gulfnews.com

Android phone threats: what you need to know

Google's smartphone platform is main target, with 99% of known 'malware'

By Naushad K CherrayilStaff Reporter
Published: 21:32 July 3, 2014

GULF NEWS

Dubai: Ten years ago, Kaspersky Lab discovered the first mobile malware — Cabir — designed to attack mobile phones.

It was infecting Symbian-powered Nokia devices by spreading through unsecured Bluetooth connections.

With its discovery, the world came to know that there was malware not just for computers but also for smartphones.

Unlike most modern malware samples, Cabir wasn't equipped with a wide range of malicious functions. Instead it made history by proving that it was possible to infect smartphones.

Due to the Cabir virus constantly searching for Bluetooth connections, it exhausted the battery life

within two to three hours apart from sending messages to premium-rate numbers.

Beginning to take shape

Related Links
Cybercriminals bank on popularity of Android
Android phone apps could contain malware

The group which created the virus — 29A — was not cybercriminals, at that time cybercrime was just beginning to take shape. They were virus writers creating malware to test and demonstrate new virus technologies and the first to create a virus for the Windows 64 platform.

Mohammad Amin Hasbini, senior security researcher, global research and analysis Team at Kaspersky Lab Middle East, Turkey and Africa, told Gulf News that the criminal group 29A is responsible for many malwares attacks like Cabir, Duts, Haiku, Stream, Lindose, and Donut, targeting mobile and Windows devices.

He said the group announced cease of operation in 2008, but they might be working under different names and operations.

Ten years after the discovery of Cabir, Kaspersky Lab's collection of mobile malware contains more than 340,000 unique samples. In January, the security solution provider had 200,000 unique samples in January 2014.

New modifications

In 2013, Kaspersky Lab detected 143,211 new modifications of malicious programs for mobile devices. Most malicious mobile apps principally aimed to steal money, and subsequently personal data.

"In 2013, 3.90 million installation packages were used by cybercriminals to distribute mobile malware. Overall in 2012-2013, we detected approximately 10 million

unique malicious installation packages compared to 2.7 million in December 2012. In late 2011, roughly 65 per cent of mobile threats targeted the Android platform; by late 2012, that percentage was just short of 94 per cent. In 2013, the figure shot up to 98.05 per cent," he said.

"In the first quarter of this year, the percentage of threats targeting Android exceeded 99 per cent of all mobile malware and we believe it will remain popular among cybercriminals in 2014 as well," he said.

He said that all devices are targeted but due to open architecture adopted on Android platform, mobile malware are targeting Android devices. IOS devices have more vulnerabilities compared to Android devices, but Android devices are targeted by more malware.

In the first quarter, 110,324 new malicious programs for mobile devices and 1,182 new mobile banking Trojans were detected.

At the start of the year, Kaspersky Lab had logged 1,321 unique executables for mobile banking Trojans, and by the end of the first quarter, that number jumped to 2,503. As a result, over the first three months this year, the number of banking Trojans nearly doubled.

As before, the threats are most active in Russia, Kazakhstan, Belarus, and Ukraine.

Kaspersky Lab products blocked a total of 1,131,000,866 malicious attacks on computers and mobile devices in the first quarter of 2014.

Kaspersky Lab solutions repelled 353,216,351 attacks launched from online resources located all over the world.

Kaspersky Lab's web antivirus detected 29,122,849 unique malicious objects: scripts, web pages, exploit, executable files, etc.

“We believe the mobile threat landscape is still in its early growth phase, criminals are still looking for what they can do and methods to abuse different types of mobile devices. We are seeing many malicious functions being transposed from computer devices to mobile devices. We recently found Ransomware targeting Android devices,” Hasbini said.

Demanding ransom

Ransomware is a kind of virus that demands a ransom or compensation from the victim by locking his device, holding his data or by making it difficult for the victim to find a solution to remove a virus installed on his device.

A new variant of ransomware targeting users on Android is — at the very least — associating itself with CryptoLocker, which is known for encrypting critical computer files and demanding ransom to decrypt them.

Cybercriminals gain their attention towards a technology when it has a larger footprint like Microsoft on PC, Android on phone and Adobe in applications or when the systems is highly critical which could bring a financial gain or a production loss. Any technology which falls to these criteria is always susceptible to attacks.

The most attacked and vulnerable PC operating system is Windows XP Professional. Kaspersky Security Network statistics had received more than 1,240 million attack notifications on Windows XP in 2013, which represent about 28 per cent of all attack notifications.

Running outdated and therefore unsupported versions of software represents a massive risk for users. Java 6 is a fine example of this. In February 2013, Oracle stopped providing updates and patches for the platform. Merely six months later, the industry witnessed a

tremendous spike in both the volume and sophistication of attacks that exploit the vulnerabilities of Java 6.

And because Oracle no longer provides patches for the platform, these exploits become cumulative and the platform becomes less secure with each passing day.

“Cybercriminals often reverse-engineer released patches to check which flaws that have been addressed and use that knowledge to target older, especially unsupported version of the software,” said Pradeesh VS, General Manager at ESET Middle East.

Concerns about BYODS

Android mobile malware is also rapidly becoming more widespread in the Middle East, and this is causing companies to have more concerns about adopting a Bring Your Own Device strategy.

Although removable media and local networks are still the primary method for spreading malware in the region, there is an increase in the use of drive-by downloads which exploit vulnerabilities in browsers and their plug-ins. M

Malware spread via social networks (especially Facebook and Twitter) has increased sharply in the Middle East, probably due to the massive rise in social network users in the region — now 88 per cent of the Middle East online population uses social networks daily.

Volatile regional situation

Another reason for spreading malware is to capitalise on interest in the volatile political situation in the region — by creating fake links to political news and videos, criminals can direct users to malicious websites to exploit vulnerable browsers and download malware.

“Removable media and local networks are still dominating the malware. By January 2014, we are detecting 315,000 malicious files every day, most of them are targeting computer devices through removable media, local networks or internet networks, mainly because they are used everywhere,” Hasbini said.