Paranoid Android: just how insecure is the most popular mobile platform?

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Network Security*

Sometimes it feels like we're reliving the 1990s. Google's Android platform has spawned an ecosystem inhabited by enthusiasts, geeks, hackers (in the good sense), consumers and business users all keen for the latest toys and entranced not only by the utility and attractiveness of the system but also by its openness and community atmosphere. However, just as with earlier versions of Windows, there's a dark element and its name is malware. In this first of three articles, to be run over successive months, we look at why this situation has come about and why Android has become a viable platform for cyber-criminals.

Popular platform

According to how you measure it, Android has moved ahead of iOS as the most popular smartphone platform in most territories. It generally lags way behind as far as tablets go – the iPad retains something of a stranglehold on that market – but significant numbers of Android tablets are being sold nonetheless. IDC figures from May 2012 give Android 59% of the worldwide market for smartphones against 23% for iOS.[1] And a number of online advertising companies have now positioned Android as the most-used smartphone platform worldwide. In July 2012, for example, Adfonic credited Android with 46% of ad impressions against 34% for iOS. More surprisingly, smartphone shipments are said to outstrip those of PCs.

It's no wonder, then, that mobile devices are increasingly the focus of cybercrime activity. There are plenty of figures around about how quickly malware on Android is increasing. None of the actual numbers – mostly from anti-malware vendors – precisely match, but they all paint the same worrying picture. So let's look at a few examples.

In its quarterly malware report, Kaspersky said that the number of malware programs trebled in Q2 2012, rising to 14,923. Nearly half (49%) of these were multi-function trojans capable of both stealing data and downloading new modules from Command and Control (C&C) servers. According to the 'Mobile Threat Report Q2 2012' from F-Secure, the firm received 5,033 previously unseen malicious Android files in the second quarter of 2012, most of them hosted on third-party app stores. That was an increase of 64% compared with the previous quarter.[3]

"There were 3.7 million phones infected in those six months. That is a substantial achievement for cyber-criminals"

This picture is echoed by other sources. Beijing-based security firm NetQin reported that mobile malware infections in the first half of 2012 were up 177% compared with the same period the previous year.[4] That could reflect the larger number of smartphones in use as much as any increase in the penetration of malware, but it still meant there were 3.7 million phones infected in those six months. That is a substantial

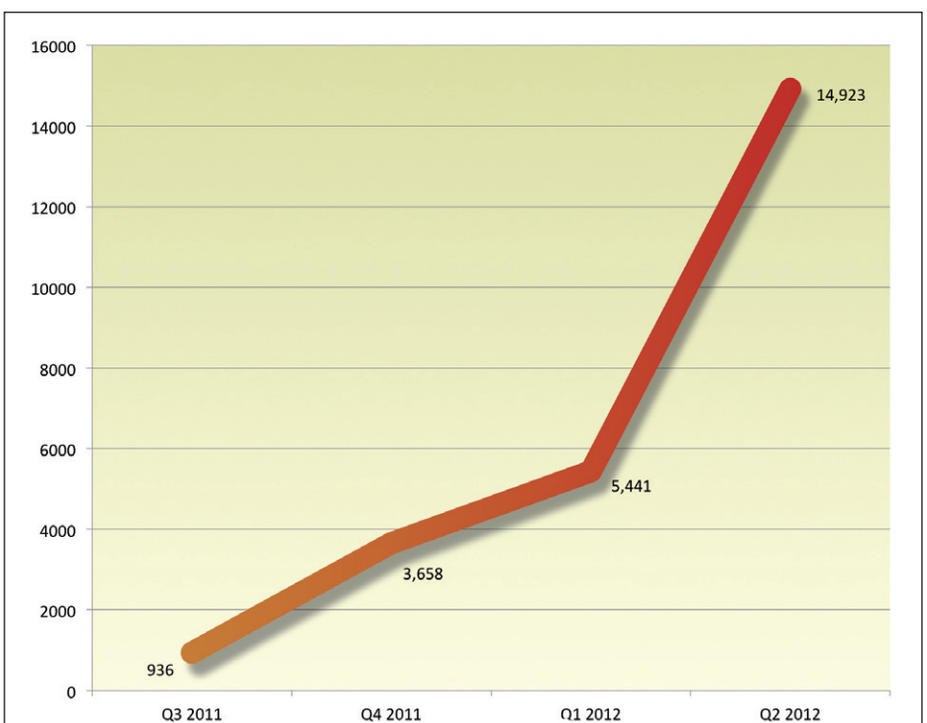


Figure 1: The second quarter of 2012 saw a tripling in the number of malware samples seen by Kaspersky.

