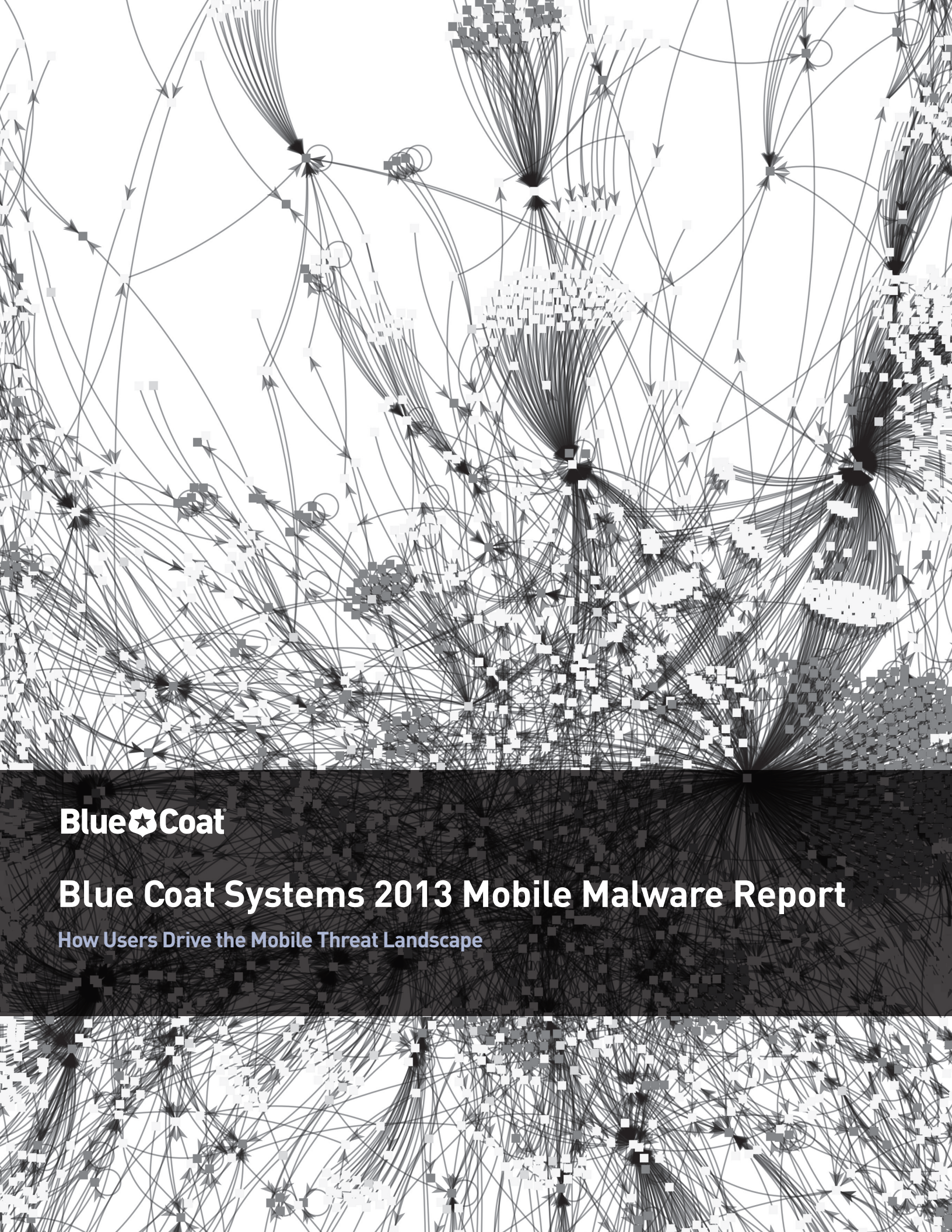


Blue Coat

Blue Coat Systems 2013 Mobile Malware Report

How Users Drive the Mobile Threat Landscape

Table of Contents

Summary of Key Findings

Mobile users are transforming the scope and volume of human interactions globally. This transformation is enabled by the ubiquity of mobile devices, unprecedented access to the Internet from virtually any location and a growing wealth of mobile applications.

Mobile devices in the enterprise represent the confluence of personal and corporate needs and usage. Businesses are challenged to keep pace with the proliferation of mobile devices and maintain control over them as they strain the boundaries of corporate control.

The unfettered growth in mobility has also created an alluring opportunity for cybercriminals to generate profits through mobile malware. This report examines the mobile threat landscape and the behavioral patterns of mobile users that make them most vulnerable to data loss, malicious applications, fraud and other mobile threats.

Data in this report comes from the Blue Coat WebPulse collaborative defense and the Blue Coat Security Labs. WebPulse analyzes requests in real-time from 75 million users worldwide to gain a comprehensive view of the web and malware ecosystems. By tracking malnets, WebPulse also delivers the industry's only Negative Day Defense.

