ThreatMon

Ransomware Group Activity Report

30.09.2022- 16.10.2022

in @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 98 ransomware attacks. The USA was the most targeted country. In addition, the most targeted sectors are Industry, Health and Automotive.

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 that two-week period, LockBit 3.0 was the most active ransomware group.

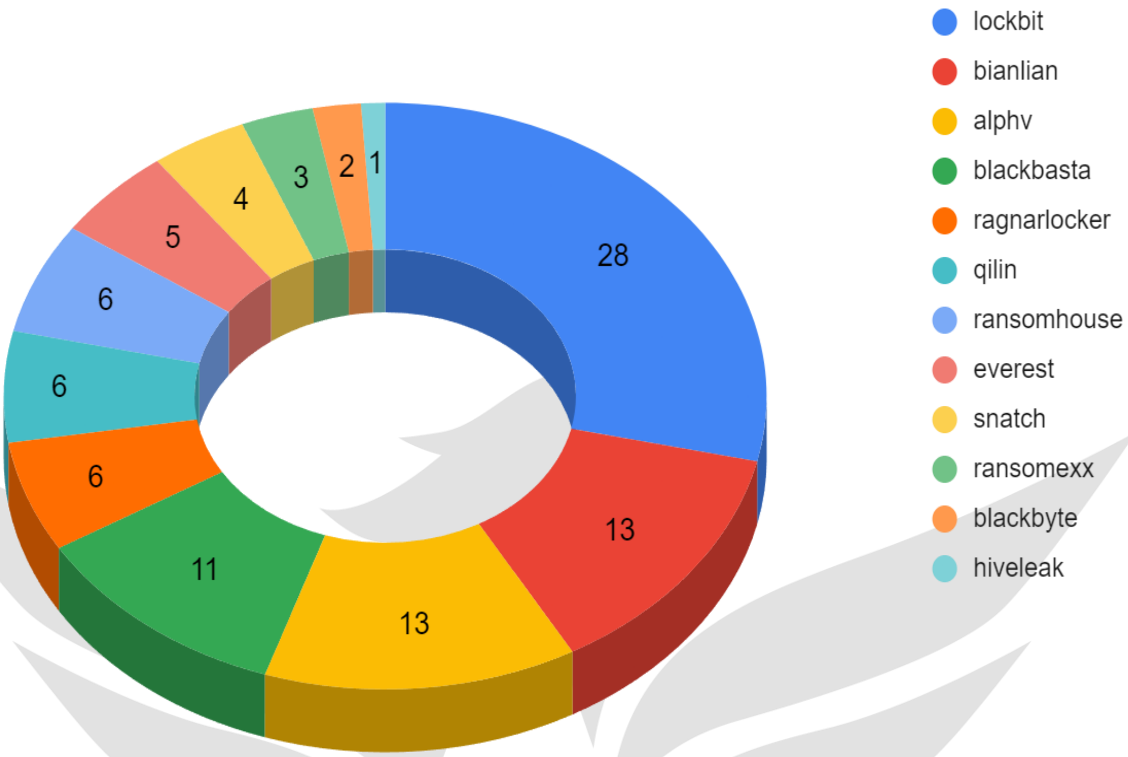
During the two-week period, LockBit 3.0 was the most active ransomware group. 17.09.2022 - According to the report dated 30.09.2022, the LockBit 3.0 group, which carried out 70 fewer attacks, attacked 28 times in two weeks. It mostly targeted the Industry sector.

In this report, BianLian and AlphaHV were second with 13 attacks and BlackBasta third with 11 attacks.

The country most targeted by the BianLian ransomware group is the United States. BianLian mostly targeted Television, Industry and Agriculture sectors.

