SINGAPORE Threat Landscape Report



socradar.io



Table of Contents

Executive Summary	3
Technical Details	4
Dark Web Threats	5
Recent Dark Web Activities Targeting the Entities in Singapore	
Ransomware Threats	11
A Closer Look into The Top 3 Ransomware Groups	13
Recent Ransomware Attacks Targeted Entities in Singapore	16
Stealer Log Statistics	19
Phishing Threats	21
DDoS Attack Statistics	23
Lessons Learned: Key Insights and Strategic Recommendations	24



Executive Summary

Top Takeaways

Sector-Specific Targeting:

Retail trade, finance, and information services stand out as the top targeted sectors in Singapore, comprising over 34% of observed incidents. This highlights the heightened cyber risks faced by customer-facing platforms, financial institutions, and organizations managing vast volumes of digital information.

Ransomware Threats:

The manufacturing sector is the primary target of ransomware in Singapore, accounting for 31.58% of reported incidents. Other affected industries include wholesale trade (12.87%) and real estate (11.11%), emphasizing the ransomware threat's reach into both industrial and service-oriented sectors.

Phishing Attacks:

Information services bear the brunt of phishing activity, making up 39.24% of attacks. Public administration (15.23%) and construction (11.71%) follow, signaling a broadened threat landscape where both government and infrastructure-related entities face heightened credential theft risks.

HTTPS Adoption in Phishing:

A striking 82.40% of phishing websites in Singapore now utilize HTTPS, significantly reducing the reliability of SSL indicators as a sign of trustworthiness. The remaining 17.60% still use HTTP, reinforcing the need for advanced detection methods beyond basic browser cues.

Diverse Threat Activity:

Data breaches and database compromises dominate the threat landscape, constituting 59.49% of observed incidents. Access-related threats—including RDP and VPN compromises—account for a combined 23.21%, underlining the continued focus of cyber threat actors on infiltrating internal systems and exfiltrating sensitive data.



Technical Details

This report is based on data collected between January 2024 and April 2025.

In the following chapters, you will be reading about the various aspects of the cyber threat landscape in Singapore.

In the **Dark Web Threats** chapter, we analyze activities from dark web forums, Telegram channels, and other underground platforms where threat actors communicate, trade illicit data, and discuss cyber attack methodologies.

In the **Ransomware Threats** chapter, we present detailed insights into ransomware groups targeting Singaporean entities, including their operational patterns, targeted industries, and attack methodologies.

The **Stealer Logs Statistics** chapter explores credential theft incidents in Singapore. With stolen credentials being a major vector for cyberattacks, this section highlights critical insights into leaked user information and targeted domains.

The **Phishing Threats** chapter examines how threat actors create fraudulent websites to deceive users. By understanding these tactics, organizations can implement effective countermeasures to protect their employees and customers.

Finally, the **DDoS Attack Statistics** section provides an overview of distributed denial-of-service (DDoS) attacks, outlining the intensity and frequency of these threats and their impact on Singaporean organizations.



Cyber Threat Landscape in Singapore



Dark Web Threats

Distribution of Dark Web Threats by Industry



Retail Trade emerges as the most targeted industry, accounting for 12.46% of dark web-related threats.

Finance and Insurance follow closely at 11.85%, reflecting persistent threat actor interest in financial fraud and ransomware schemes.

Information ranks third with 10.03%, emphasizing ongoing risks to data-driven and digitally dependent sectors.

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







Distribution of Dark Web Threats by Post Type

Selling dominates dark web activity at 64.97%, reflecting a thriving underground market for stolen data and illicit access.

Sharing follows at 31.07%, enabling further cyber threats by distributing data, tools, or techniques.

Hack announcements make up 3.95%, often signaling recent breaches and potential follow-up exploitation.



Distribution of Dark Web Threats by Threat Types Data/Database 59,49% Access 14,87% 5,13% Admin Access **RDP** Access 4,62% VPN Access 3,59% Sensitive Data 2,56% Credit Card 2,56% Customer Data 2,05% Website 2,05% DDOS 1,54% Shell Access 1,03% Tools/Service 0,51% 0,00% 10,00% 20,00% 30,00% 40,00% 50,00% 60,00% 70,00%

Data and database compromises dominate the threat landscape with 59.49%, underscoring a major focus on stealing, leaking, and monetizing sensitive information.

Access-related threats follow at 14.87%, reflecting persistent attempts to gain unauthorized entry into internal systems, often through credentials or backdoor sales.

