COMPUTER FORENSICS AND SECURITY INSTITUTE

CFSI

CFSI.CO

2025 CARIBBEAN RANSOMWARE REPORT

DARK WEB THREAT INTELLIGENCE
RANSOMWARE LEAK SITE MONITORING

21	11	11
ATTACK LISTINGS	THREAT GROUPS	COUNTRIES HIT

PREPARED BY SHIVA PARASRAM

CFSI · JANUARY — DECEMBER 2025

CFSI

Computer Forensics and Security Institute 2025 Caribbean and CARICOM Ransomware Report

Dark Web Threat Intelligence • Ransomware Leak Site Monitoring

January – December 2025

Prepared by: Shiva V.N Parasram
Computer Forensics and Security Institute (CFSI)
www.CFSI.co

Contents

About CFSI

The Computer Forensics and Security Institute (CFSI), registered in 2011, has been a provider of Cyber, Risk, InforSec and MSSP services including but not limited to consultancy, vulnerability assessments, penetration testing, digital forensics, incident response, cybersecurity awareness training, risk management, advanced information security training and MSSP services for the past **15 years** for regional and international clients. CFSI specializes in Red, Blue and Purple Teaming and training in these highly specialized service areas offered by a team of subject-matter experts.

Additional Services offered include:

- Enterprise Cybersecurity Risk and Threat Consultancy
- Risk Consultancy and vCISO Services
- Vulnerability Assessments and Penetration Testing
- Incident Response and Digital Forensics
- Dark Web, Breach and Data Leak Monitoring
- Threat Intelligence and Analysis
- Enterprise Cybersecurity Awareness Training
- Advanced Cyber Security Training as the only Authorized Training Centre (ATC) for EC-Council certifications in the Caribbean (CEH, CHFI, CCISO etc.).
- Free Cybersecurity workshops and webinars under our **CFSI CyberFence** initiative to provide free training (with certificates) to the public - https://www.youtube.com/channel/UCuLa9ZWl3XSRNMSI0lEBPIA

LinkedIn Page - https://www.linkedin.com/company/cfsi-cybersec

Web: www.CFSI.co

CFSI Service Catalogue: Download the Service Catalogue here. MSSP Services to be added soon.

About the Author

Name: Shiva V.N Parasram. (https://www.linkedin.com/in/shiva-parasram/)
Title: Vaayu's Daddy, Enterprise Risk Consultant, Penetration Tester, Forensics Investigator, Senior Cybersecurity Lecturer, Certified EC-Council Instructor, Author, Dark Web and Ransomware Researcher and owner of the Computer Forensics and Security Institute (CFSI).
Certifications: MSc Network Security (Anglia Ruskin, UK), CCISO, C|RAGE. CEH, CHFI, ECSA, CCNA, MCSA, CND, CTIA, ISC2 CC, Security+, Network+, A+.

Publications:

- Digital Forensics with Kali Linux 3rd Edition – Packt Publishing - 2023
- Digital Forensics with Kali Linux 2nd Edition – Packt Publishing - 2020
- Kali Linux 2018: Assuring Security by Penetration Testing - 2018
- Digital Forensics with Kali Linux 1st Edition – Packt Publishing - 2018

Certified EC-Council Instructor for the following international certifications:

Shiva Parasram is the only **Certified EC-Council Instructor (CEI)** in the Caribbean for the following courses. CFSI is also the only EC-Council **Authorized Training Center (ATC) in the Caribbean.**

- Certified Chief Information Security Officer (CCISO)
- Certified Responsible AI Governance & Ethics Professional (C|RAGE)
- Certified Ethical Hacker (CEH)
- Computer Hacking Forensics Investigator (CHFI)
- Certified Threat Intelligence Analyst (CTIA)
- Certified Network Defender (CND)

1. Executive Summary

This report is the third annual CFSI Caribbean and CARICOM Ransomware Report, compiled through continuous monitoring of over 100 ransomware group dark web leak sites throughout 2025. The report documents ransomware attacks where Caribbean and CARICOM organizations were listed as victims by ransomware threat actors on their official leak pages.

In 2025, the Caribbean experienced an unprecedented escalation in ransomware activity. A total of 21 confirmed ransomware attack listings were recorded against organizations operating across 11 Caribbean countries and territories, representing a significant increase from previous years. Attacks were carried out by 11 distinct ransomware groups, with the Qilin ransomware group emerging as the dominant threat actor in the region, responsible for 8 of the 21 listings.

