



INTEGO SECURITY MEMO – November 23, 2009

iPhone Worm Creates Botnet, Copies Personal Data

Malware: iPhone/iBotnet.A

Discovered: November 21, 2009

Risk: Medium

Description: For the third time this month, malware targeting the iPhone has surfaced. The first such malware changed wallpaper on iPhones¹, and the second harvested personal data from iPhones². This new malware, that Intego calls iBotnet.A, is by far the most sophisticated iPhone malware yet: it is not only a worm, capable of spreading across a network, but also hijacks iPhones or iPod touches for use in a botnet.



It is important to note that standard, non-jailbroken iPhones or iPod touches are not at risk; it is extremely dangerous to jailbreak an iPhone because of the vulnerabilities that this process creates. (Estimates suggest that 6-8% of iPhones are jailbroken.) Jailbroken iPhones at risk are those where ssh is installed, and where the default password has not been changed.

This worm starts by searching its local network, as well as a number of IP address ranges, for available devices to infect. The address ranges it scans include those of ISPs in the Netherlands, Portugal, Hungary, Australia, and if an appropriately unprotected iPhone is found, the worm can copy itself to these devices.

When active on an iPhone, the iBotnet worm changes the root password for the device (from “alpine” to “ohshit”), in order to prevent users from later changing that password themselves. It then connects to a server in Lithuania, from which it downloads new files and data, and to which it sends data recovered from the infected iPhone. The worm sends both network information about the iPhone and SMSs to the remote server. It is capable of downloading data, including executables that it uses to run and carry out its

¹ <http://blog.intego.com/2009/11/09/worm-affects-jailbroken-iphones-changes-wallpaper>

² <http://blog.intego.com/2009/11/11/intego-security-memo-hacker-tool-copies-personal-info-from-iphones/>

actions, as well as new files, providing botnet capabilities to infected devices. (A botnet is a network of infected computers or devices that can be controlled by hackers to attack other computers, serve malware, send spam, serve pages or images, and much more.)

The worm also gives each infected iPhone a unique identifier; this to be able to reconnect easily to any iPhones on which valuable information is found, but also to ensure that only infected iPhones can connect to the server. Finally, it changes an entry in the iPhones /etc/hosts file for a Dutch bank web site, to lead Dutch users who connect to this bank site to a bogus site, presumable to harvest user names and passwords.

Means of protection: Intego VirusBarrier X5 detects and eradicates this malware, which it identifies it as iPhone/iBotnet.A, on iPhones that it can scan from Macs with VirusBarrier X5 installed, with its virus definitions dated November 22, 2009 or later. The only other way to remove this malware is to totally wipe and restore the iPhone using iTunes.

We would like to stress that users who jailbreak their iPhones are exposing themselves to known vulnerabilities that are being exploited by code that is circulating in the wild. If users install ssh, they should change the default password, which is widely known. While the number of iPhones attacked may be minimal, the amount of personal data that can be compromised, and the ability of this new worm to create a botnet, strongly suggests that iPhone users should stick with their stock configurations and not jailbreak their devices.

Intego thanks Scott McIntyre, Chief Security Officer of the Dutch ISP XS4ALL, for his help in isolating and analyzing this worm.

