Researchers measure smartphone malware infection rates

April 8 2014

Researchers show that infection rates in Android devices at around 0.25 percent are significantly higher than the previous independent estimate. They also developed a technique to identify devices infected with previously unknown malware.

There is a steady stream of news stories and announcements about how many more new strains of Android malware appear in every passing year. Data showing infection rates in the real world has been hard to come by. There is a lot of data about the number of different malware samples discovered but not so much about the extent they are actually found in the wild. If smartphones are infected to the same extent as personal computers used to be, the resulting damage would be much more severe.

The few estimates that were out there vary greatly: ranging from more than 4 per cent of Android devices, according to an estimate by an anti-virus company, to less than 0.0009 per cent of smartphones in the US, according to a different estimate by group of academic researchers from the US.

What is the reason for this disparity?

University of Helsinki researchers working at the Intel Collaborative Research Institute for Secure Computing (ICRI-SC) will present a paper at this year's World Wide Web conference which provides an answer to

this question based on their work in the "Malware Insights" project.

The project team, consisting of Hien Truong, Eemil Lagerspetz, Sourav Bhattacharya, and Petteri Nurmi working under the guidance of Professor N. Asokan and Professor Sasu Tarkoma have been investigating the true extent of malware infection in Android devices. Working with Adam J. Oliner from the UC Berkeley AMP Lab, they discovered that infection rates in Android devices at around 0.25 per cent are significantly higher than the previous independent estimate. The project collected anonymized data from over 50 000 devices during a seven-month period.

An arXiv research report based on the work being done at the "Malware Insights" project at the department of Computer Science, has been featured in *MIT Technology Review*'s "Emerging Technology From the arXiv" section.

The researchers also speculated that smartphones infected with malicious apps may have other, benign, apps in common, possibly because the users purchase them all from the same app market. Based on this conjecture, the researchers investigated if it is possible to develop a technique to identify devices infected with previously unknown malware. In their dataset, this approach is up to five times more likely to identify infected devices than by choosing devices at random.

The Malware Insights project is part of the research being done at the Intel Collaborative Research Institute for Secure Computing (ICRI-SC).

More information: arxiv.org/abs/1312.3245

Provided by University of Helsinki