Key findings for 2025 include the following: every month from February through December 2025 recorded at least one Caribbean ransomware attack listing; Barbados was the most targeted country with involvement in 9 attack listings; the finance, real estate, and government sectors were the most frequently targeted; and the majority of attacking groups operate under a Ransomware-as-a-Service (RaaS) model, lowering the barrier to entry for cybercriminals.

Globally, ransomware activity surged throughout 2025. Monthly publications grew from 546 in December 2024 to approximately 800 in October 2025. The number of active ransomware groups monitored increased from 53 to over 84 during the same period, with dozens of new groups emerging throughout the year.

Important Note: The victims listed in dark web leak publications are typically organizations that chose not to pay the demanded ransom. The actual number of ransomware attacks in the Caribbean is likely significantly higher, as many victims which pay ransoms typically do not publicly disclose incidents and are not published on dark web leak sites and forums as victims. Additionally, several Caribbean nations lack mandatory breach notification legislation, making comprehensive tracking difficult.

2. Methodology

This report was compiled through systematic, ongoing monitoring of ransomware group dark web leak sites (also referred to as Dark Web Leak Sites or DWLS) throughout 2025. The researcher monitored over 100 groups of which there were at least 80 active ransomware group leak pages, on a regular basis, documenting all publications and listings involving Caribbean and CARICOM-based organizations.

Data collection involved recording the ransomware group name, victim name, date of listing, country of operation of the victim, industry sector, and publication status. No victim data was downloaded, saved, or shared at any point during this research. All screenshots referenced were taken directly from official ransomware group leak sites on the dark web for documentation purposes only.

Organization names have been intentionally omitted from this report to protect the identity of victims, as the purpose of this report is to raise awareness of the ransomware threat landscape in the Caribbean rather than to expose individual organizations. CFSI and the researcher make no assumptions on the security posture of the victims.

The global ransomware statistics presented in this report (monthly publication counts and group counts) are based on the researcher's direct monitoring and may differ slightly from other sources due to differences in counting methodology, particularly regarding groups such as Babuk-Bjorka which frequently re-listed publications from other groups.

3. 2025 Caribbean Ransomware Attack Listings

The following table documents all 21 confirmed ransomware attack listings involving Caribbean and CARICOM organizations during 2025. Organization names have been omitted to protect victim identity.

#	Month	Threat Group	Country / Countries	Industry Sector
1	February	**SafePay**	Jamaica	Distribution
2	March	**Akira**	Bahamas	Transportation, Real Estate, Corporate Advisory & Publishing
3	March	**Rhysida**	British Virgin Islands	Government / Public Sector
4	March	**KillSec3**	Cayman Islands	Finance
5	March	**RansomHub**	Jamaica	Finance
6	April	**Lynx**	Barbados, Jamaica & Trinidad and Tobago	Fast Food & Restaurant
7	April	**Qilin**	Barbados	Tourism & Hospitality
8	May	**SafePay**	Jamaica	Retail Tech & Printing
9	June	**Weyhro**	Trinidad & Tobago, Barbados, Grenada & St. Lucia	Real Estate
10	June	**Qilin**	Barbados	Public / Government
11	July	**Qilin**	Barbados	Marine / Tourism
12	July	**Qilin**	Barbados	Financial & Consulting
13	July	**Qilin**	Curacao	Financial & Investment

14	August	**Akira**	Guyana	Agriculture / Export
15	August	**Qilin**	Trinidad & Tobago	Finance
16	September	**Medusa**	Trinidad & Tobago	Government Research
17	September	**Qilin**	Aruba	Utility / Critical Infrastructure
18	October	**Play**	Bahamas	Retail
19	November	**Qilin**	Barbados	Business Solutions
20	November	**SafePay**	Barbados	Electrical
21	December	**Lockbit5**	Trinidad & Tobago, Barbados, Grenada & St. Lucia	Real Estate

Note: *Additional attacks occurred in the Caribbean during 2025 that were not listed on dark web leak sites. These incidents demonstrate that the 21 listed attacks represent only a portion of actual ransomware activity in the region.*

4. Analysis by Country / Territory

Ransomware attacks in 2025 impacted organizations across 11 Caribbean countries and territories. Some attacks affected organizations operating in multiple countries simultaneously, resulting in counts that exceed the total of 21 individual listings.