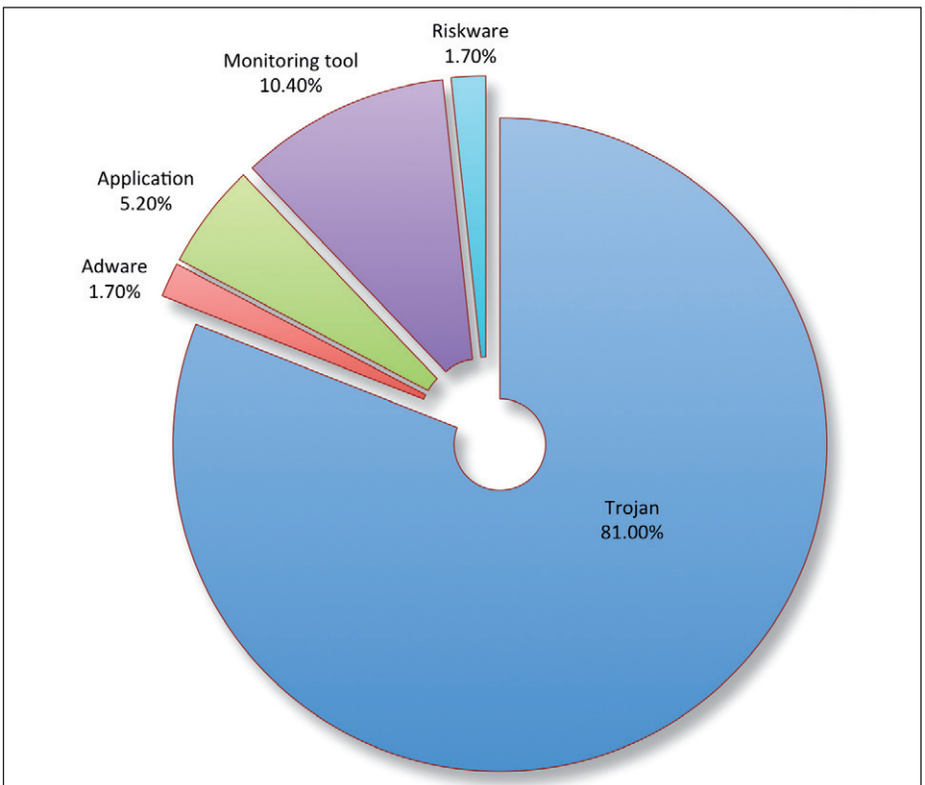


Figure 2: Mobile threats by type, Q2 2012. Source: F-Secure.

achievement for cyber-criminals, even if the percentage of devices that become infected remains the same (and there's no reason to suppose it will).

NetQuin also noted that, whereas in 2011, 60% of the malware was aimed at Symbian, in the first half of 2012, 78% of it was for Android. In its Q1 malware report for 2012, McAfee said that mobile malware is now "targeted almost solely at the Android platform", with the number of samples having jumped 1,200% compared with the previous quarter.[5] And to drive the point home, Juniper Networks' '2011 Mobile Threats Report' reported that while malware in general grew by 155% over the course of that year, Android malware jumped 3,325%.[6]

In July 2012, Trend Micro said it had seen Android malware being used for targeted (or so-called Advanced Persistent Threat, APT) attacks, as well as samples of malware with nascent Remote Access Trojan (RAT) capabilities.[7] These were found while monitoring a 'Luckycat' server, normally used as a C&C server for PC malware.[8] Trend had predicted that there would be 129,000 malicious apps for Android by the end of 2012, but later revised this upwards, to 250,000.

