

The Emerging Mobile Malware Threat

Perry Carpenter, CISSP, CIPP

November 18, 2006

Executive Summary

The emerging mobile malware threat

Many analysts predict that the growing power, functionality, and popularity of smartphones may make mobile platforms an irresistible target for malware authors by the end of 2007. By this time, it is expected that there will be sufficient adoption of feature-rich smartphones coupled with the emergence of a dominate operating system. Smartphones capable of being infected will comprise roughly one third of the mobile phone market.

The current state of mobile malware

Malware for mobile devices exists today; most current examples have been written simply to prove the possibility, rather than for truly malicious purposes. However, because malware authors are able to leverage PC based malware experience within the mobile environment, the evolution of mobile malware is occurring with significant velocity. As the use of mobile devices for financial transactions and for housing sensitive personal/corporate data increases, malware authors will gain sufficient motive to focus their attention on mobile platforms.

As of this writing, mobile malware is capable of the following actions:

- Spreading via Bluetooth, MMS
- Sending SMS messages
- Infecting files
- Enabling remote control of the smartphone
- Modifying or replacing icons or system applications
- Installing “false” or non-operational fonts and applications
- Combating antivirus programs
- Installing other malicious programs
- Blocking memory cards
- Stealing data

Smartphones employ myriad communication vectors thereby increasing the potential propagation methods for mobile malware. Such methods include:

- Serial/USB port desktop synchronization
- Personal area networks (IrDA, Bluetooth)
- Wireless wide area phone networks (CDMA, GPRS, 1xRTT, EV-DO)
- Wireless local area networks (802.11, WiFi)
- Wireless metropolitan area networks (802.16, WiMax)
- Memory cards
- MMS downloads

The sophistication of mobile malware is has achieved rough parity with PC based malware. For example, mobile malware authors now employ blended attacks

resulting in malware with multiple propagation methods capable of infecting or utilizing multiple device-types/platforms, and performing multiple functions (such as keylogging and transmitting the resulting data via SMS).

Future Trends

Mobile malware will likely mature in parallel with the mobile industry as a whole. That is, as mobile commerce gains popularity, malware will be written to exploit that functionality by finding ways to harvest account numbers and credential sets, re-route transactions, or cause financial damage. Similarly, as location based services gain popularity, malware may be written which will surreptitiously transmit location data to criminals.

Current Industry Response

Most antivirus vendors, mobile carriers, and security advocates are beginning to mobilize.

- Several antivirus vendors currently offer anti-malware products for mobile devices.
- Sprint/Nextel recently announced a comprehensive security offering which includes mobile anti-malware, mobile firewall, device encryption, and policy-based device management options.
- CTIA, while downplaying the threat, suggests employing SMS and MMS filtering
- The Trusted Computing Group is creating standards for the development of secure mobile platforms

Recommendations

Begin taking proactive measures now. Recommendations include:

1. Support, and participate in, the Trusted Computing Group's Mobile Phone Work Group.
2. Ensure that antivirus software is installed and up-to-date on any desktop PC which is used to synchronize with mobile devices.
3. Build antivirus measures into the carrier networks in addition to handsets
4. Implement SMS and MMS message scanning/quarantining
5. Install firewall software on mobile devices
6. Turn off Bluetooth and 802.11 radios by default
7. Ensure that by default Bluetooth and 802.11 features operate in 'non-discoverable' mode
8. Encrypt sensitive data on mobile devices
9. Educate customers on how to detect suspicious messages, websites, and downloads
10. For businesses, create and enforce policies regarding the management of mobile devices within the corporate environment
11. Consider implementing security services for smartphone customers as a cost of business

Call to Action

While mobile malware proliferation has not yet reached epidemic proportions, this does not mean that the industry should stand idle. The wireless industry should begin defending against mobile threats now by creating resilient infrastructures which are content aware, educating users, and implementing technical safeguards on mobile devices.

Table of Contents

- Executive Summary i
 - The emerging mobile malware threat i
 - The current state of mobile malware..... i
 - Future Trends..... ii
 - Current Industry Response..... ii
 - Recommendations ii
 - Call to Action iii
- Table of Contents..... iv
- Table of Figures v
- 1 Introduction 1
- 2 A vision of the future 1
 - 2.1 Factors necessary to create a mobile malware problem2
 - 2.1.1 Widespread adoption of smartphones..... 2
 - 2.1.2 Emergence of a dominate mobile phone operating system 3
 - 2.1.3 Ability to exchange executable files 3
 - 2.1.4 Well-documented development tools 4
 - 2.1.5 Presence of vulnerabilities or coding errors 4
 - 2.1.6 Motive 4
 - 2.2 The European situation.....5
 - 2.3 Current smart phone adoption statistics & predictions.....7
 - 2.4 Mobile malware propagation methods translate into increased virulence.....7
 - 2.5 Blended attacks8
 - 2.6 A mobile threat scenario9
 - 2.6.1 Short example of mobile malware in action..... 10
 - 2.6.2 Commentary on example 10
- 3 Mobile Malware History 11
 - 3.1 June 2004 – present 11
 - 3.2 Mobile Malware Families 13
- 4 Current Trends..... 15
 - 4.1 Mobile Spyware 15
 - 4.2 SMiShing 16
 - 4.3 Cross-Platform Mobile Infectors 16
- 5 Future Threats 17
 - 5.1 m-Commerce 17
 - 5.2 Location Based Services (LBS) 18
- 6 What is the industry doing?..... 18
 - 6.1 Antivirus Vendors..... 19
 - 6.2 Mobile Carriers 20
 - 6.3 Cellular Telecommunications and Internet Association (CTIA)..... 21
 - 6.4 Trusted Computing Group Specification..... 21
- 7 Countermeasures 22
- 8 Conclusion..... 22

Table of Figures

Figure 1: Growth in mobile malware from June 2004 (Cabir) to Aug. 30, 2006. ...	1
Figure 2: Countries where Cabir was detected (September 2005)	6
Figure 3: Rise in smartphone adoption from 2003 – mid 2006	7
Figure 4: Summary of recognized mobile malware families as categorized by Kaspersky Lab.	13
Figure 5: The increase of known mobile malware variants	14
Figure 6: Increase in known mobile malware families.....	14
Figure 7: Sampling of current anti-malware offerings for smartphones.....	20

1 Introduction

The purpose of this paper is to evaluate the threat that malware poses to mobile devices, end-users, and carriers. The factors contributing to the mobile malware threat will be presented along with a brief analysis of the current trends with respect to each factor. A short history of mobile malware will serve to illustrate the types of attacks which are possible – and are currently being exploited. Current trends and future concerns will be discussed. Lastly, recommendations to mobile users and carriers will be presented.

2 A vision of the future

Most industry analysts agree that smartphones (mobile phones which combine the functionality of a traditional mobile phone with that of a PDA) will eventually rival the functionality and power of desktop based personal computers.¹ As mobile phones become more feature-rich, and their use for commerce increases, these devices will likely become ripe targets for hackers, identity thieves, and organized crime rings. Simply put, “[t]he convergence of mobile devices and commerce creates ‘perfect storm’ conditions for the emergence of significant mobile malware development/attacks.”²

If the rise in mobile malware between June 2004 and August 2006 is any indication, the popularity of mobile threats will continue to grow at an exponential rate.

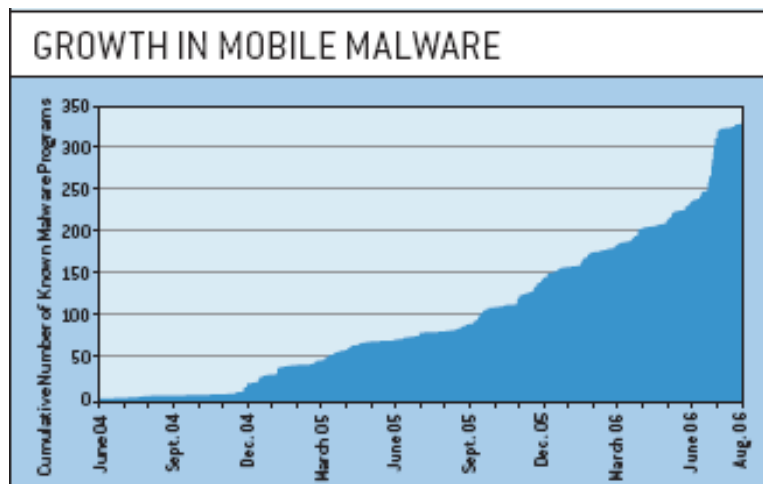


Figure 1: Growth in mobile malware from June 2004 (Cabir) to Aug. 30, 2006. Hypponen, Mikko. (November, 2006). Malware Goes Mobile. *Scientific American*, 295, 70-77

¹ Vamosi, Robert. (February 17, 2006). Your smart phone has a dumb virus. *ZDNet Security Watch: Don't get burned by viruses and hackers*. http://review.zdnet.com/4520-3513_16-6442087-1.html. Accessed October, 2006.

