THE CYBERSECURITY NEEDED TO FIGHT STATE-SPONSORED ATTACKERS

Even as COVID-19-inspired remote working has brought headaches for cybersecurity professionals, they are having to face up to new threats

WRITTEN BY:
WILLIAM SMITH

A recent spate of state-sponsored security breaches has put even more focus on the need for cybersecurity, but in the face of such sophisticated attackers, what can ordinary businesses do?

According to Paul Baird, Chief Technology Security Officer, UK, Qualys, "State-sponsored attacks have a single and specific end goal of breaching a target's network and they often won't stop until they succeed, regardless of what defences are in place. This is vastly different compared to your 'everyday' hacker who is less fussy and will exploit any weak spot if it presents a money-making opportunity. In an effort to combat this, companies should consider their security strategies in great depth, although this is often easier said than done." Of course, the ideal response is hampered by the reality of budgets, so measures must be chosen intelligently. "CISOs would love to utilise every technology possible to ensure protection from the perimeter, through to each endpoint and everything in between," says Baird. "Sadly, company resources are

“STATE-SPONSORED ATTACKS HAVE A SINGLE AND SPECIFIC END GOAL OF BREACHING A TARGET’S NETWORK”

PAUL BAIRD
CHIEF TECHNOLOGY SECURITY OFFICER, UK,
QUALYS

Technology.
technologymagazine.com
TOP 100 Women
Brought to you in association with:
IBM
2021

"ATTACKERS WILL ALWAYS DEVELOP THEIR METHODS TO FIT THE TARGET"

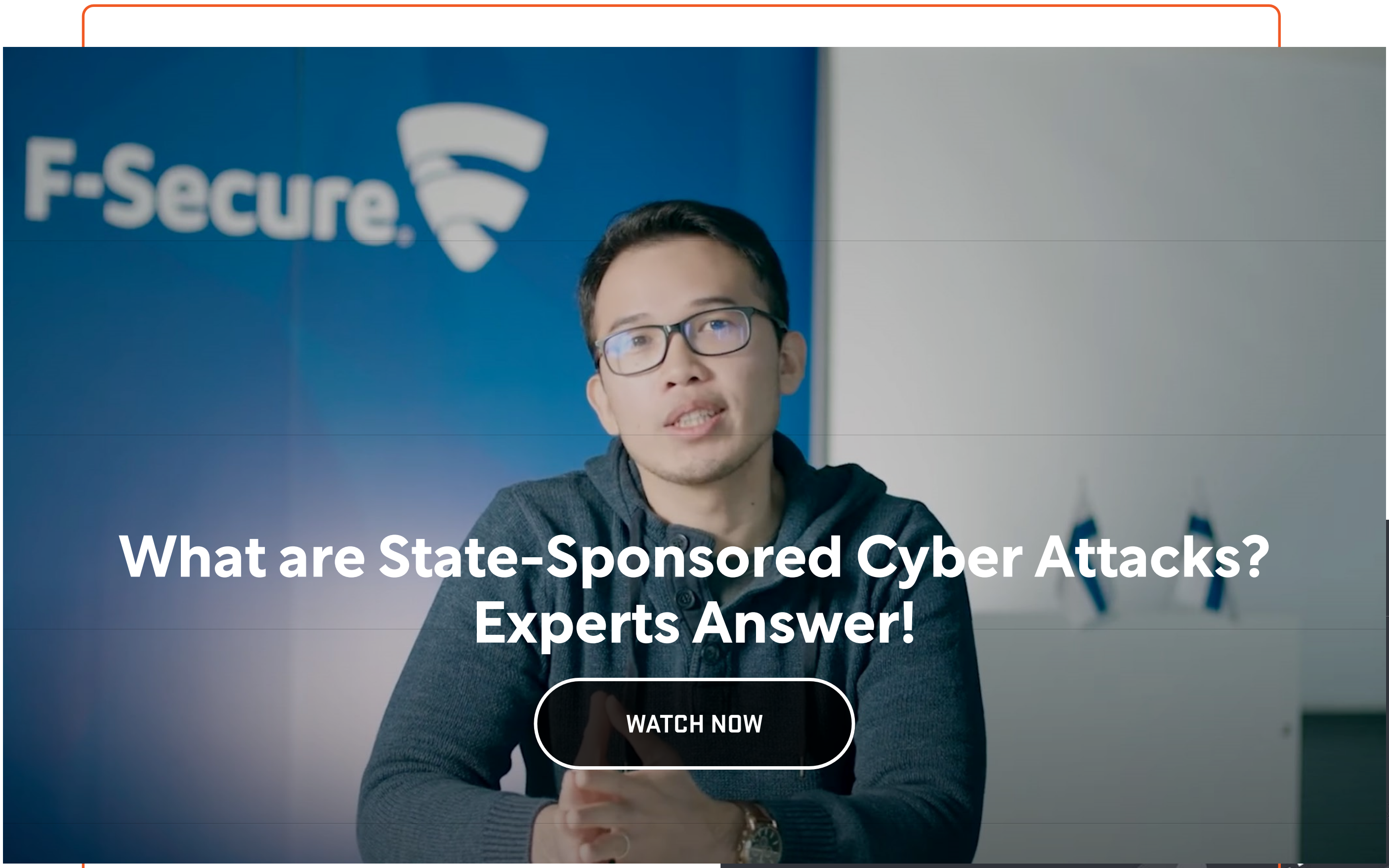
DAVID WARBURTON
PRINCIPAL THREAT RESEARCH EVANGELIST, F5

finite and hard choices have to be made as to which areas to defend."

