



Vincent Yiu [Follow](#)

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

Mar 11 · 5 min read

Alibaba CDN Domain Fronting

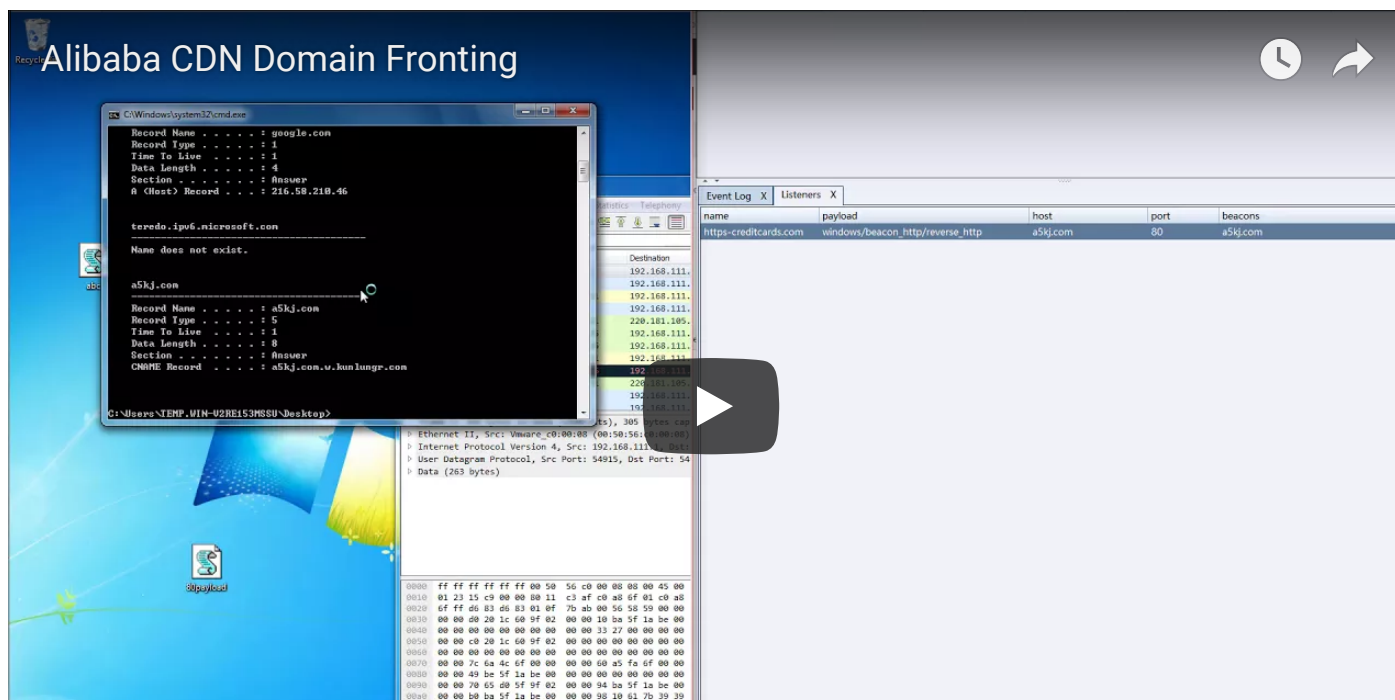
Author: [@vysecurity](#)

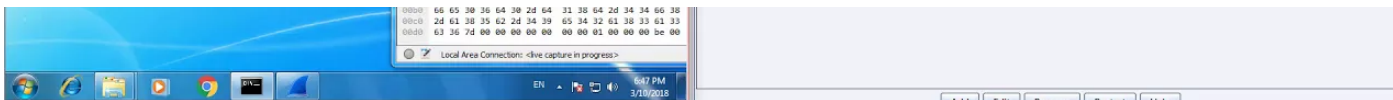
It's been a while since Domain Fronting has been out, we've been discussing the idea of using various CDNs such as Azure, Google App Engine, and Amazon CloudFront for domain fronting. That's all become a reality now, as attackers move to better command and control obfuscation and masquerading as legitimate traffic. I published a post last year on Domain Fronting and using high reputation domains to hide your traffic. Since then, there's been many new posts on using GAE, and Azure. From there, I even published a large list of potential, as well as validated domains that can be used for fronting. I even went through all the CloudFront domains to reduce it to a list of about 55,000 domains that would serve legitimate SSL certificates. With that not being enough, I published a further post on finding targeted CloudFront instances that may be relevant to your target.

It's been a great year for domain fronting. For some red team veterans, there's been a concern that the proxy SSL interception and host header re-write can break the C2 channel. That's fine, we have other techniques for that coming out later on in the year.

TDLR: Going to show you how to Front through an Asian cloud provider network and show you a few new advantages.

