UNKNOWN TERRITORY

Carolyn Crandall *explains what CISOs can do to stay ahead of the game when it comes to cyber security*

Cybersecurity has traditionally been a discipline of prevention. Like sentries charged with defending their castle, a chief information security officer (CISO) will deploy the best possible defensive measures to protect against cyber attackers. The castle has its high walls and moats and the network has defensive barriers such as firewalls, anti-virus and endpoint detection and response (EDR) as first lines of defence to secure their environment.

Attackers, however, are very persistent and patient. The odds are that eventually they will find a way through. They know that if they enter slowly and stealthily, they can find ways to bypass perimeter security controls and keep the CISO and security team unaware that an intrusion has occurred until it is just too late.

While defenders have long understood that it is a matter of 'if, not when' a security breach will occur, in recent years the scales have tipped even further against them. Threat actors are becoming increasingly bold and aggressive, using automated tools to elevate both the volume and sophistication of their attacks.

It is no longer a viable strategy to build castle walls and hope these defences will be enough to repel the next attack when it inevitably comes. CISOs know they must reinforce their defences with alternative measures that can tip the odds back in their favour by discovering and derailing their adversaries' attacks. Relying purely on defensive techniques that start after an exploit has begun is no longer enough if CISOs want to outmanoeuvre their adversary.

Breaches have not only become more common, but also more costly. The FBI recently reported cyberattack complaints to their Cyber Division are up to as many as 4,000 a day representing a 400 percent increase from what they were seeing pre-Coronavirus. Interpol also cited seeing an alarming rate of cyberattacks targeting major corporations, governments and critical infrastructure.

The cost for losses increased in 2019 by over 30 percent over the same period, going from $229,000 to $369,000. While defenders had been losing ground to the attackers in recent years, the COVID-19 pandemic merely accelerated the process. Lockdown and social distancing measures forced most businesses around the world to transition rapidly to widespread remote working, opening up fresh opportunities for cybercriminals to enter the network.

Only a tiny minority of firms were prepared for the switch. In the UK, the ONS found that only 5.2 percent of the workforce worked from home regularly last year. In 2020, this figure skyrocketed to 49 percent.

Many organisations have found themselves in entirely unknown territory. Operational pressures meant focussing on enabling employees to get up and running quickly and security teams did what they could to protect the organisation. However, there's little that they could do to consistently and reliably check whether employees' machines had become infected with malware.

Threat actors were quick to capitalise. Phishing campaigns with COVID-related themes spiked by over 30,000 per day according to Microsoft, and attackers looked for vulnerabilities on insecure devices to exploit or to establish backdoors.

Unpatched Virtual Private Networks (VPNs) also provided a point of entry. In August, for example, cybercriminals posted more than 900 usernames and passwords for the Pulse Secure VPN service on Russian-language Dark Web forums. The credentials, which also included SSH keys and IP addresses for Pulse Secure servers, may have been the result of an exploit known as CVE-2019-11510. Although the provider patched the vulnerability last year, many firms had not updated their software. The cybercriminals had evidently been harvesting data and biding their time. The pandemic provided the perfect opportunity to exploit the stolen credentials and capitalise on the challenges that traditional security tools have in detecting the unauthorised use of these credentials.

CYBER ATTACKS HAVE INCREASED 400 PERCENT COMPARED WITH PRE-CORONAVIRUS LEVELS

VPNs are a particularly popular target for threat actors. Once they have acquired log-in details, it is a relatively easy step to navigate upstream and access the network. In regular times, an unexpected VPN connection from a user might trigger an immediate red flag. But with the entire workforce logging in remotely, it is much easier for an imposter to slip through undetected, particularly if the company has not had time to realign its defences. Even measures such as behavioural analysis will need recalibration as the modelling for anomalous behaviour may no longer fit.

Lockdown has forced businesses to transition rapidly to widespread remote working

In addition to switching tactics to exploit the COVID crisis, that latest escalation uses advanced persistent threat (APT)-style tactics. This switch does not merely amount to an increase in zero-day malware exploits, but a long-term approach in which attackers focus on going 'low and slow'. Instead of immediately exfiltrating as much data as possible or detonating a ransomware attack to incapacitate their target, attackers will maximise dwell time and lateral movement, remaining undetected to achieve their aims.

As long as they keep up to date with the latest threat intel, endpoint detection and response (EDR) solutions can generally alert security teams on the threat signature of most malware so they can shut it down. But other malicious activities, such as credential theft, port probing and attempts to enumerate Active Directory to acquire user data are much harder to detect with standard tools. By successfully exploiting a remote machine, attackers can focus on compromising that device and then slowly hunting through it for prizes such as active admin credentials. From here, they can escalate to achieve broader access privileges. They use these to fingerprint other endpoints in the network and scope out how to move laterally without being noticed.

