Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Cyberthreats are going mobile and it’s time to take action

Tom Davison, Lookout

The world recently experienced an accelerated shift towards a remote working environment under Covid-19. Before the pandemic, workforces primarily relied on desktops and corporate network servers, with only 5% of UK workers operating from home. That number is now 72%. As many of us continue to work away from the office and try to juggle personal responsibilities, we are finding new ways to stay productive – this includes using our mobile devices more.

With mobile devices now at the centre of our lives, they have access to sensitive private and corporate information. And just as the world has gone more mobile, cybercrime has too. Because we have our mobile devices on us at all times, hackers are adapting and focusing their efforts on them. But how is this achieved?

A spectrum of attacks

There are different ways attackers can go about exploiting an individual’s mobile device. They could tailor an attack to a single high-value target, or they might cast a wide net to try to maximise gain.

One of the most common methods is to infect smartphones with malicious apps. These apps are unlikely to be found on official app stores like the Apple App Store or the Google Play Store. Instead, they tend to be found on third-party stores that do not vet their apps as thoroughly as official stores. The goal is to trick the user into downloading the malware onto their device. Attackers can achieve this in various ways, such as sending phishing links or attachments using email, messaging apps, social media platforms, even dating apps.

Some malware may disguise its malicious intent by providing genuine functionalities. These so-called ‘trojan’ apps run malicious activity in the background of an app while performing a legitimate function, making them difficult to detect.

Physical compromise

Not all attacks are remotely conducted, however, as some hackers may attempt to physically compromise devices. Malicious actors can download malware onto mobile devices to which they have physical access. Some methods do not need any interaction from the device owner at all. Well-funded attackers may use malware that exploits operating systems, giving them control of the mobile without any cooperation from the victim. These are called ‘zero-click attacks’ as the target simply has to receive a text, email or chat message for the malware to be activated. This is one of the most sophisticated methods of attack, as well as one of the most expensive.

Another one of the most popular attack methods is mobile phishing. Phishing has been a long-term issue for security professionals on desktop devices with email. But it has changed with the rise of mobile devices. On mobile you can deliver a malicious link in countless ways, including SMS text messages, social media and chat apps. Phishing is especially effective on mobile as users are more likely to trust a text message link than an email link. The mobile experience also hides a lot of the known signs of phishing scams, such as the entire URL of a web page, to accommodate small screen sizes. This makes phishing scams harder to detect, and is the reason they are on the rise.

Attack motivations

The motivations for mobile phone attacks can be divided into two categories: financially motivated and data motivated attacks.

The majority of mobile attacks are money-driven, with financial gain being described as the biggest motivator for cyber criminals, with an estimated $1.5tr annually in gains. Some of the less-complex financially motivated mobile threats are ad-related attacks, such as click fraud and adware. Ad-related attacks can cause annoying data over-usage fees for the users, but the true victim of these scams are the advertisers that pay per click on their ads, with part of the revenue skimmed by the fake clicks that the malware generates.

A higher-impact financial malware is crypto-mining or proxy malware. Proxy malware allows third parties to use a device’s Internet connection, which increases the user’s data usage, while also hiding the cyber criminal’s nefarious activities. This not only has financial implications for victims but may have legal consequences if other crimes appear to be sourced from their device.

Chargeware is another similarly costly attack. This is where the actions of the malware have a direct cost on the user and mostly it impacts phone bills as attackers send premium SMS messages without delivering any useful service in return.

Some of the more-sophisticated financially motivated mobile malwares are banking trojans and credential-stealing apps. Just like the phishing-based analogues, these apps trick users into entering...
their details for online banking, email or social media accounts into a fake login screen. Some hacking groups have been known to develop customisable malware that can be resold to multiple actors. The skimmed credentials may then also be sold on the dark web and then finally used to steal money from bank accounts, impersonate victims or send spam messages.

Data motivated

The objective with data-motivated attacks is different from financially motivated attacks, as cyber criminals are wanting to access sensitive data stored on the mobile device. Data-motivated malware is usually referred to as spyware or surveillanceware, with stalkerware also growing in popularity.

These apps may be used by jealous spouses to spy on their partners, or they may be used by state actors and law enforcement agencies to gain intel. Non-state actors usually do not have the skills or resources to build their own surveillanceware operations so use surveillance-as-a-service operators or purchase low-cost software. Nation-state actors, on the other hand, develop their own mobile surveillance tools, while some buy products from third-party sources as well.

Victims of mobile attacks

Who or what becomes a victim of a mobile attack depends on the methods and motivations of the malicious actor. Financially motivated threats, such as chargeware, adware and banking trojans, are typically targeted at any individual or organisation. Financially motivated hackers simply seek to exploit anyone they can financially gain from. Alternatively, data-motivated attacks tend to target victims in pursuit of specific information.

Key decision-makers and holders of important information are usually more at risk of being victims of surveillanceware attacks than the general public. Victims of data attacks are also decided by the price of the malware used, as some malware is priced at tens of thousands of dollars per targeted device. Therefore only a limited number of high-value targets warrant the expense of surveillanceware, while lower-end spyware and stalkerware is used across all parts of society.

Protecting your device

It is important to protect your mobile device just as you would any desktop computer. First, it is good practice to install apps only from official app stores such as Apple’s App Store or the Google Play Store. Unlike third-party app stores, official stores vet their apps vigorously, making them a safer option. Second, users must be extra vigilant when following links sent via messages or when opening web pages while on a mobile, as it is harder to identify phishing attacks compared to desktops.

But even the most well-trained users can be affected by a scam. Therefore, be sure to use up-to-date security software for your smartphone, just as you would for your laptops and desktops. Furthermore, having a dedicated mobile security solution will help defend users against malware, device compromise and phishing attacks, thereby protecting data from exposure.

As our dependency on mobile devices increases, so will the number of attacks. Mobile devices provide the opportunity for limitless financial gain and data theft. In order to protect ourselves against malicious actors, we must stay vigilant, protect our data and defend our devices, remaining fully cognisant of their value to attackers.

About the author

Tom Davison is technical director, international at Lookout where he leads a team of mobile security experts who advise on mobile security best practice and strategy. Prior to Lookout, Davison has held leadership roles in Tier 1 security vendors.

References

1. Cotton, Barney. ‘How many people in the UK worked from home prior to coronavirus outbreak?’. Business Leader, 25 Mar 2020. Accessed Mar 2021. www.businessleader.co.uk/how-many-people-in-the-uk-worked-from-home-prior-to-coronavirus-outbreak/81646/.
2. ‘2020 Mobile Phishing Report from Lookout shows 37% sequential increase in the first quarter of 2020’. Lookout, 2 Jun 2020. Accessed Mar 2021. www.lookout.com/company/media-center/press-releases/mobile-phishing-report-shows-37-percent-increase-in-first-quarter-of-2020.
3. ‘Financial gain is the biggest motive behind most of the cyber attacks’. Kratikal Tech, 12 Jul 2019. Accessed Mar 2021. https://kratikal.medium.com/financial-gain-is-the-biggest-motive-behind-most-of-the-cyber-attacks-cc8d35106410.
4. Bauer, Adam; Kumar, Apurva; Hebeisen, Christoph. ‘Lookout discovers new mobile surveillanceware developed by Russian defense contractor Special Technology Center’. Lookout, 24 Jul 2019. Accessed Mar 2021. https://blog.lookout.com/monokle.