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 **two weeks** of ransomware activity by tracking ransomware groups' posts on Dark Web leak sites.

According to ThreatMon's two-week security survey, there were **61** ransomware attacks. The USA 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

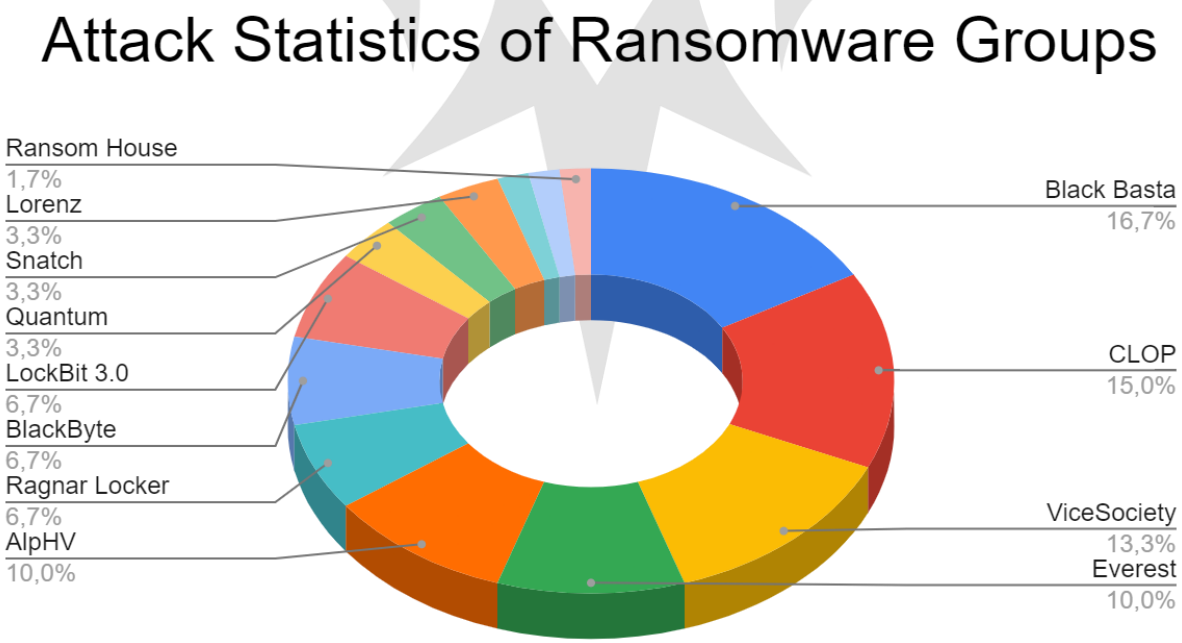
During this two-week period, the BlackBasta ransomware group was the most active. LockBit, which has been the first in every report for a long time, has hardly entered the ranking this time.

During the two-week period, BlackBasta was the most active ransomware group. Black bass, which carried out a total of 10 attacks in a two-week period, mainly targeted the Industry sector.

In this report, CLOP was second with 9 attacks and ViceSociety was third with 8 attacks.

