THE MOBILE MALWARE PROBLEM

THE QUESTION ISN'T "IS IT REAL?" – IT'S "WHAT DO WE DO ABOUT IT?"

STRATEGIC WHITE PAPER

Many mobile operators – and their subscribers – believe malware is exclusively a problem in the PC domain. But as growing numbers of users are learning, malware is burrowing its way into the mobile platform, with potentially significant consequences both for individuals and the providers whose networks they depend on. This Kindsight white paper looks at the rapid escalation in mobile malware attacks and the strategies operators can employ to combat them.

TABLE OF CONTENTS

RECOGNIZING THE MOBILE MALWARE PROBLEM

The mobile network is the latest battleground between Internet security vendors and cybercriminals that develop malware — malicious software or code designed to exploit PCs and, now, mobile devices such as smartphones and tablets. Mobile operators take pride in offering subscribers a fast and reliable network — but malware infections can quickly undo their efforts and have a severe impact on the overall service experience. In addition, the increasing sophistication of malware and the ubiquitous, 'always-on' nature of subscriber devices puts the risk of infection — whether on the mobile operator's own network or via a roaming network — beyond their control.

The Rise of Mobile Malware

In the early 1990s, very few PC users had any concept of the threat posed by malware. Anti-virus software was not widely deployed at the time, and much of the earliest malware was not designed to maliciously exploit other systems: it consisted mostly of pranks intended to expose vulnerabilities found in Windows.

Clearly, the sophistication of PC malware has increased dramatically over the past 15 – 20 years. Today's varieties focus on fraud, identity theft and distributed denial of service (DDoS) attacks. They have become stealthier, finding new and innovative ways to conceal themselves on PCs and spread undetected. Despite billions of dollars invested in R&D to combat malware, it is estimated that approximately 30 – 50 percent goes undetected by anti-virus software. Kindsight Security Labs has found that 15 – 20 percent of home networks consistently show infections, including Trojans, botnets, spambots and keyloggers.

The first virus capable of infecting mobile devices without needing a PC to transmit itself was discovered in the summer of 2004, when the Cabir worm began affecting phones running the Symbian operating system (the dominant platform at the time). Although essentially harmless (spreading via Bluetooth signals, it caused the message "Caribe" to be shown on the phone's display), it proved that mobile devices are not immune to viruses — and opened the door for more dangerous malware in the years following. (According to a study conducted by SMobile Systems, by 2009, one in 63 Symbian devices were infected by spyware, worms or Trojans.)

The first confirmed malware affecting Apple iPhones appeared in late 2009. However, because such malware could be transmitted to and infect only 'jailbroken' iPhones (i.e., devices altered by the user to run software not authorized by Apple), these incidents were not considered particularly worrisome.

Malware for Google Android devices began to appear in Chinese app markets in late 2010. The security industry tracked a number of different types at this time, including DroidDream, Geinimi, GGTracker, Plankton/Tonclank and Hong Tou Tou. However, much like the original Cabir worm, these programs were more 'proofs-of-concept' than sophisticated attacks.

That quickly changed in 2011 when a number of vendors and other observers detected a notable rise in malware communications — more specifically, the command-and-control (C&C) protocols used by malware to call home with stolen information — coming from Android devices. Lookout Mobile Security reported that upwards of one million people were affected by Android malware in the first half of 2011. The number of infections

