GLOBAL LOGISTICS & TRANSPORTATION INDUSTRY Threat Landscape Report



socradar.io



Table of Contents

Executive Summary	3
Technical Details	4
Recent Dark Web Activities Targeting the Logistics Industry	
Ransomware Threats	10
A Closer Look into The Top 3 Ransomware Groups	13
Recent Ransomware Attacks Targeted the Logistics Industry	16
Stealer Log Statistics	18
Phishing Threats	22
Strategic Recommendations	24



Executive Summary

Top Takeaways

- The majority of stealer logs are related to the **Transportation and Warehousing** sector (64.33%), with **FedEx**, **UPS**, **and DHL** leading the list of domains. These global giants face the brunt of cyber threats due to their central role in global trade and logistics.
- The United States (13.72%) stands out as the top target by threat actors, followed by Ukraine and the United Kingdom. The U.S. is a prime focus for attackers due to its vast logistics network, while Ukraine's geopolitical situation has made it a target for state-sponsored cyberattacks.
- **Truck Transportation (59.66%)** is the most targeted sub-sector for ransomware attacks, highlighting the vulnerability of fleet management and logistics coordination systems. **Water and Air Transportation** are also heavily targeted, indicating a broad attack strategy aimed at halting global trade.
- Over 2.28 million credentials and 117K victim IPs have been exposed through stealer malware, indicating widespread compromises of logistics employees' personal or corporate devices. Password hashes and credit card details are also at risk, underscoring the need for enhanced endpoint security and credential management.
- DHL is a frequent target of phishing campaigns, with attackers leveraging tracking and delivery status pages to steal sensitive information.
- While HTTPS (58.22%) is more commonly used in phishing attempts, the use of HTTP (41.78%) remains a significant concern. This underscores the importance of web filtering and user education on secure browsing practices.

Cybersecurity Threats in Transportation and Warehousing





Technical Details

Dark Web Threats

Distribution of Dark Web Threats by Industry



The Transportation and Warehousing sector is the most targeted (64.33%), indicating that cybercriminals prioritize broad supply chain disruptions, likely aiming at third-party logistics providers and warehouse management systems.

Air Transportation (18.31%) follows, likely due to the critical nature of airline operations and valuable passenger/cargo data. Water (9.04%) and Rail Transportation (5.47%) are less targeted but still significant, possibly due to their role in global trade and freight movement.

Truck Transportation (2.50%) and Couriers & Express Delivery (0.36%) face minimal exposure, suggesting lower digital attack surfaces or less financially lucrative data for threat actors.

This distribution highlights the need for enhanced cybersecurity in logistics hubs and supply chain networks, particularly for warehousing and large-scale transport providers.





Distribution of Dark Web Threats by Country

The United States (13.72%) is the most targeted, likely due to its vast logistics infrastructure and the presence of major global supply chain hubs. Ukraine (4.57%) stands out, potentially linked to geopolitical cyber warfare and disruptions in critical transport networks.

This data suggests attackers prioritize major economies and geopolitical hotspots, emphasizing the need for regional cybersecurity collaboration and industry-wide threat intelligence sharing.

