BIZCOMMUNITY

# The developing cyberthreat landscape

By Riaan Badenhorst

15 Jan 2018

2017 saw many organisations across the globe fall victim to some very serious cyberattacks. In fact, the WannaCry and ExPetya ransomware attack(s) clearly demonstrated that it doesn't always take a hugely sophisticated outbreak to cause massive damage.

Riaan Badenhorst, general manager at Kaspersky Lab Africa

The reality is that the cybercriminal industry is growing – leaving many wondering when, and if, their business will be 'next on the list' and what the consequences will be.

According to our research (in partnership with B2B International), large enterprises in the Middle East, Turkey and South Africa pay an average of $591K per security incident. While costly, the real challenge presented by targeted attacks is that they also cause severe reputational damage to a business – one where costs can run very high.

> ***Of course, we know that the cyberthreat landscape is growing at a quicker pace than it did years ago. Given this, what type of attacks are likely to be seen in 2018 and beyond, as cybercriminals become more tactical in their approach?***

## The continued rise in ransomware

The past year has seen many cases of ransomware attacks emerge. Most recently was Bad Rabbit. In fact, the number of ransomware notifications reported by Kaspersky Lab in the META region increased by 36% in 2017 (compared to the first quarter of 2016).

#BizTrends2018: Business intelligence trends to watch in 2018
Yolanda Smit 11 Jan 2018

These incidents will likely continue into 2018 – given the increased availability of ransomware-as-a-service. Ransomware is growing in sophistication and diversity, offering a lot of ready-to-go solutions to those with fewer skills, resources or time – through a growing and increasingly efficient underground ecosystem.

## An increase in high-end mobile malware

As the world has continued to be heavily reliant on mobile technology, over the past few years, the security community has uncovered advanced malware targeted at mobile devices which, when combined with exploits, creates a very powerful cybercrime weapon against which there is little protection.

Our assessment is that the total number of mobile malware existing in the wild is likely higher than currently reported, due to shortcomings in telemetry that makes these more difficult to spot and eradicate.

> ***We estimate that in 2018 more high-end APT malware for mobile will be discovered.***

## More attacks targeted at routers and modems

A known area of vulnerability that has been vastly unnoticed over the past few years is that of routers and modems. Used in many enterprises, these pieces of hardware tend to be everywhere as they play an important role in daily business operations.

These ‘little’ computers are internet-facing by design and therefore are a key target for an attacker with the intent on gaining access to a network, and could even allow an attacker to hide their trail.

Given that not much attention has been paid to these devices, attackers will likely place a strong focus on using these in their tactics in 2018.

## A focus on cryptocurrency

Not so long ago, there was only one cryptocurrency – Bitcoin. Today, however, as many as 50 of them exist. In fact, in some countries, governments and banks have to accept cryptocurrencies, which means that banks are considering developing their own financial blockchain-based services.

However, as with any new technology, there is the risk of new threats and vulnerabilities. Cryptocurrencies are no

exception. Towards the end of 2017, our researchers discovered a new CryptoShuffler Trojan, which was designed to change the addresses of users' cryptocurrency wallets in the infected device's clipboard (a software facility used for short-term data storage). While clipboard hijacking attacks have been known for years, redirecting users to malicious websites and targeting online payments systems, involving a cryptocurrency host address, have been rare.

> ***Yet, as cryptocurrencies gain traction, so too will threats targeted at this digital currency.***

If we take the above into consideration and just given the harsh realities felt by the WannaCry ransomware attack – not to mention the highly destructive ExPetr/NotPetya/Petya attacks that occurred in 2017 – more needs to be done in the way of cybersecurity by organisations.

#BizTrends2018: Diversifying connectivity - key in 2018

Riaan Maree 10 Jan 2018

Businesses must invest 'differently' in cybersecurity measures – focusing on solutions that offer them the ability to be 'threat intelligent' and well prepared should an attack occur. Furthermore, to ensure better protection against unknown attacks, following the below steps can be useful:

- Install critical software patches released by developers and use the latest software versions always in business networks.
- Ensure that security solutions are switched on for all nodes on a corporate network.
- Avoid running open attachments from untrusted sources.
- Always backup sensitive data to external storage - and keep it offline.

It only takes one successful attack on the company's IT network for the cybercriminal or gang to steal critical company data or hold a business 'ransom'. While 100% protection against attacks can never be guaranteed, having a view of possible threats and placing a focus on cybersecurity measures can go a long way in minimising the possible damages.

*View more ICT trends in the BizTrends2018 special section.*

## ABOUT RIAAN BADENHORST

Riaan Badenhorst joined Kaspersky Lab in January 2011. He headed up the corporate sales division, focused on growing Kaspersky Lab's market share in both the Enterprise and SMB sectors in sub-Saharan Africa. In October 2012 Badenhorst was appointed as managing director for the Africa region and has been heading Kaspersky Lab operations in the region ever since.

- How many abandoned online accounts do you have? - 14 Feb 2020
- #BizTrends2018: The developing cyberthreat landscape - 15 Jan 2018
- #BizTrends2017: What will the cyber threat space hold in 2017? - 10 Jan 2017

View my profile and articles...