What can we learn from Covid-19 cyber attacks?

Throughout the pandemic, cyber threat actors have not let a single opportunity slip by. They have preyed on fear and concern around Covid-19 with phishing attacks while also capitalising on security flaws within the remote workforce. And that, in turn, has had a significant impact on security professionals' roles - a recent survey from $(ISC)^2$ found that 81% of respondents' job functions had changed during the pandemic.

Photo by ThisIsEngineering© from Pexels

The good news? There are plenty of lessons to be learned from the attacks that have been executed, ones that will shape the direction that organisations take regarding cybersecurity for years to come.

Cyber criminals' benefit from panic and emotional distress

Social engineering attacks remain the fastest way to exploit a target – they can be quickly spun up and also have the highest rate of return as compared to other techniques. Even during normal times, these cyberattacks prey on vulnerabilities and panic, so it is no surprise that the pandemic has only underscored the value and effectiveness of this method for cybercriminals who hope to capitalise on the situation.

Many of the Covid-19 phishing campaigns that security teams have seen over the past few months have targeted hospitals, medical equipment manufacturers, and health insurance companies. Where many see panic in the shortage of medical equipment and supplies, attackers see ideal opportunities to capitalise on fear and misinformation.

A major theme among these campaigns has been the creation of texts and emails that look like they were sent by organisations like the Centres for Disease Control (CDC) or the World Health Organisation (WHO). By sending communication that appears to be coming from organisations as familiar as these two, threat actors know that recipients are more likely to open the message and then click on a link or download an attachment.

This displays a perennial problem with security, regardless of how many measures you take, the human psyche remains the weakest link. Where humans face emotional, physical, and financial distress, they can become targets for attackers.

Tried and true cyberattack methods come out on top

The majority of attacks during the pandemic have been delivered via email, meaning mass spam campaigns have been taking place. This is backed by the fact that, in March alone, the FortiGuard Labs team saw a 131% increase in viruses, which should come as no surprise considering email attachments are the most common vendors of such malicious content.

Some of these attacks have been targeted, some are part of a “spray and pray” tactic. Others fall under the category of distributed denial-of-service (DDoS). And the sheer volume of remote work has also played a significant role in how effectively these attacks are executed. Today, almost everyone is connected to the Internet for the bulk of the day.

It's their primary connection to the outside world, whether it be for work or fun. Unfortunately, this activity often happens on the least secured networks or devices, rather than in far more secured corporate environments, offering attackers an effective springboard to access critical information.

While email is being exploited to deliver malware such as viruses or ransomware, that is because bad actors know that businesses are more likely to pay a ransom if it cuts off access to the critical infrastructure and information their users and customers need to ensure business continuity.

Due diligence is more important than ever

Interestingly, these attack methods themselves aren't new. In fact, many of the techniques used in cyberattacks during the pandemic have not been innovative or novel – they're all the same tricks bad actors have relied on for years.

This is a matter of practicality, as attackers are unlikely to change tactics until they see a diminishing rate of return. And while systems behind the corporate firewall may have been hardened, many of the devices and networks being used by remote workers have not. Bad actors are also aware that people's cyber hygiene may be worse than usual – a by-product of fear and anxiety. This makes it even easier to execute the same attacks they've always relied on.