AVG Technologies' report for Q2 2012 noted a sharp increase in social engineering-based attacks targeting mobile users.[9] It's a phenomenon the firm had warned about in previous reports but, according to Yuval Ben-Itzhak, CTO, in the report's introduction: "The trend has only increased in the last three months with the prime target still the Android platform". He adds: "In our experience, a platform only needs to have 10% market share to become sufficiently worthwhile to malware authors so it's no surprise that Android is attractive. While mobile as an attack channel may not be as lucrative as the PC, in the future this is likely to change with the proliferation of connected mobile devices."

The rise in the number of smartphones and tablets in use makes this a target-rich environment for malware writers. That's likely to encourage more investment by cyber-criminals, with the potential for the emergence of a vicious spiral. Unquestionably, there's money to be made here. PhonepayPlus, the UK regulator responsible for premium-rate phone-paid services, has just levied a fine of £50,000 on a company that it says is responsible for placing malware on users' phones. Connect Ltd (trading as SMSBill) was also ordered to repay the costs incurred by users – estimated at £100,000-250,000 – when their phones starting sending premium-rate SMS messages. Given that Connect is based in Moscow, it remains to be seen whether it will pay up.

Comparisons to Apple

In any discussion of Android – and especially one that goes into technical detail – it's hard not to make comparisons with Apple's iOS platform for the iPhone and iPad. When held in public, such discussions quickly become almost religious in fervour. However, some comparisons are essential and illuminating because they show how the malware menace on Android is partly due to the philosophical and commercial approaches Google adopted in developing the platform. Android isn't entirely open, but it is far more accessible than iOS. It therefore appeals to those with hacker sensibilities.

"It's a platform that lends itself to hacking. While vendors may try to lock it down, it's trivially easy to eradicate vendor-loaded 'bloatware' and to gain full control by achieving root access"

A great deal of the security of the iOS platform stems from Apple's 'walled garden' approach. Only one manufacturer makes devices for this platform and there is no forking or fragmentation of the OS. A significantly high proportion of iOS devices have up-to-date versions of the OS because Apple makes it easy to do that and, indeed, applies pressure to do it. Apps can be downloaded only though the iTunes App Store, so they are all vetted and digitally signed by Apple. From a security standpoint, it works well. Unless, that is, you've 'jailbroken' your device. This allows you to obtain apps from third-party markets, such as Cydia,

that have not been vetted or signed and have no trustworthy provenance. A large percentage of iOS devices are jailbroken because there are many people who like Apple products and the apps available for them but don't like being told what to do with their own property.

Jailbreaking is one way to freedom, but people who really care about such things tend towards Android. It's because of Linux. There's a lot you can do with the devices – such as writing and loading your own code – without going cap-in-hand to the OS provider. It's a platform that lends itself to hacking. While vendors may try to lock it down, it's trivially easy to eradicate vendor-loaded 'bloatware' apps (typically by 're-ROMing' to remove unwanted, branded software) and to gain full control by achieving root access. But in the process, as we'll see, the platform becomes open to abuse.

For the record, the current author has both an iPhone, which has not been jailbroken, and an Android smartphone, which has been re-ROMed and rooted. Some readers might regard this as the best, and the worst, of both worlds.

Mobile attitudes

The past few years have seen at least some progress in raising the awareness of the general public to security threats to their desktop and laptop PCs. It's rare now for someone running a Windows computer not to have anti-malware installed, along with at least some inkling about the threats posed by email attachments and so on. This raised consciousness does not seem to have transferred to the mobile world, however. Perhaps because these devices evolved from relatively simple mobile phones, people don't associate PC-domain dangers with smartphones.

They do, however, understand that these devices carry information worth protecting. A paper by researchers at the University of California, Berkeley, sponsored by Nokia, found that most people regard the information on their phones to be personal and private – to the same degree as that on their desktop and laptop PCs – and are unhappy about the idea of this data being harvested.[10] Yet few are aware of how much of this data is supplied to app vendors and other organisations during the normal operation of the device. Given the low rate of uptake of anti-malware and other security software on mobile devices, there is clearly a dangerous disconnect here.

Multiple platform issues

Not every issue covered here is unique to Android. In the malware world generally there is a trend to push exploits up the software stack, exploiting application layer software such as Flash or Java. This makes the malware effectively cross-platform, giving it a much broader range of targets. The same is true in the mobile world, although it usually requires more effort by the cyber-criminals in developing or purchasing multiple exploits for the various platforms.