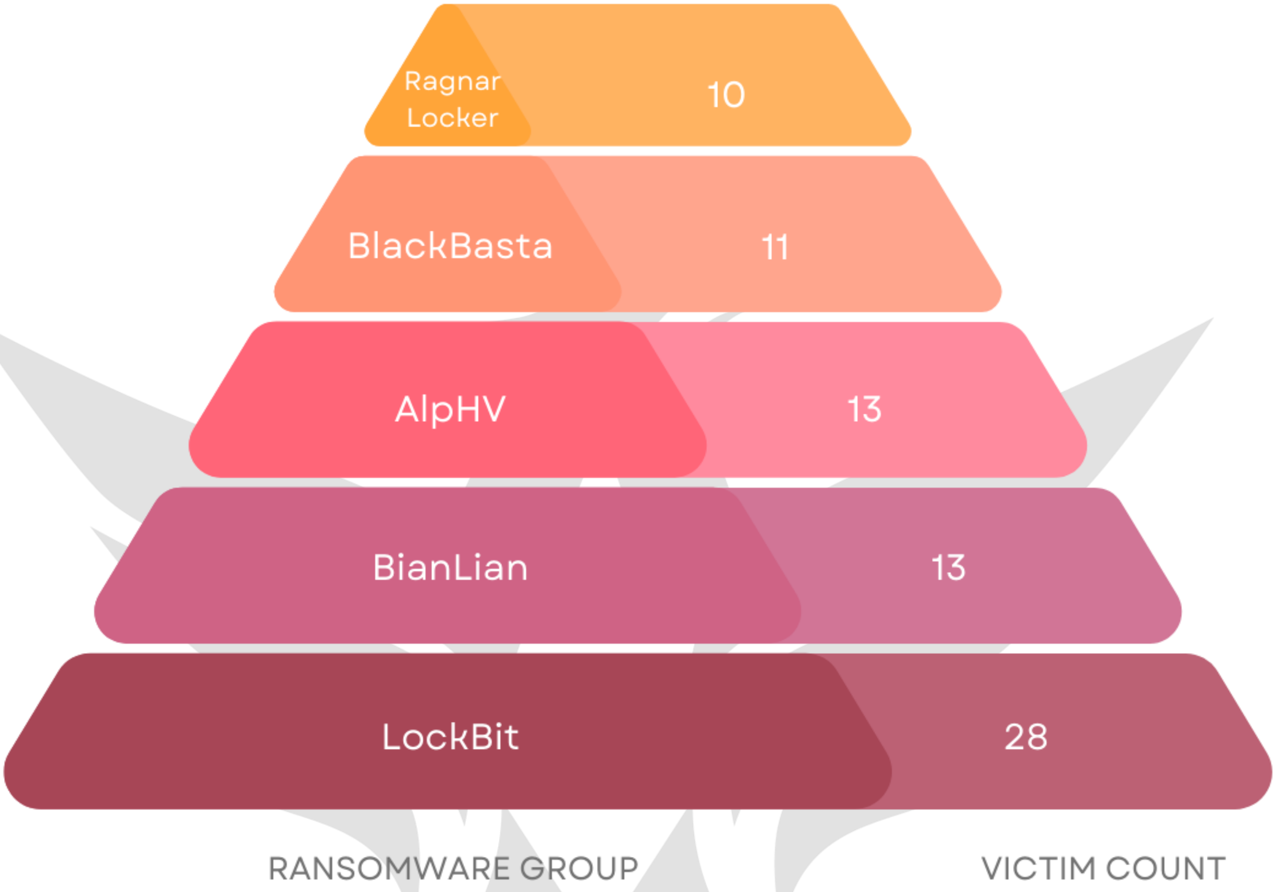
AlphaHV, on the other hand, targeted the United States the most, as did BianLian. It also made the most attacks in the Television and Industry sectors, similarly.

BlackBasta, who came in third in this bi-weekly report, was the country most targeted by the United States. The most targeted sector was Build and Industry.



