HosTaGe: a Mobile Honeypot for Collaborative Defense

[Tool Demo]

Emmanouil Vasilomanolakis, Shankar Karuppayah, Max Mühlhäuser, Mathias Fischer
Telecooperation Group,
Technische Universität Darmstadt
Center for Advanced Security Research Darmstadt (CASED)
firstname.lastname@cased.de

ABSTRACT

The continuous growth of the number of cyber attacks along with the massive increase of mobile devices creates a highly heterogeneous landscape in terms of security challenges. We argue that in order for security researchers to cope with both the massive amount and the complexity of attacks, a more pro-active approach has to be taken into account. In addition, distributed attacks that are carried out by interconnected attackers require a collaborative defense. Diverging from traditional security defenses, honeypots are systems whose value lies on in being attacked and compromised. In this paper, we extend the idea of *HosTaGe*, i.e., a low interaction honeypot for mobile devices. Our system is specifically designed in a user-centric manner and runs out-of-the-box in the Android operating system. We present the design rational and discuss the different attack surfaces that *HosTaGe* is able to handle. The main contribution of this paper is the introduction of the collaborative capabilities of *HosTaGe*.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous; D.4.6 [**Operating Systems**]: [Security and Protection - Invasive software]; C.2.0 [**Computer-Communication Networks**]: General: Security and Protection

General Terms

Security

Keywords

Mobile Honeypot; Android; Hostage; Security

1. INTRODUCTION

The growth of the number of mobile devices, and subsequently the amount of users, has created not only a whole new landscape with various advantages, e.g., better overall user-experience and communication capabilities, but also potential threats. Moreover, the availability of free and open wireless networks has increased tremendously to cope with the connectivity demands of these users. From airports and coffee shops to university and company networks, the probability of discovering such a wireless network is high. Users tend to use these networks, without knowledge of their trustworthiness, reliability and security. This lack of security awareness combined with recent trends such as the *bring-your-own-device* can have severe effects to the global network security landscape.

This new large ecosystem of users, devices, and networks can be seen in a twofold and contrary manner. On the one hand, the wireless networks can be exploited by adversaries as an attack medium to compromise or infect the connected machines and devices using malware. This has already been observed in many cases, e.g., malware crafted for mobile operating systems (OSs) adding thousands of devices to botnet networks like *Android.Bmaster*[1]. On the other hand, we argue that these devices and networks can be defended and at the same time utilized to create a rival community of defenders that collaborate and exchange alert information, thus substantially reducing the attacking surface.

From conventional networks, additional defenses like Intrusion Detection Systems (IDSs) [2] and dynamic firewalls are known for the detection of malicious behavior. However, these defenses are usually passive, and deployed on non-mobile devices. IDSs tend to be resource exhaustive and thus not applicable to mobile devices. Moreover, firewalls cannot protect from all types of malicious activities and usually require complex configurations that might overwhelm ordinary users.

In contrast to the aforementioned lines of defense, honeypots, i.e., systems whose value lies solely in being probed, attacked or compromised [5], can provide a more active and in-depth view on attacker activities. Moreover, low-interaction honeypots, simulating network operations on a TCP/IP stack level, can provide a lightweight and straightforward defense mechanism, that is especially suited to protect mobile and resource-constrained devices.

Existing work in this direction [3, 9, 8] usually focuses on the detection of mobile-OS specific attacks only. For instance, Mulliner et al. were the first to discuss the idea of a honeypot for smartphones, by providing initial ideas, challenges and an architecture of such a mobile honeypot [3]. In addition, the majority of honeypot proposals have been focusing only on implementing novel detection meth-

SIN '14, September 09 - 11 2014, Glasgow, Scotland Uk

http://dx.doi.org/10.1145/2659651.2659663.

