Combating ransomware

By Colin Thornton

7 Jun 2017

In a previous article, we examined the rise of ransomware and some of the issues that people need to be aware of when addressing this scourge. But given how instances of attacks are increasing, people need to go on the offensive when dealing with one of the fastest-growing fields in cybercrime.

Unlike other forms of malware, ransomware is directly focussed on financial gain. Once a corporate (or personal) system is infected with the malicious code, cyber criminals can encrypt data, demand payment that usually takes the form of bitcoins, and then release that data back to the organisation or individual.

Colin Thornton

According to Eset South Africa, paying for ransom is a dangerous option: “For starters, there is no guarantee your files will be returned or that the malware will be removed. Will the hacker exploit you again in six months’ time?"

> *So, is ransomware the newreality that organisations and individuals are faced with in the online world?*
>
> The very nature of ransomware can make many feel powerless to respond. One of the key steps to take is to install security software that is frequently updated with the latest anti-malware and anti-virus definitions. And while there are many freely available solutions on the market, it is always good to opt for software that can analyse the behaviour of malware and determine the next action of the threat based on attack patterns, techniques, and crowd-sourced threat intelligence.

Awareness is growing

Fortunately, awareness against ransomware is growing. The Dutch National Police, Europol, Intel Security, and Kaspersky Lab have joined forces to launch an initiative called No More Ransom, a new step in the cooperation between law enforcement and the private sector to fight ransomware together. No More Ransom is an online portal that informs the public about the dangers of ransomware and helps victims recover their data without having to pay ransom to cyber criminals.

Comabting ransomware [part I]
Colin Thornton 30 May 2017

“The biggest problem with ransomware is that when users have precious data locked down, they readily pay criminals to get it back. That boosts the underground economy, resulting in an increase in the number of new players and a number of attacks. We can only change the situation if we coordinate our efforts to fight against ransomware. The appearance of decryption tools is just the first step on this road. We expect this project to be extended, and soon there will be many more companies and law enforcement agencies from other countries and regions fighting ransomware together,” states Jornt van der Wiel, security researcher at the Global Research and Analysis Team of Kaspersky Lab.

Battle lines drawn

Increasingly, other large technology companies and government organisations are using special teams focused on not only better pro-active protection, but also on going on the offensive against malicious users and groups.

These so-called Red Teams or Red Forces act as independent groups that challenge all aspects of the cyber security of a company. This sees them carrying out trial attacks on themselves - and using the learnings/insights to try and take out the hackers directly by infecting their systems.

The battle lines have been drawn. Now is the time to act.

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...