CFSI

Computer Forensics and Security Institute

2026 Mid-Year Caribbean Ransomware Report

Dark Web Threat Intelligence • Ransomware Leak Site Monitoring

January 2026 – June 2026

CFSI

Computer Forensics and Security Institute

2026 Mid-Year Caribbean

Ransomware Report

Dark Web Threat Intelligence • Ransomware Leak Site Monitoring

January 2026 – June 2025

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

Table of 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
- MSSP Services
- 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: https://www.linkedin.com/company/cfsi-cybersec

Web: www.CFSI.co

CFSI Service Catalogue: Download the full 2026 Service Catalogue here.

About the Author

Name: Shiva V.N Parasram.

LinkedIn: 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). Shiva currently holds several Risk and InfoSec Consultancy roles for several regional institutions including the Barbados National Cybersecurity Unit and a large regional financial institution.

Certifications: MSc Network Security (Anglia Ruskin, UK), CCISO, C|RAGE, CAIPM, CEI, CEH, CHFI, ECSA, CCNA, MCSA, CND, ECIH, ECES, CSA, CTIA, ISC2 CC, Security+, Network+, A+, TM.

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
- Author of all CFSI Caribbean Ransomware Reports (2023 – 2026)

Certified EC-Council Instructor (CEI):
CFSI is also the only EC-Council **Authorized Training Center (ATC) in the Caribbean.**

1.Executive Summary

This report is the CFSI 2026 Mid-Year Caribbean and CARICOM Ransomware Report, the fourth in CFSI's ongoing series of Caribbean ransomware intelligence publications. Compiled through continuous monitoring of ransomware group dark web leak sites from January through June 2026, it documents all ransomware attacks where Caribbean and CARICOM organizations were listed as victims by ransomware threat actors.

In the first half of 2026 alone, the Caribbean recorded 21 confirmed ransomware attack listings equalling the total for the entire year of 2025 in just six months. Attacks were carried out by 12 distinct ransomware groups across 5 Caribbean countries and territories, signalling a dramatic acceleration of the ransomware threat in the region.

The Dominican Republic emerged as the most targeted country with 7 listings, followed by Jamaica (6), Bahamas (5), Turks and Caicos (2), and Bermuda (1). LockBit ransomware operation (including its v5 variant) was the most active group with 4 Caribbean listings, followed by Payload (3). Notably, 8 of the 12 groups observed had no Caribbean presence in 2025, indicating a significant expansion of the threat actor landscape targeting the region.

Several developments are particularly alarming: one Caribbean organization may have perhaps paid a ransom and was subsequently delisted from a leak site; a government law enforcement agency was listed as a victim; leaked proof-of-compromise data from one attack contained the passport biodata of a citizen from another Caribbean country; and the food production and government sectors each saw 3 attacks, joining finance and tourism as the most targeted sectors.

Important Note: As with prior reports, the attack listings documented here represent only those published on dark web leak sites. Organizations which pay ransoms are typically delisted or never published. The actual number of ransomware attacks in the Caribbean during this period is likely significantly higher.

2. Methodology

This report was compiled through systematic, ongoing monitoring of over 100 ransomware group dark web leak sites (DWLS) from January through June 2026. The researcher documented all publications and listings involving Caribbean and CARICOM-based organizations, recording the ransomware group name, date of listing, country of operation, industry sector and publication status.

No victim data was downloaded, saved or shared at any point during this research. Organization names have been intentionally omitted from this report to protect victim identity, consistent with CFSI's established methodology across all previous Caribbean ransomware reports.

3. Mid-Year 2026 Caribbean Ransomware Attack Listings

The following table documents all 21 confirmed ransomware attack listings involving Caribbean and CARICOM organizations during the first half of 2026. Organization names have been omitted to protect victim identity.

#	Month	Threat Group	Country	Industry Sector
1	January	**Sinobi**	Bahamas	Retail and Distribution
2	February	**The Gentlemen**	Dominican Republic	Food Production
3	February	**Clop**	Bermuda	Real Estate / Construction
4	February	**The Gentlemen**	Jamaica	Finance
5	February	**Clop**	Jamaica	Tourism
6	February	**Lockbit5**	Turks and Caicos	Tourism
7	March	**Payload**	Dominican Republic	Food and Beverage Production
8	March	**Qilin**	Bahamas	Entertainment
9	April	**Payload**	Jamaica	Finance and Investment
10	April	**Lockbit5**	Dominican Republic	Energy / Gas / Distribution
11	May	**IncRansom**	Bahamas	Construction and Renewable Energy
12	May	**Krybit**	Dominican Republic	Food

