THE GROWING THREAT OF RANSOMWARE

What is ransomware?

It's a type of malicious software that denies users access to their data unless a ransom is paid.

Most common variants: Cryptolocker, CrySis, WannaCry, Bad Rabbit, ExPetr.

850,970,000

The total number of ransomware infections detected in 2018. Ransomware attacks are increasing more than 300% year over year.[1]

84% of IDC survey participants experienced a malicious attack in the past 12 months (that they know about)[2]

89% of which were successfully attacked[2]

93% of which resulted in data corruption or loss[2]

Who's Affected?

90%

of all financial institutions have experienced ransomware in the past year[1]

of healthcare organizations saw an increase in ransomware infection rates from 2017 to 2018[1]

The 5 Industries Most Vulnerable to Cyber-Attacks

- Small and Medium-Sized Businesses
- Healthcare
- Government Agencies
- Energy Industry
- Higher Education[3]

Financial Impact

The Ransom

$11.5 billion — The cost of ransomware damages were $6B in 2017. And are predicted to hit $11.5B by 2019.[4]

$1,200 per machine — The cost of ransom paid out per infected machine by 70% of those affected.[5]

Downtime

$8,851 per hour — The average internal cost of downtime per hour for a US business per infected machine.[5]

Defense Strategy

Protection from ransomware is not enough. You need an IT resilience plan that will allow you to recover from an attack.

Train employees and staff on awareness, the risks and impact of ransomware, and how to execute your IT resilience plan.

Never open suspicious links. Treat email attachments from unknown senders with extreme caution. If in doubt, don't open it.

Learn how to mitigate cybersecurity threats like ransomware and recover in minutes.

CONTACT US

RapidScale
A Cox Business Company

POWERED BY Zerto

Sources
[1] 27 Terrifying Ransomware Statistics & Facts You Need To Read | [2] 2019 IDC State of IT Resilience Report | [3] CDN Networks | [4] Cybersecurity Ventures | [5] Osterman Report