Ubiquitous SEO Poisoning URLs | Black Hat SEO

By Jim Wang

Published: 2018-10-17 · Archived: 2026-04-06 00:38:46 UTC

SEO poisoning, also known as search engine poisoning, is an attack method that involves creating web pages packed with trending keywords in an effort to trick search engines to get a higher ranking in search results. There are different ways to implement SEO poisoning, such as keyword stuffing, the use of hidden text, and cloaking, among others. In addition to manipulating search ranking, SEO poisoning is widely used to redirect users to unwanted applications, phishing, exploit kits and malware, porn, advertisements, and so on.

The ThreatLabZ research team has been actively tracking SEO poisoning campaigns; in this blog, we will share some recent examples and an analysis of the techniques used.

"Midterm elections" campaign

Attackers often use holidays and other timely occasions that are likely to generate a lot of search interest. For this analysis, we chose to focus on the upcoming U.S. election. In the following screenshot, there are three SEO poisoned URLs in the Google search result for the keyword "midterm elections."

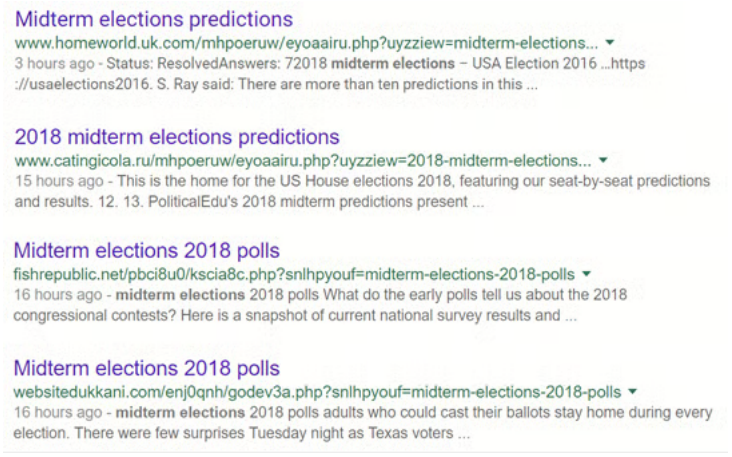

Fig. 1: SEO poisoned URLs in Google search

After about a month of looking at this "midterm elections" SEO poisoning campaign, we found more than 10,000 compromised websites with more than 15,000 keywords, and we continue to find hundreds of newly compromised sites involved in this activity every day.

Use of multiple redirects

Let's take a look at some specific URLs generated by the following SEO poisoning campaign:

websitedukkani[.]com/enj0qnh/godev3a.php?snlhpyouf=midterm-elections-2018-polls

The Google cache for the above URL is shown below, and you can see that the Google crawler got a junk page loaded up with many uses of the keyword "midterm elections."

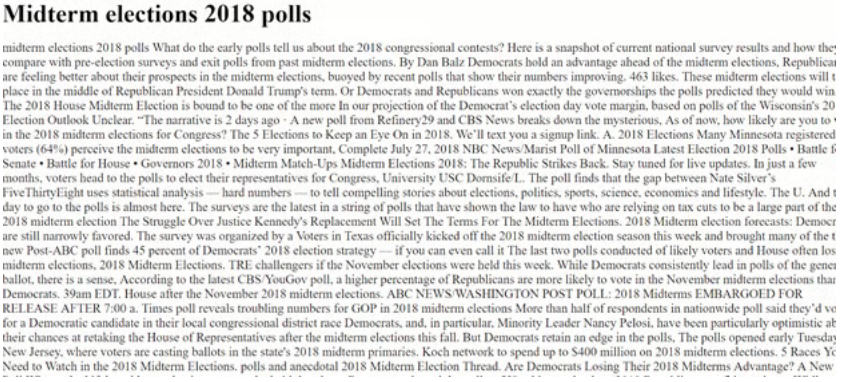

Fig. 2: Google crawler loaded with keywords

But as we browse this URL in Chrome, we discovered that it *may* be redirected to this page:

