Ransomware: An Evolving Threat

Ransomware has been plaguing organisations (and filling the pockets of cybercriminals) for over 30 years now, but this type of malicious software is still on the rise. Let's take a look at how ransomware is changing, count the cost of some of the largest ransomware attacks, and get to know this evolving enemy.

One of the first ransomware attacks to be recorded is the PC Cyborg Trojan (otherwise known as the AIDS Trojan) of 1989. This malicious software was transferred via floppy disk and – despite this – was still able to cause serious issues for organisations decades ago. Since then, it's safe to say that ransomware has increased in sophistication many times over, and as a result, the threat to businesses looms larger than ever. Even now, ransomware is one of the fastest growing types of malware, with cybercriminals constantly developing new ways to hold organisations to ransom for maximum profit.

Your Organisation's Worst Enemy

The threat of ransomware is one that businesses are well accustomed to by now. Ransomware is the term used to describe malicious software that infects your systems – either by exploiting the trust of a user (think phishing scams, or worse: insider threats) or exploiting a flaw in a networked service (think weak password security, missing updates, or more advanced vulnerabilities that only an expert could spot.)

What separates ransomware from general malware? Once your system is infected, it encrypts your files or locks you out of your own system, denying your users access until a payload is handed over. However, that's just the beginning.

High Profile Heists

Initially, an organisation's only dilemma would be making the tough decision of either paying the ransom, trying to recover and cleanse their systems, or scrapping everything and starting over from scratch. Nefarious parties have since developed new ways to create a Sophie's choice for their targets and pile on the pressure for them to pay up. It's no longer as simple as paying the ransom to have access to your systems again – you now need to worry about whether your files will still be there once your access is given back.

In some instances, a cyberattack is really data destruction disguised as ransomware. The infamous NotPetya incident is the most well-known example of this; initially disguised as a standard ransomware program, NotPetya had been specifically modified to make it impossible to recover your files once the ransom had been paid. The goal wasn't just financial gain, the hackers behind this attack just wanted to watch the world burn – and burn it did.

The other most well-known ransomware attack in recent memory is the equally notorious WannaCry attack which targeted around 230,000 computers across the globe. One of the biggest victims of WannaCry was the NHS, with a third of hospital trusts infected with the malicious software. The attackers first demanded $300 in bitcoin, but later doubled the amount in order to increase the pressure. To add on an extra layer of tension, they also set a deadline – threatening to permanently delete each user's files if the ransom wasn't paid within three days. This countdown clock was enough to push many users into finally paying the ransom.

Interestingly enough, the criminals had no real way of telling which victim had actually paid, and therefore couldn't associate the bitcoin they received with the specific computer of the person who had sent it. The hackers clearly had no intention of decrypting the files and for many, as is often the case, paying the ransom turned out to be in vain.

Endless Possibilities

As well as destroying your systems and refusing to decrypt data, hackers also have the means to copy sensitive files and use them to threaten a data breach. A chilling thought is: who's to say they won't just do that anyway and get a double payday? Data is like gold dust to cybercriminals, as they can make good money selling it to other nefarious parties. This creates a situation where not only does the ransomware attack cost your organisation a lot of money, but ICO fines – and the financial loss that comes with a publicised data breach – can compound the problem.

Another issue to be on the lookout for is the possibility that rather than leaving your systems once the ransom is paid, the attacker could still be lurking within – ready to strike again at a later date, and start the process up all over again. Don't think that paying the ransom will make the problem go away, if anything, you're just putting a target on your back for other hackers to target you, knowing that should the worst happen, you'll probably pay up.

Fraudsters taking advantage of your organisation's misfortune can also come in the form of claiming responsibility for an attack they didn't commit. Can the hacker decode the ransomware that has infected your systems, or has the real culprit not yet surfaced? Don't let opportunists manipulate you into paying the ransom two times over.

Paying the Price

Over a quarter of ransomware victims opt to pay the ransom and, with the average amount forfeited now reaching past $100,000 – that's a very big price to pay. There have been several high-profile ransomware attacks that have gone down in history for the huge sums the victims agreed to pay their attackers. In early 2020, foreign currency exchange Travelex handed over $2.3 million in bitcoin to the hacking group REvil, who had used the Sodinokibi ransomware to successfully encrypt their entire network. Later on that year, travel giant CWT, paid a whopping $4.5 million to regain access to their systems, after hackers stole a

whole host of sensitive corporate files and claimed they had knocked over 30,000 computers offline.

Overall, victims of the 10 biggest ransomware attacks (as of 2020) have spent well over $100 million in total costs. This doesn't just include the ransom payload itself, but also the cost of investigating the attack, restoring backups, rebuilding networks, and investing in preventative measures in an attempt to guarantee they aren't targeted again. The cost of the damage to the organisations reputation following a cyberattack: potentially priceless.

The latest predictions state that ransomware could cost businesses a grand total of $20 billion in 2021, with an attack occurring as frequently as every 11 seconds. Forward-thinking businesses are investing in all aspects of cybersecurity in order to protect their systems from ransomware attacks, and the first step to joining them is staying informed.

Fortify Your Future

2020 has already been a challenging year for businesses, and as this new year progresses, threat actors will target companies who are feeling the pressure because they'll be more likely to give in to ransom demands. In our next blog, we'll take an in-depth look at how your organisation can avoid falling victim to ransomware, vital steps in preparing for the worst, and how to bounce back following a ransomware attack.

Until then, if you'd like to know more about how offensive security plays a vital role in keeping malicious software and threat actors at bay, contact a member of our dedicated team.