A system that facilitates malware identification in smartphones

September 9 2014

Researchers at Universidad Carlos III de Madrid have developed a tool to help security analysts protect markets and users from malware. This system allows a large number of apps to be analyzed in order to determine the malware's origins and family.

Malware is a type of malicious program whose general aim is to profit economically by carrying out actions without the user's consent, such as stealing personal information or committing economic fraud. We can find it "in any type of device ranging from traditional cell phones to today's smartphones, and even in our washing machine," explained one of the researchers, Guillermo Suarez de Tangil, from the Computer Science Department at UC3M.

With the massive sales of smartphones in recent years (more than personal computers in all of their history), malware developers have focused their interest on these platforms. The amount of malware is constantly increasing and it is becoming more intelligent; for that reason, "security analysts and market administrators are overwhelmed and cannot afford exhaustive checking for each app," noted Guillermo Suarez de Tangil. The development of this type of malicious programs has become a large industry that incorporates code reuse methodology. "They don't create a program from scratch, but rather they create a new sample," he stated.

The tool, developed by these UC3M researchers, baptized DENDROID and detailed in a study published in the review *Expert Systems with*

Applications, allows security analysts to scrutinize a large quantity of apps to determine the origins of a malware sample and the family to which it belongs. In addition, if a classification not directly matching a specific family is found, it allows a phylogenetic tree to be extracted from the application to determine the malware's possible ancestors. "The developers generally reuse components of other malwares, and that precisely is what allows us to construct this genetic map," Guillermo Suárez de Tangil explained. This information allows security analysts to take on the challenge of analyzing samples of malware never seen before.

The antiviruses used in smartphones employ detection engines based on signatures, which identify a specific type of malware from some features previously observed. "For this reason, its effectiveness is questionable," elaborated Guillermo, because smartphone resources are more limited that those of a PC. Furthermore, the high frequency of new pieces of malware makes it impossible to incorporate signatures at the same time," he pointed out. In contrast, the new tool they have developed "will help an analyst to protect markets and ensure that users will not need to completely depend on detectors in smartphones", the researcher concluded.

More information: Dendroid: A Text Mining Approach to Analyzing and Classifying Code Structures in Android Malware Families. Authors: G. Suarez-Tangil, J.E. Tapiador, P. Peris-Lopez, J. Blasco. Review: Expert Systems with Applications. Elsevier, vol. 41:4, pp. 1104-1117 (2014). DOI: 10.1016/j.eswa.2013.07.106

Provided by Carlos III University of Madrid

Citation: A system that facilitates malware identification in smartphones (2014, September 9)

retrieved 25 April 2024 from
https://phys.org/news/2014-09-malware-identification-smartphones.html