ThreatMon

Ransomware Group Activity Report

18.12.2022 - 01.01.2023

in @threatmon

@MonThreat

ThreatMon

Ransomware Group Activity Report

ThreatMon Threat Intelligence created a report on **two weeks** of ransomware activity by tracking posts by ransomware groups on Dark Web leak sites.

According to ThreatMon's two-week security survey, there were **94** ransomware attacks. The United States was the most targeted country. In addition, the most targeted sectors are Industry, Education and Health.

ThreatMon will continue to share monthly ransomware reports. You can easily access these posts from our social media accounts.

Key Points:

1. Number of Attacks by Ransomware Groups
2. Number of Attacks by Countries
3. Number of Attacks by Sectors
4. IOC List of Ransomware Groups

Table of Contents

1. Number of Attacks by Ransomware Groups

The most active group during this two-week period was the **LockBit 3.0** ransomware group. LockBit 3.0 had **2** missing attacks compared to the number of attacks in the report last week, but it has been the most active ransomware group of the past two weeks.

Targeting the **Health** sector the most, **LockBit** took the **Industry** sector as the second target and the **IT** sector as the third target.

Targeting the **United States**, the most as a country, LockBit targeted **New Zeland** as the second and **United Kingdom** as the third.

The second most active group during this two-week period was the **Royal** ransomware group. Royal has carried out a total of **22** attacks in the past two weeks.

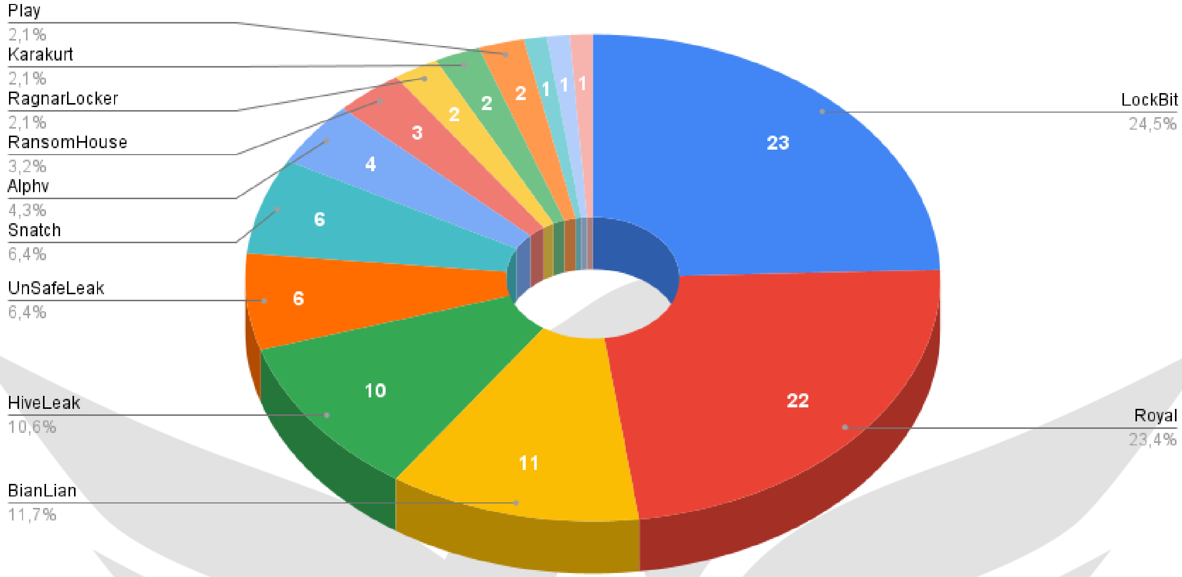
Targeting the **Education** sector the most, **Royal** took the **Industry** sector as the second target and the **Energy** sector as the third target.

Targeting the **United States** the most as a country, **Royal** targeted **Brazil** second and **Germany** third.

The third most active group during this two-week period was the **BianLian** ransomware group. BianLian carried out 13 attacks in last week's report, but **11** attacks in this two-week report.