	Employ SOCRadar C contours	TOTAL 270					Altra	
	(D) Attack Surface Manager	Employee Leaks OVP Leaks						
Image: marked	Digital Risk Protection	Black Market Botnet Data P	1 Exposure M C	Content Suspicious Content				Credit Cord(s) Detected on Hocker Forum Digital Risk Protection > Fraud Potention > States Credit Cord Detection
Image: Market market Market market market Market market market Market market market market Market market market market Market market market market market Market market market market market market Market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market market	()) Dark hat Hostong	Black Market ID Source	Stealer Log Preview	Related Assets	Price	Status	Obtain Progress	
Image: Section of the section of th	Ry Bond Puterton	Market- Russen Market	Open Preview D		10.00 \$	Action Nation	NEQUEST OF TAN	; 🖾 ष 📮 🐨 🗳
 I Maré giang Maréna Anna Carange Managan Maréna Maréna Anna Anna Anna Anna Anna Anna Anna A	G vit homeon	Market- Presion Market	Open Preview ()	and percent states in the	10.00 \$	Action Matting	NEQUEST OFTAN	í
Control Participante Control Cont	CE Surface Head Mandoorg	Market-presses Review Market	Open Preview 🔁		10.00 \$	Action Walling	REQUEST OFTAN	
Contraction of the second on the secon	(2) DW Configuration	Market-presenting Russian Market	Open Predev 🗋		12.00 \$	Action Walking	REQUEST DETAIN	DETAILS
Martingen Marken (m. March (m. March (m. Margen Marken (m. Ma	(A)	Market-programm Remian Market	Open Predev D	Reparementation and	12.00 \$	Active Walking	REQUEST DETAIN	Following cards are shared on a Hacker Forum. SOCRadar
Image: Section of the section of th	() Cyter Intel Intelprot	Market-(Instantion Research Market	Open Preview 🕃	(rel presentation are	12.00 \$	Action Matting	NEQUEET DEDAN	matched and obtained those cords with your company.
Image: Second processing Name Second processing <td< td=""><td>(m) incidents ></td><td>Market-remember devesis</td><td>Open President 🔁</td><td>No prevalence in the local</td><td>35.00 \$</td><td>Action Waiting</td><td>REQUEST OF THE</td><td>DETECTION & ANALYSIS</td></td<>	(m) incidents >	Market-remember devesis	Open President 🔁	No prevalence in the local	35.00 \$	Action Waiting	REQUEST OF THE	DETECTION & ANALYSIS
Constrained in the second of the second	(G. Aquers	Market- III Market Russian Market	Open Presiev 🕃		20.00 \$	Active Walting	REQUEST CRIMIN	
Austration Sanchard Control Contence Control Control Control Control Control Control Control Cont	90 Settings >	Market-remember Genesis	Open Preview 🕃	the property of the local	20.00 \$	Active Walling	REGUEST CETWN	4
Adde sing A		Market-19756279 Russien Market	Open Presiew 🐧		20.00 \$	Action Waiting	REQUEST CRIMIN	RESPONSE
Addres Stands Stands Northern Company Stands S		Market-Indian Genesis	Proview Not Found	Contract general contracts and	05	False Positive	REQUEST OFTAN	
		Market-Telephone Genesis	Preview Not Found	And the second second second	0.5	Falle Positive	REQUEST OBTAIN	POST-INCIDENT ANALYSIS
		Market-1000000 Russian Market	Open Preview 🕃	desperant date to an	10.00 \$	Action Walling	REQUEST CIRTAIN	
O Mader Sector Auser Mater Operation Sector HL21 Mader Sector Mater Mader Sector 20 × - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -		Market-10000007 Russler Market	Open Preview C	And the second second second	10.00 \$	Action Walting	REDUKST ORTAN	MITIGATION
hemi prape ≥ ∨ Bootg11a.br/seros		Market- Russier Market	Open Preview 🕃		10.00 \$	Action Risking	RECUEST CRIMIN	
		Records per page: 25 . V		<	> >> of 15 entries			



SOCRadar's Advanced Dark Web Monitoring

SOCRadar's Advanced Dark Web Monitoring

provides Spanish organizations with critical insights into hidden threats targeting their sectors, including Retail Trade, finance, and Insurance, which have faced significant risks over the past year. With real-time tracking of underground chatter and sensitive data exposure, SOCRadar enables proactive defense against Dark Web threats.

Activate your <u>free demo today</u> to safeguard your organization's most valuable assets.





Distribution of Dark Web Threats by Threat Categories

The high percentage of Hack Announcements (44.47%) suggests that cybercriminals prioritize publicizing breaches, likely to enhance their reputation, intimidate victims, or attract buyers for stolen data.

Selling (28.54%) and Sharing (26.04%) indicate that logistics-related breaches often lead to data monetization or free distribution of stolen assets, posing risks of credential stuffing, fraud, and supply chain disruptions.

Partnership/Cooperation/Offer (0.59%) and Buying (0.36%) are minimal, implying that direct purchases or collaboration among criminals are secondary compared to selling and exposure strategies.

This trend highlights the need for proactive cyber defense, breach monitoring, and dark web surveillance to mitigate risks before stolen data is exploited.

Is Your Organization Exposed on the Dark Web? Get your free report now and stay ahead of cyber threats: <u>SOCRadar's Free Dark Web Report</u>







Distribution of Dark Web Threats by Threat Types

The dominance of Website-related posts (54.09%) suggests that cybercriminals frequently target or discuss compromised logistics websites, possibly for defacement, phishing, or credential leaks.

Data/Database (29.63%) postings indicate a significant focus on stolen sensitive records, such as customer information, shipment details, or internal logistics systems data.

Access (14.59%) implies that threat actors are actively selling or distributing unauthorized entry points, likely involving compromised credentials, RDP, VPN access, or initial footholds into company networks.

This emphasizes the need for strong website security, data encryption, and access controls to mitigate exposure on dark web forums.



Recent Dark Web Activities Targeting the Logistics Industry

The Alleged Database of a European Airport Transfer Service is Leaked



A threat actor has reportedly claimed responsibility for leaking a substantial database containing sensitive information about an airport transfer service based in a European country. The post, which surfaced on a dark web forum monitored by SOCRadar, allegedly reveals details of customers who utilized the service between 2016 and 2024.

