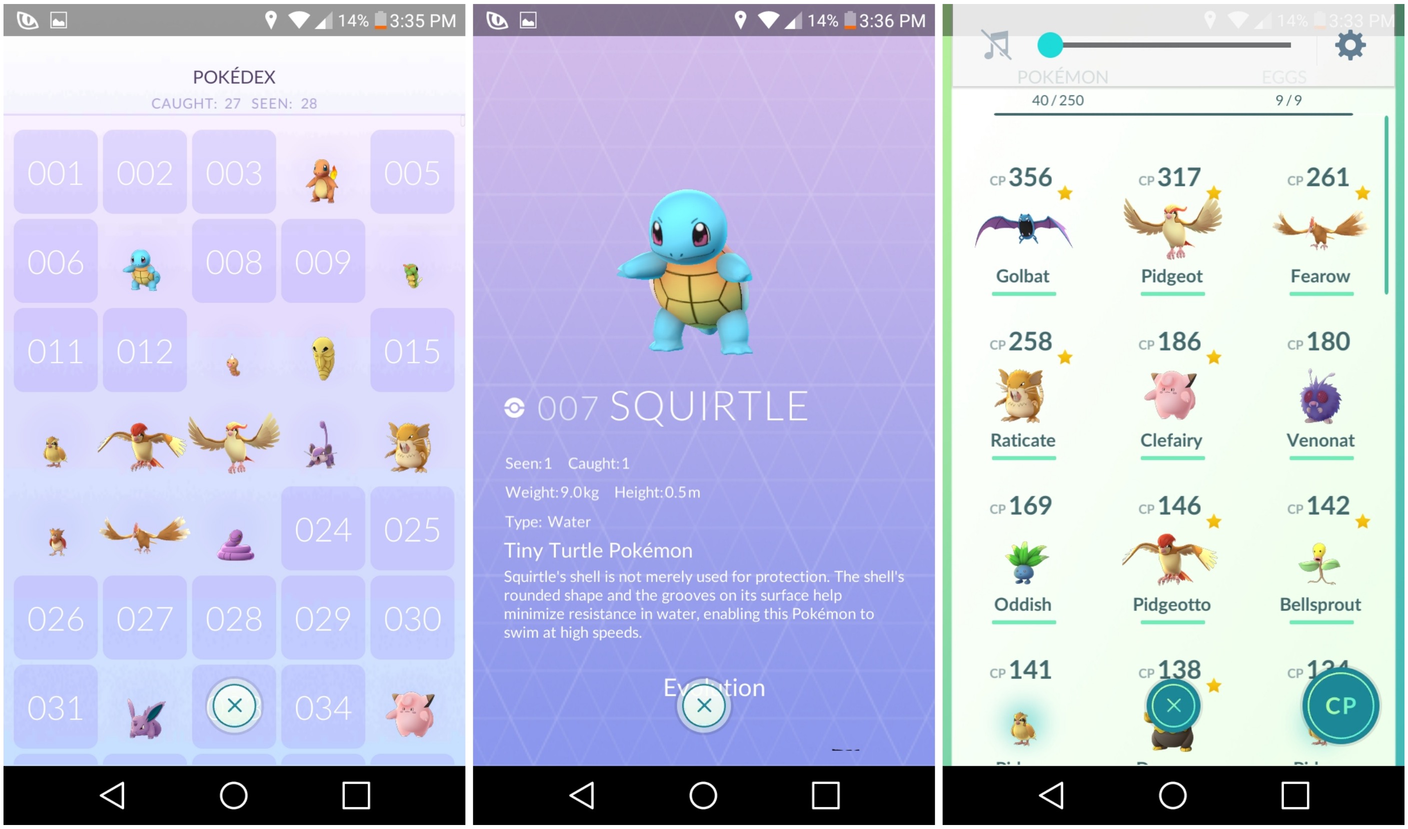
Pokémon Go API Fiasco Exemplifies Mobile API Security Concerns

It seems as though just about everyone lately is either playing or talking about the runaway phenomenon that is Pokémon Go. Pokémon Go may be one of the fastest, if not *the* fastest, growing mobile games the world has ever seen. This location-based augmented reality game for iOS and Android has already reached over 100 million downloads and generated over $160 million in worldwide net revenue since its release on July 6. In the short time since its launch, Pokémon Go has amassed a huge demographically diverse fanbase, a fanbase that includes many developers.



