供应链投毒后，我们的选择还剩下哪些？

TheMoon (https://www.54yt.net/author/1/) 2024 年 07 月 11 日 25 次浏览 1 条评论 7135 字数
随笔 (https://www.54yt.net/7/)

(https://cdn.54yt.net/usr/uploads/2024/07/3477431422.webp)

前言

从早前的LNMP、OneinStack到XZ Utils，再到现在的Staticfile、BootCDN；供应链攻击总是让人猝不及防。纵观这些被攻击的项目，往往都是无处不在，经常被大家所使用，但是却并没有给提供者带来什么收入。
在突然有一天，提供者感到疲惫不堪，却又迫于用户们的压力无法关停服务的情况下，突然有新的组织/个人来帮助一起进行开发或提供服务，甚至是直接的现金收购/服务赞助；在这种情况下，接受帮助自然是首选的方案。
我认为建立有效的捐助途径不失为缓解这一问题的良方，正如AlmaLinux、RockyLinux或是cdnjs、jsdelivr一样，这些服务背后都有着可靠的企业长期提供捐助承诺，也帮助项目不断成长和有效地提供服务。

序幕

和WDCP、LNMP、OneinStack一样，这次的Staticfile、BootCDN、Polyfill事件也是背后指向同一个组织[[1]]。
更进一步的研究表明这些组织似乎会恶意攻击其他提供类似服务的供应商，同时采取接触洽谈来并入攻击目标。
在这种做法下，曾经由七牛云提供服务的Staticfile.org (http://Staticfile.org)被易手，而原先由个人提供服务、由又拍云提供接入服务的BootCSS (https://www.bootcss.com/)也同样被易手。

但是这些背后的交易在事件发生前却没有人进行公开，也许是原来的提供者厌倦了日复一日付出却看不到回报的生活，也许是这些组织瞒天过海许下了虚假的承诺，让原本积累了大量用户的基础服务成为了这些组织用来攻击用户们的利刃。

探究

大多数关于这次攻击的报道集中于一个星期之前，然而事件的开始却远早于这个时间。一年以前，V2EX社区就有用户发文表示BootCSS的静态资源被投毒[2]。
通过查阅记录可以发现，BootCSS.com由王赛于2012年底批量注册，建站初期主要提供的是BootStrap介绍和交流[3,4,5]。于此同时进行批量注册的还有golaravel.com等一系列技术栈的中文网，猜测是想使用站群方式来进行项目文档的本地化，同时积累受众用户。

京ICP备11008151号-21	-	gridsome.cn
京ICP备11008151号-22	-	miragejs.cn
京ICP备11008151号-23	-	romejs.cn
京ICP备11008151号-26	-	yarnpkg.com.cn
京ICP备11008151号-27	-	preactjs.com.cn
京ICP备11008151号-30	-	yarnpkg.cn
京ICP备11008151号-31	-	reactnativejs.cn
京ICP备11008151号-34	-	strapi.cn
京ICP备11008151号-36	-	nextra.cn
京ICP备11008151号-4	-	golaravel.com

(https://cdn.54yt.net/usr/uploads/2024/07/1112609884.webp)
在2013年十一月初，BootStrap中文网上线了OpenCDN加速服务，由又拍云赞助，提供cdnjs的国内镜像[6]。

(https://cdn.54yt.net/usr/uploads/2024/07/1920556555.webp)

(https://cdn.54yt.net/usr/uploads/2024/07/1160348877.webp)
也许是由于用户的增长又拍云难以承担高额的成本，又或者是又拍觉得收益无法Cover成本，这段关系一直持续到了2017年年底[7]。自此之后的一段时间，提供服务的CDN便开始快速变更，从白山云到京东云，最终到了10月份由于账单压力或是其他原因出现了大面积的服务中断[8]。

V2EX › 程序员

BootCDN 应该是停止服务了

2 · SukkaW · SukkaW · 2018-10-01 11:34:06 +08:00 · 17630 次点击

这是一个创建于 2109 天前的主题，其中的信息可能已经有所发展或是发生改变。

1. www.bootcdn.cn 上现在获取的文件链接全部是 cdnjs.cloudflare.com 的
2. BootStrap 中文网 v3 文档 中的「开始使用」里的 CDN 范例已经更改为 cdn.jsdelivr.net
3. www.bootcdn.cn 自己的静态文件都在用 cdn.jsdelivr.net 加载