13	May	**LockBit ***	Jamaica	Communications
14	May	**Genesis**	Jamaica	Public
15	June	**IncRansom**	Bahamas	Finance and Investment
16	June	**Payload**	Dominican Republic	Retail
17	June	**Gunra**	Bahamas	Legal
18	June	**Pear**	Jamaica	Government
19	June	**Spacebears**	Turks and Caicos	Telecom
20	June	**LockBit**	Dominican Republic	Tourism
21	June	**Krybit**	Dominican Republic	Government / Law Enforcement

** **Listing #13:** This LockBit listing targeting a major company in Jamaica was subsequently removed from the leak site, indicating the victim could have paid the ransom or some agreement was reached…*

4. Monthly Breakdown

Every month from January through June 2026 recorded at least one Caribbean ransomware attack listing, continuing the sustained cadence first observed in 2025. Activity accelerated sharply in June with 7 listings, the highest single-month total in CFSI's three years of monitoring.

Month	Listings	Groups Active
January	1	Sinobi
February	5	The Gentlemen (2), Clop (2), Lockbit5 (1)
March	2	Payload, Qilin
April	2	Payload, Lockbit5
May	4	IncRansom, Krybit, LockBit, Genesis
June	7	IncRansom, Payload, Gunra, Pear, Spacebears, LockBit, Krybit

The trajectory is clear: a single listing in January, 5 in February, then a steady buildup to 7 in June. This acceleration mirrors the global ransomware trend, where activity surged across all regions in Q2 2026.

5. Analysis by Country / Territory

In the first half of 2026 attacks were executed against organizations across 5 Caribbean countries and territories. While the number of affected countries is fewer than the 11 seen in 2025, the concentration and volume of attacks is significantly higher, with multiple countries experiencing repeated targeting.

Country / Territory	Number of Attack Listings
Dominican Republic	7
Jamaica	6
Bahamas	5
Turks and Caicos	2
Bermuda	1

Key Country Observations

- **Dominican Republic** was the most targeted country with 7 listings showing a dramatic shift from 2025, when the Dominican Republic had zero Caribbean ransomware listings in CFSI's report. Six different groups targeted the country: The Gentlemen, Payload (2), Lockbit5, Krybit (2), and LockBit. Industries targeted include food production, food and beverage production, food, energy/gas, retail, tourism and government/law enforcement. The listing of a government law enforcement agency (Krybit, June) is particularly concerning.
- **Jamaica** was the second most targeted with 6 listings, a significant increase from 4 in the full year of 2025. Groups targeting Jamaica included The Gentlemen, Clop, Payload, LockBit, Genesis, and Pear. The LockBit attack on a major company (#13) resulted in the victim being delisted. A government health agency was also targeted (Pear, June).
- **Bahamas** recorded 5 listings, up from 2 in all of 2025. Groups included Sinobi, Qilin, IncRansom (2) and Gunra. The Qilin attack (#8, March) on an entertainment company

is notable because the leaked proof-of-compromise data contained the passport biodata of a Trinidad and Tobago citizen, illustrating the cross-border privacy implications of ransomware attacks.

- **Turks and Caicos** appeared for the first time in CFSI's Caribbean ransomware reporting with 2 listings: a tourism company (Lockbit5, February) and a telecommunications provider (Spacebears, June). Both attacks target sectors critical to the island's economy.
- **Bermuda** also appeared for the first time with 1 listing: a real estate and construction company targeted by Clop in February. This aligns with Clop's well-documented mass exploitation campaigns targeting file transfer vulnerabilities.

6. Analysis by Threat Group

12 distinct ransomware groups were responsible for the 21 Caribbean attack listings between Jan – June 2026 amounting to more groups in six months than the 11 observed across all of 2025. Critically, 8 of these 12 groups (The Gentlemen, Payload, Krybit, IncRansom, Sinobi, Genesis, Gunra, Pear, and Spacebears) had no Caribbean presence in 2025, indicating a significant broadening of threat actors targeting the region.

Ransomware Group	Caribbean Listings	Model
LockBit (incl. v5)	4	RaaS
Payload	3	Double Extortion
The Gentlemen	2	RaaS
Clop	2	RaaS
Krybit	2	RaaS
IncRansom	2	RaaS
Sinobi	1	Unknown
Qilin	1	RaaS
Genesis	1	Unknown
Gunra	1	RaaS
Pear	1	Unknown
Spacebears	1	RaaS

The Most Active Caribbean Threat in Q1 and Q2 2026

The LockBit operation (including its v5 variant) was the most active group targeting the Caribbean in Q1 and Q2 2026 with 4 listings across 3 countries. This represents a significant comeback for the group, which had only 1 Caribbean listing in all of 2025.

