BIZCOMMUNITY

The business of organised cybercrime

By Simon McCullough

6 Feb 2019

Team leader, network administrator, data miner, money specialist. These are just some of the roles making a difference at today's enterprises. The same is also true for sophisticated cybergangs.

Many still wrongly believe that the dark web is exclusively inhabited by hoodie-clad teenagers and legions of disaffected disruptors. The truth is, the average hacker is just a cog in a complex ecosystem more akin to that of a corporate enterprise than you think. The only difference is the endgame, which is usually to cause reputational or financial damage to governments, businesses and consumers.

Source: pixabay.com

There is no way around it; cybercrime is now run like an industry, with multiple levels of deceit shielding those at the very top from capture. Therefore, it’s more important than ever for businesses to re-evaluate cybercriminal perceptions and ensure effective protective measures are in place.

Current perceptions surrounding cybergangs

Cybergangs as a collective are often structured like legitimate businesses, including partner networks, resellers and vendors. Some have even set up call centres to field interactions with ransomware victims.

Meanwhile, entry-level hackers across the world are embarking on career development journeys of sorts, enjoying opportunities to learn and develop skills. This includes the ability to write their own tools or enhance the capabilities of others.

In many ways, it is a similar path to that of an intern. They often become part of sophisticated groups or operations once their abilities reach a certain level. Indeed, a large proportion of hackers are relatively new entrants to the cybercrime game and still use low-level tools to wreak havoc. This breed of cybercriminal isn't always widely feared by big corporations. They should be.

How cybergangs are using technology to work smarter and cheaper

Cybergangs often work remotely across widely dispersed geographies, which makes them tricky to detect and deal with. The nature of these structures also means that cyber attacks are becoming more automated, rapid and cost-effective. The costs and risks are further reduced when factoring in the fluidity and inherent anonymity of cryptocurrencies and the dark web.

The industry has become so robust that hackers can even source work on each link in an attack chain at an affordable rate. Each link is anonymous to other threat actors in the chain to vastly reduce the risk of detection.

IoT vulnerabilities on the rise

According to IHS Markit, there will be 125 billion IoT devices on the planet by 2030.

With so much hype surrounding the idea of constant and pervasive connectivity, individuals and businesses are often complacent when it comes to ensuring all devices are secure.

Significantly, it is easier to compromise an IoT device that is exposed to the public internet and protected with known vendor default credentials than it is to trick an individual into clicking on a link in a phishing email.

Using AI can make your business fraud-free and safer

Rob Lith 4 Feb 2019

Consequently, it is crucial for organisations to have an IoT strategy in place that encompasses the monitoring and identification of traffic patterns for all connected devices. Visibility is essential to understand network behaviour and any potential suspicious activities that may occur on it.

Why cybersecurity mindsets must change

IT teams globally have been lecturing staff for years on the importance of creating different passwords. Overall, the message is not resonating enough.

To combat the issue, businesses need to consider alternative tactics such as password manager applications, as well as

ensuring continuous security training is available and compulsory for all staff.

It is worth noting that the most commonly attacked credentials are the vendor defaults for some of the most commonly used applications in enterprise environments. Simply having a basic system hardening policy that ensures vendor default credentials are disabled or changed before the system goes live will prevent this common issue from becoming a painful breach. System hardening is a requirement in every best practice security framework or compliance requirement.

#DataPrivacyDay: 6 online privacy tips for everyone

28 Jan 2019

Ultimately, someone with responsibility for compliance, audit, or security should be continually reviewing access to all systems. Commonly, security teams will only focus on systems within the scope of some compliance or regulatory obligation. This can lead to failure to review seemingly innocuous systems that can occasionally result in major breaches.

In addition to continual access reviews, monitoring should be in place to detect access attacks. Brute force attacks can not only lead to a breach, but they can also result in performance impacts on the targeted system or lock customers out of their accounts. As a result, there are significant financial incentives for organisations to equip themselves with appropriate monitoring procedures.

Cybergangs use many different methods to wreak havoc, making it increasingly difficult to identify attacks in a timely manner. Businesses are often ignorant about the size of attacks, the scope of what has been affected, and the scale of the operation behind them. You are operating in the dark without doing the utmost to know your enemy. Failing to do so will continue to put information, staff and customers at risk by allowing cybergangs to operate in the shadows.

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...