Briefing Note

Mobile security solution review in light of the WhatsApp Pegasus hack

Introduction

Smartphones are the most powerful communication tools ever invented. We expect that our mobile communications are secure and are comfortable to use them for even the most sensitive secrets. It is no wonder therefore that mobile devices have quickly become some of the biggest targets for cyber threats such as phishing and malware. The rate at which they are used for personal as well as business, the smaller screens, and the numerous different platforms for communication all make mobile devices especially vulnerable to attack. In response to this, there are a range of tools aimed at thwarting mobile device hacks now available, however their effectiveness can be questionable - especially in response to modern, more sophisticated threats such as the WhatsApp hack discovered in May 2019.

On May 13th 2019, the Financial Times reported that a major flaw in the hugely popular messaging app WhatsApp had recently been discovered. The vulnerability was found to leverage a bug in the audio call feature of the app that enabled malicious actors to inject spyware onto the device, regardless of whether or not the call was actually picked up. The spyware used in the attack is believed to have been Pegasus, a powerful form of malware developed by the Israel-based NSO Group. The well known surveillance package usually licensed to governments for crime fighting and anti-terror investigations has the ability to collect intimate data from a device, including location data and information recorded through the microphone and camera. Although WhatsApp were quick to issue a warning and an updated version of the app to all of its users to protect against potential compromise, attacks like this beg the question: what do I need to keep my organization's mobile devices secure? What mobile security tools are available today and would they have provided any protection when confronted such a modern threat as this?

Mobile Security Tools

Anti-virus

We are all familiar with anti-virus (AV) programs from the PC world. Such programs are also available for mobile devices. However, because of the way Apple and Google have designed their operating systems AV programs can often do little to detect malware. Apple bans AV programs from its app store and while Google, with a more open attitude, allows AV programs for Android its efforts are focused on its in-house virus scanning efforts known as Google Play Protect.

How anti-virus solutions work

How mobile anti-virus solutions work is relatively straight-forward. The software checks all apps on the mobile device against a list of known malware. If it finds a previously unseen app, a copy is taken and analyzed to see if it contains any suspicious or malicious code that may pose a risk to the device and its data.

Is it effective?

Anti-virus solutions are largely ineffective in the protection of mobile devices from modern threats. Firstly, an anti-virus program is only effective if the malware is contained within an app. Any malware distributed via email, SMS or messaging service like WhatsApp would not be detected. Secondly, the program cannot stop the user from installing malware and once detected, cannot remove it from the device. Finally, it is relatively easy for malware developers to trick anti-virus software into thinking that their code is benign. If the app detects that it is being analyzed, the malware can simply change its behaviour to appear innocent and therefore render the anti-virus useless.

Mobile Device Management

Mobile Device Management (MDM) systems are often mistaken for mobile security tools when in fact they are only used by organizations to configure and manage their employees' mobile devices. They enable IT departments to do things such as distribute applications and email configurations to employee devices over the air. They can also be used to enforce basic security rules such as requiring a device to be encrypted and to have a strong password but are not designed to secure devices against cyber attacks and therefore would offer no defense against a threat like Pegasus.

Mobile Threat Defense

As mobile devices became more popular and therefore more vulnerable to threats, a range of products were launched to address the limitations of anti-virus solutions in the early years of this decade. Leading IT analysts Gartner to call this product category 'Mobile Threat Defense' (MTD). These solutions are typically deployed alongside an MDM system.

How Mobile Threat Defense works

Mobile Threat Defense products work by collecting information about device configurations, apps, and networks to identify potential risks. Organizations can then use their MDM systems to block any high risk devices from accessing corporate applications and data.

Is it effective?

MTD solutions suffer from two severe limitations affecting their ability to effectively protect from modern mobile threats:

> i) They have very limited visibility of device network traffic making it difficult for them to detect malware infection.
> ii) They have no way to automatically disable malware meaning that they cannot prevent its operation once installed on the device.

