Participatory Honeypots: A Paradigm Shift in the Fight Against Mobile Botnets

Pasquale Stirparo[1,2], Laurent Beslay[1]

[1] Institute for the Protection and Security of the Citizen
Joint Research Centre (JRC), European Commission, Ispra (VA), Italy
[2] Royal Institute of Technology (KTH), Stockholm, Sweden

Abstract. Due to the substantially different ecosystem we have to deal with when it comes to mobile security, using conventional techniques make harder to detect and react to malware attacks. We introduce the concept of *Participatory Honeypot*, a privacy-by-design system where users becomes partner of the collection of meaningful information subsequently used for the analysis.

Keywords: mobile botnet, honeypot, malware, privacy, participatory

1 Introduction and Motivations

With the exponential rising of smartphone penetration in people's daily life, mobile devices are attracting malware writers every day more. According to Fortinet, mobile malware has reached almost 200k samples increasing at the high pace of 1k new samples per day, with Android leading this market accounting for 79% of all mobile malware. This scenario triggers new security and privacy concerns. We believe that classical approaches to botnet monitoring and tracking cannot address effectively the mobile domain challenges. The reasons are mainly the differences in the infection vectors used and in the topology of the botnet. Due to the specific nature of the smartphone and the mobile ecosystem, mobile malware will hardly spread by performing network scans to look for vulnerable mobile phones to infect, therefore a typical honeypot system waiting to be attacked will not provide many information. Another classical method is the network flaw analysis, in order to find specific pattern that can be brought up to a specific malicious activity. Although traffic flaw analysis will still be very useful in the mobile environment too, emerging mobile botnets communicate via SMS or Twitter accounts, and this can be very hard to detect mainly for two reasons: a) discrimination between a valid SMS and a malicious one is not trivial, b) while standard network traffic (i.e. tcp/ip) is easier to monitor and respecting the user's privacy by properly sanitizing some contents, monitoring the outgoing and incoming SMS contents of users can be very invasive other than a tedious process. Finally, many modern malware are benign application at the beginning, downloading malicious payload afterwards as an update. However if they detect

that the mobiles are receiving random activities (meaning that could be an automated analysis system), such update is not triggered and the malicious part remain dormant.

This is the motivation behind the concept of participatory botnet detection systems we propose in Section 3: complete involvement of real users in order to provide meaningful and realistic insights on the mobile malware and botnet activity.

2 Related Work

While in the realm of classical "desktop" honeypot there is an extensive amount of work that has been done within the research community, the concept of Mobile honeypots is still new and quite unexplored. This section presents two of the most interesting concept that have been published so far.

In [1], Liebergeld, Lange and Mulliner introduce the concept of nomadic honeypot as an infrastructure to collect information on threats directly on mobile devices. In their design they employ virtualization to confine the mobile OS and remove its direct access to communication hardware. The prototype consist in a HoneypotVM running Android and an InfrastructureVM, which implements the communication part with the sensors, logging capabilities and a backchannel to communicate with the operator. This work has been developed under the EU FP7 project NEMESYS[3].

In [2], Wahlisch et al. introduce a design and implementation concept of mobile honeypot, which differs quite substantially from the previous one. According to the attacker model discussed in the paper, the authors state that there is no need to operate the mobile honeypot on real device. Therefore they implement the honeypot systems using well-known honeypot tools and connected to the UMTS network via USB stick, in the attempt to make the honeypot looking like a mobile phone. The choice of such architecture has also been driven by the aim to focus on remote attacks via the Internet.

3 Participatory Honeypot

The concepts exposed in [1] already envisage the participation of the user. That solution represents a great and important step toward what we believe to be one of the right mobile honeypot approaches, moreover we partially disagree with the authors who [2] state that "there is no need to operate the mobile honeypot on real device". However, being directly installed inside the user's device could lead to at least two serious issues:

1. if, for any reason, the VM separation get compromised the device will be out of control from the infection point of view;

[3] http://www.nemesys-project.eu/

2. it may be very invasive, and not many users may be willing to participate/ collaborate knowing that everything (SMS, calls, Internet traffic, etc.) is being monitored by a third party.