Key Takeaways:

1. Mobile threats are still largely mischiefware – they have not yet broken the device's security model but are instead more focused on for-pay texting scams or stealing personal information.
2. The most successful mobile malware tactics, including scams, spam and phishing, are classics that dominated the threat landscape when malware first moved to the web. These device-agnostic, easy-to-deploy attacks provide a natural crossover point for cybercriminals that are interested in launching attacks against mobile devices.
3. Pornography is proving to be the great weakness for mobile users. While mobile users don't go to pornography sites often, when they do, the risk of finding malicious content is nearly three times as high as any other behavior.
4. While relatively small compared to desktops threats, the mobile threat landscape is becoming active. Malnets, the infrastructures that successfully drove nearly two thirds of all web-based attacks in 2012, are setting their sights on mobile users. To date, 40 percent of mobile malware blocked by WebPulse has originated from known malnets.
5. Extending security to mobile devices will be essential for businesses that need to protect their assets as well as their employees. Cybercriminals see the value in these targets as businesses continue to adopt BYOD initiatives, and businesses need to be prepared in 2013.

Understanding the Mobile Threat Landscape

In 2012, mobile threats were a relatively small but growing percentage of overall traffic. The threat landscape was marked by a resurgence of classic scams attempting to convince users to enter sensitive information into a website that replicates a bank's website, for instance.

Malicious applications typify another sort of risk for mobile devices. These applications often exhibit malicious behavior such as texting to "for-pay" services run by the attacker or in-app purchases. Collectively, these threats don't break the security model of the phone but simply act in a manner in which they were expected to perform, albeit, for malicious reasons. They are really more mischiefware than malware.

Figure 1: Leading Mobile Threats

Malnets (malware networks) are distributed infrastructures within the Internet that are built, managed and maintained by cybercriminals for the purpose of launching on-going attacks against users over extended periods of time.

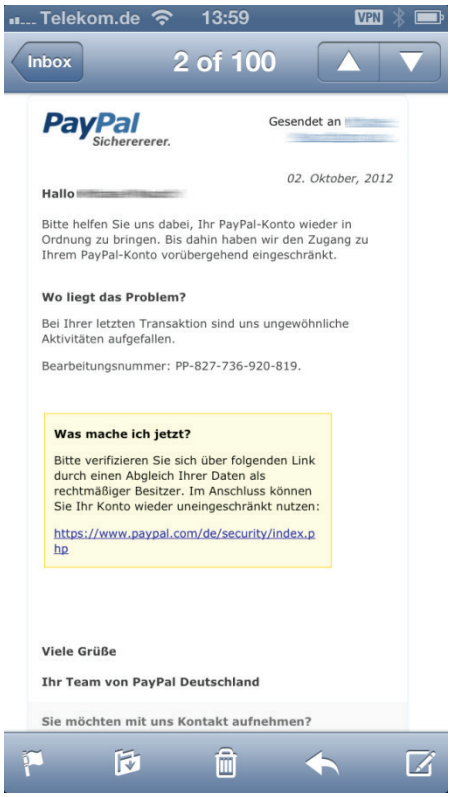
Mobile malware that truly breaks the security model of the phone is still in its infancy with little evidence of attacks beyond a few incidents that targeted the Android platform (see Targeting Android Platforms section later in the report).

In 2013, this is likely to change as adoption of mobile devices continues to grow rapidly and businesses increasingly provide access to corporate assets. According to the IDG Global Mobility Study, 70 percent of employees surveyed access the corporate network using a personally owned smartphone or tablet. This access extends to business-critical applications as well. For example, 80 percent of employees access email from their personal devices.

In the desktop world, cybercriminals can purchase exploit kits on the underground market and utilize malnet infrastructures to continually launch malware attacks on users. For mobile devices, however, weaponized exploit kits are not yet as common as exploits targeting desktop and laptop computers. However, established techniques such as pornography, spam and phishing that have worked well in the desktop world are now successfully migrating to the mobile world.

Many of these tactics are device agnostic, so expanding the attack to target mobile devices is relatively simple. Phishing, scams and spam target users on all devices in an effort to convince users to provide credentials or other confidential information, such as credit card information.

A recent phishing attack demonstrates how easy it is to be tricked into providing credentials on a mobile device. In the attack, a user received a perfectly formatted, grammatically correct phishing email informing them that Paypal had detected suspicious activity during the user's last transaction. The email went on to say that PayPal had temporarily blocked the account until the user verified the account by clicking on a link.



This is a classic phishing attack. After clicking the link in the email, the user would have been sent to a webpage that is an exact replica of the PayPal credentials page. The only exception was that the actual URL behind the link in the email did not take the user to PayPal.

Mobile Risks: Setting users up for failure

Mobile devices have empowered users, giving them access to a wealth of information and corporate assets from anywhere. Yet, we haven't put in place the tools and practices that will allow them to make good, safe choices. Essentially, we have set them up to fail.

When we think about security under the lens of mobile devices, some risks decrease, some increase and some stay the same. For example, consider the increased risk of your password being exposed to an onlooker. Mobile phones often reverse the years-long practice of instantly masking passwords when you type them in – these devices typically expose the password, character by character, to ensure your entry is correct.

It is also often harder to make good choices about the links you visit on a mobile device. Many times these links are truncated or shortened via a service such as bitly, which impedes a user's ability to make a good decision about their destination.

In the phishing attack, a user wouldn't be able to hover over the link in the email and see the true URL address. If they clicked on the link, they wouldn't see the fully resolved link in the address bar either. Further complicating the matter is behavioral conditioning. Users are taught to expect mobile websites to look different than the desktop versions. This gives attackers the ability to prey on that perception difference and craft a fake mobile site at a strange URL for an established company.