- Lockbit5 listed a tourism company in Turks and Caicos (February) and an energy/gas company in the Dominican Republic (April).
- LockBit listed a major company in Jamaica (May) and a tourism company in the Dominican Republic (June).
- **The Jamaica communications attack (#13) is particularly significant:** the victim was subsequently delisted from the leak site, possibly due to the company paying the ransom or other negotiation. It demonstrates both the severity of the attack (likely involving critical broadcast infrastructure) and the difficult decisions organizations face when operations are compromised.
- Despite law enforcement disruption (Operation Cronos, February 2024), the exposure of its leader, a database breach in May 2025 and OFAC sanctions, LockBit continues to operate and remains a persistent threat to the Caribbean.

Payload — An Emerging Threat

Payload emerged in February 2026 and quickly became the second most active group targeting the Caribbean with 3 listings, all targeting the Dominican Republic and Jamaica. The group is built on leaked Babuk source code and uses Curve25519 + ChaCha20 encryption across Windows and Linux/VMware ESXi platforms. Over 56 victims have been listed globally as of mid-2026.

The Gentlemen — The Global Phenomenon

The Gentlemen emerged in mid-2025 and became one of the most explosive ransomware operations in history, claiming over 480 victims across 66 countries by mid-2026. The group became the most active ransomware threat globally in Q2 2026, surpassing even Qilin. In the Caribbean, The Gentlemen listed 2 victims in February: a food production company in the Dominican Republic and a financial institution in Jamaica. The group offers affiliates a 90% revenue split which currently is the highest in the RaaS ecosystem and targets Windows, Linux, NAS, BSD, and ESXi environments. Its rapid scaling has been compared to the early rise of LockBit 3.0.

Clop (TA505)

Clop continued its mass exploitation campaigns in Q1 and Q2 2026 with 2 Caribbean listings: a real estate/construction company in Bermuda and a tourism company in Jamaica, both in February. Clop is well known for its exploitation of file transfer vulnerabilities (Cleo CVE-2024-50623 and CVE-2024-55956) and listed 304 companies globally in February 2025 alone. Clop's Caribbean presence in 2026 demonstrates that even mass-campaign groups now routinely sweep up Caribbean organizations.

Krybit

Krybit is a cross-platform RaaS operation that launched in late March 2026 with builders for Windows, Linux, ESXi, and NAS devices. Despite being breached by rival group 0APT in April 2026 (exposing its affiliate panel), Krybit retaliated within a day and remained operational. The group listed 2 Caribbean victims in the Dominican Republic: a food company (May) and a government/law enforcement agency (June). With over 84 global victims and an 80/20 affiliate split, Krybit represents a capable emerging threat.

Other Groups

- **IncRansom:** 2 listings in the Bahamas (construction/renewable energy in May, finance/investment in June). Also known as INC Ransom, active since 2023.

- **Qilin:** 1 listing (Bahamas, March — entertainment). The dominant Caribbean threat in 2025 (8 listings), Qilin's Caribbean activity slowed in Q1 and Q2 2026 but remains the #1 global ransomware group by volume with 1,062 victims in 2025 and 389 in Q1 2026 alone. The leaked proof-of-compromise data from this attack contained the passport biodata of a Trinidad and Tobago citizen.

- **Sinobi:** 1 listing (Bahamas, January — retail and distribution). A lesser-known group.

- **Genesis:** 1 listing (Jamaica, May — a public gaming commission).

- **Gunra:** 1 listing (Bahamas, June — a legal firm).

- **Pear:** 1 listing (Jamaica, June — a government health agency).
- **Spacebears:** 1 listing (Turks and Caicos, June — a telecom provider). Targeting a telecom provider in a small island territory poses significant implications for communications infrastructure.

7. Analysis by Industry Sector

H1 2026 Caribbean ransomware attacks targeted 11 distinct industry sectors. Four sectors were tied as the most frequently targeted, each with 3 listings: finance and investment, tourism, food/food production, and government/public sector.

Industry Sector	Listings	Entries
Finance and Investment	3	#4, #9, #15
Tourism	3	#5, #6, #20
Food / Food Production / F&B	3	#2, #7, #12
Government / Public / Law Enforcement	3	#14, #18, #21
Retail and Distribution	2	#1, #16
Construction / Real Estate	2	#3, #11
Entertainment	1	#8
Energy / Gas / Distribution	1	#10
Communications	1	#13
Legal	1	#17
Telecom	1	#19

The prominence of the food production sector (3 listings across the Dominican Republic) is a notable new trend not observed in 2025. All three attacks targeted Dominican food and beverage companies, potentially reflecting the country's significant food production and export economy.

The government and public sector was targeted 3 times: a public gaming commission in Jamaica (Genesis), a government health agency in Jamaica (Pear), and a government law enforcement agency in the Dominican Republic (Krybit).

Tourism remained a high-value target with 3 listings across Jamaica, Turks and Caicos, and the Dominican Republic. For Caribbean economies heavily dependent on tourism revenue, ransomware attacks on this sector can have outsized economic impact.

