MARSH

May 2017

CLIENT ALERT

WANNACRY RANSOMWARE VIRUS

ON FRIDAY MAY THE 12TH 2017 A RANSOMWARE VIRUS DUBBED "WANNACRY" AMONG OTHER SIMILAR NAMES, AFFECTED MORE THAN 200,000 IP ADDRESSES IN 150 COUNTRIES. VIRUS DEMANDS A PAYMENT OF APPROXIMATELY NZ$430 TO RELEASE FILES OR ENABLE COMPUTER ACCESS.

The ransomware spread via a vulnerability in machines running unpatched versions of Windows (XP through 2008 R2) by exploiting flaws in Microsoft Windows SMB Server. This vulnerability was identified by and stolen from US Intelligence entities in April 2017, and companies should have installed software update released by Microsoft in March 2017 to prevent their computers being affected. It appears many organisations ranging from hospitals, government agencies, telecommunication providers and manufacturing companies across the globe, had not completed this software update.

What is ransomware?

Ransomware, as the name suggests, holds a company's data for ransom by encrypting it and demanding a payment for the decryption key. The company's computer systems or data becomes inaccessible until the ransomware is removed or the ransom is paid. The average ransomware demand according to Symantec is US$1,077, but paying the ransom is not often advised. While sometimes paying the ransom does release your data, you will find that the attackers still have access to your systems and you are likely to then experience repeat ransomware attacks as a known "ransom-payer".

The WannaCry virus is distinct as it does not rely on victims to click on an infected link or attachment to on-spread the malware like many others. It is a worm which once inside an organisation will search for vulnerable machines, and therefore is able to infect a large number of machines exceptionally quickly.

Has it affected New Zealand businesses?

CERT NZ, the New Zealand Government cyber-security agency, has received a small number of reports from New Zealand computer users who have been affected by WannaCry but these are yet to be substantiated.

Prevention is better than cure

CERT NZ suggest the following prevention tactics to prevent your computer being infected:

- Make sure you have backed up your system and files stored securely, off-network
- Make sure you have patched your system. Organisations using any Windows system between XP to 2008 R2 should ensure that mitigations are in place, particularly the MS17-010 Microsoft patch. If you're not patched, consider disabling SMBv1 (this will stop some file sharing)
- Be careful when opening emails and clicking on links – read CERT's phishing information to know what to look out for. These emails could be from anyone, including an email address you're familiar with
- Microsoft has released updates for otherwise unsupported operating systems (OS), including Windows XP and Server 2003, which are available here. Microsoft doesn't officially provide support to these systems any longer, but has released this patch in response to the WannaCry spread
- Make sure that firewalls and anti-virus software is installed, up-to-date, and fully operational
- It is also important to ensure that staff are aware of this campaign, and reminded to be extremely vigilant with incoming emails containing links and attachments

How would a cyber policy respond?

All companies have some reliance on technology, whether it is a complete reliance on the accessibility of the network for the day-to-day running of their business, on the availability of emails for customer or supplier communication, or just to invoice their customers.

In the event that systems or data became inaccessible as a result of a ransomware virus, a cyber insurance policy can ensure that you are back up and running at the earliest possible stage. Let's take the following example of Ben's Architectural Company, who was affected by the WannaCry ransomware:

Ben arrives at his office as usual on Monday morning, ready to start his day as an architect at his family's firm. After making his coffee, he turns on his computer only to find a suspicious looking pop-up staring back at him stating his files have been encrypted, and a ransom of NZ$430 must be paid by Bitcoin in order for the files to be released. He suspects this is the virus he was reading about over the weekend!

Ben is extremely worried, but he remembers that he talked to his Marsh broker only a few months back about Cyber Insurance and purchased a cyber insurance policy. He gives his broker a call, who immediately gets in touch with the insurer to have the necessary consultants appointed to manage the issue. Ben receives advice from the IT firm appointed on what to do immediately, and then has a forensics team in the office within a few hours. While Ben's cyber policy would cover the ransom payment, Ben doesn't want to pay this as he doesn't want to be targeted again in the future! Ben's response results in the the consulting team being able to remove the ransomware after eight hours. Expert fees prove to be expensive – the total cost amounts to over $18,000 which is covered by Ben's cyber insurance policy.

Marsh Risk Consulting has teams specialising in cyber risk, forensic accounting, claims, reputational risk and crisis management. If you need help with any of these steps, contact one of the below contacts or your Marsh Client Executive.

Contacts

Marcus Pearson
Country Head New Zealand
T: +64 9 928 3079
E:marcus.pearson@marsh.com

Frederic Boles
Head of Specialities
T: +64 9 928 3125
E: frederic.boles@marsh.com