Inspiratron.org - Natural language processing, machine learning and cybersecurity

Notes on history of mobile malware

by Nikola Miloševi? - Sunday, March 31, 2013

https://inspiratron.org/blog/2013/03/31/notes-on-mobile-malware/

Mobile malware came not so long ago as PC malware. Mobile malware is almost 20 years younger, but today since almost everyone has mobile device it evolved to quite dangerous tools for attackers. Also mobile manifacturers were doing their job, creating sandbox environement in mobile operating systems, so users can be quite secure. Sandboxes helped a lot to elemenate some of the threats, but not all.

Brief history

It all started in 2004 with malware called Cabir. Cabir is a worm that was originally developed as a proof of concept by a coder named Vallez who worked as a part of the 29A group of virus writers. Cabir was written to infect Symbian-based devices and spread via Bluetooth as a .sis package. When a phone is infected with Cabir, the message "Caribe" is displayed on the phone's display, and is displayed every time the phone is turned on. The worm then attempts to spread to other phones in the area using wireless Bluetooth signals. The worm was not sent out into the wild, but sent directly to anti-virus firms, who believe Cabir in its current state is harmless. However, it does prove that mobile phones are also at risk from virus writers.

In this same year, criminals were already developing means to make money from this malicious mobile code, the Trojan Qdial, which was disguised as a cracked copy of the game Mosquitos was also targeted at users of the

Symbian s60 platform. Unknown to the victim the malware would send text messages to premium rates services, for which the handset owner would be charged, thus making an income for the criminal.

Also in that year, in November a second piece of mobile malware appeared, going by the name of Skulls. Skulls was reminiscent of the older forms of computer malware, in that while it was malicious it was not designed with the kind of criminal intent that was by now the goal of PC based malware. Skulls overwrites application files on the mobile device, causing them to stop functioning and replacing their normal icons with a skull and crossbones. Skulls was distributed through email and through peer to peer file sharing, masquerading as the attractively innocent sounding “Extended Theme Manager” which appeared to be targeted in particular at the Nokia 7160 although it would also affect other Symbian-based devices.

By 2005, mobile malware was already moving into the realms of information theft although not to the professional level of today’s modern threats. Pbstealer copied all the information from an infected devices address book.

Pbstealer was based on the earlier Cabir source code and contained the string “.:: Good artist copy, Great artist steal::.”. Another notable development in the same year was the first mobile malware to spread by using MMS messaging instead of the less effective Bluetooth that was more common at the time. Commwarrior did not carry a destructive payload, but still represented a major step in the mobile malware evolutionary scale.

However, another attractive area for criminals has been the development of malware for the J2ME (Java 2 Micro Edition). This development platform has been particularly abused because it enables criminals to overcome the problems posed by the multiple platforms in the mobile device space. Any device that incorporates a Java Virtual Machine now falls into the criminal sights and the range of infectable devices is considerably expanded. By 2009 a very large percentage of all mobile malware comprised SMS fraud Trojans designed for J2ME. SMS fraud takes several forms and includes the sending of premium rate texts, or the more socially engineered attacks where SMS are sent asking the recipient to call a number to confirm a non-existent transaction such as a purchase or a subscription service, of course the numbers too are

premium rated.

The first ever Trojan for Android was discovered in August of 2010 and Trend Micro detected it as ANDROIDOS_DROIDSMS.A. True to form it was a Russian SMS Fraud app, the sent messages to premium rate numbers.

In the same month as DROIDSMS.A, another Trojan was uncovered, masquerading as a game Tap Snake which would transmit the GPS location of an infected phone over HTTP, this location data could then be queried by another phone using the GPS Spy app.

Also in August of that year we saw the very first malware for iOS based devices, Apple's iPhone. The Ikee worm only affected jailbroken iPhones and took advantage of a default SSH password in order to replicate to other jailbroken devices. Infected devices were Rickrolled, the background was changed to an image of 80s pop warbler Rick Astley with a message that read "Ikee is never gonna give you up".

2011 has been the year that mobile malware has come of age, criminals are still exploring the multiple possibilities offered by the rich functionality and complexity of today's Smartphone.We see multi-platform attacks distributed by the same criminal groups that traditionally have focused on Wintel systems. The growth in complexity of threats, for example ZeuS malware now incorporating mobile elements aimed at intercepting SMS banking authentication codes is striking.

Source: Brief history of mobile malware by TrendMicro

End note

There is much other things to be said about mobile security like threat model, defense etc. In this article I just wanted to note some history moments. There are a lot done in anti malware fight, but it seems like it is still not enough, since mobile anti-malware apps make a lot of false positives or true negatives. There is much space for improvement. And most of today malwares on android and iOS platform are Troyans, that are by human error installed by users. So many blames for infected phones goes to human error and not knowing how to protect yourself. So one basic principle is read what app should do, think about resources it needs, and read permission. If in permission list app requires is something suspecious, don't install application. Still there are also worms, but some firewall can help you there. If your phone has some 0-day worm exploits, anti malware software can behaviour based stop some malicious actions.
