Summary of Dissecting Android Malware

Anthony Cali

Monday, February 8, 2016

According to Yajin Zhou and Xuxian Jiang of the Noth Carolina State University Android Malware has seen a significant rise in recent years. Their paper "Dissecting Android Malware: Characterization and Evolution" goes into significant detail on their findings. The paper also discusses the underlying frameworks in Android that allow for the construction and exploitation of malware.

According to Section III A. 1) most malware is inserted via repackaging. Using a real legitimate software and leeching off its userbase or updating the package with malicious code. This attack style is found in 86 percent of the malware examined. Under Section III C. 1) the authors mention about the Linux systemspace and vulnerabilities in privelege escalation. The vulnerabilities extend to the libraries such as WebKit, SQLite, and OpenSSL. Using one of these libraries malware can compromise the Android device at an OS level. Table I below shows a few of the vulnerabilities and associated malware.

Table I

Vulnerable Program	Root Exploit	Release Date	Malware
Linux kernel	Asroot	2009/08/16	Asroot
init(<= 2.2)	Exploid	2010/07/15	DroidDream, zHash DroidKungFu
adbd(<=2.2.1), zygote(<=2.2.1)	RATC Zimperlich	2010/08/21 2011/02/24	DroidDream, BaseBridge DroidKungFu DroidDeluxe DroidCoupon
ashmem(<=2.2.1)	KillingInThe NameOf	2011/01/06	-
void(<=2.3.3)	GingerBreak	2011/04/21	GingerMaster
libsysutils (<=2.3.6)	zergRush	2011/10/10	-

Overall the malware environment for Android has exploded.

Of the avaliable security suites at the time of the study the best could at best detect only 79.6 percent of all malware infections. The average detection was only around 20 percent. Thus the authors concluded that the mobile market is

a breeding ground for new and complex malware with little protection in place to stop its continued expansion and exploitation of users.