Research by The Ponemon Institute estimates that the average attacker achieved a dwell time of 206 days before detection in 2019, and we anticipate this number is likely to increase in 2020. Some particularly forward-thinking attackers appear to be content with seeding systems for attacks to be executed months down the line when the user returns to their office, enabling them to maximise their reach and impact. With threat actors intent on playing the long game to launch their attacks, the more subtle signs of intrusion often bypass traditional security defences. Attackers know all too well that only one in five alerts are considered reliable and that typically only 4 percent of malware alerts ever get investigated. This leaves ample opportunity for attack advancement with limited concern for being stopped.

There is no such thing as a silver bullet in cybersecurity. Threat actors have a vast array of tools, techniques, and attack vectors at their disposal, and no single solution or strategy can catch all of them. Organisations should employ defence in depth for their network defences and at the same time, fine-tune their existing security controls to identify the subtler signs of an APT-style attack. These should include prevention and detection controls designed for diverting advanced tactics of discovery, lateral movement and privilege escalation.

Whatever new tactics they use in their initial attack, threat actors will still need to follow certain tried and tested methods to execute their attack. To stay ahead of the game, CISOs will want to focus on these steps, ensuring they have the proper controls and tools in place for each element. Following the Mitre ATT&CK matrix

can be an advantageous way of mapping out threat tactics and defences. The matrix provides a knowledge base of adversarial attack techniques and defensive options, helping CISOs to identify gaps in their strategies.

The more layers there are to defences, the harder it is for the attacker. Defenders can up the ante considerably using additional layers to reduce gaps and quickly detect lateral movement in their network.

Most organisations will have endpoint protection to spot and block known attacks and their signatures. A good many are also adopting EDR tools to monitor for behavioural anomalies. However, these tools leave gaps when it comes to early detection of in-network threats and activities related to credential theft, discovery, lateral movement and data collection.

RELYING ON DEFENSIVE TECHNIQUES THAT START AFTER AN ATTACK HAS BEGUN IS NOT ENOUGH

This gap is where the combination of deception and denial, AKA data concealment technologies, can help CISOs to regain the advantage over their adversaries.

By hiding real assets from an attacker's sight and creating deceptive network assets, it is possible to lead the threat actor away from the most valuable assets right from the outset. Most attackers begin with automated searches for their prize. Rather than hitting an obvious defensive blockade, the attacker will seemingly locate the files they are after. However, the environment façade will have led the unsuspecting intruder into a false environment. Not only are the real assets protected – such as Active Directory objects, files and folders – the defender has gained valuable early alerts and the ability to control the attacker's path away from genuine prized assets and straight into deception decoys for observation.

Crucially, the decoy environment, and the assets it contains, must be well crafted. Files should not only appear genuine to an initial scan, but should also withstand closer scrutiny and attract attacker interaction. If the decoy assets give out all the right signals, the attacker will continue to explore the deception environment – none the wiser that they are heading down a blind alley.

In addition to an instant alarm for the CISO and their team, the decoy environment can send an immediate alert upon any interaction with the files or folders. It works for any APT-style tactics the threat actor chooses to use, giving the security team time to close in and shut down the attack before it can even begin.

Deception also offers a powerful and unrivalled opportunity to study the attackers and learn their tactics, techniques and procedures (TTPs). In normal circumstances, security teams must move swiftly to shut down an attack to prevent data exfiltration or damage to the network. In the deception environment, the security team can safely contain the attacker and study it like a dangerous insect in a glass jar.

By gaining an insight into attackers' TTPs, security teams can harden their defences, preventing repeat attempts by intruders or any other attacker using a similar approach. Deception and denial tools can also integrate with EDR, security information and event management (SIEM), security orchestration, automation and response (SOAR) and other tools, policies and procedures, to quickly convey threat data to the right people. It allows solutions that rely on signatures to receive updates immediately. Additionally, behavioural analytics models can adjust to improve the chances of identifying this type of activity as suspicious. Research has found organisations are 42 percent more likely to detect threats when deception capabilities are combined with EDR solutions.

By leveraging this invisible new layer within their defences, CISOs can lay a powerful diversion for stopping intruders in their tracks. CISOs and their teams are now on the front foot, ready to proactively close the attackers down before they can do any harm ●

Carolyn Crandall holds the roles of Chief Deception Officer and CMO at Attivo Networks. She is a high-impact technology executive with over 30 years of experience in building new markets and successful enterprise infrastructure companies.

Virtual Private Networks are a particularly popular target for threat actors