Case Study: Detecting Suspicious IoT Devices

Identifying Malfunction and Malicious Activities in Large IoT Device Fleets for Odins Solution SRL.

Solving the customer challenge

Securing Large IoT Fleets

IoT Devices have become a prio target for cybercriminal botnet operators. Large botnets for rent are based on captured IoT devices under malicious control. Detecting and fighting botnet attacks have become a major challenge for IoT device operators. It is essential as an IoT operator to detect unfriendly attacks by botnet operators as fast as possible. Counteraction are a race between attackers and operators patching vulnerable fleets of IoT devices.

Separating Attacks from Defects

On large IoT fleets there is always a significant number of devices having strange operational behavior due technical problems. Attack detection needs to separate such devices with technical problems from devices being under attack.

Reducing False Positive and False Negative Results on Attack Detection

asvin has setup an advanced analytics service at the smart campus of Murcia in Spain, to reduce false positive and false negative results in attack detection. For that, devices of the IoT solution provider Odins have been boarded to the advanced behavior monitoring provided by asvin.

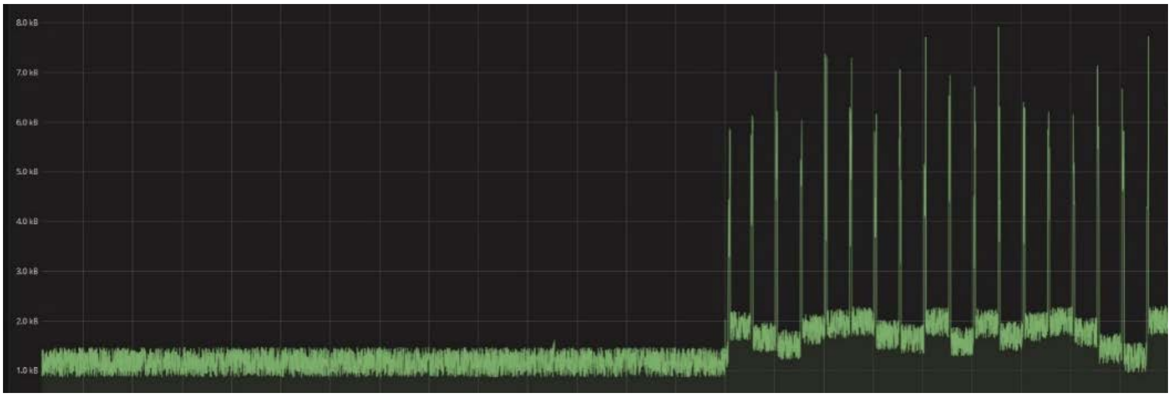
asvin solution facts

Detecting Attacks by Device Behavior

asvin is monitoring the behavior of single devices in large IoT fleets. The analyzing tools are recognizing changing patterns in device behavior such as reboot patterns and payload size. Changing patterns can be classified as technical defect or as the result of a cyberattack in progress.

Winning Time at Risk Mitigation

The pattern recognition enables operators on early detection of attacks on their IoT infrastructure. The asvin AI based algorithms are alarming on signs of malicious activities at an early stage of the attack. Operators can start immediately to plan and roll out their counteractions to condemn the attack.



Changing payload patterns of IoT devices indicating an early stage of a botnet attack on IoT devices.

About asvin

Founded in September 2018, Stuttgart-based asvin GmbH provides a platform-as-secure-solution based on Distributed Ledger Technology (DLT) for managing the software product life cycles associated with networked devices used in the Internet of Things. The applications and services support trace software, detect security vulnerabilities in IoT and IIoT to mitigate risk and ensure uninterrupted business processes. asvin was awarded the Best Cybersecurity Startup in Central Europe in 2020 by it-sa

Contact

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
Germany

Tel +49 711 220409338 0
info@asvin.io
www.asvin.io

Publisher

This case study has been published 2021 by asvin GmbH. All rights reserved.

Version 1.0, Published 09/2021