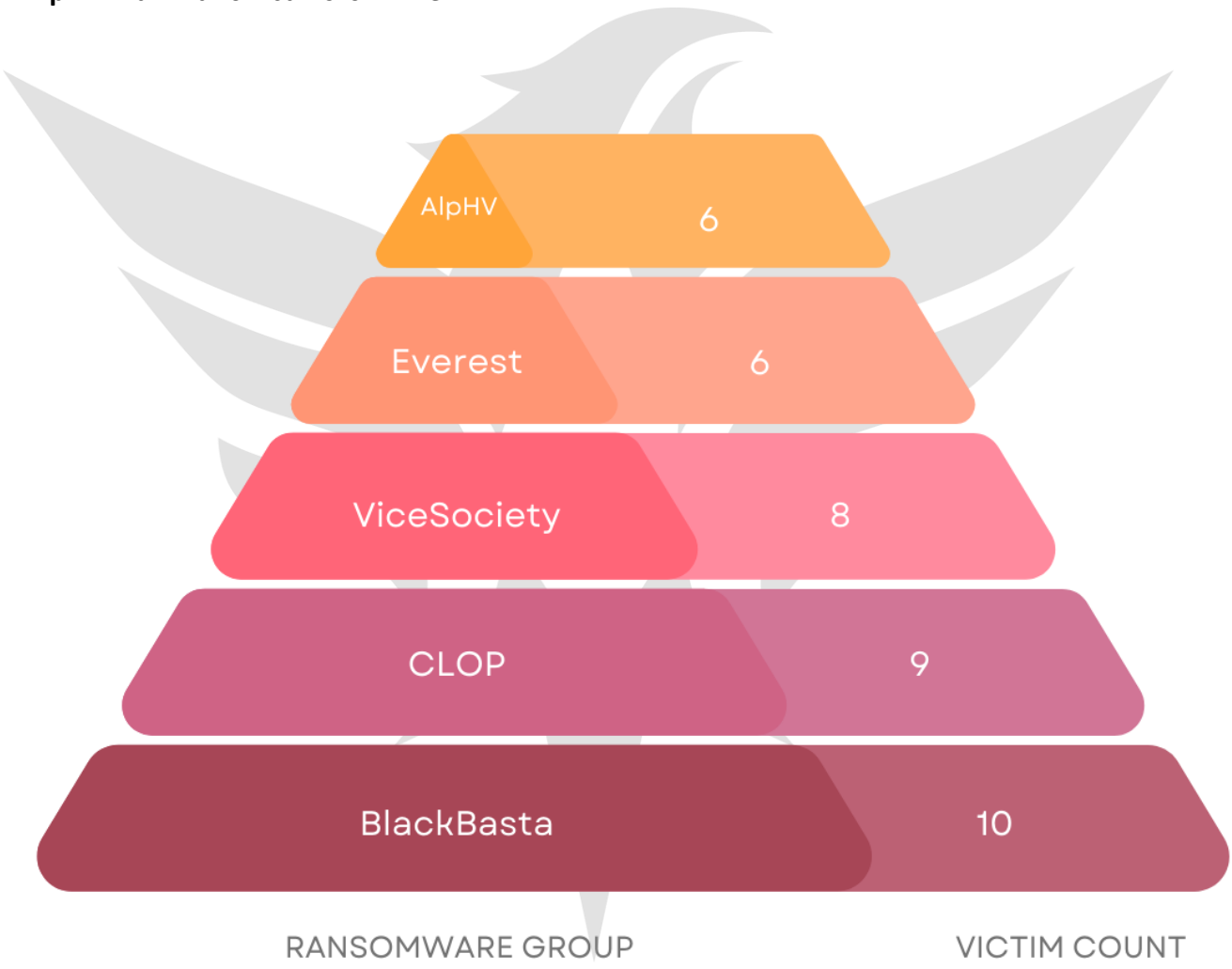
The country most targeted by the CLOP ransomware group is the United States. CLOP mostly targeted the Industry sector.

ViceSociety, on the other hand, targeted the USA and the United Kingdom the most. ViceSociety targeted the education sector the most in this report.