With such attackers able to rapidly evolve their methods, companies need to adapt their own defences at the same speed, as David Warburton, Principal Threat Research Evangelist, F5, explains: "Attackers will always develop their methods to fit the target. That said, one concept that would make a massive difference for companies targeted for state-sponsored attacks, is the idea of 'shifting security left.' Shifting security left refers to the idea of introducing security controls closer to the beginning of the software development process. It is no new concept, and one many understand at a top level. But the public discussion focuses too much on tools for code scanning and automated patching. Legacy tools such as web application firewall (WAF) are often ignored and perhaps seen as outdated now, but in fact, they still have their uses when adapted for the function. Combatting advanced nation-state attacks requires a multi-layered approach."

It's not just about technology, but also approach. "Ensuring organisations know who is accessing what data and that systems are patched and monitored, are just some of the key processes that are sometimes not followed," says Manoj Bhatt, Head of Cybersecurity and Advisory at Telstra Purple. "This can leave organisations vulnerable to basic security attacks. Technical security controls are a great start; however, security awareness and cultural investment is key."

Keeping up with the pace of such threats is an inhuman task. Luckily, AI is there to pick up the slack. One such example is "AI's automation of mundane security tasks such as vulnerability management, antivirus, identity management, and mail hygiene," says Warburton. "Google did this to good effect by employing AI to block an additional 100 million spam messages per day. Another example of AI's use is its ability to analyse high volumes of signals to identify and block seemingly legitimate transactions generated by bots. This is something humans could never achieve without a considerable investment in time and money." AI's capacity to trawl through vast reserves of data means it can also spot patterns outside the reach of humans. "AI and Machine Learning can help in the fight against cyber-crime, by learning



to recognise certain patterns based on past data analysis and reduce incident response times," says Marcin Hejka, Co-Founder and General Partner of OTB Ventures. "Traditional cyber security prevention techniques are based on using signatures to identify threats. This works well for previously known threats but is not effective for threats that have not been discovered yet."

It's not a question of AI totally replacing the human role in cybersecurity, however. "Ultimately, AI is programmable logic that looks for anomalies and behaviours," says Baird. "Once correlated, it can show an attack vector faster than a human ever could. However, AI will never replace humans entirely as SOC analysts remain the cornerstone of a defence strategy. AI can catch 90% of potential issues, but human intervention is required to work towards achieving 100% coverage." Furthermore,

"TECHNICAL SECURITY CONTROLS ARE A GREAT START; HOWEVER, SECURITY AWARENESS AND CULTURAL INVESTMENT IS KEY"

MANOJ BHATT
HEAD OF CYBERSECURITY AND ADVISORY, TELSTRA PURPLE

Bhatt warns about putting the AI cart before the horse. "Many organisations try and implement artificial intelligence as a technology driver and this can lead to failures," says Bhatt. "Planning and understanding the processes that artificial intelligence systems need to be embedded into a business is key. A growing number of systems are utilising artificial intelligence within their operations and this is predicted to increase."

Going forwards, the cybersecurity threats facing businesses are only set to multiply. "Threat trends are likely to continue to target the remote workforce as many employees have become less vigilant outside of the professional office environment," says Baird. "CISOs can't rely solely on technology to guard the perimeter, and so continued investment in staff training is vital to uphold standard security practices." Overcoming such challenges will require flexibility. "Covering the basics will become ever more challenging as the way that we do business will continue to evolve and become more flexible," says Bhatt. "Businesses want the flexibility to pick and choose technologies, along with changing the way that business is carried out from anywhere in the world. These demands will mean that the security team will need to ensure that it is staying close to the business to embed security by design principles along with supporting and enabling the innovation of businesses."

Businesses' cybersecurity efforts will

“AI AND MACHINE LEARNING CAN HELP IN THE FIGHT AGAINST CYBER-CRIME, BY LEARNING TO RECOGNIZE CERTAIN PATTERNS BASED ON PAST DATA ANALYSIS”

MARCIN HEJKA
CO-FOUNDER AND GENERAL PARTNER,
OTB VENTURES

also have to be retooled for the post-COVID-19 landscape. “As remote work and online collaboration are becoming a norm in the post-COVID world we have seen accelerated migration of companies to the cloud, which creates new vectors of potential attacks, for instance through vulnerable cloud applications, unauthorized remote access, unsecured networks or even weak passwords. The dynamic growth of IoT (Internet of Things) and the growing number of connected devices and sensors will also create new potential vulnerabilities that will certainly be explored by hackers. We may see the rise of automotive hacking as cars are becoming connected devices. Gaining control of vehicles by hackers may become a serious threat and autonomous vehicles will need to apply strict security measures.”

With emerging threats stemming from geopolitical strife and new ways of working, cybersecurity teams will need to draw on all the tools available to them, from AI to new strategies and approaches.

esri® | THE SCIENCE OF WHERE®

UNLOCKING THE POWER OF SPATIAL ANALYSIS

WRITTEN BY: WILLIAM SMITH | PRODUCED BY: TOM VENTURO