According to the threat actor, the database includes various types of information such as names, surnames, email addresses, phone numbers, the type of transfer (default or VIP), and even timestamps of the bookings. In addition, other details like the origin city, destination, and company names are reportedly included in the data.



The Alleged Database of a Railway Company is Leaked



A threat actor claiming to have obtained sensitive data from a railway company located in Eastern Europe. The alleged leak reportedly involves 570,000 records, which are said to be in JSON format. According to the post, the file is 753MB in size and has been compressed to 35MB.

Dark Storm Team Conducted DDoS Attack on a Port-Shipping & Cargo Company

The post, published on a Telegram channel, purportedly details the group's intention to launch a Distributed Denial of Service (DDoS) attack against the port's digital infrastructure.

The allegations made by the purported hacker, who remains unidentified, suggest that the attack could disrupt operations at the port, which is a key entry point for goods entering into the country.



Ransomware Threats

Distribution of Ransomware Attacks by Industry



Truck Transportation (59.66%) is the primary target, likely due to high dependency on digital fleet management, GPS tracking, and logistics coordination systems. Disrupting these operations can cause severe supply chain delays, making companies more likely to pay ransoms.

Water Transportation (22.69%) and Air Transportation (15.13%) also face significant ransomware threats, reflecting their critical role in global trade and passenger movement. Attacks on these sectors can lead to port shutdowns, flight disruptions, and cargo delays.

Rail Transportation (1.68%) and Couriers & Express Delivery (0.84%) see minimal targeting, possibly due to lower digital integration or stronger resilience measures in these industries.

This distribution suggests that ransomware groups focus on high-impact, high-disruption targets, reinforcing the need for network segmentation, regular backups, and ransomware-specific threat detection in logistics cybersecurity strategies.



Distribution of Ransomware Attacks by Country



The United States (53.85%) dominates ransomware incidents in logistics, likely due to its vast supply chain network, reliance on digital logistics platforms, and high-value targets. The U.S. is a prime focus for ransomware groups seeking large payouts and operational disruption.

Croatia (15.38%) is a surprising second, possibly indicating targeted attacks on critical maritime infrastructure or regional logistics hubs essential for European trade.

The United Kingdom (9.49%) faces steady ransomware threats, reflecting its major role in global shipping, air freight, and supply chain operations.

The heavy U.S. concentration suggests that ransomware groups prioritize wealthier economies with high digital dependency, emphasizing the need for stronger cyber resilience, rapid incident response, and industry-wide collaboration to counter these attacks.





Top Ransomware Groups Targeting the Logistics Industry

The RansomHub (12.5%) group leads in logistics attacks, likely due to its focus on high-value targets and double extortion tactics (data theft + encryption).

Play (8.33%) and Akira (7.5%) follow, both known for aggressive targeting of critical industries and leveraging customized ransomware payloads to maximize disruption.

The "Other" category (71.67%) suggests a diverse threat landscape with many smaller or emerging ransomware groups attacking logistics firms, making detection and mitigation more complex.

This data highlights the need for proactive ransomware defense strategies, including zero-trust security models, network segmentation, and robust incident response planning to counter evolving threats.



A Closer Look into The Top 3 Ransomware Groups

RansomHub



As stated on the group's About page, RansomHub is comprised of hackers from various global locations united by a common goal of financial gain. The gang explicitly mentions prohibiting attacks on specific countries and non-profit organizations. In February 2024, RansomHub posted its first victim, the Brazilian company YKP.

The gang's website states that they refrain from targeting CIS, Cuba, North Korea, and China. While they suggest a global hacker community, their operations notably resemble a traditional Russian ransomware setup. Their stance on Russian-affiliated nations and the overlap in targeted companies with other Russian ransomware groups are also worth noting.

You can visit our <u>blog post</u> for more detailed information about RansomHub.



Play Ransomware



Play Ransomware's main target is the Latin American region, and Brazil is at the top of the list. Even though they seem like a new ransomware group, their identified TTPs resemble the Hive and Nokayawa ransomware families. One of the behaviors that makes them look similar is using AdFind, a command-line query tool capable of collecting information from Active Directory.

Double extortion is a widespread technique in which cyber actors threaten to exfiltrate sensitive data. Play Ransomware also uses double extortion against its victims. They can archive the breached data with WinRAR and then upload it to file-sharing sites.

You can visit our *blog post* to read the rest of the threat actor profile.

