

Friday 07 May 2010

Welcome Luica Mak: Registered
edit my profile

log out

free 30 day trial

contact us

search

go



technology business geography plus jobs resources Total TeleVision



Keeping mobile users safe from malware is good business

By Francisco Martin Abreu, Optenet
Tuesday 04 May 2010

'Smarter operators are looking very seriously at how they can improve security for their customers...'

The huge growth in the use of the iPhone, other smartphones and mobile devices means that significantly more people are accessing sophisticated Web services such as social networking on their handsets as a matter of course. The model of a mobile phone as a simple text and voice device is fast disappearing. This shift in connectivity brings undoubted advantages to the consumer but it also exposes them to new dangers.

Of course, data security experts have been predicting a rise in mobile malware for several years but the failure of this to happen on a wide scale has led to accusations of crying wolf causing unnecessary alarm.

In a 2005 report Gartner predicted that a major phone virus would spread once two important criteria were met: smartphones capable of being infected making up around a third of the market, and the ability of those phones to exchange executable files. It predicted this would happen by early 2008. The analyst firm may have been a little early with the dates but it is fair to say that those two criteria have now been met, especially as users download and install "apps" to their phones in their millions.

Perhaps more importantly, Gartner warned that the mobile industry should not repeat the mistakes of the PC market. It said that protection for mobile users should be built into the network first with "device side protection as a last resort".

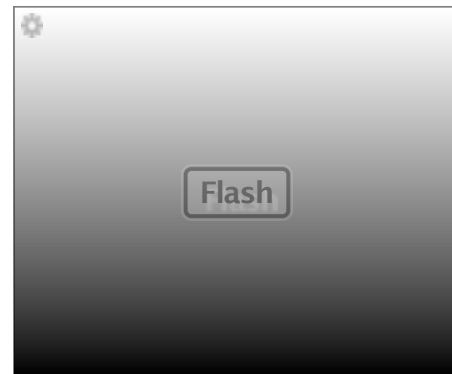
"A more futuristic approach is where the intelligence lies in the network. Prevention at the network level will always be better and smarter than using solutions at the device level" the report went on to say. In other words, Gartner was suggesting a Security as a Service (SaaS) for mobile customers, where the security software on their handset is configured, managed and updated remotely by the carrier.

Five years on, the warnings of Gartner seem remarkably prescient. In 2009 the first malicious worm written for the iPhone was discovered. There are fears among experts that the pace of development of mobile malware is now even faster than that for PCs as cyber criminals look to exploit the growing numbers of vulnerable smartphones.

Although Apple has a stringent approval process for apps, it is one that is largely concerned with quality standards and copyright, and experts believe it cannot possibly inspect the source code of every app submitted for approval.

In the Android world the situation is potentially worse as Google does not vet any of the open-source apps submitted to the Android Market for download by consumers. These and other app repositories potentially hold nasty surprises for mobile users and when Windows 7 for mobile becomes available malware writers will undoubtedly target those attracted to install apps for that operating system.

Meanwhile, Berg Insight, a telecoms analyst, reported that the number of active users of mobile banking and related financial services worldwide is forecasted to increase from 20 million in 2008



- print
- email
- reprint
- comment

search

Bookmark & Share

- digg It
- del.icio.us
- searchle
- stumbleupon

Most Read

Mobile operator app initiative takes a (very small) step forward

Alcatel-Lucent wins five-year BT 21CN deal

Huawei seeks India meeting over equipment ban

Motorola's Brown says separation is right move

US suit alleging text message price-fixing to proceed

France Telecom, Investec launch Orange Tunisia

Alcatel-Lucent shares tumble as net loss widens

H-P faces big challenges in Palm deal - Deutsche Bank

Apple to shut down Lala.com music service in May

Fastweb, Vodafone, Wind in €2.5bn broadband plan

Related Content

Friday Review: Facing East

Top 500 Ranking: Face Value

Friday Review: An iPhone-shaped hole

Quick pace needed to compete in smartphone race

RIM Co-CEO: Never been more opportunity or competition

Google drops Verizon Wireless as Nexus One partner

H-P to acquire Palm for \$1.2 billion

H-P faces big challenges in Palm deal - Deutsche Bank

recent to now



to 913 million in 2014. This growth will not go unnoticed by cyber criminals. The anticipated arrival of 3G-enabled tablet devices and smartbooks will only increase the potential for network-borne malware to wreak havoc.

Despite these challenges mobile operators should also see some opportunities; the smarter ones will be looking very seriously at how they can improve security for their customers who now expect unlimited texts and very generous monthly data allowances as a matter of course along with their smartphones. Mobile protection is likely to become a key marketing tool in the fight for subscribers always on the lookout for a better deal. The mobile operator that cannot offer sophisticated and built-in security for its customers will find it hard to survive.

Most importantly, customers should not feel that they must take full responsibility for data security. Consumers are not expected to filter their own water supply, so why should they have to screen the data that flows between handsets? A smart solution for mobile operators will be to offer their customers a Security-as-a-Service solution for protecting their email and Web traffic. Since the devices people will be using to access the Internet will be very heterogeneous with different operating systems and capabilities, a solution in the cloud adds flexibility and makes more sense than a solution based on End-Point software.

Time is quite short. The previous decade provided a few warnings and some false alarms but those operators that feel they can continue with a laissez-faire approach are mistaken. The decade ended with very real pieces of malware targeted directly at smartphones and other Internet-enabled mobile devices. Operators need to be seen to be protecting those customers who increasingly want the most sophisticated phones and want to make the most of their capabilities. A wave of mobile malware is likely to hit in the early part of the next decade and become entrenched just as it has in the desktop world during the 2000s.

It is no longer an option not to do this for operators. Those that do not take the initiative risk not only losing out to competitors but also suffering brand damage. Operators that can provide safe Internet experience are on the right track to be the winners.

Francisco Martin Abreu is president and CEO of Optenet.

Comment here

submit comment



- Newsletter Registration
- Edit My Profile
- Site Map

- TT Subscriptions
- Telecom Jobs
- World Communication Awards

- Resources
- The Editor's Cut
- World Telecoms Council

- Media Information 2010
- About Us
- World Vendor Awards

- Contact Us
- Privacy
- Home