Case study

Website wipeout

An appliance retailer suffers a significant sales shortfall after its website is taken down by hackers

The dawn of the internet has opened up a world of opportunity for businesses, allowing them to reach new markets and increase their revenues. Along with this, however, has come new risks. With many businesses now increasingly reliant on online sales, they are potentially vulnerable to financial losses should their websites become inaccessible to their customers.

One of the threats posed to businesses with an online presence are distributed denial of service (DDoS) attacks. DDoS attacks are used by cyber criminals to take down websites with many utilizing what is known as a botnet to do so. A botnet is essentially a network of “zombie” computers that are infected with malware that allows malicious actors to control them without their owners’ knowledge. When DDoS attacks are carried out in this way, the computers that make up the botnet are directed to access a particular website repeatedly and in rapid succession, flooding the website with more requests than it can handle and resulting in it appearing offline to normal internet users.

In the past, botnets were relatively difficult to assemble, but nowadays anyone can hire a botnet from the dark web and command all the computers within it to aim their access requests at a website of their choice. As a result, numerous organizations have fallen victim to DDoS attacks in recent years. For example, in late 2015 the BBC’s website was taken down for a whole morning following a DDoS attack initiated by a group of hackers, while in 2016, HSBC was hit by a DDoS attack that resulted in millions of customers being unable to access HSBC’s online banking services. Most recently, in mid-April 2019, the hacktivist group Anonymous claimed to have been behind DDoS attacks which brought down the websites of the National Crime Agency and the UK Supreme Court following the arrest of Julian Assange.

However, large, multinational corporations are not the only organizations that are targeted in this way. One of our policyholders affected by a DDoS attack was a small retailer of domestic goods. Although the majority of their sales are carried out in store, a sizeable portion come from sales through their website.

Hacker fulfils promise of attack after missed email threat

The incident began when an unidentified hacker sent an email to one of the firm's business email addresses, stating that the company's website would be taken down within 24 hours unless a payment of $4,000 in Bitcoin was made. However, this email was caught in the company's spam filters, meaning that it was not initially read by anyone at the company and so no reply was sent to the hacker.

Having not received any response to the threat after 24 hours, **the hacker stayed true to his word and looked to initiate the next phase of the attack.** Utilizing the massive number of computers under his control via a botnet, the cyber criminal directed the computers to send a vast amount of access requests to the company's website. Without any DDoS protection in place and as this was only a small business, this flood of internet traffic was well in excess of what the their website could handle. The website was soon overwhelmed and became inaccessible to genuine internet users looking to browse products.

Remedy attempts repeatedly thwarted

It was the next morning when the policyholder became aware that the website was not appearing to external users. After some initial investigations, **it was determined by the company's IT department that the website was facing a sustained DDoS attack.** In an attempt to overcome the issue, the IT team decided to block any internet traffic that came from outside the country in which they were based. This provided a very brief period of respite for the insured, with the website appearing back online, but the hacker responsible refused to give up that easily.

To overcome this new obstacle, the hacker made use of proxy servers. A proxy server acts as an intermediary between an end user and the internet, and essentially allows the end user to go online with a substitute IP address. In this case, the hacker simply switched the blocked IP addresses over to proxy servers that made it appear as if they were coming from the same country as the insured. This meant that the website was inundated with internet traffic once again, resulting in it appearing offline for a second time.

Having discovered that the website was down again, the insured's IT department tried another tactic to help remedy the situation. This time they changed the website's IP address, meaning that all of the DDoS related internet traffic was now being redirected to the old IP address. With the DDoS attack now focused on the old IP address, legitimate internet users could now access the insured's website.

However, this proved to be yet another short-lived victory. **The attacker was determined to bring the website down and force the insured into making a ransom payment,** so after realizing that the insured had changed the website's IP address, the hacker simply switched the point of attack to the new IP address, swamping the website with internet traffic once more and bringing the site to its knees.

> The hacker simply switched the point of attack to the new IP address, swamping the website with internet traffic once more and bringing the site to its knees.

Policyholder enlists the helps of CFC's cyber incident response team

After several further attempts to counter the attack meeting with little success, it was at this point that the insured got in contact with our incident response team. **Our team swiftly directed the insured towards one of our incident response partners that specializes in providing DDoS mitigation services.** This service works by providing organizations affected by a DDoS attack with access to a network of data centres with a much higher capacity to absorb the vast amounts of internet traffic being generated by the attack. In addition, the service is also able to establish the difference between legitimate and illegitimate web traffic, thereby blocking malicious requests and allowing genuine internet users to access the affected site. After submitting some key details, the company was able to gain access to this service and within a few minutes their website was up and running again without suffering any further disturbance.

Nevertheless, the company website had been down from 7 o'clock in the morning until just after 4 o'clock in the afternoon, with only a few brief moments of normality in between the hacker's various attacks. **During this time, customers had been unable to access their website and purchase any items online.** Despite seeing a resumption of sales in the days after the attack, the insured still suffered a noticeable reduction in overall sales for the month. Having budgeted for $1,126,838 in online sales for the month in question, the insured only achieved sales of $951,632, a shortfall of $175,206. After adjusting the loss to reflect that the business had been slightly behind budget in the weeks preceding the DDoS attack, and following the application of a rate of gross profit of 41%, **this resulted in a business interruption loss of $51,506,** which was picked up by the insured's cyber policy with CFC.

How to minimise the impact of a DDoS attack

This claim highlights a few key points. Firstly, it illustrates the importance of businesses investing in some form of DDoS protection, as these attacks are increasing in terms of size and power. **Indeed, some hackers are exploiting the rise of connected devices** (sometimes referred to as the Internet of Things or IoT), such as cameras, smart TVs, printers and even children's toys and baby monitors, to increase the computing power at their disposal when carrying out DDoS attacks. Depending on the size of the business in question, DDoS protection can be a relatively inexpensive purchase and is often available to businesses via their web-hosting providers. Having this protection in place can help reduce the likelihood of an organization's website being taken down by malicious actors.

Secondly, it underscores the importance of policyholders notifying incidents to their insurer as soon as they can. In this case, the company's internal IT department initially attempted to deal with the DDoS attack on their own, but unfortunately their attempts were unsuccessful. After the matter was referred to our incident response team, we managed to get the policyholder in touch with a specialist provider and get the website back online very quickly. **Had they notified the incident earlier, it would likely have resulted in the incident being resolved without any meaningful interruption** or reputational damage to their organization.

Finally, it highlights just how dependent modern businesses are on their digital assets and how important cyber insurance coverage is. **The policyholder's website was only out of action for a single working day yet it still resulted in a sizeable business interruption loss.** However, traditional insurance policies, such as standard property and business interruption cover, were designed to deal with threats to a company's physical assets, rather than their digital assets like websites, software programmes, data and electronic funds. Cyber insurance fills this gap, providing cover for digital assets against 21st century threats. ●