

Biggest ransomware outbreak reaches Australia - blueAPACHE

Canonical: <https://www.blueapache.com/blog/biggest-ransomware-outbreak-in-history-reaches-australia>

Details:

2017

Australian organisations brace for a new wave of ransomware attacks linked to WannaCry due to its rapidly developing variants and the beginning of the work week. A ransomware attack of unprecedented scale was launched over the weekend, sending tremors across the globe, and reaching Australian shores on Monday. Dubbed WannaCry, this ransomware is targeting computers running on Microsoft Windows operating system and has spread to more than 230,000 computers in over 150 countries in just two days. As reported by global news outlets, amongst those impacted are the UK National Health Service (which was forced to reject patients, cancel operations, and reschedule appointments), Spanish telecommunications sector, German railways and US-based courier, FedEx Corp. The map below shows its global spread within the first few hours, as well as Australia, Sweden and Norway where incidents have been reported since. *Source: Kaspersky Lab research How does it work? The ransomware was executed through a phishing attack via an email containing a link or a PDF file with payload. When clicked, it installs WannaCry on the targeted system. The attack vector has the hallmarks of a traditional computer worm. Once a single computer has been compromised, the worm continues to look for other vulnerable computers within the local network and infects them as well.

“The worm functionality attempts to infect unpatched Windows machines in the local network. At the same time, it also executes massive scanning on Internet IP addresses to find and infect other vulnerable computers. This activity results in large SMB traffic from the infected host” Microsoft said in a post released on Friday.

When executed, WannaCry encrypts user data and demands a payment of US\$300 in bitcoin. The ransom note indicates that if the ransom is not paid within three days, the amount will double and after seven days, the encrypted files will be deleted forever. The Server Message Block (SMB) exploit being used by WannaCry has been identified as EternalBlue, a collection of hacking tools allegedly created by the U.S. National Security Agency (NSA). EternalBlue exploits vulnerability MS17-010 in Microsoft's implementation of the SMB protocol. This Windows vulnerability is not a zero-day flaw. Microsoft issued a security patch to address it on 14 March 2017. However, delays in applying the security update and systems running on older, unsupported operating systems have left many users vulnerable. Due to the scale and spread of this attack, Microsoft have since released an emergency security patch update for unsupported version of Windows. How can you protect yourself? In spite of the far reaching ramifications of WannaCry, prevention measures only involve basic security best practices that are within reach for any organisation. This includes keeping operating systems and antivirus software up-to-date and timely deployment of security patches. The importance of end user education in preventing social engineering attacks cannot be overstated. When end users are aware of the type of threats to look out for, and the actions to take when they spot malicious activity, they can form the best layer of defence for your organisation. Our existing managed services customers who have authorised automatic patching are protected from this vulnerability as the related Microsoft security patch was deployed last month as part of our monthly patch roll-out. If you are not our customer or if have seen suspicious activity and believe your systems may have been exposed, please contact the our security team immediately.

What ransomware outbreak did you report on and when was it published?

We published a blog post titled 'Biggest ransomware outbreak reaches Australia' on May 15, 2017, about the WannaCry ransomware attack.

How widespread was the WannaCry ransomware attack according to the blueAPACHE article?

WannaCry spread to more than 230,000 computers in over 150 countries within just two days, with a ransomware attack of unprecedented scale launched over the weekend that reached Australian shores on Monday.

Which organisations were reported to be impacted by WannaCry?

impacted organisations included the UK National Health Service (which was forced to reject patients, cancel operations, and reschedule appointments), the Spanish telecommunications sector, German railways, and US-based courier FedEx Corp.

How did WannaCry infect computers?

WannaCry was executed through a phishing attack via an email containing a link or a PDF file with payload. Once clicked, it installed WannaCry on the targeted system, and the attack vector behaved like a traditional computer worm, spreading to other vulnerable computers within the local network and scanning the internet for more vulnerable machines.

What did WannaCry do once it infected a computer, and what ransom did it demand?

When executed, WannaCry encrypted user data and demanded a payment of US\$300 in bitcoin. The ransom note stated that if the ransom wasn't paid within three days, the amount would double, and after seven days the encrypted files would be deleted forever.

What exploit did WannaCry use and what vulnerability did it target?

The SMB (Server Message Block) exploit used by WannaCry was identified as EternalBlue, a collection of hacking tools allegedly created by the U.S. National Security Agency (NSA). EternalBlue exploits vulnerability MS17-010 in Microsoft's implementation of the SMB protocol.

Was the WannaCry vulnerability a zero-day flaw, and did Microsoft release a patch?

No, the vulnerability was not a zero-day flaw. Microsoft issued a security patch to address it on 14 March 2017, but delays in applying the update and systems running unsupported operating systems left many users vulnerable. Due to the scale of the attack, Microsoft also released an emergency security patch update for unsupported versions of Windows.

What protection measures do you recommend against ransomware like WannaCry?

We recommend basic security best practices including keeping operating systems and antivirus software up-to-date, timely deployment of security patches, and end user education to help staff recognize threats and respond to malicious activity, which forms a key layer of defence for

organisations.

Were your managed services customers protected from the WannaCry vulnerability?

Yes, existing we managed services customers who had authorised automatic patching were protected from the vulnerability because the related Microsoft security patch was deployed the previous month as part of our monthly patch roll-out.

What should someone do if they suspect their systems have been exposed to WannaCry?

We advise that if you are not our customer, or if you have seen suspicious activity and believe your systems may have been exposed, you should contact our security team immediately via our contact page.