Mobile Malware: The Enterprise at Risk

TABLE OF CONTENTS

I. Introduction: The Rise of Mobile Malware
   • Why CIOs and IT Managers Should Care
   • Key Findings
   • Methodology

II. The Evolving Threat
   • A Brief History of Mobile Malware
   • Resources for Tracking Emerging Threats

III. Targets and Entry Points
   • Operating Systems
   • Bluetooth
   • Messaging
   • Downloading
   • Syncing and Transferring

IV. Solutions
   • Carriers
   • Handset and OS Vendors
   • Third Parties

V. Insider Tips

April Highlights
While most mobile viruses cause minimal damage to handsets and their stored data, the costs of lost user productivity and increased IT support can be significant.

Some malware can infect a handset and jump to a PC during syncing, illustrating how quickly the mobile malware threat is evolving.

Enterprises can’t depend on carriers or vendors to analyze threats; they should assess products and cobble together their own solutions.

Malware can exploit all the ways data moves in and out of wireless devices.

Some mobile OSs are far more vulnerable to malware attacks than others – for example, Symbian.

The cost of anti-malware solutions varies widely, but expect to pay at least $1 per month per device.

Use of this PDF file is governed by the terms and conditions stated in the Subscriber License Agreement included in this file. Any violation of the terms of this Agreement, including unauthorized distribution of this file to third parties, is considered a breach of copyright. Light Reading Inc. will pursue such breaches to the full extent of the law. Such acts are punishable in court by fines of up to $100,000 for each infringement.
I. Introduction: The Rise of Mobile Malware

Today's business-class smartphones have the same memory, processing power, and application capabilities that laptop PCs had in the early part of this decade. They also run full-blown operating systems (OSs), such as Symbian or Windows Mobile. Besides the cellular connection, many have multiple options for moving data in and out, including Bluetooth and universal serial bus (USB) interfaces. These characteristics are a major reason why handsets have become an attractive target for writers of viruses and other forms of malicious software, or "malware."

A. Why CIOs and IT Managers Should Care
There are at least three reasons why this trend bears watching by CIOs and IT managers:

- **Vulnerability:** Nearly all mobile malware has thus far targeted handsets that run a full-blown OS: Palm, Symbian, Windows Mobile, and, to a lesser extent, BlackBerry. These smartphones typically cost $300 to $700, which means they're usually provided only to executives and management. As a result, the people with the most to lose -- e.g. address books with key company and customer contacts -- are also in the best position to lose it. Meanwhile, smartphone prices are falling, which improves the business case for offering them to a wider range of employees, and thus increases the enterprise's vulnerability.

- **Cost:** Although most mobile viruses (so far) cause little damage to handset functionality and stored data, their financial impact shouldn't be underestimated. Their damaging effects include lost employee productivity and increased IT support costs; users can also be socked by larger wireless bills from malware that causes the phone to send text messages -- without the user's knowledge -- to premium services charged to the phone account. Unless employees and managers scrutinize wireless bills, such charges can slip through. If the charges are so large that they're impossible to overlook, the enterprise can incur additional costs in personnel hours spent disputing them with the wireless carrier, which might not be willing to issue a refund.

- **Risk:** If a smartphone is used to store or access client information, malware can put that information at risk. As a result, the enterprise may run afoul of regulations and laws such as the Health Insurance Portability and Accountability Act in the U.S. Even if the handset is used to access that information rather than store it -- for example, using cellular to connect to the company's server -- malware can place it in jeopardy. For example, FlexiSpy is a keystroke logger that could be hacked into a Trojan for collecting information such as text messages and IP addresses visited by the phone's browser.

B. Key Findings
This report examines those three issues, as well as other ways in which mobile malware disrupts enterprises. Its key findings include:

Malware writers have demonstrated proficiency in identifying and exploiting all of the ways that data moves in and out of wireless devices. Viruses are routinely hidden in games that users download over the wireless network. Others are transferred via Bluetooth or downloaded when the user clicks on a link in a message. A few can enter a phone one way and exit another. Therefore it is necessary to implement anti-malware tools and policies to address all possible scenarios and points of vulnerability.

Although mobile malware is a relatively new phenomenon, the good news is that there's already a wide selection of tools for combating it. The bad news is that for the most part, CIOs and IT managers will have to conduct their own threat analyses, assess products for mitigating those threats, and then cobble together a solution using products from multiple vendors. The other good news is that this situation is temporary because antivirus vendors realize the importance -- and market potential -- of a one-stop shop providing an end-to-end solution.
Business-class handsets rarely ship with antivirus software pre-installed. There are a few exceptions, such as the Nokia 9300, which comes with Symantec's solution. For the most part, wireless carriers, handset vendors, and value-added resellers want to give enterprises the freedom to choose a solution. The downside is that CIOs and IT managers must research an array of variables, such as which antivirus solutions can run on which handset models. Doing such research in-house can consume significant resources because the IT department must become intimate with the nuances of many antivirus solutions, OSs, and handsets.

Enterprises should consider addressing mobile malware as part of a larger security strategy. One reason is that using the same antivirus platform or vendor for both wired and wireless devices may be less expensive or less complex than using separate platforms. Another reason is that many tools, techniques, and policies used to protect devices against other types of security threats can be effective against malware.

The ability to remotely update and repair infected handsets is a major asset. Particularly among enterprises with employees who travel extensively, the ability to repair a handset in the field can avoid $100 or more in lost productivity and shipping costs.

Malware can be screened at multiple points. Besides handset-based antivirus clients, malware can also be stopped in the wireless carrier and enterprise networks. A financial incentive to catching malware before it's sent out to the mobile device is that it doesn't waste airtime and wireless network resources. CIOs and IT managers should ask their carrier(s) if and how they screen for malware in the network.

Some mobile OSs are more vulnerable than others. Malware writers want to hit as many users as possible, so they target the most popular OSs. In the PC world, that's Windows; in mobile, it's Symbian. Microsoft is aggressively trying to build market share for Windows Mobile 5.0 in the consumer and enterprise markets, and if it is successful, that OS could be the target of more attacks. CIOs and IT managers are well advised to consider the tradeoff between popularity and vulnerability: A widely-used OS will have more parties developing business applications for it, but it will also be a larger, more attractive target for malware writers. One exception is BlackBerry: Although the OS is widely used, it has suffered relatively few attacks.

