ThreatMon

Ransomware Group Activity Report

01.01.2023 - 13.01.2023

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 **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 had **9** 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 **Consulting** sector the most, **LockBit** took the **Industry** sector as the second target and the **Automotive** sector as the third target.

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

The second most active group during this two-week period was the **AlpHV** ransomware group. AlpHV has carried out a total of **10** attacks in the past two weeks.

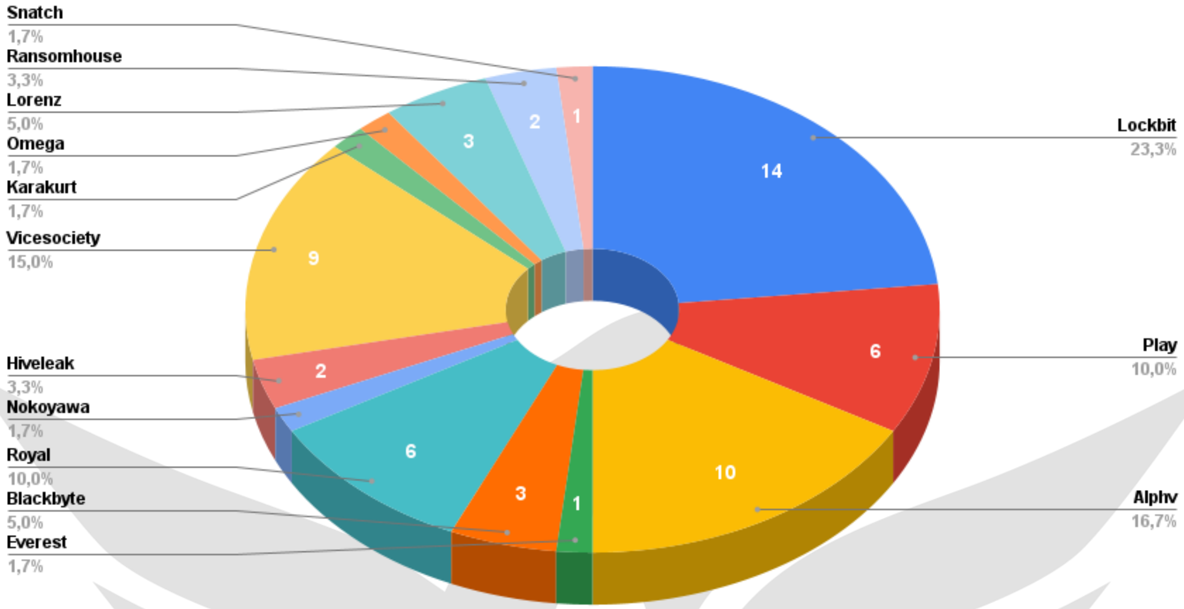
Targeting the **Industry** sector the most, **AlpHV** took the **Finance** sector as the second target and the **Energy** sector as the third target.

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

The third most active group during this two-week period was the **ViceSociety** ransomware group. ViceSociety carried out **11** attacks in this two-week report.

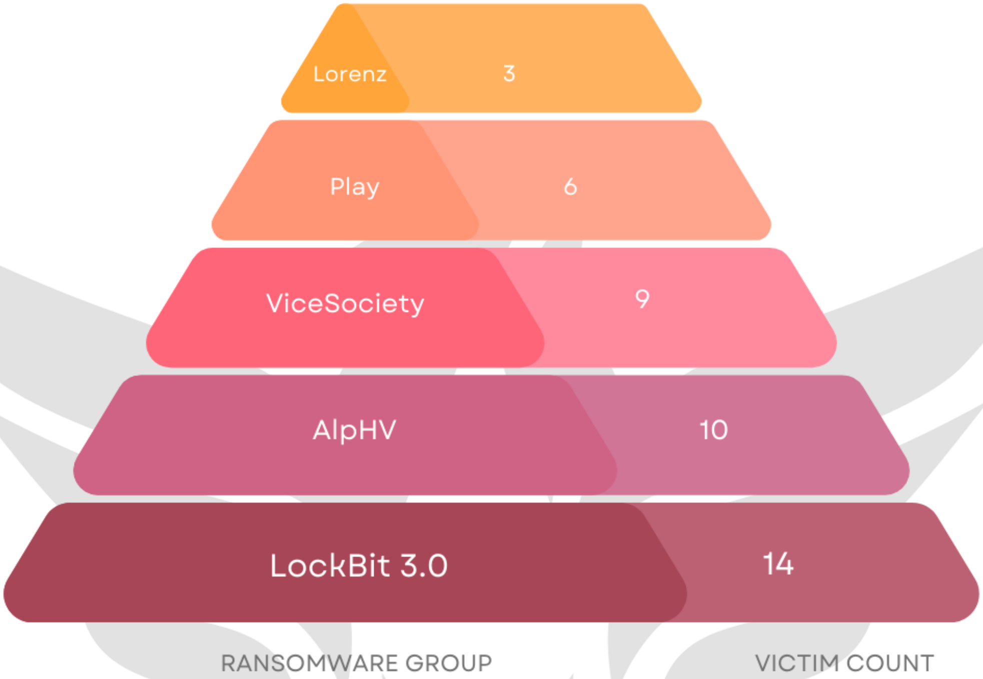
ViceSociety, targeting the **Health** sector the most, took the **Education** sector as the second target and the **Market** sector as the third target.

