ThreatMon

Ransomware Group Activity Report

17.10.2022 - 28.10.2022

@threatmon

@MonThreat

ThreatMon

Ransomware Group Activity Report

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

According to ThreatMon's one-week security survey, there were **103** ransomware attacks. The USA was the most targeted country. In addition, the most targeted sectors are Industry, Technology 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

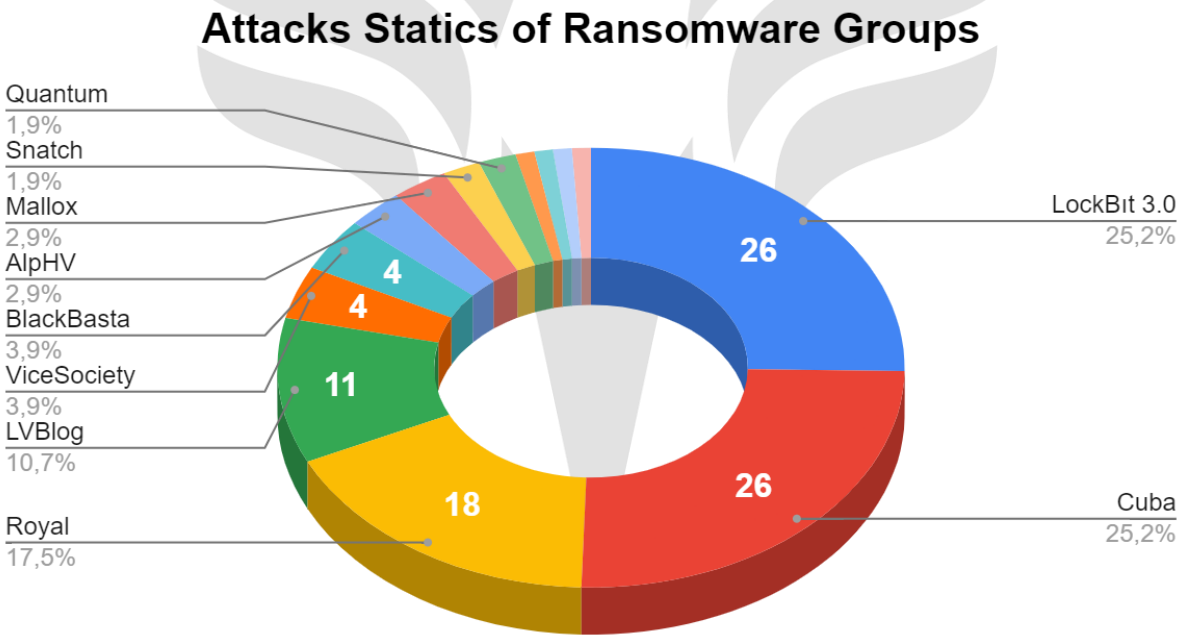
1. Number of Attacks by Ransomware Groups

During this one-week period, the most active group was the **LockBit 3.0** and **CUBA** ransomware groups. While **LockBit** 3.0 had very few attacks in the report a week ago, it took an active role at the beginning of the week. In addition, **CUBA** has carried out a lot of attacks this week, although it was not active in our previous reports.

LockBit 3.0, which was one of the most active ransomware groups during a week, and LockBit 3.0, which carried out a total of 26 attacks in a week, mainly targeted the Industry sector. It also targeted the United States the most.