Another important difference between desktop and mobile environments is that mobile versions of websites are often crafted and hosted by third parties. For the user, that means the URL might not even be a good indicator of the relative safety of the site. Accessing the website for Hilton Hotels from your mobile device, for example, redirects you to usable.net. This practice essentially conditions customers to be comfortable with going to a strange URL to find an official site and gives attackers an edge they can potentially leverage to deceive mobile users.

Mobile applications themselves also provide a point at which it is difficult for customers to make safe, well-informed decisions. In its current state, the most popular mobile applications are produced by companies with which most users are unfamiliar. If a piece of software makes it to the shelves of Best Buy, consumers perceive that both the software and the company that designed it have been vetted. In the mobile app world, new players emerge constantly with no reputation in areas like security quality. Nor is there a good mechanism for creating reputation ratings. Already, this is resulting in applications that send unencrypted personal data over open networks or collect too much personal information.

.

Behavioral Patterns of Mobile Users

To understand mobile risks, it's critical to look at the behavioral patterns of how these devices are used. On average, a user spends 72 minutes a day browsing the mobile web. This is independent of the time spent using native applications and represents the time when users are most vulnerable to threats.

During that time, users are spending more than 11 minutes with content related to computers/Internet. The remaining 60 minutes are spent looking at a variety of content, ranging from social networking and shopping to business/economy and entertainment. The diversity of topics that comprise a user's day on the web demonstrates how important mobile devices have become. By effectively putting a computer in the hands of user, mobile devices have given them access to any information from any location.

That will have security implications.

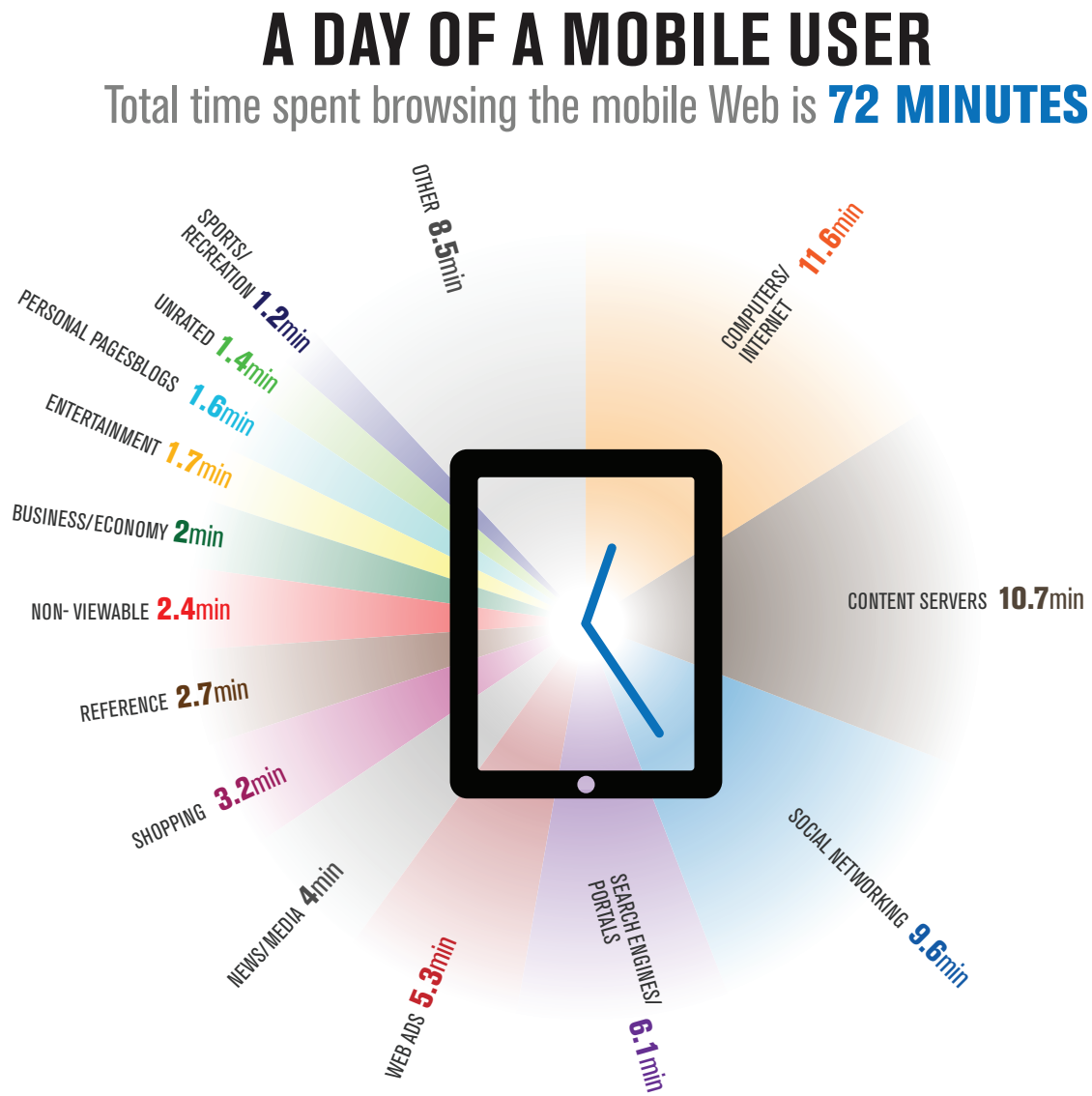


Figure 2: Where Mobile Users Spend Their Time

For mobile users, the patterns we observed in 2012 show a marked difference from the patterns of desktop users and point to the ways in which behavior can be exploited by cybercriminals.

