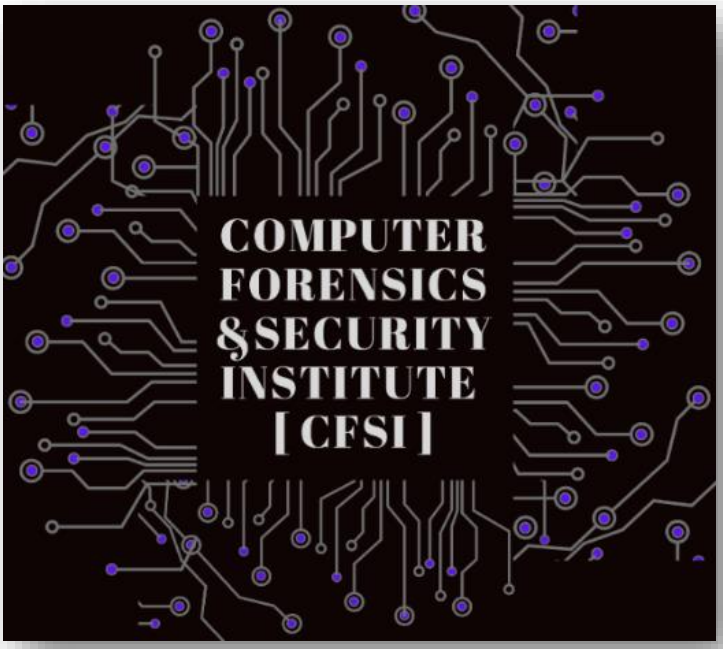
The Ransomware Roundhouse

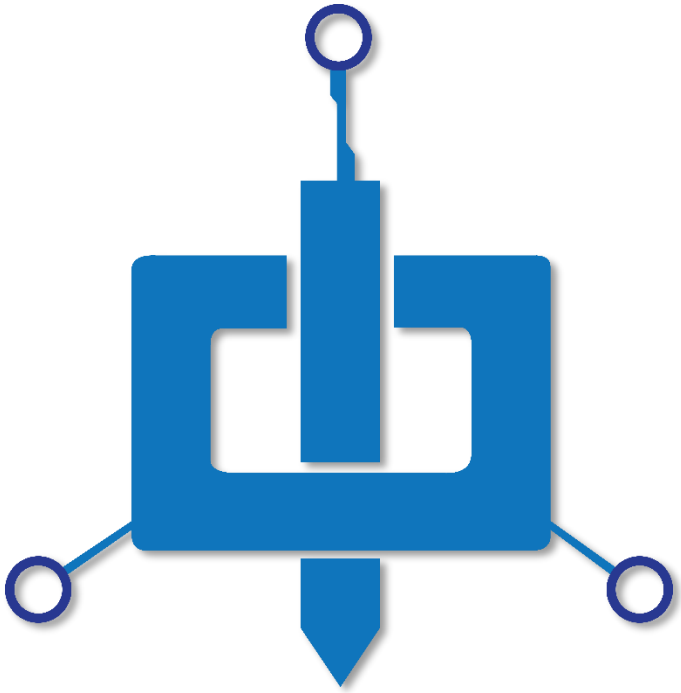
A look at published Ransomware Attacks and Data Leaks in Caricom and the Wider Caribbean including attacks on Canada.

Authors:

Shiva V.N Parasram – *MSc Network Security, CCISO, CEH, CHFI, ECSA, CND, CTIA, CCNA, MCSA, Security+, ISC2 CC, Network+, A+.*

Alex Samm – *BSc Computer Science, CEH, CTIA, CISA*


COMPUTER
FORENSICS
& SECURITY
INSTITUTE
[CFSI]



Contents

About the Researchers

Shiva V. N Parasram and Alex Samm are both professional, certified penetration testers, incident responders, forensic investigators, enterprise risk consultants, security researchers and cybersecurity lecturers/instructors.