Targeting the **United States** the most as a country, **ViceSociety** targeted **United Kingdom** second and **South Africa** third.



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

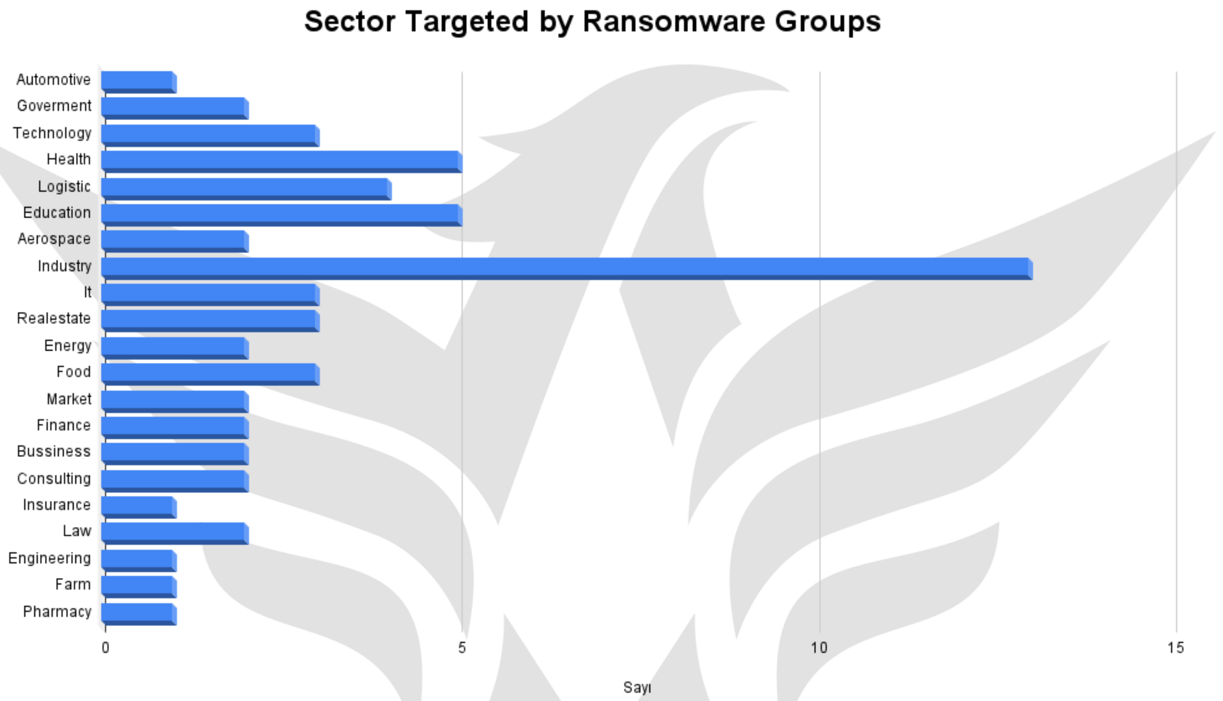
- **LockBit 3.0** is the first with 14 victims,
- **AlpHV** second, with 10 victims,
- **ViceSociety** third with 9 victims,
- **Play** fourth with 6 victims,
- **Royal** fifth with 6 victims,
- **BlackByte** sixth with 3 victims,
- **Lorenz** seventh with 3 victims,
- **RansomHouse** eighth with 2 victims,
- **HiveLeak** ninth with 2 victims,
- **Karakurt** tenth with 1 victims is in line,


Lorenz
3
Play
6
ViceSociety
9
AlpHV
10
LockBit 3.0
14
RANSOMWARE GROUP
VICTIM COUNT

2. Number of Attacks by Sectors

Ransomware groups prefer to attack the **Industry** sector in early **January**.