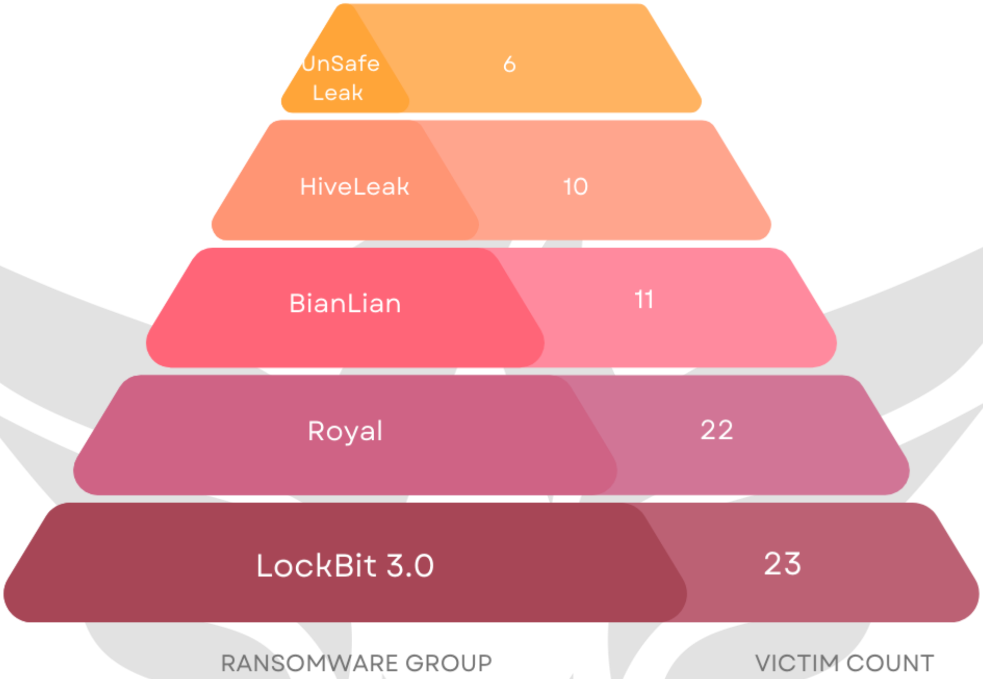
BianLian, targeting the **Industry** sector the most, took the **Law** sector as the second target and the **Travel** sector as the third target.

Targeting the **United States** the most as a country, **BianLian** targeted **Japan** second and **Canada** third.



The Ransomware Groups in the top ten are as in the image;

