ThreatMon

Ransomware Group Activity Report

13.01.2023 - 27.01.2023

@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 **59** ransomware attacks. The United States was the most targeted country. In addition, the most targeted sectors are Industry, Health and Education.

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 was the most active ransomware group in the last two weeks, with **1** more attack compared to the number of attacks in the previous two-week report.

Targeting the **Industry** sector the most, **LockBit** took the **Education** sector as the second target and the **Aerospace** sector as the third target.

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

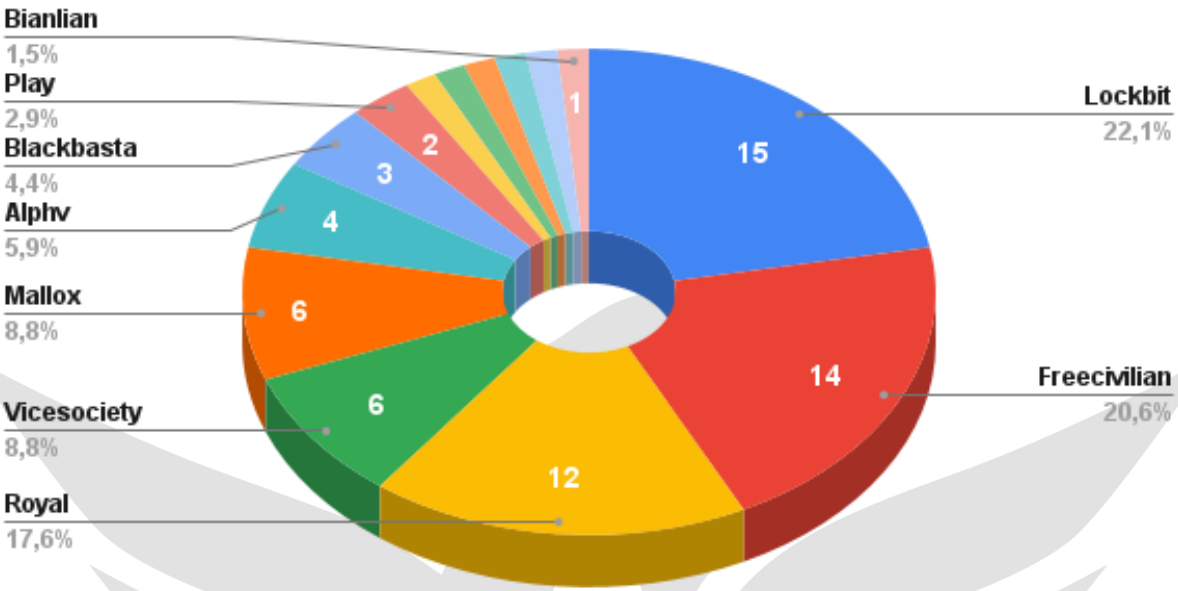
The second most active group during this two-week period was the **Freecivilian** ransomware group. Freecivilian has carried out a total of **14** attacks in the past two weeks.

Over the past two weeks, the **Freecivilian** ransomware group has only attacked the Ukrainian **government**.

The third most active group during this two-week period was the **Royal** ransomware group. Royal carried out **12** attacks in this two-week report.