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

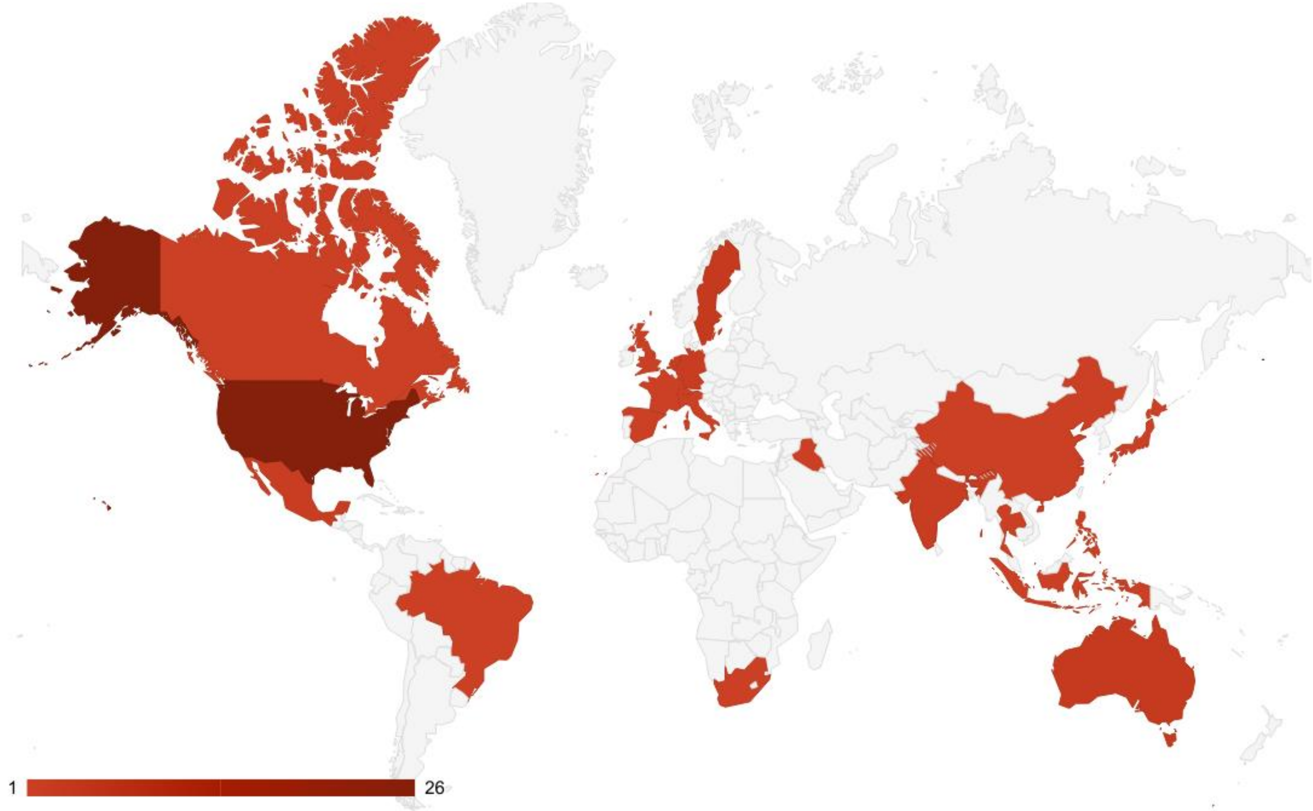


As in the previous report, not much has changed on a sectoral basis. In the previous report there were a lot of attacks on the **Industry** sector, but this week there are fewer attacks on the **Industry** sector.