For most users, mobile devices are a personal experience. Users access much more recreational content, including shopping, entertainment and personal pages/blogs, from their mobile devices than desktops or laptops. In fact, the percentage of requests for recreational content was twice as high for mobile users.

Likewise, news/media was one of the most popular categories of content requested from mobile devices. Social networking also continued to rank slightly higher for mobile users versus desktop users, as first noted in the Blue Coat Systems 2012 Web Security Report, which is interesting given the predominance of native mobile applications for social networking sites.

KEY CONTRASTS: MOBILE VS. DESKTOP USAGE

Differences in Device Purpose Drive Priorities in Web Use

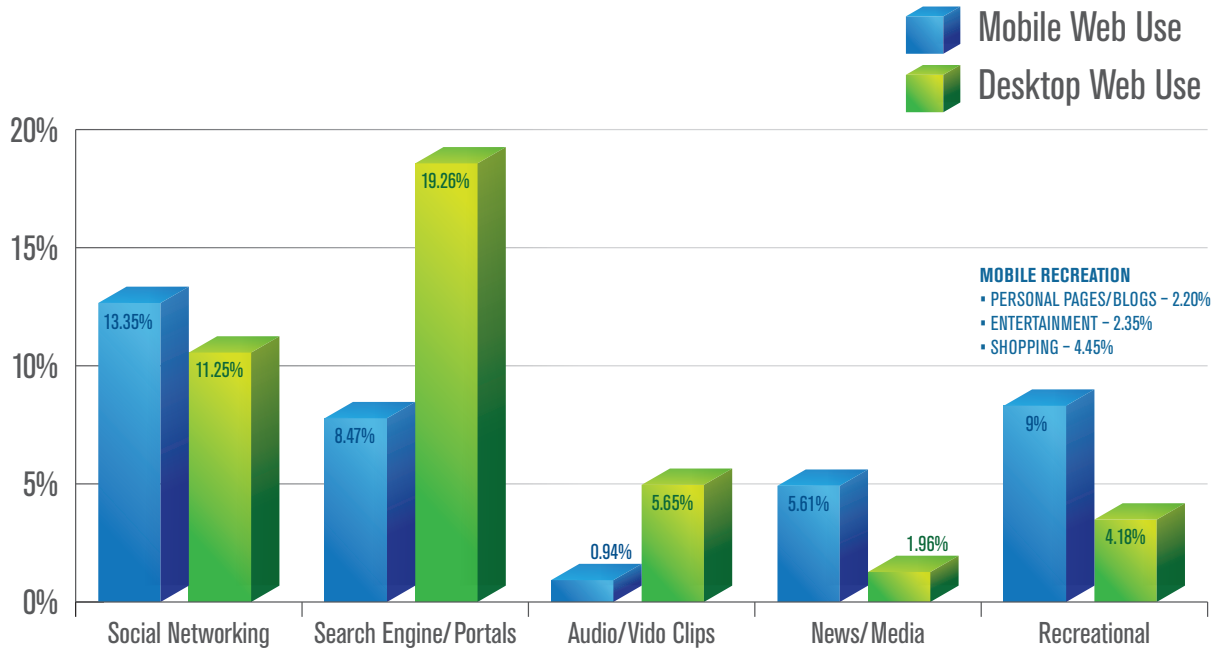


Figure 3: Most Requested Categories: Mobile vs. Desktop Users

Among the most noticeable difference between user behavior occurs within search engines/portals. Desktop users use search engines twice as much as mobile users. For mobile users, search engines ranked as the fourth most requested category of content.

This difference points to less reliance on search engines by users on mobile devices. Mobile users look for rapid access to information they need, often going directly to a source rather than waiting for search results. Additionally, the availability of native apps changes the search dynamic on mobile devices, making it easier to access the applications and features that are most important.

The high use of search engines by desktop users has driven a correlation in threat vectors, with search engine poisoning consistently ranking as the leading entry point to malware. As the mobile malware ecosystem expands, cybercriminals will likely be less inclined to spend the same level of resources targeting mobile users through search engines.

Users also favor desktops over mobile devices for audio/video content by an overwhelming margin. For desktop users, audio/video content is the sixth most requested category of content, representing more than five percent of all requests, and growing steadily. Conversely, requests for audio/video content from mobile users accounted for just one percent of all requests. The small screen impacts user experience while the lack of Flash support on some devices limits the audience for this type of content.

The uniform demand for a quality experience regardless of platform type is creating a bifurcation in the application market. Today, users will move between web, mobile web and native mobile applications, depending on which can best meet their experience expectations. For example, users are clearly opting to use web or native mobile applications to access audio/video content. These applications optimize their experience better than mobile web versions.

The search for the optimal user experience continues to condition users and extends to the use of corporate applications on mobile devices. As organizations introduce corporate app stores to better manage the applications on their network, user experience will be a key driver of adoption.

From a security perspective, users will tend to go with the application that provides the best user experience even if it is not the most secure option. For example, most organizations set size limits on email attachments. An employee facing these limits would be forced to split a large file into two different attachments, requiring effort on the part of the sender and the receiver, who would then need to piece the two files together. Alternatively, the employee could upload the file to Box.com and just send out a link. This option is not necessarily the most secure and might even violate compliance to relevant regulations.

