BIZCOMMUNITY

Are we prepared for 2019's cyber security challenges?

By Grant Hamilton

15 Jan 2019

2018 saw significant security trends developing, which show how the cyber landscape is evolving.

Source: pixabay.com

"Technology is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other", wrote novelist and scientist C. P. Snow in the *New York Times* in 1971. It still rings true today. Every new tool or technology we use introduces new vulnerabilities, giving cybercriminals opportunities for financial gain, and politically-motivated groups new opportunities to spy on individuals or cause disruption and damage to opponents.

2018 saw several large-scale cyber-incidents hitting headlines, such as the breaches affecting British Airways, Ticketmaster, Cathay Pacific and others. But there were other significant security trends developing, which show how the cyber landscape is evolving, and indicate the types of threats and attacks we can expect to see in 2019.

So what are these emerging cyber-trends?

Digging for digital gold

Crypto-miners dominated the malware landscape throughout 2018, replacing ransomware as the most popular method for cyber-criminals to earn illicit cash. Forty-two percent of organisations globally were hit by cryptomining malware last year – more than twice the 20.5% of firms affected in the second half of 2017. Its popularity is no surprise, as crypto-miners are easy to distribute, hard to trace, and can operate undetected for months, generating ongoing revenues for criminals at much lower risk compared to ransomware.

As they have proven to be highly effective, we expect to see crypto-miners continuing to dig deep into organisations' networks during 2019. Mining malware will also be refined to target scalable cloud platforms and unprotected mobile estates, tapping into the massive computing resources these offer to further grow and maximise illicit earnings.

Mobile – moving targets

Despite fleets of company-issued and BYOD mobile devices making up a large part of organisations' attack surface, mobile security continues to be overlooked. This is despite serious threats aimed at mobile estates. Throughout 2018, Lokibot – the banking Trojan aimed at Android devices which steals information and grants privileges to download further malware was in the top three mobile malware. September 2018 also saw a near 400% rise in crypto-mining malware attacks against iPhones and iOS devices.

As a result, mobile malware is expected to increase over the next year, and to see all-in-one mobile malware variants that combine banking Trojans, key-loggers and ransomware that give numerous options for attackers to profit from infecting devices. We'll also continue to discover flaws in mobile operating systems that offer attackers an easy way to attack unprotected devices – such as the Android 'man-in-the-disk' flaw which enabled apps to be targeted from a device's external storage.

Cloud concerns

The scalability and agility of the cloud allow organisations to do things they could only imagine with their traditional data centres. But the level of understanding about securing the cloud remains low.

In November 2018, Check Point revealed vulnerabilities in the cloud platforms behind the world's most popular consumer and business drones that would allow attackers to steal flight records and photos, live locations, and account information such as user profile information and credit card details – without users being aware of any intrusion.

Although the vulnerability was closed before it could be exploited, the case highlights how security is often an afterthought with cloud deployments, leaving highly sensitive data and applications vulnerable to exploitation by hackers.

We can expect to see cloud account takeovers and hacking attempts increasing over the next year, as more enterprises use SaaS applications and cloud-based email (including Office 365, GSuite and OneDrive), so businesses will need to prevent common attacks such as phishing attempts.

Rise of machine learning – for good and bad

Machine learning and AI techniques have dramatically accelerated the identification of new threats and responses to them over the past 18 months, helping to nullify new threats before they can spread widely. However, as the technology becomes increasingly commoditised, it will become more widely available – which means that cybercriminals will also start to take advantage of machine learning techniques to help them probe networks, find vulnerabilities and develop more evasive malware that has a better chance of avoiding detection.

Nation state concerns

In recent years, governments' concerns have grown over cyber threats targeting critical infrastructure like power grids, and the relative vulnerability of these essential networks. Many countries have formed bodies to oversee their national cybersecurity in preparation for such attacks.

Meanwhile, we have also seen nation state attacks aimed at domestic targets, such as the Iranian state-sponsored mobile surveillance operation against its own citizens, dubbed 'Domestic Kitten'. In place since 2016, the campaign enticed targets to download fake, decoy mobile apps loaded with spyware that collected sensitive information about hundreds of targeted citizens.

While we have yet to see non-state actors attacking critical infrastructure to inflict mass damage, nation states will most certainly continue and increase their use of cyber–warfare techniques. And cyber espionage and citizens' data privacy will become an even hotter topic of contention, especially due to such data being proven to impact on voting patterns and election outcomes.

Nano security on a global scale

While more insecure IoT devices are being built into the fabric of enterprise networks, organisations have failed to use better security practices to protect their networks and devices. IoT devices and their connections to networks and clouds are still a weak link in security.

Over the next two years, physical infrastructures will increasingly disappear into the cloud and scale up or down whenever needed. These will connect to physical devices, such as a smartphone, an autonomous vehicle, an IoT sensor, a medical device, or anything else with an internet connection. Protecting this interconnected world of devices, to stop new threats hiding in the cloud and spreading across devices undetected, will be critical.

We expect to see a new generation of protection using nano security agents - micro-scale plugins that can work with any device or operating system in any enterprise environment, from security cameras to IoT devices, to micro-services in the cloud, in hardwareless environments. These nano agents will be able to control every attribute that goes to and from the device from the cloud, and will connect to one global smart, AI-driven security system that can steer our security, making the right decisions in real time.

While innovation will continue to bring new opportunities to accelerate and enable business, cybercriminals will also seek to take advantage of those innovations for their own gain. To keep pace, organisations must be proactive, and leave no element of their attack surface unprotected or unmonitored – or risk becoming the next victim of increasingly sophisticated, highly targeted mega-attacks.

ABOUT THE AUTHOR

Grant Hamilton is country manager at Check Point South Africa