook.io/group/blackshrantac. (Access: 30.12.2025).

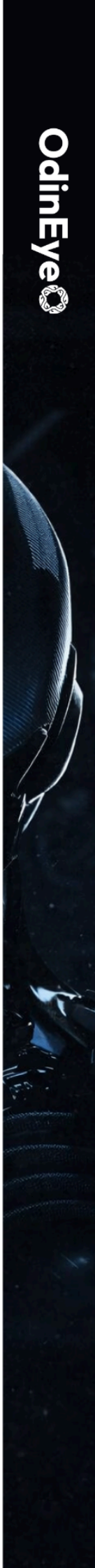
[2] Ransomware.live. *Ransomware Groups Activity and Leak Site Real-time Monitoring.* url: https://www.ransomware.live/. (Access: 30.12.2025).

[3] Hookphish. *Ransomware Group BlackShrantac hits Altas Temizlik (Turkey).* url: https://www.hookphish.com/blog/ransomware-group-blackshrantac-hits-altas-temizlik/. (Access: 30.12.2025).

[4] Dr. Disk Lab. *BlackShrantac Ransomware Grubu Teknik Analiz ve Profilleme.* url: https://drdisklab.com/ransomware-gruplari/blackshrantac. (Access: 30.12.2025).

[5] BlackFog. *Cybersecurity 101: Understanding BlackShrantac Ransomware Operations.* url: https://www.blackfog.com/cybersecurity-101/blackshrantac/. (Access: 30.12.2025).

[6] SOCRadar. *Cyber Threat Intelligence and Dark Web Monitoring Platform.* url: https://socradar.io/. (Access: 30.12.2025).



OdinEye

odineyecti.com
contact@odineyecti.com