Simpler can be safer – usually. Nearly all mobile malware thus far has targeted the four major smartphone OSs rather than the real-time OSs (RTOSs) found on phones with limited data capabilities. However, in the past three months, more viruses have appeared that attack RTOS-powered handsets by leveraging their Java capabilities. Enterprises with mid-range and low-end handsets should keep an eye out for these types of threats.

The anti-malware solution's memory requirements vary by OS. For example, Symantec says that the software for a Palm device requires 300 KB, while on Windows Mobile handset, it takes up 862 KB. When comparing anti-malware solutions, CIOs and IT managers are well advised to ask about the memory and processor requirements. If they're too burdensome, the handset's ability to perform other tasks may be reduced.

The cost of anti-malware solutions varies widely. Enterprises should expect to pay a minimum of $1 per month per device.

C. Methodology
This report is based primarily on interviews conducted in February and March 2006 with AirMagnet, the Bluetooth Special Interest Group (SIG), Credant, F-Secure, McAfee, Microsoft, Motorola, Nokia, Research In Motion (RIM), Symantec, and Symbian. This information was supplemented with secondary research, including statements in the media and at industry conferences, as well as press releases.
II. The Evolving Threat

The arrival of mobile malware was only a matter of time. It’s the unwelcome byproduct of several trends in wireless, particularly:

- **Advances in handset memory, processing power, and application capabilities:** These advances have made handsets capable of hosting sophisticated malware. They have also increased the amount and types of information that handsets can store, making it worth the effort to write malware that corrupts data and applications or steals passwords, contacts, and files.

- **The growing use of full-blown OSs:** Handset OSs were around long before the first malware appeared, but their functionality was fairly limited. More importantly, early handset OSs were primarily unique, in that the same platform wasn’t used by multiple handset vendors, or even across multiple models from the same phone manufacturer. By comparison, today’s full-blown OSs, such as Symbian and Windows Mobile, are used by dozens of vendors across dozens of models, making it possible to write a single piece of malware that targets a pool of potential victims numbering in the hundreds of thousands, or even millions.

- **More data services, technologies, and capabilities:** Packet-data technologies such as CDMA2000 and GPRS are widely available and provide enough of a pipe to deliver malware. Meanwhile, the cost of Bluetooth chipsets has fallen to the point that it is included in many more phones than just a few years ago. That adoption makes Bluetooth another way to spread malware. One example is Cabir, which appeared in June 2004 and targets handsets running the Symbian Series 60 platform.

- **More applications:** Games and ringtones are firmly in the mainstream, so even though they’re not intended for business users, most employees probably know what they are, where to get them, and how to download them. That makes hacked games an effective and common way to get viruses into phones. Many hacked games are free, making it tempting for employees to download them because it is assumed that a charge won’t appear on the company phone bill.

- **Comfort and naïveté:** With wireless data networks and applications in the mainstream, most users are now familiar with how they work and are comfortable using services such as short message service (SMS) and multimedia message service (MMS). However, they may still be unaware of the risks and fall prey to tricks that they might recognize when using a PC. For example, although most users know a Trojan can make a PC send virus-laden emails to everyone in its address book, they may be unaware that a cell phone can also be turned into a virus-spewing zombie. As a result, when they receive a wireless message from a friend or colleague that contains a hyperlink or attachment, they may blindly click on it or install it. Malware writers recognize and routinely exploit this naïveté.

A. A Brief History of Mobile Malware

Mobile malware’s history usually is traced back to 2000, when the Phage virus appeared and targeted PDAs running the Palm OS. Phage didn’t require a wireless connection to infect the device, and at the time, there weren’t yet any handsets running the Palm OS. Nevertheless, Phage has its place in mobile malware history as the first virus to attack handheld devices. The next milestone came in February 2003, when malformed vCards were sent via SMS to Nokia 6210 phones, causing them to crash.

Cabir generally is considered to be the first true mobile virus. It appeared in Asia and Europe in June 2004, and was first detected in the U.S. the following February. Cabir targeted phones running the Symbian OS, and it ran down the battery because it kept the Bluetooth radio constantly on in order to find other nearby handsets to spread to.
Some other milestones in the brief history of mobile malware include:

- **Mosquito** (June 2004): This Trojan hid inside a hacked version of the popular game "Mosquitos" and targeted Symbian handsets. Mosquito sent text messages to premium services, something that users weren't aware of until they received their phone bills. Thus Mosquito is an example of how malware can increase costs.

- **Duts.1520** (July 2004): The first virus to attack PocketPC devices.

- **Skulls** (November 2004): This Trojan disabled most phone functions by replacing their icons with a skull and crossbones symbol.

- **Lasco** (January 2005): This worm targeted phones running the Symbian Series 60 platform. It is noteworthy because it spread both via Bluetooth and by hiding in shared applications.

- **Commwarrior** (March 2005): This virus targeted Symbian Series 60 phones and was the first to spread by Bluetooth and MMS. Commwarrior used the phone's contact list to send copies of itself via MMS.

- **Cardtrap** (September 2005): This Trojan is considered the first to jump from a phone to a PC. It targets the two most widely-used OSs: Symbian in the wireless world, and Windows in the PC world.

- **Redbrowser** (March 2006): This malware appears to be the first to exploit Java 2 Micro Edition (J2ME), a collection of Java application programming interfaces used by a wide variety of handsets, not just smartphones. Redbrowser is an example of how companies that use low-end handsets are still vulnerable to some malware attacks. (For a list of J2ME handsets, [click here](#).) Redbrowser also is an example of malware that affects the enterprise's bottom line: It sends SMS messages to an address that then adds charges to the user's phone bill.

This is just a small sampling of the mobile malware that has emerged over the past two years. For enterprises, the key takeaway is that malware writers have demonstrated proficiency in identifying and exploiting all of the ways that data moves in and out of wireless devices, as well as the vulnerabilities of a particular OS. Therefore, it is necessary to implement anti-malware tools and policies to address all possible scenarios and points of vulnerability.

### B. Resources for Tracking Emerging Threats

Mobile malware continues to evolve – hence the value of anti-malware software (discussed in detail in Section IV) that automatically receives and installs updates, as standard PC programs do. CIOs and IT managers should also track new threats in order to determine whether their mobile malware solutions and policies need to be adjusted. Following are some useful resources for CIOs and IT managers looking to keep abreast of the latest threats:

- **Mobile News from F-Secure**: Helsinki-based antivirus vendor F-Secure provides this list of threats and a searchable database.