² Carpenter, Perry. (October 2006). “Mobile Malware.” Unpublished master’s essay, Norwich University, Northfield, VT, United States.

Paul Miller, the Director of Symantec's Mobile Security Group, notes that because malware authors are able to leverage PC based malware experience within the mobile environment, the evolution of mobile malware is occurring with significant velocity.³ "So, the milestones and the slope—the number of viruses we've seen in the mobile side—far outpace anything we ever experienced with the PC side."⁴

2.1 Factors necessary to create a mobile malware problem

Many analysts believe that the components necessary to create a truly significant mobile malware problem will be in place by late 2007.⁵ Therefore, it is incumbent upon mobile device manufactures, carriers, and antivirus companies to begin planning for and addressing the issue now. The threat of mobile malware increases as each of the following factors become true:^{6 7}

- Widespread adoption of smart phones
- The emergence of a dominant mobile phone operating system
- Wireless messaging to exchange executable files
- There must be well-documented development tools for the application
- The presence of vulnerabilities or coding errors
- Motive for writing malware (challenge/status/thrill, political gain, financial gain, or damage)

The following sections will briefly discuss each of these factors.

2.1.1 Widespread adoption of smartphones

In order for malware to be created, a base of devices must exist upon which the nefarious applications can be loaded. Further, in order to spread, there must be a number of similar devices placed in a situation which requires them to interoperate. For instance, if a virus is written specifically for Windows Mobile 2005, it will likely only have opportunity to spread when interconnecting with another Windows Mobile 2005 device. Therefore, in order for the virus to spread, Windows Mobile 2005 would need to be in use by a significant segment (or logically connected sub-segment) of the populous. Without widespread adoption, the malware is, in essence, quarantined.

³ Flamig, Blaine A. (December 2006). Mobile Bugs: A mere nuisance or a deadly swarm ready to attack?. *PC Today*. 4(12), 44-45.

<http://www.pctoday.com/editorial/article.asp?article=articles/2006/t0412/10t12/10t12.asp>. Accessed November, 2006.

⁴ Ibid.

⁵ Keizer, Gregg. (June 21, 2005). Don't Worry Yet; Mobile Worms Won't Show Until '07. *TechWeb*

⁶ Shor, Susan B. (June 22, 2005). *TechNewsWorld*. Mobile Malware Will Come, But When?.

<http://www.technewsworld.com/story/44079.html>. Accessed October 2006.

⁷ Gostev, Alexander. (September 29, 2006). Mobile Malware Evolution: An Overview, Part 1.

Viruslist.com. <http://www.viruslist.com/en/analysis?pubid=200119916>. Accessed October, 2006.

Industry analysts suggest that, before a major malware outbreak is possible, “smartphones capable of being infected [...] will make up around one third of the market.”⁸ Analysts further predict that the timeframe associated with the requisite market penetration is “likely no sooner than the end of 2007.”⁹

2.1.2 Emergence of a dominant mobile phone operating system

As noted in the above example, smartphones must not only gain significant penetration within the overall wireless market, but also share a common operating system (OS) or runtime environment (e.g. Java). Today, in the United States, there is a largely heterogeneous landscape of mobile platforms from which to choose. Thus, the potential for widespread virulence from mobile malware is limited. However, as demonstrated through the popularity of the Microsoft Windows PC environment, when significant market-share is achieved, the operating system becomes an attractive target to malware writers.

2.1.3 Ability to exchange executable files

In order to become virulent, malware must possess the ability to propagate; thus, the infected files must be able to be exchanged between systems.¹⁰ It is important to note that this does not necessarily require that executable files need to be exchangeable directly from phone to phone – only that infected files from one phone have a method for infecting other phones.¹¹ That being the case, the methods for exchanging files could include the sharing of memory cards or through synchronization of the smartphone to a PC.

Several methods for smartphone connectivity and file exchange currently exist. These include:^{12 13}

- Serial/USB port desktop synchronization
- Personal area networks (IrDA, Bluetooth)
- Wireless wide area phone networks (CDMA, GPRS, 1xRTT, EV-DO)
- Wireless local area networks (802.11, WiFi)
- Wireless metropolitan area networks (802.16, WiMax)

⁸ Munir, Kotadia. (June 21, 2005). Expect a ‘serious’ mobile phone virus in 2008. *ZDNet Australia*. http://www.zdnet.com.au/news/security/soa/Expect_a_serious_mobile_phone_virus_in_2008/0,130061744,139198008,00.htm. Accessed November 2006.

⁹ Ibid.

¹⁰ Shor, Susan B. (June 22, 2005). Mobile Malware Will Come, But When?. *TechNewsWorld*. <http://www.technewsworld.com/story/44079.html>. Accessed October 2006.

¹¹ Peikari, Cyrus. (March 8, 2006). Analyzing the Crossover Virus: The First PC to Windows Handheld Cross-infecter. *SAMS Publishing*.

<http://www.sampublishing.com/articles/article.asp?p=458169&seqNum=3&rl=1>. Accessed November 2006.

¹² Froemelt, Marc. (September 22, 2006). PDA & Smart Phone – Business Security Impact. *TechLinks: The Guide to Technology in Georgia*.

<http://www.techlinks.net/CommunityPublishing/tabid/92/articleType/ArticleView/articleId/3623/PDA--Smart-Phone---Business-Security-Impact-.aspx>. Accessed November 2006.

¹³ Vamosi, Robert. (February 17, 2006). Your smart phone has a dumb virus. *ZDNet Security Watch: Don't get burned by viruses and hackers*. http://review.zdnet.com/4520-3513_16-6442087-1.html. Accessed October, 2006.

- Memory cards
- MMS downloads

2.1.4 Well-documented development tools

Well-documented development tools are a requirement for any operating system to truly be accepted by the end-user community. This is because operating systems, in general, exist solely to support applications. Thus, methods and tools must be published in order to allow for application development. An unintended consequence of publishing such tools is that malware authors also gain access. This gives the authors critical information needed in the development of code targeted at exploiting vulnerabilities or coding errors within the operating system.¹⁴

2.1.5 Presence of vulnerabilities or coding errors

System vulnerabilities or coding areas are the life-blood of malware. Feature-rich operating systems usually result in unintended avenues which may be exploited by hackers or malware writers. These avenues generally exist because the developer (or development team) never anticipated the sequence of events that would lead to the vulnerability.¹⁵ Today's operating systems and applications are extremely complicated. These systems are created by humans—who are, by nature, flawed—resulting in flawed systems.¹⁶

Alexander Gostev, Senior Virus Analyst for Russian-based Kaspersky Lab, writes:

The factor which has most influence on the evolution of mobile malware is vulnerabilities in software and mobile device operating systems themselves. In the computing world, nearly all the major virus epidemics over the past few years have been caused by vulnerabilities in Windows. There are only two possible ways for remote malicious users to penetrate a potential victim system: by exploiting the human factor (social engineering) or by exploiting software coding errors (vulnerabilities). These attack vectors also apply to mobile devices.¹⁷

2.1.6 Motive

The last factor leading to the inevitability of malware is motive. Malicious code authors generally create malware for the same reason that hackers attack computer systems. The *Howard and Longstaff Computer and Network Incident Taxonomy* posits the following motives:¹⁸

- Challenge, status, or thrill

¹⁴ Gostev, Alexander. (September 29, 2006). Mobile Malware Evolution: An Overview, Part 1. *Viruslist.com*. <http://www.viruslist.com/en/analysis?pubid=200119916>. Accessed October, 2006.

¹⁵ Gibson, Steve. (November 9, 2006). Security Now 65: Why is Security so Difficult?. *Security Now! With Steve Gibson*. <http://www.twit.tv/sn65>.

¹⁶ Ibid.

