Powered by Faast

Persistent pentesting for IoT devices

What if your company was hacked through IoT devices? Webcams, printers, routers, TVs or IP phones are connected to the corporate network, they intercommunicate with other systems and external servers, opening up new attack vectors for cybercriminals.

This scenario is what moved our team of experts in hacking techniques to develop a new feature for Faast. Our persistent pentesting tool now performs a continuous scan of your systems, finding IoT devices connected to your network and detecting any configuration error or security flaw, that may allow access to your organization's data to an unauthorized user.

The first technology that persistently detects and analyzes new vulnerabilities in IoT devices

Innovation

This new feature offers a continuous and recursive scan of your organization's IoT devices.

Personalization

We adapt the scanning strategies based on the responsiveness of your system.

Global view

It implements real attackers' techniques helping to cover all stages of a cyberthreat life cycle.

Intelligence

An entirely new approach to fortifying the network and the IoT infrastructure.

Technical team

Team of experts in hacking techniques analyzes and validates the vulnerabilities detected.

Faast in your organization

- Discovers IoT devices connected to your infrastructure, those you are aware of and those you are not (Shadow IT/Shadow IoT).
- Detects the most common vulnerabilities that affect IoT ecosystems (insecure web interfaces, insufficient authentication/authorization, insecure network services, lack of transport encryption, known credentials, cross-site scripting, injections attacks).
- Identifies vulnerabilities of IoT devices in your company such as Smart TVs, VoIP PBXs or video conferencing systems that could be used as a pathway to bypass perimetral security defenses.
- Manages the vulnerabilities that affect to your IT assets using Vamps WebApp.

Target group

Our Faast technology for IoT devices is aimed at:

- Security analysts and researchers seeking new scalable security solutions to the heterogeneity of the different technologies of the millions of IoT devices.
- Companies providing security or cyberintelligence services that need to cover this new market niche.
- IT departments for which IoT device management has become a real headache.

ElevenPaths

More information on www.elevenpaths.com

A Telefónica COMPANY