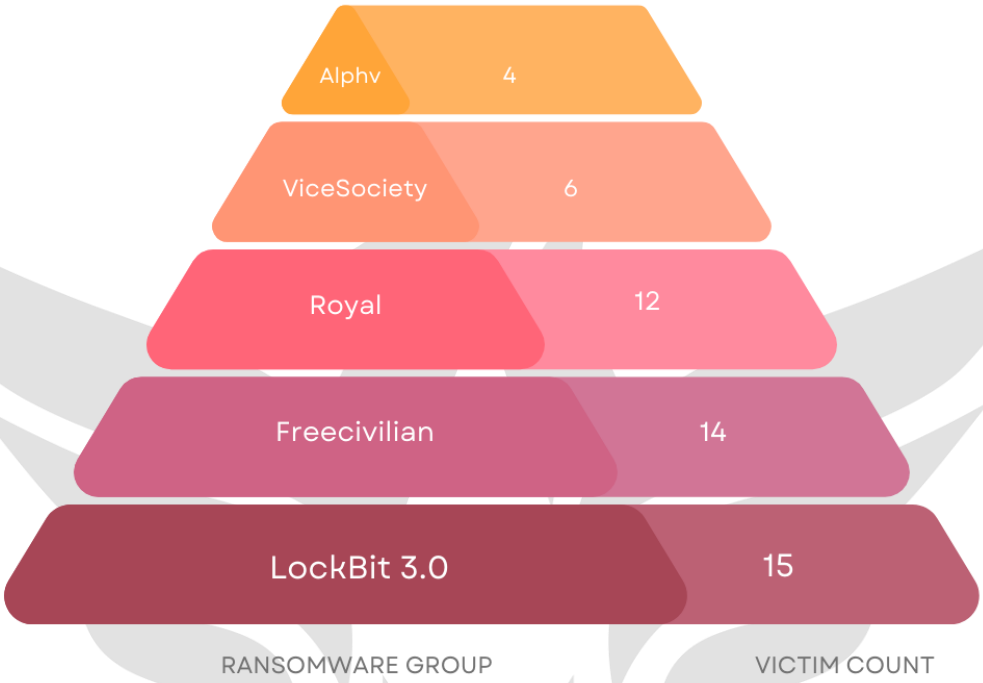
Royal, targeting the **Education** sector the most, took the **Logistic** sector as the second target and the **Law** sector as the third target.

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



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

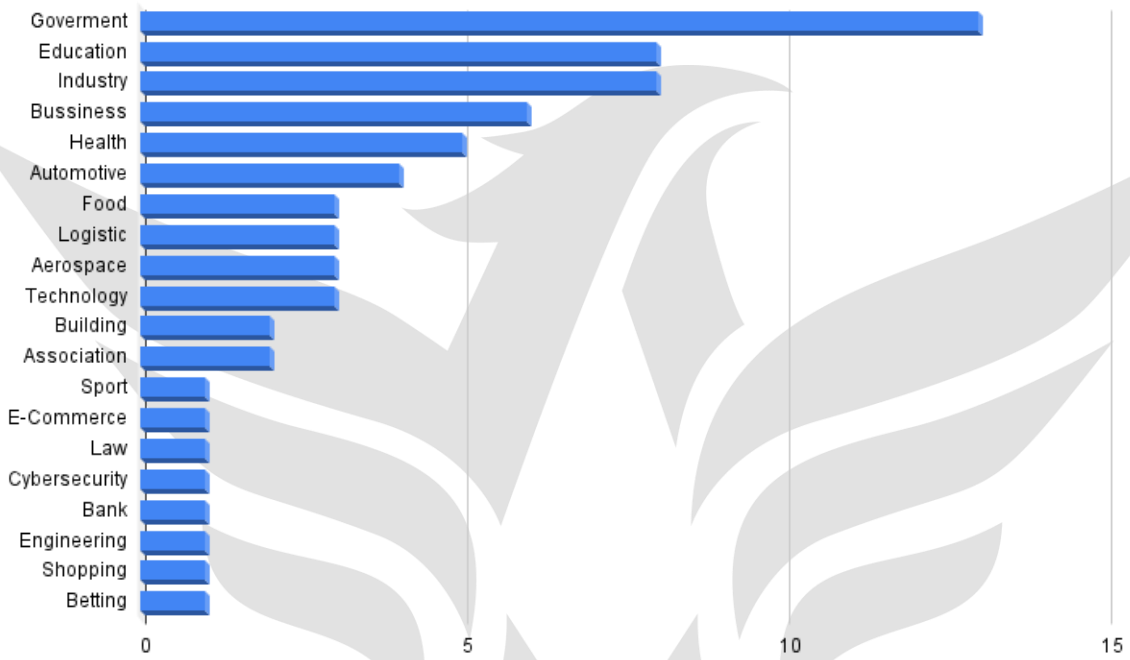
- **LockBit 3.0** is the first with 15 victims,
- **Freecivilian** second, with 14 victims,
- **Royal** third with 12 victims,
- **ViceSociety** fourth with 6 victims,
- **Mallox** fifth with 6 victims,
- **Alphv** sixth with 4 victims,
- **Blackbasta** seventh with 3 victims,
- **Play** eighth with 2 victims,
- **Ransomhouse** ninth with 1 victims,
- **BianLian** tenth with 1 victims is in line.