¹⁷ Gostev, Alexander. (October 10, 2006). Mobile Malware Evolution: An Overview, Part 2. *Viruslist.com*. <http://www.viruslist.com/en/analysis?pubid=201225789>. Accessed October, 2006.

¹⁸ Howard, John D., Pascal, Meunier. (2002). Using a “Common Language” for Computer Security Incident Information. in *Computer Security Handbook*. (4th ed). New York: John Wiley & Sons, Inc.

- Political gain
- Financial gain
- Damage

In addition, Howard and Longstaff enumerate the types of criminals likely to relate to one of the aforementioned motives. They are:¹⁹

- **Hackers** – Attackers who attack computers for challenge, status, or the thrill of obtaining access.
- **Spies** – Attackers who attack computers for information to be used for political gain.
- **Terrorists** – Attackers who attack computers to cause fear for political gain.
- **Corporate raiders** – Employees (attackers) who attack competitor's computers for financial gain
- **Professional criminals** – Attackers who attack computers for personal financial gain.
- **Vandals** – Attackers who attack computers to cause damage.
- **Voyeurs** – Attackers who attack computers for the thrill of obtaining sensitive information.

Note that, in the list above, the term 'computers' can easily be replaced with the term 'smartphones,' 'mobile devices,' or 'mobile networks.' That is, hackers and malware writers are driven by the same motives – but are targeting new platforms and technologies.

2.2 The European situation

In Europe the Symbian smart phone operating system is the market leader – enjoying a 71% market-share.²⁰ As a result, most of the mobile malware developed today targets that platform; about 10 new Symbian OS Trojans are discovered and cataloged each week.²¹ While still not at critical levels, European mobile phone users are becoming increasingly aware of malware threats.

The first truly notable mobile malware program, Cabir, a Symbian-based worm capable of spreading via Bluetooth wireless connections, was released to antivirus companies in June of 2004.²² After discovering that the worm was “in the wild,” antivirus vendors F-Secure and Kaspersky Lab undertook a joint effort to track Cabir's spread.²³ Within one year the virus had spread to more than 20

¹⁹ Ibid.

²⁰ Symbian “Fast Facts” as of July 2006. <http://www.symbian.com/about/fastfacts/fastfacts.html>. Accessed November 2006.

²¹ Gostev, Alexander. (September 29, 2006). Mobile Malware Evolution: An Overview, Part 1. *Viruslist.com*. <http://www.viruslist.com/en/analysis?pubid=200119916>. Accessed October, 2006.

²² Gostev, Alexander. (October 10, 2006). Mobile Malware Evolution: An Overview, Part 2. *Viruslist.com*. <http://www.viruslist.com/en/analysis?pubid=201225789>. Accessed October, 2006.

²³ Ibid.

countries, at which time the vendors began to lose count.²⁴ The following is a list of the countries in which Cabir was detected between July 2004 and September 2005.²⁵

1	Philippines
2	Singapore
3	UAE
4	China
5	India
6	Finland
7	Vietnam
8	Turkey
9	Russia
10	UK
11	Italy
12	USA
13	Japan
14	Hong Kong
15	France
16	South America
17	The Netherlands
18	Egypt
19	Luxembourg
20	Greece
21	Ukraine
22	New Zealand
23	Switzerland
24	Germany

Figure 2: Countries where Cabir was detected
(September 2005, combined data from F-Secure and Kaspersky Lab)

Perhaps the best known mobile malware ‘outbreak’ occurred in August 2005 at the 10th Athletics World Championship in Helsinki, Finland; during the event, the Cabir worm infected dozens of phones.²⁶ This incident was most significant because it demonstrated the ‘airborne’ nature of mobile malware which can spread via Bluetooth. In such cases, mobile malware is transmitted via close contact – similar to the human-borne flu virus.

Several other malware programs which target the Symbian platform are consistently being released and discovered in Europe and throughout the globe. However, Symbian’s lower market-share in the Americas, due to competing mobile network technologies (GSM v. CDMA) has allowed many in the US to

²⁴ Ibid.

²⁵ Ibid.

²⁶ Leyden, John. (August 12, 2005). Cabir mobile worm gives track fans the run around. *The Register*. http://www.theregister.co.uk/2005/08/12/cabir_stadium_outbreak/. Accessed November 2006.

become lulled into a false sense of security regarding mobile malware.²⁷ In an interview with Mikko Hypponen, Chief Research Officer of the Finnish antivirus company, F-Secure, PC Today columnist Blaine A. Flamig writes, “[...] because the United States is a larger battleground between competing and incompatible platforms, ‘the sooner one platform gains dominant and lasting market share, the sooner danger will focus on it.’”²⁸

2.3 Current smart phone adoption statistics & predictions

Figure 3 summarizes the dramatic increase in smartphone adoption from the beginning of 2003 through Q2 of 2006. Recently released statistics report that 34.7 million smartphone units were shipped in the first half of 2006.²⁹ This represents a 75.5 percent increase over the previous year.³⁰ By 2009, industry experts predict that 350 million smartphones will be in use.³¹

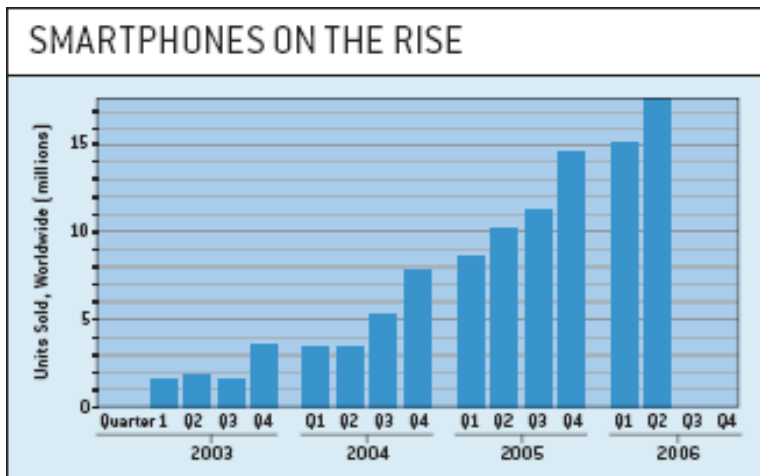


Figure 3: Rise in smartphone adoption from 2003 – mid 2006
Hypponen, Mikko. (November, 2006). Malware Goes Mobile. *Scientific American*, 295, 70-77

2.4 Mobile malware propagation methods translate into increased virulence

A recent development in mobile malware transmission methods has taken some security experts by surprise; this method has been labeled as ‘typhoid-like.’

²⁷ Carpenter, Perry. (October 2006). “*Mobile Malware.*” Unpublished master’s essay, Norwich University, Northfield, VT, United States.

²⁸ Flamig, Blaine A. (December 2006). Mobile Bugs: A mere nuisance or a deadly swarm ready to attack?. *PC Today*. 4(12), 44-45.

<http://www.pctoday.com/editorial/article.asp?article=articles/2006/t0412/10t12/10t12.asp>. Accessed November, 2006.

²⁹ Gartner.com. (October 9, 2006). Gartner Says Worldwide Combined PDA and Smartphone Shipments Market Grew 57 Percent in the First Half of 2006. *Gartner Media Relations*.

<http://www.gartner.com/it/page.jsp?id=496997>. Accessed November 2006.

³⁰ Ibid.

³¹ Hypponen, Mikko. (November 2006). Malware Goes Mobile. *Scientific American*, 295, 70-77

Like the way mosquitoes can infect multiple hosts (birds, people, etc.) with Eastern Equine Encephalitis (EEE)³² while remaining unaffected themselves by the disease, mobile devices can simply be used as carriers that leverage synching mechanisms and USB connections to infect multiple hosts and the media (permanent and removable) they have access to.³³

Further, because smartphones offer multiple methods of connectivity (e.g. Bluetooth, 802.11, EV-DO, SMS/MMS, and voice) the propagation paths available to malicious code authors are myriad. Many analysts liken the transmission paths to that of the common cold or flu. Mobile viruses can be written to find multiple points of transmission just as the common cold can be transmitted via handshakes, aerosol, or contact with recently touched surfaces such as doorknobs. An interview with Paul Miller of Symantec's Mobile Security Group notes that,

Whereas a PC virus radiates from a central point outward across networks making it easy to track, [...] a mobile virus will try to jump from device to device using any network available without always maintaining a network connection. "The phone and voice service is always there, but the data network is on a demand basis. So, if you're a virus, you're looking for any way to hop from device A to device B."³⁴

2.5 Blended attacks

Key findings presented in the Corporate Executive Board's June 2005 *Trends in IT Security Threats* report suggested that malicious code, phishing, blended attacks, mobile device viruses, and target specific attacks were all emerging security threats.³⁵ In November 2006, these "emerging" threats are all a reality. Specifically, blended attacks are being utilized on both PC and smartphone platforms in order to create multifunctional malware.