Website-related threats, including mentions of defacement, phishing infrastructure, or malware hosting, account for 2.05%, indicating a smaller yet ongoing threat vector targeting digital platforms.

Lander	
Website Website Table Mathefinite State Stat	
Control C	Forum Credit Card
A for shares Book shares Same shares Sam	
 I have normal problem in the second of the secon	
Nordengies Analysis and the schere is a second in the schere is a	
 Market 10000 Market 100000 Market 1000000 Market 1000000 Market 1000000 Market 1000000 Market 10000000 Market 10000000 Market 10000000 Market 10000000 Market 10000000 Market 1000000000000000000000000000000000000	^
Normal Control (Control (Contro) (Control (Control (Contro) (Control (Contro) (Control (Contro) (OCRador
Image: State of the state o	npany.
Common Marketings Name Market Secondary 2 SERIE Marketings	~
Image: Second	
Markingsing Mark	
Model 2009 Galaxies Name No France 65 Model 2009 Galaxies 1 Model 2009 Galaxies Name No France 65 Model 2009 Galaxies 1 Model 2009 Galaxies Name No France Staticities Galaxies 1 Model 2009 Galaxies Staticities Staticities Staticities Model 2009 Model 2009 Galaxies Staticities Staticities Staticities Model 2009 Model 2009 Galaxies Staticities Staticities Staticities Model 2009 Model 2009 Model 2009 Galaxies Staticities Staticities Staticities Model 2009	Ý
Made Search Se	
Made Same Manakara (andreas) Mage Same Same Same Same Same Same Same Sam	~
Market Hanne Role Con Name Market Hanne Market Hanne Con Name Market Hanne Market Hannet Market Hanne Market Hannet Market Market Hannet Market Market Hannet Market	
Market- Russier Market Oper Preview C. 10.00 \$ Anton Humany RECOURT OF THE	- ((
Revents per page 23 v (C) > 30 Devalues (to D of a Same	



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.



Recent Dark Web Activities Targeting the Entities in Singapore

The Alleged Databases of Several Singaporean Companies are on Sale



SOCRadar has identified a dark web forum post advertising the alleged sale of databases belonging to several Singaporean companies, including an online hotel booking platform, a jewelry store, and a gold store. The post claims the data is available in JSON, CSV, and SQL formats and exceeds 3 million records in total.

The threat actor offers to share samples via Telegram to validate the legitimacy of the leak and mandates the use of escrow for secure transactions. Additionally, the seller promotes access to "newer and more private leaks" from Singapore, suggesting an ongoing targeting of local businesses. The exact origin of the stolen data remains unverified and is only disclosed to trusted buyers.



The Alleged Unauthorized Network Access Sales are Detected for a Singaporean SaaS Company



SOCRadar has identified an alleged unauthorized network access sale on a dark web forum, targeting a prominent Singapore-based SaaS company. The seller claims to offer server-level access, boasting that the victim organization ranks among the top 10 SaaS companies in Singapore, with an annual revenue of approximately \$19 million and operations spanning five countries.

The threat actor has not publicly disclosed the full scope of access or the asking price but is actively seeking buyers. This listing raises concerns about the exposure of enterprise-grade infrastructure and the potential for lateral movement, data exfiltration, or ransomware deployment.



The Alleged Data of Singaporean Citizens are Leaked



SOCRadar has identified an alleged data leak on a dark web forum, potentially impacting Singaporean citizens. The post claims to expose 19,302 user records, including usernames, email addresses, account status, and other profile-related information.

Sample data shared by the threat actor appears to contain structured entries in JSON format, suggesting a breach of a database tied to user account systems. While the source of the leak remains unclear, the availability of samples and the nature of the exposed data raise significant privacy and identity theft concerns for individuals affected by the breach.



Ransomware Threats

Distribution of Ransomware Attacks by Industry



Manufacturing is the most targeted sector for ransomware attacks in Singapore, accounting for 31.58% of incidents, as threat actors exploit its reliance on continuous operations and vulnerable supply chains.

Wholesale Trade follows at 12.87%, suggesting ransomware operators are also focusing on sectors integral to logistics and inventory movement.

Real Estate and Rental and Leasing ranks third with 11.11%, indicating a growing trend of targeting service-based and infrastructure-dependent industries.



SOCRadar's Ransomware Intelligence Module

Explore <u>SOCRadar's Ransomware Intelligence module</u> and gain comprehensive insights with detailed group profiles, MITRE Visualizer, and actionable IOCs. These insights will empower you to stay ahead of evolving threats and enhance your cybersecurity strategy.





