Something Awesome Project

macspy - spyware for MacOS

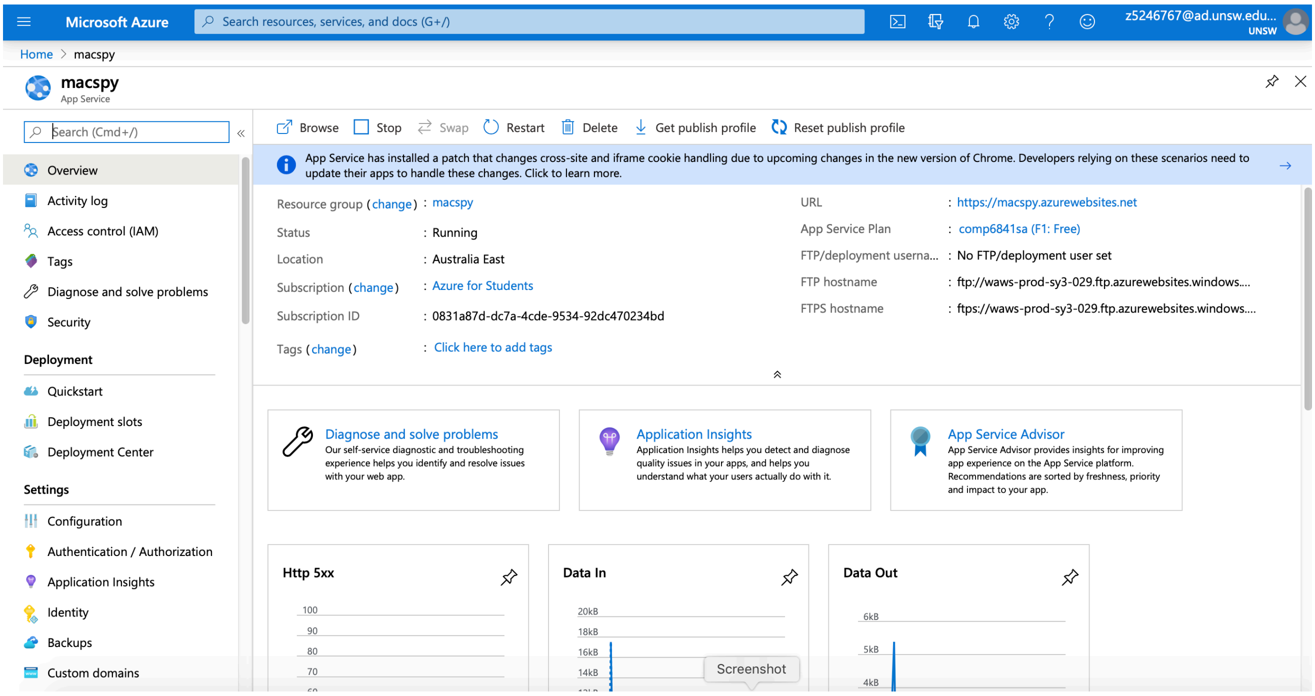
Consists of two major components - a target, who is being spied on, and an admin, who is doing the spying. The admin is able to send requests to the target for various data. The part that runs on the target's computer will discreetly collect data from the target in response and send it back to the admin.

The source code, along with the details of how to set it up and the features supported can be found here https://github.com/edwardgauld/macspy

Things I learned:
-How to assess the difficulty of tasks better.
-Problem solving. Had to research to figure out the best way to implement a feature that would work, and piece together and adapt unrelated segments of code to make it do what I wanted.
-How launch agents work and are configured
-Python3 libraries related to argument processing, data representation, audio recording and saving, socket programming, concurrent programming.
-How great decoupling and modular programming is. Keeping the 'main' code minimal made it easy to debug. The modular approach to supporting features made it very easy to integrate new ones, none of the main code had to be changed.

Other things:
I worked on trying to get a server up and working on azure so that the admin and target could move around the world and the system would still work. I also wanted to learn about C# frameworks and azure web app development.

I realised that what I wanted to do was too complicated to do in a couple weeks in addition to doing everything else. But I still learned a lot about this and made a valid start. You can view the code here https://github.com/edwardgauld/macspy0



App Service has installed a patch that changes cross-site and iframe cookie handling due to upcoming changes in the new version of Chrome. Developers relying on these scenarios need to update their apps to handle these changes. Click to learn more.

Resource group (change) : macspy
Status : Running
Location : Australia East
Subscription (change) : Azure for Students
Subscription ID : 0831a87d-dc7a-4cde-9534-92dc470234bd
Tags (change) : Click here to add tags

URL : https://macspy.azurewebsites.net
App Service Plan : comp6841sa (F1: Free)
FTP/deployment userna... : No FTP/deployment user set
FTP hostname : ftp://waws-prod-sy3-029.ftp.azurewebsites.windows....
FTPS hostname : ftps://waws-prod-sy3-029.ftp.azurewebsites.windows....

Diagnose and solve problems
Our self-service diagnostic and troubleshooting experience helps you identify and resolve issues with your web app.

Application Insights
Application Insights helps you detect and diagnose quality issues in your apps, and helps you understand what your users actually do with it.

App Service Advisor
App Service Advisor provides insights for improving app experience on the App Service platform. Recommendations are sorted by freshness, priority and impact to your app.

I also realised that the messages would not get past many firewalls, and could be detected by malware detectors. So I researched and found a cool way to get around this.
https://www.blackhat.com/docs/eu-15/materials/eu-15-Bureau-Hiding-In-Plain-Sight-Advances-In-Malware-Covert-Communication-Channels-wp.pdf
I would send the commands and data hidden in HTTP error messages, a form of stenography. Did not get to implement this and test it against the defences, but it was cool to learn about.