The Corporate Executive Board says of blended attacks:

Blended threats deploy combinations of malicious code to begin, transmit, and spread exploit code, which target systems and network vulnerabilities to obtain unauthorized access to confidential information. Blended threats target several vulnerabilities simultaneously and are capable of transmission without any human intervention. These threats continuously search for vulnerable servers and user computers to compromise.

As blended threats based attacks deploy multiple techniques simultaneously, these threats can spread to across large numbers of hosts in a short timeframe. In

³² CDC.gov. (July 2006). Eastern Equine Encephalitis Fact Sheet. *Centers for Disease Control*. <http://www.cdc.gov/ncidod/dvbid/arboreeefact.htm>. Accessed November 2006.

³³ Berlind, David. (September 6, 2006). Typhoid cell-phones: The latest threat in malware transmission. *ZDNet blog: Between the Lines*. <http://blogs.zdnet.com/BTL/?p=3565>. Accessed November 2006.

³⁴ Flamig, Blaine A. (December 2006). Mobile Bugs: A mere nuisance or a deadly swarm ready to attack?. *PC Today*. 4(12), 44-45. <http://www.pctoday.com/editorial/article.asp?article=articles/2006/t0412/10t12/10t12.asp>. Accessed November, 2006.

³⁵ Corporate Executive Board. (June 2005). Trends in IT Security Threats. *Corporate Executive Board*. Catalog No.: IEC13EKU9P.

addition, as blended threats attack on multiple levels simultaneously and deploy multiple means of transmission, they are difficult to detect.³⁶

As mobile malware becomes increasingly blended, the virulence and potential for significant impacts increase. For example, a blended attack could employ a Bluetooth vulnerability to transmit a Trojan horse program containing a keylogger which collects user credentials for online accounts and sends the credentials via SMS to a premium SMS number owned by the malware author. Thus, not only have the victim's mobile phone and account credentials been compromised, but his/her bill will reflect the escalated charges associated with premium SMS (which allows the recipient to charge a fee for the SMS session).

Further, the victim's phone may be co-opted into a botnet, thereby "...become[ing] part of a global network, with each phone potentially sending thousands of SMS messages. Considering the cost of sending SMS messages, the financial implications of having your phone hijacked could potentially be far greater than having your PC used as a vector to send spam."³⁷

2.6 A mobile threat scenario

Current and future mobile malware threats are likely to employ "blended attacks" similar to that described in the above scenario. As the power and functionality of smartphones continue to increase, coupled with increased popularity for smartphone-driven financial transactions, smartphones platforms will likely become an irresistible target for malware authors seeking financial gain – or seeking to inflict financial harm. Positing the future of mobile malware, F-Secure's Mikko Hypponen considers the current state of PC and mobile malware, writing:

Since 2003 much of the new malware appearing on PCs has been written for profit rather than for mere mischief. Organized gangs of cyber-criminals now operate all over the world. Thieves use crimeware to make money by stealing financial data, business secrets or computer resources. Spammers assemble "botnets" of hacked machines to forward bulk e-mail and phishing scams. And blackmailers extort money with threats of digital destruction or of virtual blockades that shut down a company's Web or e-mail servers.

[...] A [mobile malware] Trojan called RedBrowser sends a continuous stream of text messages from any phone it infects to a number in Russia until the user disables the phone. Each message is charged at a premium rate of about five dollars, resulting in huge bills for the unfortunate victims. Some cellular carriers hold their customers liable for such unauthorized transactions, and when they do,

³⁶ Ibid.

³⁷ Beer, Stan. (June 13, 2006). Mobile phone botnets are poised to come calling. *The Sydney Morning Herald*. <http://www.smh.com.au/news/security/mobile-phone-botnets-are-poised-to-strike/2006/06/12/1149964442180.html>. Accessed October 2006.

the criminals, who own the premium number, collect the premium fees. Luckily, RedBrowser has so far only been spotted inside Russia.³⁸

CNET Reviews editor Robert Vamosi further comments:

[S]mart phones will soon replace our laptop or desktop PCs, if not our credit cards and personal keyrings. With this in mind, the idea that a virus could cripple your smart phone starts to take on much more meaning than just not being able to make a personal phone call; a mobile-device virus could one day steal your identity or lock you out of your house.³⁹

2.6.1 Short example of mobile malware in action

CNET Reviews columnist Robert Vamosi, in his article “Your smart phone has a dumb virus,” creates a fictional scenario outlining the most common method in which smartphones are currently infected; the scenario is as follows:

It's the night of the Big Game. You've just concluded a business meeting in a strange part of town, and you stop into a sports bar for a drink and a chance to catch some of the action. Five minutes turns into 10 into 20, and suddenly you realize you're very late for your call home. You reach into your pocket and pull out your Bluetooth-enabled smart phone, but you can't dial out. A message across the display says that someone from a Panasonic phone wants to send you a message--yes or no? You look around and quickly realize that you probably don't know anyone at the sports bar, so you thumb no. The message returns. And the message keeps returning. Do you know what to do next? Do you even suspect or realize that your mobile device is about to be infected with one of about 150 known mobile-device viruses?⁴⁰

2.6.2 Commentary on example

The above scenario is strikingly similar to the method used in the previously mentioned propagation of the Cabir worm at the 10th Athletics World Championship in Helsinki, Finland. In this scenario, users who possess phones with an enabled Bluetooth connection operating in a discoverable mode are susceptible to other, nearby, phones infected with Cabir.

In these cases, users are bombarded with messages asking them to accept the message/file. They usually click “no,” but the message keeps coming back – preventing the user from being able to access the phone's other features, including making or receiving calls.⁴¹ So, in an act of desperation, the user gives up, and accepts the connection, thus infecting his/her phone with one of the

³⁸ Hypponen, Mikko. (November, 2006). Malware Goes Mobile. *Scientific American*, 295, 70-77

³⁹ Vamosi, Robert. (February 17, 2006). Your smart phone has a dumb virus. *ZDNet Security Watch: Don't get burned by viruses and hackers*. http://review.zdnet.com/4520-3513_16-6442087-1.html. Accessed October, 2006.

⁴⁰ Ibid.

⁴¹ Hypponen, Mikko. (November, 2006). Malware Goes Mobile. *Scientific American*, 295, 70-77

many Cabir variants.⁴² This happens primarily because users do not realize that, to stop the cycle, they could simply walk outside the range of the incoming Bluetooth signal (approximately 30 feet).⁴³

This scenario is disturbing because it is the equivalent to an email user being tricked into opening an attachment containing malware. The security industry has spent an enormous amount of time and effort in an attempt to educate users not to open any message or attachment from an unknown source. For smartphone users, these lessons seem to have not transitioned from the PC to the mobile domain. Clearly, this is an opportunity for mobile device manufacturers, mobile carriers, and security vendors/advocates to begin a new awareness effort targeting this area.

3 Mobile Malware History

The history of mobile malware is generally measured from June 2004 (the release of Cabir). Since that time, the rate of growth has consistently sent the message that mobile malware is emerging as a legitimate threat. To date, most of the malware targeting mobile devices has been proof of concept code written to call attention to potential threats. However, there are a few examples of code written to cause serious damage, steal data, eavesdrop on conversations, and incur additional charges on customer accounts.

The following brief summary of mobile malware history is intended to highlight the threats posed by mobile malware. The reader is encouraged to posit the potential damage posed by future malware which will blend and extend the capabilities seen thus far.

3.1 June 2004 – present

The first mobile worm, Cabir, was released in June, 2004. This worm leveraged Bluetooth functionality as its propagation method; as outlined in section 2.6.1, this worm bombarded users with requests to establish a connection such that they cannot perform other mobile phone functions until they agree to accept the connection (or move outside of the Bluetooth range of the device attempting to initiate the connection).⁴⁴

By late 2004, the first mobile phone Trojan arrived (Mosquit.a); this Trojan was also the first adware for mobile phones.⁴⁵ And in November 2005, the Skuller.a Trojan was released. This Trojan was the first to take advantage of a design flaw in the Symbian OS which allowed the “vandal Trojan” to overwrite system files.⁴⁶

⁴² Ibid.