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

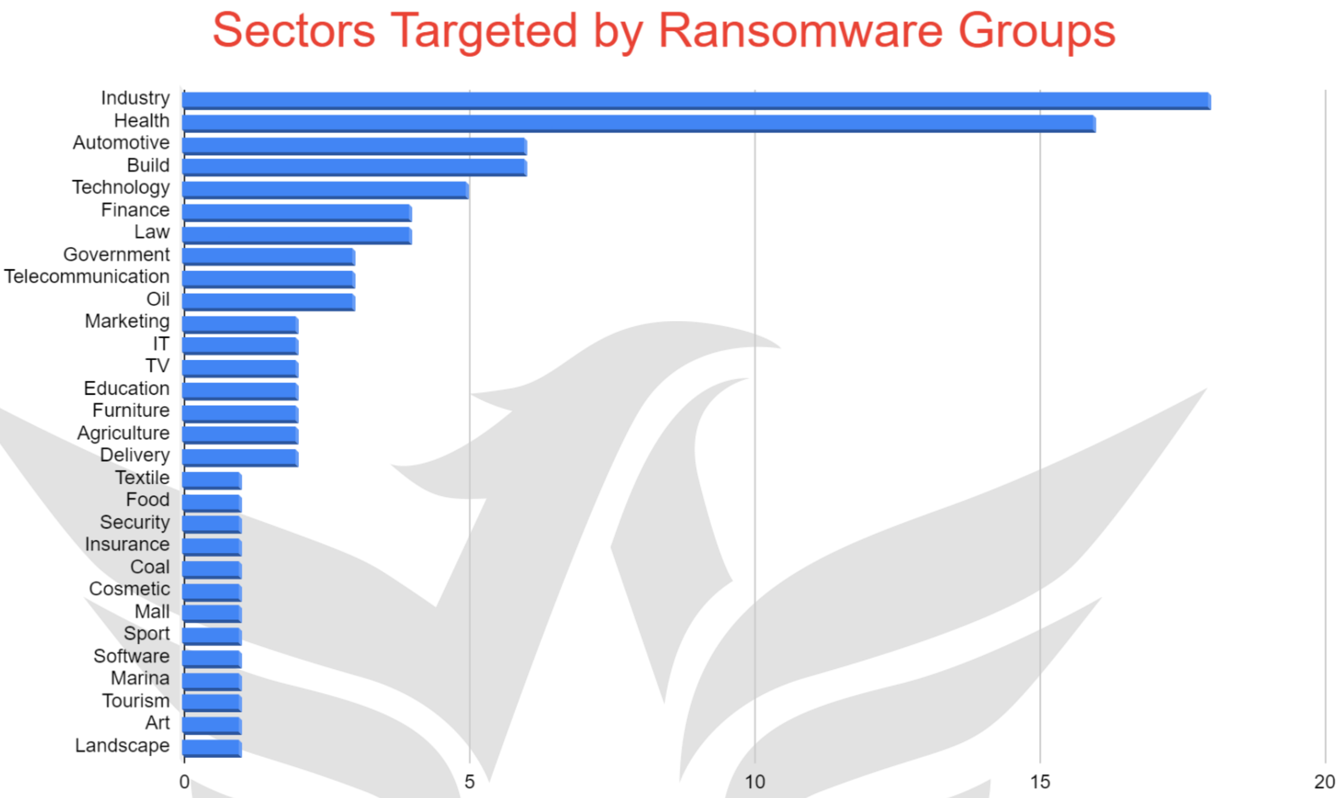
- **LockBit** is the first with 86 victims,
- **BlackBasta** second, with 17 victims,
- **BlackCat** third with 14 victims,
- **HiveLeaks** fourth with 13 victims,
- **AvosLocker** fifth with 10 victims is in line.



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.