By not paying attention to the user experience, organizations can inadvertently create security gaps.

Best Practices

Close the mobile app gap on your network. Make sure that you can see and consistently enforce policy across all three types of applications (and their operations) that may be running on your network:

1. Web applications (desktop browser)
2. Mobile web applications (mobile browser)
3. Native mobile applications

As you adopt BYOD initiatives and allow employees to access corporate assets with their own devices, be sure these controls extend to those devices as well.

Mobile Threat Vectors: User Behavior Becomes the Achilles Heel

Mobile user behavior creates opportunities for cybercriminals to lure users to malware by leveraging popular categories of content. Protecting users that are vulnerable to manipulation or behavioral exploitation can be challenging without understanding where they are most at risk. These threat vectors are driven by user choices or behavior and are designed to lead mobile users to malware. While many threat vectors correlate directly to high usage categories, there are some interesting exceptions.

In 2012, the most dangerous place for mobile users was pornography. More than 20 percent of the time that a user went to a malicious site, they were coming from a pornography site. It is important to note that mobile users are going to pornography sites less than one percent of the time. When they do visit pornography sites, though, they have a high risk of finding a threat.

Interestingly, when malware first moved to the Internet, pornography was one of the leading sources of malware for desktop users. The prevalence of pornography as the leading threat vector for desktop users has ebbed, giving way to attacks that target much larger user populations, such as search engine poisoning.

In the desktop environment, pornography continued to fall as a threat vector as it became easier to target a large number of users on places like search engines or social networking sites. It is reasonable to expect that the same will be true for the mobile environment, especially considering that in both environments pornography is not a frequently requested category of content.

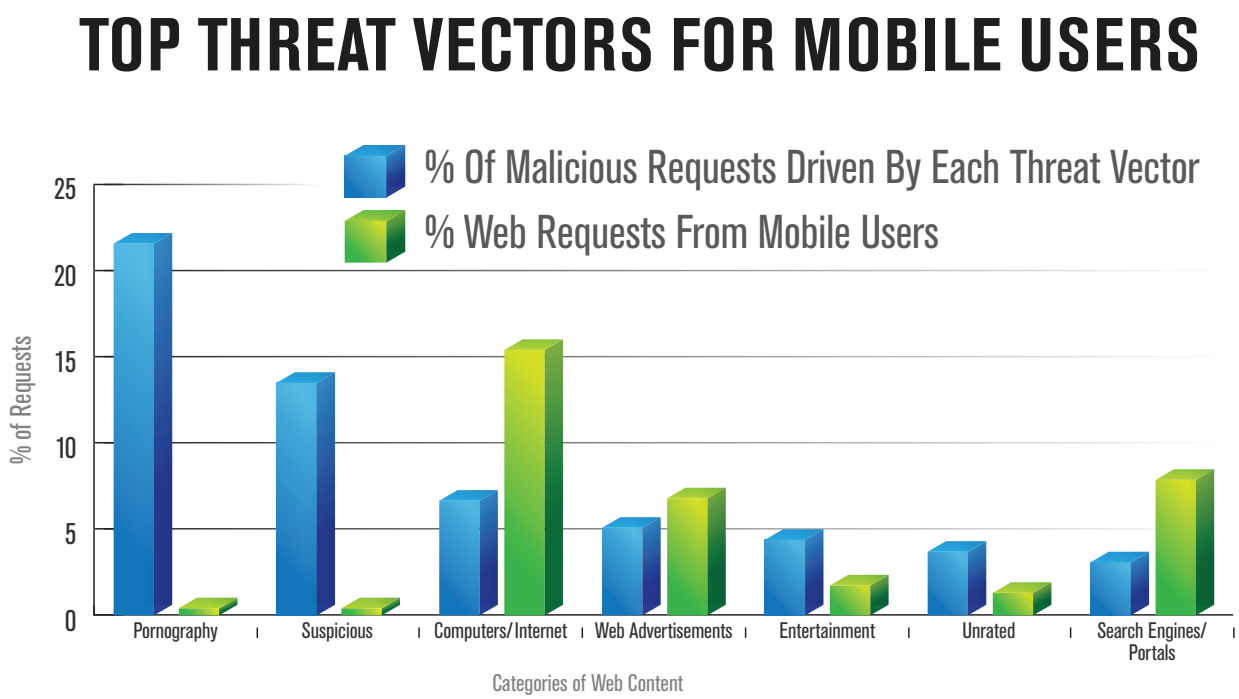


Figure 4: Percent of Malicious Requests Driven by Each Category Compared to Requests for Content in that Category

The second most popular entry point into malware was through sites categorized as suspicious. These typically include sites that are part of the Web and email spam ecosystem and aren't hosting or otherwise more explicitly linked to a malicious site.

With users spending the most amount of their mobile web browsing time accessing computers/Internet content, it's not surprising that this content is also a leading threat vector, responsible for more than seven percent of all malicious requests from mobile devices. Many of the early successful mobile malware attacks offered users an Android version of Skype or an Opera browser. This category of content, which includes sites that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies, is also frequently requested by desktop users though, as a threat vector, it is not as popular.

Web advertisements are an interesting case. They rank as both the fourth most requested category of content as well as the fourth ranked threat vector for mobile users, demonstrating that both the ad-based revenue model and malvertising attack methodology have transitioned to the mobile web nicely. Cybercriminals have been refining malvertising attacks against desktop users for several years, and it consistently appears as a top threat vector.