[1] `http://www.symantec.com/connect/blogs/androidbmaster-million-dollar-mobile-botnet`

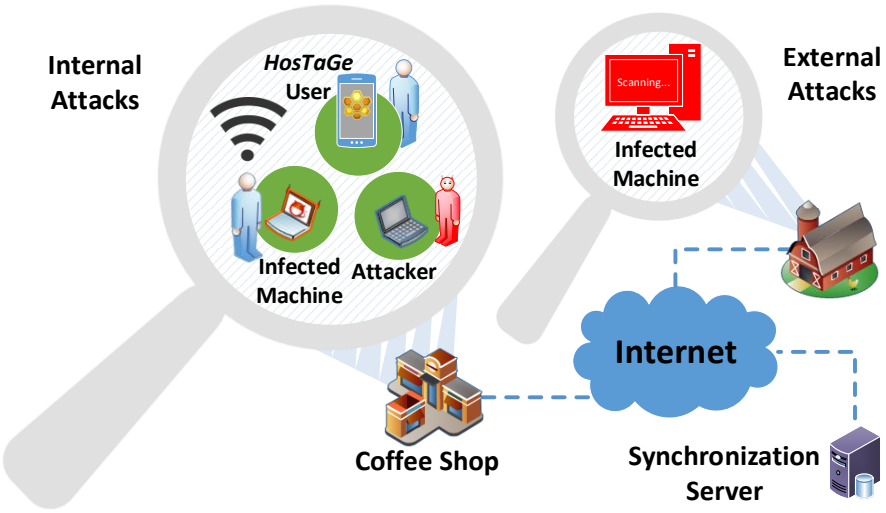


Figure 1: Attack surfaces and collaborative capabilities of *HosTaGe*

ods or concepts. Hence, user-friendly solutions were not the primary focus and only security professionals were assumed as their targeted users. However, the idea of creating user-centric honeypots is getting more attention lately. Antonatos et al. [1] proposed the "Honey@home" project, in which organizations and people can participate by deploying honeypots that report to a centralized honeypot monitoring system. Nevertheless, this approach does not include mobile devices and no clear benefits are described for the end-user to participate.

In our previous work [7], we proposed the idea of *HosTaGe* that stands for *Honeypot-To-Go*: lightweight, low-interaction, portable honeypots for mobile devices that aim on the detection of malicious wireless network environments. *HosTaGe* serves as a tool to increase the security awareness among ordinary users and allows them to check wireless networks for signs of malicious activity. Moreover, such honeypots can also assist network administrators to analyze the security status of their own networks on-the-go.

In this paper, we extend the idea of *HosTaGe* by focusing on the design rational of the honeypot as well as distinguishing the different attack surfaces that can be monitored via *HosTaGe*. In contrast to existing related work that is focusing on mobile-OS specific attacks, our proposal is based on a user-centric honeypot that runs out-of-the-box on Android mobile devices. *HosTaGe* benefits the users by providing an indication of the security state of their visited networks and thus fosters their interest and motivation to utilize the application. The main contribution of this paper is an introduction to *HosTaGe's* collaboration capabilities. We argue that to cope with the massive amount of cyber-attacks [6], there is a need for large-scale collaboration in terms of exchanging alert data among users, e.g., detecting propagation of new malware unknown to commercial anti-virus engines. *HosTaGe* supports both, remote synchronization through a central server as well as local collaboration, e.g., via Bluetooth.

The remainder of this paper is organized as follows: In Section 2 we discuss the concept behind *HosTaGe* along with the different attack surfaces it is able to handle and its collaborative capabilities. In Section 3, we describe the GUI details of our system along with insights of the user-centric approach that we followed when designing *HosTaGe*. Besides that, we also shortly discuss the limitations of our system. Section 4 provides insights on how we envision the proposed demonstration of *HosTaGe*. Finally, Section 5 concludes this paper.