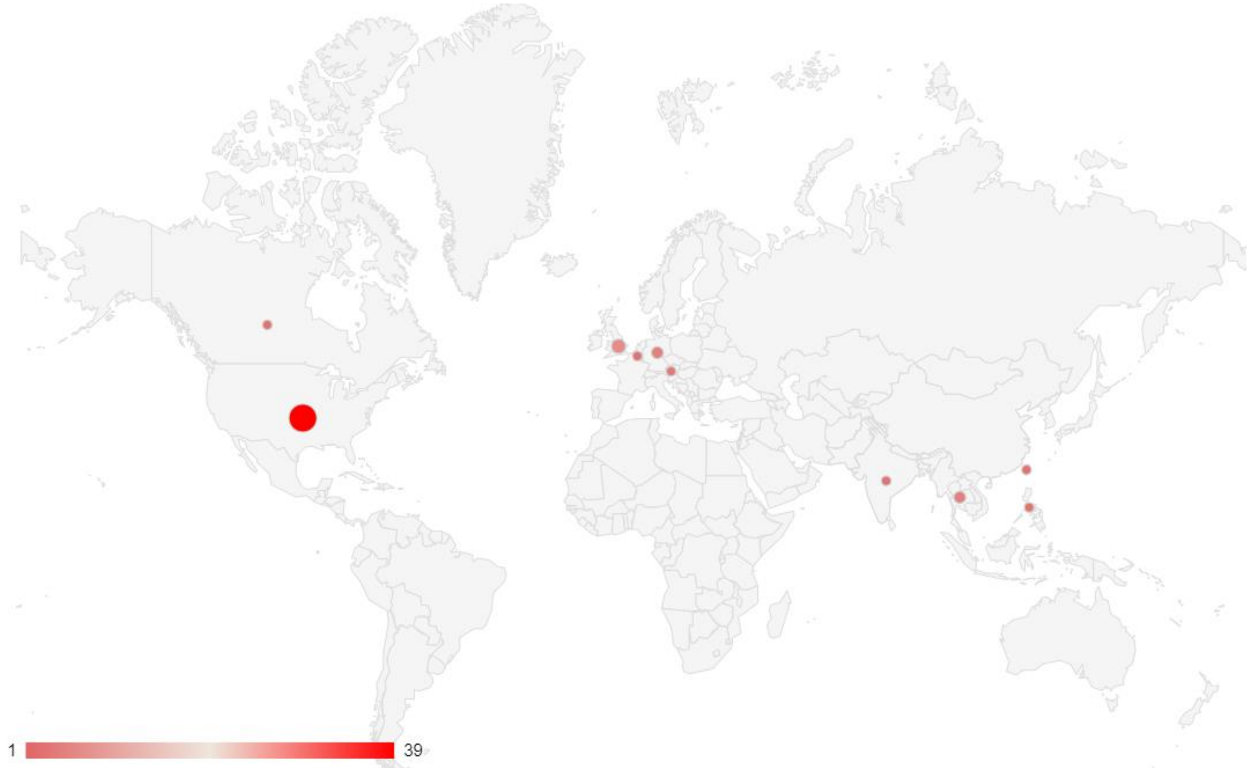


As in the previous report, there are not many sectors that have changed on a sectoral basis. As in the previous reports, there are intense attacks in the **Industry** sector. While attacks on the **Government** sector have increased a lot in the past reports, attacks on Governments have now decreased.

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

3. Number of Attacks by Countries

According to the study, the **United States** was targeted **38** times in early **October**. Much lower numbers than mid and late September, but still the most targeted country in the Ransomware report.