As an alternative, what we propose is a remote sandbox system where the user would download the application he intend to purchase, and he will use it during a limited test phase remotely on our system from his mobile phone via a mobile application provided by us. The basic concept can be summarized step-by-step as follow (see Figure 1):

1. The user interacts with the applications market via the Participatory Honeypot (PH) application and buys the one he chose;
2. The application is then installed in the user reserved space in our Participatory Botnet Detection System (PBDS);
3. When the user wants to use the application, he will launch the PH app (which will run inside a sandbox) and he will connect to the PBDS. The PH app will work like a VNC client, so the user will see the application in the smartphone's screen exactly as if it was installed directly on his device.
4. Once the testing period is over, and the application has not been flagged as malicious by the system, the user will get the application from the PBDS server to be finally installed directly on his device. Completing the system analysis, and in the light of the information provided to him by the PBDS, the user is also invited to evaluate from a privacy point of view the application at stake.

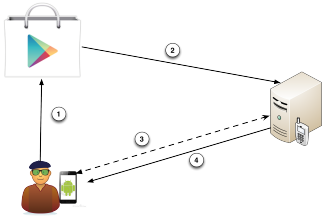

Fig. 1. Participatory Botnet Detection System (PBDS) scenario step-by-step

The scenario just described highlights immediately some of the advantages of the proposed solution:

- *Meaningful touches*: modern malware are getting intelligent in detecting if they are receiving random touches on the screen, which would mean that they are being under dynamic analysis and therefore they will keep the malicious activity dormant. The proposed solution will collect real meaningful gestures from the user that will actually be using the application for real;
- *Privacy friendly*: not being executed inside the user's real device we avoid to collect extra information that, most of the times, could be related to the user private activities and may not be always indispensable for the analysis.

4 A Privacy-by-design Information Gathering System

With the MobiLeak Project [3][4], Stirparo et al. shown that mobile applications usually handles and stores private user data improperly, therefore collecting excessive personal data in an indiscriminate way may put privacy at risk. However just not executing the monitoring systems directly on the mobile device, as in the solution proposed in Section 3, does not solve completely the risk as well. In fact, to make the PBDS appear as real as possible to the mobile application running inside the sandbox, the system still needs some personal data, e.g. user location, phone number, etc. To preserve as much as possible the privacy of the user, several mechanisms like location cloaking and the utilization of periodic pseudonyms generated using blind signatures may be used, as effectively demonstrated in [5] by Christin et al. Since the success of such system depends on the active contributions of the users, rewards and voting schemes will be put in place as incentive to participate, as well as for the operator to grade the level of users' contribution. As a contribution for a trustworthy relationships between the PBDS and the user acting as a partner, a Data Protection Impact Assessment is conducted and its results provided to the user prior to any exchange of data.

5 Conclusions

We introduced the concept and high level design of a Participatory Botnet Detection System, which involves the active participation of the users. We encourage their participation proposing solutions to protect their anonymity and privacy. We believe such an approach to be complementary with the nomadic honeypot proposed in [1], in which our privacy preserving solutions proposed in Section 4 could contribute to their backchannel that transmits the users' information.

References

1. Liebergeld, S., Lange, M., Mulliner, C.: Nomadic honeypots: A novel concept for smartphone honeypots. In: Proc. Wshop on Mobile Security Technologies (MoST13), in conjunction with the 34th IEEE Symp. on Security and Privacy
2. Wählisch, M., Vorbach, A., Keil, C., Schönfelder, J., Schmidt, T.C., Schiller, J.H.: Design, implementation, and operation of a mobile honeypot. arXiv preprint arXiv:1301.7257 (2013)
3. Stirparo, P., Kounelis, I.: The mobileak project: Forensics methodology for mobile application privacy assessment. In: Internet Technology And Secured Transactions, 2012 International Conferece For, IEEE (Dec. 2012) 297–303
4. Stirparo, P., Fovino, I., Kounelis, I.: Data-in-Use leakages from android memory - test and analysis. In: 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (WiMob'2013), Lyon, France (October 2013)
5. Christin, D., Rokopf, C., Hollick, M.: usafe: A privacy-aware and participative mobile application for citizen safety in urban environments. Pervasive and Mobile Computing (0) (2012) –