Northstream™

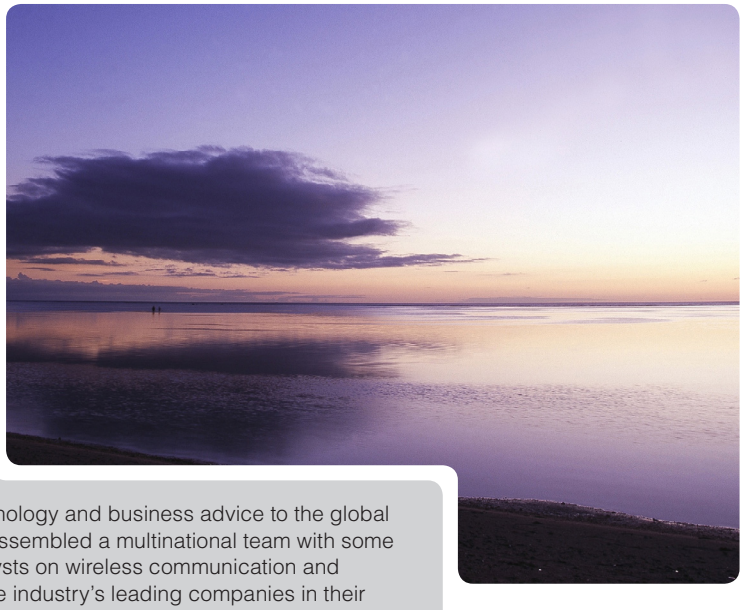
Mobile viruses – hype or real threat?

A Northstream analysis of the potential threats from mobile viruses and how the industry can strike back

Imagine your work colleagues showing you some very intimate private photos they just received – from your mobile email account. You check your outbox, but no messages were sent – and your phone book entries have been deleted. Going back to the standby screen, the family picture you had there is gone, replaced by the image of a skull. The phone bill received by your mobile operator is much higher than usual, including calls and messages you can't remember having ever made.

Today this appears a lurid tale, but can it become reality? Is the mobile industry going down the same road as the PC business, creating the need for an entirely new market for security and virus protection? Or are the recent news just hype, made by computer nerds and malware writers looking for new playgrounds?

This white paper examines the issue of mobile viruses, looking at the recently circulated news stories, assessing how dangerous mobile viruses could become and what the industry can do to counter this potential threat.



Contents

RECENT NEWS ON MOBILE VIRUSES 2

WHO COULD BE AFFECTED BY MOBILE VIRUSES 2

MEASURES AGAINST MOBILE VIRUSES 4

- Handset-centric approach 4
- Network-based virus scanning 5
- Holistic content certification approach 5
- The right way to go 5

Recent news on mobile viruses

Press articles from the last few months suggest that there are reasons to worry, at least for users of smartphones. Smartphones are mobile phones with "open operating systems" that allow adding native applications, similar to the case with a Windows programme on your PC. According to the articles, applications classified as mobile viruses or mobile worms appeared on users' devices, emptying the battery by trying to propagate themselves through Bluetooth, changing the user interface and blocking access to phone applications, or sending itself to all numbers in the address book through MMS.

While the damage done by such applications was allegedly significant in some cases, their prevalence has been very low. This is because mobile viruses so far lack the easy ways of distribution that PC viruses utilise, such as the Internet, email attachments, or instant messaging clients. Instead, they have relied on users having activated Bluetooth on their device, accepting the reception of an unknown file, and then installing it. Other viruses were spread by users installing them on a smartphone through a PC connection or, more dangerously, propagating themselves in the background through MMS.

The recent news of viruses appearing on mobile phones provided anti-virus companies good opportunities to promote their offerings: Mobile anti-virus software targeted at network operators, corporate users and consumers is available, promising protection against viruses and other harmful mobile content. At the same time, application certification programmes and testing services are promoted in the industry, emphasizing the need for quality tested mobile applications receiving digital certificates.

Who could be affected by mobile viruses

Initially, mobile viruses could appear to be most threatening for companies involved in the mobile content business, such as the makers of Java games. However looking at the possible danger coming from mobile viruses, it becomes clear that all stakeholders in the mobile industry should address the issue. The following table lists some of the threats that malicious or poorly written mobile applications could pose, and their potential consequences to mobile users:

Threat scenario: Application...	Consequence: Users might...
Accesses, modifies or propagates personal or corporate information: Contacts, calendar information, tasks, other data or media files	• Lose information required for personal or business decisions • Act based on incorrect information • Lose the ability to use their phone as a business or private tool • Lose social or business prestige when personal content is sent to others
Generates unwanted chargeable events: Phone calls, messages, data traffic	• Refuse to pay their mobile phone bill or parts of it • Be unable to use their phone when prepaid credit is used up, or the service provider blocks their account
Reduces phone usability by emptying the battery, or making certain applications unusable	• Be restricted in the ability to use their phone
Performs "denial of service" attacks to mobile network elements, Internet servers or other mobile phones	• Experience reduced terminal performance • Lose the right to use their phone once incidents are discovered