- **Symantec Latest Virus Threats**: Symantec has expanded its line of security products to cover mobile malware. This site features a list of threats and a searchable database.

- **Bluetooth Security**: This site is operated by the Bluetooth SIG. Although it's the industry body shepherding this technology, the SIG provides only basic tips for protecting against Bluetooth-enabled attacks, rather than a comprehensive, continuously updated list of known threats. This information is a good starting point for enterprises developing mobile security policies and strategies, but CIOs and IT managers will have to rely on vendor sites such as F-Secure's or Symantec's for detailed information about specific threats.
• **Symbian and Security**: Like the Bluetooth SIG’s site, Symbian's provides general security information, rather than a detailed list of existing and emerging threats. (This is largely because Symbian doesn't provide an OS that vendors simply load into their phones, but rather licenses code that vendors customize to create their own platforms, albeit ones all based on the same core.) This site's information, particularly its Security FAQs, may be useful to enterprises developing mobile malware strategies and policies.

• **Secunia Virus Information**: Security vendor Secunia's site features alerts and other information complied from a variety of sources.

• **Mobile Antivirus Researchers Association**: This site provides white papers and other information about the underlying techniques of malware, rather than a comprehensive list of threats as they emerge.
III. Targets and Entry Points

Over the past two years, malware writers have demonstrated impressive proficiency in identifying and exploiting all of the ways that data moves in and out of wireless devices. This section looks at the primary ways that malware writers are targeting mobile devices.

A. Operating Systems

Mobile OSs can be divided into two types. The best-known type, at least among users, is what is typically referred to as a smartphone OS. The four main OSs are Microsoft's Windows Mobile, PalmSource's Palm, RIM's BlackBerry, and Symbian, which is the product of an independent company of the same name owned by Ericsson, Nokia, Panasonic, Samsung, Siemens, and Sony Ericsson. Over the next year or two, Linux is likely to take its place as the fifth major smartphone OS. Its vulnerability will be determined partly by its level of popularity and partly by whether its backers learn from the shortcomings of the other four smartphone OSs.

One attribute of smartphone OSs is that they're designed to be used by multiple handset vendors for a variety of models. In that sense, smartphone OSs are no different than the Windows OS, which hundreds of PC vendors license to put on their machines.

The other main group of OSs are RTOSs, which are developed in-house by the handset manufacturer or purchased from a third party. Unlike their smartphone cousins, RTOSs have less functionality, and thus less ability to host sophisticated malware. RTOSs are also fragmented, in that multiple handset vendors rarely use the exact same version. For these reasons, RTOS-powered phones are less vulnerable to malware, though by no means immune.

Symbian is the most widely-used mobile OS, which is why it's the most targeted platform. On the plus side, Symbian has strengthened its defenses in its latest version, v9. (The first v9 handset, the Nokia 3250, shipped in February 2006.) "We have introduced platform security, which is akin to having locks on all the doors in and outside of the house, and monitoring them 24/7," says Craig Heath, product manager for security, privacy, and digital resource management at Symbian. "Essentially, it helps protect networks, phones, and users' personal information from malware by ensuring applications can only access sensitive phone capabilities (e.g. sending SMS, making calls, access to personal information on the phone etc) when they have been given specific permission to do so."

Windows Mobile 5.0 ships with a bundle of software that includes Excel, Outlook, PowerPoint, and Word. As a result, it's a good fit for business use, which is one reason why CIOs and IT managers should be aware of malware targeting the platform. So far, it hasn't been attacked as heavily as other platforms. However, that may change because Microsoft is aggressively trying to grow Windows Mobile 5.0's share of the consumer and enterprise markets. For CIOs and IT managers, this goal is noteworthy for at least two reasons:

- There are more consumers than business users, so if Windows Mobile builds a significant following among consumers, the platform will become a more attractive target for malware writers. Viruses don't distinguish between consumer and business users, so the result is that Windows Mobile's increased popularity could mean more viruses for enterprises to contend with.
- Although smartphones historically have been aimed at business users, with price tags to match, Windows Mobile 5.0 is an example of how that's changing. For example, the OS can be found on handsets discounted as low as $99, such as the T-Mobile SDA. At that price, employees that aren't provided with a phone or reimbursed for one may buy a smartphone anyway and use it for work. Unless the enterprise uses tools to identify the devices connecting to its PCs and LANs, it may not be aware of smartphone usage among employees – or the malware threat that comes with it.
Despite its cult following among business users, BlackBerry has been the target of relatively few mobile viruses. One recent example involves using images to launch denial-of-service attacks. (For more information, see BlackBerry's Technical Knowledge Center.) Another exploits the BlackBerry's Java capabilities. (For more information, see the Vulnerability Note from the U.S. Computer Emergency Readiness Team.)

CIOs and IT managers are well advised to avoid being lulled into complacency by the limited number of BlackBerry attacks. Like Windows Mobile 5.0, use of BlackBerry is expanding beyond the business-user demographic. Consumer adoption will significantly increase the number of BlackBerry devices in the market, making the OS a more attractive target for malware writers.

Despite being relatively popular, the Palm OS has been the target of surprisingly few attacks. The latest version of the Palm OS uses code signing, where unauthorized applications – such as malware – are blocked from installation and operation. (For more information, see Palm's Mobile Security: Securing the Device resource page.)

Figure 1 summarizes the current and projected future vulnerability of the major smartphone OSs.