Shiva has over 2 decades of experience and has authored 3 books on Digital Forensics and has co-authored a book on Penetration Testing (all under Packt Publishing) with Alex who is one of the very few OT (Operation Technology) Security Assessors in the Caribbean. Both Shiva and Alex and Cybersecurity Mentors at SpringBoard (US) and are Senior Lecturers at the Computer Forensics and Security Institute (CFSI) for courses such as the Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), Certified CISO (CCISO), DFIR Practitioner and several other certification courses. Shiva is the owner of the Computer Forensics and Security Institute (CFSI) and Alex is the owner of Tier 10 Technologies.

For assistance and quotations on vulnerability assessments, penetration testing, Digital Forensics and Incident Response (DFIR), Cybersecurity and Risk Consultancy and vCISO services, feel free contact us.

The CFSI Service Catalogue can be downloaded here.

Contact Info:

Shiva

Shiva Parasram – https://www.linkedin.com/in/shiva-parasram/

Website – www.CFSI.co

Emai - info@CFSI.co

Computer Forensics and Security Institute (CFSI) – https://www.linkedin.com/company/cfsi-cybersec

YouTube Channel - https://www.youtube.com/@cfsicyberfence4304

Alex

Alex Samm – https://www.linkedin.com/in/alex-samm/

Website – www.tier10tech.com

Email – alex.samm@tier10tech.com

Tier 10 Technology - https://www.linkedin.com/company/tier-10-technology/

Introduction

2023 was a tough year for Security professionals with thousands of companies falling victim to ransomware attacks globally but it was quite a lucrative year for the Ransomware groups and threat actors themselves. There were far more data leaks by Ransomware groups in 2023 than in previous years which suggests that companies were not paying the ransoms demanded for whatever reasons be it legal, financial or moral, however, according to researchers at Chainalysis.com, the amount paid in ransoms for 2023 amounted to a staggering $1.1 Billion (USD). This figure is almost double the amount paid in 2022 which totaled to $560 Million (USD).

With groups such as LockBit having listed over 1,000 victims on their official dark web leak site for 2023, this indicates that ransomware groups have become far more aggressive than seen in previous years and companies and organizations alike are in fact paying the ransoms. CARICOM (The Caribbean Community) and the Wider Caribbean were certainly not spared from these attacks with many victims data being published on the leak pages of Ransomware groups on their official dark web sites.

Following these events, **Alex Samm of Tier 10 Technology** and **Shiva V.N Parasram of the Computer Forensics and Security Institute (CFSI)** have teamed up (combined forces if you will) to produce this report, the sole aim of which is to give insights into the cybersecurity and threat landscape regionally within **CARICOM (The Caribbean Community) and the Wider Caribbean** and reveal a deeper understanding of why cybersecurity now requires more

attention and focus than ever before. Attacks on **Canadian sectors** are also listed at the end of the report for comparison purposes.

This article is a combination of research and information gathering done by Shiva and Alex conducted by tirelessly sifting through the dark web sites. In keeping with updates on various attacks, they often must scour the dark web for information about threat actors, threat vectors, Advanced Persistent Threats (APTs), releases by threat groups and general trends on attack and malware. Most of this information resides on official ransomware leak pages and dark web forums (most of which are undocumented) and hundreds of articles on the surface web (or the internet) as we know it.

Their daily dark web activities include searches on Ransomware attacks and groups in Caribbean islands as there is usually **little (and sometimes) no information** on these attacks. For their own research purposes and the benefit of their clients, they started compiling a list of attacks within CARICOM states and the wider Caribbean.

It is important to note that CARICOM comprises many but not all Caribbean countries. However, they have included non-CARICOM countries which are part of the Caribbean for the purpose of being thorough.

There exist hundreds of Ransomware groups however the focus remained on specific groups.

Reproduction and Referencing

This report's content and findings may be cited and used for further research or analysis, that is to be published in any format or used as a discussion point in any form, provided appropriate attribution is given to the authors and this work.

Corrections and Modifications

Should you wish to bring any corrections, modifications, or additions to our attention, please feel free to contact us. Credit will be given to all contributors.