Table 1: Mobile virus threats and potential consequences

Similar to the PC world, writers of mobile viruses use the principles of "social engineering" for users to feel safe while something bad is happening: For example, an application appearing as a game from a well-known content provider might turn out to send SMS to premium numbers while users are playing the game. Another application might masquerade as a financial service client branded with a bank's logo, but transmit confidential financial information to a malicious server when connected to the Internet. While social engineering in the wireless world has already happened with SMS (e.g. hoax voice mail or prize winning notifications to make users call premium-rate numbers), currently available smart-phone operating systems open up alarmingly wider possibilities for abuse.

Going beyond the direct impact on users, the consequences of mobile virus incidents could be extensive:

- Users may consider changing service provider or handset brand.
- Users might no longer access value-added services such as application download or MMS, and/or downgrade to a simpler handset model which they regard as secure and unaffected by viruses.
- Some users or corporations might seek compensation from their service provider for the financial damage caused by mobile viruses
- Consequently, service providers and handset vendors could suffer from loss of revenues, increased customer care cost, reduced customer loyalty and lowered brand image.

As per-user revenues in the mobile industry are already under pressure, it appears that none of the parties involved can afford taking those risks and that preventive countermeasures are needed.

Who could be affected by mobile viruses, and what are the risks?

- Mobile viruses could affect all players in the wireless industry.
- Possible risks for mobile users include compromise and abuse of user data, generation of unauthorised chargeable events, reduced phone usability or denial-of-service attacks.
- The first incidents have shown that mobile phones can be vulnerable to viruses. Now is the time to carefully consider countermeasures.

Measures against mobile viruses

While there is currently disagreement in the industry on how real or how dangerous the mobile virus threat is, it is worth looking at the possible reactions to the issue:

- "Wait and see" in the hope that mobile viruses are merely a hype or fad.
- Move away from open-OS smartphones back to supposedly-secure, closed devices without open execution environment.
- Strengthen handset security architectures in order to prevent virus infection.
- Deploy handset-based anti-virus clients.
- Deploy network-based anti-virus systems.
- Promote security testing and certification of mobile content, and ensure that customers buy certified content if possible.

While the wait-and-see option may appear tempting and avoids cost in the short term, it might prove the wrong choice once there are mobile virus incidents in the user base, leading to fire fighting and potentially to severe revenue or public image losses. Instead, it is better to look at the other available options and to decide on a prevention strategy related to handsets, networks or content, as discussed in the following.

Handset-centric approach

It can be questioned whether the **"Move away from open OS phones"** approach solves the problem at hand. Most service providers already have a significant number of smartphones in their user base, which will remain vulnerable until replaced by more secure devices. In addition, other handset platforms such as MIDP Java might get under attack in the future: With a growing number and complexity of Java APIs[1], the risk of implementation errors creating loopholes increases, which might motivate malware creators to target such platforms as well.

A move away from open OS devices would therefore not solve the issue. In addition, certain customer groups such as advanced private users or corporate users demand such devices, in order to benefit from the possibilities of third-party software development and installation, application multitasking or accessory usage.

The next option, **"Strengthening the security architecture of open OS phones"**, seems very reasonable, and is being worked on by handset vendors. With more and more users discovering the possibilities of open-OS phones, it is important that applications gain access only to such phone functions they have permission to. This can be managed by protection domain architectures, allocating rights to applications depending on their digital signature.

The third option falling into this category is to **"Deploy anti-virus software to mobile devices"**. This would mean to apply the same principle as in the PC world: Today, you would hardly dare to connect your PC to the Internet without regularly updated anti-virus and firewall software running in the background. This goes hand in hand with fees to anti-virus service providers and the constant need to keep the operating system up to date against newly discovered security threats.

PC anti-virus measures have become commonplace and users accept that their systems are vulnerable to worms and viruses. In the mobile world though, it is fair to believe that people have a much higher degree of trust in their devices, and that the awareness of security risks is very low.

Bringing anti-virus software to mobile phones would surely not be unnoticed by users, and might have a negative impact on the level of trust consumers have in their devices, due to the apparent analogy to PC viruses. There are other disadvantages of this approach including license cost, software deployment to the phone, traffic cost for virus database updates, and system load to the handset reducing memory and processing power available for the actual phone usage.

On the positive side, it is important to note that a device-based solution can provide full protection, covering all possible channels that malicious content could be received through – such as over the air download, Bluetooth, or a PC connection.

It is also worth mentioning that for smartphone users, the risk of losing trust in their device might be no issue. This is because many smartphone users realise that their device has capabilities similar to a personal computer, and understand that this can create vulnerabilities. The deployment of an anti-virus application might therefore not damage, but rather increase the level of trust such users have in their device.