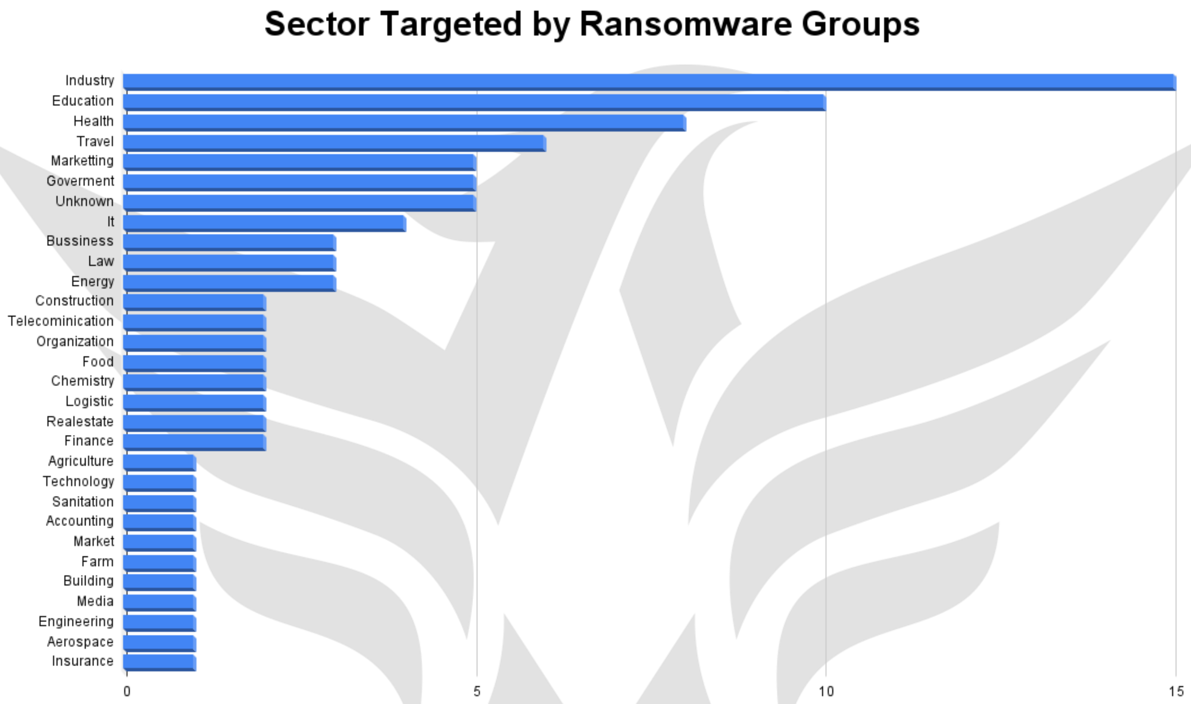
- **LockBit 3.0** is the first with 23 victims,
- **Royal** second, with 22 victims,
- **BianLian** third with 11 victims,
- **HiveLeak** fourth with 10 victims,
- **UnSafeLeak** fifth with 6 victims,
- **Snatch** sixth with 6 victims,
- **AlpHV** seventh with 4 victims,
- **RansomHouse** eighth with 3 victims,
- **RagnarLocker** ninth with 2 victims,
- **Karakurt** tenth with 2 victims is in line,


UnSafe Leak
6
HiveLeak
10
BianLian
11
Royal
22
LockBit 3.0
23
RANSOMWARE GROUP
VICTIM COUNT

2. Number of Attacks by Sectors

Ransomware groups prefer to attack mostly **Industry** sectors in early **December**.

The second most attacked sector was the **Education** sector.