⁴³ Ibid.

⁴⁴ Ibid.

⁴⁵ Gostev, Alexander. (September 29, 2006). Mobile Malware Evolution: An Overview, Part 1. *Viruslist.com*. <http://www.viruslist.com/en/analysis?pubid=200119916>. Accessed October, 2006.

⁴⁶ Ibid.

By early 2005, three main mobile malware types existed:⁴⁷

- worms that spread via smartphone protocols and services
- vandal Trojans that install themselves to the system by exploiting Symbian design faults
- Trojans designed for financial gain

The table below, compiled by Kaspersky Lab, is a summary of the major steps in mobile malware evolution since the introduction of Cabir.

Name	Date	OS	Functionality	Technology used	Number of variants
Worm.SymbOS.Cabir	Jun-04	Symbian	Spreads via Bluetooth	Bluetooth	15
Virus.WinCE.Duts	Jul-04	Windows CE	Infects files	(File API)	1
Backdoor.WinCE.Brador	Aug-04	Windows CE	Provides remote network access	(Network API)	2
Trojan.SymbOS.Mosquit	Aug-04	Symbian	Sends SMS messages	SMS	1
Trojan.SymbOS.Skuller	Nov-04	Symbian	Replaces files, icons, system applications	OS vulnerability	31
Worm.SymbOS.Lasco	Jan-05	Symbian	Spreads via Bluetooth, infects files	Bluetooth, File API	1
Trojan.SymbOS.Locknut	Feb-05	Symbian	Installs corrupted applications	OS vulnerability	2
Trojan.SymbOS.Dampig	Mar-05	Symbian	Replaces system applications	OS vulnerability	1
Worm.SymbOS.ComWar	Mar-05	Symbian	Spreads via Bluetooth and MMS, infects files	Bluetooth, MMS, File API	7
Trojan.SymbOS.Drever	Mar-05	Symbian	Replaces antivirus application loaders	OS vulnerability	4
Trojan.SymbOS.Fontal	Apr-05	Symbian	Replaces font files	OS vulnerability	8
Trojan.SymbOS.Hobble	Apr-05	Symbian	Replaces system applications	OS vulnerability	1
Trojan.SymbOS.Appdisabler	May-05	Symbian	Replaces system applications	OS vulnerability	6
Trojan.SymbOS.Doombot	May-05	Symbian	Replaces system applications, installs Comwar	OS vulnerability	17
Trojan.SymbOS.Blankfont	Jul-05	Symbian	Replaces font files	OS vulnerability	1
Trojan.SymbOS.Skudoo	Aug-05	Symbian	Installs damaged applications, installs Cabir, Skuller, Doombor	OS vulnerability	3

⁴⁷ Ibid.

Name	Date	OS	Functionality	Technology used	Number of variants
Trojan.SymbOS.Singlejump	Aug-05	Symbian	Disables system functions, replaces icons	OS vulnerability	5
Trojan.SymbOS.Bootton	Aug-05	Symbian	Installs damaged applications, installs Cabir	OS vulnerability	2
Trojan.SymbOS.Cardtrap	Sep-05	Symbian	Deletes antivirus files, replaces system applications, installs Win32 malware on memory cards	OS vulnerability	26
Trojan.SymbOS.Cardblock	Oct-05	Symbian	Blocks memory cards, deletes folders	OS vulnerability, File API	1
Trojan.SymbOS.Pbstealer	Nov-05	Symbian	Steals data	Bluetooth, File API	5
Trojan-Dropper.SymbOS.Agent	Dec-05	Symbian	Installs other malicious programs	OS vulnerability	3
Trojan-SMS.J2ME.RedBrowser	Feb-06	J2ME	Sends SMS	Java, SMS	2
Worm.MSIL.Cxover	Mar-06	Windows Mobile/.NET	Deletes files, copies its body to other devices	File (API), NetWork (API)	1
Worm.SymbOS.StealWar	Mar-06	Symbian	Steals data, spreads via Bluetooth and MMS	Bluetooth, MMS, File (API)	5
Email-Worm.MSIL.Letum	Mar-06	Windows Mobile/.NET	Spreads via email	Email, File (API)	3
Trojan-Spy.SymbOS.Flexispy	Apr-06	Symbian	Steals data	—	2
Trojan.SymbOS.Rommwar	Apr-06	Symbian	Replaces system applications	OS vulnerability	4
Trojan.SymbOS.Arifat	Apr-06	Symbian	—	—	1
Trojan.SymbOS.Romride	Jun-06	Symbian	Replaces system applications	OS vulnerability	8
Worm.SymbOS.Mobler.a	Aug-06	Symbian	Deletes antivirus files, replaces system applications, spreads via memory card	OS vulnerability	

Figure 4: Summary of recognized mobile malware families as categorized by Kaspersky Lab.

Source: Gostev, Alexander. (September 29, 2006). Mobile Malware Evolution: An Overview, Part 1. *Viruslist.com*.

<http://www.viruslist.com/en/analysis?pubid=200119916>.

3.2 Mobile Malware Families

As of August 30, 2006, Kaspersky Lab recognizes 31 specific families of mobile malware. The 31 families are logical groups, based on similar code-bases and functionality sets shared among 170 variants. Figure 5 illustrates the rise of malware variants from June 2004 through August 2006.

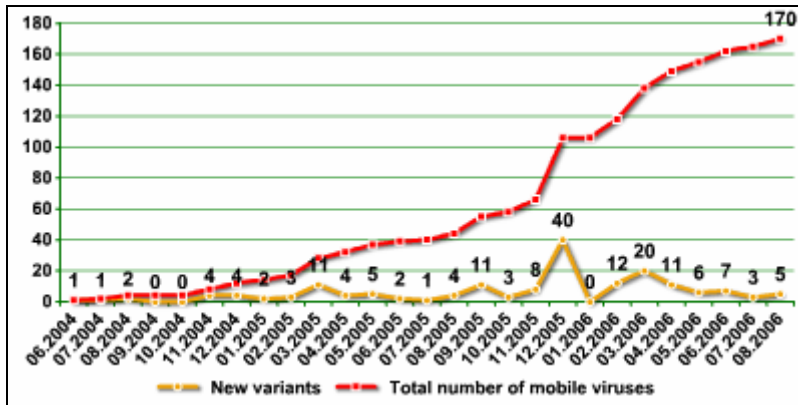


Figure 5: The increase of known mobile malware variants

Source: Gostev, Alexander. (September 29, 2006). Mobile Malware Evolution: An Overview, Part 1. *Viruslist.com*. <http://www.viruslist.com/en/analysis?pubid=200119916>

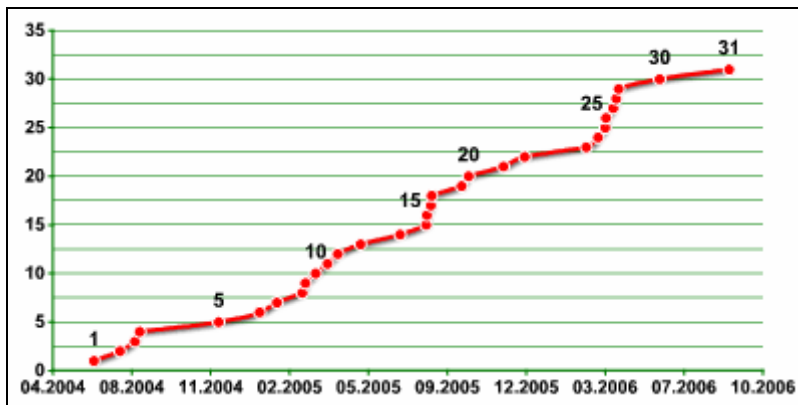


Figure 6: Increase in known mobile malware families.