What is in the report.

This report details industries of countries and islands within **CARICOM and the wider Caribbean** which have been hit by ransomware groups. For comparison, we have also included the same data for **Canada** to show that the CARICOM and the wider Caribbean are no exception to these attacks in the hope that it may help public and private organizations understand the severity of the current threat landscape.

Although we do have a full listing of all companies and organizations within the public and private sectors, the names of the victims (public and private) have been withheld as we do not wish to add further damage to the reputations of victims listed and published on ransomware leak sites as doing so would be irresponsible as they are victims of a crime.

Persons within various protective services wishing to acquire this list for research and defense purposes can contact info@cfsi.co for details on requirements and eligibility to obtain the unedited listing.

This report is also a running document and will be updated when necessary. Version control will be specified and this document is currently at v1.0 as of Monday 18th February 2024.

What is not in the report:

- Company, agency or institution names.
- Specifics about the data released other than general data.
- Information on the Ransom demands.
- Initial Access Vectors and Points of Entry.
- Speculation on the security posture of the victims.

This report is purely factual and is comprised only of information published by ransomware groups on their respective official dark web leak sites.

This report does not assume the cybersecurity status or posture of any of the CARICOM, Caribbean islands or Canadian organizations listed as ransomware attacks can happen to any organization of any size as seen worldwide.

Discussion and Analysis

The statistics and findings within this report will be discussed more in-depth in an upcoming webinar on Thursday 22nd February, 2024 on our CFSI CyberFence Webinar and will be uploaded to the **CFSI CyberFence Youtube channel** shortly thereafter.

To register for the webinar, please visit Shiva's or Alex's LinkedIn Profiles or the official LinkedIn pages of Tier 10 Technologies and the Computer Forensics and Security Institute (CFSI) for the link which will be published on Monday 19th February 2024.

We do hope that you find our efforts insightful and useful. Feel free to connect with us on LinkedIn.

Rounding out 2023

In 2023 we learned that no one was safe in the Caribbean region. The sector, size of the organization, technologies implemented, impact on the global stage, geo-political affiliations or even the GDP were of no matter. Threat actors were interested only in profits and chose their targets based on who was likely to suffer great losses (or fines where applicable), should they refuse to pay them. Every organization with an online presence or internet connection could have been targeted and no one was "safe" as the image below illustrates this.

