MOBILE MALWARE

Ash Patel *explains how mobile devices have become the enterprise's biggest attack surface*

The rise of remote work has increased the risks as users operate outside the bounds of office network controls

The rapid rise of the mobile device as the central business endpoint has disrupted many things in IT. Mobile-based work initiatives such as Bring Your own Device (BYoD) and remote work are now commonplace, but more fundamentally mobile devices are the new endpoint on which most business now happens – in or out of the office. We take meetings, we collaborate on documents, we store and send sensitive proprietary information and otherwise do business with our mobile devices. This has not only produced enormous value but opened up one of the largest attack surfaces that a modern business now possesses.

Many organisations have not yet recognised their growing fleet of devices as a potential point of compromise, continuing to rely on the security controls that characterised enterprise networks before mobile devices became a central endpoint.

In 2021, there were 7.1-billion mobile device users in the world and by 2025, that will likely reach 7.5-billion. The number of unique mobile internet users is now 5-billion and for 60 percent of the world's population, their mobile device is the way they access the internet. Similarly, 60 percent of endpoints that access enterprise assets are mobile devices.

It's not just that the sheer number of mobile devices is growing, our reliance on them is deepening too. Mobile internet traffic now accounts for almost 60 percent of global web traffic and shows no signs of stopping.

It's safe to say that the mobile endpoint is – for most people – the central endpoint in their lives. The portability and flexibility those devices allow, permit users to carry around a computer in their pocket.

For the same reasons, they've become the central business endpoint. In fact, Zimperium's 2023 Global Mobile Threat Report shows that 60 percent of the endpoints accessing enterprise assets are mobile devices. As technology has advanced, as the pace of business change has intensified and as all businesses – even SMEs – have globalised and even small businesses have started to regularly engage in international commerce, the agility that mobile devices allow has become something we all rely on.

It's been that quality which has allowed us to roll out remote work on a mass scale, and now looks to be a fixture of modern working. At the same time, BYoD has become a common feature of many businesses, allowing employees to work – and access enterprise resources – from their own devices.

This explosion in our reliance on mobile endpoints has often not been followed by a parallel accommodation in security. In fact, whatever benefits the new centrality of the mobile endpoint bring, they can also bring huge risks.

The mobile attack surface is large and because many enterprises have not yet evolved their security controls to accommodate their new reality, a large vulnerability gap has opened up.

This growing attack surface produces myriad vulnerabilities, from the devices themselves to the data transferred from them, to the apps inside of them to the basic infrastructure to which they're connected and the communication channels which can be exploited with phishing links.

One of the main characteristics of mobile devices is a blend of personal use with professional use. In this sense, vulnerabilities within employees' personal mobile devices can quickly become a risk for the business itself.

One of the fundamental qualities of the mobile device is its openness. Users can customise their own device by downloading apps. Perhaps unsurprisingly, this has become a key vector for exploitation. This takes multiple forms; many cyber criminals hide malware within apps that they smuggle onto legitimate app stores while others exploit existing vulnerabilities within.

Many vulnerabilities rise in the development of mobile applications. The high demand for new products and services has put an inordinate amount of pressure on the development process. As a result, many applications get released with vulnerabilities baked into them, waiting for attackers to exploit.

More risks emerge when we consider how often developers rely on open source code to build mobile applications. Not only are open source packages old, outdated or replete with vulnerabilities, but malicious actors have started to actively attempt to put their own malicious code into open source packages that could effectively send their vulnerabilities far and wide.

Compounding the problem is that many apps are necessary in many workplaces. Apps like Office 365 allow employees to collaborate and work with the full suite of Microsoft Office products. According to one report, however, It accounts for more than 72 percent of exploits.

There are also vulnerabilities to be found within the mobile device itself, and notably the operating systems on which they run. In 2022, 80 percent of Zero-days came from iOS, the iPhone's operating system. This could stem from the widespread availability of Apple's WebKit, which attackers can use to gain a foothold into iOS.

Meanwhile, in 2022, the Android operating system was responsible for a new record of 897 CVEs – an increase of 138 percent – up from 571 in 2021. Common vulnerabilities included code execution, system bypass and code or memory overflow attacks.

The fragmentation of the Android ecosystem between different platforms has also had a number of effects. Firstly, many attackers will now target specific Android platforms knowing that hardware and code implementation bugs exist in certain platforms but not in others. This has also made patching a more complex proposition and certain vendors may be slower to release patches while users might not know what they should download or where.

