Powered by Faast

Pentesting persistente para dispositivos IoT

O que ocorreria se hackeassem a nossa empresa através dos dispositivos IoT? Webcams, impressoras, routers, Wireless, AccessPoints, TVs ou telefones IP estão conectados à rede corporativa, intercomunicando-se com os demais sistemas e também com servidores externos, abrindo uma nova via de ataque para os cibercriminosos.

Este quadro de insegurança motivou nossa equipe de especialistas em técnicas de hacking para desenvolver novas funcionalidades para Faast. Nossa ferramenta pentesting persistente agora também escaneia os seus sistemas descobrindo os dispositivos da Internet das coisas ligadas à rede, detectando qualquer erro de configuração ou falha de segurança que permite o acesso não autorizado a dados do usuário na sua organização.

A primeira tecnologia que permite detectar e analisar de forma persistente as novas vulnerabilidades de dispositivos IoT

Inovação
Esta nova funcionalidade oferece scan constante e recursivo dos dispositivos IoT de sua organização.

Personalização
Adaptamos as estratégias de escaneamento com base na capacidade de resposta do seu sistema.

Visão global
Aplica técnicas de atacantes reais, ajudando a cobrir todas as fases de vida de uma ciberameaça.

Inteligência
Uma proposta totalmente nova para a proteção da rede e da infraestrutura IoT.

Equipe técnica
Equipe especializada em técnicas de hacking que analisa e valida as vulnerabilidades detectadas.

Faast na sua empresa

- Descobre os dispositivos da IoT conectados a sua infrastutura, tanto os que conhecem como os que não (Shadow IT/Shadow IoT).
- Detecta as principais vulnerabilidades presentes nos ecosistemas da Internet das Coisas (web de interface segura, autenticação/autorização insuficiente, serviços de sede inseguros, falta de cifras na capa de transporte, credenciais conhecidas, cross-site scripting, ataques de injeção).
- Descubra as vulnerabilidades dos dispositivos conectados a sua empresa como as televisões, centras de telefonia VoIP ou sistemas de video conferencias que possam ser utilizadas como vía de ataque, vinculado as medidas de perímetros de segurança implantadas.
- Gerir as vulnerabilidades dos seus activos da Internet das coisas através do portal online de Vamps.

A quem se destina?

A nossa tecnologia Faast para dispositivos IoT foi concebida para:

- Pesquisadores e analistas que procurem novas soluções de segurança escaláveis à heterogeneidade das diferentes tecnologias dos dispositivos IoT.
- Empresas que prestem serviços de segurança ou de ciberinteligência que precisem cobrir este novo nicho de mercado.
- Departamentos de TI para os quais a nova gestão de dispositivos IoT se transformou em um autêntico quebra-cabeça.