If you prefer videos:





Alibaba Cloud and Content Delivery Network

In this post we're going to go into using Alibaba's CDN for Domain Fronting. You might have seen Alibaba's advertisements at PyeongChang 2018. Alibaba's cloud is more predominantly used in Asia, or more specifically mainland China. Therefore, not as many targets or relevant domains will be found for Asia using CloudFront for example, they're more likely to be using Alibaba's CDN.

This post will go into how to bypass the manual verification checks. Yes, unlike Amazon, GAE, or Azure, there is actually human performed manual verification checks to ensure that the origin you are delivering content for is legitimate and follows the terms of service.

This post also indicates how to better hide your Host header in your traffic using Alibaba's cloud. Yes, unlike CloudFront, the `xxxxxxxxxxxxx.cloudfront.com` is highly signaturable and identifiable by blue team. Similar `xxxxxxxxxx.appspot.com` for GAE.

Setting up a CDN instance in Alibaba Cloud

Set up the CDN instance with the following settings. We'll go into why we need certain settings in the following sections of the post. For now, ensure that "Full-site" is checked as there's issues domain fronting for a C2 channel with any of the other options. Set to use Port 443 if you want SSL, of Port 80 if you want HTTP. Whatever you set here is important as you can't use both in Alibaba CDN. For the purposes for most of our readers, I'd suggest using Overseas. If you want a CDN instance in Mainland China you have to go through registration with the government and all that good regulation jazz.



Setting up a CDN instance on Alibaba Cloud

Manual verification check: Technique 1

This is probably the more tedious method. Host legitimate content on the origin. You can clone a website by simply using `wget -mk https://url.com` and serve that content. After the manual verification has been completed in two days, you can go ahead and change the content.

Manual verification check bypass: Technique 2

Use Alibaba's own cloud resources such as Elastic Compute Service (their version of EC2), to get an Alibaba IP address. If you set the CDN origin to an

Alibaba IP address, the verification check is instant and you don't have to wait!

Great, we can just create a 500MB RAM redirector to grab an Alibaba IP address for \$5 a month. Then create the CDN instance as shown below:



With this, it bypasses the manual verification checks and enables the resource instantly.

Host header magic, less signatures by the proxy

Another thing that I noticed was that there's no verification checks in the automated mode as long as you're using Alibaba's IP address for the origin. Therefore it was possible for me to use a domain name such as `headless.microsoft.com` for my Host header. I knew that this was possible due to my understanding of CDN and how it all works. It just so happens that this method of provisioning instances on Alibaba Cloud is flawed.



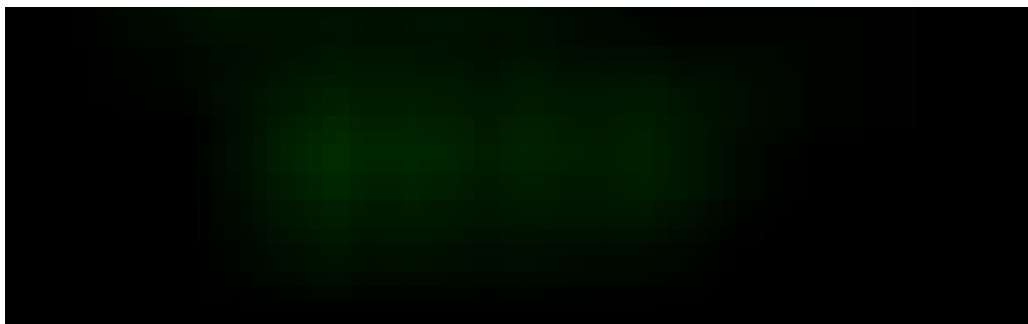


Creating automatically validated CDN instances with arbitrary Domain Names

Setting up your Malleable profile and C2

Go ahead and hook up the redirector to your C2 server. The malleable profile should have a host header set to the domain name that you specified as shown below:





Example of setting the host header

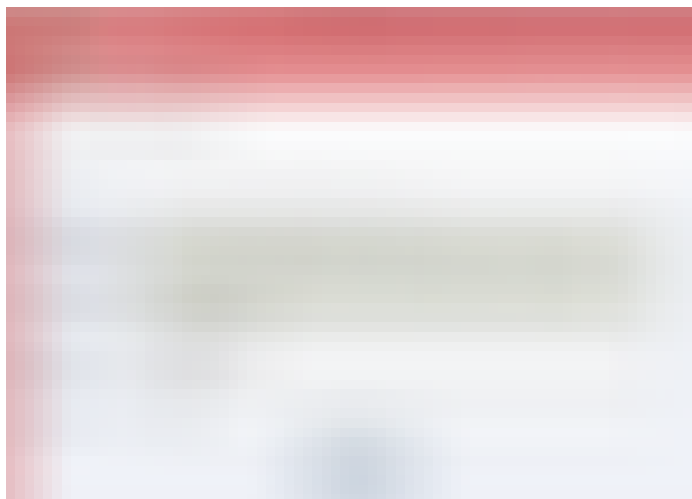
In the listener, set up the domain name to use a domain that you know is Frontable. I've found a5kj.com which shows the following result in a CNAME lookup:

```
Non-authoritative answer:  
Name:      a5kj.com.w.kunlungr.com  
Address:  42.81.4.44  
Aliases:  a5kj.com
```

