Mobile threat

February 2018

David Bird FBCS considers threats via mobile devices and explains why he thinks the future may not be so bright.

The unprecedented WannaCry ransomware and subsequent Petya destruct-ware outbreaks have caused mayhem internationally.

As a result of a remote execution vulnerability, malware has propagated laterally due to two basic root-causes: (a) out-dated operating systems (OS), and/or (b) in-effective patching regimes. Here we have a commonality with the mobile device domain.

There are many older generation devices that have different legacy mobile OSes installed that are no longer supported or updated. Legacy connected Microsoft Pocket PC palmtops and Windows CE or Windows Mobile devices are examples of tech still being used by delivery firms and supermarkets; even though they have been end-of-extended support since 2008 and 2014 respectively.

So, do we have a problem?

With over two and a half billion smartphones globally in 2016, the market is anticipated to reach at least six billion by 2020 due to the convenience of mobile back-end-as-a-service. Apparently, one vulnerability is disclosed every day, in which 10 per cent of those are critical. This figure does not include the number of internet-enabled tablets that are in circulation; in 2015, there were one billion globally, and this is expected to rise to almost one and a half billion by 2018.

Today both Android-centric manufacturers and Apple fight for dominance in the mobile device market - squeezing out Blackberry's enterprise smartphone monopoly. This has resulted in unsupported Blackberry smart-devices persisting in circulation, closely followed by successive versions of Windows Phone OS - with only 10 left supported.

This leaves Google's Android and Apple's iOS as the prevailing brands.

Apple has evolved to provide the most widely available mobile iOS updates to tackle vulnerability remediation. Whilst Google provides a patch / update cycle for their brand of Android smart-devices others lag behind; in 2016 only 15 per cent of Android devices had been upgraded to Android 6.0 Marshmallow with a third still on Android 4.4 Kitkat.

The latest iOS11 update incompatibility list only goes to reinforce the fact that older smart-devices do eventually go out-of-support. Furthermore, the use of cyberspace through smart-device proliferation brings with it inherent risks.

For example, F-Secure reported that vulnerabilities in Apple iOS devices had increased by 82 per cent in 2013 and by 2014 stated that 99 per cent of mobile malware was designed to attack Android.

In essence, a self-perpetuating paradigm exists where our civilisation has become so accustomed to smart-devices that the risks are being obscured.

The stage is set for mobile cyber carnage!

With the ascendancy of our constant need to access the online world, cybercriminals appear to be progressively targeting smartphones facilitated by incessant 'smartphone wars'. Consequently, mobile malware tradecraft has progressed significantly since the early days when Symbian OS mobile malware spawned malicious web links using short-message-service (SMS). These days the scale of nefarious activity in this domain is so startling it's causing consternation.

Attack use-cases

In 2013, Android FakeDefender began the mobile-crafted ransomware trend; by 2017 McAfee cited that Congur ransomware accounted for nine out of ten detected Android mobile hacks.

2015's DroidDream enabled a remote attacker to take control of devices, Android Exploit Masterkey turned legitimate applications into malicious Trojans, and the Basebridge Trojan was used to exploit vulnerabilities in outdated Android platforms. This year ESET identified the two-stage malware DoubleLocker, that is deployed through a malicious Adobe Flash update onto Android devices.

By 2016, Checkpoint identified a phishing campaign that fooled iPhone users into installing malicious configuration files, which exploited the SideStepper iOS vulnerability - potentially enabling them to conduct a man-in-the-middle attack. Last year Lookout acknowledged that two malware strains were available to root smartphones - including Pegasus for iOS and LevelDropper and Shedun for Android.

This year Trend Micro established that a new malware strain can exploit the Dirty COW privilege escalation vulnerability found in the Android OS kernel called ZNIU.In addition, a recent vulnerability found in iPhone firmware for iOS10, or earlier, affects its use of the wireless Broadcom chipset; enabling a hacker to conduct a localised execution attack to deploy a backdoor - presently this is only patchable by upgrading to iOS11, if you can.

Supply chain issues

In 2014, several well-established smart-device manufacturers installed fake applications of renowned variants embedded with the DeathRing Trojan; DeathRing could download SMS and WAP content from its command and control servers for nefarious purposes.

In the same year the GhostPush Trojan was found incorporated within applications hosted on Google Play Store and infected nigh on a million Android devices. The iOS XCode Ghost campaign used a subverted software development kit to embed malware into iOS applications that subsequently seeped past Apple's App Store inspection regimes.

By 2016, Kryptowire reported that cheap Android mobile phones being sold online in the US had preloaded backdoors that reported users' SMS and location data back to hackers - affecting 700 million. In 2017, the Android Trojan Xavier, related to Joymobile of 2015, was detected within more than 800 apps in the Play Store and was designed to steal users' personal data.

By this summer, Google had removed 50 malicious apps embedded with ExpensiveWall after Check Point discovered the premium-rate SMS generating malware. Not only that, Google Play Protect also discovered Lipizzan spyware on at least 20 apps hosted on the same store.

Notably in 2016, Checkpoint discovered a Qualcomm chipset vulnerability that put 900 million Android handsets at risk through a condition called QuadRooter; this could give an attacker root access to devices after using downloaded malware to undertake this incursion.

A theoretical attack known as BlueBorne has been discovered by researchers this year after finding eight Bluetooth zero-day vulnerabilities; this hypothetical attack could even occur against unpaired and undiscoverable devices, which is a little disconcerting. As a direct consequence billions of smart-devices are potentially at risk.

Does this mean a malignant mobile future?

Mobile malware has become more prevalent over successive years facilitated by advanced global cybercrime. The first port of call for attackers could be social engineering via social media, the use of malicious email attachments, phishing emails or perhaps infiltration indirectly through in-app malvertising - unprotected by in-effectual antivirus software.

Not only that, risks can come from subverted side-loaded or corrupted apps, flawed authentication or encryption mechanisms and even hacked or jailbroken devices that have been lost or stolen.

It has been identified that one in every 120 smartphones may have some form of malware infection such as: ransomware, backdoors, spyware, SMSTrojans, overly aggressive adware or potentially mutating malware.

Contrary to the recent false sense of security hyperbole, research completed by Pradeo Lab found that 50 smartphone banking apps were left wanting; on average seven security flaws were found per app.

The 2016 Nokia malware report states that smartphones accounted for 78 per cent of all mobile network infections - totalling 85 per cent of all malicious traffic; Android comprised 74 per cent and iOS devices 4 per cent.

Kaspersky detected 40 million attacks in the same year citing that cybercriminals were taking advantage of smart-devices not receiving OS updates or obtaining them late as the main cause. By this year, 19 million malware programs had targeted Android.

Initiatives such as Apple’s boot chain, keychain and runtime process security as well as security measures such as Knox, integrated into Samsung’s Android mobile phones, have gone some way to enhance security in mobile platforms.

However, there has, perhaps, been an over reliance on assumed mobile app development integrity and app code maturity. More trust verification mechanisms are needed for this market - such as AppIntegrity for Android - to safeguard the mobile software supply chain11.

Unfortunately, user ignorance is not bliss, consumers appear to be naïve enough to care little about tedious activities like performing optional software updates - a lethargic underestimation of the risks. Within a population of billions of smartphones and tablets there is a significant, and perhaps unquantifiable attack landscape, of un-patched legacy and even modern host OSes installed with legacy applications.

Whilst cyber criminals are not necessarily coordinated, there is a real and present danger that the opportunities afforded by the smart-device attack surface could grow from epidemic to pandemic proportions.