

# Modified iPhones Are Compromised By New Worm

November 25 2009, by John Messina

---



(PhysOrg.com) -- Several research security firms have reported a new worm attack against jail broken iPhones, dubbed "Ikee.B or "Duh", this worm searches for personal and banking information.

The worm spreads by using the default password for applications that can be installed on jail broken [iPhone](#). Once the iPhone is infected, the worm grabs text messages and searches for banking authorization codes used for at least one bank. The codes are then sent to a central server located in Lithuania.



With cybercriminals becoming savvier, it's only a matter of time before they find ways to infect iPhones that are not jail broken as well as other smartphone devices. Some researchers confirm that worm attacks against [mobile devices](#) are evolving and it's becoming more common for cybercriminals to target personal and financial information stored on portable devices.

Researchers have confirmed that even Bluetooth connections between portable devices can be compromised with malicious code. A Bluetooth outbreak can be easily carried out in shopping malls, airports, or libraries, anywhere a cybercriminal may find potential victims.

The new worm easily infects jail broken iPhones by a weakness introduced into an application called OpenSSH. The application uses the default password 'alpine' that the worm uses to connect to the iPhone remotely. Since there is no shell code and no buffer overflow compromising the iPhone, writing code is fairly simple.

The attacks that have target iPhones this past month, focused on jail broken phones only. In the process of jail breaking a phone, the code that prevents users from loading any application they want is removed, thereby also removing most of the security that prevents [malicious code](#) from running on the smartphone.

With the evolution of hacking into portable devices growing, it's only a matter of time before phones employing Google's [Android](#), and everything else will be compromised in one way or another.

More information: [iPhone worm Rickrolls Australia](#)

© 2009 PhysOrg.com



Citation: Modified iPhones Are Compromised By New Worm (2009, November 25) retrieved 8 April 2024 from <https://phys.org/news/2009-11-iphones-compromised-worm.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.