Mobile malware explodes, hits corporate networks

26 June 2013, by Rob Lever

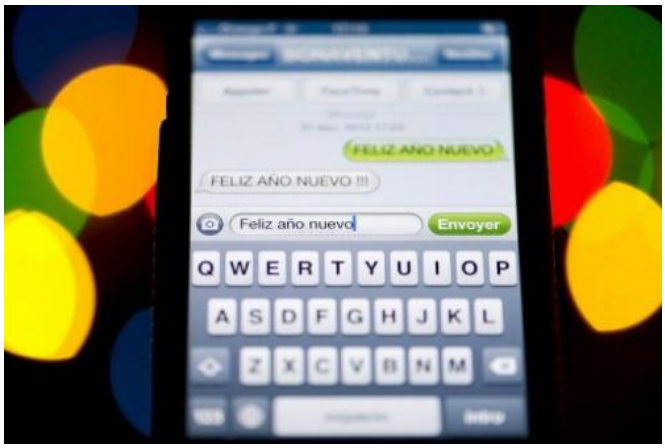

Illustration photo shows SMS text messages displayed on a a smartphone. Smartphone users have seen an explosion of malware in the past year, dominated by schemes targeting Google's Android operating system, a survey showed Wednesday.

Smartphone users have seen an explosion of malware in the past year, dominated by schemes targeting Google's Android operating system, a survey showed Wednesday.

The attacks are also starting to hit corporate networks, possibly as part of broader espionage efforts, according to the Juniper Networks Mobile survey.

The report showed a 614 percent jump in mobile malware in the 12 months to March 2013, with Android attacks accounting for 92 percent.

The prevalence of Android malware is not surprising in light of its dominance of the global smartphone market—around 75 percent—Juniper said the open platform with less regulation makes it more prone to attacks.

"Android does not have as rigorous a vetting system" as rival platforms such as Apple's iOS and BlackBerry, said Karim Toubba, a Juniper vice president.

"But the reality is that all the operating systems have vulnerabilities."

Toubba said the dominant scheme to "monetize" the attacks involves SMS text messages which infect a smartphone and surreptitiously deliver new messages to a "premium" SMS service, for a fee.

These services, which mimic legitimate ones such as those for voting on TV programs, can charge small fees such as 10 cents or 50 cents. The hackers can quickly cash in by infecting large numbers of devices, and can easily shut down and set up new numbers to avoid detection.

Hugo Barra, Google VP of product management for Android, pictured at the Google I/O conference on May 15, 2013. Some malicious software gets into official channels such as Google Play, but third-party vendors have much more malware, a survey showed Wednesday.

"They can spin it down and leave no trace," said Toubba.

The typical SMS Trojan takes in a quick $10 for the enterprise to grow exponentially in the coming attacker, with profits multiplying as the schemes are years," the report said.
repeated.

Many users are tricked into installing malware by messages or emails disguised as software updates.

Toubba said some malicious software gets into official channels such as Google Play and the Apple App Store, but that third-party vendors have much more malware.

"These marketplaces are popular targets which provide little to no review process," Toubba said.

Not surprisingly, the survey found many of these malicious apps stemming from sites in Russia and China.

Apple users who "jailbreak" their iPhones to use on unauthorized carrier networks often use these third-party networks because they may get locked out of the App Store.

Many users fail to even notice when their device is infected, because it may result in a charge of just a few cents on their phone bill.

Juniper found that more sophisticated attacks are starting to emerge, including those that create "botnets" to expand the infections, and other schemes which can be part of a broader corporate or government espionage effort.

"They can use the mobile device to do reconnaissance and go deeper into the corporate network," Toubba said.

This is particularly worrisome for companies which allow employees to use their own devices for corporate networks.

Juniper's report said it "saw several attacks that could potentially be used to steal sensitive corporate information or stage larger network intrusions."

"It is clear that the threat of mobile malware to corporate devices is no longer a theoretical one. We expect the presence of mobile malware in the