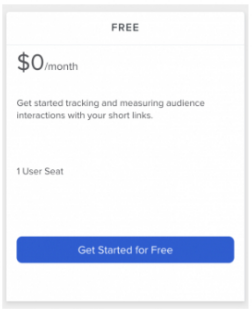
URL-Shortening Services

A tactic for disguising malicious URLs, and to prevent some aspects of automated security analysis, is the use of URL shortening services such as Bitly and Short URL. These services work by keeping a record of full URLs and generating short versions that simply redirect to the full URL. Below we will show you how we can hide the full URL using these services, and also how we can retrieve the full URL without visiting it directly.

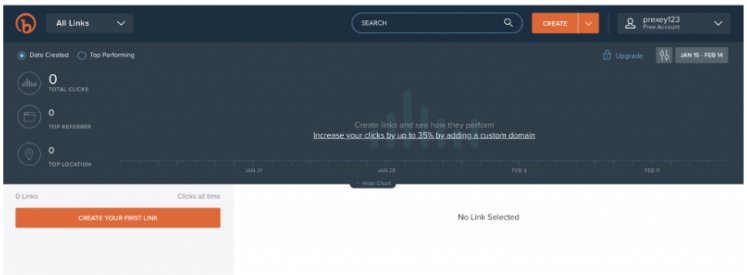
USING URL SHORTENERS

For this example, we're going to look at Bitly, which is a very popular choice for legitimate and malicious activities. You can either follow along or just watch what we do during this example.

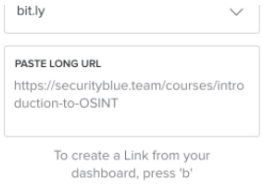
Visit https://bitly.com and make an account, selecting the free tier.



Once you're all registered and the setup is complete, you'll be presented with the Bitly dashboard, where you can create shortened URLs and monitor their activity. To create our link, click the orange "CREATE" button in the top right.

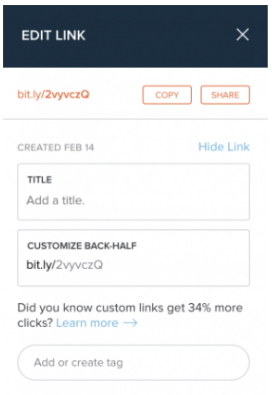


For this example, we'll be using the following destination URL: *https://securityblue.team/courses/introduction-to-OSINT*. So we enter that into the "PASTE LONG URL" box and click "CREATE" at the bottom.

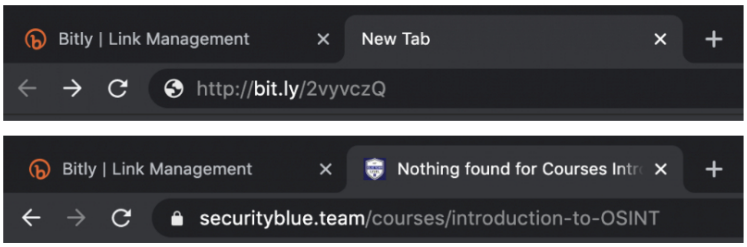


We can see at the top that we now have our own bit.ly link, which we can copy and use straight away! Below that we are given two options that we can change, the **TITLE**, and **CUSTOMIZE BACK-HALF**. The title simply changes the name of the link within your Bitly dashboard, and the below section allows you to change what comes after the "bit.ly/" part of the URL. An example of editing this would be:

- **No custom back-half:** bit.ly/2vyvczQ
- **Custom back-half:** bit.ly/ThisIsACustomBackHalf



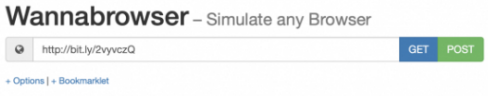
If we try to visit our default bit.ly link, it redirects us to the full URL we set when creating it. Whilst nothing is actually on this exact page we have set, if we were a phisher we would set the destination URL to be our malicious site.



ANALYZING SHORTENED URLS

Whilst there is a future section of the course that will contain detailed information on analyzing URLs, we will briefly cover how to find out where shortened URLs go, without clicking on them, as this could potentially lead us to a malicious webpage.

One good option is to use the online service WannaBrowser, which lets you simulate any browser (kind of like using a virtual machine, but just for the browser). Visit https://wannabrowser.net and paste the shortened URL before clicking on "GET".



In the below screenshot we have highlighted some important information that WannaBrowser has retrieved:

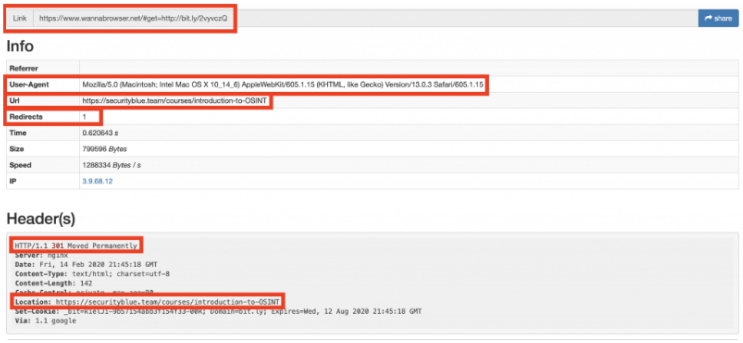
1. The first red box shows the link that WannaBrowser is using for this search. at the end it says

Exam Preparation
Using RDP and SSH
How to Start Your Exam

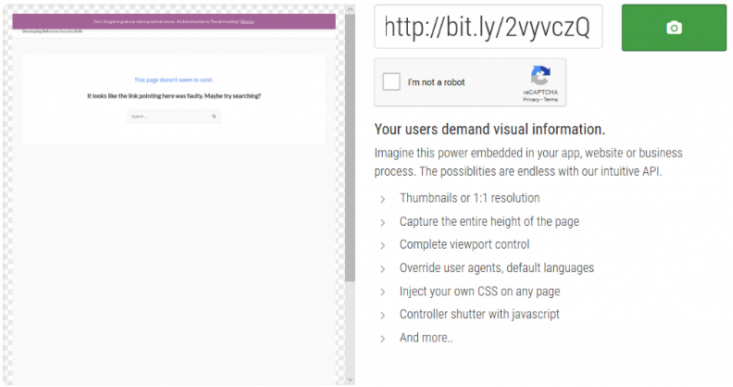
"get=http://bit.ly/2vyvczQ", which means the browser is sending a GET request to download the webpage.

2. The second box is the User-Agent string, which is the type of browser that is making the request. In this example we see "Safari" at the end, telling us the simulated browser is Apple's Safari.
3. Below that we have the final URL that was resolved, which is the destination URL we set when creating the bit.ly link.
4. Redirects list the total number of redirects before reaching a destination URL, in our case this is 1, because the bit.ly link redirected to our final URL, meaning there was 1 redirect.
5. Under the Header(s) heading, we can see that WannaBrowser encountered a 301 response code "Moved Permanently". The HTTP status code 301 is used for permanent URL redirection, which is exactly what Bitly does. With 301 redirects we should see the destination URL in the "Location" field.
6. As expected, the "Location" field shows us the URL the redirection points to.

You can read more about HTTP status codes (such as 301 Moved Permanently) at this link, created by Mozilla.



We can use a URL visualization tool URL2PNG to search for our short Bitly address. When we attempt to view the link, we can see that it is actually showing us the error page on the Security Blue Team site!



Previous Topic
Back to Lesson
Next Topic