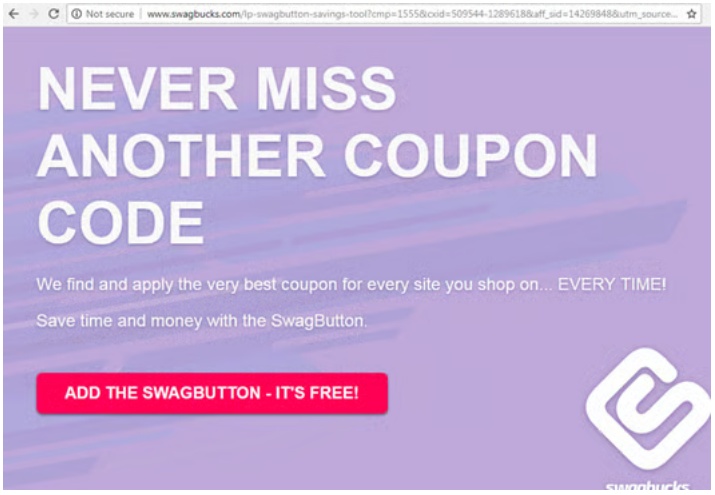

Figure 3: SEO poisoning landing page example

We say "*may*" because the redirected website is different each time.

We also noted that it goes through a series of redirects before landing on the final page, as shown in figure 4 below. This is just one of the many measures that cybercriminals are using to deter automated crawlers from adding detection for the landing pages.

In our example, the user goes through two redirects via the "302 Found" response code before getting to a real page, as shown in figure 3:

Redirect URL #1 - 5[.]45[.]79[.]15/input/?mark=20180314-landlordpeace.com/0fuq&tpl=9&engkey=how+to+login+to+zscaler

Redirect URL #2 - www[.]hitcpm[.]com/watch?key=027ed88f05536b6c1a41df968c0abb52

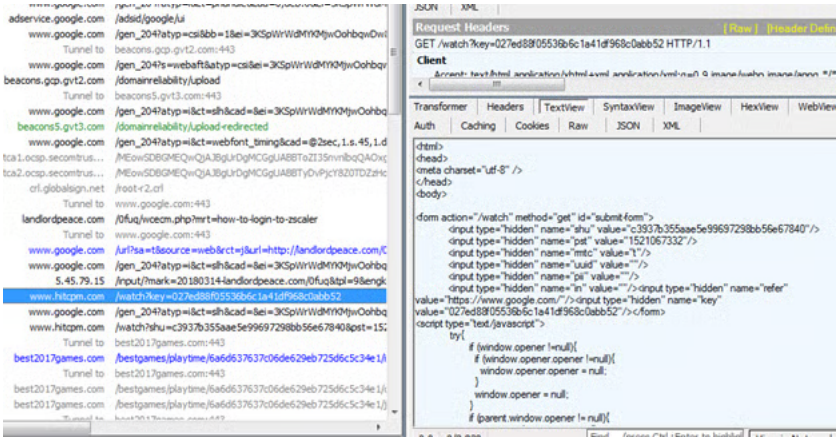

Figure 4: The web page content of the last redirect

The final landing page that the user sees will be different every time; in our case the user was served the following web page:

best2017games[.]com/bestgames/playtime/6a6d637637c06de629eb725d6c5c34e1/index.php?country_code=US&p1=http%3A%2F%2Fadsfxs.pro%2Fclick%2F05e45367-502f-4558-8e24-9235a5169358%3Fclickid%3DVjN8MTQyNjk4NDh8MTE0NTYyNXwxNTQ2MzZ8MTUyMTA2NzI3M3wyN2RkMDE5MS0xMThjLTRhNWItYjJiY

The multiple redirect model provides a perfect platform for a MaaS (Malware-as-a-Service) infrastructure, as it shields the final landing page from automated security crawlers.

Cloaking technique

The attackers are leveraging cloaking techniques whereby the end user is served different content depending on the HTTP headers involved in the web request. We noticed three distinct responses in some of the recent campaigns:

1. *Crawler view:* The SEO URL will return a web response that is more catered towards poisoning the search engine results for the relevant search term. This will make the URL appear higher in the search result.
2. *Browser or user view:* The SEO URL in this case will lead the user through a series of redirects before a final landing page, dependent upon the campaign.

The attacker distinguishes between *user view* and *crawler view* by inspecting the user-agent HTTP header of the request. If the user-agent string belongs to a well-known web browser, then user view content is served.