Mobile users who shop or conduct online banking on their smartphones are important targets for both commercial businesses and malware operators. The volume of web advertisements that are delivered through these mobile applications creates an effective entry point for cybercriminals to inject ads that lead to malicious downloads. A recent example was an advertisement for a fake Angry Birds download. The download delivered an SMS Trojan that made premium SMS calls (texts) to the malware host, which then billed users without their knowledge.

Other similar tactics involve presenting fake downloads such as PDFs, browser updates or executable files that then deliver malicious payloads designed to steal personal information and other assets.

Figure 5: Malicious Ad Serving Malware Disguised as a PDF Download

Given the success of the model in desktop environments and the seemingly successful transition to mobile environments, it is reasonable to expect malvertising will continue to be a key threat vector.

Note that social networking is absent as a mobile threat vector, despite being the third most requested category of content. One explanation is that some social networks deploy separate and distinct mobile and web-based applications. For example, the Yammer mobile application has a different URL than the web-based version. Users of social networking mobile apps are also less likely to click on links people send because it is more disruptive than opening the link in a new tab of a desktop browser.

While search engine poisoning (SEP) is a top threat tactic against desktop users, the vector will likely remain low on the list for mobile devices as long as mobile search usage remains at its current level.

Mobile Malware Tactics

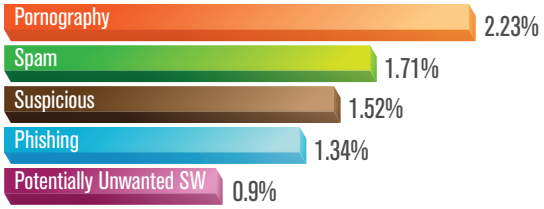
Behavioral information provides insight into where users might be targeted and the threat vectors show where they are most successfully being targeted at any given point. The tactics will now show how they are targeted.

While spam was the second highest "malicious" category of requested content, it was not an efficient tactic. Mobile devices represented 1.71 percent of all requests for spam content yet 4.39 percent of all spam websites were targeting mobile devices.

TARGETING THE MOBILE USER

CLASSIC THREATS FIND SUCCESS WITH MOBILE USERS

PERCENTAGE OF REQUESTS FROM MOBILE DEVICES TO MALICIOUS CATEGORIES



PERCENTAGE OF UNIQUE SITES REQUESTED BY MOBILE DEVICES

SPAM	4.39%
PORNOGRAPHY	3.8%
PROXY AVOIDANCE	1.2%
SUSPICIOUS	0.98%
MALICIOUS SOURCES	0.78%
PHISHING	0.77%
POTENTIALLY UNWANTED SW	0.46%

Figure 6: Relative Effectiveness of Tactics

Spam, by its nature, uses many domain names in an effort to avoid detection. In 2012, cybercriminals cycled through more than 2.5 domains for every successful attack. This high work to return ratio is in contrast to the more efficient phishing attacks.

Phishing as a tactic is a more productive method that uses fewer websites to attract a relatively larger amount of traffic. Mobile devices accounted for 1.34 percent of all phishing requests, yet only 0.77 percent of all phishing sites are targeting mobile users exclusively. This data indicate that phishing attacks on mobile devices are much more effective at driving users to their sites.

Given this dynamic, you could reasonably assume that there would be a spike in phishing attacks. However, the presence of malnets is the great equalizer. By leveraging an existing infrastructure, cybercriminals can easily change domain names for any one attack while leaving the rest of the attack path in place. This has the effect of making spam attacks relatively easy to launch and sustain despite its seemingly low rate of return.

Best Practices

- Block all content to mobile and desktop devices from dangerous categories, including pornography, phishing and spam.
- Block executable content from un-rated domains and categories that typically host malware, such as Dynamic DNS hosts.

Targeting Android Platforms

Android devices offer a unique case study on the rise of mobile malware. The unregulated app market and diversity of Android-based devices ensures that cybercriminals will find greater success targeting these platforms.

Blue Coat WebPulse collaborative defense first detected an Android exploit in real time on February 5, 2009. Since then, Blue Coat Security Labs has observed a steady increase in Android malware. In the July-September 2012 quarter alone, Blue Coat Security Labs saw a 600 percent increase in Android malware over the same period last year.

In June 2012, requests to malware targeting Android devices reached more than 1,000. While requests ebbed and flowed over the course of a 12-month period, one thing is clear: Cybercriminals are launching more threats and becoming more efficient at driving users to those threats. Prior to a period of heightened activity in May and June, the highest volume of threat activity was in November 2011, peaking at just over 500 threats for the month.

