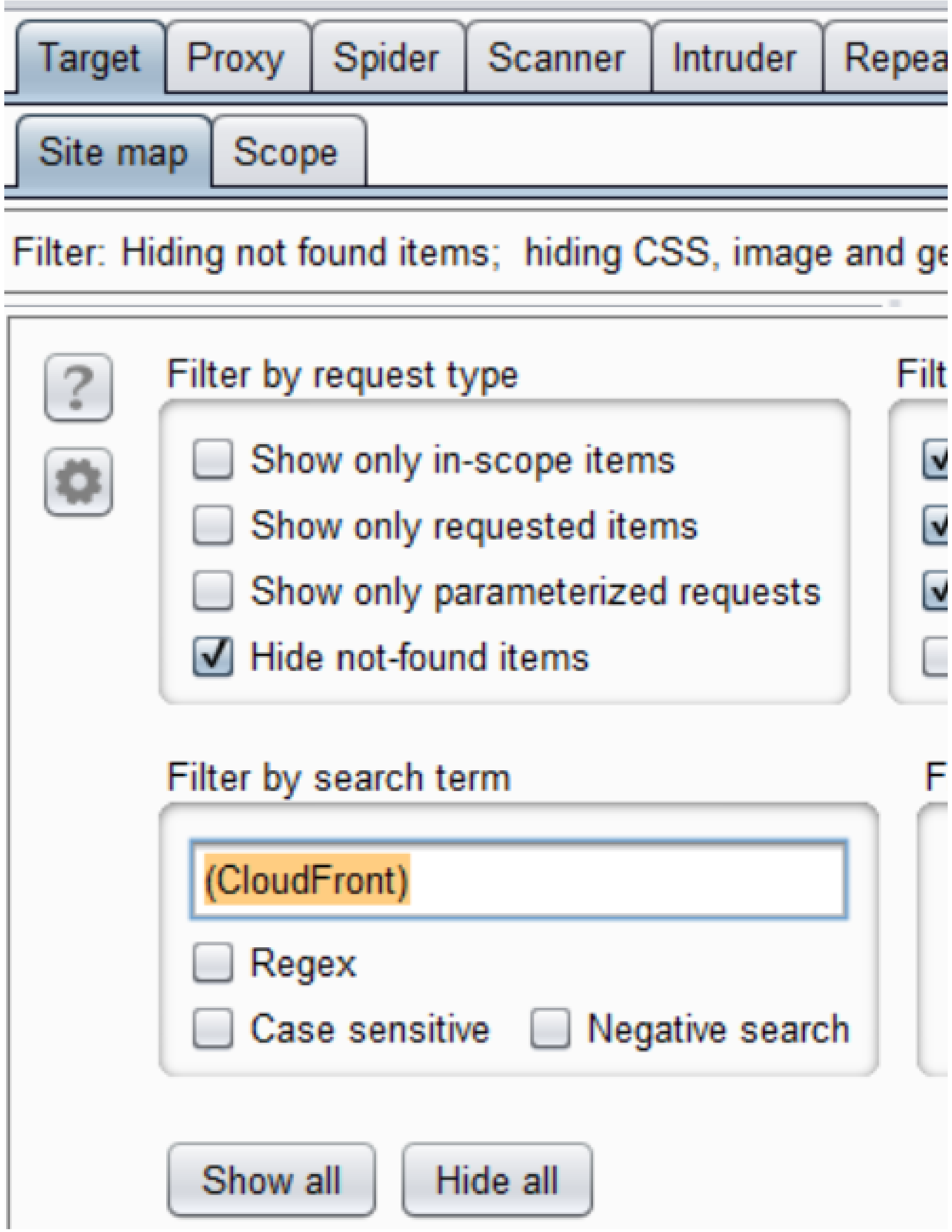
Vincent Yiu Follow
Advanced Threat Replication. Simulating real threat actors using bleeding edge techniques.
Nov 17, 2017 · 3 min read

Finding Target-relevant Domain Fronts

My last blog post on finding high-value target domains that could be used for domain fronting was quite popular—found here.

Although there are a few popular domains that everyone uses, I've also published quite a large list on GitHub for public consumption and defenders to watch for. This can be found here.

As time went on, I found that there was a need for target relevant domains, which may not be necessarily readily available in my previously discovered list. I came up with a quick way to find such domains with example traffic which could then be used to camouflage our traffic. Additionally, I've had a lot of people in the community contact me asking how I find the domain names. And yes, previously it was by scanning Alexa Top 1 million for CNAME records to Cloudfront.