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

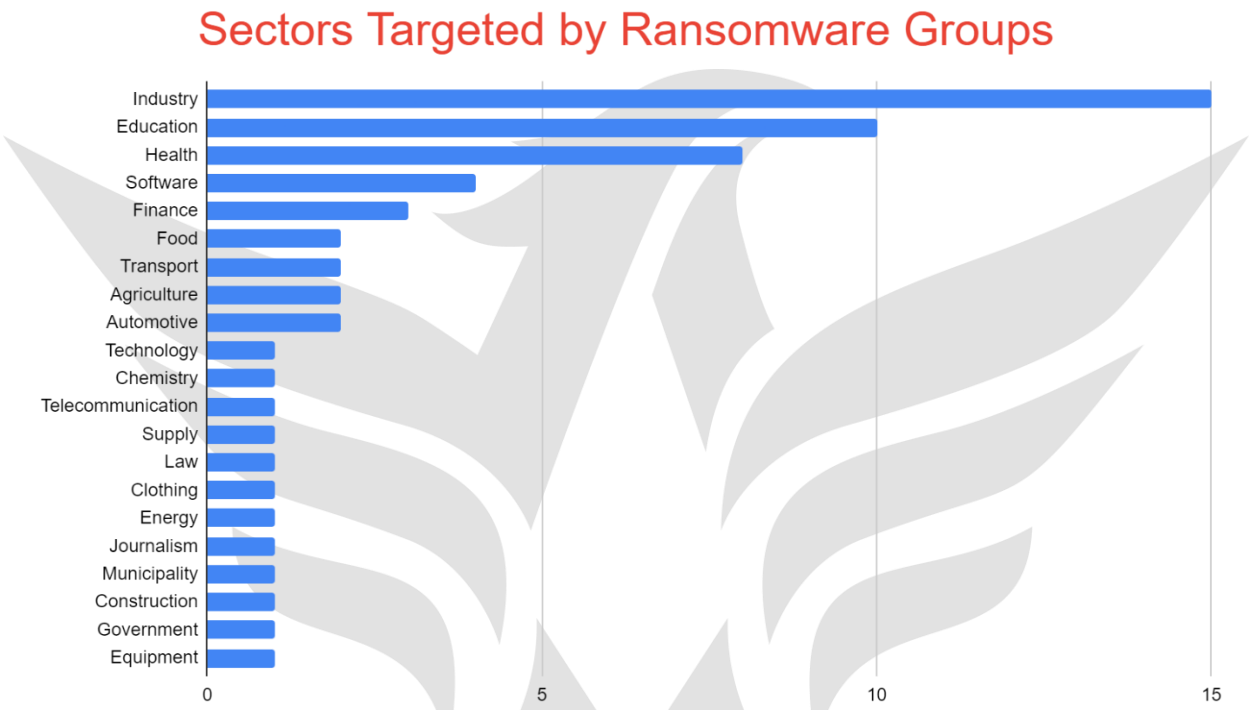
- **BlackBasta** is the first with 10 victims,
- **CLOP** second, with 9 victims,
- **ViceSociety** third with 8 victims,
- **Everest** fourth with 6 victims,
- **AlpHV** fifth with 6 victims is in line.