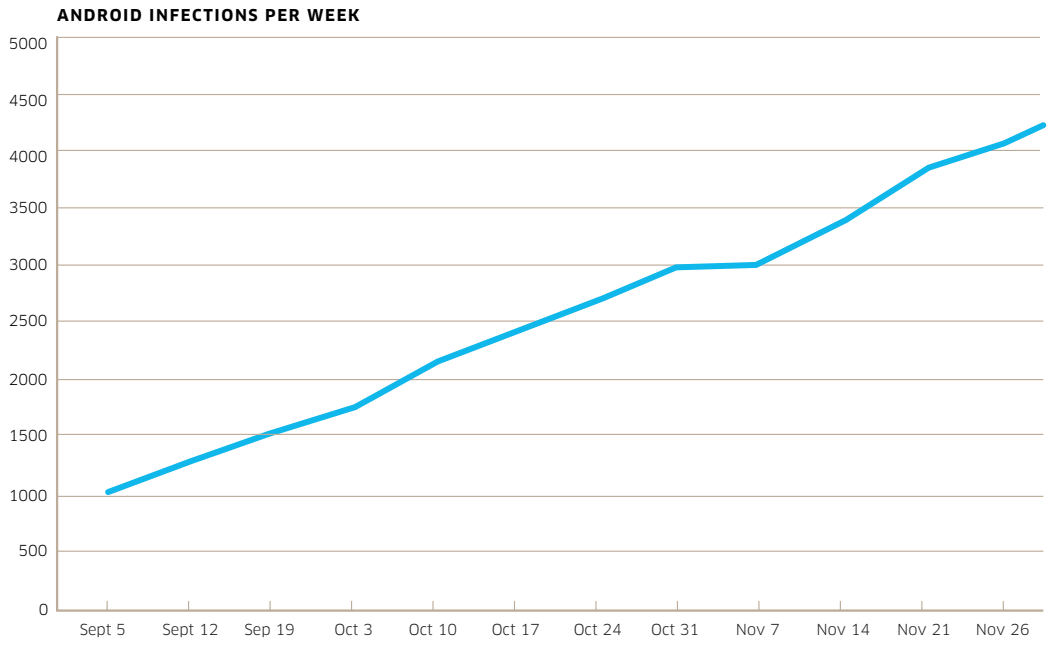
COMMON TYPES OF MALWARE

Trojan
Hidden within legitimate applications, when activated it allows criminals to gain unauthorized access to a user's computer or mobile device.

Botnet
A collection of malware-compromised devices – ranging in size from a few dozen to tens of thousands – whose actions can be coordinated by a command-and-control server. All or part of the botnet can be sold or rented to other criminals for use in spam, identity theft or distributed denial of service attacks.

Spambot
An automated program that harvests personal contact information to send unsolicited email, SMS or social media messages. In some cases, spambots can crack passwords and send its messages directly from a user's account.

Keylogger
Covertly captures passwords, usernames bank account info, and credit card numbers typed into a device, then transmits the information back to criminals.



continued to climb over the second half of the year, with Kindsight Security Labs reporting a 400 percent increase in Android infections per week from early September to late November 2011. In its *2011 Mobile Threats Report,* Juniper Networks noted a whopping 3,325 percent increase in malware specifically targeting the Android platform — from just 400 in June to more than 13,300 by the end of the year.

Why Android is Vulnerable

Among the reasons Apple's Macintosh line of PCs lost market share to Microsoft Windows in the early 1990s was the greater flexibility and openness Windows offered to developers. Unfortunately, that flexibility also created a number of security vulnerabilities, including the ability for processes to remotely take control of the operating system and replicate themselves to other networked PCs. As Windows became the dominant operating system, criminals had further incentive to write malware that could easily target and exploit millions of devices.

The same "which system will reign?" paradigm is now unfolding in the mobile realm, this time between Apple and a fierce new competitor: Google. Just as it did with the Macintosh, Apple has taken a somewhat rigid approach to applications on its iPhone; in the same way Microsoft responded with Windows, Google has countered with a much more flexible — and vulnerable — approach to apps for Android.

Unlike Apple, which only provides authorized apps through its own App Store, Android follows a *laissez-faire* philosophy whereby apps are available from a wide variety of sources beyond Google's official Android Market. Just like Windows software, anyone can post an Android app to any app market without it being subject to security verification. When an app is made publicly available, anyone can download and install it.

Compounding the problem is Google's permissions-based approach to security on Android devices. During installation, an app asks the user for permission to access everything from location data and personal contacts to SMS capabilities and system tools. Even the

simplest of apps can request a long list of permissions — and much like the instantaneous acceptance of lengthy end-user license agreements, subscribers have become accustomed to simply granting any and all permissions without a second thought.

Criminals are leveraging this permissions-based approach to infect the devices of mobile subscribers. For example, legitimate (or legitimate-sounding) apps can be packaged with executables that, in addition to installing the app, also create outbound connections to malware C&C servers. (Android apps are easy to 'Trojanize' in this manner because the app can be signed using any digital certificate and does not require one issued by Google nor does the device display the information from the certificate to let you know who the author is.) By asking for permissions that look familiar to the permissions of legitimate apps, the subscriber is likely to accept them all without hesitation — inadvertently giving criminals access to personal information, or even the ability to place calls or send SMS messages and emails from the device.

Trojanized apps are usually removed from the Android Market as soon as a problem is noticed — but by that point, some damage to subscribers has undoubtedly already been done. Google has recently taken steps to proactively scan and remove infected apps through the introduction of its Bouncer service; however, because of Android's open nature, apps that are removed from Google's Android Market will still be available for download from other places — and many third-party app markets are not quite as diligent. Fortunately, most Trojans make no attempt to conceal themselves and can easily be removed by uninstalling the infected app. That said, malware is showing ever-greater sophistication and becoming increasingly difficult to remove.