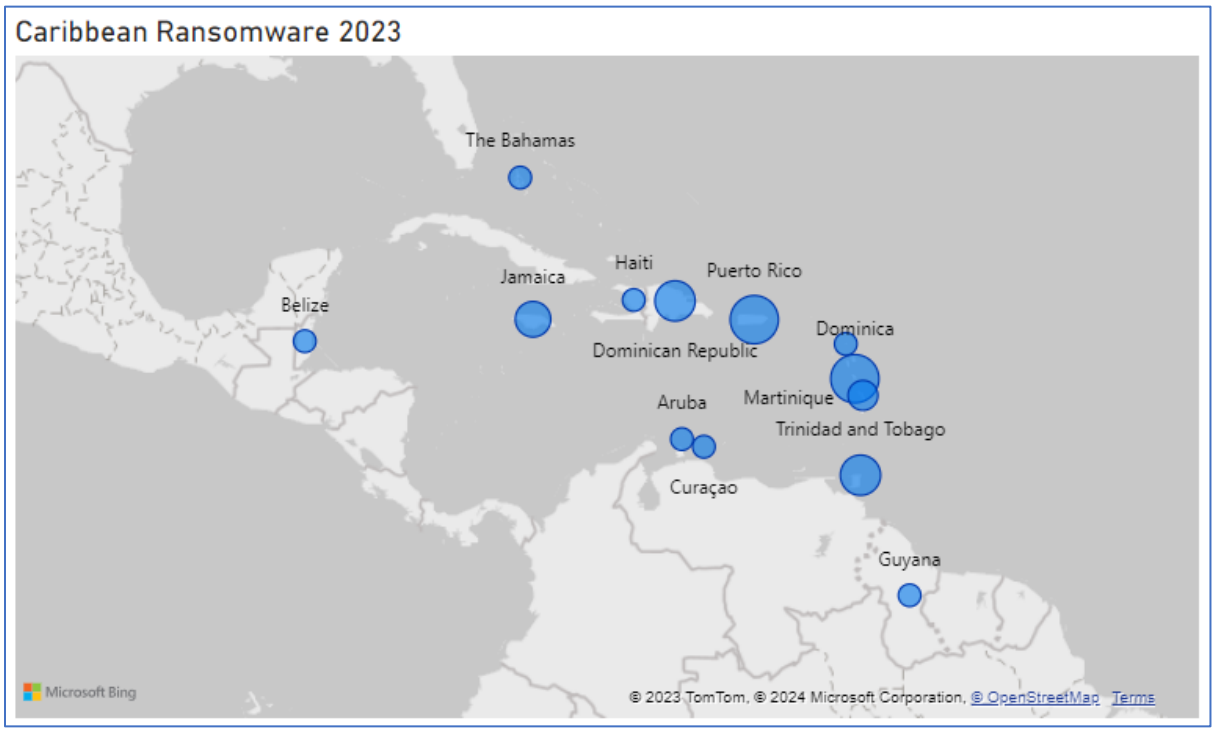


Figure 1 Caribbean Ransomware Map 2023

The blue bubbles in Figure 1 above, show all the countries which were affected by ransomware attacks, the victims of which, had their data listed or leaked by ransomware groups on respective dark web leak pages and forums. The bigger the bubble, the higher the victim count. With ransomware attacks occurring from Guyana to The Bahamas, and even as

far west as Belize, there was no limitation on industry as all companies could have been considered as potential targets.

For comparison, Figure 2 below shows the Ransomware attacks and disclosed leaks for 2022.

