THE CYBER YEAR AHEAD

Jonathan Lee *reveals important security trends to be aware of in the coming months*

Picture credit: US Dept Defense

2022 has been yet another year of immense unpredictability. The expanding digital footprints of modern organisations have transformed the security landscape, both in shape and size. And unfortunately, the average enterprise has found itself ever more vulnerable to attack.

In today's environment, traditional cybersecurity controls have become increasingly obsolete, while hybrid work and cloud-based business models have introduced a series of new risks. At the same time, threat actors have continued to develop and deploy highly advanced attack methods – from ransomware to sophisticated digital supply chain attacks – exposing both skills shortages and technology gaps.

We've seen ubiquitous pieces of software become the subject of attacks, the uncovering of the Log4j vulnerability having caused mass concern. And the proliferation and commercial availability of cyber capabilities via ransomware-as-a-service markets has made disruptive cyber tools even more widely accessible to malicious actors. This is all before we mention the impact of the war in Ukraine. Indeed, the conflict has brought the threat of highly organised and sophisticated nation state-backed actors into ever sharper focus as Russia continues to lean heavily into digital warfare as a means of supporting its on-the-ground invasion.

In all spheres, security threats remain as severe as ever. And it seems there is no simple resolution in sight as threat actors continue to adapt their techniques and unlock new and sophisticated ways to take advantage of uncertain situations.

The threat landscape will undoubtedly continue to evolve in 2023. Here, we outline some key security trends to keep an eye on.

INTELLIGENT AND EVASIVE ATTACKS

Threat actors continue to expand their understanding of the security methods and technologies being deployed by enterprises and are adapting their techniques to find ways around them. We expect to see attacks becoming increasingly evasive and intelligent, focused on bypassing commonly used defences.

We're already seeing several methods such as HTML Smuggling and websites with previously benign reputations being used to evade existing layers of protection such as firewalls, secure web gateways, malware analysis including sandboxing, URL reputation and phishing detection tools. These methods will only expand and we'll see the layering of multiple detection evasion techniques moving forward. This will make the outdated 'detect and respond' defence that many organisations rely upon as not fit for purpose.

Russia's invasion of Ukraine has added immensely to the threat landscape

BASIC SECURITY FAILURES WILL CONTINUE

Unfortunately, much of the task is being made easier for adverse actors. The attack on Uber in September 2022, for example, reiterated that basic security failures are continuing to provide wide open doors for threat actors to simply step through. In this specific instance, the perpetrator was able to obtain administrative control over the company's IT systems and security tools by exploiting an exposed PowerShell script, which contained admin credentials for the firm's privileged access management (PAM) platform.

It's a core example of the fact that threat actors often don't need to use highly sophisticated tools or techniques to gain entry to an organisation's network. Sticking to the same tried-and-tested social engineering techniques such as phishing, they continue to find success.

Interestingly, the breach did reveal that Multi-Factor Authentication (MFA) push notifications are exploitable, with the industry now demanding that passwords should be replaced completely in favour of alternative security methods such as FIDO2 passkeys and hardware tokens. However, this is unlikely to happen anytime soon owing to the heavy lifting that would be required to implement such policies at scale.

EXPECT TO SEE AN INCREASE IN BROWSER-BASED ATTACKS

Almost all work is now carried out on the internet. Indeed, Google has reported that end users spend an average of 75 percent of their working day using a web browser. As a result, the web browser has become a ballooning attack surface, and the security industry is now working to respond.

Traditionally, browser-based security controls have been deployed either as a separate endpoint agent or at the network edge, using a firewall or secure web gateway. Now, however, vendors are looking at ways to add security controls directly inside the browser. Google and Microsoft, for example, are offering built-in controls inside Chrome and Edge to secure at a browser level rather than the network edge.

With that said, as browser attacks increase with threat actors exploiting new and old vulnerabilities and using novel attack methods like code obfuscation, file encryption and HTML Smuggling, the need for innovative security technologies is clear.

PURSUE VENDOR CONSOLIDATION WITH EXTREME CAUTION

Gartner recently highlighted that organisations are looking to consolidate their security toolkits, cutting down on the number of vendors they use to reduce complexity, cut costs, boost efficiency and, ultimately, improve security.

Many firms are particularly focussed on working with fewer vendors to satisfy their security needs in areas such as secure access service edge (SASE) and extended detection and response (XDR) to improve risk posture. And while any effort to reduce risk and shore up security defences should be encouraged, we equally advise that organisations proceed with caution in pursuing vendor consolidation. Through vendor consolidation, firms could be at risk of unknowingly removing best-of-breed solutions from their security stack, which may lead to overall weakened security postures.