### Figure 1: Mobile OSs – Malware Risks

<table>
<thead>
<tr>
<th>Vendor/OS</th>
<th>Level of Attacks</th>
<th>Outlook</th>
</tr>
</thead>
<tbody>
<tr>
<td>PalmSource Palm</td>
<td>Low</td>
<td>The wild card is whether PalmSource can get its OS onto more consumer and business devices, possibly by leveraging a new Linux foundation. If it succeeds, then the Palm OS will become more attractive to malware writers.</td>
</tr>
<tr>
<td>RIM BlackBerry</td>
<td>Low</td>
<td>Despite its cult-like following, BlackBerry users are likely to remain a minority, so most malware writers will focus on rival platforms that offer more potential victims.</td>
</tr>
<tr>
<td>Symbian Symbian</td>
<td>High</td>
<td>Even if Symbian is knocked off its perch as the most widely-used smartphone OS, it will still have a large user base. Thus, it will likely remain an attractive target for malware writers for the foreseeable future. On the plus side, Symbian is doing a good job of responding by making its platform more secure, although handset licensees must also do their part.</td>
</tr>
<tr>
<td>Microsoft Windows Mobile</td>
<td>Low</td>
<td>With the new version 5.0, Microsoft is aggressively trying to build consumer and enterprise market share for Windows Mobile. If it succeeds, the OS could become a bigger target because it will represent a greater pool of potential victims for malware writers. The Windows name alone also makes it a target.</td>
</tr>
</tbody>
</table>

Source: Unstrung Enterprise Insider

### B. Bluetooth

Bluetooth is a low-power wireless technology with a range of about 10 meters. Thus its usefulness for spreading malware is limited – literally – by the fact that it can facilitate communications only between nearby devices. Bluetooth is designed for applications such as transferring files and connecting hands-free headsets. The technology is built into hundreds of models of phones currently on the market. This adoption makes it attractive to malware writers because it is a way to hit many phones at once.
The first mobile virus, Cabir, spread via Bluetooth. The technology remains a popular choice for malware writers, either on its own or paired with another technology. For example, Commwarrior spread via Bluetooth and MMS.

Besides being used as a way to spread malware, Bluetooth can also be used to facilitate other types of attacks. Two examples are "Bluejacking" and "Bluesnarfing," which exploit Bluetooth's ability to discover nearby devices and communicate with them in order to steal information such as contacts lists. These attacks show why enterprises should consider addressing malware as part of an overall security effort. For example, if the company creates a policy that Bluetooth phones should never be in discoverable mode except when exchanging information, then there is less chance that malware will be spread via Bluetooth.

Enterprises that want to create this type of policy to regulate Bluetooth use should consider tools such as AirMagnet's BlueSweep (available for free from AirMagnet's Website) as a first step in assessing the risks and options. The BlueSweep utility scans an area – such as an office floor – to identify devices with Bluetooth and create a list of the services running on them. Although BlueSweep isn't specifically designed to identify malware spreading via Bluetooth, it is useful for determining how many employees are using Bluetooth and how they're using it. If usage is high, then the enterprise should definitely consider addressing Bluetooth as part of its malware and security efforts.

Education is an inexpensive, effective defense against Bluetooth-enabled malware. "When these viruses spread, they typically require the user to accept and install the application," says Michael Foley, executive director of the Bluetooth SIG. "So it's important to educate people to not accept and install programs from people and sources they're not familiar with."

It goes without saying that in order to educate employees, the IT department must first educate itself. The catch is that keeping up with Bluetooth-enabled malware as it emerges is much easier said than done. One problem is that the Bluetooth SIG doesn't have a publicly accessible section of its Website providing a continually updated list of known threats. "It's something that we're exploring," Foley acknowledges. Until the SIG provides a clearinghouse for this type of information, enterprises must rely on antivirus vendors to provide help, in the form of security patches that are pushed to phones and updated online threat lists, such as the ones provided by F-Secure and Symantec.

Another challenge is that employees may have difficulty following policies to reduce Bluetooth-enabled functionality. A prime example is the way in which some handsets and OSs bury Bluetooth controls deep inside menus, which makes it a hassle to shut off discovery mode. If an enterprise is concerned about Bluetooth security, it should pay close attention to how the technology is controlled when selecting phones. For example, regardless of the model on which it is running, Windows Mobile 5.0 provides one-touch access to Bluetooth controls from the opening "Today" screen.

CIOs and IT managers should also consider whether the platform vendor provides tools that enable IT departments to create and enforce their own security policies for Bluetooth. "With BlackBerry, the administrator can limit what Bluetooth profiles are allowed, [such as] allowing only headsets, or take it a step further and completely disable Bluetooth, so that the radio itself is turned off, so that applications cannot access it," says Scott Totzke, director of the global security group at RIM.

**C. Messaging**

Support for SMS and MMS has been built into most handsets sold over the past two years, regardless of price or target demographic. Thus these technologies are an effective way for malware writers to attack as many users as possible.
Depending on the carrier, a user doesn't necessarily have to be on a data plan to send and receive SMS or MMS messages. Instead, they can be charged on a per-use basis where rates typically run $0.10 or more per message. Even if employees have only voice plans, messaging-enabled malware can affect the bottom line. The Redbrowser virus, as discussed in Section II, is a recent example of malware that uses SMS to run up the user's phone bill.

MMS messages can carry an installation file similar to an .exe file in the PC world. If the user clicks on it and agrees to any installation questions, the virus is installed. The first MMS-spread virus was Commwarrior, which appeared in March 2005.

MMS and SMS are also used to breathe new life into some of the oldest tricks in the book. Case in point: Most users are now aware that a virus can turn a PC into a "zombie" that sends infected emails to every person in its contact list, so when they receive an email from a person whose name or email address they know, but it has a suspicious message, they're usually savvy enough not to open any attachment, click on any links, or respond to it.

However, those same users are often unaware that a cell phone can likewise be turned into a virus-spewing zombie. As a result, when they receive a wireless message from a friend or colleague that contains a hyperlink or attachment, they may blindly click on it. Malware writers recognize and routinely exploit this naïveté.

Although anti-malware software can weed out these types of attacks, educating employees about the risks is an important additional layer of protection. "Nothing beats an educated user," says Janne Uusilehto, senior technology manager for technology platforms at Nokia.

D. Downloads

Downloads are one of the most common ways that malware is spread. One early example is Mosquito, a Trojan that hid in a free download of the popular game "Mosquitos" and forced the handset to send messages that ran up the user's bill. Many virus-laden downloads are free, making it tempting for employees to download them because they assume that a charge won't appear on the company phone bill.

Besides deploying anti-malware software that catches download-enabled attacks, CIOs and IT managers should also consider policies that forbid downloads of games, ringtones, wallpapers, and applications to company-provided smartphones. This type of policy is worth considering even if malware isn't a concern, because downloads can affect the bottom line in terms of lost productivity (e.g., employees playing games), as well as conflicts with enterprise applications and the unnecessary drag on a phone's memory and processor.