Top Ransomware Groups Targeting Singapore

Akira leads ransomware activity in Singapore, accounting for 19.10% of observed incidents, signaling its aggressive targeting across sectors.

LockBit 3.0 follows at 12.36%, maintaining its persistent and global presence.

Black Basta ranks third with 10.11%, reinforcing its role as a significant player in the ransomware ecosystem.

Other active groups include 8base (7.87%) and RansomHub (3.37%), showcasing the diverse and competitive nature of ransomware operations affecting Singaporean organizations.



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



A Closer Look into The Top 3 Ransomware Groups

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.



LockBit 3.0



LockBit 3.0, succeeding LockBit and LockBit 2.0, functions as a Ransomware-as-a-Service (RaaS) entity.

Since January 2020, LockBit has transitioned to an affiliate-based model, employing diverse methodologies to target businesses and critical infrastructure entities. Noteworthy tactics include double extortion and the utilization of initial access broker affiliates, alongside recruitment efforts involving insiders and hacker recruitment competitions.

With over 1,500 victim disclosures on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's cessation. As of the first quarter of 2023, they retain their position as the most prolific group, with over 300 disclosed victims.

You can visit our <u>blog post</u> for more detailed Lockbit 3.0 Ransomware Group information.



Black Basta



Since its emergence in early 2022, Black Basta ransomware has rapidly positioned itself as a high-impact threat group, responsible for hundreds of attacks across various industries worldwide. Its affiliation with the Russian-speaking cybercrime ecosystem and suspected links to the notorious Conti group have elevated concerns within the cybersecurity community.

Black Basta utilizes a double extortion model, exfiltrating sensitive data before encrypting systems to pressure victims into payment. Victims are threatened with public exposure of stolen data via the group's dark web leak site if they refuse to comply.

The group predominantly targets large organizations across sectors such as manufacturing, finance, healthcare, and critical infrastructure, primarily in the United States and Europe. Initial access is often gained through phishing, credential compromise, or by exploiting known vulnerabilities in remote access solutions and unpatched systems.

You can visit our <u>blog post</u> to read the rest of the threat actor profile.



Recent Ransomware Attacks Targeted Entities in Singapore

The New Ransomware Victim of qilin: ACM



SOCRadar has observed a new ransomware victim listing on the Qilin ransomware group's dark web leak site, naming A-ChieveMent Solution (S) Pte Ltd (ACM), a corporate IT solutions provider based in Singapore. The group claims to have compromised the organization's systems and is threatening to leak the exfiltrated data unless their demands are met.

The public listing of ACM by Qilin suggests that the company may have been targeted due to its IT infrastructure capabilities, which could potentially impact its clients and partners if sensitive data is released. As of now, no sample data has been shared, but the threat actor's post indicates that full disclosure may follow in case of non-compliance.





The New Ransomware Victim of Lynx: Planet One

SOCRadar has identified Planet One Pte Ltd as a newly listed victim on the Lynx ransomware group's dark web leak site. The company operates in the Custom Software & IT Services industry and is headquartered in Central Singapore, employing between 250 and 499 people, with an estimated revenue of \$50M to \$100M.

The public listing suggests that Planet One's infrastructure may have been compromised, potentially putting corporate and client data at risk. As of now, no specific details about the stolen data have been released, but the inclusion of the company on Lynx's leak site indicates extortion tactics in progress.



The New Ransomware Victim of 8base: Tan Teck Seng Electric (Co) Pte Ltd

Tan Teck Seng Electric (Co) Pie Ltd Downloaderd: 01.02.2025 Molitich: 01.02.2025 views: 81 Tan Teck Seng Rectric (Co) Pie Ltd, Gunded in 1973. The company specializes in the supply of electrical products, noulding: Seel and Rouble pipes Cable support systems Lighting protection and grounding systems Cable entries and kgs: The main clients are electrical engineering contractors and companies related to the construction industry in Singapore. http://ts.sg/ Comment: We have uplaaded confidential files that will soon fall into the hands of contractors.	
6d 10h 51m 42s	

SOCRadar has detected the listing of Tan Teck Seng Electric (Co) Pte Ltd, a Singapore-based electrical products supplier, as a victim on the 8base ransomware group's dark web leak site. Founded in 1973, the company specializes in the distribution of electrical components such as steel and flexible pipes, cable support systems, lightning protection, grounding systems, cable entries, and lugs.