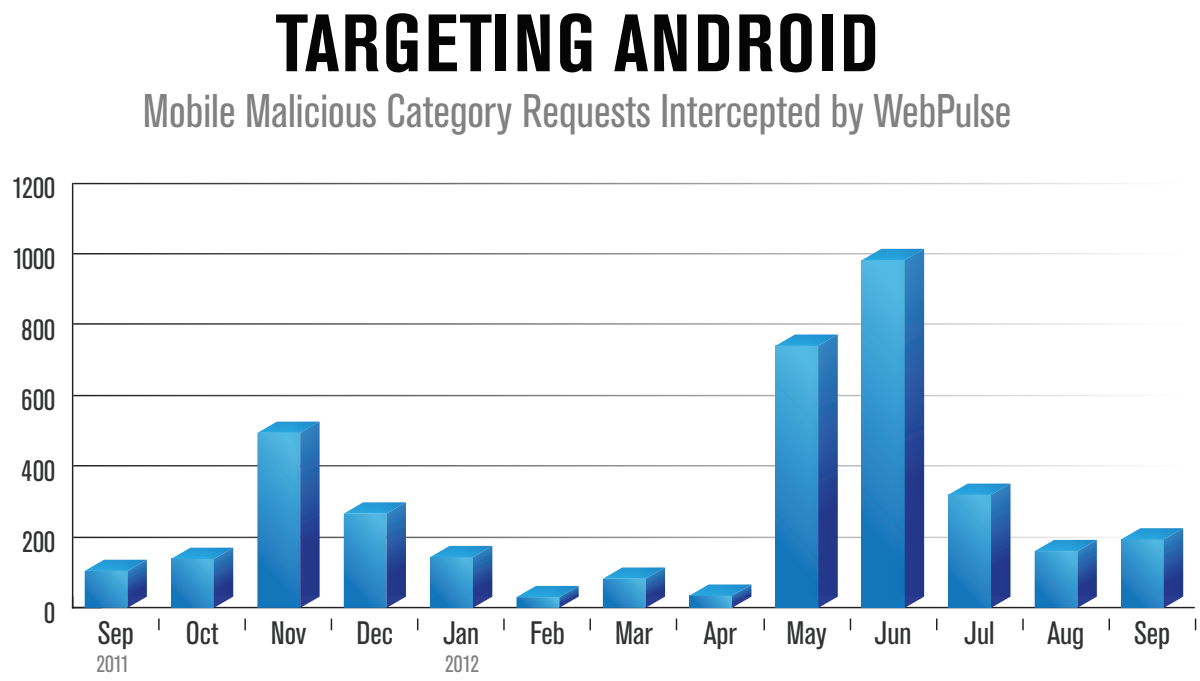


Figure 7: Volume of Requests for Android Malware

The Android-based malware blocked by WebPulse included an Android root exploit and a variety of rogue Android software. Forty percent of Android malware was delivered via malnets, demonstrating how cybercriminals can successfully utilize embedded infrastructures to attack mobile users. In the most recent six months, WebPulse also blocked an increasing number of unique malicious Android applications.

BREAKDOWN OF ANDROID MALWARE BLOCKED BY WEBPULSE IN 2012

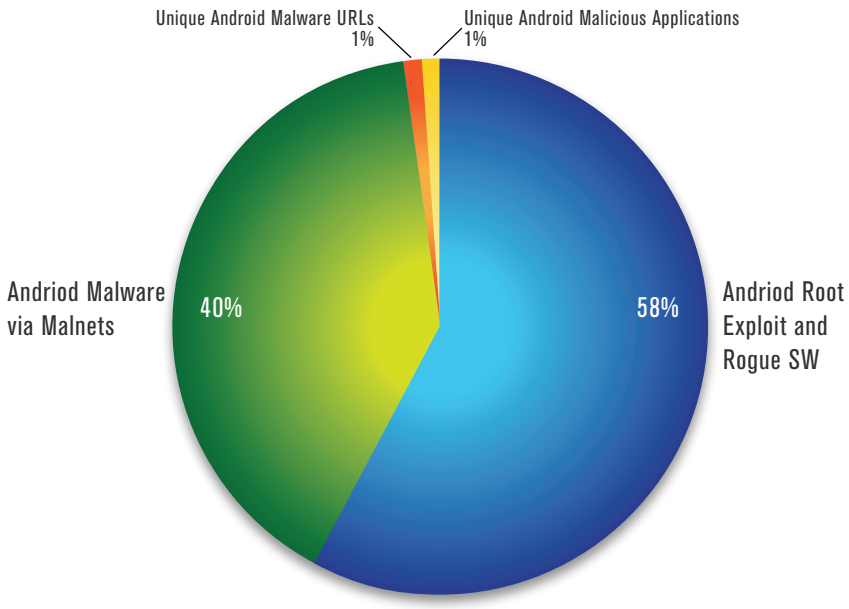


Figure 8: Android Malware Blocked by WebPulse in 2012

Best Practices: Protect Your Users and Business from Mobile Malware

- Only download mobile applications only from trusted sources.
- Extend the same threat protection in your corporate network to mobile devices in any location.
- Enforce use of trusted applications with granular native and mobile web application controls.

Delivering Mobile Malware with Malnets

Malnets revolutionized the way cybercriminals deliver malware attacks to desktop and laptop users. In 2012, they set their sights on mobile devices.

Malnet infrastructures are embedded in the Internet. They are such a powerful tool for cybercrime because they are always there, ready to be used in any attack, and are extremely adaptable. With these infrastructures, cybercriminals can launch ongoing attacks on users, targeting wide swaths of users with very little effort. Read more on malnets in the Blue Coat Systems 2012 Malnet Report.

Cybercrime organizations spent 2012 tuning malnets to require low investment and deliver high impact results. This same strategy is now being extended to mobile devices for further financial gain. This is a significant shift that will rapidly increase attacks on mobile devices.

