the Availability Digest

www.availabilitydigest.com

Mobile Device Threats to Corporate Networks

July 2013

Bring Your Own Devices (BYOD) are the new gateways into corporate networks. An increasing number of employees are using their smart phones, tablets, and notebook computers to conduct their work at home or on the road by connecting outside the corporate firewall into their companies' servers and databases. This is a great convenience for workers and represents an increase in productivity for their employers – the distinction of a fixed workday is disappearing.

Unfortunately, BYOD also means that malicious actors can gain access to a company's network by infecting these devices, which are woefully unprotected. Mobile malware is rapidly becoming a greater concern than direct infections of the systems themselves.

Mobile Malware Aimed at Android Devices is Climbing Rapidly

Mobile malware is most apt to be introduced into a mobile device by malicious applications obtained from app stores that are not vetted by Google for Android devices or by Apple for iOS devices. Because of the open source provided by Google's Android operating system, the bulk of mobile malware ends up on Android phones and tablets.[1]

According to studies conducted by McAfee and Juniper Networks, the number of malicious mobile apps has grown more than 600% in the last year alone to over a quarter-million apps. The percentage of these apps aimed at Android devices has grown from 24% to 92% over the last three years.

Juniper's report identified more than 500 Android application stores that are known to host mobile malware. 60% of these originate from either China or Russia.

Critical Threats of Mobile Malware

A common free app (one is known as *Fake Installer*) tricks users into sending messages to premium-rate numbers set up by the attackers. The user is billed several dollars for each message that is sent (either purposefully by the user or automatically by the malware). This can lead to exorbitant telephone bills for the user.

However, this is an attack directly on the user. Of more concern is mobile malware that is directed at gaining access to corporate assets. Marble Security, Inc. (www.marblesecurity.com), a company that offers a mobile-security cloud service to protect against threats to enterprise systems by mobile devices, has published a study identifying nine major mobile threats perpetrated against mobile workers. These threats are summarized below. Reference should be made to Marble's white papers[2] to gain an understanding of the protections that are available to thwart these threats.

---

[1] Mobile Malware, Mainly Aimed at Android Devices, Jumps 614% in a Year, *CIO*; July 12, 2013.

[2] Nine Critical Threats Against Mobile Workers, *Marble Security White Paper*. 2013.
How to Effectively Secure Your Network Against Mobile Threats, *Marble Security White Paper*.

Malware, Trojans, and Zero-Day Attacks

Malware, Trojans, and zero-day attacks generally infect a device by disguising themselves as legitimate apps. Trojans open back doors that remote control sites can use to infect the device with malware. Zero-day attacks use unknown vulnerabilities that are exploited to infect a device with malware before the developer of the software knows about the vulnerability.

The most significant new targets for malware are mobile devices. Infected devices allow cybercriminals to penetrate the corporate firewall and access enterprise networks. Android is clearly the number one target. Drive-by attacks on Android phones have become prevalent. With this strategy, an attacker redirects visitors of a website to one controlled by the attacker so that the attacker can download the malware of its choice.

Commercial antivirus software is the common defense against the insertion of any type of malware into a device. While these solutions are an important defense against infections, they cannot completely protect a device (and thus the enterprise) because malware authors create new versions at rates that often exceed the capacity of the antivirus vendor to identify the attack, add the defense to its product, and get updates downloaded to devices.

Anti-malware scanners for mobile devices are not nearly as sophisticated as those for PCs. The potential ramifications of an employee using an infected Android tablet or a Galaxy phone to access corporate information should be of utmost concern to a company.

Jail-Broken and Rooted Devices

Both Android and iOS devices are configured to prevent unauthorized access to privileged commands. However, this protection can be broken, especially for Android devices.

An Android devise can be modified by the user to allow applications to have root operating-system privileges. This is necessary in order to run certain apps. In a rooted device, malware can be installed that can operate at the operating-system level and that can take over all of the functions of the device.

A similar technique for iOS devices is jail-breaking. However, in the tightly controlled iOS world, jail-breaking requires bypassing several iOS security functions simultaneously and generally cannot be done by the user.

A rooted Android or jail-broken iOS device can be infected with malware that can be particularly destructive, difficult to detect, and difficult to remove. An employee may not even know that his Android has been rooted. Perhaps his teenage son has rooted it so that he can download a free app that can only run on a rooted device. The next time that the employee logs onto the corporate network, he is doing so with a compromised device.

Key Loggers

A key logger, or keystroke logging malware, inserts a driver beneath the operating system that tracks everything the user types. The key logger sends the information to an attacker's server to capture sign-on credentials, account numbers, and other sensitive data. Key loggers are one of the earliest techniques for cybercriminals to compromise virtual private networks, corporate networks, email accounts, and online banking sites.

Increasingly, key loggers have targeted Android and iOS devices. One strategy is to find an Android device that has been rooted or an iOS device that has been jail-broken so that malware can run privileged commands. In a rooted device, a key logger can be installed under the operating system.

