DHS
SUCCESS STORIES

Quokka, Inc.

TOTAL DHS SBIR INVESTMENT
$1,150,000

SBIR AWARDS
DHS

PHASE III REVENUE
$25M

8200 Greensboro Dr.
McLean, VA
www.quokka.io

Data breaches have been gaining considerable attention in recent years with more and more occurring due to firmware or hardware vulnerabilities, including on mobile devices. In 2016, mobile-security firm Quokka, Inc. (formerly Kryptowire), published a vulnerability report on a mobile phone purchased from Amazon that was discovered to have a preinstalled leakage channel. This begged the question, how many other devices were like this?

Already an area of interest within the Department of Homeland Security (DHS) Science & Technology Directorate (S&T), the DHS Small Business Innovation Research (SBIR) program released the Automated & Scalable Analysis of Mobile & internet of things (IoT) Device Firmware topic as part of its 2018 solicitation seeking proposals for solutions. Under this topic, Quokka, Inc. was selected to receive an award to develop SAFARI: Scalable Analysis of Firmware for Android and IOS. SAFARI makes it possible to identify firmware vulnerabilities at a large scale by automatically testing the security of mobile and IoT firmware and applications to the highest of government and industry software assurance standards. Analysts will no longer have to manually inspect for these pre-existing security vulnerabilities in the supply chain that can leave mobile and IoT devices open to threats such as the collection of personally identifiable information (PII) undetected by existing mobile threat detection technologies.

PHOTO CREDIT: RODION KUTSAIEV ON UNSPLASH
PUBLISHED MAY 2023

Quokka, Inc.'s efforts led to a pilot project with DHS's Cybersecurity and Infrastructure Security Agency (CISA) and the Idaho National Laboratory, resulting in SAFARI being operationalized by the government in June 2021 through a $25 million contract that will help protect citizens from costly and invasive firmware breaches.

"During this pilot project, SAFARI was used for testing firmware images of software on devices from manufacturers. We did this to identify purposeful or accidental errors and investigate those issues on a larger scale," explained Chris Gogoel, VP of Program and Product Management of Quokka, Inc. "Our strenuous testing uncovered 140 Common Vulnerabilities and Exposures (CVEs), which are very credible and serious threats. These findings have a big impact on everyone who uses an impacted mobile device and is concerned with threats to their security and privacy." With the support of DHS SBIR and S&T, Quokka, Inc. has further developed its technology and cultivated more strategic relationships and partnerships within the government and industry.

"The SAFARI tool's success in reviewing the software supply chain has drawn attention to the problem and further advancements in solutions for this threat area," said Gogoel.

Quokka's collaboration with DHS and the mobile phone companies, including original equipment manufacturer (OEM) and telecom providers, has facilitated the development of security automation initiatives that benefit individuals, government, and industries alike. The use of SAFARI has been a success as it continues to identify and fix vulnerabilities that could potentially harm citizens and consumers. Quokka, Inc. is dedicated to continuing research and development to update and advance technology to meet national security needs.

IMAGE CREDIT: FREEPIK