PRIME TARGETS

Christoph Hebeisen *reveals how as the world continues to go mobile, cyber threats are following suit*

Traditionally, cyberattacks have targeted desktop computers and servers in corporate networks. But with the evolution of technology moving our online life into the cloud – both personal and work – attackers are shifting their focus towards smartphones, tablets and Chromebooks. Not only can mobile devices access practically all of our cloud data, but many services have shifted to a mobile-first or even mobile-only model. We tend to forget that these devices are a treasure trove of personal and corporate information as we carry them with us everywhere.

Industry research estimates that there are over 5-billion mobile phone users today. From the point of view of a cybercriminal, that means they have over 5-billion potential victims to exploit. The combination of ubiquity and high value makes mobile devices a prime target for cyberattacks. Everyone owns one and we use them to do everything from working to shopping, messaging and banking.

Malicious actors can adopt a variety of methods to exploit an individual's phone. Depending on the ultimate goal, attacks can be as narrow as targeting a single individual with tailored assets, to a general campaign seeking to maximise the number of victims.

USERS NEED TO BE EXTRA VIGILANT ABOUT LINKS RECEIVED IN EMAILS, TEXT OR CHAT MESSAGES

One of the most common threats faced by mobile users are malicious apps on their device. These apps are rarely found on official apps stores like Google Play Store or the Apple App Store. More often than not they come from third-party stores, which do not vet apps as thoroughly. Other avenues of infection are malicious web pages, email attachments or even apps sent as a file transfer in chat apps. They typically lure victims into engaging with the malware with false promises, such as free services or additional functionality. These too-good-to-be-true social engineering tactics are extremely common, but due to a lack of mobile security awareness, they remain lucrative for cybercriminals. One way for malicious apps to conceal their identity is to provide legitimate functions. These so-called 'Trojan' apps perform their malicious purpose in the background.

Some attackers might even seek physical access to the unlocked mobile device as an opportunity to install malware. This is most often observed for surveillance tools in cases of intimate partners installing spying apps on their spouse's device to track them. Law enforcement and intelligence agencies also leverage such tools and may exploit physical access to the mobile device as a means of installing malware.

In addition, sophisticated, well-funded attackers develop or buy malware that exploits security vulnerabilities in apps and/or the operating system to allow them to take control of a mobile device without needing much or any cooperation from the victim. Such schemes might involve a text, email or chat message being sent to the target device. Depending on the details of the attack, exploitation might take place as soon as the victim receives the message or when a malicious link in the message is clicked. In the most sophisticated versions, no user-interaction is necessary for a successful takeover of the device by the attacker. These are what we call 'zero-click attacks'.

Another prominent and increasingly common attack method is mobile phishing. While phishing has long been a serious headache for security professionals on desktop computers and email, mobile devices are now a primary target for attackers. We now routinely observe threat actors either adding mobile pages or even targeting entire campaigns to mobile devices only. The mobile user experience also hides a lot of the telltale signs we're used to – such as the entire URL of a webpage to accommodate small screen sizes. This makes it harder even for savvy users to spot phishing attacks. Concurrently, phishing lures have diversified from email – where they face increasingly successful spam filtering – to text messages, social media and chat apps. There is now an enormous number of mobile apps with communication functionalities.

In order to better understand why mobile phones are targeted by hackers, we can divide attacks into two relatively distinct groups: financially motivated and data motivated.

The vast majority of mobile attacks are financially motivated. Like other criminals, cybercriminals are mostly interested in making fast and easy money. In fact, financial gain could be described as the biggest motive for the modern cyberattacker with estimates claiming that they rake in $1.5-trillion annually.

At the lower end of the financially motivated mobile threat complexity scale, there are ad-related attacks that include scams such as adware and click fraud. While adware can be annoying and click fraud can cause data overage fees for the users, the true victim of such malware is the advertiser who pays per 'impression' of or 'click' on their ad. The criminal skims a part of the revenue fake clicks or impressions their malware generates. Other financially motivated malware affects the user more directly such as cryptomining or proxy malware. The latter permits third parties to use the device's internet connection for their purposes, increasing data usage. Cybercriminals can use this to hide their activities. And depending on the activity funnelled through the device, this might even land an unsuspecting victim in the crosshairs of a criminal investigation.