2. HOSTAGE: A LIGHTWEIGHT MOBILE HONEYPOT

HosTaGe aims at alerting users about the security health status of a wireless network they are connected, or planning to connect. As a low-interaction honeypot, it emulates a set of services/protocols and waits for any incoming connections to these emulated services. Protocols supported by *HosTaGe* involve most of the protocols exploited by adversaries and malware, i.e., HTTP, HTTPS, SMB, Telnet, FTP, and SSH. As any incoming connections are considered malicious, all subsequent communication with *HosTaGe* is logged, for further analysis. In the following, we describe the different attack surfaces that *HosTaGe* can cover by distinguishing them into internal and external attacks. In addition, we describe how users can benefit by forming a community to exchange alert data about potential malicious networks.

Detecting malicious activities.

Malware, especially when they are new and unknown, can propagate rapidly throughout a large population of vulnerable devices. In this sense, wireless networks can provide adversaries a significantly increased attack surface. Similarly, human attackers may also target these machines to either steal credentials or compromise them. For both of these types of adversaries, honeypots can be utilized as a mean of gathering knowledge as well as an early warning system that notifies users about malicious environments.

We categorize such attacks that are launched within the same network as *internal*, indicated as *"Internal Attacks"* in Figure 1. Internal attacks may include malware propagating through infected machines and adversaries conducting scans to gather information within the connected wireless network.

HosTaGe detects any attack targeting its emulated services and notifies the user immediately. The user can then decide whether or not to continue using his device(s) in the malicious network on his own risk.

Detecting network misconfiguration.

Wireless networks that are provided by many organizations and service industries, e.g., restaurants and fast food chains, are usually aimed as an add-on service in satisfying their users' needs. However, some of the networks may cause more harm than good to their users [4]. For instance, a misconfigured network, i.e., missing network filtering or firewall rules, that exposes the users directly to the Internet may allow the user to be targeted by malware that are scanning the Internet for vulnerable machines.

We argue that network misconfiguration can potentially lead to various security issues for the users [4]. The large number of malware actively scanning over the Internet for targets, results in a successful infection within a few minutes for unpatched machines[2]. *HosTaGe* can severely reduce the network misconfiguration attack surface by either providing the opportunity to a user to check the network status or help a network administrator to conduct on-the-go security checks.

We classify such attacks that are launched from outside of the connected network as *external*, indicated as *"External Attacks"* in Figure 1. *HosTaGe* detects such attacks on the emulated services and informs the user to take the appropriate actions.

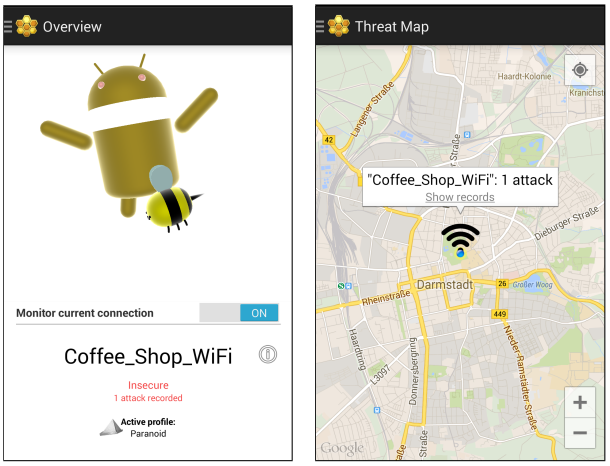
A community-based initiative.

In addition to the aforementioned capabilities, *HosTaGe* allows the users to benefit from the observations (or detections) of other *HosTaGe* instances through a collaborative exchange of alerts among them. Users of *HosTaGe* can voluntarily share the alerts that have been recorded by their device with others. The alerts contain information about the name and identity of the wireless access point and time of last detected malicious activity. Using this information, it allows other *HosTaGe's* community members to be warned, even before connecting to a network that they have never been associated to in the past.

Information can be exchanged by either synchronizing their *HosTaGe* device with a centralized server as shown in Figure 1 or directly with other *HosTaGe* devices. For synchronization with the centralized server, a connection to the Internet is required. However, device-to-device synchronization provides an alternative, if at a certain point in time, Internet connectivity is not available. This device-to-device synchronization can be done via Bluetooth or NFC.