Country / Territory	Number of Attack Listings
Barbados	9
Trinidad and Tobago	5
Jamaica	4
Bahamas	2
Grenada	2
St. Lucia	2
British Virgin Islands	1
Cayman Islands	1
Curacao	1
Guyana	1
Aruba	1

Key Country Observations

- **Barbados** was by far the most targeted Caribbean country in 2025, appearing in 9 of the 21 attack listings. Qilin alone was responsible for 5 attack listings targeting Barbadian organizations across tourism, government, marine, finance, and business solutions sectors. SafePay, Lynx, Weyhro, and Lockbit5 also targeted Barbados.

- **Trinidad and Tobago** was the second most targeted, appearing in 5 listings. Attacks came from Lynx, Weyhro, Qilin, Medusa, and Lockbit5, targeting sectors including fast food, real estate, finance, and government research.

- **Jamaica** saw 4 attack listings from SafePay (2), RansomHub, and Lynx, primarily targeting the distribution, finance, and restaurant sectors.

- **Bahamas** experienced 2 attacks from Akira and Play, targeting transportation and retail sectors respectively.

- **Curacao** was hit by Qilin in the financial sector, plus an additional unreported ransomware attack on the Curacao Tax Office in July by an undisclosed group.

- **New targets in 2025** included Aruba (Qilin targeting a utility company / critical infrastructure), Guyana (Akira targeting agriculture/export), British Virgin Islands (Rhysida targeting government), and Cayman Islands (KillSec3 targeting finance).

5. Analysis by Threat Group

11 distinct ransomware groups were responsible for the 21 Caribbean attack listings in 2025. The vast majority operate under a Ransomware-as-a-Service (RaaS) model, where the group provides ransomware tools and infrastructure to affiliates who carry out attacks in exchange for a percentage of ransom payments.

Ransomware Group	Caribbean Listings	Model
Qilin	8	RaaS
SafePay	3	RaaS
Akira	2	Team-based
Rhysida	1	RaaS
KillSec3	1	RaaS
RansomHub	1	RaaS
Lynx	1	RaaS
Weyhro	1	RaaS
Medusa	1	RaaS
Play	1	RaaS
Lockbit5	1	RaaS

Qilin — The Dominant Caribbean Threat

Qilin was the single most active ransomware group targeting the Caribbean in 2025, accounting for 8 of the 21 listings (38%). Qilin held the global number one spot for ransomware publications for six consecutive months from June through November 2025, with over 1,000 victims listed globally since 2022.

- First emerged in mid-2022 as the Agenda ransomware group before rebranding to Qilin.
- Operates under a RaaS model where affiliates receive 80–85% of ransoms.
- Ransom demands can reach as high as $50 million USD.
- Caribbean countries targeted: Barbados (5), Curacao (1), Trinidad and Tobago (1), Aruba (1).
- Industries targeted in the Caribbean: Tourism, Government, Marine, Finance, Consulting, Utility/Critical Infrastructure, and Business Solutions.

- Known to gain initial access via compromised credentials, spear phishing, and exploitation of Citrix, RDP, and Veeam (CVE-2023-27532) vulnerabilities.
- Also utilizes VPN brute-forcing and has exfiltrated data via Bluetooth in some cases.
- Deletes logs before encryption and can disable threat protection tools.
- Uses AES-256 CTR and ChaCha20 encryption with RSA-4096 key encryption.
- In May 2025, Qilin began offering legal services to affiliates as part of their RaaS program, a first among ransomware groups.

SafePay

SafePay was responsible for 3 Caribbean listings (Jamaica twice, Barbados once). First seen in late October 2024, SafePay has listed over 350 victims globally. SafePay targets distribution, retail tech, and electrical sectors in the Caribbean.

Akira

Akira contributed 2 Caribbean listings targeting the Bahamas and Guyana. Active since March 2023, Akira is not a traditional RaaS group but rather a team of highly skilled individuals possibly linked to the defunct Conti ransomware group. Akira uses double extortion, targeting both Windows and Linux systems with a focus on VMware ESXi hypervisors. Ransom demands typically range from $200,000 to over $1 million. Notably, Akira made headlines in early 2025 for deploying ransomware after compromising a webcam on a target network.

