FirstWave Security Update – "Wannacry" ransomware

15 May 2017

Highlights:

- **On May 12, "Wannacry" ransomware attacked public and private organisations worldwide**
- **FirstWave's content security platform enforced protection automatically**
- **There were no breaches seen through our platform**
- **Our cyber security team will keep monitoring to ensure variants have been detected.**

Over the weekend, FirstWave has been closely monitoring a major ransomware attack with serious global impact popularly named as 'Wannacry' or 'Wanacry'. The 'Wannacry' attack began with the spread of the WanaCrytpOr ransomware to public and private organisations worldwide. These attacks were focused on overseas countries but they have now started to affect some organisations in Australia.

A number of different threat vectors have been used in this attack, including network intrusion, email attachments and malicious URL links. WanaCrypt0r ransomware attacks begin through two mechanisms, either, an email-based phishing delivery mechanism that includes a malicious link or PDF document, or through a network-based exploit targeting internal MS Windows systems through a non-patched device. If the link or pdf document is opened, the attack results in the delivery of the WanaCrypt0r ransomware on the target system.

This attack has primarily affected organisations with large numbers of MS Windows operating systems, both server and workstations, where both endpoint security patching processes and gateway security were not adequate. FirstWave platforms provide protection independent of the underlying customer infrastructure.

FirstWave Cloud platforms use multiple layers of defence to protect against internet based vectors used by this attack. The platform incorporates world-leading multi-vector security solutions including from Cisco and Palo Alto Networks. It automatically analysed and enforced protections from this attack from the moment it began. No breaches were detected through our platform, which scans and blocks millions of emails every day and protects tens of thousands of client devices.

Our cyber security forensics team observed no cases of this attack getting beyond our first layer of defence.

Simon Ryan, FirstWave's CTO commented, *"FirstWave customers are with us for a reason, they are already security conscious and understand the seriousness of ensuring the best security posture."*

"This global event heralds the need for sweeping changes in IT administration. It is no longer acceptable to have unmaintained IT assets and companies worldwide need to face the commercial realities of the move to cloud for security."

"Some of the biggest impacts we have seen have been in the medical sector, where typically funding for maintenance is low and legacy software dependencies are high, we can expect to see big changes here also and the uptake of IOT firewalling as standard practice."

Prevention

Here are a few actions to prevent future attacks:

- Deploy effective email and web security gateways
- Identify which assets require protection, particularly those that hold important, sensitive data. These assets can include mobile devices as well.
- Patch all servers, workstations and mobile devices, as well as software applications
- Maintain current backups of critical data
- Restrict Administrator and other powerful user ids
- Restrict access to critical files
- Use multi-factor authentication
- Remove access to software for which there is no business need, e.g. Flash
- User training - Train your workforce to recognise and avoid malicious emails, links and attachments
- Employ and empower an effective IT Security Team/Advisor

For more help to prevent future attacks:

For support – support@firstwave.com.au 02 9409 7000
For sales enquiries – sales@firstwave.com.au 02 9409 7000

For media inquiries: Damian Fielke, Corporate communications, 02 9409 7005

Follow FCT on its Twitter feed: https://twitter.com/Firstwave_FCT

About FirstWave Cloud Technology

Australian cloud technology company, FirstWave, operates a technology business in the burgeoning cloud based IT managed security services market, having created an intelligent carrier grade cloud security platform for business. First Wave has delivered Software as a Service (SaaS) solutions since 2004 in a form similar to what we call "cloud" today and has a long standing relationship with Telstra. FirstWave offers a comprehensive cloud security and analytics technology solutions suite that, along with advanced mail, web & NGFW content controls, now offers unified, integrated x-threat vector advanced malware protection technology solution for any business or enterprise moving to or operating in the cloud. Over 300 customers already trust FirstWave including the largest Australian financial institutions, state and federal government, utilities, ASX listed and private companies in the mining and retail sectors. www.firstwave.com.au