86a Station Road
Yate
Bristol
BS37 4PH

+44 (0)1454 838490
Email: info@refresh-it.co.uk
Web: www.refresh-it.co.uk

10 November 2020

Ransomware: Cybersecurity's Biggest Bully Yet

Can you imagine logging into your system to access your business data and being unable to do so? Talk about your worst nightmare coming true!

Unfortunately, an increasing number of businesses around the world are living this nightmare with countless others coming in the line of fire, including yours. Ransomware is growing rapidly and crippling businesses worldwide, making up 27 percent of all malware incidents in 2020.

If you aren't already in the know, ransomware is a type of malicious software that gains access to files or systems on your network and blocks your access to them until you pay a ransom in exchange for a decryption key.

Sounds pretty serious, but why are we calling it cybersecurity's biggest bully yet? Keep reading to know all about its history, destructive impact and dangerous growth trajectory to get your answer.

Three Decades of Bullying and Counting

In 1989, ransomware claimed its first victims when a Harvard-educated biologist and AIDS researcher, Joseph Popp, distributed 20,000 floppy disks loaded with ransomware to AIDS researchers across 90 countries.

He claimed that the disks had a program that could analyze an individual's risk of acquiring AIDS via a questionnaire. The recipients were unaware of a malware program inside the disks that activated itself and locked the computers after they were powered on for the 90th time post the malware's entry into the system.

Once active, the malware displayed a message first demanding $189, and later another $378, for a software lease from a company called PC Cyborg. This attack became notoriously known as the AIDS Trojan or the PC Cyborg virus. That year, a new and formidable cybersecurity threat was born.

Ransomware's emergence, however, began nearly 20 years later when 'Police Locker' attacks burst onto the scene. These attacks used a malware that changed a user's desktop screen to depict a false note from a law enforcement agency – the police or the FBI. Interestingly, the attacks did not use encryption and could have been resolved simply by rebooting the computer, but it was the fear tactic that compelled several victims to pay hundreds of dollars in ransom.

Modern-day ransomware developers have come a long way since Joseph Popp in the late 80s, the use of RSA encryption in the mid-2000s and attacks such as Police Locker. While early ransomware developers developed the encryption code on their own, today's attackers use existing libraries, which are harder to tackle, as well as spear phishing, among other methods.

Some of the most advanced cybercriminals are making a fortune out of selling ransomware-as-a-service, which has allowed even attackers with less technical skills to carry out massive attacks. Ransomware, such as CryptoLocker, CryptoWall, Locky and TeslaCrypt, are just some of the attacks that have emerged out of this new industry.

Cryptolocker, for instance, is a malware that encrypts files on Windows devices using advanced encryption to prevent users from accessing the files on the system. To obtain a private key to access the files again, users are warned of destruction of the data should they fail to pay the ransom

The introduction and use of cryptocurrency within the ransomware industry has also made transactions more difficult to trace than conventional ones. For example, the hackers that carried out the WannaCry ransomware attacks that wreaked havoc worldwide, demanded that the ransom be paid in Bitcoin.

Through their three-decade long existence, ransomware attacks have only gone from strength to strength. While older threats reemerging is always a possibility, newer ones such as NotPetya and MAZE are constantly looking to take advantage of lapses in the cybersecurity defenses of companies worldwide.

How Ransomware Runs Your Business Into the Ground

Besides being the reason behind 41 percent of cyber insurance claims in the first half of 20202 alone, the repercussions of a ransomware attack aren't limited to just financial loss. In fact, a ransomware attack can grind your business to a halt and cause severe damage on multiple fronts.

Here's how ransomware can literally choke the life out of your business' present and future.

Loss or destruction of critical business data

Your company's data is the proverbial thread that strings various facets of your business together. Should your data become inaccessible, go missing or be destroyed, the damage can be catastrophic. Once lost, fully recovering data and knowledge is a herculean task and getting things back to some state of normalcy is an enormous exercise in itself.

Norsk Hydro, a global aluminum producer, met with a similar fate when 22,000 of its computers across 170 different sites in 40 different countries were hit by a ransomware attack in early 2019. With no access to its data, its entire workforce of 35,000 employees had to resort to pen and paper. As per a BBC report in June 2019, the attack had already cost the company £45 million in damages.