In addition to Trojans, Kindsight has also seen malware that attempts to 'root' the phone using a variety of exploits: making hidden copies of itself in system directories, installing executable binary files, deleting other applications and changing system file-access permissions. Although these techniques are not yet common, they are relatively simple to implement and can be expected to become more widespread in the next generation of malware.

Will History Repeat Itself?

In many ways, mobile Internet services are today where PC malware was in the 1990s:

- Mobile Internet services (including smartphones, tablets and EV-DO/3G/4G/LTE 'data sticks' that connect laptops to the mobile network) are relatively new.
- Financial apps (e.g., banking apps, mobile wallet services) are also very new.
- Very few people think of their mobile devices as needing the same kind of protection as their PCs.
- As mentioned above, some mobile platforms, such as Google Android, have exactly the same philosophy of openness and flexibility — and as a result, the same vulnerability — as Windows.

Combined, these elements provide fertile ground for a criminal element that, unlike in the early days of PC malware, already has years of successful identity theft and DDoS attack experience in the PC domain on which to build.

Many observers are quick to note that the infection rate among Android devices is just 0.1 percent (i.e., one in 1,000 devices), which is miniscule compared to the 15 – 20 percent infection rates in home networks seen over the course of a typical month.

But mobile malware is undeniably following a similar — and maybe even more aggressive — growth trajectory. Within a few years, the rapid exploitation of various infection techniques will make malware as problematic on mobile devices as it is on PCs — and because mobile operators are also subject to Windows-based malware coming from PCs tethered to smartphones or connected via mobile Internet (3G/LTE) sticks, malware presents a significant risk that cannot be ignored.

WHAT ARE THE CONSEQUENCES?

How Malware Affects Subscribers

For wireline technologies, one of the biggest malware-related concerns is identity theft: a serious crime in which personal information, including banking and credit card details, is stolen and used without permission to commit fraud or a number of other crimes — often with devastating financial consequences. Because today's mobile malware is not quite as sophisticated as PC-based malware, it tends to focus on a lower level of identity theft: the stealing of contact lists and address books from mobile devices in order to send unsolicited SMS and email messages under the guise of the device owner. Not only is this an inconvenience to the people receiving these spam messages, it can also cost device owners money by racking up fees for data usage or the sending/receiving of premium SMS messages. (In fact, premium SMS messages are a major moneymaker for criminals and quite common in malware targeted at the Chinese and Russian markets.)

This approach may represent the beginning of an SMS spam market that could eventually rival the traditional email spam used in wireline networks. Kindsight has also seen malware that intercepts SMS messages and forwards the content to C&C servers — a development that has significant implications if combined with banking Trojans to steal one-time banking credentials transmitted via SMS.

How Malware Affects Mobile Operators

When a Trojan first infects a PC, smartphone or tablet, it creates an outbound connection to C&C sites on the web. The Trojan connection itself does not consume significant amounts of network resources; the C&C will check in with a short message on an infrequent basis (e.g., hourly or daily). However, after laying dormant for days, weeks or even months, the Trojan connection can be used to instruct the device to join a botnet where it begins to send large amounts of spam emails or SMS messages, or targets a DNS server for a DDoS attack — actions that can place considerable strain on network resources.

But malware doesn't just consume network resources (which can be somewhat difficult to quantify). Perhaps of greater concern is the time and money it costs to deal with malware infections. For example, mobile operators may have to deal with an increased number of calls to their customer care departments as subscribers report sub-par device performance due to infections consuming battery power, CPU or bandwidth. The number of calls to billing departments may also increase as subscribers notice unexpected data and SMS charges.

To protect their networks and their subscribers, many mobile operators attempt to block communication to known C&C sites through the use of firewalls, DNS servers or policy engines on routers. Criminals, however, have developed a number of ways to counter these efforts. Some malware has very sophisticated methods of contacting a variety of different C&C sites, and criminals often stay on the move, constantly directing devices under their control to new C&Cs.

Compounding the problem is the fact that technologies used to block traffic are typically deployed at the Internet gateway — often at the last device before delivery of traffic to the public Internet. As such, network resources on the operator's side of the blocking (e.g., radio access network, backhaul bandwidth, routing and AAA infrastructure) may continue to suffer from the utilization of malware on infected devices.