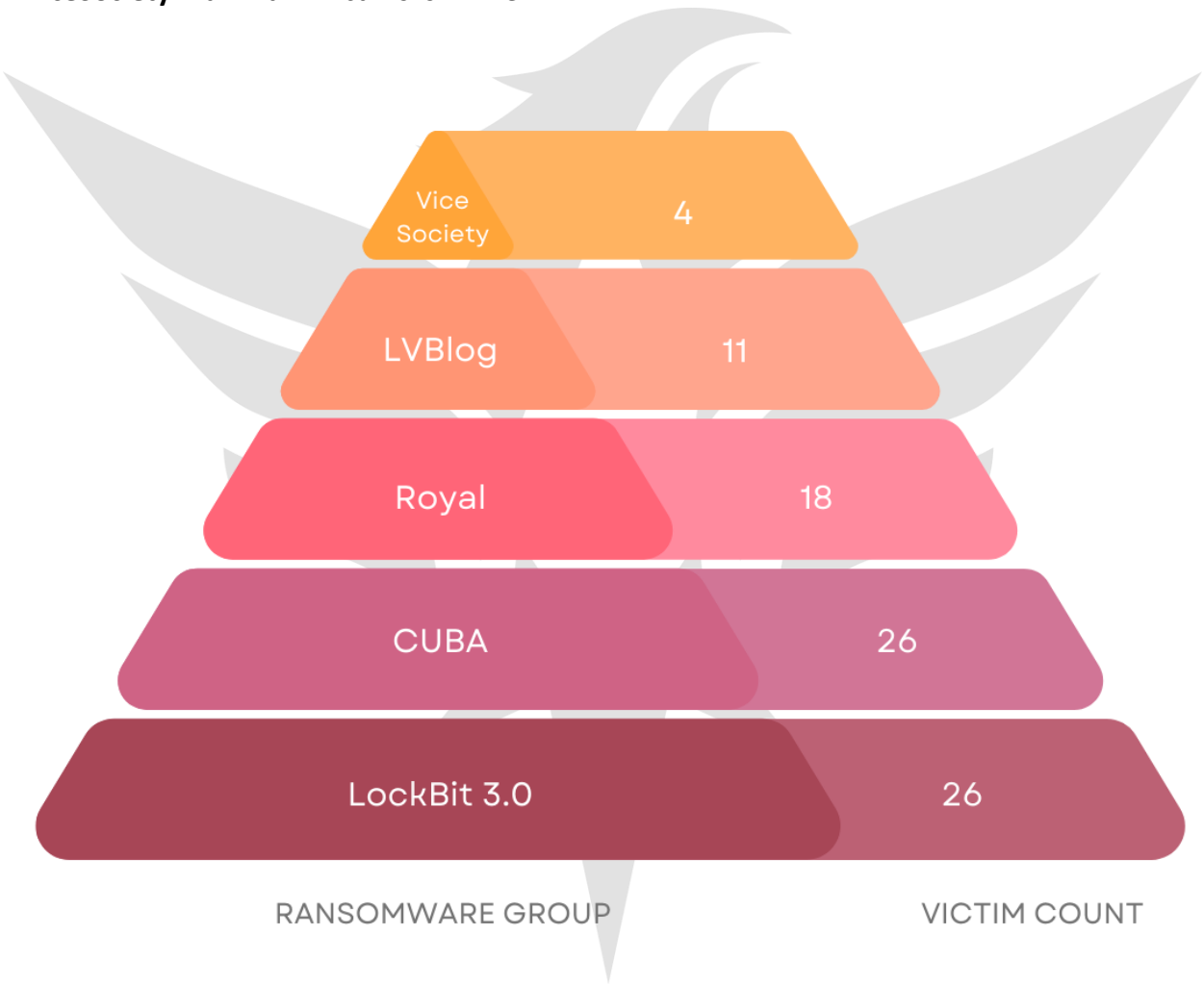
The second most active group, **CUBA**, carried out a total of 26 attacks, targeting the Technology sector in general, while targeting the United States the most as a country.

The third group in the report was the **Royal** ransomware group. Royal targeted the Healthcare sector and the United States country the most.