Alphv
4
ViceSociety
6
Royal
12
Freecivilian
14
LockBit 3.0
15
RANSOMWARE GROUP
VICTIM COUNT

2. Number of Attacks by Sectors

Ransomware groups prefer to attack the **Government** sector at the end of **January**.

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

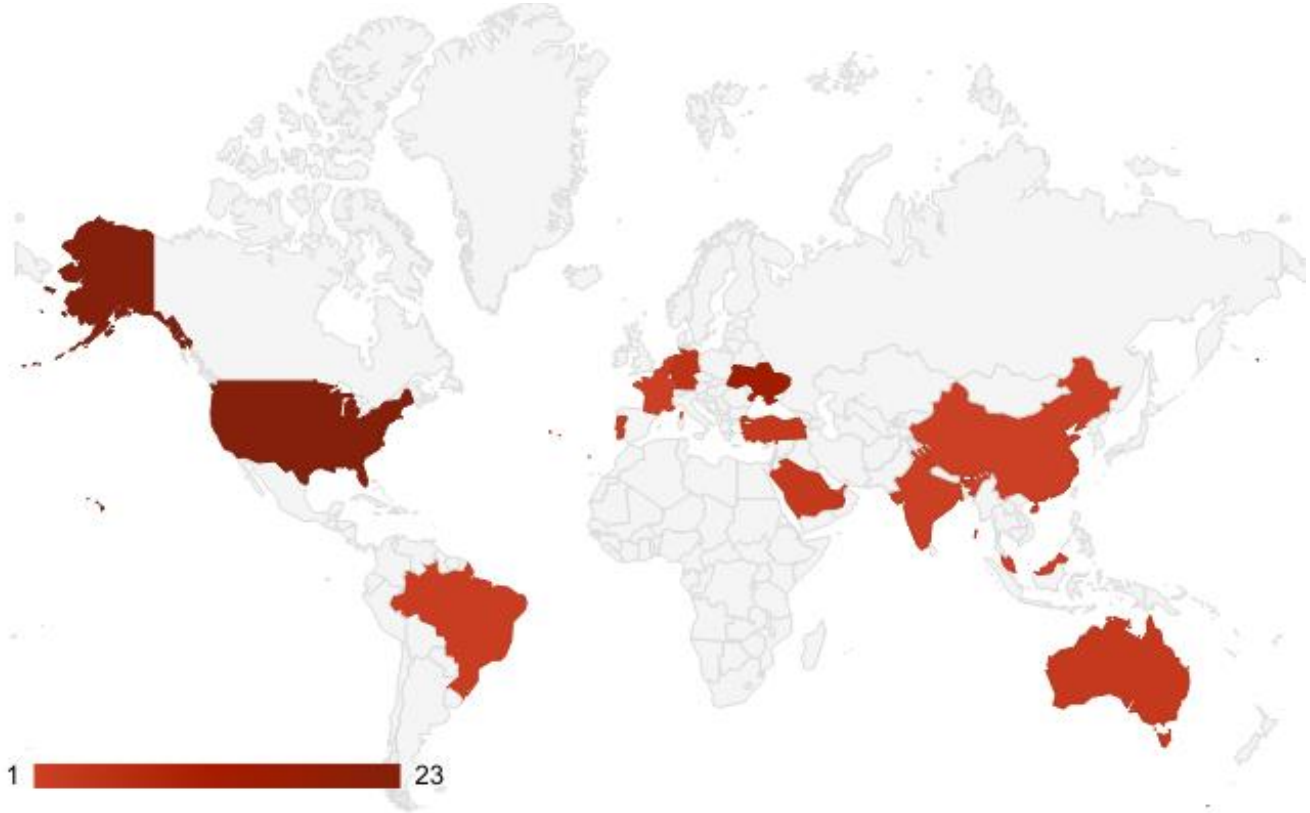


As in the previous report, not much has changed on a sectoral basis. In the previous report there were a lot of attacks on the **Industry** sector, but this week there are fewer attacks on the **Industry** sector.