Estimates claim that mobile hackers rake in $1.5-trillion every year

Another potentially costly attack for victims is chargeware, which is malware taking actions that directly cost the user money. This happens most often through charges on mobile phone bills, such as by sending premium SMS messages or WAP charges and usually without delivering any useful service in return.

At the top end of sophistication of financially motivated mobile malware are banking trojans and similar credential skimming apps. Just like their phishing-based analogues, these apps attempt to trick the user into entering credentials for online banking, email or social media into a fake log-in screen. There is a specialised Dark-Web industry supporting such attacks in which one group might develop a customisable malware and sell it to multiple actors, each of which customises the malware towards particular targets (eg a number of banks in a particular country) and deploy it. The resulting skimmed credentials might again be sold on the Dark Web before finally being used to steal money from bank accounts, send spam messages or impersonate victims.

While ransomware has recently captured a large amount of attention – mostly as a result of attacks on healthcare institutions and public administration – they are much less successful in the mobile ecosystems. In comparison with desktop computers, the operating systems of mobile devices separate apps much more strongly, thereby limiting the damage such malware can do without a full system compromise. In addition, cloud backup is commonly used by mobile users, enabling them to factory reset their device with minimal data loss.

As opposed to the financially motivated attacks described above, the objective of data-motivated attacks is to retrieve sensitive data stored on or accessible by a smartphone. Malware with this purpose is usually referred to as spyware or – more specifically – surveillanceware. Recently, malware used for spying on current or former intimate partners has received its own label – 'stalkerware' – raising public awareness about this important problem. From a technical point

of view these apps exist on a spectrum that also includes 'hacking for hire' and state actors such as law-enforcement agencies and secret services. Most non-state adversaries do not have the skill set or resources to run their own surveillance operation and therefore turn to surveillance-as-a-service operators or buy software from low-cost vendors. While some nation-state actors may develop their own custom mobile surveillance tools, many also appear to buy products from third-party sources, often domestic software or defence companies.

UBIQUITY AND HIGH VALUE MAKES MOBILE DEVICES A PRIME TARGET FOR CYBERATTACKS

Victims of mobile threats are as varied as the motivations and methods of malicious actors. Most financially motivated threats – such as adware, chargeware, banking trojans and the bulk of phishing – are broadly targeted at any individual and any organisation. As long as there is an opportunity for a hacker to gain financially, they will seek out any chance to exploit it.

With data-motivated mobile attacks like surveillanceware, threat actors usually target an individual or a small group to extract specific information. Politicians, dissidents, journalists and key decision makers are certainly at higher risk from top-of-the-line surveillanceware than the average citizen. With the license cost of this special malware measured in tens of thousands of dollars per target device, few high-value targets warrant the expense to spy on them. Lower end surveillanceware is commonly seen across all parts of society. But given its purpose, it is also used to target particular individuals.

Protecting our mobile devices from malware and other online threats is just as important as it is for desktop computers. To begin with, mobile users should only install apps from official app stores such as Google Play Store or Apple App Store. Apps offered such app stores have been vetted rigorously. So while it is not unheard of for a malware app to slip the net, the rate of malware is very small compared to most third-party stores. Users also need to be extra vigilant when following links received in emails, text or chat messages or on less than trustworthy web pages. While it might be hard to apply the same scrutiny as they would on their desktop computer before clicking a link on a mobile device, it could make the difference between being safe and getting scammed.

However, even users with the best training and intentions need a safety net for when they encounter a particularly well-targeted phishing message or when they accidentally click on a link in a moment of distraction. This is especially true when devices contain sensitive corporate data that requires strict protection. We have long accepted that internet-connected desktop computers and laptops need up-to-date antivirus software. But most mobile devices are still unprotected, while amassing functionality and accessing ever more personal data. Mobile security solutions can protect devices from malware, device compromise and phishing attacks, sparing users the experience of having their bank accounts emptied or their private data exposed.

As smartphones and other mobile devices acquire ever more functionality, our dependency on them will only increase. Their attraction to hackers and other bad actors as a lucrative target for financial gain and spying will grow in lock-step with technical progress. We have reached a critical point in this development at which the need to secure the mobile phone can no longer be ignored ●

Christoph Hebeisen leads the Security Intelligence Research division at Lookout. In this role he oversees the company's suite of research activities, which cover malware, device compromise, network threats, phishing and threat intelligence services.

One of the most common threats faced by mobile users are malicious apps