HoneyBot Services - Client Data Collection

Team CIRCL*

41, avenue de la Gare L-1611 Luxembourg Grand-Duchy of Luxembourg

*Electronic address: info@circl.lu; URL: http://www.circl.lu/

Contents

I. INTRODUCTION

CIRCL HoneyBot services consist of the distributed operation and exploitation of CIRCL HoneyBots. These services are part of a research project with the aim to improve security on Internet. A CIRCL HoneyBot is a low-interaction honeypot running on an embedded device, that is deployed in the premises of CIRCL partners. The HoneyBot listens to its unused IP [1] addresses specified by the partner [2]. The data remains the property of the partner and the partner mandates CIRCL for doing the related processing and exploitation.

II. OPERATION

The honeypot device and its software remains the property of CIRCL and is build and customized by CIRCL operators. A honeypot can be configured in two modes. In each mode all[3] packets are captured and transmitted over an encrypted channel to a CIRCL HoneyBot collector.

honeypot In this mode the HoneyBot listens on all ports TCP[4] and UDP[5]. Each connection attempt is established and timed out. In case of TCP protocol usage, when an external

host sends a SYN packet to the honeypot, the honeypot replies with a SYN/ACK [6]. Hence, it is possible to record the initial exchanged bytes. This is is particularly useful to log the requests of higher protocols. This mode should be used if the partner provides only a few IP addresses to monitor.

blackhole In this mode, the HoneyBot is completely passive and simply captures the packets. In this case, the initial interactions cannot be recorded due to the missing established handshake. This restriction, is useful when the HoneyBot partner provides more than 127 IP addresses.

In both modes, the partner must provide the following information to a CIRCL operator.

- Public IP address which is configured on its primary network interface.
- Netmask which is also configured on its primary network interface.
- The default gateway needed to reach the HoneyBot collector.
- A TCP port, denoted p which is used to export the data to a HoneyBot collector.
- Define if a management network is used or not.

If a management network is used, two network interfaces are used for the HoneyBot operation. The primary address is used for the HoneyBot data export and maintenance. The second network interface is used for the data gathering. Hence, on the second network interface a public IP is configured that is dedicated to be monitored.

Each HoneyBot has its own client x509 [7] certificate and includes a x509 certificate of the configured HoneyBot collector. When the HoneyBot is powered on, it automatically tries to establish an TLS/SSL [8]. connection over TCP (port p) to a CIRCL HoneyBot collector. When it, succeeds, it encrypts the captured data and sends it to the CIRCL HoneyBot collector. A HoneyBot has very little resources and does not buffer collected data. In case the HoneyBot looses contact with the HoneyBot collector, the data is discarded. When this happened, a HoneyBot automatically tries to reconnect to its configured collector.

III. ACQUISITION

Interested parties, having available public IP address space located in Luxembourg, can request a HoneyBot service by contacting CIRCL on the mentioned email address in this document. CIRCL is evaluating the request and notifies the requester as soon as possible. If the requester is interested in publicly mentioning its participation to the research project, a logo can be used on the CIRCL map visualization[9].

IV. MAINTENANCE

The maintenance, of the honeypot, is performed by a CIRCL operator on best effort basis. The maintenance is done via SSH, originated from CIRCL networks. Maintenance work, include configuration, fine tuning activities and debugging such as faulty data transmissions or services. In case, a CIRCL operator is not able to connect to a HoneyBot, an intervention of the partner is needed. These interventions are either a reboot of the HoneyBot device or the physical replacement of a HoneyBot device due to hardware errors.

A. Time Synchronization

Each collected packet gets a timestamp generated by the HoneyBot. Therefore, it is essential to have accurate timestamps. HoneyBots use the NTP to synchronize their local clocks.

V. DATA PROCESSING

The data recovered by a HoneyBot are stored in pcap[10] files that are rotated every five minutes. These files are then shipped to various processing nodes in the CIRCL infrastructure. Each node has a dedicated processing task. A processing task

decodes the collected data and transform it in a human readable form.

aggregates the collected or decoded data in order to have an overview.

enrich the collected data with additional knowledge from other CIRCL services.