SOCRadar	THREAT ACTOR INTELLIGENCE		
🚊 Dark Web Report	KNOW YOUR ENEMY		
© ICC Radar	Know their factics, trethniques, and past activities. Access detailed profiles and track threat actor activities.		NAME OF A DESCRIPTION O
Triveat Reports -	 Nate up very the same results and same is sense. How we have and Procedures (TTPs). Biodifies data based on active theory action is very industry or 		
(e) External Attack Surface	region.		Threat Actor of the Month 🔿
🔆 Threat Actor 🔤	Discover the adversaries targeting your industry		
() CVE Reder	Thread Type Thread Actor Name ()	Sarger Country Sarger Easters	
🔆 Сатраідтя	Thread Action V	Al County (07/27) V Al Social (34/36)	V Char Q Seed
3만 SOC Tools			
() Bunkleed			
Out free access to more toxis true SOONadar		Top Threat Actors	
Access Now	Lezerus Group	Chostwriter	NeNarro057
Company Partners Contact		A 2002	
		(i) II (i)	
	3M 55 25k Audience News IDC	Audience News IDC	S20k 6 D Autience News IOC
	👂 Target Caustries:	Taget Countries	Target Countries (m. Korea, Republic of) Netherlands (m. Korea, Republic of) Poince (m. Korea, Republic of)
	Therpet Sectors: Insulhows - Government - Technology - Energy - Pripping and Legislics -	Darget Sectors: Millary - Torreportation - Toole - Privates - Banks -	Taget Index
	 <i>€</i> Associated Mahayer/Software: <i>€</i> insummerging to the second second	 	ALCERT - MACERE
	Over-sector-control CVM-sector-control CVM-sector-control	O Resent CNTX CNE-2022-38891 CNE-2020-4888 CNE-2022-38891 CNE-2020-4888 CNE-2022-38891 CNE-2008-20250	• 312

SOCRadar enhances cybersecurity measures with its *Threat Actor Intelligence Module*, which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.

Threat Actor Intelligence Module



Akira



Since its discovery in early 2023, Akira ransomware has evolved from a seemingly ordinary addition to the ransomware landscape to a significant threat affecting many businesses and critical infrastructure entities. This evolution and the unique aesthetic of its leak site and communications have drawn attention to its operations.

The ransom group employs a double extortion strategy, first exfiltrating data and then encrypting devices within the targeted network. Payment is then demanded not only for decrypting files but also for preventing the exposure of leaked data.

The Akira ransomware group frequently demands hefty ransoms, primarily targeting large enterprises across North America, Europe, and Australia. The malware typically spreads through targeted threat campaigns using phishing emails or exploiting software vulnerabilities, focusing on industries such as education, finance, manufacturing, and healthcare.

You can visit our *blog post* to read the rest of the threat actor profile.



Recent Ransomware Attacks Targeted the Logistics Industry

RansomHub Targeted a Refrigerated Freight and Logistics Company

About/ Contact/

RansomHub	Home/
<u>. com</u>	
This publication will be made public on 3 PM March 1.	
.com has been breached. Their computer infrastructure has been temporarily locked, and 189 GB of sensitive data (971,778 files) have been extracted.	
Since February 4 , we have engaged in negotiations with the company, yet they have refused to cooperate. Despite multiple opportunities to resolve this matter discreetly, they have chosen to ignore the consequences.	
As a result, Welcompanies.com will now face severe financial and reputational damage. The exposure of confidential files will lead to regulatory investigations, lawsuits, operational downtime, and irreversible loss of trust from clients and partners. The cost of legal action, compliance penalties, and reputational recovery will far exceed the opportunity they had to settle this directly.	
The insurance company responsible for cyber risk coverage, has failed to fulfill its obligations to protect its client. Despite having an active cyber insurance policy, the company took no timely action to prevent data leakage or mitigate damages. Their inaction allowed the situation to escalate, leaving sensitive data at risk and their client in a vulnerable position.	
You can download all files from this publication by clicking \ensuremath{HERE} .	
 Information about extracted files Full Listing (click to download). Full Listing (archived): Listing.zip 3.93 MB 	
2. Chat History (update on 3 PM March 1)	
3. Information about CEO, Co-Owner and Founder 3.1. CEO () Passport: WELLE COPPE	

A (0)

In the ransomhub ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as a refrigerated freight and logistics company based in De Pere, Wisconsin. They specialize in providing temperature-controlled truckload and logistics services across North America.





INCRansom Targets European Airline Companies

In the incransom ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as an airline from Europe.

APT73 Targets APAC Airline Companies 19

In the APT73 ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as an airline from the APAC region.