END USERS SPEND AN AVERAGE OF 75 PERCENT OF THEIR WORKING DAY USING A WEB BROWSER

WEAPONISED FILES

Malicious payloads remain a prevalent feature in most attack sequences. Interestingly, these are increasingly taking the form of weaponised files that have been altered with the intent of infecting a target endpoint.

Specifically, there has been a striking uptick in the use of weaponised decoy documents during template injection attacks. A threat that initially emerged after Microsoft introduced the new Office Open XML File Format specification in 2007 (which made it possible to embed resources directly within a document), attackers today are now injecting URLs hosting malicious templates into XML files. As a result, they're able to execute a form of attack that uses legitimate software to perform nefarious actions – when weaponised documents are opened, they attempt to download and execute a malicious template.

What is particularly concerning about the use of weaponised documents and template injection attacks is the fact that they can appear to be completely benign to many security tools. Indeed, they leave no trace of malicious URLs or exploit markers, enabling them to bypass traditional detection-led solutions.

INTERNATIONAL TENSIONS

As mentioned, the Russian invasion of Ukraine has added a concerning dimension to the threat landscape, paving a path of greater activity among nation state-backed actors. Indeed, Russia has ramped up its use of cyberattacks in the international arena. And as relations between Putin and the west continue to sour, many believe that a full-scale global cyber war could begin to open up.

Time contributing editor and retired 16th Supreme Allied Commander at NATO, Admiral James Stavridis, recently voiced his views that NATO should: "strongly consider a response in the world of cyber, particularly going after Russian military capabilities aggressively" in the face of Russia's cyber escalation.

This, of course, could be an extremely dangerous new frontier for either side to begin exploring more actively. The consequences of a full-scale cyber war would no doubt be far reaching and devastating. However, given the current level of international tensions, it's not out of the question, with several nation-state-lead cyberattacks already making the headlines multiple times in recent years.

▶

POISON COOKIES

The role of the cookie is likely to come under greater scrutiny as awareness over the use and management of personal data continues to heighten. Yes, cookies can make our online lives easier by saving browsing information, keeping users signed into frequently used websites and remembering specific site-related preferences. However, there is growing concern that organisations could be collecting more information than many would typically be comfortable with.

Cyber concerns are naturally beginning to creep in as well. Indeed, it is becoming more feasible for threat actors to poison cookies, leading to session hijacking, the exposure of sensitive information, or even the full-scale takeover of an account that could have catastrophic consequences for user and organisation alike.

> EXPECT TO SEE ATTACKS BECOMING INCREASINGLY EVASIVE AND INTELLIGENT TO BYPASS DEFENCES

DEVELOPING DEFENCES

In 2022, the cybersecurity threat landscape has continued to evolve and diversify. And there is nothing to suggest that this momentum will slow in 2023 – a year that's anticipated to provide yet more turbulence. Given the uncertainty, it is important that organisations work quickly to build in the policies, technologies and capabilities required to protect themselves properly.

Unfortunately, many common security solutions have been rendered largely ineffective against current threats, let alone future ones. To be proactive in defending against increasingly frequent and advanced cyber threats, firms need to adopt innovative and progressive approaches to cybersecurity.

While continuous improvement will be key in continually adapting and responding to any changes, vital policies such as Zero Trust will go a long way in improving security postures.

Fortunately, this is a positive trend that we can expect to see in 2023, with many organisations already exploring Zero Trust as a policy in a more active manner. According to a survey from Verizon, presented in its 2022 Data Breach Investigations Report, 82 percent of respondents revealed that they had adopted or were considering adopting a Zero Trust approach to security.

What is the benefit of Zero Trust? Unlike outdated detect-and-respond solutions that weren't built for cloud operating models and browser-based operations that now dominate our working world, Zero Trust has been designed to address risks in the current environment.

It recognises trust in a network as a vulnerability, demanding that all traffic (be it emails, documents, websites, videos or other) should always be scrutinised and verified. Equally, it advocates the 'principle of least privilege' where users are only given access to the enterprise resources and applications they truly need to carry out their daily tasks effectively.

Together, these policies build resilience. Should attackers gain access to a network, they won't be able to move freely, mitigating or limiting the potential damages of any attack. Indeed, there are tools available to support organisations in achieving Zero Trust in the truest sense, with isolation technology being a prime example.

Isolation works by moving the browser execution process away from the desktop and into the cloud, rendering only safe web content on the endpoint. As a result, no active content from the internet – be it good or bad – is ever downloaded directly to the endpoint. Unlike other technologies, isolation isn't 'almost safe'. Rather, it can wholesale stop cyberattacks at source, 100 percent of the time by ensuring that attackers never have an opportunity to execute their payloads ●

Jonathan Lee is Senior Product Manager at Menlo Security.

As tension between Putin and the west increases, a full-scale global cyber war is a distinct possibility

Picture credit: Shutterstock