Geschrieben von: Philipp
TUESDAY, 10 NOVEMBER 2009 08:29

In Australien verbreitet sich derzeit der erste iPhone-Wurm. Dieser ist ausschließlich auf jailbreaked iPhones zu finden. Als Sicherheitslücke wird dabei ein vom User installierter offener SSH-Server ausgenutzt.

Da die System-User *mobile* und *root* auf allen iPhones das gleiche Paßwort haben, brauch der Wurm nur die IP-Adressen entsprechender iPhones zu finden und kann sich mit Hilfe dieser System-User auf das Gerät kopieren. In Australien hat der Mobilfunk-Provider Optus für UMTS-Geräte einen festen IP-Adressbreich und erleichtert somit dem Wurm das Auffinden infizierbarer Geräte.

Der Wurm selber wird unter dem Namen "ikee" geführt und richtet verhältnissmäßig wenig Schaden an. Nachdem er sich auf ein iPhone kopiert hat, setzt er als Hintergrundbild ein Bild des Sängers Rick Astley mit dem Zusatz "ikee is never going to give you up (You have been Rickrolled)". Zusätzlich wird der SSH-Dienst gelöscht und die Suche nach weiteren offenen iPhone's beginnt erneut.

Um sich vor dem ikee-Wurm zu schützen, brauch der iPhone-Besitzer einfach nur das Passwort der System-User *mobile* und *root* ändern, muß dabei jedoch bedenken, das nach dem Einspielen einer neuen Firmware, diese sich wieder zurücksetzen.

Der C-Code des Wurm ist bereits im Internet frei erhältlich, somit ist davon auszugehen, das veränderte Varianten des Wurmes auch außerhalb Australiens aufzufinden sind bzw. werden.