Stealer Log Statistics

Stealer Log Statistics: Top Domains in the Logistics Industry

	Rail & Truckin	ng Companies	Third-Part & Plat	y Software forms	
	up.c	om	wisetechg	lobal.com	
	CSX.0	com	descart	es.com	
	cn.	са	cargow	ise.com	
	jbhun	t.com	fourkit	es.com	
	knight-sv	wift.com	project	44.com	
Global Lo Transportatio	gistics & n Companies	Freight Fo Supply Chai	rwarding & n Companies	Port & Term	inal Operators
dhl.c	om	flexpo	rt.com	dpwo	rld.com
fedex.	com	expedit	ors.com	global	psa.com
ups.c	om	cevalogi	stics.com	portofrott	erdam.com
maersk	com	dsv.	com		
kuehne-na	agel.com	хро.	com		
cma-cgr	n.com				
hapag-llo	yd.com				

Top Domains in the Logistics Industry







Stealer Logs - Distribution of the Compromised Data

The high volume of exposed credentials (2.28M) suggests that many logistics employees or contractors have compromised devices, likely due to phishing, weak security hygiene, or lack of endpoint protection.

The exposure of 117.2K victim IPs highlights a significant risk of targeted attacks, as threat actors can geolocate users, exploit vulnerabilities, or conduct follow-up intrusions into corporate networks.

39.8K exposed credit cards reveal financial fraud risks, possibly linked to logistics e-commerce platforms, corporate payment systems, or fuel card usage.

This data underscores the urgent need for multi-factor authentication (MFA), endpoint security, and employee cybersecurity awareness training to mitigate stealer malware threats in the logistics industry.





Stealer Logs - Distribution of the Compromised Data by Victim Country

The United States (9.43%) has the highest number of stealer malware infections, likely due to its large logistics workforce and high digital integration in supply chain operations. Employees using infected personal or corporate devices pose a serious risk to enterprise security.

India (7.08%) follows, reflecting its growing logistics sector and large workforce, where cyber hygiene gaps and reliance on personal devices for work could contribute to infections.

Brazil (4.31%) indicates a regional cybercrime concern in Latin America's logistics infrastructure, possibly tied to increasing digital transformation and inadequate endpoint protections.

This distribution suggests that logistics employees across key global markets are frequently compromised, reinforcing the need for strong endpoint protection, network access controls, and phishing-resistant authentication to prevent further data leaks.



SOCRadar's Identity & Access Intelligence Module

SOCRadar's Identity & Access Intelligence Module

can detect stealers on your devices and identify their location, facilitating a secure working environment. Changing passwords without eliminating stealers is insufficient to secure your organization, as it will only provide new passwords to threat actors.





Stealer Logs - Distribution of the Compromised Data by Domains and Sub-Sectors

The top three most searched domains are fedex.com (26.44%), ups.com (24.86%), and dhl.com (22.19%), probably due their global presence and central role in logistics. These companies and their employees likely represent the highest-value targets for stealer malware due to their extensive customer and employee databases.

maersk.com (15.26%) follows, with a notable portion of global container shipping under its belt, making it a valuable target for attackers looking to exploit sensitive shipping or freight data.

hapag-lloyd.com (5.10%) and expeditors.com (1.03%) also attract significant attention, indicating a focus on major international shipping and logistics companies.

The lower percentage for companies like cma-cgm.com (0.94%) and jbhunt.com (0.83%) suggests less exposure.

This data highlights the importance of securing high-profile logistics platforms, particularly in the top global shipping and courier services, to prevent data theft and enhance cybersecurity measures.



Phishing Threats



Phishing Attacks - Distribution by Phishing Page Title

The overwhelming majority of phishing attempts show a "None" (62.39%) or "-" (6.85%) designation for page titles, likely indicating generic phishing pages or attempts to hide the identity of the phishing target. This suggests a high volume of unsophisticated or low-targeted phishing campaigns.

The presence of legitimate tracking and delivery status pages for DHL (3.04%) and general DHL references (2.95%) indicates that attackers are leveraging brand impersonation, with DHL being a key target for phishing campaigns, likely to exploit user trust and gain access to sensitive information such as shipping or customer data.

This data underscores the importance of phishing awareness, verification processes, and protective web filtering systems to safeguard logistics employees and customers from social engineering and credential theft.



Phishing Attacks - Distribution by SSL/TLS Protocol



The data shows that HTTPS (58.22%) is slightly more prevalent than HTTP (41.78%) in phishing attempts, which aligns with the fact that many phishing sites are now using HTTPS to appear legitimate and bypass browser security warnings. This tactic increases the credibility of the phishing pages, making them harder to detect for users.

However, the HTTP prevalence still represents a significant portion, as non-encrypted HTTP pages can easily be identified by security filters and browsers, which may flag them as insecure.

Overall, this highlights that while HTTPS phishing sites are more sophisticated, traditional HTTP-based phishing pages still remain a concern, particularly for organizations lacking web filtering solutions. The trend emphasizes the need for advanced phishing detection systems and education on verifying URLs and secure connections.