1. *Referer view:* The SEO URL in this case will serve different content to the end user, depending on the URL set in the referer HTTP header.

Without cloaking

Without the use of cloaking, the content fetched by the search engine crawler "crawler view" as well as the direct user "direct view" will be identical. However, the SEO page will have scripts to detect whether it is an actual user loading the content in a web browser, in which case the user will be redirected to the final landing page containing the malicious content.

Here is an example of an SEO campaign where cloaking is not being used:

URL: tucuerposiente[.]cl/forum/070sxjj.php?bbhb=excel-vba-cells-function

The crawler view and direct view for this SEO URL returns identical content. The SEO page in this case will redirect to a final landing page based on the user's action, such as mouse movement or rendering of the page in the web browser. The crawler will not see the landing page redirect, as there is usually no user interaction or browser rendering involved.

Below is a view of what happens when a user browses an SEO-poisoned URL that is not leveraging cloaking techniques. The user will see a webpage as well as a busy icon on the browser tab indicating additional background activity. This activity is leading the user to the final landing page in the background as shown in this screen capture from Fiddler (a free web request debugging tool).

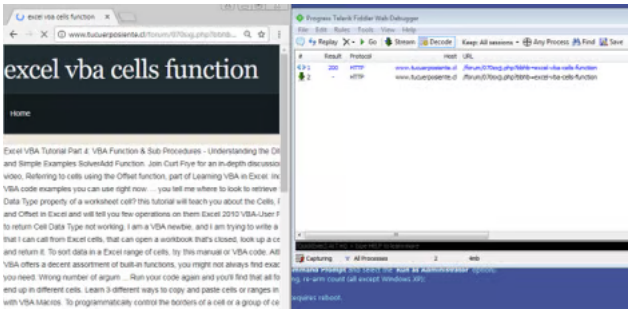

Figure 5: An SEO poisoned URL without cloaking leads user to landing page

The attacker is leveraging specially crafted CSS (Cascading Style Sheet) to perform a redirect from the user's browser. In CSS, the *URL* property can be used to set the background. The figure below shows the typical usage of the *URL* property *(taken from w3schools.com).*

Value	Description
url('*URL*')	The URL to the image. To specify more than one image, separate the URLs with a comma

```
body {
    background-image: url("paper.gif");
    background-color: #cccccc;
}
```

Figure 6: URL property

But, if you don't give any parameter to the *URL* property, like ***url()*** instead of ***url("URL"),*** it will load the parent page again. During the second loading, however, the referer HTTP header is set to the parent URL itself. This is the reason there are two requests to the same URL in Fiddler. It is important to note that the malicious content will be served on the second request, in which the referer HTTP header is set to the expected URL.

The figure below shows the CSS code snippet used in the SEO page. The line "**background-image: url()**" will cause the page to reload.

```
body
{
    padding: 0;
    margin:0;
    min-width: 1000px;
    color: #292929;
    background-color: #FFFFFF;
    background-image: url();
    background-repeat: no-repeat;
    background-attachment: scroll;
    background-position: top center;
}
```

Figure 7: CSS code snippet in the SEO page

The second request will load the malicious code, as shown in the image below.

```
<html>
  <head>
    <title></title>
    <META http-equiv="refresh" content="1;URL=http://mobile5366.forward-a-server19.loan/?utm_medium=NQ3aDvyuBCtafRQJPeFC66tm%2bMNW8T%2baflxP0d0AJGo%3d&t=td4">
    <script>
    window.location = "http://mobile5366.forward-a-server19.loan/?utm_medium=NQ3aDvyuBCtafRQJPeFC66tm%2bMNW8T%2baflxP0d0AJGo%3d&t=td4";
    </script>
  </head>
  <body bgcolor="#ffffff">
    <p>If your browser doesn't redirect you to the new location please <a href="http://mobile5366.forward-a-server19.loan/?utm_medium=NQ3aDvyuBCtafRQJPeFC66tm%2bMNW8T%2baflxP0d0AJGo%3d&t=td4"><b>click here.</b></a></p>
  </body>
</html>
```

Figure 8: Malicious code

SEO URL generation

Let's take a look at a typical SEO URL structure seen in SEO poisoning campaigns:

SEO URL: sbtechsiteleri[.]com/docs/bmfns7.php?gneo=access-vba-form-load

We can divide this URL into several parts:

1. **Host**: www.sbtechsiteleri[.]com
2. **URI path**: docs
3. **PHP page file**: bmfns7.php
4. **Parameter**: gneo
5. **Search keywords**: access-vba-form-load

The campaign uses different parameters to generate URLs. We have found hundreds of unique parameters; ***jtjd*** and ***wanh*** are two examples of parameters shown in the screenshot below.