E. Syncing and Transferring

One reason behind the popularity of smartphones is that they can sync with a PC in order to transfer files and information such as contacts and calendar items. The downside is that syncing can create security risks for both the smartphone and the PC to which it is connected.

In the case of malware-related risks, one threat is a new breed of virus that can spread from a smartphone to a PC, or vice versa. "It is very likely that there will be others of the same sort coming out in the future," says Anton von Troyer, product marketing manager at F-Secure.

These hybrid viruses pose a particular threat in an enterprise environment, because if the infected phone syncs with a PC located behind the firewall, the virus could conceivably hop onto the company's LAN and spread to other PCs. This possibility is another reason why enterprises should consider addressing mobile malware as part of a larger security strategy. It also highlights why enterprises might want to consider using the same vendor or security product to address both wired and wireless threats.
Two examples of this new species of virus are:

- **Cardtrap**: This Trojan first appeared in September 2005 and now includes 12 known variants. Cardtrap infects Symbian-powered handsets with at least two worms, one of which resides on the phone's removable memory card, if it has one. When that card is inserted in a Windows PC, the worm attempts to install itself on the computer. Thus Cardtrap targets the two most widely-used OSs: Symbian in the wireless world and Windows in the PC world. As its creator noted: "This virus closes the gap between handhelds and desktops. Now it's one big world, open to all."

Cardtrap is also an example of how a virus can cause more damage when it's being removed. For example, the Cardtrap.I variant corrupts the phone by removing OS components. To restore them and remove Cardtrap, the user must do a hard reset, which deletes information such as contact lists and third-party applications. If the infection occurs while an employee is on the road and the phone has her only contact list, the financial impact includes lost productivity. For more details on Cardtrap.I, see F-Secure's Virus Description and Symantec's Security Response.

- **Cxover**: Also known as Crossover, this Trojan appeared in late February 2006 and is the first known virus to jump from a Windows PC to a handset running the Windows Mobile OS. Crossover was released as a proof-of-concept virus rather than into the wild, but it's naïve to assume that this genie will go back in the bottle. For more information, see Mobile Antivirus Researchers Association and F-Secure's Virus Information Page.
IV. Solutions

As the number and severity of mobile malware threats has grown, so has the selection of solutions. This section looks at the current options. It's important to note that the vendors and products mentioned do not make a comprehensive list. Instead, they're provided as a representative sampling intended to serve as a starting point for enterprises developing mobile malware strategies and policies.

A. Carriers

Most wireless carriers are essentially Internet service providers (ISPs). In a wired world, consumer-focused ISPs historically let their customers tackle viruses and malware. But over the past few years, many have started bundling antivirus protection as market differentiators – effectively turning a problem into an opportunity. This trend may eventually repeat itself in the wireless world, where carriers use bundled antivirus protection as a way to attract and retain consumers. Indeed, a few wireless carriers already sell handsets with anti-malware software pre-installed. Three examples are NTT DoCoMo, Orange Switzerland, and T-Mobile Germany.

On the enterprise side, however, it's highly unlikely that carriers will make a practice of shipping handsets with pre-loaded anti-malware solutions. The main reason is that they don't want to limit customer options. For example, an enterprise that uses Symantec products for PC and server security may want to stick with that vendor for mobile devices for reasons such as economy of scale or simplicity of product management. Carriers have a vested interest in leaving those decisions up to enterprises because limiting customer choices limits sales opportunities.

Carriers can play an important role in fighting malware, particularly by screening for it in their networks so that it's never sent out to user devices. When selecting a carrier, enterprises should ask each operator to describe how it screens for malware or, if it doesn't, whether it plans to. This additional layer of protection is particularly useful for smaller companies that have limited resources to devote to combating mobile malware in-house.

B. Handset and OS Vendors

Like carriers, handset vendors are leaving anti-malware product decisions up to enterprises, for the same basic reason: They don't want to limit customer options. There are a few exceptions, such as RIM, which makes not only the BlackBerry platform and most of the devices it runs on, but also the servers that reside in the carrier or enterprise network to handle wireless email traffic. In the enterprise, this server sits behind the firewall to provide an additional layer of security.

"A malicious email attachment sent to the enterprise would have to traverse the perimeter anti-spam, antivirus, and other email security defenses that an enterprise would have in place," says RIM's Totzke. "Since the BlackBerry Enterprise server is an extension of an existing inbox, it only accesses messages that end up in the email server (Exchange/ Domino/GroupWise), so it benefits from those email security defenses."

Another way that handset vendors enable enterprise anti-malware efforts is by building support for over-the-air (OTA) updates into their handsets. As its name implies, OTA uses the wireless network to download information – in this case, updated virus definitions. The basic concept is similar to how products such as Symantec's Norton AntiVirus push updates to client software on PCs. Microsoft uses a similar approach for Windows Update on PCs.

"Vendors should also start to think on ways to update the OSs and firmware software on the phones," says F-Secure's von Troyer. "That way, users would not have to go to a repair shop to update their devices but would get an automatic update over-the-air. This is a big problem that vendors should address. In the PC world, Microsoft is doing this already, and most likely it will become an issue for [handset] vendors as malware spreads and uses OS vulnerabilities."
There are at least two reasons why this scenario is likely to occur. First, many carriers already use OTA updates for tasks such as patching buggy software. This technology can be adapted for sending antivirus updates and repairing infected handsets. Because the OTA client resides deep inside the phone, while malware does its dirty work higher up, at the application level, an infected handset still should be able to accept a virus patch. Second, the selection of OTA-equipped handsets is significant and growing. LG and Sony Ericsson are among the vendors currently shipping OTA-ready phones. As the installed base of OTA handsets grows, it becomes more viable for battling malware.

To understand how OTA can reduce malware costs in an enterprise environment, suppose that an employee is traveling and her phone becomes infected. Because she's away from the office, she can't simply walk the phone to the IT department for repair. Instead, she loses productivity by calling the help desk and following instructions for repairing the phone. If her salary is $60,000, and she spends three hours dealing with the infected phone, the malware's cost is a minimum of $86.55. There's also the cost to staff a help desk to deal with mobile malware. If a technician makes $40,000, then the three hours working with an employee costs $57.69. If their phone conversation is enough to repair the phone, then the total cost is $144.24.