This is perhaps best illustrated by the 'Zeus in the Mobile' (ZitMo) trojan. In an effort to provide additional security for online banking users, banks have turned to mobile devices as a means of providing out-of-band authentication. For certain transactions, such as funds transfers, the bank sends an SMS message containing a Transaction Authentication Number (TAN) to a mobile number associated with the user's account. The user then enters this mobile TAN (mTAN) into the bank's website via his or her computer.[11]

"How great that problem is tends to get obscured by over-enthusiastic press reports and pushy anti-malware companies trumpeting every new exploit as though it's a harbinger of doom"

In September 2010, researchers spotted the first sample of a version of the notorious Zeus banking trojan crafted especially for mobile platforms in a bid to subvert this authentication method. The sole purpose of the ZitMo trojan is to steal mTANs. It works alongside the PC-based version of Zeus, which detects when the victim is connecting to online banking and presents a fake login screen, capturing the user's credentials. Updated versions of Zeus also prompt for a mobile phone number. The victim would then be sent a message encouraging him or her to install a 'security certificate' – in fact, the ZitMo malware. With both infections in place, the cyber-criminals could connect to the victim's bank using the stolen credentials and transfer funds. If the bank sends an mTAN to the customer's phone, this is intercepted by ZitMo, which forwards the code to the cyber-criminals, allowing them to complete the transaction. Spanish security firm S21sec was the first to identify ZitMo, in Sept 2010, at which point the malware targeted the Symbian and BlackBerry platforms. Windows Mobile and Android versions followed, the latter being detected in July 2011. In Aug 2012, Kaspersky's SecureList reported new strains – mainly for BlackBerry, but also for Android.[12] By and large, however, this kind of multi-platform effort is rare.

Target of opportunity

In analysing both the potential vulnerabilities of Android, and the ways in which it has already been exploited, it's important to retain a sense of perspective. Yes, there's a real problem here, but just how great that problem is tends to get obscured by over-enthusiastic press reports of malware infections and pushy anti-malware companies trumpeting every new exploit as though it's a harbinger of doom. It can easily seem as though everyone in the world is writing malware for Android.

At a recent conference, Dan Guido of Trail of Bits and Mike Arpaia at iSEC Partners presented quite a different view. They run the Mobile Exploit Intelligence Project (MEIP), which has grown out of a similar project for desktop platforms.[13] The aim of this intelligence-driven programme is to ignore the hype that inevitably surrounds the kinds of proof-of-concept attacks and theoretical vulnerabilities – presented at security conferences and instead focus on actual exploits and attacks. They then try to

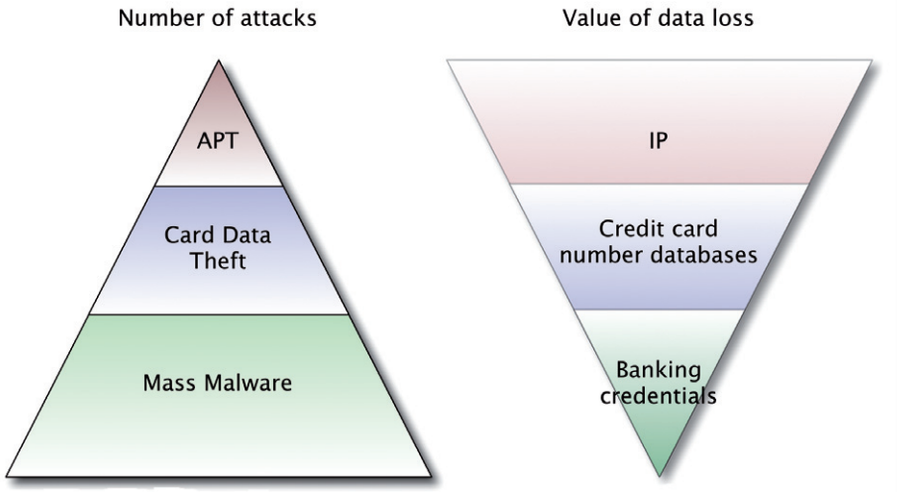


Figure 3: Maslow's hierarchy of Internet threats.

infer what kinds of malicious activities we might see in the future. "This is less hypothetical and more concrete than what most security professionals do," claimed Guido at Black Hat Europe 2012.[14] A key element of this is 'attacker math', looking at an attacker's incentives and cost/benefit calculations.

