KNIGHTINK

ALL THAT WE LET IN:
HACKING 30 MOBILE HEALTH APPS AND APIS

According to Mobius MD, there are now over 318,000 mHealth apps available in major app stores. Over 60 percent of people have downloaded an mHealth app, which is now more common of a smartphone activity than online banking, job searches, or accessing schoolwork or educational content (Pew Research, 2015). With the pandemic pushing more patients towards virtual visits with their family physician and mental health provider, hackers have begun shifting their attention to this new attack surface in search of protected healthcare information (PHI) which is now demanding more of a payout per record than credit card numbers on the dark web.

Summary

This paper details the results of a 6-month long vulnerability research campaign into the compromise of 30 mobile health apps and APIs to demonstrate a systemic lack of hardening of mHealth apps and APIs to sufficiently secure protected healthcare information (PHI).

Author Information

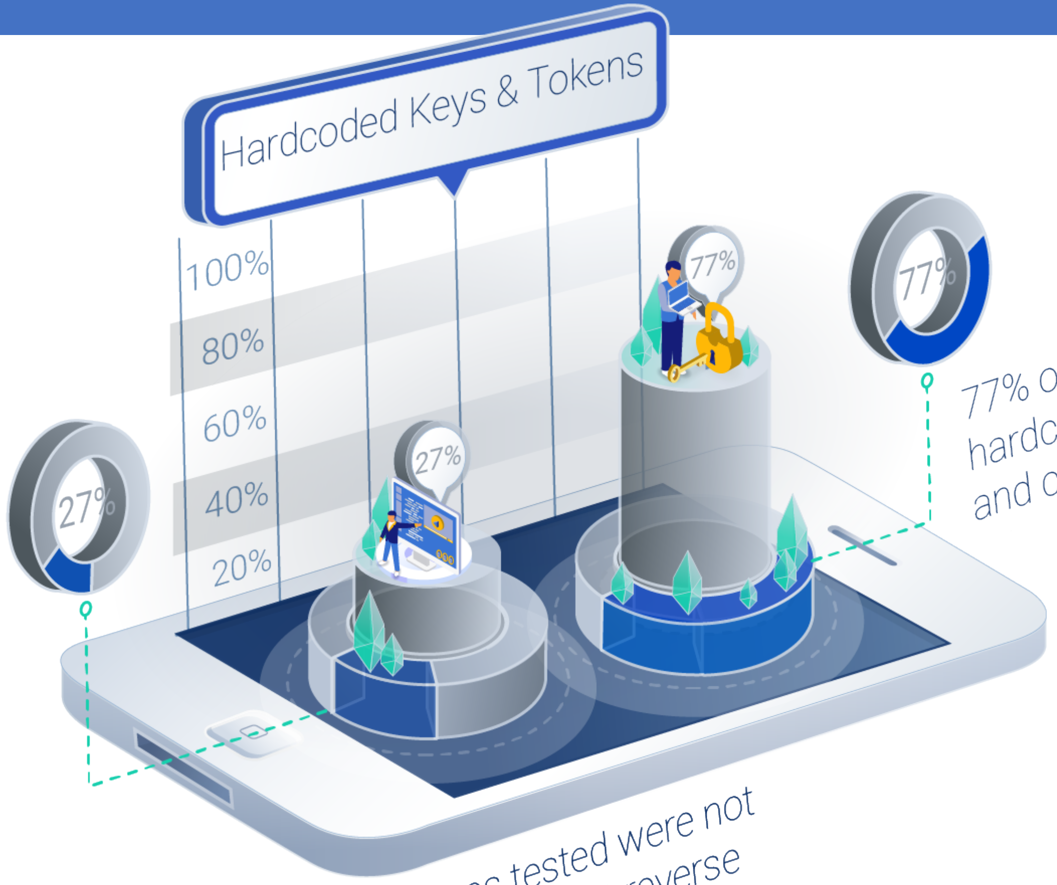
Alissa Valentina Knight
Partner
Knight Ink
1980 Festival Plaza Drive
Suite 300
Las Vegas, NV 89135
ak@knightinkmedia.com

Publication Information

This white paper is sponsored by Approov.

Initial Date of Publication:
February 03, 2021
Revision: 1.0

THE FACTS ON VULNERABILITIES IN MOBILE HEALTH APPS AND APIS



77% of the apps contained hardcoded API keys, tokens and credentials.

27% of apps tested were not obfuscated against reverse engineering.

