WHITE PAPER | DATE 2020

A WHITE PAPER ON RANSOMEWARE ATTACK TRENDS IN 2020

BY
VANGARU KOUSHIK

Table of Contents

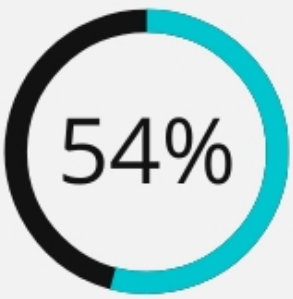
Introduction

The threat of ransomware is becoming a more serious concern to many businesses, consumers, and government agencies as their technical infrastructure evolves. Ransomware is a type of virus that is used by criminals to block access to crucial system files and network segments; these attacks allow the attacker to keep data sources hostage in exchange for a ransom. These types of attacks are frequently handled with multimillion-dollar compensation and the recovery of access to the data sources in question.

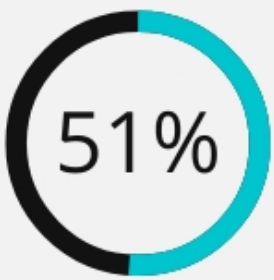
Ransomware trends of 2020

Prevalence of ransomware

According to a study published by Sohos half the organizations around the world were hit by ransomware. 51% of organizations reported that they have been hit by ransomware. In comparison to prior years, organizations reported a small decrease in attacks. In a previous poll commissioned by Sophos and published in 2017, 54 percent of respondents said they had been struck by ransomware in the previous year.make it even better.

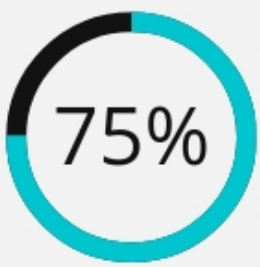


2017

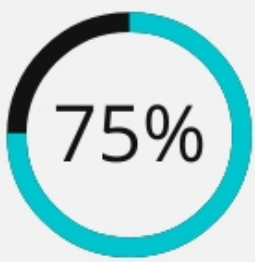


2020

INDIA



BRAZIL



TURKEY

TOP 3 COUNTRIES TO BE HIT BY RANSOMWARE IN 2020

MOST AFFECTED BUSINESSES

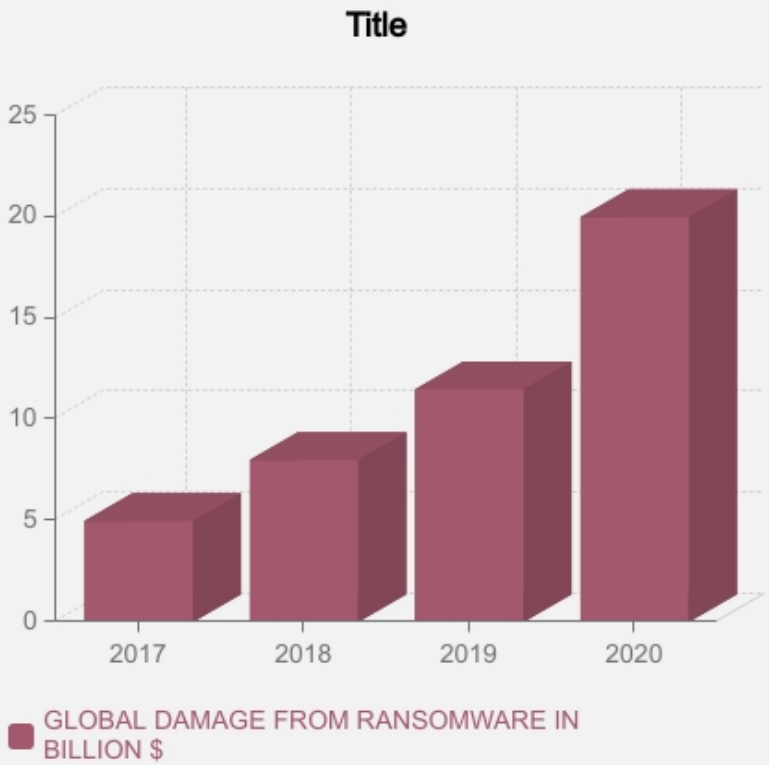
From a local food retailer to a multi-national company, ransomware attacks continue to loom over cyberspace.