Seen: 1 Caught: 1

Weight: 9.0kg Height: 0.5m

Type: Water

Tiny Turtle Pokémon

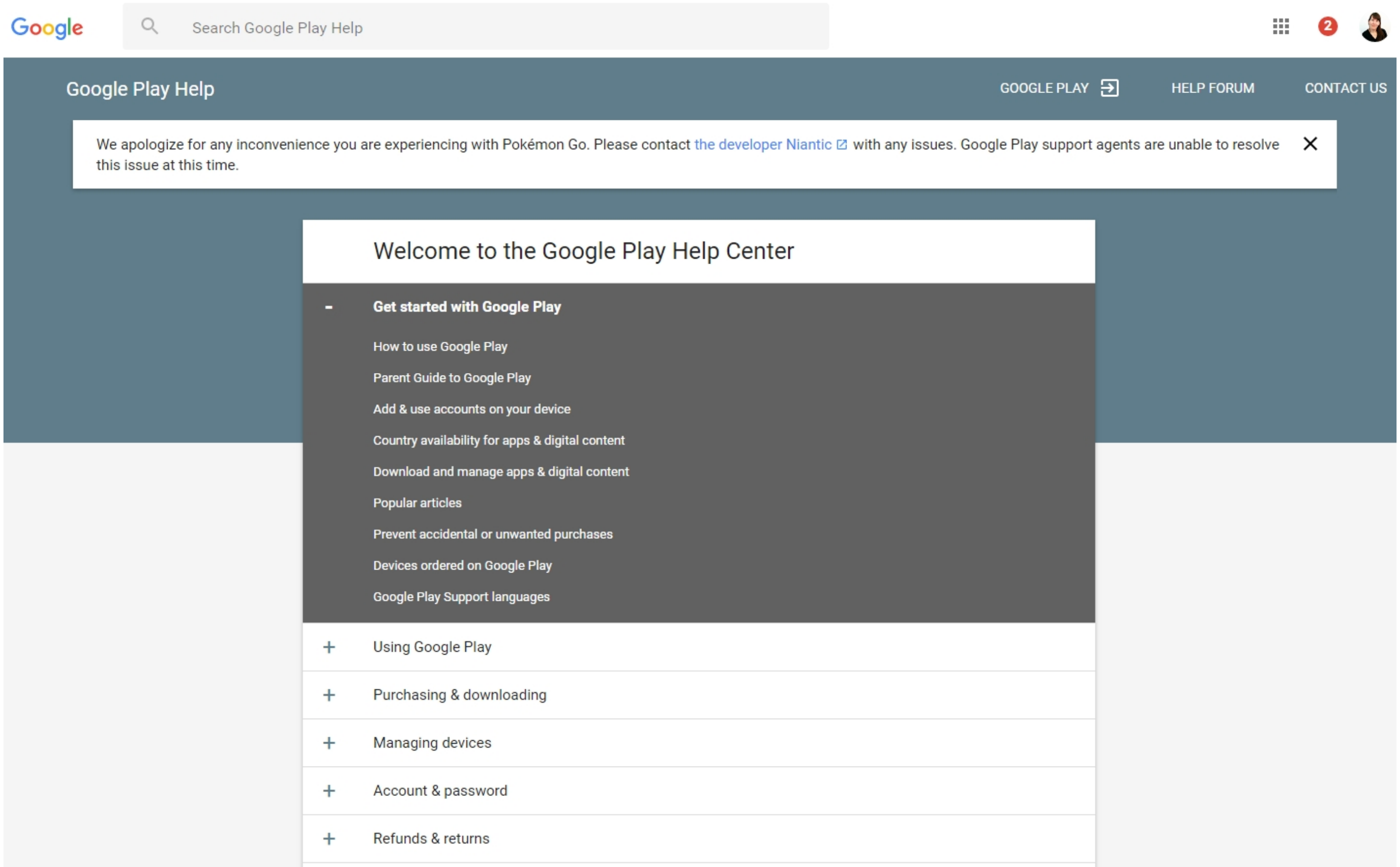
Squirtle's shell is not merely used for protection. The shell's rounded shape and the grooves on its surface help minimize resistance in water, enabling this Pokémon to swim at high speeds.