Serving primarily electrical engineering contractors and construction-related companies in Singapore, Tan Teck Seng plays a key role in the local infrastructure supply chain. The alleged ransomware attack raises concerns over the potential compromise of operational data and business continuity disruptions. As of now, the threat actor has not disclosed specific data samples.



Stealer Log Statistics

Stealer Log Statistics: Top Domains in Singapore

Stealers are a type of tool that collects sensitive data from victims' systems, primarily targeting login credentials, session tokens, and personal information. These logs, often produced by malicious software such as info stealers or keyloggers, can contain detailed information about the websites users visit, their login activities, and the credentials they input. Attackers use stealer logs to harvest credentials, gain unauthorized access to accounts, and orchestrate further attacks, including fraud, identity theft, or lateral movement within a network.

Monitoring and analyzing stealer logs is critical for identifying active threats and understanding attacker behavior, as these logs reveal which platforms are being targeted and how attackers are exploiting victims' data. By tracking these logs, organizations can gain valuable insight into high-risk domains, detect compromised accounts early, and implement targeted defensive measures to mitigate damage.

In order to detect these logs, it is useful to check the most visited domains in a specific country or industry. We analyzed the logs from the following domains in order to identify the leaked credentials that can be used to attack organizations in Singapore.



The graph below showcases the distribution of the compromised user data obtained through Stealer Logs across the highest-traffic domains associated with Singapore.



Stealer Logs - Distribution of the Compromised Data



Email and password combinations dominate the compromised data landscape, with 644,213 records exposed, reinforcing that credential theft remains a primary objective in stealer log campaigns.

Password hashes follow at 151,736, indicating attackers' efforts to reverse or misuse encrypted credentials for unauthorized access.

Victim IP addresses (45,400) and credit card data (26,621) further demonstrate the breadth of sensitive information being harvested and circulated across underground forums.



SOCRadar's Identity & Access Intelligence Module

<u>SOCRadar's Identity & Access Intelligence Module</u> 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.



Phishing Threats

Phishing Attacks - Distribution by Industry



Information Services are the top target of phishing attacks in Singapore, accounting for 39.24% of incidents, reflecting attackers' focus on data-rich environments and digital platforms.

Public Administration follows at 15.23%, indicating growing attempts to compromise government portals and officials through deceptive campaigns.

Construction ranks third with 11.71%, suggesting that even traditionally offline sectors are increasingly vulnerable as they adopt digital tools and workflows.



Phishing Attacks - Distribution by SSL/TLS Protocol



The majority of phishing domains (82.40%) now use HTTPS, underscoring a widespread tactic where attackers mimic legitimate, secure-looking websites to gain user trust. Meanwhile, 17.60% still operate over HTTP, possibly reflecting less sophisticated setups or rapid deployment priorities.

Despite the presence of HTTPS, users should not assume a site is safe. Threat actors increasingly abuse SSL certificates to make phishing sites appear credible. This trend highlights the need for vigilant URL inspection and layered security awareness, rather than relying solely on the padlock icon or HTTPS prefix.



DDoS Attack Statistics

- The peak bandwidth witnessed during a DDoS attack reached 728 Gbps, highlighting a significant capacity from the cyber threats.
- The highest recorded throughput during these incidents was 393.99 Mpps.
- Most DDoS attacks lasted between 81.45 minutes on average.
- 87,382 DDoS attacks were recorded, highlighting the high frequency of cyberattacks and illustrating the general threat landscape for Singapore.



Top DDoS Attack Vectors



Enhance your DDoS defense with <u>SOCRadar's DoS</u> <u>Resilience Free Tool</u>, a sophisticated tool designed to assess and fortify your infrastructure's resilience to DoS attacks.