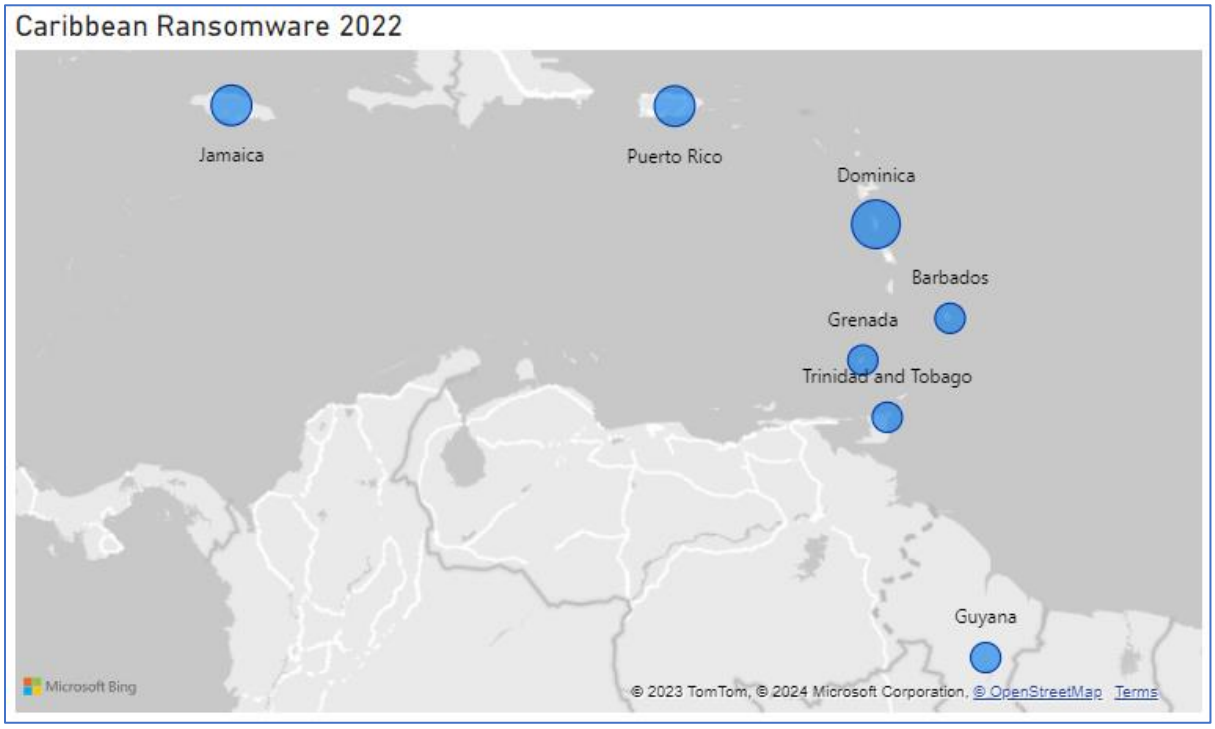


Figure 2 Caribbean Ransomware Map 2022

The table below details the number of listed attacks and data-leaks for all affected CARICOM Nations and Caribbean Islands.

Country	Hits
Dominica	6
Puerto Rico	6
Dominican Republic	4
Trinidad and Tobago	4
Jamaica	3
Martinique	2
Antigua and Barbuda	1
Aruba	1
Belize	1
Curaçao	1
Guyana	1
Haiti	1
The Bahamas	1
Total	***32***

In October 2023, we saw what would be considered one of the major ransomware incidents which was an attack on an ISP and Telecommunications company in Trinidad and Tobago which saw the PII (Personally Identifiable Information) of thousands or customers leaked online which is still available to this day. This remains an issue as the information released to the public by the company was inaccurate on multiple occasions and at many levels including a parliamentary level.

Following this, there was a massive 500GB data-leak of a regional wholesale and retain distributor which saw documents allegedly belonging to several chains throughout the Caribbean, released by the threat actor according to the file listing on the official dark web page of the threat actor.

There were several other breaches which were reported regionally however the scope of this report covers only what was published by ransomware groups. More will be discussed in the upcoming webinar.

Figure 3 below shows the attacks on CARICOM Nations and Caribbean Islands by Sector for 2023.