Other Notable Groups

- **Rhysida:** Targeted the British Virgin Islands, selling access to 240GB of stolen government data (passports, IDs) for 5 BTC (~$480,000). First seen May 2023, famous for attacking the British Library.
- **KillSec3:** Listed a major financial institution in the Cayman Islands. Spawned from KillSec2 which operated between October 2023 and 2024. Offers services including penetration testing and DDoS via their dark web site.
- **RansomHub:** Hit a financial institution in Jamaica. One of the top global ransomware groups since inception in February 2024, operating as a RaaS.

- **Lynx:** Targeted a fast food and restaurant company with operations across Barbados, Jamaica, and Trinidad and Tobago. Not a stranger to the Caribbean, having previously listed a Caribbean company in August 2024.
- **Weyhro:** A lesser-known but emerging RaaS group first seen in December 2024. Targeted a real estate company operating across Trinidad and Tobago, Barbados, Grenada, and St. Lucia. Uniquely, Weyhro publishes an analysis report of exfiltrated data for each victim.
- **Medusa:** Listed a government research facility in Trinidad and Tobago with a $100,000 USD ransom demand. First spotted mid-2021, Medusa is known for being more public than other groups, maintaining active social media on Telegram, Facebook, and X.
- **Play:** Hit a retail company in the Bahamas. Also known as PlayCrypt, with over 1,000 victims globally since late 2022. Targets Latin America heavily.
- **Lockbit5:** Listed a real estate organization operating across Trinidad and Tobago, Barbados, Grenada, and St. Lucia (the same organization previously targeted by Weyhro). Lockbit5 appeared in late 2025 as a possible continuation of the Lockbit legacy after law enforcement disrupted LockBit operations in February 2024 during Operation Chronos.

6. Analysis by Industry Sector

Caribbean ransomware attacks in 2025 targeted a broad range of industries, demonstrating that no sector is immune. Financial services and real estate were the most frequently targeted sectors.

Industry Sector	Number of Listings
Finance	3
Real Estate	2
Distribution	1
Transportation, Real Estate, Corporate Advisory & Publishing	1
Government / Public Sector	1
Fast Food & Restaurant	1
Tourism & Hospitality	1
Retail Tech & Printing	1
Public / Government	1
Marine / Tourism	1
Financial & Consulting	1
Financial & Investment	1
Agriculture / Export	1
Government Research	1
Utility / Critical Infrastructure	1
Retail	1
Business Solutions	1
Electrical	1

The diversity of targeted industries is notable and concerning. Beyond traditional high-value targets like finance and government, threat actors also went after tourism and hospitality, agriculture and export, utility and critical infrastructure, marine tourism, retail, electrical services, and business solutions providers. This breadth of targeting suggests that Caribbean organizations across all sectors should consider themselves potential targets.

The attack on a utility company in Aruba (Qilin, September) is particularly concerning as it represents a direct threat to critical infrastructure. Disruption of utility services can cascade across other sectors including health, finance, and daily life, especially in island economies that often depend on single service providers.

7. Global Ransomware Landscape — 2025 Context

The Caribbean ransomware threat exists within a broader global context of rapidly escalating ransomware activity throughout 2025. The following table summarizes monthly global ransomware publication statistics as tracked by CFSI.

Global Trends Observed in 2025

- **Explosion of new groups:** Dozens of new ransomware groups emerged throughout 2025, with the total number of monitored groups growing from 53 in December 2024 to over 84 by November 2025. New groups appeared nearly every month, including FunkSec, Frag, NightSpire, CrazyHunter Team, VanHelsing, Weyhro, Satanlock, Devman, Nova, Beast, and many others.
- **Qilin dominance:** Qilin seized the global number one position in June 2025 and held it through November 2025 (at minimum), replacing RansomHub and Clop which had previously led. Qilin listed approximately 720+ victims between 2023 and 2025.
- **Clop's massive campaign:** In early 2025, Clop (TA505) conducted a massive campaign exploiting Cleo file transfer vulnerabilities (CVE-2024-50623 and CVE-2024-55956), listing 304 companies in February 2025 alone.
- **Lockbit evolution:** Despite law enforcement disruption in February 2024 (Operation Chronos), LockBit released version 4.0 in February 2025 with new capabilities including a 'Quiet Mode.' By late 2025, Lockbit5 appeared with a new leak site, though its infrastructure may have already been exposed.
- **Law enforcement actions:** The 8base ransomware group was disrupted under Operation Phobos Aetor with 4 arrests. A Lockbit developer was extradited to the United States on charges related to extracting at least $500 million in ransomware payments.
- **Double listing phenomenon:** Throughout 2025, multiple instances were observed where different ransomware groups listed the same victims. Groups such as Babuk-Bjorka frequently re-listed publications originally posted by other groups.
- **RaaS model dominance:** The vast majority of active ransomware groups in 2025 operated under a Ransomware-as-a-Service model, enabling rapid scaling of attacks by allowing affiliates to use established tools and infrastructure.