Strategic Recommendations

- Enhance Endpoint Security: Implement advanced anti-malware, regular device audits, and employee training on safe browsing practices.
- **Strengthen Phishing Defense:** Invest in phishing detection systems, web filtering tools, and employee training on recognizing phishing attempts.
- Enforce Multi-Factor Authentication (MFA): Apply MFA across critical systems to protect against stolen credentials.
- Fortify Ransomware Defenses: Regularly back up data, segment networks, and develop incident response plans for ransomware attacks.
- Monitor Dark Web Activity: Use dark web monitoring to detect exposed company data early and respond quickly to breaches.
- Collaborate on Cyber Threat Intelligence: Share insights with industry peers and stay informed about emerging threats and new attack vectors.
- Secure Communications and Data: Ensure encryption for sensitive communications and transactions, and train employees on secure data handling.
- **Proactive Vulnerability Management:** Regularly apply patches and conduct penetration testing to address potential system vulnerabilities.
- **Build a Cybersecurity Culture:** Foster ongoing employee training, phishing simulations, and establish clear security policies to ensure a security-first mindset across the organization.s to safeguard sensitive information from cybercriminal exploitation.



SOCRadar provides Extended Threat Intelligence (XTI) that combines: "Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services." SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by 21.000+ companies in 150+ countries

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.



START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.