MOBILE INTERNET TRAFFIC NOW ACCOUNTS FOR ALMOST 60 PERCENT OF GLOBAL WEB TRAFFIC

The literal mobility of the mobile device is also a potential risk factor. As mobile devices go around in users' pockets, they can connect with all manner of insecure infrastructure which permit attacks against the device. Public wi-fi is a common cause for concern and often leaves mobile devices exposed to attack. The same goes for home networks, which are often not secured with the same vigilance that an office network might be. When devices connect to corporate assets over insecure infrastructure, those corporate assets can become exposed to the same risks that the mobile device is. The rise of remote work has clearly increased these risks as users work from mobile devices far outside the bounds of office network controls.

The myriad vulnerabilities that can be present on or in a device can serve as breach points into users' personal data or that of their employers. In this way, reliance on mobile devices is a crucial risk centre for many enterprises.

This is underpinned by yet another trend. The fluidity that modern work demands often permits unmanaged devices. These are the uncontrolled mobile endpoints that employees will often use to carry out their jobs, but without the necessary security controls that are normally required to access their employer's infrastructure. This can happen for a number of reasons, but often because the sheer number of devices that can interface with corporate assets far outstrips many enterprises' ability or desire to discover, manage and protect them. Unfortunately, this also stops those enterprises from actually securing this growing new attack surface.

Cyber criminals will go where there is data to steal. The amount and variety of mobile malware is expanding in line with the expansion of the mobile device as the central business endpoint. From 2021 to 2022, the amount of unique mobile malware samples grew from 611,000 to 925,000, a growth of

51 percent. Similarly, the amount of mobile malware we discovered on devices grew from 1 in 50 Android devices in 2021, to 1 in 20 in 2022.

Zimperium analysis of the 3.8-million Android samples in a popular malware repository found that as many as 23 percent of those samples were malicious. Analysis of the iOS samples found that 24 percent were malicious.

VULNERABILITIES WITHIN EMPLOYEES' MOBILE DEVICES CAN QUICKLY BECOME A BUSINESS RISK

Phishing attacks against mobile devices are growing too, possibly because the average mobile user is six times as likely to click on an SMS phishing link than an email phishing link. Nearly all of the phishing sites – 80 percent – that Zimperium found in 2022 were focused on mobile devices.

The first step to securing mobile devices is for enterprises to actually recognise the problem: That mobile devices have grown so far and so fast that they've become a huge and often unprotected attack surface. Recognising that involves adhering to five key principles that accommodate this new reality.

Protect the device Firstly, risk has to be assessed as close to the user, device or point of entry as possible. It's not good enough to merely protect the connection between the devices and the enterprise. Instead, organisations will need to start prioritising the security by discovering, managing and protecting all mobile devices and apps.

Enable visibility Enterprises need to operate in a known state, establishing complete visibility into their mobile ecosystem. They also need to enable automatic assessment of vulnerabilities. Safeguards in this area need to be measurable and auditable to regularly check whether they're performing as intended.

Detect and respond Mobile detection and response needs to be bolstered. Detecting anomalies and prioritising them based on context will allow the most sensitive vulnerabilities to be fixed first. Similarly, embedding security across device and application lifecycles, using risk-based response and enabling zero trust assessment of mobile endpoints are crucial steps.

Automation Automating these security processes to the greatest extent possible, will permit a proactive and scalable approach to mobile security. This should include the ability to automatically isolate the compromised devices and untrusted environments that introduce risk.

Compliance In an enterprise environment, mobile endpoints often deal with a mix of both corporate and highly personal data. As such, this is a key point of compliance sensitivity. When thinking about mobile device security, the risk of compliance failures must be minimised and the personal data of the device user must be protected from compromise without compromising user privacy.

The shadow of any big innovation in IT is the disruption which it brings. The mobile revolution has enabled countless other new innovations which we now take for granted. While we're appreciating what we have, we often don't pay attention to what we've lost. If we want to preserve the gains that mobile devices have granted us, then we need to accommodate the seismic shifts which it has brought about ●

Ash Patel, Zimperium's GM EMEA, has more than 20 years of experience in the Cyber Security industry, working with people across vendors, resellers and distributors, and at all levels through the channel and end-user. He now leads the Zimperium organisation in EMEA.

Unmanaged devices used by employees are often used without the security controls normally required to access their employer's infrastructure