Detection of IoT Malware in Computer Networks

Daniel Uhříček [1] Supervisor: Karel Hynek [1]

[1]Faculty of Information Technology, Czech Technical University in Prague

Motivation

Consumer-based IoT devices are ever and again found to have low-security standards. SOHO routers, smart cameras and other widespread devices connected to the internet are targeted by IoT malware due to their weak default credentials or remote code execution vulnerabilities. The thesis researches the behavior of current IoT malware families on the network level and aims to raise the situational awareness of network monitoring operators by identifying infected hosts, command-and-control (C&C) servers, and ongoing attacks.

Datasets

We gathered and validated two existing IoT datasets:

1. **UNSW IoT traces** [3] introduces tens of 24 hours long pcaps with 28 unique IoT devices from six device categories. For our problem, all generated flows were considered benign.
2. **Aposemat IoT-23** [2] is also divided into several long pcaps, called scenarios. Each scenario presents sole IoT malware family; namely, it is Mirai, Torii, Gafgyt, Kenjiro, Okiru, Hakai, Hajime, and Hide and Seek.

Furthermore, benign part was extended with anonymized **CESNET captures** from selected `/24` subnet of public IP addresses. The captures followed similar port distributions as seen in UNSW IoT traces and Aposemat IoT-23 datasets. Malicious part was extended with **custom C&C dataset** produced in a controlled, virtualized environment by deploying three representatives from major IoT malware families which each implement different communication protocol – Tsunami variant leveraging IRC; Gafgyt variant using a simple text-based protocol; and Mirai variant implementing a custom binary protocol.

Prototype

The proposed solution was implemented in the form of software prototype capable of processing real network traffic as part of NEMEA [1] – modular, flow-based network detection system.

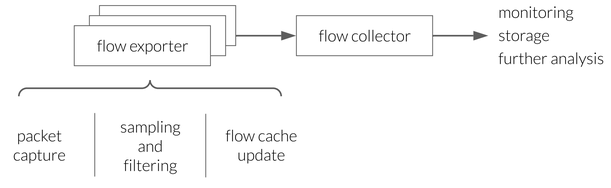

Figure 1. Generic architecture of flow monitoring.

The software prototype evaluates results per time bin of fixed configurable length, possibly receiving flows from multiple flow exporters.

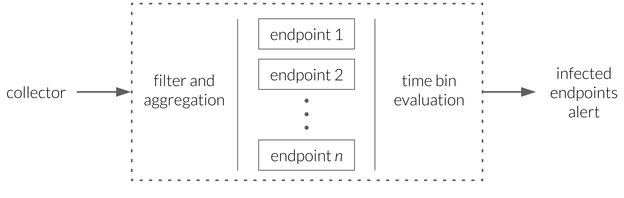

Figure 2. Top-level design of the proposed detection system.

Classifiers

We proposed a method of combining heterogeneous indicators using **informed meta-classifiers**. Each informed meta-classifier can be tied to a malware family and is implemented either as weighted majority voting or Boolean expression.

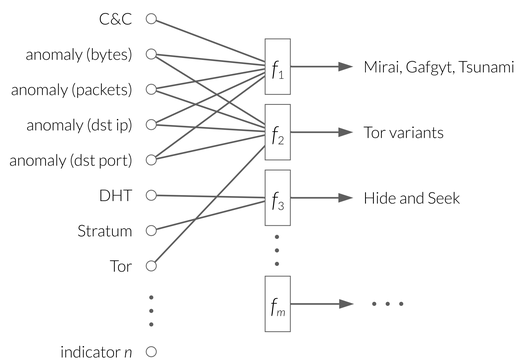

Figure 3. Informed meta-classifiers consuming indicators.

There are two types of classifiers: (1) classifiers producing one result per evaluation time bin, (2) classifiers producing n, further aggregated, results.

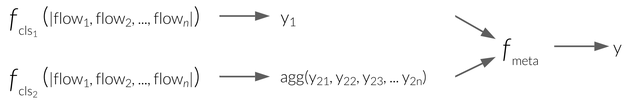

Figure 4. Two types of meta-classifiers' inputs.

C&C communication classifier

C&C classifier is a machine learning classifier built on top of 48 statistical features extracted from packet statistics (such as traffic rates, occurrence of TCP flags, or distributions of packet lengths and packet inter-arrival times).

Univariate anomaly classifier

Due to memory constraints of monitoring potentially large amount of devices, different online anomaly detection methods were considered. In the thesis, we modelled four distinct time series for each of monitored devices – sum of sent bytes, number of transmitted packets, unique destination IP addresses, and unique destination ports, using Brown's simple exponential smoothing with prediction intervals estimated from one-step forecast errors.

Signature based classifiers

Behavior of IoT malware which is rather deterministic can be captured using traditional pattern matching methods for selected application-layer data, or first n bytes of flow's payload. For demonstration, three types of of signature based classifiers were implemented to discover: (1) DHT protocol, (2) Stratum protocol, (3) Tor communication.

Evaluation

The final dataset for evaluating C&C classifier had a total of 147 374 benign instances and 1896 C&C instances. Training pipeline incorporated SMOTE oversampling, feature standardization, and a classifier. Two best performing models, comparable in terms of standard classification metrics, were AdaBoost and Random Forest.

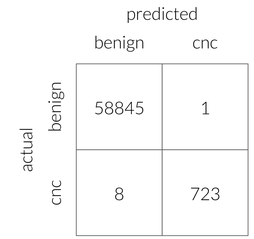

Figure 5. Confusion matrix of the AdaBoost C&C classifier.

System as a whole was evaluated on 40 hours of anonymized CESNET captures (total of 9.4 million flows). We registered no false positives and the detection algorithm behaved as expected. Finally, we proceeded with the evaluation on **real world malware samples active in April 2021**. Set of 105 IoT malware pcaps (provided by Avast s.r.o.) were manually annotated with potential C&C servers, mining pools, DHT nodes, and volumetric anomalies; and compared with the actual results.

combination	count
cnc + anomaly (bytes + packets + dst ip)	52
cnc + anomaly (bytes + packets + dst ip) + tor	16
cnc + anomaly (bytes + packets)	2
cnc	8
dht + anomaly (bytes + packets + dst ip + dst port)	9
dht + anomaly (bytes + packets + dst ip + dst port) + tor	2
stratum + anomaly (bytes + packets + dst ip)	7
stratum + anomaly (bytes + packets + dst ip) + tor	3
anomaly (bytes + packets + dst ip)	6

Table 1. Positive indicators results on the Avast malware dataset.

77/83 C&C flows present in the Avast data were correctly identified. 42 unique reassembled TCP streams and 37 unique C&C servers were reported. All anomalies were correctly recognized. The system was able to detect new variants of IoT malware and apart from the expected detections, we were able to match indicator combinations to different IoT malware family – Mozi.

References

[1] Tomas Cejka, Vaclav Bartos, Marek Svepes, Zdenek Rosa, and Hana Kubatova. Nemea: A framework for network traffic analysis. In *2016 12th International Conference on Network and Service Management (CNSM)*, pages 195–201, 2016.

[2] Agustin Parmisano, Sebastian Garcia, and Maria Jose Erquiaga. *A labeled dataset with malicious and benign IoT network traffic*. [online], January 2020. Stratosphere Laboratory [cit. 2020-10-01].

[3] Arunan Sivanathan, Hassan Habibi Gharakheili, Franco Loi, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman. Classifying iot devices in smart environments using network traffic characteristics. *IEEE Transactions on Mobile Computing*, 18(8):1745–1759, 2019.