Kaspersky Lab: cyber-security trended in 2015

In 2015, the word "cyber-security" entered popular culture. Perhaps for the first time in history, issues relating to the security of the Internet and the protection of internal networks were discussed by, and became relevant to every sector of the economy as well as everyday life: from finance, manufacturing/industrial, automotive and aircraft to wearable devices, healthcare, dating services and more.

©Gleb Shabashnyi via 123RF

2015 saw near-exponential growth in all areas related to cyber-security. In fact, Kaspersky Lab has seen a massive growth in detected threats in South Africa over the last year: according to KSN the threats detected locally in 2014 compared to threats detected until mid-November 2015 tripled. Says Dirk Kollberg, senior security researcher, global research and analysis team at Kaspersky Lab: "Such an increase certainly shows that South Africa is a growing target for cybercrime, and a country that needs to pay attention to this reality and the future trends and predictions in this space."

Complexity of attacks

For Kaspersky Lab, the overriding trend in 2015 globally has been increased complexity in cyber-attacks. The growing number of attacks, the numbers of both attackers and their victims, together with a greater focus on cyber-security in defense budgets, new or enhanced cyber-laws, international agreements and new standards - 2015 redefined the rules of the game. This year, agreements on cyber-security were signed between Russia and China, China and the United States, and between China and the United Kingdom. These agreements include not just a commitment to mutual cooperation but an assurance that both sides will seek to prevent attacks on each other.

Cyber-activity during 2015 is described by Kaspersky Lab's Global Research and Analysis Team (GReAT) as "elusive" - full of cyber-criminals that are proving hard to catch, cyber-espionage actors that are even harder to attribute, and with privacy often the most elusive of all. Cyber-attacks have achieved the impossible: they have thinned the walls of bedrooms and offices around the world.

"Select any economic sector at random, and the chances are high that you'll find something in the media about a cyber-security incident or problem. The same goes for all aspects of everyday life. This year's cyber-events have resulted in a sharp increase in interest, not only in the world's media but also in the entertainment industry. Movies and television programmes featuring cyber-security issues sometimes resulted in experts appearing as themselves. However, in addition to the positive changes of increased public awareness of risk and how to avoid it, 2015 also resulted in some negative outcomes. Unfortunately, for many, cyber-security has become linked to terrorism. Today, attacking and defending internal and external networks, such as the Internet, are subjects of considerable interest to various illegal groups," continues Kollberg.

2015 predictions

A year ago, the director of Kaspersky Lab's GReAT team, Costin Raiu, predicted a few trends for advanced, persistent cyber-threats in 2015. As the year was to show, his forecast was accurate:

- The evolution of malware techniques. In 2015, GReAT discovered previously unseen methods used by the Equation group, whose malware can modify the firmware of hard drives, and by Duqu 2.0, whose infections make no changes to the disk or system settings, leaving almost no traces in the system. These two cyber-espionage campaigns surpassed anything known to date in terms of complexity and the sophistication of techniques.

- The merger of cybercrime and advanced persistent threats. In 2015 the Carbanak cyber-criminal gang stole up to $1 billion from financial institutions worldwide using targeted attack methods.

- New methods of data exfiltration. Satellite Turla was found to use satellite communications to manage its command-and-control traffic.

- An APT arms race. French-"speaking" Animal Farm and Arabic-"speaking" Desert Falcons were two of many cyber-threats seen during the year.

- Targeting executives through hotel networks. This prediction was later modified to include any venue where a high-profile target could be targeted outside the protected corporate perimeter. For example, the Duqu 2.0 malware infections were linked to the P5+1 events and venues for high-level meetings between world leaders.

- Precise attacks merged with mass surveillance. Animal Farm's targeted cyber-attacks merged with DDoS attacks from the same threat actor, which is rare for advanced targeted cyber-campaigns.

- Threat actors add mobile attacks to their arsenal. Desert Falcons targeted Android users.

APT wars

What Kaspersky Lab's GReAT didn't anticipate was that in 2015 we'd see wars between APTs. In 2015, Kaspersky Lab recorded a rare and unusual example of one cybercriminal attacking another. In 2014, Hellsing, a small and technically unremarkable cyber-espionage group targeting mostly government and diplomatic organisations in Asia, was subjected to a spear-phishing attack by another threat actor, Naikon, and decided to strike back. Kaspersky Lab believes that this could mark the emergence of a new trend in criminal cyber-activity: the APT wars.

In total, Kaspersky Lab's Global Research and Analysis Team issued 14 public reports on APT attacks in 2015: Duqu 2.0, Darkhotel - part 2, Naikon, MsnMM Campaigns, Satellite Turla, Wild Neutron, Equation, Blue Termite, Hellsing, Carbanak, Desert Falcons, Animal Farm, Spring Dragon and Sofacy. These advanced actors "speak" different languages: traces hidden in the APTs were in Russian, Chinese, English, Arabic, Korean, and French. They targeted financial institutions, government, military and diplomatic organisations, telecommunications companies and energy firms, political activists and leaders, mass media, private business and more. The attacks were all global.