When it comes to mobile, the MEIP has found plenty of potential attacks. "But from the concrete data we see that actually very few of these possibilities are being explored," said Guido. "Mobile malware today is exploring very small numbers of attack vectors – not the ones that are being discussed at conferences. So we need to find the sweet spot – the spot at which the attacks are actually happening – and what attacks people need to defend against now. Because any investment you make defending against attacks should have the best possible return."

Arpaia added: "We surveyed all the mobile malware campaigns that we could find – hundreds of them." They looked at how the malware was distributed, how it exploited flaws, what kinds of flaws, and whether it escalated privileges. They then focused solely on those that did escalate privileges. They also concentrated on malicious ways of gaining access to data from other apps and ignored toll fraud-type apps that sign you up for premium-rate services and so on, most of which are delivered in the form of malicious apps, so no exploit is required. The latter are arguably the most common type of Android malware, so the MEIP is looking at a very specific part of the problem.

"All the exploit code has been released by the security research community. The malware community doesn't write its own exploit code and hasn't demonstrated any ability to do so, so far"

By the time of their presentation, they had collected over 500 examples of attack campaigns, but identified only 81 malware families, just 16 of which escalated privileges using a mere three jailbreak methods – all written by the same author and all of which used the same attack vector. Privilege escalation requires some form of 'jailbreak'. And much of the jailbreak code out there is viewed as at least semi-legitimate. Geeks provide jailbreak code to allow fellow enthusiasts to use their devices the way they want to. At the time of the presentation, MEIP had collected 26 jailbreaks from 10 authors. Guido and Arpaia also said that all the exploit code they've seen has been released by the security research community. The malware community doesn't write its own exploit code and hasn't demonstrated any ability to do so – so far. Most malware probably makes use of the smaller group of jailbreaks/exploits that affect Android generally, rather than specific devices. And of those, only a few are used in malware. For example, Exploid, RageAgainstTheCage and GingerBreak target Android versions 2.1, 2.2.1 and 2.3.4 – ie, one per major Android release prior to ICS. Again, it's worth emphasising that these figures are related only to the subset of threats analysed by the MEIP.

The lesson, then, is that although there may be a lot of noise in terms of Android malware, much of it involves a small amount of 'background' activity, in terms of the attack code being written and the flaws being exploited – at least as far as the kinds of exploits with which the MEIP concerns itself.

Attacker incentives

When it comes to the nature of the attacks we're seeing on Android, Guido and Arpaia referred to Maslow's Hierarchy of Internet Threats. The attacks that yield the greatest value (per hit) are Advanced Persistent Threats (APTs), but on the whole, mobile platforms haven't shown themselves to be a suitable vector for this. Similarly, with Card Data Theft (CDT), crime gangs want 100 million card details at one hit and so are not all that interested in stealing one set of data at a time from mobile devices. However, mass malware makes a lot more sense on mobile. You still go after one client at a time but on a massive scale.

The cost of an attack is based on the cost of the vector (to gain access) and the cost of the jailbreak (to escalate privileges to exploit the device). For an attack to be worthwhile, attackers need to gain more than they spend – it's simple economics. There are certain characteristics that make a platform attractive to attackers:

- If you can remain anonymous, so you don't get caught.
- If you can do it repeatedly.
- If you have an attack that you know works and allows you to change components, pulling the maximum value from each device compromised.
- If there are enough targets.

- If the devices contain information that's valuable and can be monetised.

The MEIP identifies four main attack vectors for mobile malware:

1. Mobile advertisements.
2. Close access – anything that requires close proximity, such as physical access to the device, NFC, Bluetooth etc.
3. Mobile web browsing.
4. App stores.

