Case study

Malware mayhem

A targeted ransomware attack on a technology provider opens up a can of worms

Ransomware is one of the fastest growing forms of cybercrime in the world. According to our own claims data, in 2016 ransomware accounted for little over a tenth of cyber insurance claims by number. By 2017, that figure had risen to nearly a quarter. But with ransomware now an established method of attack, we are starting to see it evolve.

In the past, it was common for ransomware to be distributed widely without a specific target in mind, in the hope that a small number of individuals and businesses would be caught out. Because this approach was not targeted and the cybercriminals who used it did not have a sophisticated understanding of their victims, the actual ransom amounts demanded were fairly modest – typically around $300.

However, we are now witnessing a shift, seeing cybercriminals starting to specifically target vulnerable companies and encrypt their data and systems with ransomware. **And because they have a better understanding of their victims, these cybercriminals are also raising their ransom demands accordingly, with many requesting amounts in excess of $50,000.**

One of our insureds affected by such a loss was a small technology firm that specialises in providing hosted platforms, with a particular focus on insurance brokerages. These platform services allow the insurance brokerages to track their insurance renewals, send out renewal reminders to their clients, source quotes from markets and purchase products from third-party insurance providers. This meant that the companies that used this software were highly dependent on our policyholder's platform to carry out their day-to-day operations and service their clients.

Encryption key costs hundreds of thousands

In July 2018, the technology firm's system was accessed by hackers, who encrypted not only all of their data but all of their applications too, meaning that our policyholder's customers were no longer able to log in and use the platform. **The business's back-ups were also compromised by the attack, which meant that any recovery was rendered impossible.**

In order to decrypt the systems, the hackers demanded 75 bitcoins in ransom. At the time of the attack, this was the equivalent of some $579,450.

> It transpired that a second group of cybercriminals had utilised the same vulnerability in their systems that the other attackers had used.

It was at this point that the insured reported the event to our incident response team. The team quickly engaged one of our partners that specialises in dealing with incidents such as this. They have particular expertise in negotiating ransom demands with cybercriminals and procuring cryptocurrencies to facilitate payment. They got in touch with the hackers from the contact information provided on the ransom note and **managed to reduce the ransom demand down by two thirds to 25 bitcoins.** Payment was arranged and the decryption key was duly provided.

Using the decryption key, we were able to decrypt and reboot the firm's systems, but that wasn't the end of the matter. Even though their data and applications were no longer encrypted, **a scan of their system indicated that their servers were still infected with malware.** It transpired that a separate group of cybercriminals had utilised the same vulnerability in their systems that the other attackers had used.

Just a short time before the targeted ransomware attack, this other group had deployed a malware variant throughout the insured's systems that was designed to harvest banking details from users. Thankfully, this threat was detected quickly and a subsequent forensic investigation found that no PII had been accessed by the attackers.

Residual malware wreaks havoc

Nevertheless, this was a **particularly sophisticated strain of malware which acted like a worm** with a morphing feature in place that meant that each time it was removed from a particular location, it was reinstalled under a new name in a new location. The malware was causing widespread disruption to the firm's systems and because the insured had some 150 servers under their control, the morphing feature made any attempt to control the malware and clean the servers exceptionally difficult and impractical to carry out in a reasonable timeframe.

The decision was therefore taken to work with the insured's datacentre provider to create all new servers and then transfer the decrypted data and applications onto them. **The datacentre provider had to procure additional hardware and human resources to enable this transfer** and the decrypted data and applications had to be scanned with anti-malware and threat hunting software to ensure that it was clean and safe to move over to the new environment.

All of this was done as quickly and efficiently as possible, but as there were so many servers, it still took the best part of two weeks before the insured could regain access to the majority of their servers.

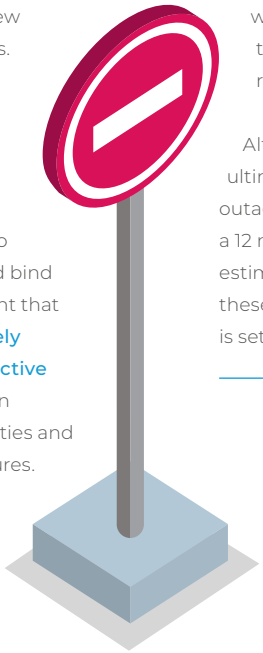
All of this was done as quickly and efficiently as possible, but it still took the best part of two weeks before the insured could regain access to the majority of their servers.

