BIZCOMMUNITY

A new phase of cyber warfare has begun

By Simon McCullough

7 Aug 2019

Hackers acting on behalf of nation-state powers are no longer just out to disrupt critical infrastructures - they're also actively seeking trade secrets. New battle lines have been drawn across the world, and organisations need to tool up accordingly.

Simon McCollough is major channel account manager, F5 Networks

The recently released Verizon Data Breach Investigations Report (VDBIR) is an eye-catching case in point, noting a sharp uptick in nation-state attacks, rising from 12% of all analysed breaches to 23% in the past year. Twenty-five percent of breaches are currently influenced by cyber espionage, rising from 13%.

Hackers' goals

Further research compiled by the Swedish Security and Defence Industry Association (SOFF) echoes VDBIR's 25% espionage figure but also breaks the issue down by sector.

Remarkably, 94% of all attacks currently aimed at the manufacturing industry are motivated by espionage, usually with the intent to steal trade secrets or sabotage plants.

As an example – and a mere tip of the iceberg – Norwegian software firm Visma recently revealed that it had been targeted by hackers from the Chinese Ministry of State Security attempting to steal trade secrets.

In another notable instance, Boeing revealed that, between 2009 and 2014, Chinese hackers were able to gain network access to steal 65 gigabytes of data on military aircrafts. The nature and style of the attack come as no surprise. Manufacturing – along with public administration and educational services – tend to aggregate large volumes of attractive, highly sensitive data.

SOFF predicts that security researchers now spend 90% of their time looking into espionage-based targeted attacks. Ten years ago, they would spend similar amounts of time focusing on criminal campaigns.

The financial impact associated with data breaches, espionage-based or not, are too consequential for organisations to ignore. SOFF also adds that it is worth understanding how 90% of the impacts caused by a cyberattack tend to be hidden (beyond the obvious outlay for mitigation, customer notification or legal action).

The techniques

In the last year alone, recent Infosec analysis shows an explosion of underground hacker marketplaces on the dark web. There are at least 300 hacker communities in existence, some with as many as half a million registered users, all packed to the gills with resources and disruptive tips.

In another alarming trend, hackers acting on behalf of nation-states are also increasingly carrying out zero-day attacks. Cybersecurity Ventures research predicts there will be one zero-day attack a day by 2021.

Unfortunately, a zero-day attack is the first instance of a vulnerability being exploited so, if adequate defences aren't in place, organisations will have to a messy clean-up operation on their hands.

Another favoured technique is phishing, whereby attackers trick employees into providing their credentials and log-in details via fraudulent emails and communication. A recent analysis from PhishMe found that phishing emails are responsible for 91% of cyber-attacks – a concerning trend, but one that could soon be reversed with adequate training mechanisms.

How to stay one step ahead

The number of state-sponsored attacks is only going to rise with the imminent impacts of trends like 5G and IoT. New attack surfaces are always expanding for switched on cybercriminals.

As you'd expect, a range of new technologies are emerging to aid the fightback. For example, AI solutions are being developed that can analyse all traffic in real-time to spot unusual behaviours and anomalies previously out of sight. These types of AI are explicitly designed to understand how traffic is meant to function, automatically flagging problems as they occur.

Whatever the technology mix looks like, both now and into the future, there will always be a need to apply security at every level and on every surface: endpoint, application, and infrastructure.

Applications require consistent, intelligent and adaptable policies wherever they reside (on-premises, in the cloud or in a multi-cloud environment). Protecting perimeters is no longer enough.

Modern authentication techniques, such as the "principle of least privilege" and two-factor authentication, should become the norm.

As ever, organisations should constantly review and update security settings and tools, running regular penetration tests to monitor and improve staff behaviour. Organisations also need to control wayward BYOD activity and ensure all staff are equipped with the tools they need to do their jobs safely. It is a dangerous world out there.

Pre-emption, prevention and continuous education are the ways ahead.

ABOUT SIMON MCCULLOUGH

Major Channel Account Manager at F5 Networks

- Try to tackle cybersecurity during #RWC2019 - 20 Sep 2019
- Stay safe from cybercrime with what's left of 2019 - 30 Aug 2019
- Multi-cloud's new multiculturism - 21 Aug 2019
- A new phase of cyber warfare has begun - 7 Aug 2019
- The ABC of DevOps - 27 Jun 2019

View my profile and articles...