INSTITUTO SUPERIOR TÉCNICO
Departamento de Engenharia Informática
Forensics Cyber Security
MEIC-A 2016-2017 – 1st Semester

Email Location Track

Group 9
Dharita Queshil, Nº75669
Daniel Trindade, Nº76349
Miguel Viegas, Nº76532

1. Introduction

An email is an alternative way of sending information from one person to another by the internet. It's easy to use, faster and above all, nowadays, it's totally free. However, there is one subject that can make us think twice before watching or reply to an email: security and integrity of information.

Day by day, there have been more and more attacks to the network (and their users), and exchanging emails are a good "weapon" for these attacks. For example, a hacker could manage to send an email to a simple network user, that possess an email account, and in it, it has a link to a malicious website - Phishing.

There's clearly a problem among the internet in want to rely or not, when we receive an email. The receiver should be able to detect some information of an email before opening it.

2. The Idea

We present Email Location Track (ELT). The main goal of this tool is to trace the route of the email from the sender to the receiver, this means we save the information about all the servers where the email goes through until it reaches the destination.

With the IP addresses collected from the header of the email we can get the location of the receiver, the sender and all the servers. We are also going to collect all the basic information from the email header, like sending and reception time, the email address of the sender and the receiver.

It is possible to have some extras on this tool, for example, knowing if there were any changes in the sender's IP address, this can make us detect spoofing attacks. We can also retrieve the public data from the google account and all the other social networking websites.

In conclusion, this tool will be used to detect the location from where an email was sent.

3. Implementation

To find the sender's location, the tool must receive, as the input, the header of the email that was sent. With that input, the tool will analyze the header and obtain, with a parser, several aspects like: Who was the receiver of the email (Delivered-To), who was the sender (Return-Path) and from which IP address, and which hours, that email was sent (Received/X-Received/Date). The first output will be the precise location/coordinates of the sender's IP. For that, the tool will use the help of an API[1] that will return information about the IP address location.

As for the second output, the tool will elaborate a network path with the course of the email. It will make one table that contains information from every server/machine of the course that email took: IP address, DNS, Coordinates and Location of the machine and the ID of the server. With the information of the coordinates, the tool will define, in a map, a possible path of the course of the email by comparing the location of the different servers zones, using the Google Maps API[2].

As an extra, this tool will also look for identity information of the Sender by looking is email in social networks like google account and other social networkings websites. This will be, if possible (if the user has social networks associated with the email), the third and last output of the ELT tool.

4. Architecture

We opt to use javascript to develop the ELT tool. It's a inductive language in which we are familiar and is one of the best to conjugate with the API's and other tools we are going to use.

To obtain the coordinates of the IP address, in the first and second output, we are going to use the IP *Geolocation API*[1]. Furthermore, we are also using the API *Geolocation: Displaying User or Device Position on Maps*[2] to make the trace/path of the course of the email.

Finally, to find information on social networks we may use FB 6!! API[3] or one of the developer tools from Google Plus[4]. Also we may use the API enrichment from ClearBit[5] that can give to us useful information of the email owner. As pointed from the third section, this part is an extra, and could be made from different forms, so it may lead to future changes if necessary.

5. Testing

For testing we will use an account to receive all the emails. This emails will be send by the three elements of the group, each using a different email service, to test the majority of cases that are the most common nowadays.

We will test also sending emails from various places so the emails takes different routes and so confirm if our tool can always identified the correct route. Confirming this kinds of test will be done comparing the results of our tool to the results from others tools in our disposal[6].

Beside all this test, that are consider the normal cases, we will test some special cases. One of them is if one of the users, sender or receiver, use VPN's. And if our tool reacts how is aspected, comparing to the tool mentioned previously. This is a way of testing the situation of sending email from different places.

For the more tech savvy, it's possible that one of the users changed their IP address, and doing it so hiding their location. About our tool we will not reveal the real location of the user but we will try to identify if the IP address wasn't modified.

About the withdrawing of information of the user from the email address, will be tested in controlled environments where we know both users information and we see if our tool obtains the correct information.

[1] http://ip-api.com/json/

[2] https://developers.google.com/maps/documentation/javascript/tutorials/geolocation?hl=en

[3] https://developers.facebook.com/

[4] https://developers.google.com/+/web/api/javascript

[5] https://clearbit.com/docs#enrichment-api-person-api-email-lookup

[6] http://www.cyberforensics.in/OnlineEmailTracer/index.aspx or http://whatismyipaddress.com/trace-email