Security

Be prepared for the rise in mobile malware

Every large business has now suffered a malware attack – with 89 percent experiencing a man-in-the-middle attack over Wi-Fi. While the vast majority of attacks are on Android devices, iOS devices are not immune to breaches[1].

With a growing number of mobile business users in their sight as potential victims, cybercriminals are expanding their attack vectors. Attack types include complex phishing attacks, mobile remote access Trojans, ransomware, fake apps and infostealers.

Cybercriminals are also taking over mobile devices to launch massive, sustainable attacks. These mobile botnets can be spread through hidden worms and Trojans that have been unintentionally downloaded and can be triggered via emails, apps and websites. Once the malware has gained access it starts communicating with and receiving instructions from command and control servers. Mobile device cross-contamination is rapid, giving botnets the power to bring down multinationals, financial infrastructures and governments.

All these attacks cost cybercriminals little to perpetuate, but they can bring them large rewards at your expense.

All manufacturers have had exposures:
All mobile devices have inherent security risks. Android and iOS now account for 94 percent of the mobile operating system market worldwide[5]. While the vast majority of attacks are on Android devices, iOS is not immune to attack. Malware in iOS isn't as prevalent as Android due to Apple's store requirements, it is open to others such as network attacks and side-loaded apps installed in jailbroken devices.

Growing risks

54 **is the average number of malware attacks per business[2]**

75% **of organizations have had at least one jailbroken iOS device or rooted Android device connected to their corporate networks[3]**

$26.4m

Potential cost of a mobile data breach for a large enterprise[4]

Just one third of enterprises have deployed a mobile defense solution[6]. Mobile devices will become an increasingly vulnerable spot if enterprises don't take action. The threats are only going to get bigger and more widespread – protecting your mobile workforce is critical in protecting your reputation and your bottom line.

orange™ Business Services

The five major threats to mobile security and some helpful tips to counter

System vulnerabilities

Mobile device operating systems provide vulnerabilities for attack. New versions are often late to market, and critical updates and fixes stalled. Android is open source so if a developer makes an insignificant change it can create a security hole. iOS is less vulnerable as Apple controls the OS, and doesn't release the code. There is more malware and OS attacks targeted at Android, but iOS is still exposed to risk.

Take action:

1. Continuously analyze devices for system vulnerabilities and suspicious behavior.
2. When a threat is identified, automatically mitigate risk until the threat is eliminated.

Rooting and jailbreaking

'Rooting' in Android and 'jailbreaking' in iOS enables customizations and configurations not provisioned by the manufacturer, such as installing spyware. Mobile device management (MDM) and enterprise mobility management (EMM) systems provide static root indicators. But it isn't enough as cybercriminals can block requests to avoid detection. Advanced solutions with a dynamic threat response layer are necessary. An integrated Security Information and Management System (SIEM) enables centralized reporting of your security events, which can result in attacks being detected that escaped other means. Some SIEMs can stop attacks in progress.

Take action:

1. Use static and dynamic detection methods for rooting and jailbreaking.
2. Monitor all configuration changes made.
3. Use behavioral analysis to spot suspicious behavior.

Trojans

A type of malware that is carried with an app or installed through an unsecure network connection. Often disguised as a legitimate program, once downloaded the malicious code can do everything from track locations and extract call log information to eavesdropping on conversations.

Take action:

1. Capture and reverse-engineer apps for analysis to expose any suspicious behavior and examine malicious programs.
2. Automate responses and user notifications with remedial moves to eliminate malware.
3. Dynamically trigger device policy changes in your MDM or EMM systems.

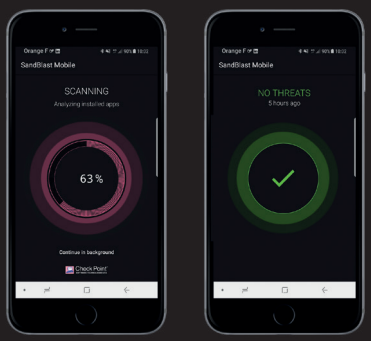
The wild west of mobile apps

Malicious apps can steal data and take control of mobile devices. Popular apps can be reverse-engineered, injected with malicious code and uploaded to storefronts. These malicious apps can be financially motivated, activated to steal data or seize control of the microphone and camera on the device.

Take action:

1. Uncover malicious code in apps by looking for unique binary signatures.
2. Capture apps as they are downloaded and run them in a virtual sandbox to analyze behavior.
3. Determine where the app came from and monitor its installation process.

1, 2 and 3. Checkpoint Mobile Threat Research Team. 4. Forrester Research mobile smartphone and tablet report 2017. 5. The Ponemon Institute 2016. 6. The growing threat of mobile device security breaches – Dimension Data 2017



Orange Cyberdefense

Mobile Threat Protection from Orange

Embeds an easy-to-deploy app that runs in the background of the user's device on both iOS and Android platforms. It protects the device with accurate threat detection from types of known and unknown risks (malware, network and OS breaches, phishing by texts), without impacting device performance or battery life. The user is alerted if there is an attack. A comprehensive dashboard via an administrator portal provides a 360 degree view of threats with detailed information on each threat.

Simple and easy to install, compatible with any operator and available on a monthly subscription calculated as close as possible to your use. Mobile Threat Protection from Orange really is a no brainer when it comes to safeguarding your mobile fleet.

For more information contact your Sales Representative.

Follow us:
https://www.orange-business.com/en/products/mobile-threat-protection