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

3. Number of Attacks by Countries

According to the study, the United States received a total of **26** attacks this two-week. The second of this week was United Kingdom with 6 victim, and the third was the Sweden.



Important Ransomware Group Activities

FreeCivilian

According to the Darkweb Ransomware activity detected by the ThreatMon Threat Intelligence team, a **pro-Russian ransomware** group called **FreeCivilian** has launched a ransomware attack on the **Ukrainian government**.

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	6d6930d0af84cfa9baac15afc06cc20db5a6b1729837076a623e3acea85dfd28
LockBit 3.0	SHA-256	8bb8901d08673acae9210a915460fcb872a7b162f7ade6f82e4e7f8b33a39f12
LockBit 3.0	SHA-256	19fd40bbfd799ae29c2d261e18776f8a1f82328f80dca1cda3c23ee66fe38265
LockBit 3.0	SHA-256	54b45f35926b12f7853e4854ae1d0a233ba1817451450d9b9fdf4e9b1412024f
LockBit 3.0	SHA-256	2ecf1fe02d8fb099b68e4d9bceeeadbe5fc8347f5a76d52f35ed48b516963735
LockBit 3.0	SHA-256	6d6930d0af84cfa9baac15afc06cc20db5a6b1729837076a623e3acea85dfd28
LockBit 3.0	SHA-256	5181d2e71e8e73a82712a483a80aaea94e1efa785f2b8b8ee9641544c0b652f0
LockBit 3.0	SHA-256	cc58dcd32a440e7f95d19b653a55c1e2c383efc2bd19443238dd3008c1cbe147
LockBit 3.0	SHA-256	d1a4e6a654f0f8afa998099cd95faf882918a9d266028b578be7bcf4e123ba17
LockBit 3.0	SHA-256	2ecf1fe02d8fb099b68e4d9bceeeadbe5fc8347f5a76d52f35ed48b516963735
LockBit 3.0	SHA-256	1a53460ac8889d82b47b704638f0fa9affc3d7ae5ad6f4cb7d02dce67f10e292
LockBit 3.0	SHA-256	f588bb8ccdb3f42a5496320a2ada62fde9b4f62a4b032898269fdf2b30e435bf
LockBit 3.0	SHA-256	c7c9eae3014b1a74ca28502dd405cad8beb0816be1cf72be09a1b85bc872171e
LockBit 3.0	SHA-256	93235f529380142c6fb6ddd92925b87fbe6a66eb6eb2d5516c64dc4ebc21a4af
LockBit 3.0	SHA-256	6f4b3d01bc6352bbd27fb34a11fbbf6ed76d13b44c00917da50b319be268a670
LockBit 3.0	SHA-256	ff1675c74d25d4f967c5a20b198568e5cf8796b844e234205bc57dece8bf3294
LockBit 3.0	SHA-256	ea09f2602ffeabc7f0c1fb4f85177e2a2f6cd5da255c5c6ddec928fa834ac50b
LockBit 3.0	SHA-256	5181d2e71e8e73a82712a483a80aaea94e1efa785f2b8b8ee9641544c0b652f0
LockBit 3.0	SHA-256	f2339af63aacd5774958493d0ceead11477487f941c668a85b1f5f2e69efd078
LockBit 3.0	SHA-256	a7b1c239363c65345a84a1db7c12236445a588f1cdd9d204a0a8816b6a7dfbce
LockBit 3.0	SHA-256	48a17965c09265af50b57858c2eb998161ad9c794b47518cb02a91e9752520b1
LockBit 3.0	SHA-256	5a6ab286167ab7562f9b81ce35dd2592195d56bb1b41858e56a9b675b15b89a9
LockBit 3.0	SHA-256	cca82a51574a59586e518ff82f2b5a8e0522f0306ddc221be800cff0aaecaf6b
LockBit 3.0	SHA-256	ea49b0e546b2dc7b757db0606b2f6938f5adde2f44a3ca00299484922c25c916
LockBit 3.0	SHA-256	7a29396c6d1694100f379bab9d505d1d2f699a2cea04c1b2016a7df8ac25b9e1
LockBit 3.0	SHA-256	024569fc4f3ad57d299ca3b07b8984b4aea164720c30f98f4de4abb33e0fefef
LockBit 3.0	SHA-256	c898a07ac3e02231a48bf55bd8828d4c77c7ea3c5cfe80e9eec44c81cb476cbb
LockBit 3.0	SHA-256	92ebb2dce3e8f3d0e919c0342fdbe9a37d672a0cca6b105395745ebc783de6e5
LockBit 3.0	SHA-256	3092f9333b35820452ac1cfeef9ac3ca31c7e55b6542bf1ba7a661f3bb734741
LockBit 3.0	SHA-256	70b44333f5f30e21af276d2b2d2f4e6c55096cccf9c5de374b069e9e57aa8520
LockBit 3.0	SHA-256	9063d570ba7a4a070a9eb9d9bc32736271a9e36330cb766b6b1eaf781f6ad902
LockBit 3.0	SHA-256	77bb89305af11dffd9dae45ef727f4bee42c7dcb7cf960ddbf2a7012ee6c9997
LockBit 3.0	SHA-256	fa301009c4bfe1c66a9e33f41e7783dd5c5a4dd42bb6ff771c80dadcf8e71640
LockBit 3.0	SHA-256	4e3cb67f5e6d03d30ce5aec1b3db930bad9b0766f560dc9d118271db1d585db6
LockBit 3.0	SHA-256	fe75d0662ae9fd86b959e799405a05d3dd6e61e5239ae320662b3a4c1d36d78c
LockBit 3.0	SHA-256	1bd9426232d1ca052d01283b0239ad02ebd66d9ac48d9107f10b1c463da2d51d
LockBit 3.0	SHA-256	744250911f663ab967196b31e4a3b11631f0df76aba6f30e8f0f5c5d0463ade6
LockBit 3.0	SHA-256	e4a2260bcba8059207fdcc2d59841a8c4ddbe39b6b835feef671bceb95cd232d
LockBit 3.0	SHA-256	2aea219886d4c7db413aa251a4d1b9e9a9d4c82f5a9cbea8676ecf6380a5e53d