SOURCES: KNIGHT INK, LLC
RESEARCHER: ALISSA V. KNIGHT
WEB: WWW.KNIGHTINKMEDIA.COM
EMAIL: INFO@KNIGHTINKMEDIA.COM

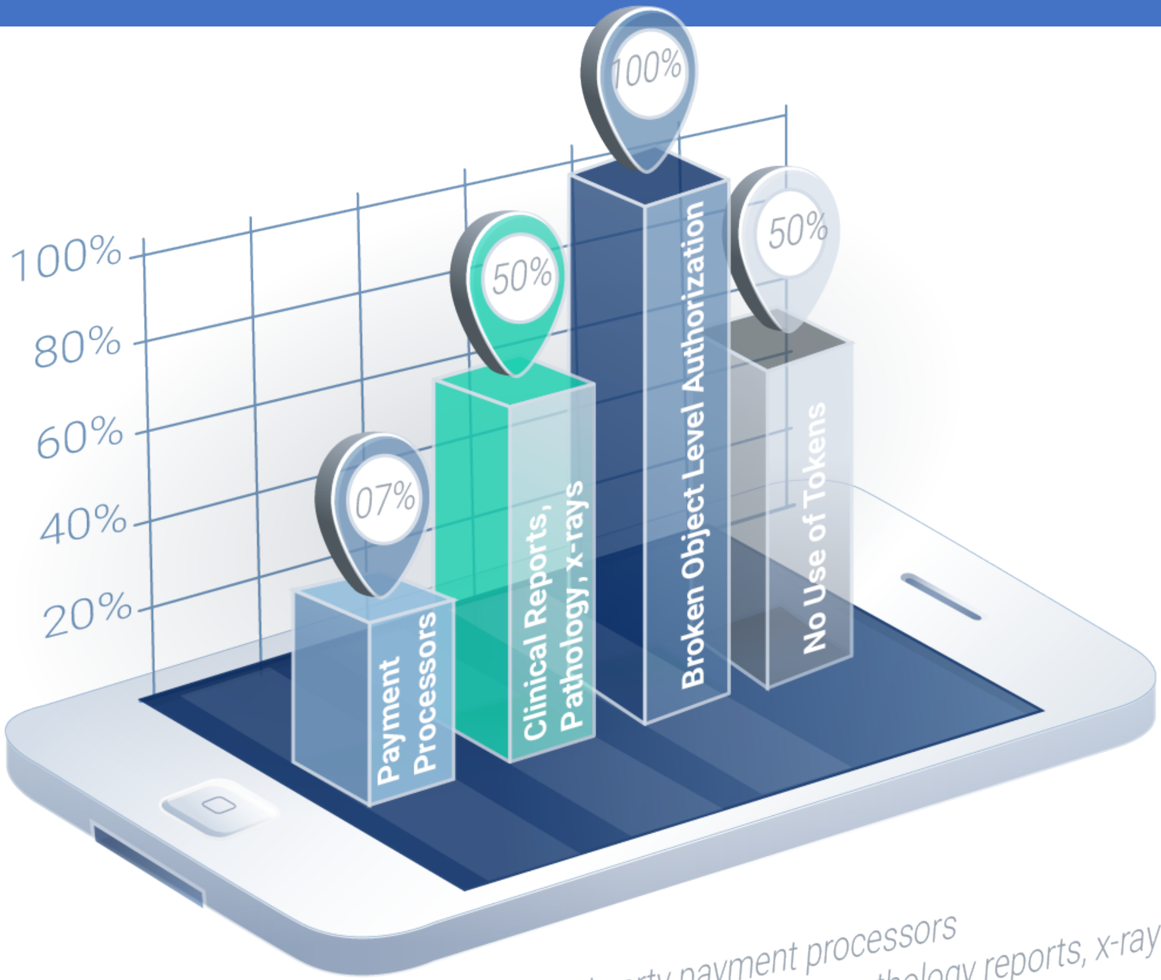
OFFICE:
1980 FESTIVAL PLAZA DR
SUITE 300,
LAS VEGAS, NV 89135

KNIGHTINK

RESEARCH SPONSORED BY:
approov

DOWNLOAD THE WHITE PAPER AT
WWW.APPROOV.IO/MHEALTH/HACKING

THE FACTS ON VULNERABILITIES IN MOBILE HEALTH APPS AND APIS



07% of apps contained hardcoded keys to 3rd party payment processors

50% of the APIs allowed unauthorized access to clinical reports, pathology reports, x-rays

100% of the APIs were vulnerable to broken object level authorization vulnerabilities