8. Key Observations and Caribbean-Specific Trends

Sustained Monthly Attack Cadence

For the first time, the Caribbean experienced at least one confirmed ransomware attack listing in every single month from February through December 2025. This 11-month streak demonstrates that ransomware attacks on the Caribbean are no longer sporadic events but a persistent, ongoing threat.

Repeat Victimization

At least one organization was targeted by two different ransomware groups in 2025: a real estate company operating across Trinidad and Tobago, Barbados, Grenada, and St. Lucia was first listed by Weyhro in June and then by Lockbit5 in December. This pattern of repeat targeting highlights that a previous ransomware incident does not preclude future attacks, and may in fact make an organization a more attractive target.

Barbados Under Siege

Barbados emerged as the most heavily targeted Caribbean nation in 2025, involved in 9 of 21 attack listings. Qilin alone targeted Barbadian organizations 5 times between April and November across multiple industries. This concentration of attacks suggests either specific targeting interest or potentially systemic vulnerabilities within the Barbadian digital landscape that multiple threat actors are exploiting.

Critical Infrastructure at Risk

The September 2025 Qilin attack on a utility company in Aruba marked a troubling escalation, as it targeted critical infrastructure that entire populations depend on. Qilin explicitly stated that total disruption of services was possible. For small island developing states where single providers often serve entire populations, such attacks could have devastating cascading effects across healthcare, finance, and daily life.

Government Sector Under Threat

Government and public sector organizations were targeted in multiple countries including the British Virgin Islands (Rhysida), Barbados (Qilin), Trinidad and Tobago (Medusa), and several unlisted incidents including the Curacao Tax Office, Jamaica's Registrar-General, and the University of the Bahamas. The theft and sale of citizens' personal data, including passport biodata and national ID information, poses severe national security and privacy risks.

Lack of Breach Notification Legislation

The absence of mandatory breach notification legislation in many Caribbean jurisdictions continues to hamper accurate assessment of the true scope of ransomware activity. The 21 attack listings documented in this report represent only those published on dark web leak sites. Many attacks go unreported, and victims who pay ransoms are typically never listed publicly.

9. Conclusion

The 2025 CFSI Caribbean and CARICOM Ransomware Report paints a sobering picture of the evolving ransomware threat landscape facing the Caribbean region. With 21 confirmed dark web leak site listings across 11 countries and territories, carried out by 11 distinct ransomware groups, and attacks documented in every month from February through December, 2025 marks the most active year for Caribbean ransomware activity on record.

The dominance of Qilin, responsible for 38% of all Caribbean listings, the targeting of critical infrastructure in Aruba, the sustained attacks against Barbados, and the involvement of both established groups like Akira, Medusa, and Play as well as emerging groups like Weyhro and Lockbit5, collectively demonstrate that the Caribbean ransomware threat is growing in both scale and sophistication.

The global ransomware ecosystem that enables these attacks continued to expand dramatically throughout 2025, with the number of active groups nearly doubling and monthly publication counts reaching historic highs. The proliferation of the Ransomware-as-a-Service model means that capable attackers need not be highly technical themselves; they can leverage the tools, infrastructure, and even legal services provided by established groups.

As we look ahead, proactive investment in cybersecurity defenses, regional cooperation, legislative frameworks, and workforce development will be critical to improving the Caribbean's resilience against this persistent and escalating threat. The cost of inaction will only increase.

Computer Forensics and Security Institute (CFSI)

Dark Web Threat Intelligence • Penetration Testing • Incident Response • Cybersecurity Training

Disclaimer: This report is provided for informational and awareness purposes only. No victim data was downloaded, saved, or shared during the research process. Organization names have been intentionally omitted to protect victim identity. The information contained herein is based on publicly observable dark web leak site data and may not represent the complete picture of ransomware activity in the Caribbean.