If the phone can't be repaired in the field, there are additional costs, such as overnight shipping to send the employee a temporary replacement phone and maintaining a supply of backup phones for these types of emergencies. If the infected phone is the employee's only way to access contact lists and mobile enterprise applications, additional costs could include more lost productivity. If the phone number can't be immediately transferred to the replacement phone, productivity may be lost playing phone tag with those who don't have the new, temporary number.

In this example, OTA could reduce malware-related costs in a couple of ways. The ideal scenario would have periodic malware updates sent via OTA so that her phone never gets infected in the first place. In that case, the above costs are completely eliminated. In another scenario, her phone still gets infected, but the IT department uses OTA to repair it remotely. In that case, the cost is a few personnel hours for the mobile employee and the technician to resolve the problem, but there's less bottom-line impact because the repair process is faster and because there's no need to issue a temporary replacement phone.

The above scenario also shows why it's a mistake to downplay the mobile malware threat. Granted, most viruses haven't caused the same level of damage to data and applications that their wired cousins do in the PC world. But their bottom-line impact can be just as significant.

Finally, enterprises should check the Websites of their handset vendors for information about malware products that have been tested for use with their phones. Some vendors are better than others in terms of providing direct access to such information. One example is Nokia, whose [Mobile Security Webpage](#) provides an overview of the security vendors it works with. In case some of the information is out of date, CIOs and IT managers are well advised to confirm this information before purchasing products.

C. Third Parties
Not surprisingly, well-known security vendors such as McAfee and Symantec have offered mobile malware products for years. As with their PC cousins, the value of these products depends not only on their features, such as the entry points that they monitor, but also on the vendor supplying them. That's why CIOs and IT managers should scrutinize how assiduously the vendor updates virus definitions and the options for pushing them to devices instead of relying on employees to download them.

Enterprises should also consider the overall user-friendliness for both the IT staff and the end users. Figures 2 and 3 show examples of client-side user interfaces for anti-malware products.
When assessing anti-malware client software, enterprises should consider their handset capabilities. Anti-malware software takes up memory and processing power, so it’s important to ensure that the solution doesn’t put a drag on performance. The anti-malware solution’s memory requirements can vary significantly by OS. For example, Symantec says its software for a Palm device requires 300 KB, while on Windows Mobile handset, it takes up 862 KB.

Cost is another consideration. It’s difficult to provide even ballpark estimates for enterprise-wide deployment because there are so many variables, such as volume discounts, reseller markups, and whether the mobile malware product can be bolted onto a security platform that the enterprise already uses. Although enterprises should review as many mobile malware solutions as possible, CIOs and IT managers are well advised to pay close attention to products from vendors they already use. By going with the same vendor, the enterprise may be able to reduce costs, such as with a loyalty discount, or because the IT staff doesn’t need to learn an entirely new platform in order to start protecting mobile devices.

Figure 4 provides examples of mobile malware products. This list is representative rather than comprehensive; it is intended to serve as a starting point for IT departments researching products that suit their company’s specific needs. The prices listed are retail, so volume purchases should be somewhat cheaper. As with antivirus products for the wired world, the product price also
varies according to whether it includes one or two years of updates. Links to product information are provided, partly because the list of supported phones and platforms is subject to change.

**Figure 4: Anti-Malware Product Overview**

<table>
<thead>
<tr>
<th>Vendor/Product</th>
<th>Price</th>
<th>Supported Devices/OSs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airscanner Corp. Mobile Antivirus for Windows Mobile Smartphone</td>
<td>$29.99</td>
<td>Any handset running Windows Mobile Smartphone 2003 or 5.0, with a minimum of 2MB available RAM, and an ARM or XScale processor</td>
</tr>
<tr>
<td>BullGuard Ltd. Mobile Antivirus</td>
<td>N/A</td>
<td>Any handset running Windows Mobile 2003 or 5.0, with a minimum of 1.5MB available RAM; Symbian Series 60 or 80, with a minimum of 400KB of available RAM; or Symbian UIQ, with a minimum of 2MB of available RAM</td>
</tr>
<tr>
<td>F-Secure Corp. (HEL: FSC1V) Mobile Antivirus</td>
<td>€28.65 (about $34.63)</td>
<td>Symbian Series S60 (Nokia 3230, 3650, 3660, 6260, 6600, 6630, 6670, 6680, 6681, 6682, 7610, 7650, N70, N90, and N-Gage, Panasonic X700 and X800, Siemens SX1); Symbian Series 90 (Nokia 7710); Windows Mobile Pocket PC 2003 (Qtek 9090, 2020, and S100, MDA II, III, and Compact, HP iPAQ 6500, 6515, and 6300, SPV M1000); Windows Pocket PC 5.0 (Qtek 9100 and 9000, MDA Pro); Windows Smartphone 2003 (Motorola MPX220, Qtek 8200, 8010, 8020, and 8100, SDA and SDA Music); Windows Smartphone 5.0 (Qtek 8310 and 8300); Minimum of 850KB of available RAM required, regardless of OS</td>
</tr>
<tr>
<td>Kaspersky Lab Inc. Antivirus Personal</td>
<td>£12 (about $20.87)</td>
<td>Microsoft Smartphone 2002 or Windows Mobile 2003 for Smartphone, with minimum of 100KB of available RAM</td>
</tr>
<tr>
<td>McAfee Inc. (NYSE: MFE) VirusScan Mobile</td>
<td>$29.99</td>
<td>Microsoft Smartphone 2003, including Motorola MPX200, Audiavox SMT5600, Qtek 8010, Sierra Wireless VOQ A11, HP iPAQ 6315, Samsung SPH i700, and Siemens SX66</td>
</tr>
<tr>
<td>Symantec Corp. (Nasdaq: SYMC), Mobile Security 4.0 for Symbian</td>
<td>$44.95</td>
<td>Symbian OS 7.0s, 8.0a, Series 60 v2, Series 80 v2</td>
</tr>
<tr>
<td>Trend Micro Inc. (Nasdaq: TMIC) Mobile Security v2.0</td>
<td>$24.95</td>
<td>Microsoft Windows Mobile 2003 and 5.0; Symbian OS 7.0s, 8.0a, 8.1a, Series 60, OS 7.0, UIQ 2.0/2.1</td>
</tr>
</tbody>
</table>

*Source: Unstrung Enterprise Insider*
V. Insider Tips

Insider Tips is a standard section in Unstrung Enterprise Insider reports. Its purpose is to provide guidance for enterprises considering a particular technology, application, service, or product – in this case, solutions and policies for combating mobile malware.