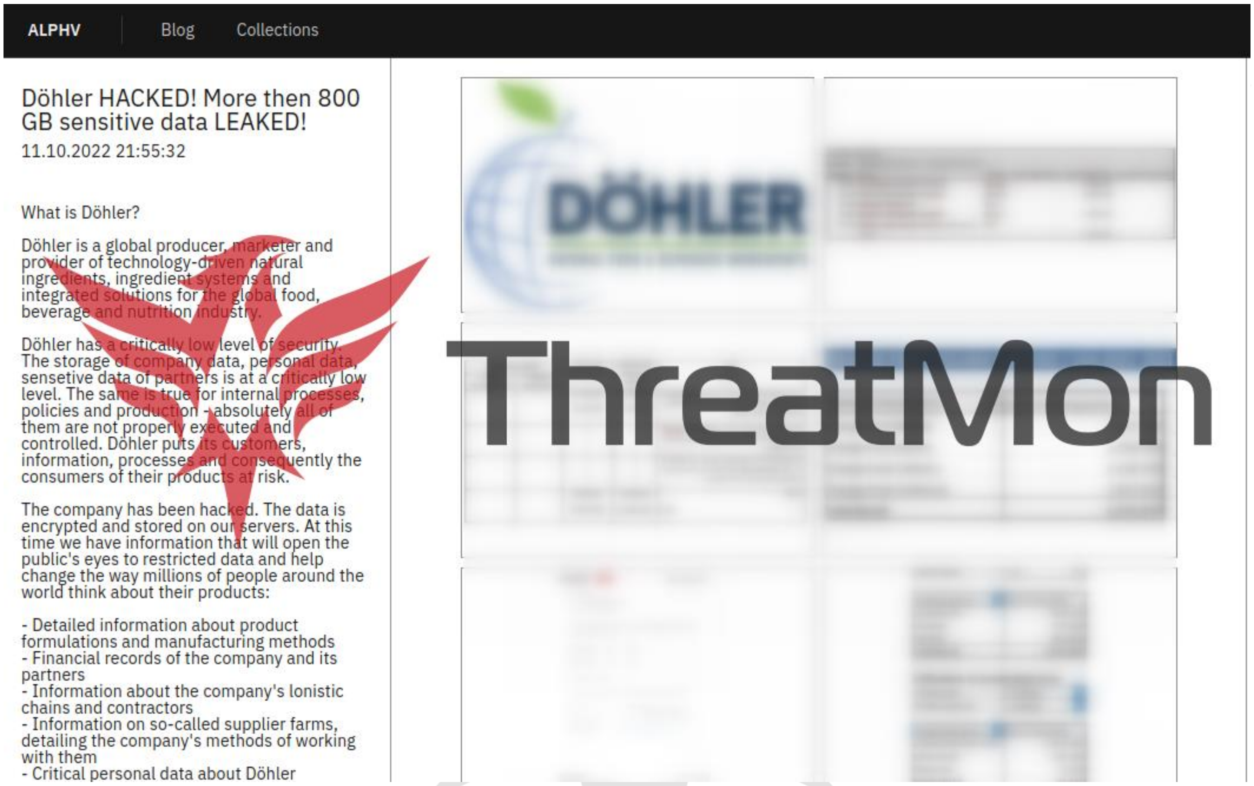
The second most targeted country was the **United Kingdom**, and the third was the **Philippines**.

United Kingdom was also in the top **10** in previous reports, but by the beginning of October, the attack against the Philippines has increased considerably. The Philippines, which did not make the top ten in other reports, is currently in third place.

Important Ransomware Group Activities

AlpHV

According to the Darkweb Ransomware activity detected on October 11, 2022, during routine scans by the ThreatMon Threat Intelligence team, the Alphv Ransomware group announced that it hacked **Döhler**, a **Germany-based food** company that provides food services to the whole world.



Döhler HACKED! More then 800 GB sensitive data LEAKED!

11.10.2022 21:55:32

What is Döhler?

Döhler is a global producer, marketer and provider of technology-driven natural ingredients, ingredient systems and integrated solutions for the global food, beverage and nutrition industry.

Döhler has a critically low level of security. The storage of company data, personal data, sensetive data of partners is at a critically low level. The same is true for internal processes, policies and production - absolutely all of them are not properly executed and controlled. Döhler puts its customers, information, processes and consequently the consumers of their products at risk.