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

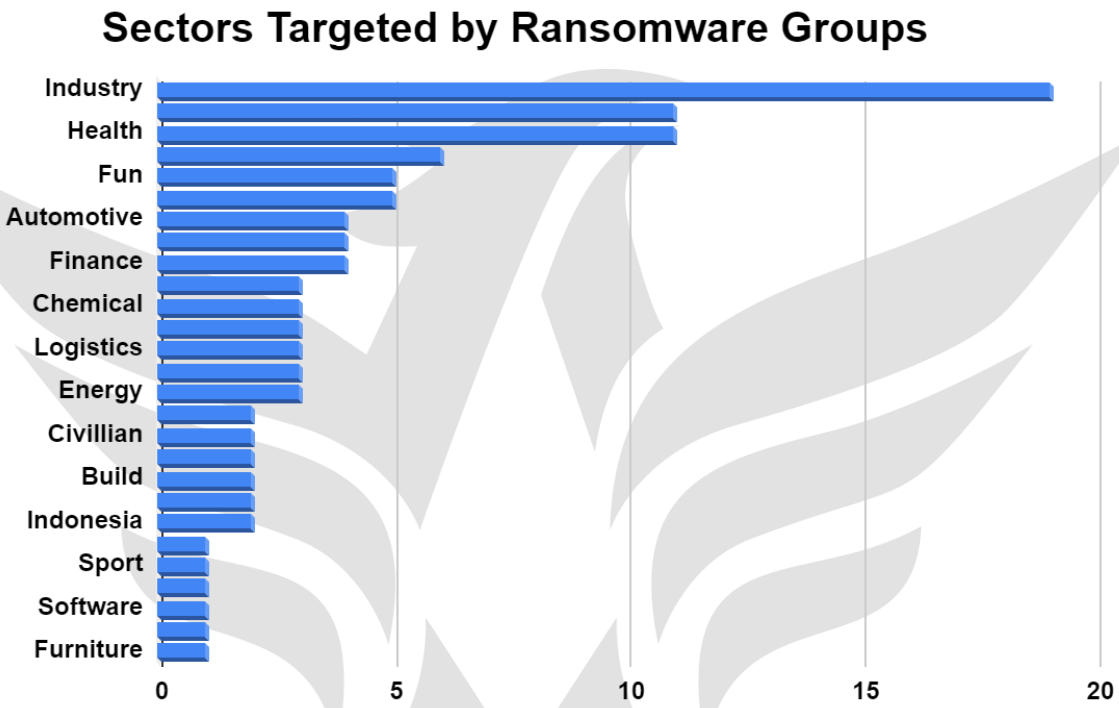
- **LockBit 3.0** is the first with 26 victims,
- **CUBA** second, with 26 victims,
- **Royal** third with 18 victims,
- **LVBlog** fourth with 11 victims,
- **ViceSociety** fifth with 4 victims is in line.



2. Number of Attacks by Sectors

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

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



As in the previous report, there are not many sectors that have changed on a sectoral basis. As in previous reports, there are intense attacks on the **Industry** sector. The **Health** and **Fun** sector also ranks second and third.

The target of current attacks are Industry, **Health** and **Fun** sectors.

3. Number of Attacks by Countries

According to the study, the United States was targeted 47 times in early November. There are more attacks than in the previous report.

