#RansomAware

Share your story

TALION

#RansomAware

Turning the tide on today's biggest cyber threat

2020 was tough, the world found itself in unfamiliar territory, we faced the challenges of remote working and while doing so ransomware found a gateway to thrive.

Worldwide organisations found themselves under a new level of pressure, in a year where ransomware attacks not only grew drastically in numbers, but broke records for its reckless and damaging methods.

More recently, organisations including Colonial Pipeline, Ireland's Health Service Executive and AXA have suffered major attacks at the hands of the threat, putting terabytes of data at risk and potentially netting cybercriminals millions.

Ransomware is rife today, over half (57%) of UK companies have reported being victim to ransomware[1]; it would seem no company is immune to the threat.

Today ransomware is an enterprise-level criminal industry, with new data showing that in just nine months the attackers behind DarkSide earned over $90 million[2] – highlighting that every attack they carried out ended in a payment.

The reason attacks are so profitable is because most ransomware victims feel they have no option but to pay. When the choice is between business continuity and the loss of customer data or paying a five-million-dollar ransom demand, taking the financial hit may seem like the safest bet. Everyone can then move on, forget about the attack, and pretend it never happened: it was just a very close call.

But this response benefits only the cybercriminals. The more companies talk about ransomware, the more we can learn about the threat and improve defences. There is no need to hide any more, ransomware is affecting everyone.

The Ransomware pandemic

A ransomware attack happens every 11 seconds[3]

Global ransomware damages are set to reach $20 billion in 2021[4]

1 Purplesec
2 ZDNet
3 & 4 Cybercrime magazine

The #RansomAware Campaign

We are creating a movement to encourage organisations to share intelligence on ransomware attacks. We will create a cybersecurity community where organisations feel able to talk about attacks, share their experiences and inform others, even if this must be done anonymously.

Cybersecurity Ventures predicts that a ransomware attack occur every 11 seconds and the latest forecast for global ransomware damages is set to reach $20 billion in 2021[5]. Getting hit with ransomware is NOT a cybersecurity failure, today it is a fact of life.

As part of the movement, we will encourage organisations to share their ransomware stories via social media using the #RansomAware hashtag. We believe that the more companies who expose how they were attacked, by whom, if they paid the ransom and if their data was recovered, the more we can learn about attacker tactics, techniques, and procedures to build better defences: Forewarned is Forearmed.

We believe we are stronger together. That's why we're forming a coalition of businesses, industry bodies, academia, government, influencers and media to stop cyber shaming, share intelligence and fight back against the onslaught of ransomware attacks.

Information sharing is the only way to get ahead of the cybercriminals. They collaborate to make their attacks more successful, so we must collaborate to make our defences stronger.

Find out more at talion.net/ransomaware, simply use the hashtag **#RansomAware** to spread the word, or to become a coalition member please contact:

Amy Perez
Marketing Director
Talion
aperez@talion.net

OR

Lucy Harvey
Account Director
Eskenzi PR Ltd.
lucy@eskenzipr.com

The Ransomware pandemic

57% of companies in the UK have reported being victim to ransomware[6]

92% of organisations who paid a ransom in the past 12 months did not get all of their data back[7]

The average ransom demand is $10,000 with some groups asking up to $5million[8]

5 Cybercrime magazine
6 Purplesec
7 Teiss
8 ITPro