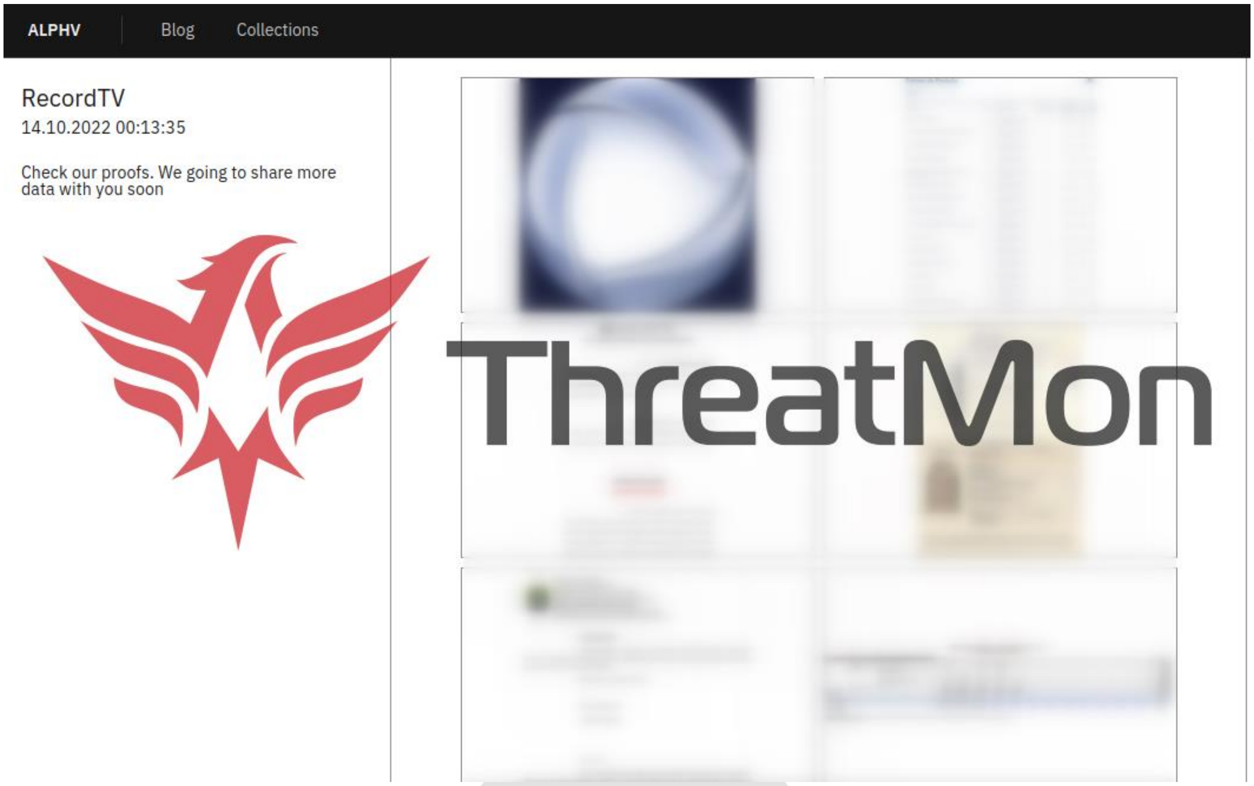
The company has been hacked. The data is encrypted and stored on our servers. At this time we have information that will open the public's eyes to restricted data and help change the way millions of people around the world think about their products:

- Detailed information about product formulations and manufacturing methods
- Financial records of the company and its partners
- Information about the company's lonistic chains and contractors
- Information on so-called supplier farms, detailing the company's methods of working with them
- Critical personal data about Döhler

The ransomware group has announced that it has leaked more than **800GB** of data belonging to the company.

AlpHV

According to the Darkweb Ransomware activity detected by the **ThreatMon** Threat Intelligence team on October 14, 2022, the **Alphv** Ransomware group announced that it hacked **RecordTV**, a local television channel serving in Brazil.