VI. PROCESSING RESULTS RETRIEVAL

HoneyBot services are designed to help a partner to improve his security monitoring. Therefore, the processing result retrieval depend on the partner. Some partners simply want a document with overall statistics, other partners want to integrate HoneyBot services into security monitoring solutions in their infrastructures. The data processing results retrieval is negotiated with each partner. Options are, PDF documents sent by email or json documents [11] retrieved via a RESTful Web Services. [12]

Appendix A: Legal Disclaimer HoneyBot Services - Template

Between

CIRCL - Computer Incident Response Center Luxembourg
c/o "security made in Ltzebuerg" (SMILE) g.i.e.
41, avenue de la gare
L-1611 Luxembourg
Grand-Duchy of Luxembourg

and

Partner TBD
Address
hereafter called the Partner

(hereafter individually called the Party or collectively the Parties)

(1) Object
The Partner has asked CIRCL to conduct the following activities (hereafter called the "HoneyBot Services") :

Install in the Partner premises an embedded device (
Soekris net5501-70 or equivalent)
Use a virtual collector installed in the CIRCL infrastructure
Do a regular analysis of the collected information by a CIRCL operator

To operate, the HoneyBot device must be assigned a dedicated IP address (IPv4 and/or IPv6) and a default gateway. The HoneyBot device is by default listening on all TCP and UDP ports. The management communication done to the collector is done using SSH (RFC 4251) on a commonly agreed port. HoneyBot Services will regularly export the collected data to CIRCL via TLS/SSL

(RFC 5246) using another common agreed port. The management and data export are separated in order to ensure an adequate level of auditing and monitoring from the Partner infrastructure.

CIRCL will provide the Partner specific and required hardware and IT security expertise in the course of the HoneyBot Services on a best effort basis.

(2) Disclaimer

The HoneyBot Services will be conducted by CIRCL without any representations or warranties, express or implied.

In particular, CIRCL does not warrant the Partner that:
(a) the HoneyBot Services will be constantly available, or available at all; or
(b) the HoneyBot Services will be complete, true, accurate, up-to-date, or non-misleading.

The Parties should not use the results from the HoneyBot services in order to conduct law enforcement related activities. The sole goal of HoneyBot services is to affine security monitoring.

(3) Ownership of Hardware and Collected Data

All Hardware installed by CIRCL will remain the ownership of CIRCL.

All data collected in the framework of the HoneyBot Services will remain the sole ownership of the Partner.

In order to conduct the HoneyBot Services accordingly, the Partner authorizes CIRCL to use and analyse an anonymized version of the collected data in order to affine security monitoring. This authorisation will survive the term of this agreement.

It is understood by the Parties that the collected data are very focused and therefore will just improve the understanding of the security issue similar to the collected data of the HoneyBot.

(4) Limitation of liability

Both the Partner and CIRCL will not hold each other liable of any indirect loss and/or expense (including loss of profit) suffered by a Party in the framework of the HoneyBot Services.

(5)Confidential information

Both Parties shall maintain this Agreement as confidential. Either Party shall release no information about this Agreement, or the related terms.
Information about the Partners business or computer systems or security situation that CIRCL obtains during the course of the HoneyBot Services will not be released to any third party without prior consent.

CIRCL and the Partner may from time to time impart to each other certain confidential information including specific documentation. Each party agrees that it shall use such confidential information solely for the purposes of the HoneyBot Services and that it shall not disclose directly or indirectly to any third party such information either expressed or otherwise.

(6) Territoriality

This contract is subject to the laws of the Grand Duchy of Luxembourg.
All disputes arising out of this contract shall be subject to the exclusive jurisdiction of the Grand Duchy of Luxembourg.

(7)Price and duration

The HoneyBot services is provided as a free of charge service by CIRCL. The Partner will not pay for any activities in relation with the HoneyBot services.

The HoneyBot services and the availability of CIRCL equipments are provided for a period of three months starting from the date of this agreement signature. The HoneyBot services is tacitly renewed except if one of the party explicitly ask for termination.

---

[1] IPv4 (http://www.ietf.org/rfc/rfc791.txt) or IPv6 (http://tools.ietf.org/html/rfc4291)

[2] If only one IP addresses is configured, the data export and maintenance traffic is filtered out.

[3] Except data export and maintenance packets.

[4] http://www.ietf.org/rfc/rfc793.txt

[5] http://www.ietf.org/rfc/rfc768.txt

[6] http://www.ietf.org/rfc/rfc793.txt

[7] http://tools.ietf.org/html/rfc5280

[8] http://www.ietf.org/rfc/rfc5246.txt

[9] http://map.circl.lu/

[10] http://www.tcpdump.org/

[11] http://www.ietf.org/rfc/rfc4627.txt

[12] RESTful Web Services. Leonard Richardson, Sam Ruby. O'Reilly Media, Inc., Dec 17, 2008.