LockBit 3.0	SHA-256	b30cf6fa9d6c3f83297f33271808170f7f5808a1ae189cb1088748bf14d91747
LockBit 3.0	SHA-256	384406221f7a028ea4094072ce819ab664b6e43df148887f9794734f15855ca7
LockBit 3.0	SHA-256	87658a3c5cd72eddc1f3c52b489ed43e59a0d044c849f300e0f7537568e0502f
LockBit 3.0	SHA-256	08f5fa00c8602b9ca095062a1976a6fec9c9c1ba78442a1c3439a43ed6066320
LockBit 3.0	SHA-256	34fa7d9b2f0499db6bacf9630176e64e45521328937c6abf8c783df7276ae30c
LockBit 3.0	SHA-256	8645d03bf286068284d53bdde57f42d7a2d25204b850e48e486a1cbd8fbd8281
LockBit 3.0	SHA-256	291ae4c5073c93db10a956071dba23ebae34032ae2fa3229f8abce314316397e
LockBit 3.0	SHA-256	9d3bd40aa55bd1857b4b8a50d32638ca2a51b2772455bc2d29d07cfa296b243d
LockBit 3.0	SHA-256	0adcd16429a3926e2cd8d054febc83ff6bc90404edd4b1d48049554d0acffb89
LockBit 3.0	SHA-256	5e7933423103afd6abae77fba9aa18456e60b73922a327fd08303cdb760586c1
LockBit 3.0	SHA-256	582a003798f1bff747256102e5af344219813205b728cf3213100ba5f5c08507
BlackByte	SHA-256	a1d5f41922a69e14738acf56ab35e3339706d5264d6b1fc56a600b84885598fb

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

ThreatMon

45305 Catalina cs St 150, Sterling VA 20166