Screenshots of the Pokémon Go mobile game on Android.

Dozens of developers have reverse engineered the private, internal Pokémon Go API creating a number of unofficial APIs and third-party apps. There are quite a few tools available like mitmproxy and SSL Packet Capture that developers can use to reverse engineer APIs. Reverse engineering APIs is a piece of cake to do on any mobile app. Not long ago, the API powering the messaging/social mobile app Peach was reverse engineered and made available via unofficial Swift and Mac clients.

While some of the third-party Pokémon Go apps have been created as a means to "cheat" the game, the majority of them have been created as alternatives to broken game features. One of the biggest complaints from players about Pokémon Go has been the broken 3-step Pokémon tracker. Millions of players have been turning to unofficial Pokémon Go tracker apps like Pokévision until Niantic, the developer of Pokémon Go, issued cease-and-desist letters shutting down most of the unofficial APIs and third-party apps.

The move by Niantic to shut down unofficial third-party Pokémon Go apps has only further angered many players and developers who have been already loudly complaining about problems with the game. Niantic has also now removed the 3-step Pokémon tracker feature from Pokémon Go, while at the same time shutting down unofficial third-party Pokémon Go tracker apps. This is not going over well with many Pokémon Go players who believe that the Pokémon tracker feature is a crucial part of the game. There have been so many complaints about Pokémon Go, even more now with the shutdown of unofficial third-party apps, that Google has posted a note at the top of the Google Play help section directing complaints to Niantic.


Google
Search Google Play Help
Google Play Help
GOOGLE PLAY
HELP FORUM
CONTACT US

We apologize for any inconvenience you are experiencing with Pokémon Go. Please contact the developer Niantic with any issues. Google Play support agents are unable to resolve this issue at this time.

Welcome to the Google Play Help Center

- Get started with Google Play
How to use Google Play
Parent Guide to Google Play
Add & use accounts on your device
Country availability for apps & digital content
Download and manage apps & digital content
Popular articles
Prevent accidental or unwanted purchases
Devices ordered on Google Play
Google Play Support languages
+ Using Google Play
+ Purchasing & downloading
+ Managing devices
+ Account & password
+ Refunds & returns

