The **B**lack **K**ite **R**esearch & **I**ntelligence **TE**am (**BRITE**)

BLACK KITE

spent 2023 analyzing and identifying risk vectors. Over the course of the year, this is what they found:

EXPLOITING VULNERABILITIES

has become the most common method for access than other attack vectors.
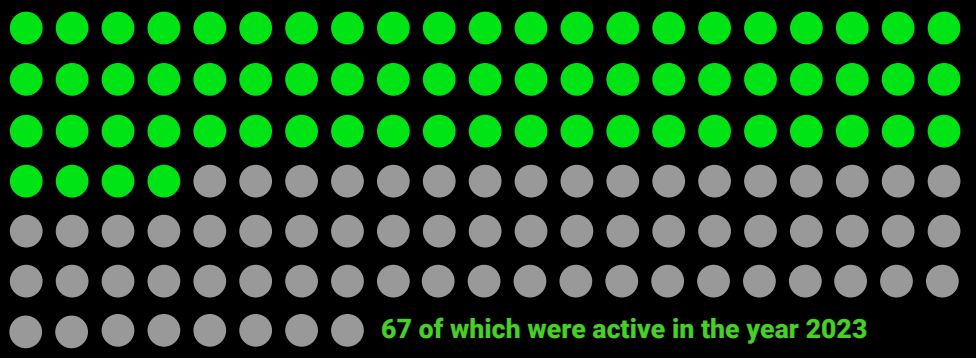
VENDOR RISK INTELLIGENCE:

Initiated
42
FOCUS TAGS
mostly around 0-day vulnerabilities or vulnerabilities exploited in the wild by threat actors such as ransomware groups.

Tagged more than
600
COMPANIES
that use MOVEit servers

RANSOMWARE:

Monitored
134
RANSOMWARE GROUPS

67 of which were active in the year 2023

DID YOU KNOW:

Lockbit has the biggest share in this set of victims. 21% of victims were published by Lockbit. Closest rival is **AlphV/Black Cat**, with almost 9% of the share.

While **Play**, **8base**, and **Akira** are putting themselves in the top ranks, **Noescape, Cactus, Ryhsida, Snatch,** and **INC Ransom** are some other examples that increased their share in the second half of the year.

We also found that a company with a Black Kite RSI value above 0.8 is **almost 27 times more likely to experience a ransomware attack** than a company with an RSI value below 0.2.
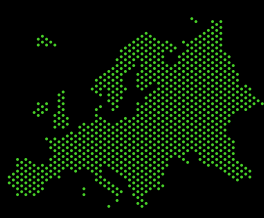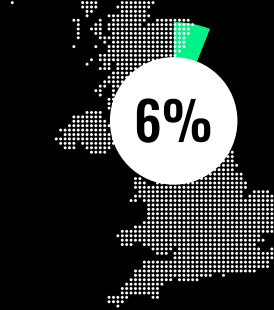
GEOGRAPHICAL RANSOMWARE STATS

MOST TARGETED

46%
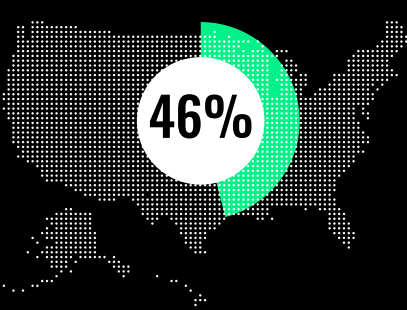
46% of the victims are in the US. US victims ratio among all victims only saw a minimum of 37.5% in May.

SECOND MOST TARGETED

6%

The second most targeted country is the UK with 6%.

Then some European countries such as

GERMANY (4%)
ITALY (3.7%)
FRANCE (3%)
SPAIN (1.9%)

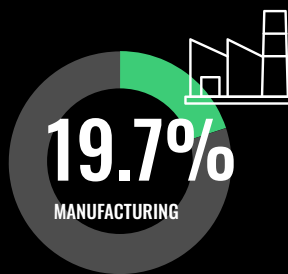and well-developed countries such as

CANADA (4%)

AUSTRALIA (2.2%)

BRAZIL (1.5%)

INDUSTRY-BASED STATS:

Throughout the year, two industries, (1) **Manufacturing** and (2) **Professional, Scientific, and Technical Services**, are always the top industries targeted. Their ratio is usually close to each other, but **Manufacturing** (19.7%) is slightly higher than **Professional, Scientific, and Technical Services** (18%). We observe that targeting the Manufacturing industry increased in the second half of the year.
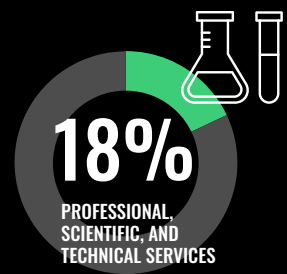
The next tier of industries targeted by Ransomware groups are **Finance and Insurance** (6.1%), **Health Care and Social Assistance** (6%), and **Educational Services** (6%).
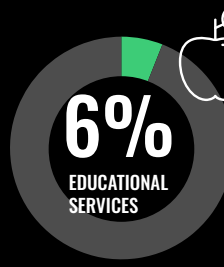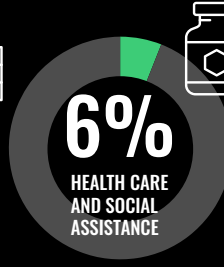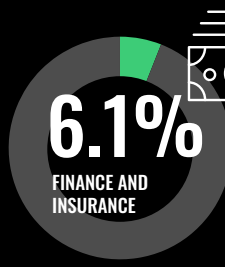
The following industries follow this tier with ratios ranging between 4.9% and 5.3%: **Information**, **Retail Trade**, and **Construction**.

We have also observed that there is a trend in targeting the **Healthcare** and **Information** industries in the second half of the year.

19.7%
MANUFACTURING

18%
PROFESSIONAL, SCIENTIFIC, AND TECHNICAL SERVICES

TOP TARGETED TIER

6.1%
FINANCE AND INSURANCE

6%
HEALTH CARE AND SOCIAL ASSISTANCE

6%
EDUCATIONAL SERVICES

INFORMATION

RETAIL TRADE

CONSTRUCTION

RANGING FROM
4.9-5.3%

MORE THAN
250
COMPANIES EXPERIENCED DATA BREACHES

CAUSED BY
81
VENDORS

IMPACTING UP TO
1,150
ORGANIZATIONS

3RD-PARTY AND 4TH-PARTY DATA BREACHES

81 vendors caused data breaches for more than 250 companies. This number reaches up to 1150 when the fourth and Nth parties are included.

STEALER LOG FILES

In 2023, Black Kite collected almost 6,400 Stealer Log files in 2023.

The minimum number of **machine information** in a single Stealer log file is
27,000

The total **password information** determined out of these stealer logs is around
11.3 MILLION

The number of **email addresses** collected from the stealer logs is around
6.1 MILLION

The number of **cookie session information** is
433 MILLION