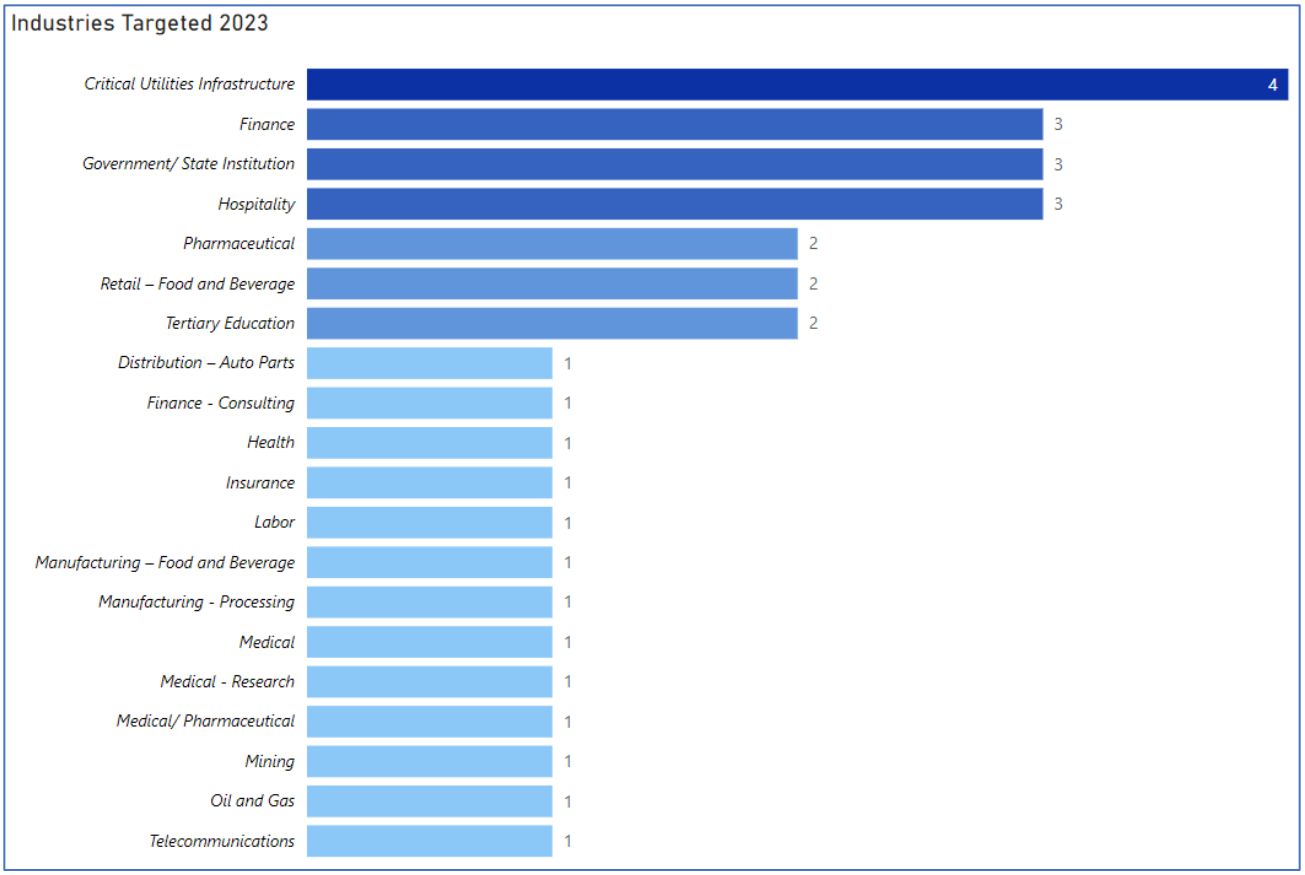


Figure 3 Industries Targeted in the Caribbean 2023

For comparison, here are the states from Canada, showing industries affected by the respective group. The images show 2023 and 2022 and you'll notice a significant increase with 2023 having 56 industries affected while in 2022 only 20.

Canada Ransomware 2023

Group	Number of Industries
8Base	1
Akira	4
Alphv	8
Avoslocker	1
Bianlian	6
Black Suit	1
Everest	3
Inc Ransom	1
Lockbit3	15
Medusa	9
Metaencryptor	1
Money Message	1
Noescape	2
Nokoyawa	3
Ransomware Blog	1
Royal	2
Snatch	2
Total	**56**

Figure 4 Count of Industries hit by the respective ransomware groups in 2023

Canada Ransomware 2022

Group	Number of Industries
Alphv	3
Avoslocker	1
Bianlian	2
Blackbasta	3
Hive	3
Lockbit3	2
Quantum	2
Ransomexx	1
Royal	3
Snatch	1
Total	**20**

Figure 5 Count of Industries hit by the respective ransomware groups in 2022

Affected CARICOM Member Nations :

1. Antigua and Barbuda
2. The Bahamas (a member of the community but not of its Single Market and Economy)
3. Barbados
4. Belize
5. Dominica
6. Grenada
7. Guyana
8. Haiti
9. Jamaica
10. Trinidad and Tobago

Ransomware Groups responsible for Data Leaks within CARICOM:

	Group	Status
1.	8Base	Alive
2.	Akira	Alive
3.	AlphV	Alive
4.	AvosLocker	Alive
5.	Blackbasta	Possibly Inactive
6.	Daixin	Active
7.	Data Leak	Inactive
8.	Hive	Inactive
9.	Karakurt	Inactive
10.	Knight	Active
11.	Lockbit3	Active
12.	Medusa	Active

13.	Noescape	Active
14.	Play	Active
15.	Quantum	Inactive
16.	Ragnarlocker	Inactive
17.	RansomEXX	Active
18.	Ransomhouse	Active
19.	Relic	Inactive
20.	Rhysida	Active
21.	Royal	Inactive
22.	Vicesociety	Inactive

