Australia victim to more than 200,000 ransomware attacks in past two months alone, finds Trend Micro

Australia second most affected country in the world for exploit kit ransomware as Angler Exploit Kit targets local businesses and consumers

SYDNEY, 13 July 2016 – Trend Micro found that Australia has been one of the primary targets for a major exploit kit ransomware infection over the past two months, with more than 224, 000 ransomware attacks in the April/May period. Of these attacks, more than 213, 000 have been as a result of the Angler Exploit Kit.

The high volume of exploit kit ransomware attacks in Australia, second only to Japan in the same period, is due to a ransomware infection vector move toward URL and Exploit Kits.

Around the world, more than 66 million ransomware-related threats have been detected/blocked by Trend Micro from January to May of this year, with almost 700,000 of those in Australia and more than 19,000 in New Zealand.

“With the growing threat of ransomware attacks specifically aimed at Australian organisations, we recommend that enterprises and small businesses are more vigilant than ever,” said Indi Siriniwasa, enterprise sales and channel director for Trend Micro Australia and New Zealand. “The new ransomware families have sophisticated delivery and evasion techniques such as self-destructing after they successfully complete their routine. The best way to defend against this sophistication is to use a multilayered security approach.”

“Australia has really been targeted by cybercriminals with this Angler Exploit Kit and it is Australian consumers that will suffer,” said Tim Falinski, consumer director, Trend Micro Australia and New Zealand. “Consumers should make themselves aware of the threats and ensure all their devices – from smartphones to PCs to connected smart devices – are protected.”

64% of ransomware threats were seen at the email layer. This is due to ransomware being largely distributed via spam, either as a macro or JavaScript attachment, or via a clickable link in the message body.

34% of ransomware-related threats are blocked in the URL layer. These URLs are usually compromised sites, malvertisements, or landing pages that host exploit kits leading to ransomware. A very small percentage (2%) of ransomware-related threats are ransomware detections blocked at the file layer.

From January to May 2016, Trend Micro has so far seen 50 new ransomware families. Of these, 19 ransomware families arrived via spam, while six of these new ransomware families arrived via exploit kits. All of these new families still encrypt files and drop ransom notes.

About Trend Micro

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centres, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defence with centralised visibility and control, enabling better, faster protection.

With more than 5,000 employees in more than 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organisations to secure their journey to the cloud. For more information, visit TrendMicro.com.au.

Contacts

Michelle Bong
+61 422 966 013
mailto: michelle@benchpr.com.au