These are the most targeted and affected industries by ransomware attacks in 2020:

SECTOR	2020 rank	2019 rank	change
Finance and insurance	1	1	-
Manufacturing	2	8	6
Energy	3	9	6
Retail	4	2	-2
Professoinal Services	5	5	-
Government	6	6	-
Healthcare	7	10	3
Media	8	4	-4
Transportation	9	3	-6
Education	10	7	-3

HOW MUCH DID RANSOMWARE COST IN 2020

Ransomware costs businesses billions of dollars each year. By the end of 2019, cybercriminals using ransomware had made off with a reported $11.5 billion in ransom payments. By the end of 2020, that number is projected to reach $20 billion.



It can be gathered from the graph that the estimated global damage from ransomware in 2020 has increased 15x of 2017.

ROLE OF CYBERSECURITY INSURANCE

ONE IN FIVE HAVE HOLES IN THEIR CYBERSECURITY INSURANCE

Cybersecurity insurance is now the norm, with 84% of organizations reporting that they have it. However, only 64% have cybersecurity insurance that covers ransomware. This means up to one in five organizations (20%) are paying for cybersecurity insurance that doesn't cover ransomware

Given that, as we've seen, 51% of organizations experienced ransomware in the last year, and with average remediation costs of US$761,106, organizations should question the value of insurance that excludes ransomware.

RANSOMWARE PAYOUTS

- Recently, the University of Utah's College of Social and Behavioral Sciences (CSBS) paid a ransom of $457,059.24 to the attackers to retrieve the decryption key to the seized information.
- Haldiram, prominent Indian sweets and snacks firm, was recently targeted by an unknown ransomware gang. The attackers gained access to the company's sensitive data and demanded a ransom of 7.5 lakh rupees (about $ 10,220).
- According to the research, the average payment following a ransomware attack in 2020 rocketed up 171% to $312,493 compared to $115,123 in 2019.
- The average cost of ransom per incident in 2020 is $8,100.

CONCLUSION

In conclusion ransomware attacks, has proved that their impact can be devastating to small business owners and organization. Ransomware is not only threats to small business and organization it has an impact on people as well. Here are a few measures to follow in order to minimize the risk of being held hostage in ransomware attacks:

- Start with the assumption that you will be hit Ransomware it doesn't discriminate:
  every organization is a target, regardless of size, sector, or geography. Plan your cybersecurity strategy based on the assumption that you will get hit by an attack

- Invest in anti-ransomware technology to stop unauthorized encryption:
  24% of survey respondents that were hit by ransomware were able to stop the attack before the data could be encrypted.

- Protect data wherever it's held:
  Almost six in 10 ransomware attacks that successfully encrypted data include data in the public cloud. Your strategy should include protecting data in the public cloud, private cloud, and on premises.

- Make regular backups and store offsite and offline:
  56% of organizations whose data was encrypted restored their data using backups last year. Using backups to restore your data considerably lowers the costs of dealing with the attack compared with paying the ransom.

- Ensure your cyber insurance covers ransomware:
  Make sure that you're fully covered if the worst does happen.

- Deploy a layered defense:
  Ransomware actors use a wide range of techniques to get around your defenses; when one is blocked, they move on to the next one until they find the chink in your armor. You need to defend against all vectors of attack.

Learn more about ransomware trends in 2020 by following the links below:

- https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
- https://securityintelligence.com/posts/threat-actors-targeted-industries-2020-finance-manufacturing-energy/
- https://purplesec.us/resources/cyber-security-statistics/ransomware/
- https://www.checkpoint.com/downloads/products/ransomware-trends-prevention-and-response-whitepaper.pdf