The cost to deal with the incident and get the insured back up and running came to just over $353,000. This included $193,150 in respect of the ransom payment and a further $30,000 in fees to negotiate the original figure down and procure the decryption key; $45,000 to engage forensics to carry out an investigation of the insured's computer systems; and $85,000 to work with the insured's datacentre to create new servers and transfer the insured's data and applications.

The unfortunate knock-on effect

While all this was going on, brokerages that used the firm's software were completely unable to access the platform. **This meant that brokers were unable to process customer renewals or carry out mid-term adjustments, causing a variety of difficulties for these brokers' clients.** For example, brokers were unable to pass on certificates of liability insurance to their customers, meaning that these businesses had no proof of insurance coverage in place.

An additional problem that these brokerages faced was in relation to their new business enquiries. With the platform out of action, they had no way of uploading new client data onto the system to source quotes and bind policies. This meant that **they had to actively turn away prospective clients**, resulting in missed opportunities and reduced sales figures.



Throughout the outage period, the insured tried to placate their customers by ensuring that they were kept in the loop and fully updated on any developments, and they decided not to bill their customers for the two weeks of downtime.

The insured receives their income on a monthly basis, and the cost of the rebates to customers came to $61,538. In spite of these measures, **the lack of service following the attack meant that 14% of the insured's customer base chose to cancel their contracts and move to alternative platform providers**, with all of the customers citing the system outage as the rationale behind their decision.

Although the claim and the ultimate repercussions of the outage have yet to fully play out, over a 12 month indemnity period the estimated income loss as a result of these customers moving elsewhere is set to come in at nearly $230,000.

The importance of incident response and other lessons learned

This claim highlights a few key points. Firstly, it shows the increasing severity of ransomware incidents. In the past it may have been feasible for a company to pay off a $300 ransomware attack without necessarily requiring a cyber insurance policy. But with targeted attacks like this on the rise, the likelihood of being extorted for large sums of money is only increasing and having a cyber insurance policy in place to deal with these kinds of incidents is essential.

In addition, this claim illustrates how **dealing with a ransomware incident is rarely a simple matter of the ransom payment being made and the business in question automatically regaining access to their systems and data**. In reality, decrypting computer systems and ensuring that they are free from any residual infections and vulnerabilities can be a labour intensive process lasting days or even weeks, depending on the size of a business's network.

This claim also demonstrates how important it is to work with an experienced cyber insurer with a dedicated incident response team in place. **When you buy a cyber policy, you are not just buying a promise to pay valid claims. You are also paying for a service to help and advise you when things go wrong.** This includes access to a whole range of network partners who are effectively on retainer to the policyholder through their purchasing of a cyber policy, which many small businesses might not otherwise be able to afford.

At CFC, we have nearly 20 years' of experience in the cyber market and during this time we have built up a substantial partner network, ensuring our incident response team knows who to turn to when specific events occur. The use of specialist partners in this case enabled the insured to negotiate the ransom amount down significantly, arrange payment and decrypt and clean the data and applications before transferring it to a new environment. **Had they not had this service in place, the costs incurred would likely have been much higher** and their inability to provide a service to their customers would have been prolonged.

Finally, this claim illustrates just how dependent modern businesses are on their digital assets, and how **an incident at just one part of the technology supply chain can have a domino-like effect further down the line.** Not being able to access their data or applications meant that our policyholder couldn't provide a service to their clients, and this in turn meant that the brokerages that used their platform couldn't provide a service to their customers, resulting in reputational harm and loss of income for both the insured and their direct customers.

> At CFC, we have nearly 20 years' of experience in the cyber market and during this time we have built up a substantial partner network, ensuring our incident response team knows who to turn to when specific events occur.

For the insured as the platform provider in this case, their cyber policy covered them for the costs of paying the ransom, repairing their computer systems and for their loss of income. For the insured's customers who are reliant on the platform, it's important to note that most IT providers have standard terms of service that completely limit their liability in the event that an outage results in consequential financial loss to their customers. But having a cyber policy should provide cover for any business interruption loss that they suffer as a result of a system outage at their technology supplier.

The message then is clear: any business that relies upon their computer systems to operate needs a cyber insurance policy in place.

cfcunderwriting.com