Our employees use a variety of handsets from different vendors, and with multiple OSs. How do we protect a multi-vendor, multi-OS environment?

Look for mobile malware products that work across multiple OSs. For example, if your handsets run Windows Mobile 2003, Windows Mobile 5.0, and Symbian 8.0, consider a product such as Trend Micro Mobile Security, which supports those three, plus others.

Memory is another consideration. A multi-OS product might protect all of your devices, but still be a poor fit if some of your handsets can barely meet its memory requirements.

Also, keep in mind that many anti-malware policies are OS- and vendor-agnostic. For example, a policy that prohibits employees from downloading ringtones or games – which can be infected with malware – is effective regardless of the OS or handset model.

Some of our employees travel abroad. Does roaming affect mobile malware risks and solutions?

So far, most mobile malware has appeared in Asia and Europe before spreading to other parts of the world, such as the U.S. (That's partly because wireless data usage traditionally has been highest in Asia and Europe, so there's a larger pool of potential victims.) As a result, employees who travel to those areas may be at higher risk. If the budget for mobile malware solutions is limited, these devices should be a priority.

A second consideration is how the anti-malware platform is updated. For example, if an employee is roaming, can updates still be pushed to her device? Some wireless carriers don't support data roaming, or support only basic data services such as SMS, and these variables may affect updating. Enterprises should ask the security vendor to describe how updates are issued and whether roaming can affect the update process.

Some of our employees use handsets that they purchased and were reimbursed for. They are/were free to choose whatever model they wanted, within a certain price range. How do we accommodate these variables in our mobile security strategy?

An audit is a good start. Use it to build a database of key information such as vendor, model number, and OS, including version. Some employees may not know this information, so collecting it may require them to call or visit the IT department.

With that information, you can begin to narrow the field of anti-malware products by, for example, comparing each product to your handset portfolio. With employees free to make their own purchasing decisions, chances are high that you'll have a multi-vendor, multi-OS environment. In that event, see the answer to the first question for additional guidance.

Some threats are relatively OS-agnostic. For example, a virus that uses MMS to spread may affect all of your devices because the technology is supported by almost all handsets sold over the past two years. Education and policy are two ways to address these types of broad-reaching threats. For example, employees should be made aware that a cell phone can also be turned into a virus-spewing zombie. As a result, when they receive a wireless message from a friend or colleague that contains a hyperlink or attachment, they should be trained to review it carefully instead of simply clicking on it.
Another example is downloads, which are supported by a wide variety of handset models and OSs. If many employee handsets can download applications such as games, ringtones, and wallpapers, employees should be educated about how downloads are used to spread viruses. A policy forbidding downloads can provide an additional layer of security. At the very least, employees shouldn't be reimbursed if the downloads don't pertain to their jobs – creating a financial disincentive for those who don't want to pay for them.

Some employees may try to sneak through such purchases. Hence the importance of making employees justify expenses on their wireless bills. This requirement has a side benefit applying to all OSs and handset models: Some mobile malware sends messages to premium numbers, running up the user's bill. A policy requiring employees to justify wireless expenses could eliminate the chance the company will unwittingly pay for these types of malware-related charges.

Only some of our employees are provided with data rate plans. What's the malware risk for employees who have voice-only plans?

The risk level depends on the carrier. Some have voice plans that won't allow any data usage – even SMS – unless the customer signs up for that option. Others have voice plans that allow some data usage, which is charged on a per-use basis, such as for each received SMS.

If your employee voice-only plans fall into the latter category, they're potentially vulnerable to malware such as Redbrowser, which sends SMS messages to an address that then adds charges to the user's phone bill. These employees should be educated about malware risks and subject to policies such as justifying all expenses on their monthly wireless bill.

When WiFi's security issues started getting a lot of attention a few years ago, we started periodically scanning our offices to detect risks, such as unauthorized access points. Should we do the same thing for Bluetooth?

It's definitely worth considering, partly because Bluetooth is one of the ways that malware frequently spreads, and partly because basic Bluetooth-detection tools, such as AirMagnet's BlueSweep, are free. If employee Bluetooth usage is high, then you may need to consider addressing it as part of your malware and overall security efforts.

Many of our handsets use Symbian, which is the OS that malware writers have targeted most. Should we consider migrating to another platform in order to reduce risk?

Not unless another platform offers comparable or better functionality and third-party application selection. Although malware is an increasingly serious risk for enterprises, it shouldn't be a decisive factor in choosing handsets. On the desktop side, that would be like replacing PCs with Macs or Linux computers simply because Windows is the most targeted computer OS. Pick the platform that best fits your business needs and then protect it.

You said that enterprises should expect to pay a minimum of $1 per month per device for anti-malware solutions. How can we calculate the ROI?

For starters, estimate costs such as IT department personnel hours for preventing and responding to malware. The prevention side includes time spent evaluating anti-malware products, developing policies, and building a database of employee devices if you don't already have one. Those tasks may take more than one person, but let's say that they require two mid-level IT employees a total of one month. If salaries are $50,000 each, then two months' worth of personnel hours works out to about $8,333.

Prevention is an ongoing task that includes evaluating new threats and periodically checking that products and policies are effective. If that's enough work to make up a quarter of an IT staffer's workload, there's an additional annual cost of about $12,500, pushing the total so far to $20,800.
Here's where things get less clear-cut: No single anti-malware solution is perfect, so you'll need to estimate the costs of dealing with the viruses that slip through. Those costs are related to the number of employees with cell phones. For example, if a few thousand employees have cell phones, then the chances are higher that some of them will become infected than if only a couple of hundred employees have phones. If the number of potential infections is high, you may need to staff up your IT help desk to field such calls. In that case, one cost is the salary or salaries of the extra staff.

Other costs apply outside of the IT department, for example the cost of lost productivity due to employees wasting time grappling with infected phones. That cost could be measured in terms of average hourly wage multiplied by the number of employees likely to be infected in a given year. For example, if 200 employees are likely to be hit with malware, and they make an average wage of $35 per hour, then the lost-productivity cost could be $7,000 annually.

These types of calculations can help CIOs and IT managers determine the business case for deploying anti-malware solutions. This process also highlights the value of doing a threat analysis first to determine the scope of the problem. If the risk and scope are low, policies and procedures such as those discussed in this report may be an affordable yet effective alternative to deploying anti-malware solutions.

