DeepSec 2016 Talk: Obfuscated Financial Fraud Android Malware: Detection And Behavior Tracking – Inseung Yang

Posted on **November 09,2016** by **sanna**

In Korea in particular, hackers have distributed sophisticated and complex financial fraud android malware through various means of distribution, such as SMS phishing, Google play, compromised web servers and home routers (IoT). In some cases, both smartphone and PC users are targeted simultaneously.

Inseung Yang and his team collect mobile android malware via an automated analysis system, detect obfuscations and malicious packer apps. In his presentation Inseung Yang will describe trends of malicious android apps and obfuscated mobile malware in Korea. He'll explain the policy methods for Korean mobile banking and the attack methods used by hackers, f.ex. the stealing of certifications, fake banking apps that require the security numbers issued to users when they open their accounts, Automatic Response Service(ARS) phishing attacks in conjunction with Call Forwarding, and the requesting of the One Time Password(OTP) number.

But Inseung will not only talk about recent trends of obfuscated malicious android apps in Korea, he'll also explain various mobile protection techniques to prevent you from obfuscation, packing and anti-debugging and other methods used to obstruct the detection and analysis of malware.

Image not found
http://blog.lyang.net/wp-content/uploads/2016/11/inseung-yang.jpg
inseung-yang — Inseung Yang is a member of the Analysis Team at KrCERT/CC, KISA.

Posted in:Conference,Development,Internet,Report,Security |
Tagged:Analysis,Android,DeepSec,Detection,Fraud,Malware,Prevention,Talk | With 0 comments