23



Lessons Learned: Key Insights and Strategic Recommendations

- Singapore's Expanding Threat Landscape: The cyber threat landscape in Singapore continues to evolve rapidly, with multiple sectors including retail, finance, and information services, facing persistent targeting by cyber threat actors. These industries remain attractive due to their reliance on digital platforms and sensitive data.
- Ransomware Threats Targeting Core Infrastructure: Ransomware remains the most disruptive cyber threat, with the manufacturing sector accounting for 31.58% of incidents. The continued activity of groups like Akira, LockBit 3.0, and Black Basta reinforces the urgency for organizations to establish advanced data protection, endpoint monitoring, and rapid response capabilities.
- Rise in Dark Web Exposure: SOCRadar observed a significant number of dark web listings involving Singaporean businesses and citizen data, including database sales, network access offerings, and leaked personal information. These findings suggest ongoing underground targeting campaigns against both corporate and individual digital footprints.
- Credential Theft via Stealer Logs: Singaporean organizations are increasingly impacted by stealer log activity, with over 640,000 leaked email-password pairs identified. Attackers utilize these credentials to orchestrate further intrusions, making multi-factor authentication (MFA) and proactive identity monitoring essential.
- Phishing Attacks Leveraging HTTPS: With 82.40% of phishing websites using HTTPS, traditional browser trust indicators have become unreliable. Information services, public administration, and construction sectors are most impacted, emphasizing the importance of user education and phishing-resistant technologies.
- DDoS Threats Demonstrate High Frequency and Scale: Singapore experienced 87,382 DDoS attacks, with peak bandwidth reaching 728 Gbps. These attacks demonstrate increasing capability among threat actors to disrupt availability, especially via common vectors like DNS amplification and TCP SYN floods.



Strategic Recommendations:

- Leverage Threat Intelligence for Proactive Defense: Continuously monitor dark web platforms and ransomware leak sites to detect early warning signs of targeting. Utilize CTI platforms like SOCRadar to gain visibility into emerging threats.
- Implement Strong Identity and Access Management: Enforce multi-factor authentication (MFA) across all access points and regularly audit user credentials. Detect leaked credentials early using stealer log monitoring tools.
- Enhance Ransomware Preparedness: Conduct regular backup and restore drills, isolate critical infrastructure, and deploy EDR/XDR solutions for early detection. Develop a tested ransomware response plan to minimize operational downtime.
- Strengthen Email Security and Phishing Defense: Use advanced email filtering, DNS-based blocking, and phishing-resistant authentication. Supplement with security awareness training focused on identifying fake HTTPS sites and social engineering.
- Secure Supply Chain and Third-Party Integrations: Evaluate vendor security postures and monitor third-party risks, especially for SaaS providers and IT infrastructure partners.
- Bolster DDoS Mitigation Strategies: Employ cloud-based DDoS protection services, regularly test mitigation systems, and understand common attack vectors to harden exposed assets.
- **Promote Collaboration and Intelligence Sharing:** Engage with national cybersecurity agencies and industry ISACs to share insights, gain broader threat visibility, and improve coordinated response capabilities.

Ready to take action?

Grab your free Dark Web Report now and instantly discover what the dark web knows about your organization!

Free
Dark Web Report
Find out how popular you are on the dark web
With SOCRadar Labs's Dark Web Report, instantly find out if your data has been exposed on dark web forums, black market, leak sites, or Telegram channels.
198.643 Times Dark Web Scan Performed
Email Address / Domain Name



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 V	ear .						-1
OpperFrouger Vetersteten	• 00	MAS REPUTATION ATTRONS 17	6 PHO20 HEBSTS 1 STAM 1 ATTORES 8 STATE 1 BROOMAN		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	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 0 0 0 0 0	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 Frequency 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 Inama Inama Calo Twa Mana Inggo Sala Nama Inama Inama Inama Inama Inama Inama Inama	Description 0 0 0 0 0 0 0 0 0 0	Status Attais Maring Attais Maring Action Warring Action Warring Action Warring Action Warring Action Warring	Incident - - - - - - - - - - - - -	First Been 2923-08-21 2923-07-15 2923-07-08 2923-06-00 2923-06-00 2922-08-09 2922-08-15 2922-08-19 2922-08-19 2922-08-19	Last Been 2023-09-20 2023-09-05 2023-09-05 2023-09-05 2023-09-04 2022-09-04 2022-09-18 2022-09-18 2022-09-18	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.Analizabe APT AFTACKERS Preserva Pres	Marcaw Russime Grant all 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 2023-09-05 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 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	0	Marcaw Roame Gor Howsthew Paper of Marca Paper of Marca 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 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	Lest Been 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 2022-04-21	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 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 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-06-01 2922-07-08 2922-08-02 2922-092-08-02 2922-092-08-02 2922-092-08-02 2922-092-08-02 2922-092-08-02 292-092-08-02 292-092-08-02 2922-092-08-02 292-092-08-02 292-092-08-02 292-092-08-02 292-08-02 292-08-02 292-08-02 292-08-02 292-08-02 292-08-02 292-08-02 292-08-02 292-08-02 292-08-02 292-08-02 292-08-02 292-08-02 202-00	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