The advantage of this community-based initiative is that, *HosTaGe* users who are not able to detect attacks, e.g., users with non-rooted devices, can still benefit from the information provided from other members of the community. All users can utilize the *HosTaGe*'s ThreatMap (c.f. Section 3.1) that is an interactive map containing the location and the name of wireless networks around them, that have been deemed as malicious in the past. From that point onwards, users are advised to make a decision on whether they want to connect to a network.

[2]`https://isc.sans.edu/survivaltime.html`



(a) Threat Indicator (b) ThreatMap

Figure 2: Graphical User Interface of *HosTaGe*.

3. POWER TO THE USER: A USER-CENTRIC HONEYPOT-TO-GO

In this section, we give insights on the *GUI* design of *HosTaGe* along with a short description of the essential user-centric parts of the application.

For the optimization of the user experience, three user studies have been conducted. The first was based on the prototype's GUI, as described in our previous work [7], and was the basis for the complete redesign of the application's interface. The remaining user studies were conducted alongside the iterations within the software development cycle, providing dynamic and valuable feedback.

Overall 62 participants of mixed age and gender took part in the user studies. Some of the supplementary interesting findings are described in the following. An average of 72% of the total participants tend to utilize publicly available wireless networks and 64% of the respondents would be interested on alerts about the safety of such networks. Moreover, an average of 76% participants claims that they would avoid wireless networks that are labeled as unsafe. Furthermore, 82% of the participants claimed they do not use any kind of security software in their mobile devices, a finding that illustrates the need for security awareness and user-friendly/centric security applications. In addition, *HosTaGe* can indirectly benefit users without security software, since it can act as an early stage detection/alert mechanism and thus support security vendors to contain new threats.

3.1 HosTaGe components

In the following, we focus on some of the specific user-centric and user-friendly components of *HosTaGe*: *Threat Indicator*, *ThreatMap*, *Profile Manager*, *Alert Data Synchronization* as well as various other enhancements.

- *Threat Indicator:* The default view of the application is designed in such a way that *HosTaGe* immediately conveys the network security status via a *Threat Indicator* as seen in Figure 2(a). Via four different animations, the application indicates all possible states of the honeypot in the connected wireless network: 1) *Enabled* 2) *Disabled* 3) *Previously Attacked* 4) *Attacked.*

- *ThreatMap: ThreatMap* is a visualization mechanism for *HosTaGe* to geographically illustrate the recorded attacks via a multitude of techniques, e.g., GPS data and GeoIP discovery. This results on the creation of a heat map of infected networks that the user can avoid as well as share with other users, as we describe in the following *Alert Data Synchronization* paragraph. A view of the *ThreatMap* is shown on Figure 2(b).
- *Profile Manager:* Through the *Profiles* menu, the user can easily choose from a list of profiles that offer combinations of OSs and services that the honeypot will emulate, e.g., a Windows XP machine, a Web server, etc. In addition, advanced options are also offered, e.g., the creation of custom profiles.
- *Alert Data Synchronization:* As an additional proactive mechanism, our system allows alerts to be synchronized within the *HosTaGe* community. Hence, users are well-informed of even malicious wireless networks that have never been connected to in the past. The synchronization is possible through both device-to-device, via NFC and Bluetooth, as well as remote synchronization via a centralized server.
- *Other Enhancements:* Many additional features exist in order to assist the user, such as *statistics* and alert *records* of the monitored networks. Moreover, to support advanced users and network administrators, additional settings are configurable. For instance, the user can activate specific ports and services through the *Services* menu. Finally, in-depth customization of the honeypot can be made via the *Advanced Settings* section within the *Settings* menu.

3.2 Limitations

It is important to mention a limitation that stems from the Linux-based nature of the Android OS, which prevents applications to have direct access to privileged network ports, i.e, ports below 1024. As such, *HosTaGe* cannot emulate services that are utilizing these privileged ports, e.g., HTTP, SMB, SSH, unless the host device is *rooted*. This limitation is overcomed by the *Alert Data Synchronization* (cf. Section 3.1) feature that allows users to benefit from other devices that actively utilize *HosTaGe*. Therefore, *non-rooted* devices can still function, by providing crucial information to the users via the *ThreatMap* feature.