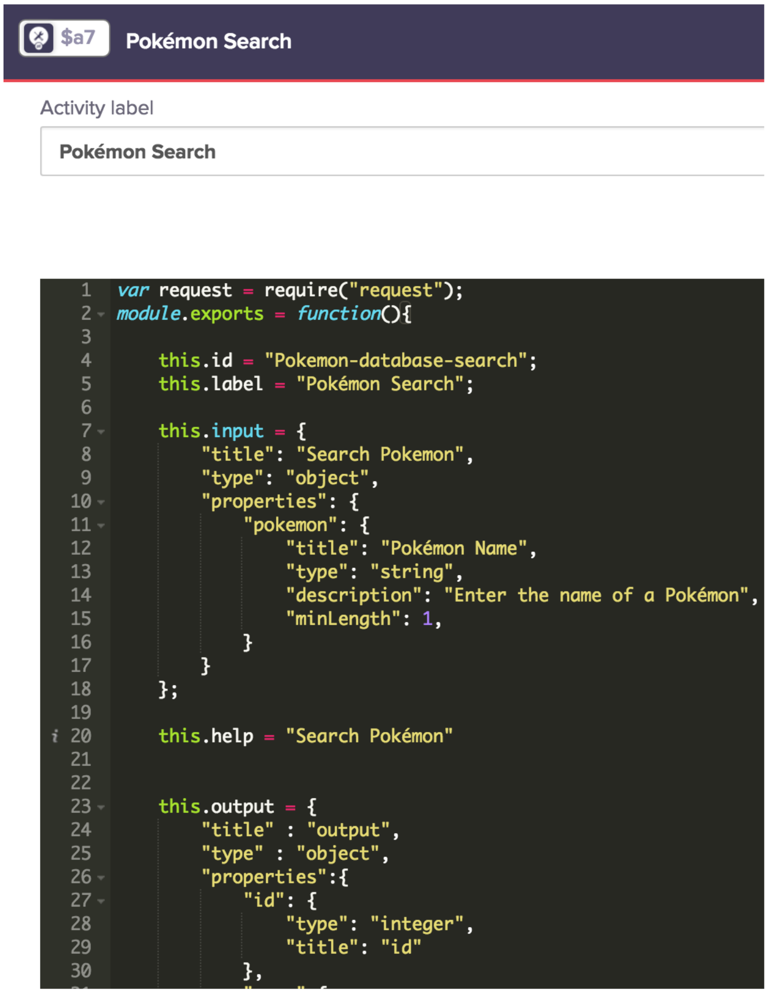
ProgrammbleWeb reached out to Kurt Collins, director of technology evangelism and partnerships, Built.io, who provided some of his views about unofficial third-party Pokémon Go apps and API security.

"From a revenue and security perspective, Niantic absolutely needs to shut down third-party applications. There's entirely too much information available in Pokémon Go. Niantic has a responsibility to their users to shut down any unauthorized access to their private APIs," says Collins. "With that said, when an app starts to see a growing number of unauthorized applications, that's a sign that they have an extremely engaged community whose needs aren't being fulfilled." Collins went on to say that "while they [Niantic] need to protect their players, they also need to build a public API/SDK as soon as possible so as to control the growth of the ecosystem. Without releasing their own APIs, Niantic runs the risk of losing control of their user and developer base."

While the majority of the unofficial third-party Pokémon Go apps are the products of developers who are simply enthusiastic fans of Pokémon Go, there are serious security concerns when it comes to the unauthorized use of internal or private APIs. It is very important that the developers of mobile apps are well-versed in a security-first approach to API development. Unfortunately, there are far too many mobile apps using APIs that are lacking even the basic countermeasures, let alone anything sophisticated to prevent unauthorized use of their APIs.

"There are existing security standards that limit the damage that can be caused by unauthorized access: OAuth and SSL being two of the primary ones," says Collins. "An API call will always be made in the open since the URL often includes the function being called on the server. However, if developers utilize industry standard security practices, they will limit the amount of damage that can be done from a security perspective."

Niantic is cracking down primarily on third-party apps that are using the private, internal Pokémon Go API. However, it is possible to create companion solutions for Pokémon Go that do not involve reverse engineering its API or violating the game TOS. Parthiv Patel, technical marketing manager at Built.io, was able to create a Pokémon Go solution using Built.io Flow's new activity builder and Pokéapi, a RESTful Pokémon Data API. The Built.io Flow activity Patel built can look up information about any specific Pokémon, allows users to see what the possible evolution of one of their Pokémon might be, and provides information about how to use specific Pokémon and what they can do.