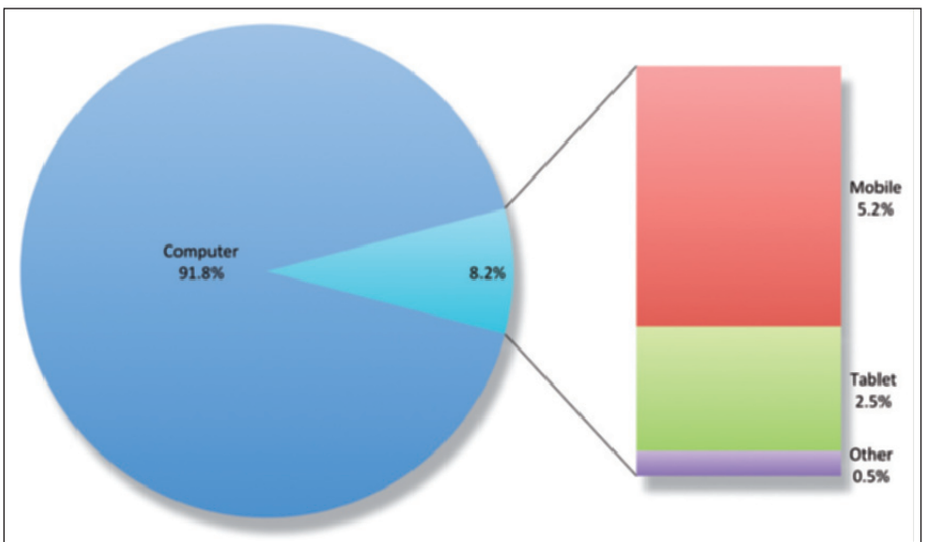
We'll examine advertising channels in a subsequent feature. As far as close access is concerned, there have been numerous proof-of-concept attacks but, according to Guido and Arpaia, no genuine exploits in the wild. Any exploit that requires close proximity or possession of the device doesn't scale well, so while it might be used for targeted compromise of a single victim (for espionage, perhaps), it's unlikely to be used for mass malware.

"Mobile browsing is how most people predict these types of attack are going to happen, because it's very easy to imagine – and possible"

The mobile browsing issue is interesting. Browser technology has shown itself to be endlessly exploitable, and Android is no exception. "Mobile browsing is how most people predict these types of attack are going to happen, because it's very easy to imagine – and possible," said Guido. "So it all comes down to, is it profitable? Is there enough potential revenue there?"

Some stats indicate that only about 8% of web traffic comes from mobile devices. This figure is almost certainly out of date, thanks to the more pleasurable experience of browsing on a tablet, compared with a smartphone. But growth is still likely to be slow given that many online services, such as social networking, news services and so on, provide their content through dedicated apps rather than the browser. For the attacker, mobile web browsing also presents a very fragmented user base, with multiple OS versions, multiple versions of Flash (or none at all) and so on. This would require multiple exploits, raising the cost of a malware campaign. MEIP believes the mobile web browsing vector offers 10-20 times fewer potential targets than the desktop. "These attacks are not happening," said Guido. "They're possible, but they're not happening."

The key vector, then, is the online app store. This is a subject to which we'll turn in more detail in a subsequent article, but the key point here is that app store distribution offers a huge number of potential targets. Google Play is delivered with every Android device (and the same is true of Apple's App Store and iOS). The cost of exploitation is low because you don't need to buy a jailbreak exploit – you just get users to install the app. The cost of submitting apps is very low. And attackers can reduce the cost of 'SEO' or marketing by hitching a ride on current events: the Olympic Games, for example, were accompanied by a number of Olympic- or sports-themed malware apps.



Figures for the US at the end of 2011 show that mobile devices comprise a small proportion of web traffic – although it is increasing. This affects the viability of advertising as a mobile malware vector. Source: ComScore Device Essentials, Dec 2011.

Confused picture

If all this seems to form a rather confused picture, it's not entirely surprising. Android is still a relatively new platform, and the large-scale exploitation of it by malware authors is newer still. While cyber-criminals are happy to rely on the so-far limited number of exploitation methodologies and vectors, security researchers are busy pulling the platform to pieces to see where the bad guys might choose to strike next.

Coming next

In next month's issue of *Network Security*, we'll look more closely at the Android platform itself, to see how some of the issues are baked into the very architecture and how poor developer practices are leaving users vulnerable. And in the following issue, we'll take a closer look at the malware and how it is distributed.