BootCDN 这一波应该是有计划的停止服务的。

BootCDN

中国最著名的公共 CDN 服务之一

(2013 - 2018.10)

第 1 条附言 · 2018-10-01 12:10:21 +08:00

得到 BootCDN 站长消息，他已经在做 301 了。 推荐替代的公共 CDN 服务商

- https://www.jsdelivr.com - Prospect One
- https://css.loli.net - @Showfom
- https://cdn.baomitu.com - 360 奇舞团

另附一骗我自己的博客文章 以全新的视角来评测公共 CDN

(https://cdn.54yt.net/usr/uploads/2024/07/1410603159.webp)
在恢复后，原先的服务开始由猫云提供，自此开始BootCDN的服务出现了一些不连续的中断事件[9]。

(https://cdn.54yt.net/usr/uploads/2024/07/38043456.webp)
2019年3月、10月、2020年1月陆续出现小规模的中断，尽管如此，但是在接下来的几年时间中，猫云一直为BootCDN提供加速服务，只是加速域名从 `cdn.bootcss.com` 更换为了 `cdn.bootcdn.net`；而于此同时百度静态资源公共库则彻底停止了服务。

V2EX › 程序员

百度静态资源公共库怎么突然关闭了，大厂也不咋靠谱

zw1234 · 2018-12-26 15:08:37 +08:00 · 11726 次点击

这是一个创建于 2023 天前的主题，其中的信息可能已经有所发展或是发生改变。

简介

百度静态资源公共库 是稳定，快速，全面，开源的国内 CDN 加速服务。

稳定，快速

由百度遍布全国各地 100+个 CDN 节点提供加速服务。 让开源库享受与百度首页静态资源同等待遇。 全面，开源 收录超过 180+开源库，并且这个数字正在不断增加。 百度静态资源公共库服务不仅在Github 开源库上接受任何人的提交请求，同时实时同步国外如 CDNJS 上优秀的开源库。