Breakdown of Affected CARICOM Nations:

1.Antigua and Barbuda

Group	Status	Industry	Date Published
AlphV	Active	Tertiary Education	2023-09-19

2.Bahamas

Group	Status	Industry	Date Published
8Base	Active	Medical	2023-08-24
8Base	Active	Medical	2023-08-24

3.Barbados

Group	Status	Indstry	Date Published
Data Leak	Inactive	Insurance	2022-12-02

4.Belize

Group	Status	Industry	Date Published
Ragnarlocker	Inactive	Critical Utilities Infrastructure	2023-07-10

5.Dominica

Group	Status	Industry	Date Published
DataLeak	Inactive	Insurance	2022-12-09

6.Grenada

Group	Status	Industry	Date Published
DataLeak	Inactive	Insurance	2022-12-02

7.Guyana

Group	Status	Industry	Date Published
Play	Active	Mining	2023-03-27
Vicesociety		Manufacturing	2022-03-27

8.Haiti

Group	Status	Industry	Date Published
Lockbit3	Active	Finance	2023-10-06

9.Jamaica

Group	Status	Industry	Date Published
AlphV	Active	Finance	2023-09-23
Lockbit3	Active	Hospitality	2023-08-30
Blackbasta	Inactive	Retail – Food and Beverage	2023-07-22
Lockbit3	Active	Distribution	2022-09-27
Lockbit3	Active	Hospitality	2022-12-09
RansomEXX	Active	Telecommunications	2021-10-24

10.Trinidad and Tobago

Group	Status	Industry	Date Published
8Base	Active	(Details withheld)	-
Lockbit3	Active	Manufacturing – Food and Beverage	2023-12-07
RansomEXX	Active	Telecommunications	2023-10-27
Royal	Inactive	Insurance	2023-05-3-22
Royal	Inactive	Oil and Gas	2023-05-22
Hive	Inactive	Retail – Food and dBeverage	2022-08-18

Breakdown of Other Affected Caribbean Islands:

11. Aruba

Group	Status	Industry	Date Published
Knight	Active	Manufacturing - Processing	2023-12-08

12.Curacao

Group	Status	Industry	Date Published
Akira	Active	Critical Utilities Infrastructure	2023-12-06

13.Dominican Republic

Group	Status	Industry	Date Published
Alphv	Active	Critical Utilities Infrastructure	2023-02-23
Alphv	Active	Pharmaceutical	2023-08-04
Medusa	Active	Health	2023-06-05
Rhysida	Active	Government/ State Institution	2023-10-04

14.Martinique

Group	Status	Industry	Date Published
Lockbit3	Active	Hospitality	2023-11-21
Rhysida	Active	Hospitality	2023-06-09

15.Puerto Rico

Group	Status	Industry	Date Published
Blackbasta	Inactive	Finance - Consulting	2023-11-07
Daixin	Active	Retail – Food and Beverage	2023-02-11
Karakurt	Inactive	Retail - Clothing	2022-10-05
Lockbit3	Active	Distribution – Auto Parts	2023-02-15
Lockbit3	Active	Labor	2023-10-19
Noescape	Active	Medical - Research	2023-10-31
Relic	Inactive	Medical - Health	2022-11-14
Vicesociety	Inactive	Government/ State Institution	2023-03-23

Ransomware Groups Responsible for Data Leaks in Canada

As seen in the tables above, many of the groups responsible for the attacks in CARICOM and the Caribbean are active internationally. This suggests that CARICOM and Caribbean step up their security to an international level as the threat is global with no discrimination based on company size, sector or location.

