Mobile Application Company Solves Complex Security Challenges

What happens when security vulnerabilities in a popular mobile app threaten to damage the game's integrity?

When a mobile application company released a successful new game, they found themselves faced with security challenges. Due to the popularity of its game, hackers began attacking vulnerabilities within the game that could damage the integrity and lead to cheating and devaluing the game economy.

To help protect the integrity of its game, the company had to find a partner to help them understand the weaknesses in their current security controls, and come up with creative solutions to keep hackers at bay.

What was the best way to approach this challenge?

- Perform an application security research assessment to provide insight into the effectiveness of current controls. Create a custom solution to improve security.
- Identify specific attack vectors, or areas of weakness, that a hacker might try to compromise and provide possible remediation.

PROJECT OVERVIEW

Organization Size:
Less than 500 employeess

Organization Industry:
Mobile application company

Challenge:
To create a custom solution to address issues with cheating and increase security within a mobile game application.

IMPACT

- Received a custom solution that increased efficacy of the application's security controls
- Improved security so the application was not an easy attack target
- Allowed for continued integrity of the game, leading to decreased user turnover
- Addressed possible attack vectors and offered ideas for improving security

MOBILE APPLICATION SERVICES:

Creating a Custom Solution

Information Gathering

Optiv gathered information on the current state of operation, then designed a custom security control to increase communication channel integrity. This helped ensure that data consumed by users was legitimate.

Reverse Engineering and Applying Controls

Optiv applied reverse engineering, or taking apart an application to the binary level and interpreting the machine code. This allowed them to see how attackers were seeking to defeat game protections. Then they implemented anti-reverse engineering controls to make the game a very expensive target for cheating.

Auditing the Server Structure

Next they audited the server structure, finding ways to secure controls for user settings so they can't be changed by an attacker.

Threat Modeling

By developing a threat model, Optiv showed how the application processes data, as well as likely attack vectors that might be used by hackers to compromise the application. The team then re-tested its custom solution against potential threats to make sure the entire application was as secure as possible.

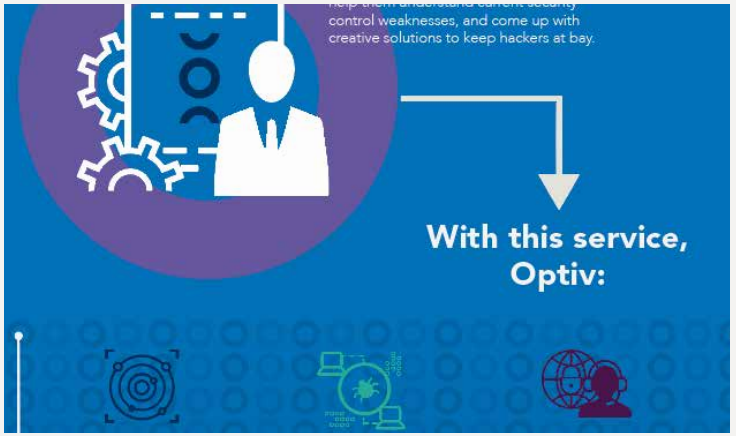
Securing Vulnerabilities and Restoring Game Integrity

If mobile application users think, even for a second, that a game is somehow "rigged," they will lose interest and the company will lose revenue. When this company found that teams of hackers were attacking the game and allowing users to cheat, it knew it had a serious security situation on its hands.

Optiv addressed the client's concerns and researched in-depth information to best understand how the application authenticated users, how those users sent information back to the server, and how hackers could potentially manipulate each of those steps and destroy the game's credibility.

As a result, the client:

- Gained a detailed understanding of the effectiveness of its current security controls.
- Received a custom solution that addressed security weaknesses.
- Increased the attack difficulty, making the game less of a target.
- Restored confidence in users that the game is reliable and legitimate.



View the Client Spotlight Infographic at www.optiv.com/resources/library

OPTIV

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

1125 17th Street, Suite 1700 | Denver, CO 80202 | 800.574.0896 | www.optiv.com

2.16 F1