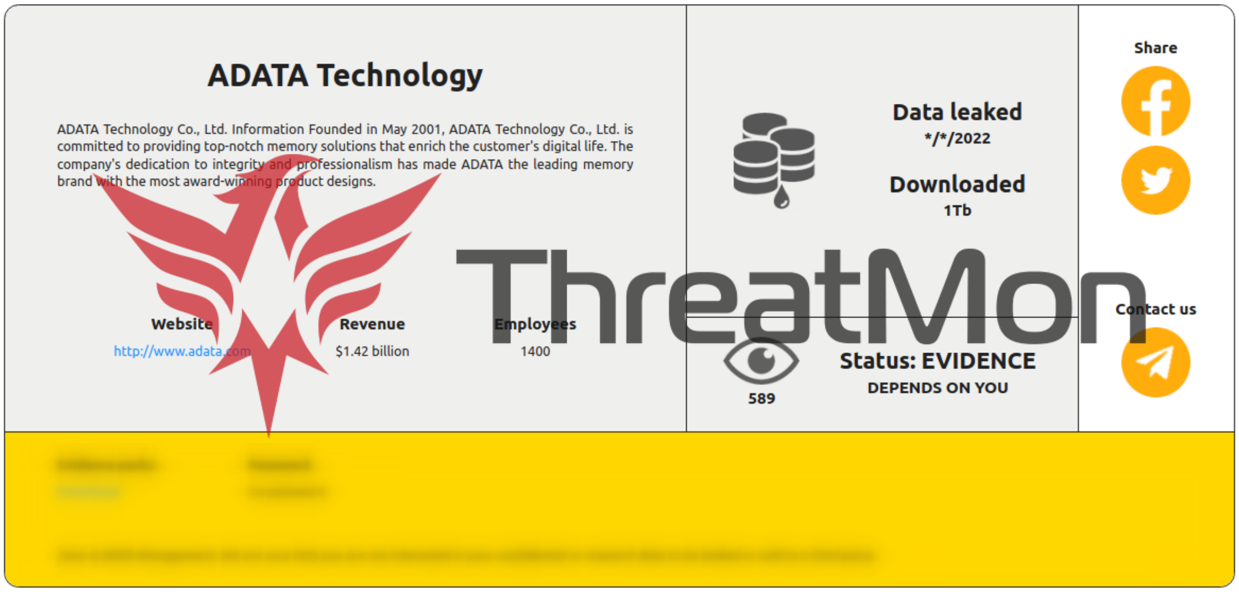


RecordTV
14.10.2022 00:13:35

Check our proofs. We going to share more data with you soon

RansomHouse

According to the Darkweb Ransomware activity detected by the ThreatMon Threat Intelligence team on October 12, 2022, the **RansomHouse** Ransomware group has announced that it has leaked data from ADATA, a globally known technology company.



ADATA Technology

ADATA Technology Co., Ltd. Information Founded in May 2001, ADATA Technology Co., Ltd. is committed to providing top-notch memory solutions that enrich the customer's digital life. The company's dedication to integrity and professionalism has made ADATA the leading memory brand with the most award-winning product designs.