	Group	**Status**
1	8Base	Active
2	AlphV	Active
3	Avoslocker	Inactive
4	BianLian	Active
5	Black Suit	Active
6	Everest	Active
7	Inc Ransom	Active
8	Lockbit 3	Active
9	Medusa	Active
10	Metaencryptor	Active
11	Money Message	Active
12	No Escape	Active
13	Nokoyawa	Active
14	Ransomware Blog	Active
15	Royal	Inactive
16	Snatch	Active

Canadian Sectors and Industries Affected by Ransomware Group Data Leaks (Sorted by Group)

Group	Status	Industry/Sector	Date
8Base		Broker Management Solutions	11/6/2023
Akira		Online Flower Retail	11/29/2023
Akira		Healthcare	11/8/2023
Akira		Music Education and Instruments	7/21/2023
Akira		Travel Services	5/10/2023
Akira		Travel Services	5/4/2023
Alphv		Manufacturing of Sheet Metalwork	12/28/2023
Alphv		Law Firm	9/3/2023
Alphv		Insulation Manufacturing	6/26/2023
Alphv		Furniture Retail	6/18/2023
Alphv		IT Lifecycle Solutions	5/26/2023
Alphv		Real Estate and Construction	3/17/2023
Alphv		Home Improvement & Hardware Retail	2/22/2023
Alphv		Wealth Management	2/6/2023
Avoslocker		Mining	2/14/2023
Bianlian		Airline	10/11/2023
Bianlian		Law Firm	6/13/2023
Bianlian		Housing	5/18/2023
Bianlian		Energy (Petroleum and Natural Gas)	4/10/2023
Bianlian		Manufacturing for Mining and Industrial Applications	3/28/2023
Bianlian		Wheel and Rim Manufacturing	3/5/2023
Black Suit		Construction Supply	6/18/2023
Everest		Construction	8/28/2023
Everest		Real Estate	8/28/2023
Everest		Construction	8/28/2023
Everest		Construction	8/28/2023

Everest		Construction	8/28/2023
Everest		Aerospace	1/3/2023
Inc Ransom		Labor Union	12/20/2023
Lockbit3		Education	12/7/2023
Lockbit3		Freight and Logistics	11/11/2023
Lockbit3		Labor Union	10/19/2023
Lockbit3		Snow Removal Equipment Manufacturing	10/6/2023
Lockbit3		Weather Information and Data Management	9/22/2023
Lockbit3		Kitchenware Distribution	9/20/2023
Lockbit3		Information Technology Solutions	9/4/2023
Lockbit3		Oil and Gas Exploration and Production	5/28/2023
Lockbit3		Management Consulting	5/22/2023
Lockbit3		Chemical and Refrigerant Gas Production	5/3/2023
Lockbit3		Industrial Motors and Equipment	3/20/2023
Lockbit3		Mining and Tunneling Products	3/10/2023
Lockbit3		IT Solutions for Office Furniture Industry	3/10/2023
Lockbit3		Retail (Books and Music)	2/28/2023
Lockbit3		Truck Parts Distribution	2/15/2023
Medusa		Automotive Repair and Maintenance Services	11/17/2023
Medusa		Payment Processing Solutions	11/13/2023
Medusa		Professional Association for Psychologists	11/5/2023
Medusa		Legal and Social Services for Indigenous Peoples	10/23/2023
Medusa		Indigenous Community Administration	10/23/2023
Medusa		Battery and Scrap Metal Resale	9/27/2023
Medusa		Fasteners and Packaging Solutions	8/25/2023
Medusa		IT Services for Manufacturing and Distribution Companies	5/22/2023
Medusa		Dental Services	4/23/2023
Metaencryptor		Animation and CG Production	8/17/2023

Money Message		Computer Hardware Manufacturing	4/8/2023
Noescape		Wholesale Floristry	10/24/2023
Noescape		International Governance	9/11/2023
Nokoyawa		Door Lock Manufacturing	7/20/2023
Nokoyawa		Medical Education	7/20/2023
Nokoyawa		Professional Association for Nurses	7/20/2023
Ransomware Blog		Construction	8/3/2023
Royal		Organic Food Manufacturing	4/10/2023
Royal		Construction Services	1/21/2023
Snatch		Professional Association for Psychologists	11/29/2023
Snatch		Professional Association for Nurses	5/22/2023