

A Brief History of Mobile Malware



A Brief History of Mobile Malware

The story of malware for smartphones begins as far back as 2004.

This was the year that [Cabir](#) made its first appearance. 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. It didn't take long for this original proof-of-concept to be picked up by others with more mischievous intent and new, more powerful variants were already in the wild by the end of that year.

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.

The numbers in this instance were based in the UK, Germany, the Netherlands and Switzerland. Over time this has developed into the major money-making scheme for criminals, even on newer platforms.

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. The [second variant](#) of Skulls also incorporated the Cabir worm to further aid in propagation; infections with this variant are distinguishable from the original because the icon was no longer changed to a skull and crossbones, but to a jigsaw piece. This marked the beginning of a trend and Cabir became the propagation vehicle of choice, incorporated into many of the examples of other malware at the time.



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 (information that could contain things like usernames and passwords) and then attempted to transmit it to any Bluetooth enabled device within range. 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.

Although all the malware referenced above targeted *Symbian*-based devices it is worth noting that malware for the Windows CE also surfaced but was much less prevalent. Although Windows CE was nominally less secure than *Symbian*, the latter was very much the dominant mobile operating system and, true to form criminal intent was focused on the biggest bang for the buck.

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.

Skip forward just one year to 2010 and the landscape has been radically altered, Gartner reported that Smartphone sales increased over 70% in comparison to 2009 and two new Operating Systems have come to dominate the arena; *iOS* for Apple's iPhone and Google's *Android*. Criminals have not been slow to realise the potential afforded by these new platforms, particularly Google *Android* which in August 2011 was [reported](#) to have cornered almost 50% of worldwide Smartphone market share.



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. The new capabilities of the modern Smartphone though, offer more nefarious opportunities to the enterprising criminal. 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". This initially mischievous worm was soon picked up and modified to incorporate rudimentary botnet functionality and used in an attack against customers of ING bank in the Netherlands to steal banking information. To date no iOS malware has been discovered in the official App Store, or that can affect non-jailbroken devices, but as jailbreakme.com web-based jailbreaking service shows it is possible to direct an iPhone browser to a website that exploits a vulnerability in order modify the iPhone. It is surely "when" rather than "if" this method is used to spread malware.

Initially the *Android* malware was spread using third-party App Marketplaces, the openness of the app distribution ecosystems certainly facilitated this kind of misuse. In contrast to Apple, there is no enforcement of a single App Store model and no vetting of code before *Android* apps are published, leaving the responsibility entirely with the user. Google do maintain the ability to "remote kill" malicious apps in the event of abuse. However, in March of 2011 [the largest collection to-date of Trojanised apps was discovered](#), and this time on the *Android* Market. The repackaged versions of more than 50 legitimate apps included the [rageagainstthecage or the exploit](#) exploit, which is capable of gaining root access to the device. This malware went by the name of [DroidDream](#). Not only did these Trojanised apps steal device details such as IMEI and IMSI but they also installed further hidden



malware which siphons even more user information off the device and into the hands of criminals. This second payload also contained a dropper capable of downloading further malicious code. Google were forced to use their kill switch, but the big question remains; if the initial infection had downloaded further malware, was the kill switch truly effective. To rub salt into the wound, once Google released their official *Android* Market Security Tool to clean up the modifications made by the malware, [criminals immediately seized the opportunity to repackage and Trojanise that selfsame tool](#) and release it into the wild. This malicious version was an information stealer and backdoor for cybercriminals. Since that time, more and more malicious *Android* apps have been surfacing with routines that [forward all SMS messages, spy on GPS location, send premium rate SMS, act as an SMS relay](#) and most recently of this writing [eavesdrop on telephone conversations](#) under the guise of a Google+ app.

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. Of course the sheer volume of mobile malware is a long way from the epidemic proportions of *Windows*-based malware, but criminal interest is clearly there and clearly growing. 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. Criminals are driven by consumer behaviour and as the money-making opportunities move to mobile platforms criminals will, in fact already are, following.



Securing Your Journey
to the Cloud

ABOUT TREND MICRO™

Trend Micro, Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our website at www.trendmicro.com.

TREND MICRO

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800.228.5651

Phone: 1 +408.257.1500

Fax: 1 +408.257.2003

www.trendmicro.com