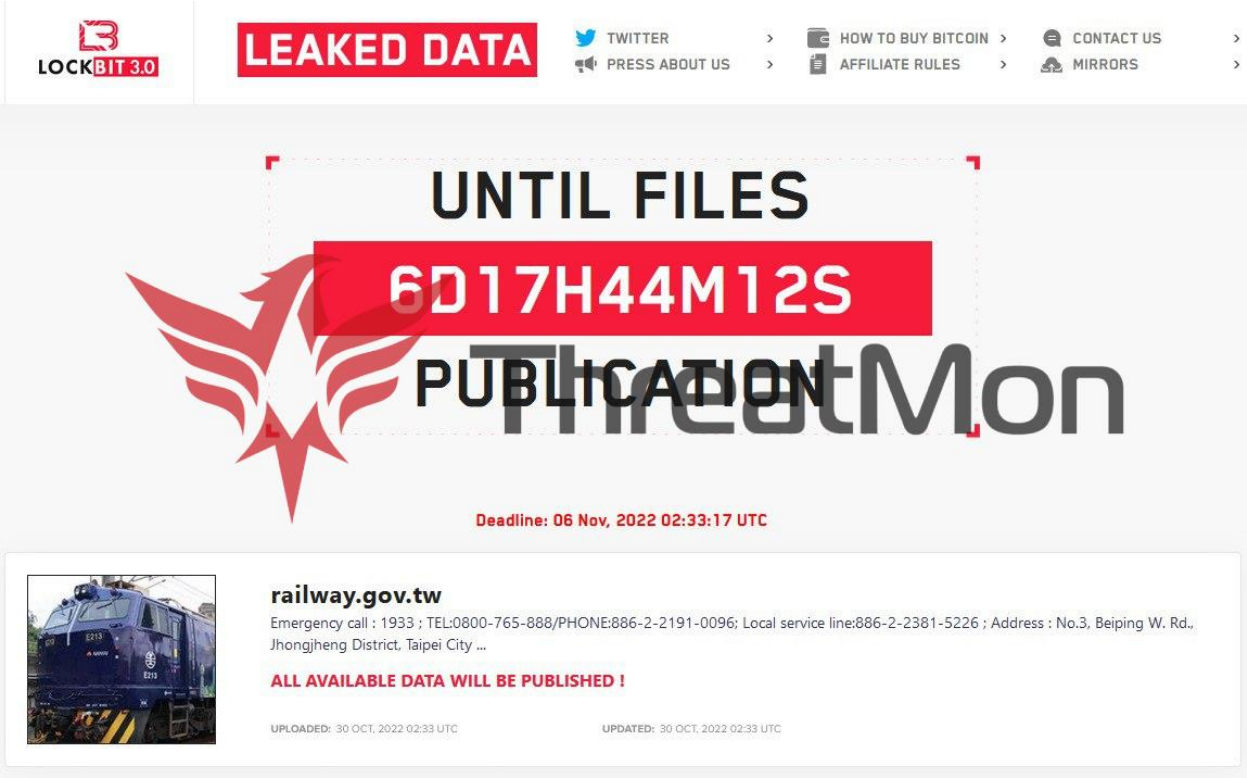
The second most targeted country was the **United Kingdom**, and the third country was Spain and France.

United Kingdom is in the top 3 as in the previous reports. Attacks on **Spain** and **France** were also detected as 7.

Important Ransomware Group Activities

LockBit 3.0

In the ransomware activity that ThreatMon Threat Intelligence team detected in an analysis of dark web activity conducted on October 31, **LockBit 3.0** found that the group had attacked the Taiwanese Ministry of **Railways**.