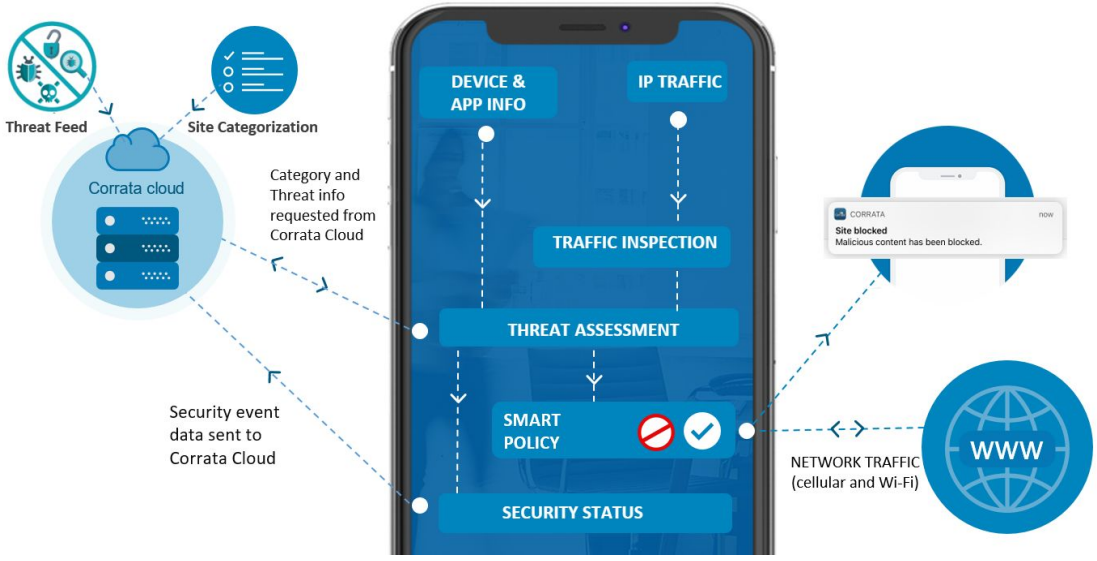
A MTD solution would have provided no protection from the WhatsApp hack. None of the settings that MTD monitored would have disclosed that malware like Pegasus had been installed on a device, leaving it to operate without any interference.

Corrata's Solution

Recognizing the limitations of these traditional tools, Corrata has pioneered a new approach to mobile device security. Our approach is about protecting the device rather than simply monitoring it and our vision is to act like an immune system for your mobile device - protecting against attacks and fighting back against those that occur.

How Corrata's solution works

Corrata's solution is based on our patent pending SafePathML technology. SafePathML creates the equivalent of an enterprise grade firewall installed on each device. Once installed the firewall has complete visibility and control over all network traffic to and from the device. Every server to which the device attempts to connect is reviewed in real-time no matter what protocol is being used. Using dynamic rules, called Smart Policy Protection, connections to suspicious hosts are blocked. This stops devices connecting to malware download servers. Where the malware download is well disguised Corrata will detect it once it attempts to communicate with its command and control infrastructure. Such connection attempts are immediately blocked which has the impact of preventing the malware from sending any data back to its owners.



Is it effective?

Corrata's approach protects against phishing by blocking all access to phishing sites, while the risk of mobile malware infection is combated by blocking access to malware download sites. Malware which has been installed on the device is also disabled by blocking communications with its Command and Control servers.

In the WhatsApp case, the Pegasus malware was disguised as an inbound VoIP call and once installed, was known to communicate to servers controlled by its owners NSO. Corrata's SafePathML technology would have complete visibility

over device network traffic to detect these connection attempts. Our Smart Policy Protection would then flag and block any suspicious attempts, reporting them automatically to information security teams and disabling Pegasus.

NSO, like others who operate malware, constantly change their server infrastructure and make significant efforts to avoid detection. Security solutions, like anti-virus or MTD, which rely on lists of known malicious domains and IP addresses don't work against sophisticated actors. In contrast, Corrata uses its Smart Policy Protection feature to spot these suspicious connections. Smart Policy Protection uses a combination of device traffic analysis, global internet categorization data, and information about domain registrations to identify newly created malware servers.

Key takeaways:

- The WhatsApp hack has raised awareness of the vulnerability of mobile devices and helped to dispel a level of complacency about the threats. It has become crucial to ensure that our security software offers the best possible protection against the most determined attackers.

- Corrata has developed a new approach to mobile security. Rather than just providing visibility of risks, it proactively protects against them by acting as a firewall between the malicious actors and your mobile device.

Want to find out more about mobile threats and how to ensure you are protected?
Contact Corrata today.