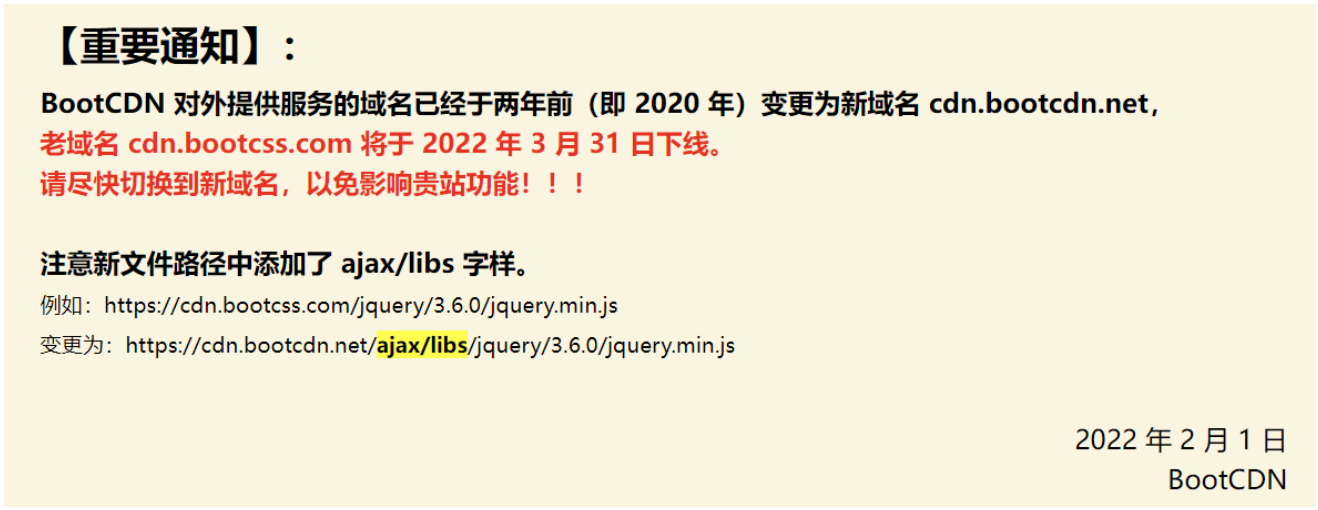
地址： http://cdn.code.baidu.com/

gayhub： https://github.com/Clouda-team/baiducdnstatic

一直还能用，现在网站打不开了，不过引入的静态资源还在 https://libs.baidu.com/jquery/1.9.0/jquery.min.js

(https://cdn.54yt.net/usr/uploads/2024/07/3918692803.webp)
时间来到2022年，在1月份经历了中断后，2月份猫云或许是基于和又拍云同样的原因停止了赞助，服务商也从此开始变更为了极兔云[10]。

(https://cdn.54yt.net/usr/uploads/2024/07/1065401829.webp)
或许是由于极兔云本身是融合CDN服务，与上一家同样类型的赞助商服务相冲突的原因，BootCDN发布公告表示将下线 `cdn.bootcss.com` 域名。



(https://cdn.54yt.net/usr/uploads/2024/07/3816909016.webp)
在此期间，jsDelivr的备案被关停、解析被污染，从此基本断绝了在中国大陆的使用。

梦醒

2023年4月份，BootCDN的三个关联域名[bootcdn.net,bootcdn.cn,bootcss.com]ICP备案变更为 郑州紫田网络科技有限公司 ，同时域名注册商也从阿里云转入腾讯云，由此揭幕了噩梦的来临[11]。

ICP备案号

网站名称	-
备案域名	bootcdn.net
备案类型	企业
备案主体	郑州紫田网络科技有限公司
备案号	豫B2-20070002-15
备案时间	2023-04-25 09:34:48

(https://cdn.54yt.net/usr/uploads/2024/07/1176657452.webp)
2023年6月份，开始有用户陆续发现部分静态资源内存在投毒行为[12]。

V2EX › 分享发现

Bootcss CDN 疑似被投毒

2 amber0317 · 2023-06-20 07:37:44 +08:00 · 3646 次点击

这是一个创建于 386 天前的主题，其中的信息可能已经有所发展或是发生改变。

现象

使用手机 Chrome 访问某数码论坛时会自动跳转到奇怪的网站，而且是在帖子加载完成后才动态跳转。不稳定复现，仅在 Chrome 上偶现，Edge 无法复现，桌面浏览器无法复现。

(https://cdn.54yt.net/usr/uploads/2024/07/2720012797.webp)
即便到现在，投毒行为仍在继续，大量用户反馈存在资源被投毒[13]。

(https://cdn.54yt.net/usr/uploads/2024/07/2002450129.webp)
自此BootCDN这个拥有十多年历史的国内静态资源加速服务彻底沦为了攻击者的工具，恶意代码随意被嵌入无数正在使用的网站中。而由于BootCDN历史久远，以至于许多生产环境甚至都不知道他们曾经引入了该服务。而这样的攻击相信还会继续持续下去，直到大家渐渐意识到...又或是仍旧...