We don't have much room in this year's budget for buying anti-malware products. What are some low-cost options that we can implement today?

Education and policies are your least expensive options, although keep in mind that they're not totally cost-free because you'll have to devote at least some IT personnel hours to creating and enforcing them.

A few suggestions:

- If employees have Bluetooth-equipped handsets, visit Bluetooth's Wireless Security page for basic tips on protecting against Bluetooth-enabled attacks.
- If employees have Symbian-powered handsets, visit Symbian's Security FAQs page for basic tips on protecting these devices.
- Limit wireless data service to employees who require it for their jobs. Restricting access to downloads and messaging blocks the major entry points for malware. This policy also has a side benefit: Employees aren't wasting time playing games and messaging.
- For employees who must have data access, educate them about the risk of downloading attachments, even when these appear to be from someone they know. The same applies to hyperlinks in messages.

The vendor we currently use for PC and server antivirus protection also makes products for wireless devices. Should we stick with them for mobile-malware solutions as well?

The only answer that applies across the board is that it's definitely worth considering. One potential advantage is that you may be able to negotiate a loyalty discount. Another possible reason is that mobile security solutions can simply bolt onto your existing IT security products. If that's the case, then sticking with the same vendor and platform may be more cost-effective, because your IT staff won't have to spend time learning the nuances of another vendor's mobile-malware solution.

That said, the decision should also come down to features. For example, if another vendor's product has features that your current vendor's doesn't, and you believe those features are important, then it may be a mistake to stick with the incumbent.
We’re periodically refreshing our employee handsets. What should we consider regarding support for anti-malware solutions?

First, don't base your choice of handset and OS solely on whether they're more or less vulnerable to malware. That's an important consideration, but the priority should be the usual criteria, such as selection of third-party applications, data capabilities, and the rate plans offered by the carrier network it uses.

Once you've narrowed the field based on those criteria, ask each handset vendor under consideration to provide a list of anti-malware solutions that have been tested to work with those models. It's worth verifying that information with the malware vendors, too. Also, consider factors such as the user-friendliness of the client that resides on the device, any adjunct management tools for the IT department, and how the product gets updated virus definitions to the device.

---

**Research Analyst:** Tim Kridel ([tkridel@kc.rr.com](mailto:tkridel@kc.rr.com))

**Editor:** Dennis Mendyk ([mendyk@heavyreading.com](mailto:mendyk@heavyreading.com))

**Support:** [www.unstrung.com/enterprise](http://www.unstrung.com/enterprise) ([insider@unstrung.com](mailto:insider@unstrung.com))
SUBSCRIBER LICENSE AGREEMENT
Any Unstrung Enterprise Insider report ("Report") and the information therein are the property of or licensed to Light Reading Inc. ("Light Reading") and permission to use the same is granted to annual or single-report subscribers ("Subscribers") under the terms of this Subscriber License Agreement ("Agreement") which may be amended from time to time without notice. When requesting a Report, Subscriber acknowledges that it is bound by the terms and conditions of this Agreement and any amendments thereto. Light Reading therefore recommends that you review this page for amendments to this Agreement prior to requesting any additional Reports.

SUBSCRIPTION RENEWAL
For convenience, subscriptions purchased by credit card will be auto-renewed at the end of the subscription term. Prior to that auto-renewal you will receive a notice that will include instructions for updating your subscription or payment information and for opting out of the auto-renewal process.

OWNERSHIP RIGHTS
All Reports are owned by Light Reading and protected by United States Copyright and international copyright/intellectual property laws under applicable treaties and/or conventions. Subscriber agrees not to export any Report into a country that does not have copyright/intellectual property laws that will protect Light Reading's rights therein.

GRANT OF LICENSE RIGHTS
Light Reading hereby grants Subscriber a personal, non-exclusive, non-refundable, non-transferable license to use the Report for research purposes only pursuant to the terms and conditions of this Agreement. Light Reading retains exclusive and sole ownership of each Report disseminated under this Agreement. Subscriber agrees not to permit any unauthorized use, reproduction, distribution, publication or electronic transmission of any Report or the information/forecasts therein without the express written permission of Light Reading. Subscribers purchasing site licenses may make a Report available to other persons from their organization at the specific physical site covered by the agreement, but are prohibited from distributing the report to people outside the organization, or to other sites within the organization. Enterprise Level Subscribers, however, may make a Report available for access on computer intranets or closed computer systems for internal use under their service agreements with Light Reading.

DISCLAIMER OF WARRANTY AND LIABILITY
Light Reading has used its best efforts in collecting and preparing each Report.

LIGHT READING, ITS EMPLOYEES, AFFILIATES, AGENTS, AND LICENSORS DO NOT WARRANT THE ACCURACY, COMPLETENESS, CURRENTNESS, NONINFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OF ANY REPORTS COVERED BY THIS AGREEMENT. LIGHT READING, ITS EMPLOYEES, AFFILIATES, AGENTS, OR LICENSORS SHALL NOT BE LIABLE TO SUBSCRIBER OR ANY THIRD PARTY FOR LOSSES OR INJURY CAUSED IN WHOLE OR PART BY OUR NEGLIGENCE OR CONTINGENCIES BEYOND LIGHT READING'S CONTROL IN COMPILING, PREPARING OR DISSEMINATING ANY REPORT OR FOR ANY DECISION MADE OR ACTION TAKEN BY SUBSCRIBER OR ANY THIRD PARTY IN RELIANCE ON SUCH INFORMATION OR FOR ANY CONSEQUENTIAL, SPECIAL, INDIRECT OR SIMILAR DAMAGES, EVEN IF LIGHT READING WAS ADVISED OF THE POSSIBILITY OF THE SAME. SUBSCRIBER AGREES THAT THE LIABILITY OF LIGHT READING, ITS EMPLOYEES, AFFILIATES, AGENTS AND LICENSORS, IF ANY, ARISING OUT OF ANY KIND OF LEGAL CLAIM (WHETHER IN CONTRACT, TORT OR OTHERWISE) IN CONNECTION WITH ITS GOODS/SERVICES UNDER THIS AGREEMENT SHALL NOT EXCEED THE AMOUNT YOU PAID TO LIGHT READING FOR USE OF THE REPORT IN QUESTION.