2. Number of Attacks by Sectors

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

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

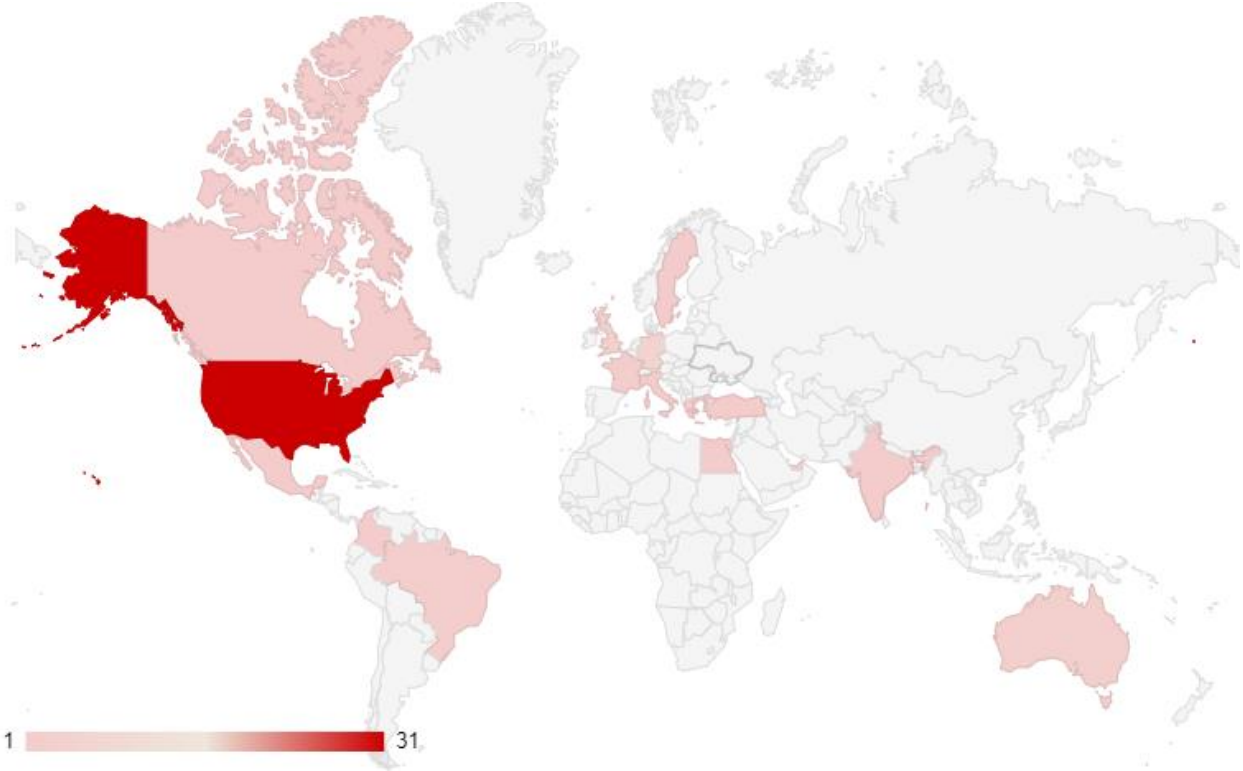


As in the previous report, there are not many sectors that have changed on a sectoral basis. As in previous reports, there are intense attacks in the **industry** sector. Attacks on the health and **education** sectors gained momentum.

The target of current attacks is **Industry** and **Education** sectors.

3. Number of Attacks by Countries

According to the study, the United States was targeted 31 times in late October. Much lower numbers than mid- and late-September, but still the most targeted country in the Ransomware report.



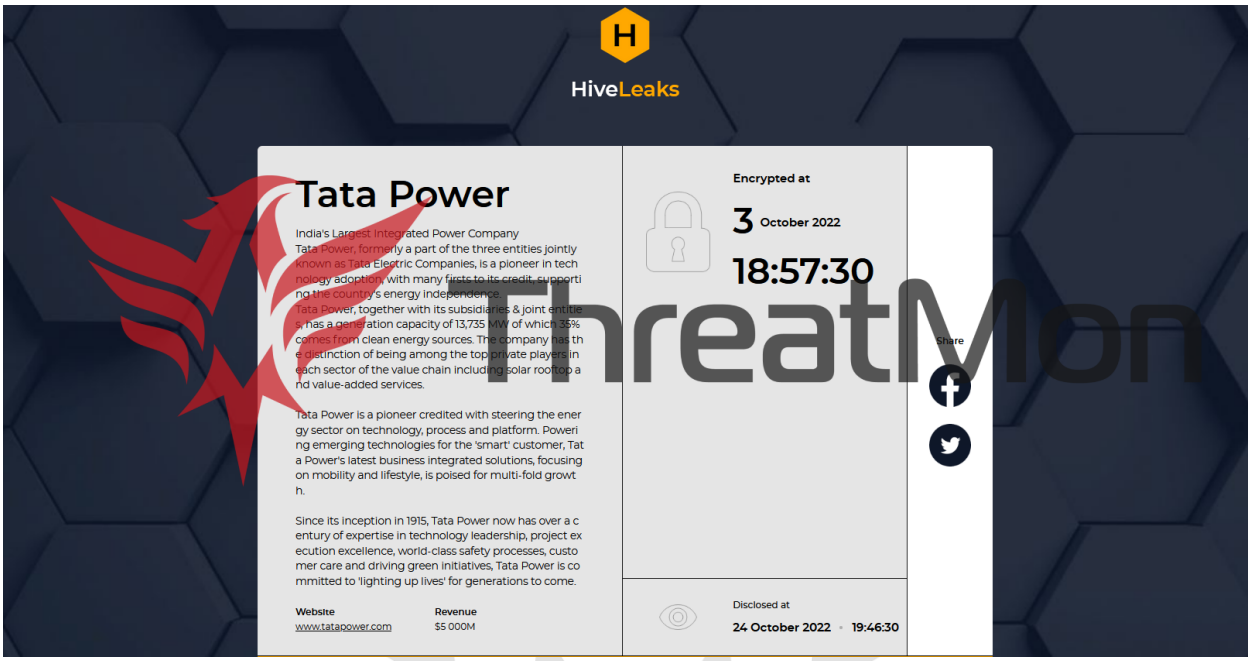
The second most targeted country was **Germany**, and the third country was the **United Kingdom**.

