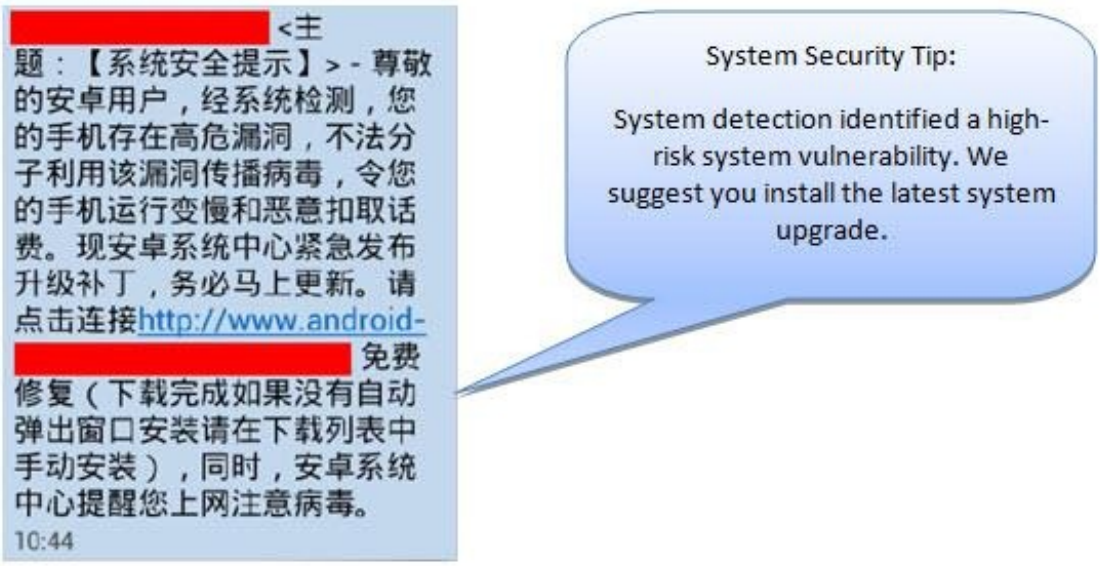
NQ Mobile Alerts Mobile Users to New Android SMS Malware Threat

April 11, 2012



UpdtBot spreads via SMS messages

San Jose, CA (RPRN) 04/11/12 — - Today, NQ Mobile Security Research Center, in collaboration with the leading cyber security expert Dr. Xuxian Jiang <http://www.csc.ncsu.edu/faculty/jiang> at North Carolina State University, and chief scientist for NQ Mobile is alerting Android users to a recently discovered malware strain. UpdtBot disguises itself as a system upgrade and spreads via SMS messages, which contain a link to the malicious application file. Once installed, UpdtBot registers a remote Command and Control (C&C) server, which instructs the infected device to send text messages, make phone calls, and download and install apps.

How it works

UpdtBot spreads via SMS messages, which tell users their system is at risk and they need to install the latest system upgrade. The message contains a URL link, which claims to link to an important system upgrade but really links to the malicious app. Once a device is infected,

UpdtBot can send SMS messages, make phone calls, and install software.

Mitigation

Because UpdtBot disguises itself as a system update file and can be remotely controlled by its author(s), we believe it poses a serious threat to mobile users. Our research shows that more than 160,000 Android users have been

affected by UpdtBot. While we don't have any statistics on

how it's being used by the cybercriminals who created it, we believe they'll attempt to make money off it. Once it's installed, the malware authors can instruct it to send messages or make calls to costly, premium-rate numbers. They can also download apps, which can quickly result in a high mobile device bill.

To protect yourself from UpdtBot (and other forms of malware), we recommend that you follow a few common-sense guidelines:

1) Only download applications from trusted sources, reputable application stores, and markets, and be sure to check reviews, ratings and developer information before downloading.

2) Before you install an app, carefully review the "permissions" and make sure you're comfortable with the data they'll be accessing.

3) Watch out for unusual or suspicious behavior on your mobile devices, such as unauthorized charges to your phone bill, text messages from unknown sources, and decreased battery life.

4) Download up-to-date mobile security software on your mobile device, such as NQ Mobile Security, which scans your apps for malware and helps you locate a lost or stolen device. All NQ Mobile Security users are automatically protected from this malware and all other mobile threats.

Media Contact Name: brent bucci
Media E-mail: bbucci@mww.com
Media Web Address: http://research.nq.com/?p=410

Main image credits: http://research.nq.com/?p=410
Body image credits: NQ Mobile

About the author:

RushPR News is a social media newswire service created to help you with content creation and distribution to news outlets and social media networks. RushPRnews can also assist you with your web strategies with experts advices and strategies at an affordable cost. Write us at news@rushprnews.com

Filed Under: BREAKING NEWS, Technology, GOOGLE NEWS, MSN NEWS, New Media - WEB 2.0, Social Media, PRESS RELEASE, Wireless - MOBILE PHONE, WI FI, YAHOO NEWS

RUSH PR NEWS newswire and press release services at rushprnews.com / Anne Howard annehowardpublicist.com

Content- Legal Responsibility - All material is copyrighted - You may repost but you MUST link back to the original post on your page and acknowledge Rush PR News as the news source. Rush PR News is not legally and/or morally responsible for content of press releases, opinions expressed or fact-checking.

Rush PR News cannot be held legally responsible for material published and distributed through its newswire service or published in its press-room and therefore cannot be sued for published material. Third-party must be contacted directly to dispute content.

Rush PR News is not the contact for material published.