Filter: Hiding not found items; hiding CSS, image and ge

Filter by request type

- □ Show only in-scope items
- □ Show only requested items
- □ Show only parameterized requests
- ☑ Hide not-found items

Filter by search term

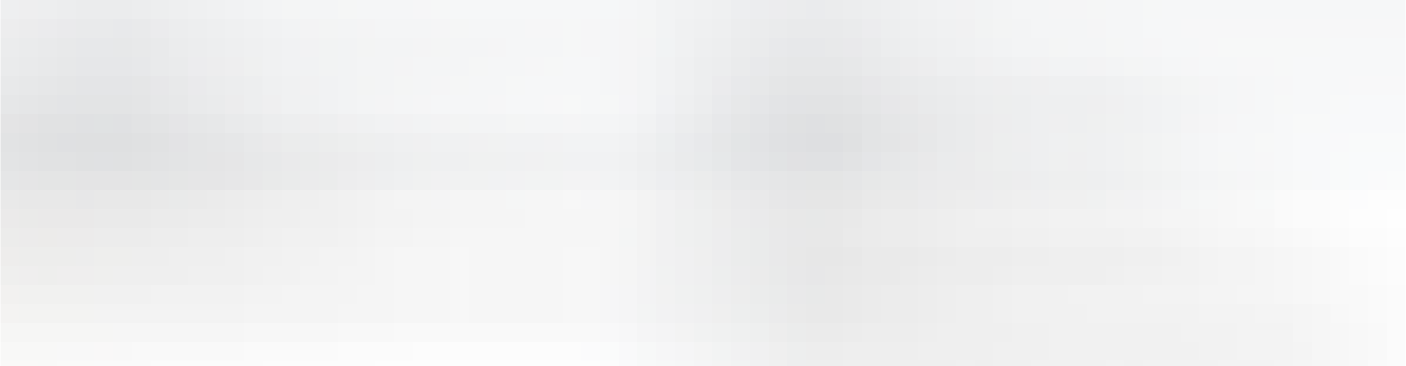
(CloudFront)

- □ Regex
- □ Case sensitive □ Negative search

PortSwigger’s Burp Suite is a popular, widely known and used tool. In this post I will make use of this tool to easily extract a list of CloudFront domains.

Configure a web browser as you normally would and begin browsing the internet. The first idea would be to browse your target organisation or affiliate’s websites— this generates a lot of traffic. Next I would go onto Google and begin searching for terms that may be related to the industry that particular target is in. In order to filter the large number of domains accessed quickly to possible domains, set a filter in the Target tab for “(CloudFront)”.

For example, if it was a company in the automotive manufacturing industry I could search for terms like “sports car”, I find links to websites such as Masersati.com which uses scripts.sophus3.com which is a CloudFront domain to serve scripts. See following.