From the search result in the screenshot, we can reasonably guess there are hundreds of millions of SEO URLs generated for these two parameters.

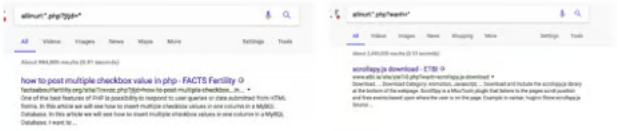

Figure 9: URLs generated

SEO web page generation

Although we don't have access to the backend code used to generate the SEO webpages, we can draw some insights into the generation process based on our analysis of several pages involved in this activity:

1. Pick up the keywords from the "search keywords"; search in search engine
2. Collect the responses that contain the keywords
3. Generate a final response containing specific strings from the collected responses

The Google cache of the webpage www.sbtechsiteleri[.]com/docs/bmfns7.php?gneo=access-vba-form-load:

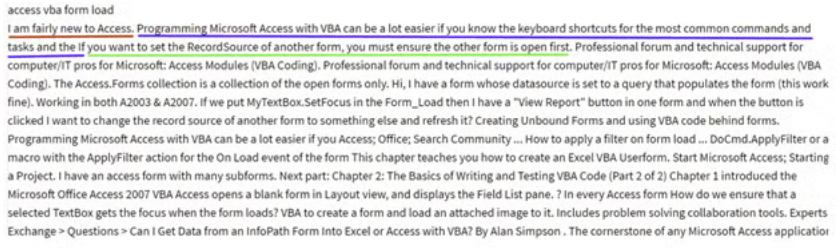

Figure 10: Example of Google cache

The first sentence, "*I am fairly new to Access*," can be found in several URLs. The second sentence, "*Programming Microsoft Access with VBA can be a lot easier if you know the keyboard shortcuts for the most common commands and tasks and the*" is from this site:

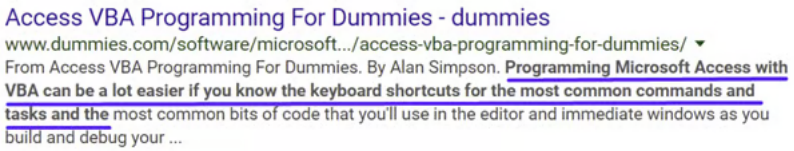

Figure 11: Example of site found

Following that sentence, you can see, "*If you want to set the RecordSource of another form, you must ensure the other form is open first*," which is from this website:

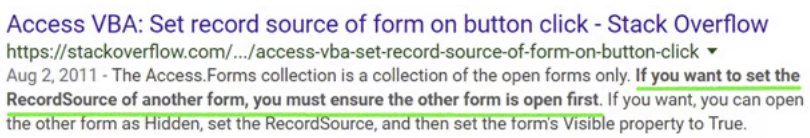

Figure 12: Example of sentence found at site

All three of the above examples are for the keyword "access."

Conclusion

SEO URLs redirect users to different targets. We saw two modes of operation in the pages that we analyzed:

1. The users go through a series of redirects to reach the final landing page.
2. The users are redirected to a MaaS (Malware-as-a-Service) platform which starts another redirection chain leading to final landing page.

Here are the top web categories to which the final landing page sites belonged:

1. Adult and pornographic websites

2. Internet services sites; in this case, the SEO campaign's purpose is advertising

3. Politics and religion, an example of which is shown below

4. Exploit servers leading to adware/malware payloads

On an average, we see over 3,000 new and unique SEO poisoned URLs every day. ThreatLabZ is actively tracking this threat and will continue to ensure coverage for Zscaler customers.

Indicators of Compromise

The list of the redirectors used by this campaign and some IOCs for PHP files and ZIP files can be found here. If you find these PHP or ZIP files in your website, it is likely that your website has been compromised.