8. Comparison: Mid-Year 2026 vs Full Year 2025

The following table compares key metrics between the first half of 2026 and the full year of 2025, highlighting the accelerating pace of Caribbean ransomware activity.

Metric	2026 (Jan–Jun)	2025 (Jan – Dec)
Total attack listings	21	21
Countries / territories affected	5	11
Distinct ransomware groups	12	11
Most targeted country	Dominican Republic (7)	Barbados (9)
Most active group	LockBit (4)	Qilin (8)
Months with ≥1 attack	6 of 6 (100%)	11 of 12 (92%)
Government sector listings	3	3
Delisted (ransom paid)	1 confirmed	0 confirmed

Key Comparisons

- **Equal volume in half the time:** 21 attack listings in 6 months equals the entire 2025 total of 21. If this pace continues, 2026 could see over 40 Caribbean ransomware listings by year-end.
- **New threat actors:** 8 of the 12 groups active in H1 2026 had no Caribbean presence in 2025 (The Gentlemen, Payload, Krybit, IncRansom, Sinobi, Genesis, Gunra, Pear, Spacebears). Only LockBit, Qilin, and Clop carried over from 2025.
- **Geographic shift:** The Dominican Republic went from 0 listings in 2025 to 7 in H1 2026, becoming the most targeted country. Conversely, Barbados (the most targeted in 2025 with 9 listings) had 0 listings in H1 2026.

- **New territories:** Turks and Caicos and Bermuda appeared in CFSI's reporting for the first time, expanding the geographic footprint of Caribbean ransomware.
- **LockBit's resurgence:** After just 1 Caribbean listing in 2025, LockBit surged to 4 in H1 2026, reclaiming the top spot from Qilin (which dropped from 8 in 2025 to 1 in H1 2026).
- **First confirmed ransom payment:** The delisting of entry #13 represents the first documented instance of a Caribbean organization paying a ransomware demand in CFSI's three years of reporting.

9. Key Observations and Trends

The LockBit Delisting:

Entry #13 — a LockBit attack on a major communications company in Jamaica in May 2026 was subsequently removed from LockBit's leak site. This delisting suggests that the victim organization may have either paid the demanded ransom or engaged in other types of negotiations. This is the first confirmed instance of a Caribbean being and delisted, documented across CFSI's annual reports.

Cross-Border Data Exposure

The Qilin attack on an entertainment company in the Bahamas (#8, March) revealed a concerning cross-border dimension: the leaked proof-of-compromise data published on Qilin's dark web site contained the passport biodata of a Trinidad and Tobago citizen. This demonstrates that ransomware attacks in one Caribbean country can directly compromise the personal data of citizens from other Caribbean nations, amplifying the regional impact of what might appear to be a localized incident.

The Dominican Republic: Most Targeted

The Dominican Republic's emergence as the most targeted Caribbean country in Q1 and Q2 (7 listings, up from 0 in 2025) is the most dramatic geographic shift in CFSI's reporting history. Six different groups targeted the country across food production, energy, retail, tourism, and government/law enforcement. The targeting of a government law enforcement agency (POLITUR, the tourism police) by Krybit in June is particularly alarming and could expose sensitive law enforcement data.

Government Sector Escalation

Three government or public sector entities were targeted in Q1 and Q2 2026: a public gaming commission, a government health agency, and a government law enforcement agency. The targeting of law enforcement represents a new escalation in the Caribbean context and suggests that threat actors are becoming bolder in their selection of victims, undeterred by the potential consequences of attacking government entities.

The Accelerating Threat Landscape

The fact that Q1 and Q2 2026 matched the entire number of listings in 2025 total in just six months reflects a broader global trend. Globally, The Gentlemen alone claimed 300+ victims in Q2 2026, Qilin maintained its position as a top-tier threat with 389 victims in Q1 2026 alone and the total number of active ransomware groups continues to grow. The Caribbean is not immune to these trends but is experiencing them in real time.

Emerging Groups Targeting the Caribbean

The appearance of 8 groups with no prior Caribbean presence (The Gentlemen, Payload, Krybit, IncRansom, Sinobi, Genesis, Gunra, Pear, and Spacebears) suggests that the Caribbean is increasingly on the radar of a broader range of threat actors. This may be driven by the perception that Caribbean organizations have lower cybersecurity maturity, less robust incident response capabilities, or limited law enforcement capacity to investigate and prosecute cybercrimes.

10. Conclusion

The 2026 Mid-Year CFSI Caribbean and CARICOM Ransomware Report documents a troubling acceleration of the ransomware threat facing the region. With 21 confirmed attack listings in just six months matching the entire 2025 total carried out by 12 distinct groups across 5 countries, the data is unambiguous: the Caribbean ransomware threat is intensifying.

If the current pace continues, 2026 will surpass 2025 as the most active year for Caribbean ransomware by a significant margin.