

THE 5 MOST DISRUPTIVE LEGENDS OF RANSOMWARE

Here is the dreaded and alarming list of top ransomware groups.

Ransomware is a high-profile attack that's malicious and known to be the most devastating on the internet. It stands as the biggest terror for every business.

THE STATS SPEAK

The average ransomware attacks in 2023 is **\$1.54 million**, which is double the 2022 figure of **\$812,380**.

As of 2023, over **72%** of businesses worldwide were highly affected by the ransom.

There is a rapid rise of **13%** in the last five years in ransomware attacks, with an average cost of **\$1.85 million** for every incident.

Ransomware attacks are spiking rapidly. Expertise in these devastating attacks has driven the invention of a new business model in Ransomware-as-a-Service (RaaS).

Keep an Eye Out on the Top Ransomware Groups

LOCKBIT

Through Q1 2023, around **1,653** total victims were found on LockBit leak websites.

BLACKCAT

Mainly uses 'quadruple extortion' and provides affiliates with **90%** as payouts.

CONTI

Contributes for **>1000** of total attacks around the globe.

GRIEF

Targets organization with a revenue of **\$5 million** US dollars or even higher.

REVIL

One of the foremost ransomware groups to adopt **Revil** extortion scheme.

Immediate Actions Against Protecting Ransomware

A powerful multi-layered approach can go a long way in protecting your data against ransomware groups.

Active Directory

- Using multi-factor authentication
- Updating software and patches
- Use strong passwords

Recovery and Backups

- Encrypt backups
- Fixed backup copies
- Strong retention policies

Network

- Micro-segmentation, a network security approach
- Intrusion Prevention Systems (IPS)
- Role-based access control (RBAC)

Cloud

- Use secure APIs.
- Strong access controls
- Data masking

Security Made Easy. Defend Your Data Fortress Today!

To know more about safeguarding your data, cybersecurity trends and a lot more, check out www.secureitworld.com.