STRATEGIES FOR TAKING ON MOBILE MALWARE

In the infancy of malware, network operators relied on blacklists of IP addresses, domains and URLs known to be the C&C head-ends for malware. Based on this information, inline policy engines and web filtering platforms would be used to attempt to block communication to known malware sites. Although this is an important layer of the overall response to malware, it has proven to be insufficient in recent years:

- Criminals have developed sophisticated methods for changing the C&C head-ends of their malware, meaning that blacklists become obsolete within days, even hours.
- Criminals have found ways to control malware from reputable sites and domains, making it increasingly difficult for web filtering and policy engines to distinguish between 'good' and 'bad' traffic. As a result, blocking can inadvertently impact authentic traffic, much to the dismay of subscribers looking to conduct legitimate communication with websites and portals that have malware affecting only a portion of the site. This is also a well-known approach to inflicting DDoS attacks — by making legitimate websites look like C&C head-ends, criminals can damage the reputations of these sites by having network operators block access to them.

The enterprise world provides a good example of the type of two-pronged strategy needed to combat malware effectively. In corporate environments, both the network and the device are protected: the network via intrusion detection/prevention appliances, firewalls and policy-based controls on the types of traffic allowed in and out; and client devices primarily with anti-virus/anti-malware applications. The two modes of protection work in concert — and a similar approach is required for mobile networks, where operators are in fact ideally positioned to offer both. (For more, see sidebar.)

Yet despite the advancing sophistication of today's malware, many mobile operators continue to be virtually blind to the full extent of the problem within their networks — they simply react to incidents as they occur and have no proactive processes in place to address malware. As more and more applications come to mobile networks, this reactive approach becomes increasingly risky — and will ultimately result in service issues, outages and lost customers.

To develop effective, proactive policies for addressing malware, mobile operators must first measure the problem to be able to answer questions such as:

- How many subscribers are infected?
- What are the most serious infections?
- Which devices are most/least infected?
- How do these infections impact the subscriber and the network?

Based on this information, a mobile operator's response to malware may fall into two main categories:

- Network actions
- Subscriber notification

DEVICE-BASED VS. NETWORK-BASED MALWARE DETECTION/ REMEDIATION

Client-based anti-virus software is an important element of any approach to online security. Unfortunately, most mobile device do not have a security app installed – and if we look at what happened in the PC world many do not keep it up to date or purposely turn it off due to a negative impact on application performance.

For an 'always-on' solution that cannot be disabled and is constantly aware of the latest threats, mobile operators should complement client-based security with a network-based approach – an additional layer of protection that detects malware communications, such as C&C protocols, within network traffic.

Ideally, device-based and network-based solutions would work with and strengthen each other – for example, network-based detection could send an alert to device-based app if it detected an attack missed by the app and have it remove the malware.

For more information about networkbased security, please refer to Kindsight's white paper, *The Case for Network-based Malware Detection: The Need for an Additional Layer of Protection.*

Network Actions

Block

Through the use of web-filtering platforms or by changing firewall rules, mobile operators can respond to malware by blocking all or a portion of traffic from or to a specific IP address, domain or URL. Blocking is considered to be a non-real-time response to malware; operations staff assesses the recommended blocking action and typically implements it manually rather than automatically.

Quarantine

In this approach (which is currently more common in wireline networks than mobile networks), severely infected subscribers are placed in a 'walled garden', which effectively disables their access to the public Internet. The only webpage a quarantined subscriber can access is a captive portal — a page internal to the operator's network that informs the subscriber of his/her suspended service status and provides instructions on how to remove the infection.

Quarantining the subscriber in a walled garden is an excellent way to remove malware traffic from the network and to protect the subscriber from identity theft attacks. However, some subscribers — especially those who do not understand the risk infections pose to their personal data — will find it a severe inconvenience to be placed in a walled garden. Despite the potential of protection, a walled garden can lead to a negative subscriber response; as a result, this service option must be implemented carefully.

Subscriber Notification

Different forms of malware represent different levels of risk to subscribers and to the network. But should subscribers be informed of all instances of malware detected in the network, regardless of the threat they pose? The strategy for notification depends on the operator's processes and services for remediation. For mobile operators, a range of notification options can be considered:

- **Provide no notification:** The nature of the subscriber base and devices connected to the network may be such that a specific response to malware is not required in the short term. However, the mobile operator will continue to monitor the infection rate to see when (not if) that status changes.
- **Manually contact infected subscribers:** Some mobile operators will choose to manually contact a small number of subscribers with the most serious infections. In these instances, customer care staff may decide to disable a subscriber's service until the infection is addressed, inform the subscriber of the infections observed, and offer assistance to address the infection. Forms of notification may include phone calls, automated voicemails, emails, SMS messages or interstitial messages (i.e., inserting a screen featuring an alert message before allowing the subscriber to view his/her intended webpage).
- **Automatically contact infected subscribers:** When a new infection has been identified, the mobile operator's security service can be configured to automatically notify the subscriber of the issue via email, SMS or mobile app. This is an effective option when the operator already has well-defined remediation services to follow the notification.

