Privacy Policy

BASTION

Date
15 February 2021

Classification
Public

Author
SIDN Labs

Page
1/3

Contact
T +31 (0)26 352 5500
support@sidn.nl
www.sidn.nl

Offices
Meander 501
6825 MD Arnhem
The Netherlands

Mailing address
PO Box 5022
6802 EA Arnhem
The Netherlands

Title of application/study	BASTION: firmware-BASed honeypoT Internet Of thiNgs
Policy start date	15 February 2021
Purpose of application/study	In our SPIN project, we are working on ways of improving the security of home networks that include insecure IoT devices. In order to develop methods and technologies for detecting insecure IoT devices, we need to know more about the characteristics of such devices. The data from the IoT honeypot can help us to build a picture of the patterns followed by attacks on IoT devices. The BASTION project has therefore been set up under the umbrella of SPIN. We have previously used IoT honeypots in the MINIONS-NL project (see associated MINIONS-SPIN submission dated September 2019). However, the data collected in that project was subsequently found to cover only Mirai-related botnets. Furthermore, we had access only to the results of analyses, not to the raw network data. For the BASTION project, therefore, we intend to set up our own honeypots. In phase 1, we will use generic honeypots, calibrated specifically for IoT infections. The specific calibration will involve simulating the CPU architectures used for IoT devices, having certain ports open (e.g. Telnet on port 23 for the detection of Mirai attacks) or supporting particular vulnerabilities. In phase 2, we will use firmware files from actual IoT devices and run them in a virtualised environment. We will then

simulate (vulnerable) IoT devices and monitor how botnets attack them.

In both phases, the aim is to attract automated attacks, observe what action is taken and what implications those actions have for a device's network traffic. The resulting datasets can then be used to refine SPIN's detection capabilities, and to train our machine learning models to recognise abusive network traffic.

Personal data

The network traffic may include personal data, in the form of IP addresses identified as associated with (1) scanning IoT devices for vulnerabilities or (2) sending commands to devices, e.g. with the aim of installing malware.
The IP addresses of possible victims that we record may also include personal data, in the event that a DDoS attack is mounted on a device at the IP address of a natural person. In that event, we will also process the command, including the victim's IP address.

Such personal data processing is inherent to the study, since the network data supplied to us includes IP addresses and processing is deemed to begin as soon as the data is recorded. Processing is also necessary for understanding features of IoT behaviour, such as the sources of IoT malware (country, provider, home or business connection, etc). The network traffic that is processed and retained is not user traffic; it is traffic generated by malware.

Legitimate basis

The processing serves a reasonable interest. The processing of personal data is necessary for effective research into the security of IoT devices, with a view to developing methods and technologies for improving internet security.

Filters

No filters will be applied in the context of the study.

Retention

After two years, the data files will be anonymised by removing any personal data (IP addresses). Any data files that cannot be anonymised will be deleted.

Access

Access to the data is restricted to:

- The SIDN Labs SPIN/BASTION team
- The systems administrators at SIDN and SIDN Labs can log in to the VMWare cluster and are (theoretically) able to grant themselves access to the data.

The data is stored on a virtual server, to which only the people referred to above have access. Log books are maintained, enabling retrospective data access checking.

Publication/sharing

We intend to publish research findings that we make on the basis of the data. The publications will include descriptions of the data, including analyses and (anonymised) examples.

The collected (network traffic) data will additionally be made available on the SPIN IoT data platform, implying that the associated analyses will be in the public domain. However, steps will be taken to ensure that any such information that might related to individual people, such as IP addresses, is anonymised.

The collected data will not be made public, but may be shared with research centres (universities), providing that we have an applicable data sharing agreement with each such centre, under which the accuracy, purpose limitation, security and publication requirements of this policy are assured.

Type

Research and development

Other security measures

The virtual server is connected to the SIDN Labs network and protected by the SIDN Labs firewall. As a result, it is accessible only from the SIDN Labs network. Access from external locations is possible only by logging in via the SIDN Labs VPN, which requires authentication by means of a personal certificate in combination with a user name and password.

The virtual server runs on the latest Ubuntu LTS server operating system, with automatic updates enabled. Regular manual update checks are also performed.