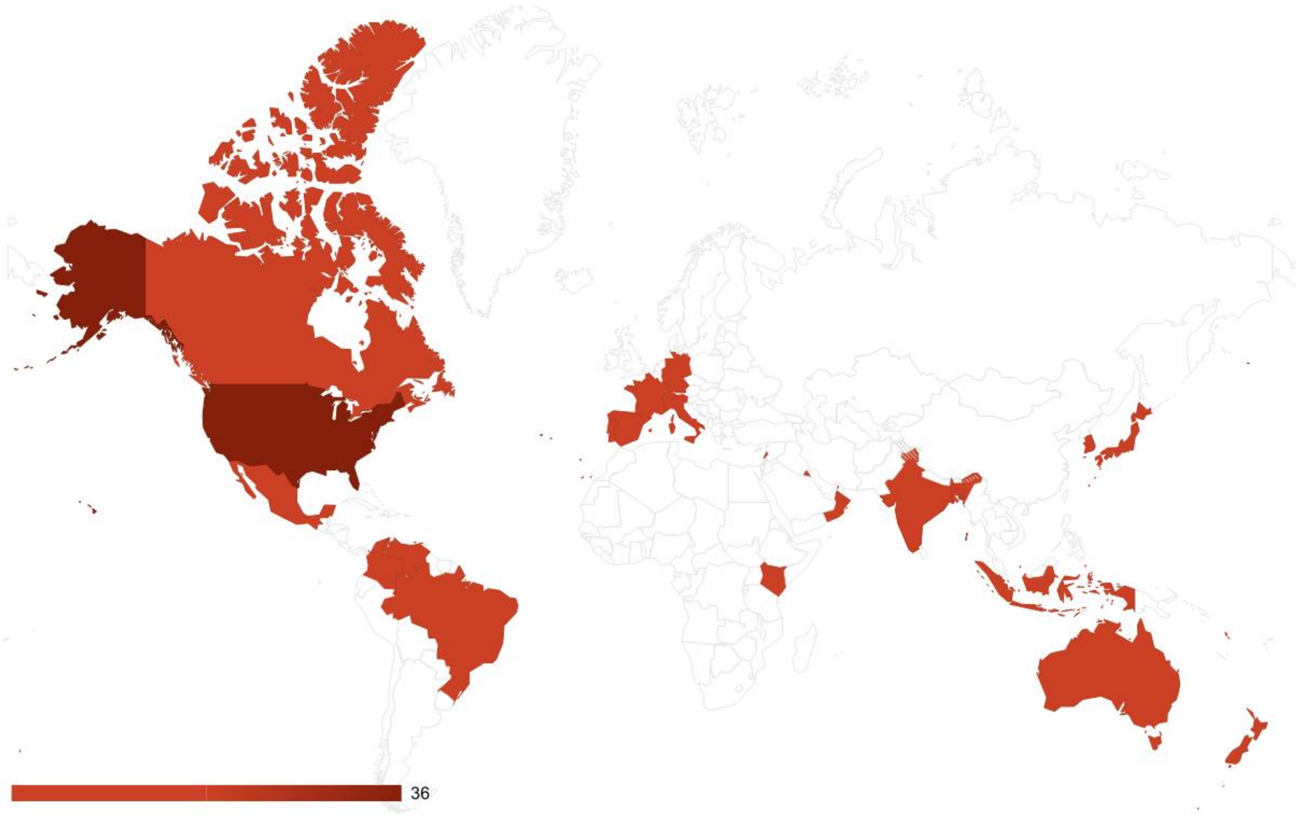


As in the previous report, there are not many sectors that have changed on a sectoral basis. The previous report had a lot of attacks on the **Industry** sector, but this week there are more attacks on the **Industry** sector.

The target of current attacks is **Education**, **Health** and **Travel** sectors.

3. Number of Attacks by Countries

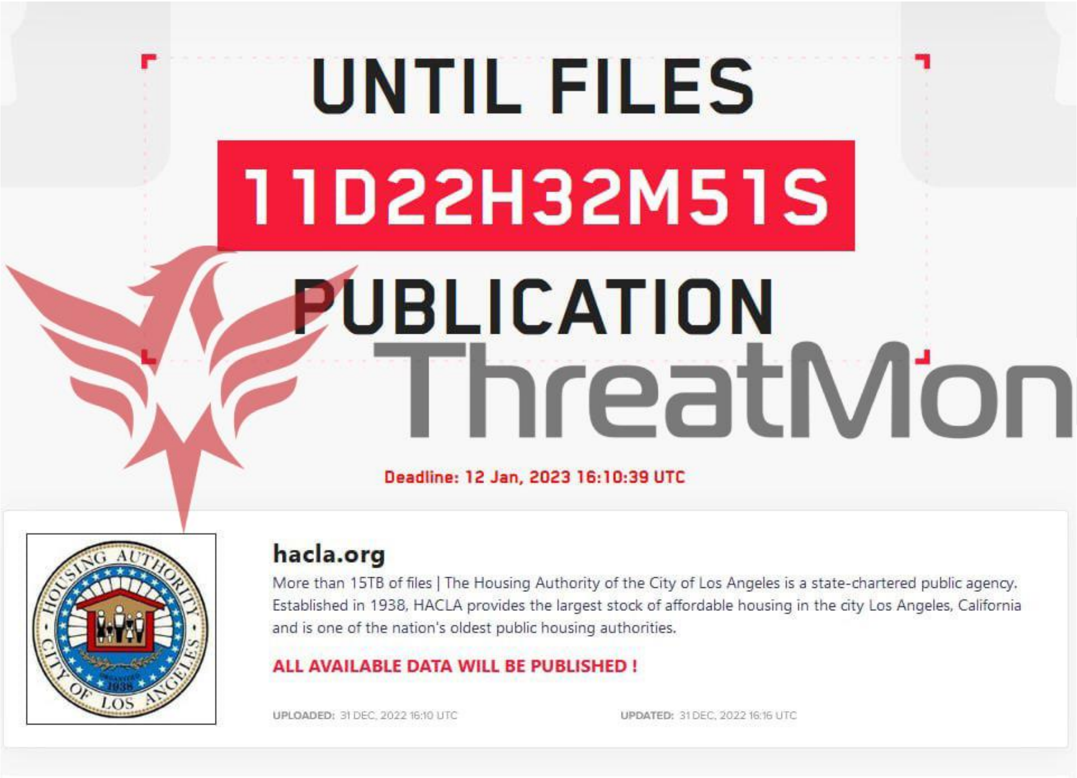
According to the study, the United States received a total of **36** attacks this two-week. The second of this week was New Zeland and Brazil with 6 victim, and the third was the Australia.