Source: Gostev, Alexander. (September 29, 2006). Mobile Malware Evolution: An Overview, Part 1. *Viruslist.com*. <http://www.viruslist.com/en/analysis?pubid=200119916>

Research performed by Kaspersky Lab suggests that mobile malware is currently capable of performing the following functions:⁴⁸

- Spread via Bluetooth, MMS
- Send SMS messages
- Infect files
- Enable remote control of the smartphone
- Modify or replace icons or system applications
- Install “false” or non-operational fonts and applications
- Combat antivirus programs
- Install other malicious programs
- Block memory cards
- Steal data

⁴⁸ Gostev, Alexander. (September 29, 2006). Mobile Malware Evolution: An Overview, Part 1. *Viruslist.com*. <http://www.viruslist.com/en/analysis?pubid=200119916>. Accessed October, 2006.

Referring to the categorization of mobile viruses, Kaspersky Lab Senior Virus Analyst, Alexander Gostev states,

We have to acknowledge that today's mobile viruses are very similar to computer viruses in terms of their payload. However, it took computer viruses over twenty years to evolve, and mobile viruses have covered the same ground in a mere two years. Without doubt, mobile malware is the most quickly evolving type of malicious code, and clearly still has great potential for further evolution.⁴⁹

4 Current Trends

4.1 Mobile Spyware

In March 2006 antivirus company F-Secure discovered, and reported as malware, a program called FlexiSPY Light – sparking much controversy.⁵⁰ This software is a commercial product, marketed as a spouse monitoring tool, that records information about a user's mobile phone calls, saves the data, and then surreptitiously sends the information via SMS to a server hosted by the vendor. Vervata, the product's vendor, touts the application as “the world's first spy application designed and built exclusively for the mobile phone [that is] absolutely undetectable by the user.”⁵¹

The company further promises that development on a more powerful version is underway which will relay real-time conversations.⁵² F-Secure's labeling of FlexiSPY as malware was controversial because installation of the product requires physical access to the mobile device. However, F-Secure's position is that the software acts in a malicious manner by spying on the phone's user and being undetectable.⁵³

Regardless of whether or not FlexiSPY should be deemed malware, there is the possibility that such software could be combined with a propagation mechanism such as Cabir and included as the payload for a Trojan horse program. The successful blending of these components leads to a truly powerful tool useful to corporate spies, identity thieves, foreign governments, or organized crime rings. In addition, the theft of corporate documents containing customer information may trigger data breach notification requirements such as stated in California's SB1386 and similar laws enacted or pending in over 30 additional states.⁵⁴

⁴⁹ Ibid.

⁵⁰ Leyden, John. (March 2006). Trojan row over spouse monitoring software. *Channel Register*. <http://www.channelregister.co.uk/2006/03/30/flexispy/>. Accessed November 2006.

⁵¹ Ibid. Quoting from Vervata's website (<http://www.FlexiSpy.com/light.html>).

⁵² Ibid.

⁵³ Ibid.

⁵⁴ National Conference of State Legislatures. <http://www.ncsl.org/programs/lis/cip/priv/breach.htm>. Accessed November 2006.

4.2 SMiShing

Another recent trend is the targeting of mobile phones for phishing messages. In August of 2006, McAfee Avert Labs Blog reported the new trend, and labeled it “SMiShing.”⁵⁵ The name is intended to be a cross between the terms SMS (Short Message Service) and “phishing.”

SMiShing represents another new type of blended attack. In reported incidents, attackers attempt to use social engineering techniques to trick users into navigating to malicious websites via their PC. McAfee’s David Rayhawk describes the attack as follows:

[U]sers have started receiving SMS messages along these lines: “We’re confirming you’ve signed up for our dating service. You will be charged \$2/day unless you cancel your order: www.smishinglink.com”. (This is an example and was not a real url at the time of writing)

While some might recognize this as a scam, many unsuspecting users would not. Fearful of incurring premium rates on their cell phone bill, they visit the Web site highlighted in the message. Once they arrive at the URL, they are prompted to download a program which is actually a Trojan horse that turns the computer into a zombie, allowing it to be controlled by hackers. The computer then becomes part of a bot network, which can then be used to launch denial of service attacks, install keylogging software and steal personal account information and other malicious activities. Because monitoring botnet activity is complex, it is challenging to know the current scope of the problem.⁵⁶

As this technique grows in sophistication, attackers will likely attempt to create associated websites which are browser aware; this would allow the attacker to target multiple versions/types of malicious code intended to exploit specific vulnerabilities in whichever platform the victim uses to navigate to the site (whether via smartphone or PC).

4.3 Cross-Platform Mobile Infectors

For increased effectiveness, mobile malware authors are beginning to create malcode that is operating system aware. This new breed of malware is intent on survival and the ability to successfully propagate. Viruses such as Cardtrap-A can infect mobile devices running the Symbian 60 operating system, spread via Bluetooth and MMS, and infect the phone’s memory card with a Win32 operating system virus.⁵⁷ If a user attempts to read the memory card on a Windows PC, the system will be infected.

⁵⁵ Rayhawk, David. (August 25, 2006). SMiShing - an emerging threat vector. *McAfee Avert Labs Blog*. <http://www.avertlabs.com/research/blog/?p=74>. Accessed November 2006.

⁵⁶ Ibid.

⁵⁷ Leyden, John. (September 22, 2005). PC-hopping mobile malware sighted. *The Register*. <http://www.securityfocus.com/news/11328>. Accessed November 2006.

A recently released virus, Crossover, performs the opposite function of Cardtrap-A; it attempts to infect mobile devices from a PC.⁵⁸ A description of the virus functionality is as follows:

When executed from Win32, the Trojan checks what version the current OS is; if it is not Windows CE or Windows Mobile, the virus makes a copy of itself and puts a startup command in the registry key of local-machine-current-version-run. The trojan then quietly waits for an ActiveSync connection to be detected; it can wait indefinitely. When an ActiveSync connection is detected, the trojan automatically copies itself to the handheld device and remotely executes the trojan. The handheld device is now infected. The Trojan will then begin to delete documents on the handheld.

[...]

Upon execution, the malware will first check to see what type of host operating system on which it resides. If the OS is not Windows CE or Windows Mobile, it will assume it is a desktop running some flavor of Windows. If the malware does not detect the mobile environment, it will make a copy of itself in the Windows folder and will add a registry entry pointing to the new file at HKLM\Software\Microsoft\Windows\CurrentVersion\Run to execute the new file each and every time the OS is rebooted. Then the executable goes into a loop until an ActiveSync connection is detected.⁵⁹

As the functionality of cross-platform infectors is expanded upon, mobile malware will undoubtedly gain increased virulence. Malware authors will look to exploit this capability to reach the greatest possible number of platforms and victims.

5 Future Threats

The convergence of technologies and services made possible by smartphones will likely give rise to malware that is more invasive than ever before. Many aspects of society are embracing the mobile phone as a way of life – the one piece of equipment (or accessory) that is never left behind. Because these devices are always at hand, consumers will begin to use the devices in ways which are more integrated into their daily lifestyles. Two examples are mobile commerce and location based services.

5.1 m-Commerce

The emergence of mobile based commerce, known as m-Commerce⁶⁰ (e.g. online banking, stock trading, shopping, and proximity payments) will offer an attractive target to the identity thieves and attackers seeking financial reward. m-

⁵⁸ Peikari, Cyrus. (March 8, 2006). Analyzing the Crossover Virus: The First PC to Windows Handheld Cross-infecter. *SAMS Publishing*. <http://www.sampublishing.com/articles/article.asp?p=458169&seqNum=3&rl=1>. Accessed November 2006.

⁵⁹ Ibid.

⁶⁰ Mobile Payment Forum. <http://www.mobilepaymentforum.org/home>. Accessed November 2006.

Commerce will offer malware authors the same financial motives within the mobile domain as currently exist with the PC domain. At that time, there will likely be blended attacks using multiple propagation methods which install keyloggers for purposes of sending SMS messages containing sensitive account information and credential sets back to systems controlled by the attacker.

Some security analysts also posit that, at that time, attackers will have the incentive necessary to utilize smartphones as zombies within a botnet.⁶¹

5.2 Location Based Services (LBS)

The author has not currently seen reports or speculation regarding this, but believes that, as mobile carriers adopt and sell product offerings involving location based services (direction and tracking services based on global positioning systems embedded in smartphones), malware authors will see value in this data.

Malcode associated with location based services could be integrated into products such as FlexiSPY, allowing an attacker to know and track the whereabouts of an individual victim. Thus, services currently intended to help concerned parents keep a close eye on their children, such as Verizon's "Chaperone" offering,⁶² may become avenues for unspeakable abuse.

