ITPP1085
ICT

ARC'14
مؤتمر مؤسسة قطر السنوي للبحوث
QATAR FOUNDATION ANNUAL RESEARCH CONFERENCE
Towards World-class Research and Innovation

MobiBots: Risk Assessment Of Collaborative Mobile-to-Mobile Malicious Communication

10.5339/qfarc.2014.ITPP1085

Abderrahmen Mtibaa, Ph.d.; Hussein Alnuweiri; Khaled Harras

Corresponding author :
amtibaa@tamu.edu
Texas A&m University, Doha, Qatar

Abstract

Cyber security is moving from traditional infrastructure to sophisticated mobile infrastreless threats. We believe that such imminent transition is happening at a rate exceeding by far the evolution of security solutions. In fact, the transformation of mobile devices into highly capable computing platforms makes the possibility of security attacks originating from within the mobile network a reality. All recent security report emphasize on the steadily increase of malicious mobile applications. Trend Micro, in their last security report, shows that the number of malicious application doubled in just six months to reach more than 700000 malwares in June 2013. This represents a major issue for today's cyber security in the world and particularly in the middle east. The last Trend Micro report shows that the United Arab Emirates has "by far" the highest malicious Android application download volume worldwide. Moreover, Saudi Arabia, another middle eastern country, register the highest downloads of high-risk applications.

We believe that today mobile devices are capable of initiating sophisticated cyberattacks especially when they coordinate together forming what we call a mobile distributed botnet (MobiBot). MobiBots leverage the absence of basic mobile operating system security mechanism and the advantages of classical botnets which make them a serious security threat to any machine and/or network. In addition, MobiBot's distributed architecture (see attached figure), its communication model, and its mobility make it very hard to track, identify and isolate. While there has been many android security studies, we find that the proposed solutions can not be adopted in the challenging MobiBot environment due to its de-centralized architecture (figure). MoBiBots bring significant challenges to network security. Thus, securing mobile devices by vetting malicious tasks can be considered as one important first step towards MobiBot security.

Motivated by the trends mentioned above, in our project we first investigate the potential for and impact of the large scale infection and coordination of mobile devices. We highlight how mobile devices can leverage short range wireless technologies in attacks against other mobile devices that come within proximity. We quantitatively measure the infection and propagation rates within MobiBots using short range wireless technology such as Bluetooth. We adopt an experimental approach based on a Mobile Device Cloud platform we have build as well as three real world data traces. We show that Mobibot infection can be really fast by infecting all nodes in a network in only few minutes. Stealing data however requires longer period of time and can be done more efficiently if the botnet utilizes additional sinks. We also show that while MobiBots are difficult to detect and isolate compared to common botnet networks, traditional prevention techniques costs at least 40% of the network capacity. We also study the scalability of MobiBots in order to understand the strengths and weaknesses of these malicious