Important Ransomware Group Activities

LockBit 3.0

According to Darkweb Ransomware activity detected by ThreatMon Threat Intelligence Team, **LockBit** 3.0 Group attacked the **host organization in Los Angeles** in its attack. 15TB of data was leaked in the attack.



UNTIL FILES

11D22H32M51S

PUBLICATION

Deadline: 12 Jan, 2023 16:10:39 UTC

hacla.org

More than 15TB of files | The Housing Authority of the City of Los Angeles is a state-chartered public agency. Established in 1938, HACLA provides the largest stock of affordable housing in the city Los Angeles, California and is one of the nation's oldest public housing authorities.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 31 DEC, 2022 16:10 UTC

UPDATED: 31 DEC, 2022 16:16 UTC

5. IOC List of Ransomware Groups

ThreatMonIT recommends adding shared IOCs to your blacklists of security devices to avoid ransomware attacks. We will share with you as we reach new IOCs.

Group Name	Type	Indicator
LockBit 3.0	SHA-256	B4B64A9BE8E9D1A54232D81AE56E7D801827739EADA17DC92659B98D7189ACD2
LockBit 3.0	SHA-256	92EBB2DCE3E8F3D0E919C0342FDBE9A37D672A0CCA6B105395745EBC783DE6E5
LockBit 3.0	SHA-256	12FE5477FF75361DA81C170C132A1090390972279B17F3BB5FEF6A5CCC91326A
LockBit 3.0	SHA-256	8776879E76C6554C6B746CF17A258527B1A1FE19720E8516CCABB50750F71830
LockBit 3.0	SHA-256	622D8808B869AE33B580D9060C6316923AAB4F69359D6C8F80D041BB48F27B48
LockBit 3.0	SHA-256	407E95B0115F91ADA6732377DA7D074EE4E116F69CD3E833A6AB958CC359B4D3
LockBit 3.0	SHA-256	B5313A1A23ABB2232B90AF58BFA71AA05B482EAB675B636764EE6A6AEC40617C
LockBit 3.0	SHA-256	0706CE6FAD6AA38F780F5660B2D2CC51F9F649E2341E5FCC5943A549D0F816E6
LockBit 3.0	SHA-256	EE2115E39FFC78A185D533FAB74EE5683F233C3D0865443EA9FCADEAD1FC99EA
Cuba	SHA-256	0BFB61B8A16CEEFC98ED0B2563F2616211E8CBD624858BB7942B03F6F6E0A7A6
Cuba	SHA-256	A5CFF4EF10C2291A814F453BFEA694123BA30BD0D660AB9DDEEF3F6B91F1F3F1
Cuba	SHA-256	CAAAF5A9D077AF7F77E16469651385EFC39C0C088836B971F591EAF39F385DD3
Cuba	SHA-256	BDCC007B734EF4CCFACD2F70DFAC61F6FC979C71C55D3CADF653CACBF1E55AB5
Cuba	SHA-256	B7F2D03FCD9AE1C8B12622C9DB7486CCFA996A292500B7A5A145DB5316C39877
Cuba	SHA-256	C5763D02907D55E01668B58F182EA1E74C9343C8723B08DB4539CF79FC82BC46
Cuba	SHA-256	DD48F1529EAEE73703902BFE0273163C6DB80FF9ABF7AD76DF424D46AAF20344
Cuba	SHA-256	E142B6B6A514A3790ED0C4434BF7C3105EAF7A70061D4D8FD020319AB4D77B66
