Comabting ransomware

By Colin Thornton

30 May 2017

Even though local statistics are difficult to come by given the sensitive matter of the issue, ransomware is on the increase in South Africa and the rest of the world. It is also not only large multi-nationals being targeted - even individuals are feeling the ire of malicious users trying to extract monetary gain in exchange for the safe release of corporate or personal data.

© JavadR via pixabay.com

With the FBI estimating that profits relating to ransomware exceeded a billion dollars last year, it is clear to see why it is such an enticing avenue to pursue fraudsters. In fact, research by Kaspersky Labs shows that the average amount of money stolen in individual ransomware attacks increased from $472 in 2015 to $482 last year.

Additionally, according to a Trend Micro report, 38% of ransomware victims decided to pay the ransom with the US Department of Justice - rating this form of attack as the biggest cyberthreat for 2017.

South Africa's ranking

Ransomware, also referred to as cryptomalware, generally enters company networks through email attachments. And while being a global phenomenon, the Kaspersky research shows that South Africa moved up the list of 117 most attacked countries to 31st in November.

So how do you protect yourself against attacks? One of the key elements is to provide employees with security awareness training. This is important to prevent them from clicking on phishing links sent in emails.

Of course, if the worst has already happened, what is there to do?

Andy Patel, a security expert at F-Secure, says you need to respond to such an incident in a level-headed manner.

Isolating and remediating affected machines

“You’re going to want to start by isolating and remediating affected machines before restoring data from backups and ensure that you have the right protection on your network to prevent it happening again. Make sure you don’t restore the original infection vector during that process. And when your systems are back up and running, remember to kick off a root cause analysis. Learn from the experience and improve your processes and systems to avoid future infections,” he says.

However, this does mean that you need to backup your data to a safe location as quickly as possible (if you are not doing so already). This at least enables you to be up and running faster and restore business operations quickly.

Of course, simply backing up to a removable hard drive is no longer good enough…

The importance of data means that you need to ensure you have robust backups in place, should the worst happen. As such, the 3-2-1 rule applies - which states that you need to implement three backups of your important data on two different media with one of them being kept offsite. This should be seen as an essential part of any business continuity or data recovery strategy.

After all, can you really afford not to keep your sensitive information safe?

Read the second article in this series...

Combating ransomware [part II]

Colin Thornton 7 Jun 2017

ABOUT COLIN THORNTON

Colin founded Dial a Nerd in 1998 as a consumer IT support company and in 2002 the business- focused division was founded. Supporting SME's is now its primary focus. In 2015 his company, merged with Turrito Networks who provided niche internet services outside of the local network. These two companies have created an end-to-end IT and Communication solution for SME's. Colin has subsequently become the managing director of Turrito. Contact him at info@dialanerd.co.za

- Understanding SA's 5G reality - 4 Apr 2019
- Why your business needs a cloud architect - 21 Feb 2019
- Privacy vs Profit: Will 2019 be the year of consumer paranoia? - 26 Nov 2018
- Why SMEs should be looking at cyber insurance - 28 Sep 2018
- Why your future digital ID should harness blockchain technology - 23 Aug 2018

View my profile and articles...