Researchers discover dangerous ways computer worms are spreading among smartphones

April 9 2014

Professor Kevin Du conducted research on HTML-5 apps at Syracuse University's L.C. Smith College of Engineering and Computer Science. Credit: Syracuse University

Professor Kevin Du and a team of researchers from the College of Engineering and Computer Science at Syracuse University have recently discovered that some of the most common activities among smartphone users—scanning 2D barcodes, finding free Wi-Fi access points, sending

SMS messages, listening to MP3 music and watching MP4 videos—can leave devices vulnerable to harmful "computer worms."

These worms can infiltrate smartphones through apps designed in a specific computer language/code—and they can do more harm than just steal the device owner's personal information, researchers warn. They can also spread to the owner's friends and personal contacts.

"These attacks target an increasingly popular type of app known as HTML5-based app," says Du who worked on the research with students Xing Jin, Tongbo Luo and Derek G. Tsui. "Traditionally, apps are developed using a platform's native technologies, such as Java in Android and Object C in iOS. HTML5-based apps do not use platform-dependent native technologies, but use JavaScript instead, which is universally supported by all platforms.

"The advantage for developers is clear: write an app once and it can run on all major platforms," Du explains.

The team has so far identified 14 vulnerable HTML5-based apps from three types of mobile systems, including Android, iOS and Blackberry. Developers of those vulnerable apps have been informed and in an effort to give them time to fix the problem, researchers have decided not to disclose the names of the vulnerable apps.

"Imagine you're at the airport and you want to find the free Wi-Fi. When you scan, your phone is going to display the Wi-Fi access points. That could be an easy channel for a hacker to inject malicious worm code into your smartphone," Du says. "Once the worm takes control, it can duplicate itself, and send copies to your friends via SMS messages, multimedia file sharing, and other methods."

Researchers are currently working to develop solutions to help users and

app developers detect and prevent such attacks.

Details of how attacks can occur this attack are described in a paper titled "XDS: Cross-Device Scripting Attacks on Smartphones through HTML5-based Apps" that the team will present at the Mobile Security Technologies workshop in May.

Du and his team are continuing their research to see what other apps might be at risk.

"We are launching a large scale search in the Google Play market and expect to find more vulnerable apps," says Du. "By 2016, it's estimated that more than fifty percent of the mobile apps will be produced using HTML-5 technology. This is just a disaster waiting to happen," he adds.

More information: www.cis.syr.edu/~wedu/attack/

Provided by Syracuse University