Cuba	SHA-256	E214BD3C2C17FAA46AC065888FA6B2C2097305E2F1C1EE46CDBD180E254B7DFA
Cuba	SHA-256	D22BE0BF708D81D72E535E538D08F8576C79DD3F5A7B23CC93952D560C7E1C66
Cuba	SHA-256	1ADC99F82DE60973CF48C8123727A03B2751CCC67756A685F5A1C426B0BECBD1
Cuba	SHA-256	3E5DD23AD7CE360DED21C758D538F6D30D63CA621CE582F51BAED9EE5058FEE1
Cuba	SHA-256	D44028B7608526043683C77CFB32EF47E966B57C09110B46490CE738E2BE09B1
Cuba	SHA-256	6CAEA7523F269229751 7CB372A6B840C60E4AD1E20A5B14B93C67C1C7D655C60
Cuba	SHA-256	EDC480AA00393A5FC3E0D13C852C28CEAE159E18220A0714504D9A628B10F03D
Cuba	SHA-256	E84061409282650613725AB5E76C4FC656216EF2E0862AE39C72427351936D54
Cuba	SHA-256	FAEC9307E9D87C908A7CDA543D83AECF1F57F3417C23DFB0B2FD195CEC1212CF
Cuba	SHA-256	6335DAE48DA752A0EAC00DC62ABBF195E5A645D198B5997F21C02397F7498F78
Cuba	SHA-256	29D873740798302BD7E413C4DC49D1565CF9DC8B483AC23F554372150E052EB
BlackCat	SHA-256	21DE46ADEB3989E6543B75E08D1ED59685821613D3E4E8008C694D3BC7143CC2
BlackCat	SHA-256	B9C894D5BD6979D314F62EF9E7F5367F097645D7E7DC361A7AC1BF6B39A5A72A
BlackCat	SHA-256	3539C61962135C39176BA278FFFE871D39D7F2055000650F8B13BDCAD2D0D502
BlackCat	SHA-256	D0A91A7FDAF19A825CF4EAFD186D5DA7079CFE9B54F7D51B850E6AF303725483
BlackCat	SHA-256	6762FA1F49B436F8D7180B06A8BAD76F70E2BC1403F28B194A58EE96118F2462
BlackCat	SHA-256	4E526790AF180C4BA5D55F32BBC716A02CD92D29E07D99F6B112BE6F77EDC291
BlackCat	SHA-256	8EE191B51B853ADDC862307C8F641BD251A8B7DD88263D228453BB06882F2464
BlackCat	SHA-256	779850280CE47128FBA4FD259012589619DB7958C6599C0AC2C29BE5F816DA16
BlackCat	SHA-256	C4C49D2DA33892FC0FB8D961A5D504B9F458206E0366132C8A0D017D6E8767FF
BlackCat	SHA-256	E24DBE52EC795C6AB434CD8AC7AA0F3AFA536C2D22660CC0A4885400E5A2CEEC

BlackCat	SHA-256	74ABC075FC1D5C8985C952AFC25A48BA874E76F96AF4DC33414E84DB9E10B9EE
BlackCat	SHA-256	0556FD67CF6EAAEE474EB5CE2493097ED612BF31E2ACD57D27CBC46D5451ED13
BlackCat	SHA-256	1969D1A7F08933AC364924475DB158D38E338267CBAFFC34DF81064461FC2F75
BlackByte	SHA-256	59A5745E61DF891F76D047C34A24C69BD48163C2213ECEB6D7DF6D1AA9068A89
BianLian	SHA-256	42B0606AA2C765C0B0789B47EBD3A3F43144DC0C20B2FF6DB648AC5FEB0A37A3
BianLian	SHA-256	3A2F6E614FF030804AA18CB03FCC3BC357F6226786EFB4A734CBE2A3A1984B6F

You can follow our GitHub Repository to get better IOC data!

GitHub

ThreatMon

45305 Catalina cs St 150, Sterling VA 20166