Website	Revenue	Employees
http://www.adata.com	$1.42 billion	1400

Data leaked
//2022

Downloaded
1Tb

589

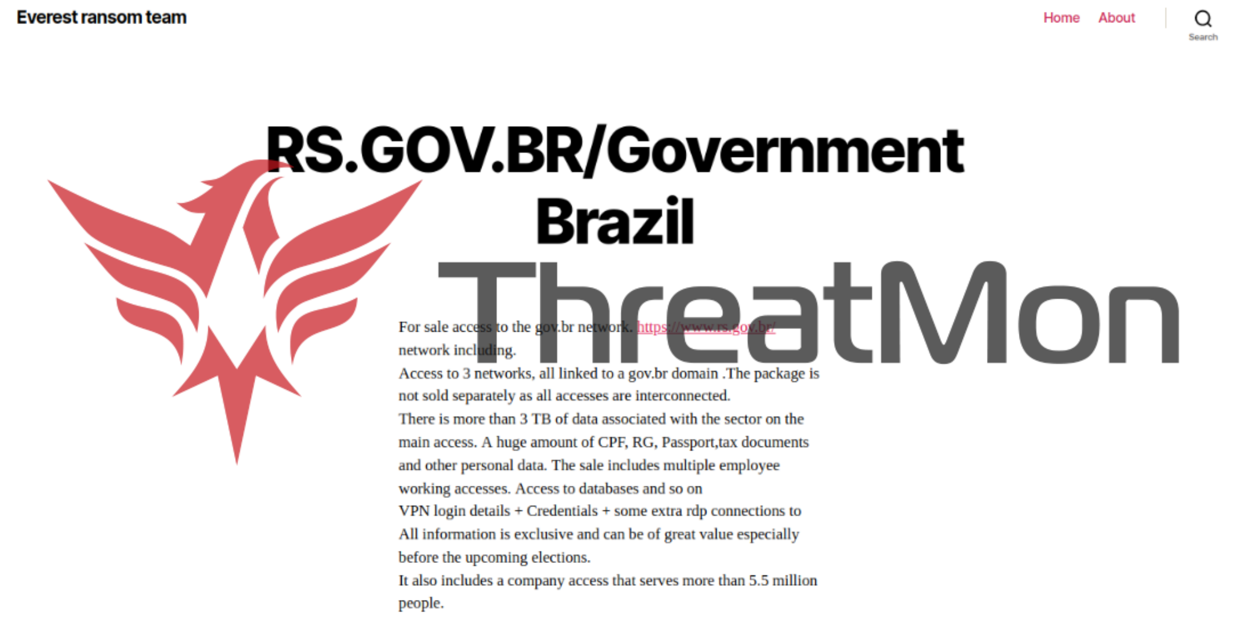
Status: EVIDENCE
DEPENDS ON YOU

[redacted]

Announcing that it leaked more than **1TB** of data, the ransomware group did not release any samples of the data.

Everest

According to Darkweb Forum activity detected by the ThreatMon Threat Intelligence Team on October 10, 2022, the **Everest** Ransomware group has announced that it has leaked data belonging to the **Brazilian**



RS.GOV.BR/Government Brazil

For sale access to the gov.br network. https://www.rs.gov.br/ network including.

Access to 3 networks, all linked to a gov.br domain .The package is not sold separately as all accesses are interconnected.

There is more than 3 TB of data associated with the sector on the main access. A huge amount of CPF, RG, Passport,tax documents and other personal data. The sale includes multiple employee working accesses. Access to databases and so on

VPN login details + Credentials + some extra rdp connections to

All information is exclusive and can be of great value especially before the upcoming elections.

It also includes a company access that serves more than 5.5 million people.

The leaked data is **3TB** in size and includes the data of 5.5 million people.

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	329E77A8A304E38CE4C4ED8906F9A7594377A3DA64505FD1935B58ACFC9AB4B9
LockBit 3.0	SHA-256	5FBCECCBB5ED4D38FBC2D3F86D1C0AFC7D74FDE74BE009B0EC6C4C812F39ADE8
LockBit 3.0	SHA-256	A8996BEE8934BAB480A4A48247612DC2AB1828A9A31C10B98FB20B47F5298AD9
LockBit 3.0	SHA-256	B240B6861889734EEE778D92BC1E2930E10570FE41D84A1A79CC518DC93F4E09
LockBit 3.0	SHA-256	EA028EC3EFAAB9A3CE49379FEF714BEF0B120661DCBB55FCFAB5C4F720598477
LockBit 3.0	SHA-256	1B52C957068EE20C7B703EB4A96882B8EDEEF31C5E9ECF481484FC4E433D3DCE
LockBit 3.0	SHA-256	16A707A3965EBD71EBC831B68863B855B2C8D60AEF8EFDEF1E0C0A6CC28E9BC7
BlackBasta	SHA-256	699AAEA1598A034CDE7ED88CD8A8A36FD59447E09BDDEF566357061774C48A76
BlackBasta	SHA-256	9A55F55886285EEF7FFABDD55C0232D1458175B1D868C03D3E304CE7D98980BC
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

ThreatMon

45305 Catalina cs St 150, Sterling VA 20166