6 What is the industry doing?

F-Secure's Mikko Hypponen likens the mobile malware issue as it exists in 2006 to the state of PC malware in 1998. Hypponen warns:

In 1988 many computer experts dismissed viruses as inconsequential novelties. That assessment proved regrettably naive. For mobile malware, the time is now 1988, and we have a brief window in which to act to avoid repeating the mistakes of the past.

One such mistake was to underestimate how quickly malware would grow in prevalence, diversity and sophistication. Prevalence is a function of both the population of potential hosts for virtual pathogens and of their rate of infection. The target population for malicious mobile software is enormous and growing by leaps. There are now more than two billion mobile phones in the world.

It is true that the great majority of these are older cell phones running closed, proprietary operating systems that are largely immune from viral infection. But customers are quickly abandoning these devices for newer generations of smartphones that run more open operating systems, Web browsers, e-mail and other messaging clients and that contain Flash memory card readers and short-

⁶¹ Hypponen, Mikko. (November, 2006). Malware Goes Mobile. *Scientific American*, 295, 70-77

⁶² Verizon Wireless. (June 12, 2006). Verizon Wireless Launches "Chaperone" Service – A Great Tool To Keep Your Family In Touch . *Verizon Wireless News Center*. <http://news.vzw.com/news/2006/06/pr2006-06-12.html>. Accessed November 2006.

range Bluetooth radios. Each of these features offers a conduit through which malware can propagate.⁶³

Recognizing the coming danger, vendors and mobile carriers are beginning to take action. Within the past several months, multiple antivirus vendors have announced new or updated mobile security offerings. Further, mobile carriers are either beginning to offer, or are researching, mobile security at the network and handset levels. However, some analysts and mobile industry insiders believe that the threat is overstated.^{64 65 66}

6.1 Antivirus Vendors

Antivirus companies such as F-Secure, McAfee, Trust Digital, and Symantec are beginning to offer anti-malware for smartphones. For example, F-Secure's *Mobile Anti-Virus* product offers the following features (as stated on the vendor's website):⁶⁷

- Provides real-time on-device protection with automatic over-the-air antivirus updates through a patented SMS update mechanism or HTTPS connections.
- Transparent real-time protection against harmful content in the device and memory cards
- Automatic antivirus database updates from F-Secure Anti-Virus Research to the mobile terminals over an HTTPS data connection or incrementally with SMS messages
- Automatic detection of GPRS connections for updates from the terminal
- Over-the-air activation off the antivirus service through HTTPS
- Automatic updates of the F-Secure Mobile Anti-Virus client
- Digitally signed antivirus databases and database updates.

Vendors also recognize that antivirus represents only one measure of protection against malware. Therefore, vendors are also beginning to offer more encompassing products, such as F-Secure's *Mobile Security* product which includes the features listed above with the addition of a smartphone-based personal firewall.⁶⁸

⁶³ Hypponen, Mikko. (November, 2006). Malware Goes Mobile. *Scientific American*, 295, 70-77

⁶⁴ Hines, Matt. (April 18, 2006). Analysts Speak Out on the Wireless Security Hype. *eWeek.com*. <http://www.eweek.com/article2/0,1895,1950790,00.asp>. Accessed November 2006.

⁶⁵ Anonymous CTIA official. (November 10, 2006). Telephone interview.

⁶⁶ Hoskyn, Jane. (June 9, 2006). Symbian dismisses smartphone security risk: Mobiles can be 'keystones of security' if used correctly. *IT Week.com UK*. http://www.itweek.co.uk/vnunet/news/2157916/symbian-dismisses-smartphone?vnu_it=itw_art_related_articles. Accessed November 2006.

⁶⁷ F-Secure. F-Secure Mobile Anti-Virus. <http://www.f-secure.com/estoreusa/avmobile.html>. Accessed November 2006.

⁶⁸ F-Secure. F-Secure Mobile Security. <http://www.f-secure.com/estoreusa/avmobilesecurity.html>. Accessed November 2006

Some Protective Software for Smartphones		
COMPANY	PROGRAM NAME	SUPPORTED OPERATING SYSTEMS
F-Secure	Mobile Anti-Virus	PocketPC, Symbian, Windows Mobile
	Mobile Security	Nokia Communicators
McAfee	VirusScan Mobile	PocketPC, Symbian, Windows Mobile
Symantec	AntiVirus for Handhelds	Palm, PocketPC, Windows Mobile
	Mobile Security	Symbian
Trend Micro	Mobile Security	PocketPC, Symbian, Windows Mobile

Figure 7: Sampling of current anti-malware offerings for smartphones.

Source: Hypponen, Mikko. (November, 2006). Malware Goes Mobile. *Scientific American*, 295, 70-77

6.2 Mobile Carriers

In September of 2006, Sprint/Nextel announced a new mobile product offering that is likely to cause other mobile carriers to take note. The offering, Sprint Mobile Security, is marketed as a complete security solution.⁶⁹ The following services are offered as components within the Sprint Mobile Security suite:⁷⁰

- Data Protection
 - Device or File encryption
 - Mobile VPN
- Threat Prevention
 - Antivirus / anti-malware
 - Firewall
 - Remote device lock
 - Remote data wipe
- Compliance
 - Device policy compliance to corporate standards
 - Automatic remediation which will update non-compliant devices automatically

As businesses and individual smartphone users become increasingly security conscious with regard to mobile devices, offerings such as Sprint Mobile Security should attract customers. The PC security market is currently dominated by product suites offering antivirus, anti-spyware, anti-phishing, and firewalls. Users will likely seek the same comprehensive protection when selecting a mobile security solution.

⁶⁹ Sprint/Nextel. (September 19, 2006). Sprint Mobile Security Offers unmatched Seamless End-User Security for Mobile Workforce. *Sprint Nextel*. http://www2.sprint.com/mr/news_dtl.do?id=13420. Accessed November 2006.

⁷⁰ Ibid.

6.3 Cellular Telecommunications and Internet Association (CTIA)

In a brief interview with a CTIA official, the author received the impression that the Washington DC based organization is relatively unconcerned with the mobile malware threat.⁷¹ CTIA's focus lies in protecting the interests of mobile carriers. The author's understanding is that, while CTIA is researching the issue, they will only become active once the level of fraud affecting mobile carriers increases above 3%.

The CTIA official believed the mobile malware issue to be exaggerated by the antivirus industry and largely a burden that should be born by the consumer. The official did state, however, that carriers should be employing SMS and MMS filtering, as well as staying informed of current developments – being ready to react if there is a sudden increase in mobile malware activity or consumers are impacted such that they demand the carriers to act.

6.4 Trusted Computing Group Specification

The Trusted Computing Group's Mobile Phone Work Group (see: <https://www.trustedcomputinggroup.org/groups/mobile>) is currently developing specifications for mobile devices. The Mobile Trusted Module (MTM) specification is expected to be completed by the end of 2006 and will "create an industry wide approach to developing mobile devices that includes stronger security, ensures data privacy, and reduces the risk of malware-ridden mobile devices infecting company networks."⁷²

The group has enumerated 11 use cases intended to define the base for a trusted mobile computing model; as stated by technology journalist Neal Leavitt, use cases will enable:⁷³

- mechanisms to ensure that no one has tampered with a device's hardware and software;
- device authentication to protect and store owner-identity-related information and thus to determine whether a thief or other unauthorized person is trying to operate a phone;
- IP protection to restrict use of third-party content;
- the safe download of updates, patches and other software;
- secure channels between different parts of the phone—such as a subscriber identity module and the processes that use the SIM's data—to prevent keystroke logging or other types of tampering by malware;

⁷¹ Anonymous CTIA official. (November 10, 2006). Telephone interview.

⁷² Greenemeier, Larry. (October 16, 2006). Information Week. *New Standard Promises Better Security for All Mobile Devices*. <http://www.informationweek.com/security/showArticle.jhtml?articleID=193302684>. Accessed October 2006.

⁷³ Leavitt, Neal. (December 2005). Will Proposed Standards Make Mobile Phones More Secure? *Computer* (38)12. 20-22. <http://www.leavcom.com/pdf/Standards.pdf>. Accessed November 2006.