MOBILE SECURITY AS A VALUE-ADDED SERVICE

Many technologies and processes can be used to protect the mobile network and subscribers from malware — all of which must come at a cost to the mobile operator. This means there are some business decisions to be made vis-a-vis the cost-benefit analysis of managing the risk/impact of malware and the extent to which subscribers should fund malware detection, notification and remediation.

Market research and evidence from Kindsight deployments find that consumers value an additional layer of protection — and are willing pay a few dollars each month for it. Offering mobile security as a fee-based service does make it a more complex solution to implement and maintain (for example, due to the processes required to enable subscribers to order the service, or the coordination of billing for it). However, eliminating the impact of malware on the mobile network through this additional layer of protection has significant value for the consumer — and leveraging this opportunity makes perfect sense for mobile operators.

In addition to implementing mobile security as a fee-based service, operators can utilize creative financing mechanisms to generate revenue while providing value to their subscribers — for example, by providing mobile security to subscribers at no cost if they opt in to relevant advertising.

Some operators consider mobile security to be a substantial differentiator over their competitors, choosing to forego the opportunity to generate fee-based revenue or ad monetization in exchange for market differentiation and leadership.

Whether delivered on a paid or no-cost basis, an effective remediation service should include some of the following elements:

- Self-service, step-by-step instructions on removing the malware
- Easy-to-use tools known to be effective in removing specific malware infections
- Options for telephone/email/chat support with technicians who can help the subscriber through remediation
- Options for subscribers to take their smartphones to the mobile operator's stores to get assistance, swap for an uninfected device, etc.

ADDRESSING THE MOBILE OPERATOR'S NEW REALITY

With the number of infected Android devices climbing quickly over the second half of 2011, mobile operators need to realize that malware is no longer a problem exclusive to the PC domain. Exponentially more sophisticated than the harmless worms that first appeared on phones in 2004, today's malware not only compromises subscribers' personal and financial data but also ties up network resources and costs mobile operators considerable time and money.

Developing effective strategies to combat mobile malware requires operators to first measure and fully understand the extent of the problem. They have to choose either to monetize these actions — through monthly subscription fees or bundling with other services — or keep them free as a competitive differentiator. Regardless of which is chosen, remediation efforts should be easy to use and provide several options to help subscribers remove malware from their devices.

ABOUT KINDSIGHT SECURITY LABS

Kindsight Security Labs focuses on the behavior of malware communications to develop network signatures that specifically and positively detect current threats. This approach enables the detection of malware in the service provider network and the signatures developed form the foundation of Kindsight Security Analytics, Kindsight Broadband Security and Kindsight Mobile Security solutions.

To accurately detect that a user is infected, our signature set looks for network behavior that provides unequivocal evidence of infection coming from the user's computer. This includes:

- Malware command and control (C&C) communications
- Backdoor connections
- Attempts to infect others (e.g. exploits)
- Excessive e-mail
- Denial of Service (DoS) and hacking activity

There are four main activities that support our signature development and verification process.

1. Monitor information sources from major security vendors and maintain a database of currently active threats.
2. Collect malware samples (> 10,000/day), classify and correlate them against the threat database.
3. Execute samples matching the top threats in a sandbox environment and compare against our current signature set.
4. Conduct a detailed analysis of the malware's behavior and build new signatures if a sample fails to trigger a signature

As an active member of the security community, Kindsight Security Labs also shares this research by publishing a list of actual threats detected and the top emerging threats on the Internet and this report.

Kindsight is a network-based security product line within Alcatel-Lucent's Platform Business. The Kindsight portfolio enables Internet service providers and mobile network operators to detect threats, send alerts, block infected devices and protect subscribers. It also analyzes Internet traffic for malware and pinpoints infected devices to identify risks and take action. To generate revenue and increase brand loyalty, Kindsight also enables communication providers to launch differentiated, value-added services that combine network-based and device-based security for complete protection.

Alcatel·Lucent