Unplanned downtime

As of Q1 of 2020, the average downtime due to a ransomware attack is 16 days. The very thought of businesses not being able to progress for weeks on end is sure to give any owner sleepless nights. Unfortunately, this is the grim reality that numerous businesses, especially small and medium-sized ones, are grappling with. Besides suffering $300 million in business interruption losses due to a ransomware attack, Danish transportation and logistics giant Maersk faced a 20 percent drop in shipping volume due to the downtime it experienced during a ten-day recovery effort.

Loss of productivity

Efficiency is key to any business' success and is a proven way of keeping customers happy while keeping costs low. But do you know what happens when productivity takes a massive hit? Ask British pharmaceutical and CPG maker Reckitt Benckiser, which lost $140 million due to disrupted production and supply chains, courtesy the NotPetya ransomware.

Just goes to show you that time really is money!

Disruption of business in the post-attack period

Paying ransom to retrieve data access is one thing but making a full recovery after a ransomware attack is a different kettle of fish altogether. The downtime following an attack is so profound that it leaves businesses in shambles for weeks on end, making recuperation and recovery incredibly painstaking.

Erie County Medical Center (New York, USA) went through a six-week ordeal of manual operations and a recovery process costing $10 million after losing access to 6,000 computers due to a ransomware attack.

Damage to hostage systems, data and files

86a Station Road
Yate
Bristol
BS37 4PH

+44 (0)1454 838490
Email: info@refresh-it.co.uk
Web: www.refresh-it.co.uk

10 November 2020

There's no guarantee that you will recover your data in its original state even after paying ransom. Certain crucial servers, data, software and files could be severely or permanently damaged by a ransomware attack and it goes without saying that retrieving them while running daily operations becomes a mammoth challenge.
The United Kingdom's National Health Service (NHS) lived through this ordeal when several of its centers had to be shut down during the WannaCry outbreak in 2017. Several medical and emergency services were impacted for days as the NHS fought its way back to normalcy.

Loss of reputation

The expression "once bitten, twice shy" is most appropriate when describing the behavior of customers and companies towards a business hit by a ransomware attack. Despite making a recovery, your business could receive a cold shoulder from the market until you rebuild your reputation – a task that could take years of hard work.

A Bully Getting Stronger by the Day

With the possibility of an organization falling prey to ransomware every 11 seconds by 20214, this cybersecurity bully isn't getting any weaker. In fact, attackers are coming up with newer ways to extort money, such as exfiltrating data and threatening to release it over the Internet if the ransom is not paid. The attackers behind the Maze ransomware, which surfaced in May 2019, adopted this methodology, while new ransomware such as Sodinokibi, Nemty and Clop seem to be following suit.

Most importantly, there's no guarantee that you will regain access to your files even after paying the ransom. Only 26 percent of organizations hit by ransomware got their data back after paying a ransom. Moreover, for organizations that did pay the ransom, the average cost to rectify the damage was nearly $1.45 million while the average cost for organizations that did not was $732,520. If this doesn't warrant a wake-up call, we don't know what will.

A Weak Defense Equals Surrender

Most organizations, especially small and medium-sized businesses, either assume that they will never experience a ransomware attack or that their cyber insurance will bail them out by paying the ransom. While the former is a misconception that needs to be done away with, the latter is still a possibility, but only if your cyber insurance covers ransomware. While 84 percent of businesses have cyber insurance, only 64 percent have policies covering ransomware.

Remember, a weak defense against ransomware is tantamount to leaving your business' future in the lurch.

You no longer have the time or the liberty to put off investing in best-in-class cybersecurity solutions that can help you adopt a preventative approach towards fighting ransomware. Having a trusted MSP partner will make it easy for you to adopt best practices such as endpoint security and backup, identity and access management, automated phishing defense, Dark Web monitoring, and security awareness training.

While no one can ever guarantee 100 percent protection against ransomware, there's a lot you can do currently to build a resolute defense against it.

Get in touch with us and let’s talk about how you can ward off cybersecurity’s biggest bully before it puts your business’ future in jeopardy.