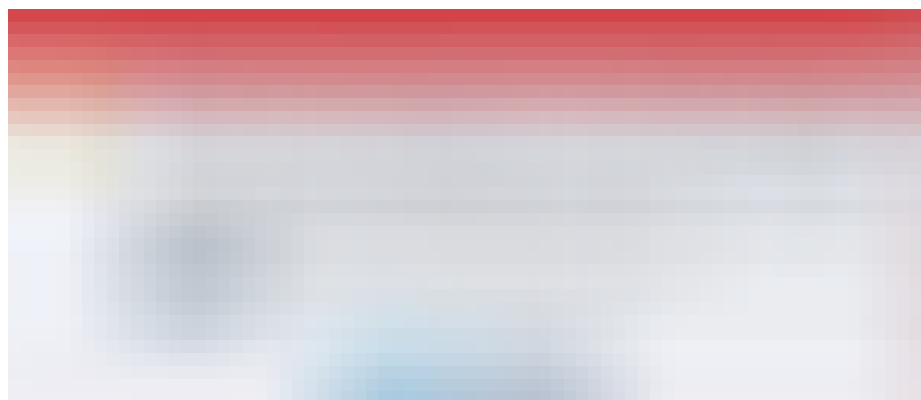
Frontable Domain

We can see that it's a frontable domain by the iconic "kunlungr.com" which belongs to Alibaba's CDN.

To set up the listener, we can apply the following settings:



Setting up a fronting listener for a5kj.com



Once this is set up, roll your payloads as usual. And you will find that you can front through Alibaba's cloud. If you inspect the host header, you will see that it says the arbitrary domain name that you specified. This means that you're

no longer stuck with host headers for “cloudfront.com” or “appspot.com” for example.

Conclusions

I brought up the idea of using Alibaba’s cloud for Domain Fronting since the whole technique started to get weaponised for offensive operation purposes. I’ve not yet seen anyone publish content on how to use Alibaba’s cloud effectively for Fronting. This is the first post, and I hope that it can inspire more security researchers to break out of the shell in one ecosystem to try and utilise weaponisable resources world-wide. You will see what I mean by this with my later posts.

[Ssl](#)[Red Team](#)[Red](#)[Hacking](#)[Domain Fronting](#)

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.

50



Vincent Yiu

Follow



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

☐ Show only requested items

☐ Show only parameterized requests

☒ Hide not-found items

More from Vincent Yiu

Finding Target-relevant Domain Fronts



Vincent Yiu
3 min read

23 |



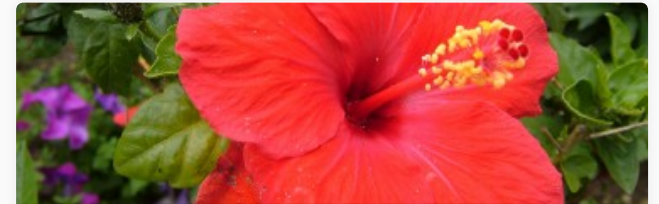
Related reads

Safe Red Team Infrastructure



Tim MalcomVetter
5 min read

134 |



Also tagged Reds

Just Saying Hi ...



San Cassimally
1 min read

190 |

Responses

Write a response...



[lichin](#)

Apr 13

Hi Vincent,

Thanks for sharing. We were trying to use the full-site CDN service here on AliCloud international site. But it doesn't work here. Just wondering was this demo on Alicloud China site or International site?

Many thanks,

Lizzie

1 response 



[Vincent Yiu](#)

Apr 13

Hi Lizzie,

I used the international site as I am based in the UK. Though to register for some services you may need to validate your ID, which you may or may not want to do.

Hope it helps.

Vincent

1 response 




lichin

Apr 16 · 1 min read

Thanks Vincent.

We are based in the UK, too. And we have passed the real-name validation, too. But we see: “Currently you can not add Full-site domain now. It’ll be reopened soon. We apologize for any inconvenience caused during this time.” when we select “Full-Site” option... And also we filed a ticket to the support, and...

[Read more...](#)

1 response 



Vincent Yiu

Apr 16 · 1 min read

Lizzie,

I was using the Alibaba 2 month free trial with real-name verification and I believe that I did in-fact have full-site acceleration, linked to a ECS instance.

Perhaps they took it down after this post, for a bit of revamping?

Read more...

1 response 

Show all responses