Activity label

Pokémon Search

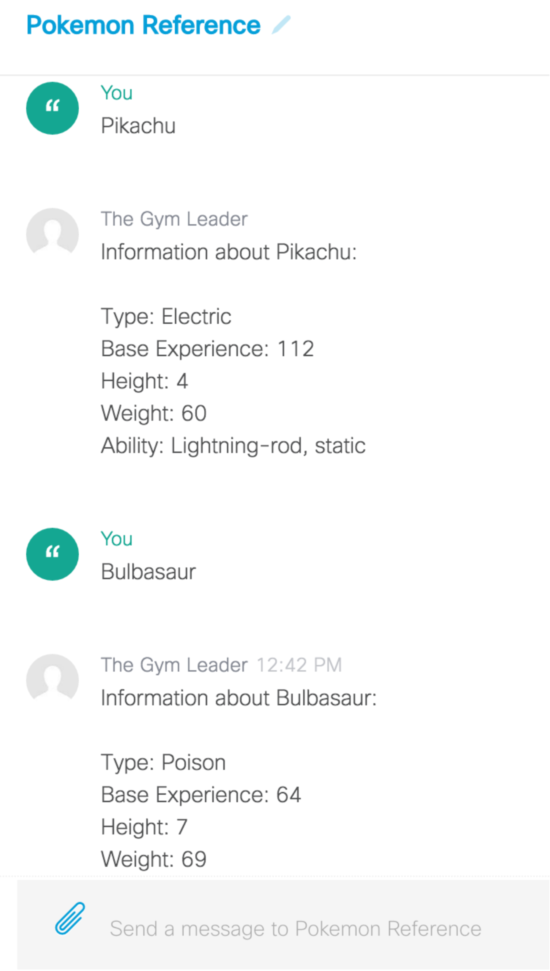
```
var request = require("request");
module.exports = function(){

    this.id = "Pokemon-database-search";
    this.label = "Pokémon Search";

    this.input = {
        "title": "Search Pokemon",
        "type": "object",
        "properties": {
            "pokemon": {
                "title": "Pokémon Name",
                "type": "string",
                "description": "Enter the name of a Pokémon",
                "minLength": 1,
            }
        }
    };

    this.help = "Search Pokémon"


    this.output = {
        "title" : "output",
        "type" : "object",
        "properties":{
            "id": {
                "type": "integer",
                "title": "id"
            },
```



You

Pikachu

The Gym Leader

Information about Pikachu:

Type: Electric
Base Experience: 112
Height: 4
Weight: 60
Ability: Lightning-rod, static

You

Bulbasaur

The Gym Leader 12:42 PM

Information about Bulbasaur:

Type: Poison
Base Experience: 64
Height: 7
Weight: 69

Screenshots of Built.io Activity Builder Pokémon Go integration code and Cisco Spark room message.

Patel also connected the Built.io Flow activity with Cisco Spark so that he could easily query the service from his phone or computer. He set up a trigger to start the flow any time a new message appeared in a Spark room. The flow parses the message, takes the Pokémon name and enters it into the custom Pokémon activity. The Pokémon activity GETs the relevant information from Pokéapi and then messages it back to the Spark room.

"Pokémon has always had a passionate fanbase who have created guides, databases, and other services related to the game," says Patel. "With the proliferation of APIs, we were able to connect these projects to services such as Spark or Twitter to provide instant access to these massive data sets."

It appears that Niantic is taking steps to further lock down the private, internal Pokémon Go API; however, the company may find protecting their intellectual property a very difficult and daunting task. Considering the mind-boggling popularity and rapid growth of Pokémon Go, reverse engineering may very well be a perpetual problem for its developers.

"From the perspective of keeping control of your intellectual property, reverse engineering is a problem. Although, in today's day and age, it's harder to reverse engineer an app given that you often only have access to the byte code on the client and can't easily access the code on the server," says Collins. "That's not to say that you can't get clues of what the server is doing since many of the API calls are initiated from the client in the first place. I don't consider this a glaring oversight in mobile API security as much as an inherent risk in deploying applications in general."

It will be interesting to see how Niantic handles the rapidly growing demand for new Pokémon Go features, fixes, and open APIs as well as the security of the Pokémon Go API. How the company handles the complaints of players and responds to third-party developers will determine if Pokémon Go becomes a platform with a massive and vibrant application ecosystem or just a passing fad.