Prior to 2012, mobile-specific attacks launched from malnets consisted primarily of malicious Java apps. Malnet components serving malicious Android apps first appeared in October 2011. It wasn't until February 2012, though, that malnets targeting mobile users showed real activity. That month, Blue Coat Security Labs saw not only a significant surge in mobile malware but the adoption of classic evasion techniques as well.

The impact of this shift has been noticeable. Since early 2012, cybercriminals have expanded their infrastructure to launch attacks on mobile devices. In 2012, mobile traffic to malnets increased to two percent of overall malnet traffic. This growth is further evidence that mobile malware is poised to make an impact in 2013.

The growth in requests to malnets from mobile devices was driven by eight unique malnets in 2012. Three of the malnets, Narid, Devox and Criban, targeted mobile devices exclusively while the others simply expanded their malicious activities to include mobile devices. Narid and Devox are no longer active malnets. Criban continues to show a low level of activity with 83 new hosts over the past year. The maximum number of hosts used in a given day was 3.

THREE LARGEST MOBILE MALNETS

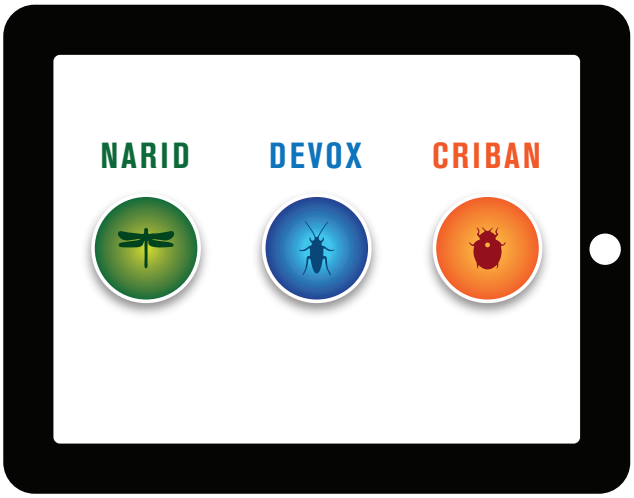


Figure 9: Leading Malnets Exclusively Targeting Mobile Devices

It is clear that in 2012, malnets were in an experimental phase of targeting mobile devices. They will continue to invest in their strategies, develop better tactics and show greater success in 2013.

Anatomy of a Mobile Malware Attack

In September, Blue Coat Security Labs examined an Android attack launched by a known malnet. In this particular attack, a user was offered an Android version of Skype via a website that lived on a shared web host with many other sites. There was nothing suspicious about the web host though the fact that the offer was delivered via a Russian website should have been an immediate red flag for users.

When a user clicked on the download button, they were relayed to a different website that was in a bad Internet "neighborhood" – one known to be associated with suspicious and malicious activities. The user was then relayed to another known suspicious site for the actual download.

At the time of this attack, the download was recognized by only 10 of the 41 anti-virus engines in Virustotal.

During the same week that this attack occurred, one of the mobile malware malnets used 38 domain names and another used 14 domain names for a variety of sites that were involved in attacks. Among the sites were two Flash update sites, four pornography sites, a movie site, a couple of browser sites and several general "file" and "app" sites.

The diversity of these concurrently running attacks shows that although mobile malware is in the early stages, it is clear it will continue to grow and become a problem for users as well as businesses that allow those users access to the corporate network.

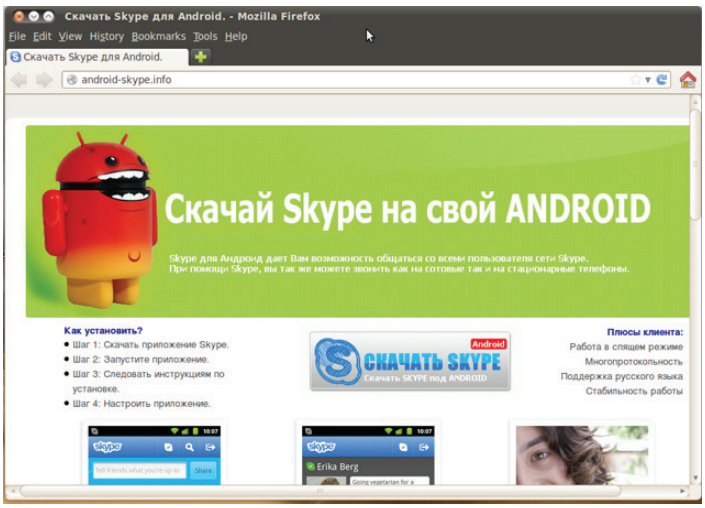


Figure 10: Malware Attack Offering Android Version of Skype

Summary

Mobile users represent a complex and growing constituency for organizations today. Those that can securely manage mobile devices can gain a competitive advantage by enabling their employees to be more productive. As businesses increasingly open their networks to mobile devices, cybercriminals will be knocking at the door. As we have seen in this report, they are already arming themselves for an attack.

Extending an enterprise-class web security solution to include mobile devices is a good first step towards protecting your employees. By closing the mobile security gap and enabling access to corporate assets with appropriate policy controls, businesses can proactively protect themselves against this evolving mobile threat landscape while capitalizing on the innovation and productivity of a mobile workforce.

Blue Coat Systems, Inc. • 1.866.30.BCOAT • +1.408.220.2200 Direct
+1.408.220.2250 Fax • www.bluecoat.com

v.BC-2013-MOBILE-MALNET-SECURITY-REPORT-V1D-0213