C Destenants	Inpers	onating Domains	Rogue Mobile Application	s Social Media Risks	Bad Reputation									- 1
	Reputa	ion by Category					History By Y	ear .						-1
OpperFrouger Vetersteten	• 00	MAS REPUTATION ATTRONS 17	6 PHOED HEBSTES 1 STAM 1 ATTORES 8 STATE: 1 BRICKMAN		IN 57 DINROLT 5 DINTPHANAD 9 Presidentia 6	TABLE 2 PUTA: 4	60 60 30 20 10 0	2017	2018	2019 255	0	2021	2022	
C2 Surface Vieto Hankoring			APT 1	PHOHIMUMAA, 1										
Cyber Threat Intelligence										Allina				
Cyber Thread Intelligence	Q s	with								All time	8	×	1 2 0	
Cyber Threat Participante Cyber Threat Participante Space Threat Participante Space Threat Participante	Q s	sarch								All time	a	×	t 😢 n	
B Def Carlgandan Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Carl Trinct Institigence Trinct Institigence Trinct Institigence Trinct Institient Trinst Trinstiti	Q, 5 136	sarch Total Bad Reputati	on							All time	8	×	2 2 m	
Corr Contiguestion Color Thread Prederes Color Thread Prederes Color Thread Prederes Color S Frequents Secrets Secrets Secrets	Q 5 136	arch Total Bad Reputation	on Category	Maintainer	Description	Status	Incident	First Seen	Last Seen	All time Update Frequency	Ci Actions	×	E S Traings	136
Deer Configuration Captur Threat transformer Captur T	Q 9	rarch Total Bad Reputation	on Category PHESHING/MALIALARE	Multiliter	Description	Status Action Walking	Incident .	First Seen 2023-08-21	Last Seen 2023-09-20	All time Update Frequency 24 hours	Cil Actions Eil	×	Featured Filters All Findings	136
Contraction Capture Thread Presidence Capture Thread	Q 8	sarch Total Bad Reputation	on Critigory Preshtoszimaukare APT	Maintainer Staater Staater Silvana	Description ©	Status Action Vitating Action Vitating	beident	First Seen 2023-08-21 2023-07-15	Last Seen 2023-09-20 2023-09-05	All time Update Frequency 24 hours 24 hours	Actions B: B:	×	Featured Filters	136
Deer Configuration Cupler Threat Paralleproce p Cupler Threat Paralleproce p Configuration p Second p Second p	Q 9	arch Total Bad Reputation	on Cangory PHISHING/MALINARE APT ATTACKEPS	Maintainer Grantenser Gater Trans History Transfillation	Description © ©	Status Action Walting Action Walting Action Walting	Incident	First Seen 2023-09-21 2023-07-15 2023-07-08	Last Seen 2023-09-20 2023-09-05 2023-08-07	All time Update Frequency 24 hours 24 hours 24 hours	Actions E2 E2 E2	×	Peatured Filters Al Findings Action Waiting	2 2 136 136
Correctionation Capar Transformation		serch Total Bad Reputation	on Cangory PHSHN02AALMARE APT ATLEXERS PHSHN05	Malatalow Research Option Theorem Hillenson Respect to 10 Research	Cescription 0 0	Status Action Walting Action Walting Action Walting Action Walting	Incident - -	First Seen 2023-08-21 2023-07-15 2023-07-08 2023-06-20	Last Seen 2023-09-20 2023-09-05 2023-08-07 2023-09-04	All time Update Preparay 24 hours 24 hours 24 hours 24 hours 2 hours	Artices E E E E E	× 1	Constant	136
Corr Confusion Confus		serch Total Bad Peputati Rem	on Cangury Presenvity/MALKARE APT ATTACKERS Presenvit Presenvit Presenvit	Malatalwer Senamener Spaler Three Allanes Hangari Lali Mananasi	Cescription 0 0 0 0 0	Status Autor Violing Autor Violing Autor Violing Autor Violing Autor Violing	Incident - - -	First Deen 2923-09-21 2923-07-15 2923-07-08 2923-05-29 2923-05-29 2923-05-62	Last Been 2023-09-20 2023-09-05 20223-09-05 20223-09-04 2023-09-04	All time Update Prequency 24 hours 24 hours 24 hours 2 hours 2 hours 2 hours	Artices 22 23 25 25 25 25 25 25 25 25 25 25 25 25 25	×	Constructed Filters Al Findings Action Waiting Resolved	2 2 136 136 0
D The Configuration Count Transformer Count Transforme		narch Total Bad Peputati	00 Congory PreServiz/AALUARE APT ATTACKERS PreServis PreServis PreServis	Marcaw Reame Spart Intern Ream Ream Ream Ream	Cescription C C C C C C C C C C C C C C C C C C C	Status Altar Maring Altar Maring Altar Maring Altar Maring Altar Maring Altar Maring	Incident - - -	First Dees 2023-09-21 2023-07-15 2023-07-08 2023-07-08 2023-06-02 2022-09-15	Last Seen 2023-09-20 2023-09-05 2023-09-05 2023-09-04 2023-09-04 2023-09-04 2022-10-04	All time Update Prequency 24 hours 24 hours 24 hours 24 hours 2 hours 2 hours 1 day	Artions E E E E E E E E E E E	×	Constructed Filters All Findings Action Waiting Resolved	2 2 136 136 0
E produktion) (i) Guie thread readpoors) (ii) Fockers) (ii) Fockers) (iii) Fockers		arch Total Bed Reputation	on Congony PEGEHNIZ/MALKARE APT ATTACEERS PEGEHNIS PEGEHNIS PEGEHNIS	Mataw Reams Sair Two Ream Ream Ream Ream Ream Ream Ream Ream	Description 0 0 0 0 0 0 0	Satur Altar Malay Altar Malay Altar Malay Altar Malay Altar Malay Altar Malay Altar Malay	Boldert - - - - -	First Been 2023-09-21 2023-07-15 2023-07-08 2023-06-02 2023-06-02 2022-09-15 2022-09-15	Last Seen 2023-09-20 2023-09-05 2023-09-05 2023-09-04 2023-09-04 2023-09-04 2022-10-04 2022-10-04	All time Update Frequency 24 hours 24 hours 24 hours 2 hours 2 hours 1 day 1 day	Artices E E E E E E E E E E E E E E E E E E E	×	Peatured Fitters Al Findings Action Waiting Nesolved Falso Positive	2 0 136 0 0