- the secure download and subsequent management of digital tickets, which represent proof that a user has the right to access and use network-based services or resources;
- the secure execution of payments made via a mobile phone;
- the ability to determine that software downloaded for use on a phone is safe and to remove or at least not execute unsafe software; and
- ways to prevent unauthorized parties from accessing or viewing information stored on a device.

The creation and implementation of such standards will aid in the establishment of a more secure environment for mobile users and carriers. Enhanced security should foster greater faith in new technologies, allowing mobile device manufacturers to continue to add new features, encouraging m-Commerce, and enabling smartphones to truly become a lifestyle device.

7 Countermeasures

Wireless carriers must recognize mobile malware threat and begin taking proactive measures now. Recommendations include:

1. Support, and participate in, the Trusted Computing Group's Mobile Phone Work Group.
2. Ensure that antivirus software is installed and up-to-date on any desktop PC which is used to synchronize with mobile devices.
3. Build antivirus measures into the carrier networks in addition to handsets
4. Implement SMS and MMS message scanning/quarantining
5. Install firewall software on mobile devices
6. Turn off Bluetooth and 802.11 radios by default
7. Ensure that, by default, Bluetooth and 802.11 features operate in 'non-discoverable' mode
8. Encrypt sensitive data on mobile devices
9. Educate customers on how to detect suspicious messages, websites, and downloads
10. For businesses, create and enforce policies regarding the management of mobile devices within the corporate environment
11. Consider implementing security services for smartphone customers as a cost of business

8 Conclusion

Most analysts predict that the growing power, functionality, and popularity of smartphones may make mobile platforms an irresistible target for malware authors by the end of 2007. While mobile malware proliferation has not yet reached epidemic proportions, this does not mean that the industry should stand idle. The wireless industry can begin defending against mobile threats now by creating resilient infrastructures which are content aware, educating users, and implementing technical safeguards on mobile devices.

Bibliography and Resources

- Beer, Stan. (June 13, 2006). Mobile phone botnets are poised to come calling. *The Sydney Morning Herald*. <http://www.smh.com.au/news/security/mobile-phone-botnets-are-poised-to-strike/2006/06/12/1149964442180.html>. Accessed October 2006.
- Berlind, David. (September 6, 2006). Typhoid cell-phones: The latest threat in malware transmission. *ZDNet blog: Between the Lines*. <http://blogs.zdnet.com/BTL/?p=3565>. Accessed November 2006.
- CDC.gov. (July 2006). Eastern Equine Encephalitis Fact Sheet. *Centers for Disease Control*. <http://www.cdc.gov/ncidod/dvbid/arbor/eeefact.htm>. Accessed November 2006.
- Carpenter, Perry. (October 2006). "Mobile Malware." Unpublished master's essay, Norwich University, Northfield, VT, United States.
- Flamig, Blaine A. (December 2006). Mobile Bugs: A mere nuisance or a deadly swarm ready to attack?. *PC Today*. 4(12), 44-45. <http://www.pctoday.com/editorial/article.asp?article=articles/2006/t0412/10t12/10t12.asp>. Accessed November, 2006.
- Froemelt, Marc. (September 22, 2006). PDA & Smart Phone – Business Security Impact. *TechLinks: The Guide to Technology in Georgia*. <http://www.techlinks.net/CommunityPublishing/tabid/92/articleType/ArticleView/articleId/3623/PDA--Smart-Phone---Business-Security-Impact-.aspx>. Accessed November 2006.
- F-Secure. F-Secure Mobile Anti-Virus. <http://www.f-secure.com/estoreusa/avmobile.html>. Accessed November 2006.
- F-Secure. F-Secure Mobile Security. <http://www.f-secure.com/estoreusa/avmobilesecurity.html>. Accessed November 2006.
- Gibson, Steve. (November 9, 2006). Security Now 65: Why is Security so Difficult?. *Security Now! With Steve Gibson*. <http://www.twit.tv/sn65>.
- Gartner.com. (October 9, 2006). Gartner Says Worldwide Combined PDA and Smartphone Shipments Market Grew 57 Percent in the First Half of 2006. *Gartner Media Relations*. <http://www.gartner.com/it/page.jsp?id=496997>. Accessed November 2006.
- Gostev, Alexander. (September 29, 2006). Mobile Malware Evolution: An Overview, Part 1. *Viruslist.com*. <http://www.viruslist.com/en/analysis?pubid=200119916>. Accessed October, 2006.
- Gostev, Alexander. (October 10, 2006). Mobile Malware Evolution: An Overview, Part 2. *Viruslist.com*. <http://www.viruslist.com/en/analysis?pubid=201225789>. Accessed October, 2006.
- Greenemeier, Larry. (October 16, 2006). Information Week. *New Standard Promises Better Security for All Mobile Devices*. <http://www.informationweek.com/security/showArticle.jhtml?articleID=193302684>. Accessed October 2006.
- Hines, Matt. (April 18, 2006). Analysts Speak Out on the Wireless Security Hype. *eWeek.com*. <http://www.eweek.com/article2/0,1895,1950790,00.asp>. Accessed November 2006.

Leavitt, Neal. (December 2005). Will Proposed Standards Make Mobile Phones More Secure? *Computer* (38)12. 20-22. <http://www.leavcom.com/pdf/Standards.pdf>. Accessed November 2006.

Leyden, John. (August 12, 2005). Cabir mobile worm gives track fans the run around. *The Register*. http://www.theregister.co.uk/2005/08/12/cabir_stadium_outbreak/. Accessed November 2006.

Leyden, John. (September 22, 2005). PC-hopping mobile malware sighted. *The Register*. <http://www.securityfocus.com/news/11328>. Accessed November 2006.

Leyden, John. (March 2006). Trojan row over spouse monitoring software. *Channel Register*. <http://www.channelregister.co.uk/2006/03/30/flexispy/>. Accessed November 2006.

Mobile Payment Forum website. <http://www.mobilepaymentforum.org>.

National Conference of State Legislatures. <http://www.ncsl.org/programs/lis/cip/priv/breach.htm>. Accessed November 2006.

Greenemeier, Larry. (October 16, 2006). Information Week. *New Standard Promises Better Security for All Mobile Devices*. <http://www.informationweek.com/security/showArticle.jhtml?articleID=193302684>. Accessed October 2006.

Hypponen, Mikko. (November, 2006). Malware Goes Mobile. *Scientific American*, 295, 70-77

Keizer, Gregg. (June 21, 2005). Don't Worry Yet; Mobile Worms Won't Show Until '07. *TechWeb Technology News*. <http://www.techweb.com/wire/security/164901569>. Accessed October 2006.

Peikari, Cyrus. (March 8, 2006). Analyzing the Crossover Virus: The First PC to Windows Handheld Cross-infecter. *SAMS Publishing*. <http://www.sampublishing.com/articles/article.asp?p=458169&seqNum=3&rl=1>. Accessed November 2006.

Rayhawk, David. (August 25, 2006). SMiShing - an emerging threat vector. *McAfee Avert Labs Blog*. <http://www.avertlabs.com/research/blog/?p=74>. Accessed November 2006.

Shevchenko, Alisa. (September 21, 2006). An overview of mobile device security. *Viruslist.com*. <http://www.viruslist.com/en/analysis?pubid=170773606>. Accessed October, 2006.

Shor, Susan B. (June 22, 2005). *TechNewsWorld*. Mobile Malware Will Come, But When?. <http://www.technewsworld.com/story/44079.html>. Accessed October 2006.

Sprint/Nextel. (September 19, 2006). Sprint Mobile Security Offers unmatched Seamless End-User Security for Mobile Workforce. *Sprint Nextel*. http://www2.sprint.com/mr/news_dtl.do?id=13420. Accessed November 2006.

Symbian OS "Fast Facts." <http://www.symbian.com/about/fastfacts/fastfacts.html>

Trusted Computing Group Mobile Phone Work Group. <https://www.trustedcomputinggroup.org/groups/mobile>

Vamosi, Robert. (February 17, 2006). Your smart phone has a dumb virus. *ZDNet Security Watch: Don't get burned by viruses and hackers*. http://review.zdnet.com/4520-3513_16-6442087-1.html. Accessed October, 2006.

Verizon Wireless. (June 12, 2006). Verizon Wireless Launches “Chaperone” Service – A Great Tool To Keep Your Family In Touch . *Verizon Wireless News Center*.
<http://news.vzw.com/news/2006/06/pr2006-06-12.html>. Accessed November 2006.