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	7775C69795384C210F948B3C6D5B1A14A6C1EBB3CF156A63007FA7D749D90B6A
LockBit 3.0	SHA-256	1E9DBB8067B810A7EFBA676F83F0F250708C15B5BFF58CC5E0D5635B7EC6E05F
LockBit 3.0	SHA-256	DCCD5BF6F9172A5A40FE7D98AD9E0895AF833984899B2854AC1513459D009D69
LockBit 3.0	SHA-256	FAAA06208ACDF230496128DFD656984D3F0F99A9B5BE4F2CBAAEC0BB830BDCF9
LockBit 3.0	SHA-256	F978A39F80FE81BE9F9F98B00ADF88A8B7300BD5D311597D00DAA47DA3676369
LockBit 3.0	SHA-256	931622391C1324DC7964AA5576B1A7A168382B0DCE22399FBECA9AED468138F3
LockBit 3.0	SHA-256	40B2724E08232E2A46F3EE36E9B0E5EE2BB49E81570ABEB28035ADC71DB8AC99
LockBit 3.0	SHA-256	7878F6F17B90A1695D73DE830DFDD8BDC62F365DAB88BD42B13226668F913254
LockBit 3.0	SHA-256	8B3D44F099888635FC995A5362159BBEC7DA1954EAA2FED7BA41650447CF2277
LockBit 3.0	SHA-256	BCACA6FC1D5ABE8D437D22FC4FAD17CB37EB727F84F4F07DA1F98D279575E1F0
LockBit 3.0	SHA-256	C6902F14BAFB0FA5C7B46A3AFE0FF71245C0BB26AC07B187FF58FD3FA381DBCB
LockBit 3.0	SHA-256	4672F4ADE47A4717255DB6BCD9AE1FB6F4D71E85D059BB08E65DF55D416126EB
LockBit 3.0	SHA-256	9FEED0C7FA8C1D32390E1C168051267DF61F11B048EC62AA5B8E66F60E8083AF
LockBit 3.0	SHA-256	BDC2801E747EE4DD2B50B1ECD3FA3EB53B6C8101EC37EFF8D18E485A7F4A7BD0
LockBit 3.0	SHA-256	E216372E4328F1CF5CF39A73540B508ADC8D777FEF90CA77AF635C2331DEB5CC
LockBit 3.0	SHA-256	5B9E6D9275E9523AA3945BE891745442A07B936EE5236E23934250BA3844F65F
LockBit 3.0	SHA-256	74B4D14D2D1AF6642D5867EB89C277AA02F5E4AC667D87B5ACA380F40EABE1BF
LockBit 3.0	SHA-256	50FAD26D726E0AF6DBED3225267934AE9EF22B31E48FC623CE93BA582A7E6110
LockBit 3.0	SHA-256	EA6D4DEDD8C85E4A6BB60408A0DC1D56DEF1F4AD4F069C730DC5431B1C23DA37
LockBit 3.0	SHA-256	A696AD284E82463E8E7942976BC517FEB4247E42D14595C5997C2E6558DC17A9
LockBit 3.0	SHA-256	2F9C6EE5A9736C34715A0715C43592E84054C4A595DB1E3E86544912E4FA273A
LockBit 3.0	SHA-256	DCBC6A5F2F02209075BF3C2249D740CB16A1CA4C9706D8E0AD8C22F19E9AED2A
LockBit 3.0	SHA-256	C765054B9257AEC7B891164C84765A57D5BADC659CDA230CF67B2F7BC5112278
LockBit 3.0	SHA-256	B7A17D6F314FA58A8F36B9B15B730ED4F9DDE19BC00101F9B0433C733D4D54BB
LockBit 3.0	SHA-256	890C8453F6D62E49B77614199599848E6C58BFD38255BE7D3809444012349ED4
HiveLeak		F0E8EEB7582943E3DBB78F3D39E265998E7C82F0FF368603E09382B8F2AA0F80
HiveLeak		27C9E57A7B2AB447E43F4053C05C9DEA128811255F9FE9E7722EE26A834BFD38
HiveLeak		C72C3E4322467501ECDD4DD18E879E4EA65DCA03D9DC9F7F0282E092AF553E0E
HiveLeak		8C5526650D48864F1584FCF74F9C29A77430EB1FFC58D215CB4D4E33C7B7C1F0
HiveLeak		50CCB1B00BDD8FC3D8957BDF718C17887ED3CD59DFBEB247193A33041CF6E03B
HiveLeak		DD7A018D9EE987FD7027E438B2636E802D98C2DD7ACEAF2EC6DB711FB08C6DAB
HiveLeak		B4297174E47D9ED2808524165BB5C09D0CB85E342DB72B955EDD4D5A0C490F9E
HiveLeak		83A361E88CB033FB4E3067A00DC0E1458DC2DCC68B9E0D01F4EA16B50DB9EE11
HiveLeak		25D18C3823A3B210A18E69C823CE4C59FAB298C315AC2A5D891027921D1C6D7E
HiveLeak		CD9077BF07EB4183AA5D7093CD32C9FDDC43E2ECBA91A682D666B041C39A4CD2
HiveLeak		76960749ED11D97582923E31D59115910AE74D8753C8E92F918F604CA8A0D26D
Cuba		3DE7F2811389605BA6A33FB638A0843F9F53F00CA4D3F7C162B5A3B3CCCF4B8A

Royal		9DB958BC5B4A21340CEEEB8C36873AA6BD02A460E688DE56CCBBA945384B1926
Blackbasta		48976D7BF38CCA4E952507E9AB27E3874CA01092EED53D0FDE89C5966E9533BB
Snatch		384F06A404160E73164B7DE7F9675E472BF4DA5683A63486BF0F711D72836A84
Snatch		BD210A991A37E78DEB6CD2E00AB60445326CA9DAFD2E5C4CCC71028D88B4A70F

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

GitHub Link: [ThreatMon 28.10.2022 - 04.11.2022 Ransomware Report]

ThreatMon

45305 Catalina cs St 150, Sterling VA 20166