Correspondence Court Instantingtone Court Instantingtone Courters Courters Courters Courters Courters Courters Courters Courters Courters		arch	on Computy PHISHING/MALINARE APT ATTACERS PHISHING PHISHING PHISHING PHISHING PHISHING PHISHING PHISHING	Mataw Inamo Colo Twa Mano Colo Twa Mano Panano Panano Panano Panano Panano Panano Panano	Description 0 0 0 0 0 0 0 0 0 0	Status Attais Matring Attais Matring Action Watery Action Watery Action Watery Action Watery Action Watery Action Watery	Incident - - - - - - - - - - - - -	First Been 2923-08-21 2923-07-15 2923-07-08 2923-06-00 2923-06-00 2922-06-09 2922-06-09 2922-06-19 2922-06-19 2922-06-19	Last Been 2023-09-20 2023-09-05 2023-09-05 2023-09-04 2022-09-04 2022-19-04 2022-99-18 2022-99-18	All time Update Frequency 24 hours 24 hours 24 hours 24 hours 2 hours 2 hours 1 day 1 day 3 Months	Actions E E E E E E E E E E E E E E E E E E E	×	1 2 m Featured Filters All Findergs Action Walting Resolved False Positive	2 0 136 0 0
E 97 Companies		arch.	or Cangory Preserva.Autobate APT ATTACKERS Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Preserva Prese	Marcaw Russime Grant all Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russime Russi	Description 0 0 0 0 0 0 0 0 0 0 0	Status Albar Mallay Albar Mallay Albar Mallay Albar Mallay Albar Mallay Albar Mallay Albar Mallay Albar Mallay Albar Mallay Albar Mallay	Incident - - - - - - - - - - - - -	First Been 2923-08-21 2923-07-15 2923-07-08 2923-06-20 2923-06-20 2923-06-20 2923-06-20 2923-06-20 2923-06-20 2923-06-21 2922-06-21 2922-06-21	Last Seen 2023-09-20 2023-09-20 2023-09-05 2022-09-05 2022-09-04 2022-09-04 2022-09-04 2022-09-18 2022-09-18 2022-04-21	All time Update frequency 24 hours 24 h	Artors E E E E E E E E E E E E E E E E E E E	×	C Featured Filters All Findings Action Walking Resolved False Fostive	2 2 136 136 0
Der Conjunte Ouer fonsterlangene		arch	or Cengory PEGENROVALIKABLE AFT ATTACESES PEGENRO PEGENRO PEGENRO SMITP MX REPUTATION MMEDINIC	Mataw Kasama Gala Tana Masa Tagata Mataga Mataga Nataga Sanahili sala at ganahili sala at ganahili sala at	Description 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Bakes Action Walking Action Walking Action Walking Action Walking Action Walking Action Walking Action Walking Action Walking Action Walking	Incident - - - - - - - - - - - - -	First Seen 2923-09-21 2923-09-21 2923-07-08 2923-07-08 2923-06-02 2923-06-02 2923-06-02 2922-09-15 2922-04-11 2922-04-11	Last Seen 2023-09-20 2023-09-20 2023-09-05 2023-09-05 2023-09-04 2022-09-04 2022-09-04 2022-09-18 2022-09-18 2022-04-12 2022-04-12	All time Lipidate frequency 24 hours 24 hours 24 hours 2 hours 1 day 1 day 1 day 3 Months 3 Months	Actions Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colored Colore	×	2 A Findage Action Waiting Resolved False Positive	136 136 0
 B Ortunation (a) the threat relations (a) the threat relations (b) the threat relations (c) the threat relations		arch	01 Calapany Pressensitional Annual Annual Art Artacessis Pressensis Pressensis Pressensis Pressensis Pressensis BMTP MK REPUTATION BMTP MK REPUTATION Pressensis	Marcaw Roame Gor Howsthew Paper of M Paper of M Paper of Marca Roam Roam Roam Roam Roam Roam Roam Roa	Description 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Babus Action Valinity Action Valinity Action Valinity Action Valinity Action Valinity Action Valinity Action Valinity Action Valinity Action Valinity Action Valinity	Incident - - - - - - - - - - - - -	First Seen 2923-08-21 2923-07-15 2923-07-08 2923-07-08 2923-06-00 2923-06-00 2923-06-00 2923-06-00 2923-06-00 2922-06-19 2022-06-11 2022-06-11	Last Seen 2022-09-20 2023-09-20 2023-09-05 2023-09-05 2022-09-04 2022-09-04 2022-09-18 2022-09-18 2022-04-21 2022-04-21 2022-04-21 2022-04-12	All time Lipidat Preparay 24 hours 24 hours 24 hours 24 hours 24 hours 2 hours 1 day 3 Months 3 Months 3 Months 3 Months	Actions De De De De De De De De De De De De De	X	5 2 C C C C C C C C C C C C C C C C C C	2 3 136 136 0
E produces ⊕ (due branchespece) ⊕ nomen (€ Aport ⊕ temp) ∳ temp)		Total Bod Reputation	on Congony Personal Advantage APT ATTACKING Personal Personal Personal Personal Personal MITP AK REPUTATION Personal MITP AK REPUTATION Personal Personal Personal MITP AK REPUTATION Personal Personal Personal MITP AK REPUTATION Personal Personal Personal MITP AK REPUTATION Personal Personal MITP AK REPUTATION Personal Personal MITP AK REPUTATION Personal MITP AK REPUTATION MITP AK REPUTATIO	Ketter Reame (per Nearthere Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Reame Re	Description 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Datus Allan Halloy Allan Halloy	Incident - - - - - - - - - - - - -	First Been 2923-08-21 2923-07-15 2923-07-08 2923-07-08 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-06-02 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-07-08 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-09-02 2923-02 292-09-02 2923-02 292-09-02 2923-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02 292-02	Last Been 2023-09-00 2023-09-05 2023-09-05 2023-09-04 2022-09-04 2022-09-04 2022-09-18 2022-09-18 2022-04-21 2022-04-21 2022-04-21 2022-04-12 2022-04-12 2022-04-12	All time Lipidat Preparany 24 hours 24	Artions E2 E2 E2 E2 E2 E2 E2 E2 E2 E2 E2 E2 E2		Image: Control of Con	126 136 0