Another technique is for the user to install a virtual keyboard, which allows the user to insert small icons such as smiley faces in text messages and emails. The virtual keyboard app may be infected with a key logger.

Compromised Wi-Fi Hotspots

Wi-Fi hotspots are popping up everywhere. Employees access their corporate networks from coffee shops, airports, hotels, and many other places. Wi-Fi hotspots often lack firewalls or web intrusion systems. Corporate data is vulnerable whenever an employee logs into a Wi-Fi hotspot.

Wi-Fi networks are frequently configured so that anyone on the network can see all of the network traffic. If an employee uses a non-encrypted session to access his Facebook account, his session can be read by a hacker. The hacker can send emails with malware or malicious links to all of the employee's Facebook friends, including several of his co-workers.

Monitoring open Wi-Fi networks is a trivial effort. For instance, Firesheep, a commercial downloadable app, allows a hacker to see any unencrypted traffic on a network.

Poisoned DNS

Regardless of platform type, devices are configured to use a DNS service to route their URL requests to an appropriate IP address representing the website they are directed to access. DNS services are provided by ISPs, Wi-Fi hotspots, hotels, airports, and anywhere else a mobile device is likely to connect to the Internet. Essentially, the user is being asked to trust the DNS server being provided to him, but he has no knowledge or control over that DNS server.

It is possible for hackers to hijack a DNS server and redirect traffic to a malicious DNS server that points users to a web site that looks just like their corporate, banking, or retail web site to which they are connecting. There, the hacker can capture the employee's password and credentials and gain access to his accounts and often to the corporate network.

As an example, in late 2012, DNS servers were poisoned in Romania and Pakistan. The entire countries were routing traffic to fake, malicious websites.

Malicious and Privacy Leaking Apps

If only Apple App Store and Google Play applications are being used on iPhones and Androids, and the devices are not jail-broken or rooted, the devices should be relatively secure.

However, there are legitimate applications that can gain access to sensitive corporate information. For instance, a productivity app may request access to the device's address book. The contents of the address book may be downloaded to an app server, where it may be compromised by a hacker. This means that cybercriminals may have in their possession the names, positions, telephone numbers, and email addresses of many of a company's employees. This gives the hacker everything he needs to know for spear phishing and advanced persistent threats against many of the company's employees.

In another scheme, hackers download popular applications such as Angry Bird for Android and insert malicious code to steal information. The infected applications are then posted to malicious Android app websites. With hundreds of such sites, it is unreasonable to assume that employees will download apps only from Goggle Play.

Cybercriminals have also been creating fraudulent online banking apps. Potential victims are then sent emails inviting them to download the apps.

Unpatched OS Versions

A lesson learned in the PC marketplace is that the latest patches must be applied to the operating system. Many of these patches close security vulnerabilities that can be used to exploit the device. Older versions are almost always subject to zero-day attacks (unknown vulnerabilities at the time of the release of the operating-system version), known threats, and malware designed to attack certain versions of an operating system.

It is now possible to read the operating system version for Android and iOS devices. System administrators can set policies as to whether to allow access to the corporate network by a device with an unpatched operating system.

Spear Phishing

Spear phishing (or just phishing) is the practice of targeting individuals in a company rather than every subscriber to a particular service. Spear phishing represents a significant threat to businesses.

There are two primary methods for phishing – emails and SMS text messages. For a typical email attack, the attacker obtains an employee's email address and sends him an email with a malicious link or that points him to an infected website. If the employee clicks on the link or visits the malicious web site, his device becomes infected.

Spam filters have been an effective defense against phishing attacks to some extent. However, in 2012 alone, more than 300,000 new phishing sites a month were discovered. Spam filters just cannot keep up with all of these.

With SMS phishing, a user is sent a text message to try to get him to log on to his banking account or onto his corporate network.

Advanced Persistent Threats

Advanced persistent threats (APTs) are attacks carried out by criminal organizations (or even states) that have the resources and time to figure out how to get into any corporation's network. A recent example is the USD $45 million heist against two Middle Eastern banks using compromised gift cards.[3].

Even some of the most sophisticated and highly secured networks have fallen prey to APTs. In 2011, RSA Security was breached and its entire database of RSA tokens was stolen. In this case, RSA was targeted simply by phishing. Phony emails purportedly coming from the human resources department were sent to a half-dozen employees advertising open jobs. When the employees downloaded the infected PDF file attached to the message, the attackers had access to the network.

Once malicious software is on an end-users device that is connected to the corporate network, either at the office or through a VPN, hackers are free to escalate privileges on the company's servers and database and monitor everything on the network.

Summary

Attacks against corporate networks invariably begin by stealing an employee's credentials. When employees access the network from a device that is beyond the control of IT, the risk represents the weakest point in the network. While no single solution can protect against the constant explosion of cyber threats, IT must better protect the mobile devices used by the company's mobile workers. Help is available from companies such as Marble Security that specialize in mobile device protection.

[3] The $45 Million ATM Heist, *Availability Digest*; May 2013.
http://www.availabilitydigest.com/public_articles/0805/45-million_atm_heist.pdf