About the author

Steve Mansfield-Devine is a freelance journalist and author specialising in information security. He is editor of Network Security *and its sister publication* Computer Fraud & Security. *He is also a Certified Ethical Hacker.*

References

1. Fingas, Jon. 'IDC: Android has a heady 59% of world smartphone share, iPhone still on the way up'. Engadget, 24 May 2012. Accessed Aug 2012. www.engadget.com/2012/05/24/idc-q1-2012-world-smartphone-share.
2. Lunden, Ingrid. 'Adfonic: Android

tops iOS as most popular platform on global ad network; iPhone, iPad still top devices'. TechCrunch, 18 July 2012. Accessed Aug 2012. http://techcrunch.com/2012/07/18/adfonic-android-tops-ios-as-most-popular-platform-on-global-ad-network-iphone-ipad-still-top-devices/
3. 'Mobile Threat Report Q2 2012'. F-Secure. Accessed Aug 2012. www.f-secure.com/weblog/archives/MobileThreatReport_Q2_2012.pdf.
4. Kan, Michael. 'Mobile malware cases nearly tripled in first half of 2012, says NetQin'. Computerworld, 31 Jul 2012. Accessed Aug 2012. www.computerworld.com/s/article/9229802/Mobile_malware_cases_nearly_triple_in_first_half_of_2012_says_NetQin.
5. 'McAfee Threats Report: First Quarter 2012'. McAfee Labs. Accessed Aug 2012. www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf.
6. '2011 Mobile Threats Report'. Juniper Networks, Feb 2012. Accessed Aug 2012. www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf.
7. Genes, Raimund. 'DEFCON 2012: Android malware in Luckycat servers'. TrendLabs Malware Blog, 27 Jul 2012. Accessed Aug 2012. http://blog.trendmicro.com/defcon-2012-android-malware-in-luckycat-servers/.
8. 'Luckycat Redux: Inside an APT campaign with multiple targets in India and Japan'. Trend Micro Research Paper. Accessed Aug 2012. www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf.
9. 'AVG Technologies Q2 Community Threat Report'. AVG. Accessed Aug 2012. http://mediacenter.avg.com/en/press-tools/avg-threat-reports/avg-community-powered-threat-report-q2-2012.html.
10. Urban, J; Hoofnagle, C; Li, S. 'Mobile phones and privacy'. BCLT Research Paper Series, UC Berkeley Public Law Research Paper No. 2103405, 10 Jul 2012. Accessed Aug 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405.
11. 'Zeus-in-the-Mobile – Facts and Theories'. SecureList, 6 Oct 20122. Accessed Aug 2012. www.securelist.com/en/analysis/204792194/ZeuS_in_the_Mobile_Facts_and_Theories.
12. 'New ZitMo for Android and Blackberry'. SecureList, 7 Aug 2012. Accessed Aug 2012. www.securelist.com/en/blog/208193760/New_ZitMo_for_Android_and_Blackberry.
13. Trail of Bits research page. Accessed Aug 2012. www.trailofbits.com/research.
14. Black Hat Europe 2012. Accessed Aug 2012. http://www.blackhat.com/html/bh-eu-12/bh-eu-12-archives.html#guido.

The promise of managed security services


Colin Tankard

Colin Tankard, Digital Pathways

The market for managed security services is showing strong levels of growth. According to a report issued by Infonetics Research in 2012, the worldwide market for managed security services was worth $11.7bn in 2011 and will grow to $18bn in 2016.[1] Among the reasons for the growth are the increased importance of network security and risk management owing to the growing volume and sophistication of network security incidents.

According to the author of the Infonetics report, the increase in attacks developed for web applications is another key driver, especially as organisations need to manage and protect an ever-growing number of Internet-enabled devices connecting to their networks, including desktops, laptops, servers, smartphones and tablets. By outsourcing security needs to a managed service provider, organisations can achieve consistent protection regardless of device type, the location of the user, the operating system or browser.

At the same time, corporate governance and regulatory compliance requirements are forcing organisations to ensure that data and systems are adequately protected and to monitor the effectiveness of controls. However, many organisations lack the resources or knowledge to effectively manage such needs, leading them to seek out specialists who can help them.

Rise of clouds

Managed services have long been used by large enterprises for a variety of needs. More recently, the managed service model has been adapted to the needs of small and medium-sized organisations, especially given the rise in cloud computing. Such a model