HosTaGe is a honeypot and thus inherits their structural disadvantages, i.e., a honeypot will only detect attacks that are actively targeting it. In addition, one may argue that the environments that we are mainly focusing on, e.g., coffee shops, are dynamic and thus infected machines may not be present in the network anymore. Nevertheless, a network that is labeled as harmful by *HosTaGe* indicates that it is either misconfigured or that infected machines (or adversaries) utilized it -at least once- for malicious activities. *HosTaGe* also provides the user with the total number of attacks that occurred in these networks. Hence, the user can make an informed-decision on whether to connect to a network based on the provided information.

4. DEMO

In the considered demonstration, a testbed to mimic the environment as shown in Figure 1 is set-up. Through simulated attacks, we demonstrate the detection capability of *HosTaGe*. Moreover, the features described in Section 3.1 are explained, to show the different ways in which *HosTaGe* users can utilize the application to assess the health status of a wireless network. Furthermore, the real world practicality of our system is shown, via the usage of a number of malware in a contained environment.

5. CONCLUSION

With the vast availability of wireless hotspots around users, these networks no longer serve only as a service to the users but also as an attack surface for adversaries targeting vulnerable devices. We argue that this problem can be alleviated using a community-based initiative that aims to share the knowledge about infected or misconfigured networks with other users within the community.

In this paper, we presented *HosTaGe*, a user-centric and user-friendly honeypot that runs out-of-the-box on mobile devices. *HosTaGe* aims on the detection of malicious network environments, misconfigured networks as well as to act as a catalyst to boost security awareness amongst ordinary users. The alerts generated and exchanged will encourage users to be more cautious when connecting to public wireless networks. Moreover, they can indirectly reduce the success of malware propagation in such hotspots. Specifically, users can avoid infected or misconfigured networks, or ensure that their system is patched and updated beforehand.

6. REFERENCES

[1] S. Antonatos, M. Locasto, and S. Sidiroglou. Defending Against Next Generation through Network / Endpoint Collaboration and Interaction. In *3rd European Conference on Computer Network Defense*, pages 131–141. Springer US, 2009.

[2] B. I. A. Barry and H. A. Chan. Intrusion Detection Systems. In *Handbook of Information and Communication Security*, pages 193–205. Springer Berlin, 2010.

[3] C. Mulliner, S. Liebergeld, and M. Lange. Poster : HoneyDroid - Creating a Smartphone Honeypot. In *IEEE Symposium on Security and Privacy (S&P)*, 2011.

[4] B. Potter. Wireless hotspots: petri dish of wireless security. *Communications of the ACM*, 49(6):50–56, 2006.

[5] L. Spitzner. Honeypots : Catching the Insider Threat. In *Computer Security Applications Conference*, pages 170–179. IEEE, 2003.

[6] Symantec. Internet Security Threat Report. Technical Report April, 2013.

[7] E. Vasilomanolakis, S. Karuppayah, M. Fischer, M. Mühlhäuser, M. Plasoianu, L. Pandikow, and W. Pfeiffer. This Network is Infected : HosTaGe - a Low-Interaction Honeypot for Mobile Devices. In *Security and privacy in smartphones & mobile devices*, pages 43–48. ACM, 2013.

[8] M. Wählisch, T. C. Schmidt, A. Vorbach, C. Keil, J. Schonfelder, and J. Schiller. Design, Implementation, and Operation of a Mobile Honeypot. Technical report, 2013.

[9] M. Wählisch, S. Trapp, C. Keil, J. Schönfelder, T. C. Schmidt, and J. Schiller. First Insights from a Mobile Honeypot. In *ACM SIGCOMM*, pages 305–306. ACM, 2012.