[1] API: Application Programming Interface; components of the Java environment providing access to network services and phone features.

Network-based virus scanning

This option would mean to **"Install network-based anti-virus systems"**, with the objective of preventing poorly written or malicious content from reaching users' devices. The main advantage of a network-based anti-virus solution is that there is no need for software updates on the terminal. Any content delivered from the protected server can be scanned at ingestion, before content delivery, or at both stages.

The downside is that the protection does not go beyond the network where the anti-virus solution is installed. An operator implementing such a solution would either have to establish a walled garden for content distribution (so that mobile users cannot download content from anywhere but the service provider's own portal), or accept the risk of content coming from other sources potentially damaging its own business - neither option being very attractive. An additional drawback to mention is the reduced service performance that a virus scanning proxy would probably cause.

While a network-based server can reduce the virus threat, vulnerabilities remain. Service providers do not control local connectivity such as Bluetooth, which is a widely used distribution method for mobile content and hence potentially for mobile viruses. In addition, mobile phones supporting Wireless LAN support another channel for content download that would not be covered by a network-based anti-virus solution.

Holistic content certification approach

This option means to **"promote security testing and certification of mobile content"**. We call this holistic because it embraces various processes and service enablers across the value chain, and requires coordinated efforts of various industry stakeholders (service providers, handset manufacturers, content providers and others) to work.

In this context, content certification means that mobile applications distributed by a service provider are certified to meet a certain level of quality and integrity. To become certified, an application must undergo a set of tests to verify that it is free from errors and will work as expected on the targeted handset models. Once all tests are passed, the application receives a digital signature, which also certifies that it originates from the source it claims to be from.

Application certification can protect from security risks, as tested content potentially has much lower risks of being affected by viruses and other bad elements. However, customers will still be able to download untrusted applications from other sources, which are not certified and can potentially contain harmful or malicious elements. As for the previously discussed option, this risk could only be eliminated by an unpopular walled-garden approach where customers are restricted to download content from specific sites only. Therefore some risk remains, but this can be mitigated by the handset giving users a security alert before the download of untrusted content.

It should also be noted that besides the quality assurance, content certification can enable improved user experience and enriched application features. This is because a digital signature can give an application extended rights to access privileged phone functionalities, or authorise the application to access them in the first place.

The right way to go

Comparing the investigated alternatives, Northstream regards the option of application certification as an obvious choice. In addition, service providers with a significant share of smartphone users are advised to evaluate the offerings of anti-virus companies as well.

The right way to go:

- Deploying carrier-grade anti-virus solutions now would mean to overrate the current threat coming from mobile viruses. However, service providers need to consider how to protect smartphone users from malicious content, and should evaluate the offerings of anti-virus companies. In parallel, smartphone vendors are improving their device architectures to make future models more secure.
- Prevention is better than cure: Tested and certified mobile content, distributed to handsets with a correctly implemented security architecture will support an enhanced user experience with better features and provide a good level of protection against security risks.
- There are a number of industry initiatives and companies offering content certification, aiming at standardised testing and quality criteria. Industry-wide certification is the key to low-cost, efficient quality assurance for mobile content.

We see the following reasoning for this recommendation:

- The mobile virus threat is not yet so imminent that it would require carrier-grade deployments of anti-virus solutions. Nevertheless, service providers should be prepared to offer device-based anti-virus protection to smartphone users, focusing on corporate customers with a large base of such devices in the service provider's network.
- Generally, prevention is better than cure: Quality assurance during content development is less expensive and more efficient than fire fighting when viruses are already spreading through the customer base.
- Application certification enables customers to distinguish trusted from untrusted applications, and to benefit from the user experience and features certified content offers. Note though that this requires correct and unified security architecture implementations on the handset to work – also in this area industry players need to work together to enable a coherent and secure end-to-end user experience.

Industry-wide certification initiatives are already available to facilitate the distribution of certified content. The most prominent ones are "Java Verified" for MIDP 2.0 Java content, "Symbian Signed" for Symbian OS applications, and "Designed for Windows Mobile" from Microsoft.

As the threat scenarios coming from mobile viruses develop, so will the certification criteria in the industry have to evolve. Today, most testing focuses on functionality and platform compatibility, while little effort is placed on security. In the future, an increasing amount of testing time will be spent on security testing. A successful testing programme will ensure that the danger coming from mobile viruses is kept under control, while the certification criteria allow efficient testing and thereby low cost and industry-wide acceptance.

Northstream recommends this combined approach of device protection and content certification for service providers to enhance the attractiveness of their content offering, while keeping the mobile virus threat under control.

Contact us for more information on what you can do to grow your mobile content business, and manage the threat your customers are exposed to.

Contact

Northstream has studied all aspects of mobile services. Please contact us if you would like to find out more about this or about our company and the services we provide.

E-mail us at info@northstream.se or call us at +46 8 564 84 800 (SE)