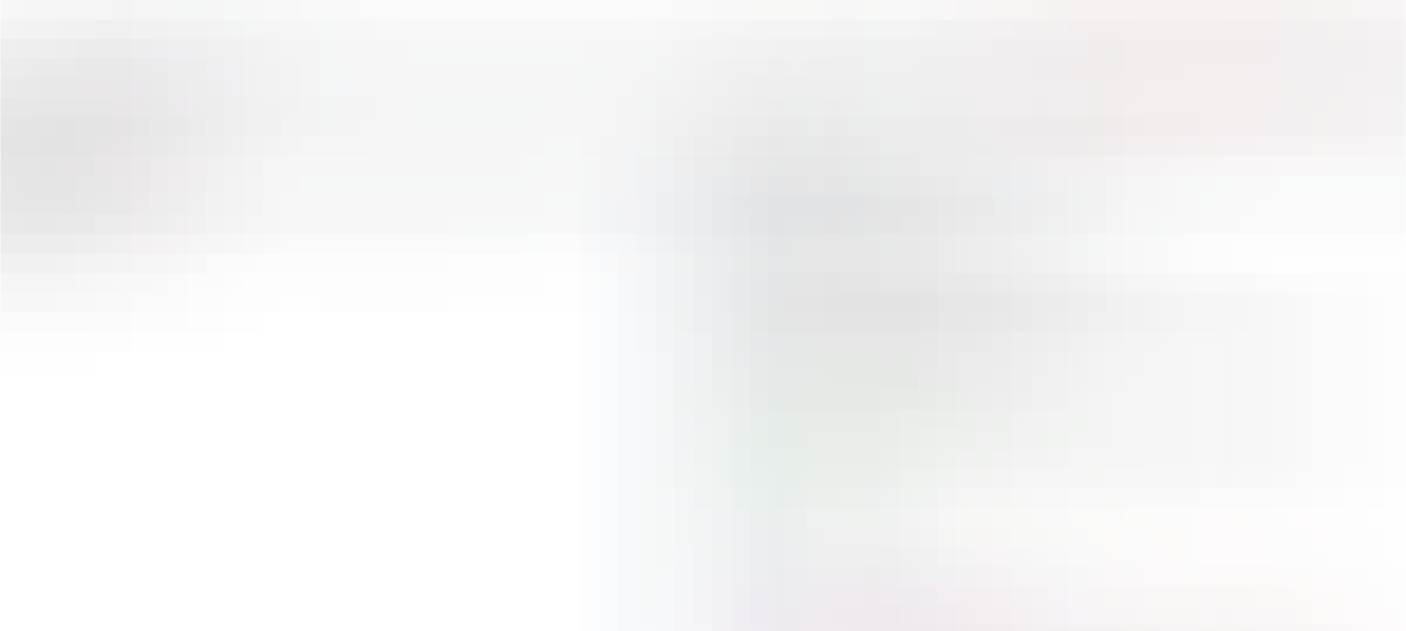


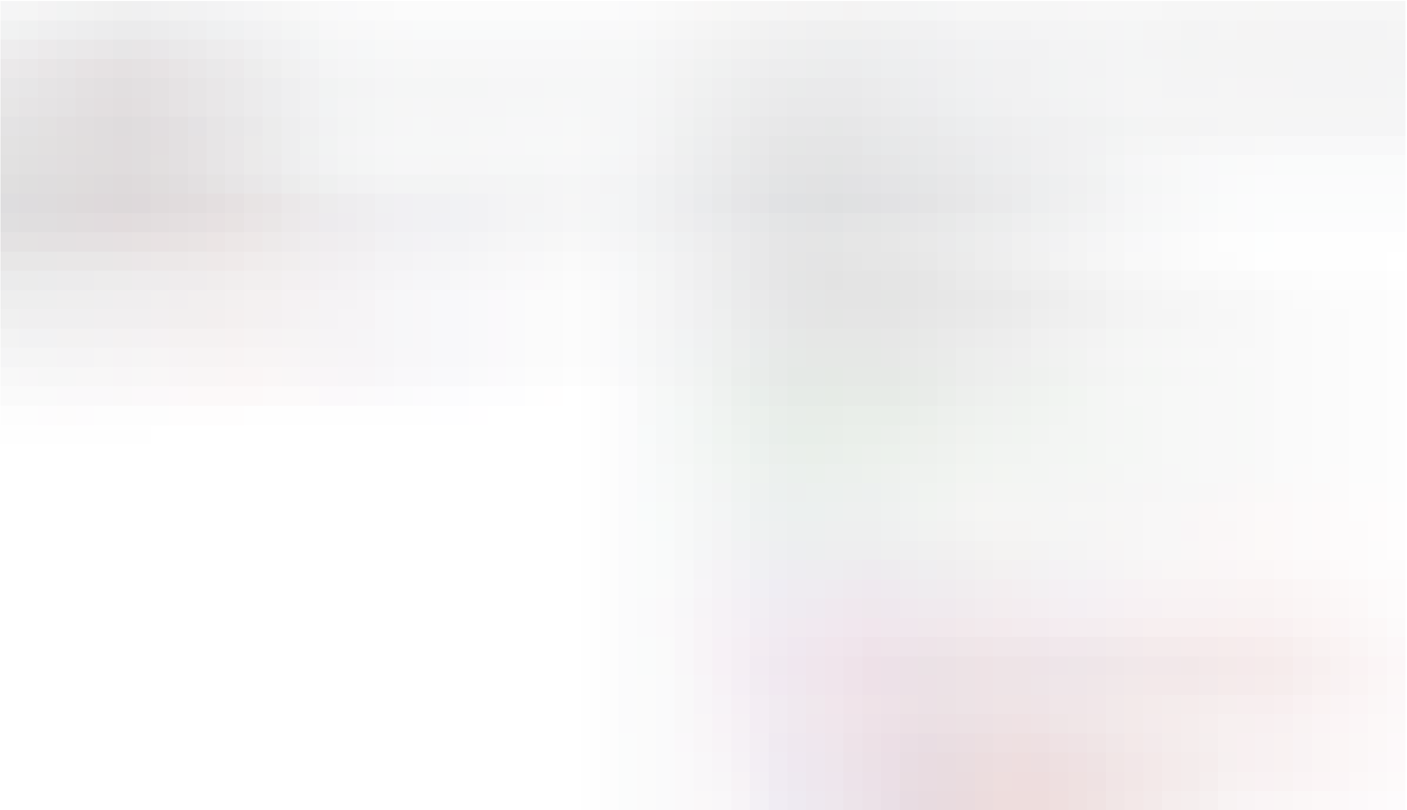
Changing up the Host to another known CloudFront domain such as beacon.uber.com, we retrieve a different set of content and know that the domain front was successful. Following screenshot shows the content retrieval through the scripts.sophus3.com domain.

At this point, we have found a domain, related to cars, used by Maserati in it's content delivery. The domain is on CloudFront, and we can use this to craft traffic for command and control channels based around this data.

Reviewing the original data, we can see that it fetches a script, c2 content can be sent through as a GET parameter or Referer and responses can easily be modified within the script body as a comment.

More examples such as domains that would blend in a lot better in a large organisation are displayed below:





SEO

Like what you read? Give Vincent Yiu a round of applause.

From a quick cheer to a standing ovation, clap to show how much you enjoyed this story.

23

Vincent Yiu

Advanced Threat Replication. Simulating real threat actors using bleeding edge techniques.

Follow

Also tagged SEO ★

9 Keys To Getting Your E-commerce Store Ranked On…

Richard K. Yu
5 min read

780

Top on Medium

An Ambitious Person's Brutally Honest Take On Work-Life Balance

Michael Simmons
15 min read

7.6K

Top on Medium

12 Common Ways You're Sabotaging Your Mood And Your…

John Gorman
10 min read

13K

Responses

Write a response…