BIZCOMMUNITY

2015: the year when businesses safeguard themselves from cybercrime

By Doros Hadjizenonos

23 Jan 2015

Last year was a difficult time for businesses when it came to cybercrime. In the US, organisations including Sony and eBay were compromised when hackers tried to steal personal and company information. But probably the biggest event of 2014 was Heartbleed, a flaw in the OpenSSL system that exposed internet users' passwords and allowed hackers to steal information.

Closer to home, the South African Post Office lost R42 million when it became a victim of hacking and a number of local websites, including Starbase Telecoms and Infoware Studios, were compromised in a mass hacking of outdated content systems. Most concerning was the attack on a South African Police Service-run website, which revealed the identities of whistle-blowers, possibly jeopardising their safety.

Cybercrime costs the South African economy a whopping R5.8 billion a year with more than one million South Africans falling victim to cybercrime over the past year. Organisations that do not implement robust security measures - which need to be constantly monitored and adapted to emerging and changing threats - expose themselves and their stakeholders to risk.

Check Point Software Technologies has conducted an analysis of the key trends and threats currently facing businesses and governments worldwide.

Precise and refined techniques

What the experts have long referred to as cyberwar is but the trend towards increasingly specific attacks with a targeted objective. These are backed by highly organised groups that use precise and refined techniques, making traditional anti-malware solutions highly ineffective. We are seeing that most of these attacks come from Russia or China, but also from other countries like Japan, India and Brazil.

The attacks on South African organisations were targeted and confirm the global trend of 'cyberwar'. 'Big cybercrime' is promoted by a new generation of organised groups whose operations are increasingly politically motivated.

There is a huge black market in the world that many people are unaware of. For example, a hacker who discovers an unknown security threat can charge about R500,000 for it, or can command a multimillion-rand fee to plan an attack against a government.

Some of the trends and key concepts in the current security landscape in South Africa are:

- **Distributed Denial of Service (DDoS)**: This criminal activity was used to attack the website of various local gaming platforms. This computer attack involves many computers continuously requesting certain information to the attacked network until saturation and, therefore, its downfall;

- **Advanced Persistent Threats (APTs)**: An attack of this type is common against governments, with infiltration attempts from coordinated groups of up to 20 hackers. ATPs are high-profile, sophisticated and carefully constructed attacks, and do not always point to known programs;

- **Redirecting emails**: This method is especially damaging because, in many cases, sufferers are not aware of it, at least for some time. It is the method reported by the State Security Agency, which said its websites and servers had been attacked, redirecting emails from managers to spies, who would extract all kinds of information;

- **Social engineering**: This is the preferred method when launching attacks from malware or phishing techniques to companies and agencies. The 'hooks' are varied. For example: hackers will call a person by name, or, if the person is part of the HR department, will send an email entitled 'Payroll updated'. This technique is associated with one of the most serious illegal intrusions into corporate networks in recent history;

- **Unknown malware**: During 2013, there was a surge of a more intelligent, sophisticated and tougher malware that was established and maintained throughout 2014. Threat emulation sensors revealed that between June and December 2013, one in three organisations downloaded at least one file infected with unknown malware. New complication tools known as 'crypters' allowed cybercriminals to evade detection by anti-malware software; and

- **Organised cybercrime groups**: Cybercriminals today operate in groups of various sizes and types. Some have very similar structures to any legitimate company, with teams of experts like quality and project managers. Others even have members with expertise in marketing to spread threats and information easily through social networks and forums, from which botnets and malware can spread.

In conclusion, it is imperative that companies and government agencies identify their critical data and surround it with the necessary safeguards to protect it. The new threat prevention techniques, such as emulation solutions, are presented as an effective protection for the most demanding corporate networks and are critical.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet
- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...