The **United Kingdom** still maintains its top-three score, but Germany is in the second place in this report, having a hard time making it into the top five.

Important Ransomware Group Activities

HiveLeak

According to the **Darkweb** Ransomware activity detected by ThreatMon Threat Intelligence Team, **HiveLeak** Ransomware group announced that it attacked and leaked data on TATA Power, a subsidiary of Indian technology group **TATA Group**.



The ransomware group announced that in the attack, it leaked sensitive data belonging to TATA Power, such as e-mail addresses, addresses, passports, phone numbers, employee sensitive information, financial information, and tax payments.

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	54489DFAB5D689CD969E26E32285029095088C2673F96A9BC3DF6EC14CA0A6B2
LockBit 3.0	SHA-256	59779870A470717B0B2A391E0B30E2C04F5E29B194DC22CD329AC0436EFEF3B4
LockBit 3.0	SHA-256	A1093069E2B142AEDAAF8501EFDE6EACE0F24EAAA676751749886199A94ECB0B
LockBit 3.0	SHA-256	876253092458C2278B9E4902A50BC3DEAA425F29A102738E443C895FE575685E
LockBit 3.0	SHA-256	D1DB7049178C924B53116F3993760AE2C250C52DDC459F616D7D587DDAA50707
LockBit 3.0	SHA-256	161C951E6D2E8D07571FC451A28A9FEAFB672C1F05586768F8178F33A9D74EFB
LockBit 3.0	SHA-256	3B52DB44C2CDD8ADFACB906362837ED449E96FCF761DE4B1F26388B66B6EDABE
LockBit 3.0	SHA-256	F5AC867014DF2A215903CDF5A5C4C34970E026725DBA2B2EF6B1515A46045930
BianLian	SHA-256	1FD07B8D1728E416F897BEF4F1471126F9B18EF108EB952F4B75050DA22E8E43
BianLian	SHA-256	DDA89E9E6C70FF814C65E1748A27B42517690ACB12C65C3BBD60AE3AB41E7ACA
BianLian	SHA-256	D602562BA7273695DF9248A8590B510CCD49FEFB97F5C75D485895ABBA13418D
Alphv	SHA-256	98436725DE8CE25AC7A3155F56B9D622FA4DD800AE581D7DD9F22BC1B7887525
Alphv	SHA-256	86CCC74375405EF5A86BB26071EC345D3D800438D1E0CAA4A6D0CB43BD8562DF
Alphv	SHA-256	5165CD61158A14BA2F90C275D29D8271B1F0C5669EBCDC620EDD86EE90474DBC
Alphv	SHA-256	8DC43793450F2C7F5953E0EB912356113346B6AFD48F9400A26C35CDF0FFDD07
BlackBasta	SHA-256	699AAEA1598A034CDE7ED88CD8A8A36FD59447E09BDDEF566357061774C48A76
BlackBasta	SHA-256	9A55F55886285EEF7FFABDD55C0232D1458175B1D868C03D3E304CE7D98980BC
BlackByte	SHA-256	44A5E78FCE5455579123AF23665262B10165AC710A9F7538B764AF76D7771550
BlackByte	SHA-256	1DF11BC19AA52B623BDF15380E3FDED56D8EB6FB7B53A2240779864B1A6474AD
BlackByte	SHA-256	EB24370166021F9243FD98C0BE7B22AB8CBC22147C15ECEF8E75746EB484BB1A
RagnarLocker	SHA-256	3DDDC43094E3B65F3DA251B9ABE774029C252456AA6D9614733DA74859FA9215

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

GitHub Link: [ThreatMon 17.10.2022 - 28.10.2022 Ransomware Report]

ThreatMon

45305 Catalina cs St 150, Sterling VA 20166