50% of the APIs did not implement tokens

SOURCES: KNIGHT INK, LLC
RESEARCHER: ALISSA V. KNIGHT
WEB: WWW.KNIGHTINKMEDIA.COM
EMAIL: INFO@KNIGHTINKMEDIA.COM

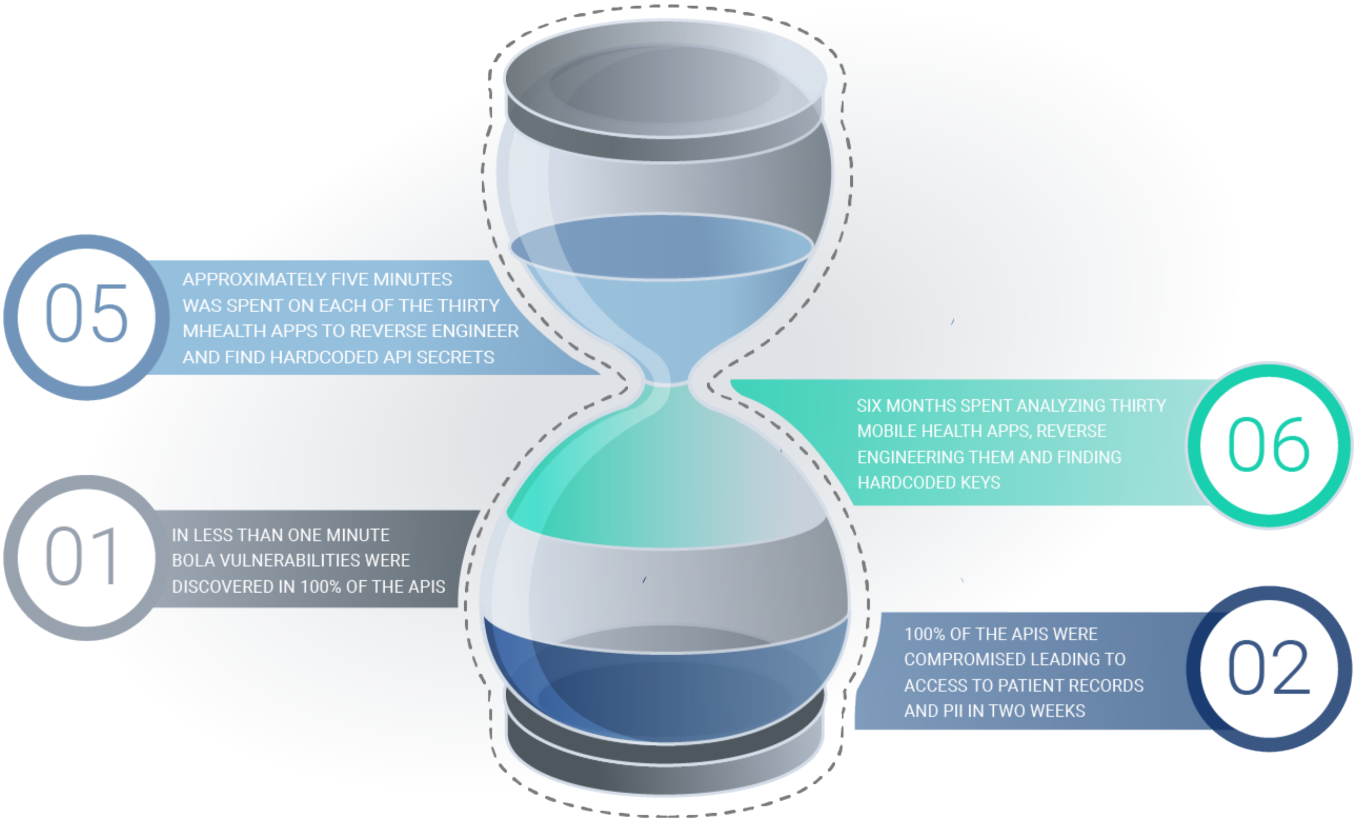
OFFICE:
1980 FESTIVAL PLAZA DR
SUITE 300,
LAS VEGAS, NV 89135

KNIGHTINK

RESEARCH SPONSORED BY:
approov

DOWNLOAD THE WHITE PAPER AT
WWW.APPROOV.IO/MHEALTH/HACKING

THE FACTS ON VULNERABILITIES IN MOBILE HEALTH APPS AND APIS



05

APPROXIMATELY FIVE MINUTES WAS SPENT ON EACH OF THE THIRTY MHEALTH APPS TO REVERSE ENGINEER AND FIND HARDCODED API SECRETS

06

SIX MONTHS SPENT ANALYZING THIRTY MOBILE HEALTH APPS, REVERSE ENGINEERING THEM AND FINDING HARDCODED KEYS

01

IN LESS THAN ONE MINUTE BOLA VULNERABILITIES WERE DISCOVERED IN 100% OF THE APIS

02

100% OF THE APIS WERE COMPROMISED LEADING TO ACCESS TO PATIENT RECORDS AND PII IN TWO WEEKS

SOURCES: KNIGHT INK, LLC
RESEARCHER: ALISSA V. KNIGHT
WEB: WWW.KNIGHTINKMEDIA.COM
EMAIL: INFO@KNIGHTINKMEDIA.COM

OFFICE:
1980 FESTIVAL PLAZA DR
SUITE 300,
LAS VEGAS, NV 89135

KNIGHTINK

RESEARCH SPONSORED BY:
approov

DOWNLOAD THE WHITE PAPER AT
WWW.APPROOV.IO/MHEALTH/HACKING

Knight Ink
1980 Festival Plaza Drive
Suite 300
Las Vegas, NV 89135
ak@knightinkmedia.com