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

3. Number of Attacks by Countries

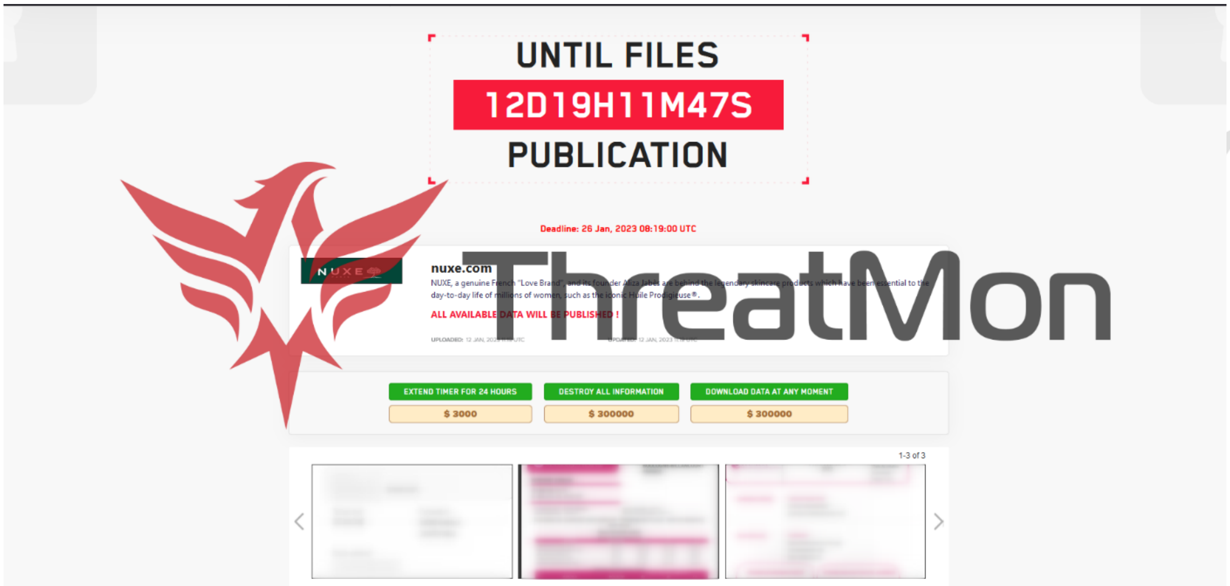
According to the study, the United States received a total of **26** attacks this two-week. The second of this week was United Kingdom with 6 victim, and the third was the Sweden.



Important Ransomware Group Activities

LockBit 3.0

According to the Darweb Ransomware activity detected by the ThreatMon Threat Intelligence Team, the Ransomware group **LockBit 3.0** leaked close to 30GB of data belonging to the **France-based cosmetics company Nuxe**. Among the leaked data are financial documents and documents containing chemical data.



UNTIL FILES
12D19H11M47S
PUBLICATION

Deadline: 26 Jan, 2023 08:19:00 UTC

nuxe.com

NUXE, a genuine French "Love Brand", and its founder Aliza Jabès are behind the legendary skincare products which have been essential to the day-to-day life of millions of women, such as the iconic Huile Prodigieuse®.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 12 JAN, 2023 11:19 UTC UPDATED: 12 JAN, 2023 11:19 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	1DDDD103482E6057CCEB35EECB20D8C7371F04AA04160C51F6A54D182BEF9F28
LockBit 3.0	SHA-256	D67B630523734689EB56DD0B61A42627D71C5C2A1FD0B873B0F50C781ECC056D
LockBit 3.0	SHA-256	8DFB58B5FB4E02923576D7A5A7E492DD44BA7613B19F481C1358AF521A4E0038
LockBit 3.0	SHA-256	7A59F387A926696968BEA7C8F891E79D7410C989BD6F20B77A3E5A2A29F0363E
LockBit 3.0	SHA-256	907DBD30488D89D7AEDD51E3DB8025B45356F23DED6FE496BE4BFE3FEFD02854
LockBit 3.0	SHA-256	D641AD955EF4CFF5F0239072B3990D47E17B9840E07FD5FEEA93C372147313C5
LockBit 3.0	SHA-256	92FC4B11841D923FD61C3A52FDE9FF17BA62FED5C31CA6BAA0681D6ABB76D957
LockBit 3.0	SHA-256	07A14091D3474BA6328C11B9C6E8B0179E1D5E631ACB9C5D2FC94F0202BE52E9
LockBit 3.0	SHA-256	C597C75C6B6B283E3B5C8CAEEE095D60902E7396536444B59513677A94667FF8
LockBit 3.0	SHA-256	7B9428E4DE23CDCF17346C776B29B50405D5E19986DE7004D94C6B7C374B449A
LockBit 3.0	SHA-256	0C26AF70969FABA8B3E60A5758C41A61A522AE3796BD6F93C37103E135DB6CF6
LockBit 3.0	SHA-256	637D5A2FDA898B6B9A774FB879BEF249D35E6C20906627FA0E33372C85F9A2FC
LockBit 3.0	SHA-256	90F509D90E386243434D0CF8764F99C099AC9F1E575DA435FF06457BAF0A48E5
LockBit 3.0	SHA-256	C0EB42FC6FB1BED8C7B1C75F4A58CB0A91D30FCF52B9A431F925C1577153C79F
LockBit 3.0	SHA-256	A9633E2C0EE1C0115F3EBAED015FAB85AE12BD18BD1AD7A116F31551EDD1ECCE
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	0EC61A80E61F56F460FC42E5D4F0ACCEC2B04C8DB98C28ED4534946214076F2A

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

GitHub Link: Link

ThreatMon

45305 Catalina cs St 150, Sterling VA 20166