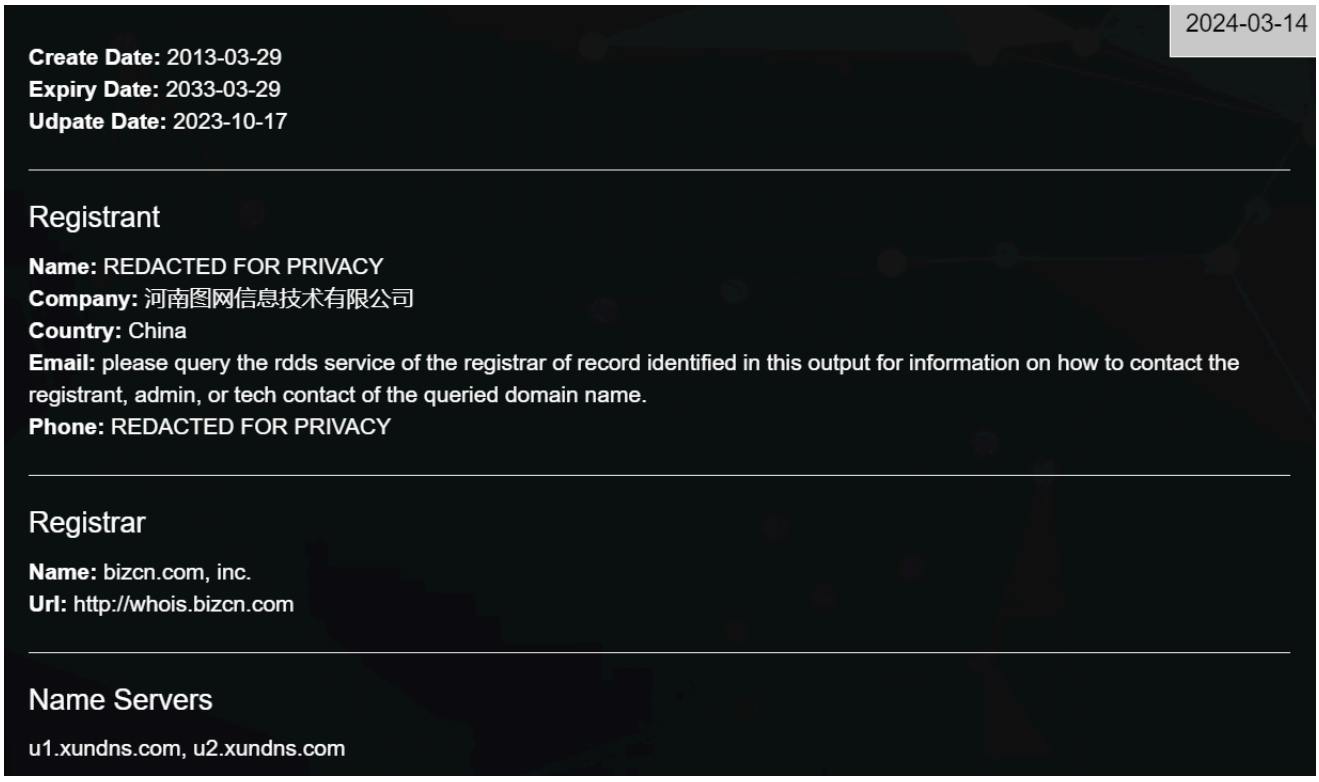
巧合

无独有偶，原本由七牛云提供服务的Staticfile CDN于2023年10月进行了备案信息变更和注册局转移[14]。

ICP备案号

网站名称	-
备案域名	staticfile.net
备案类型	企业
备案主体	河南泉磐网络科技有限公司
备案号	豫ICP备20013748号-5
备案时间	2023-10-11 13:12:11

(https://cdn.54yt.net/usr/uploads/2024/07/3469569330.webp)



(https://cdn.54yt.net/usr/uploads/2024/07/1910424045.webp)
两个关联域名 `staticfile.org` 和 `staticfile.net` 被转入 河南泉磐网络科技有限公司 。
而先前BootCDN所转入的公司名称为 郑州紫田网络科技有限公司 ， 两者同为河南省郑州市的相同类型公司。
而先前 `Ze-Zheng Wu` 所发现的几个域名由统一组织控制高度符合[15]。
通过天眼查查询可知紫田科技旗下知名的一个产品为 `51.La` 站点统计平台。

(https://cdn.54yt.net/usr/uploads/2024/07/1919039665.webp)
通过Bing搜索不难发现在2023年集中出现大量使用该统计平台遇到劫持的案例。

搜索 COPILOT 图片 视频 地图 资讯 更多 工具

约 3,040,000 个结果

主机吧
https://www.zhujib.com/famous_website…

知名网站统计工具51啦统计代码疑被非法被劫持 - 主 …

网页 2023年6月27日 · 51啦 网站劫持. 今天一大早有站长反馈，自己网站安装51啦统计代码疑似被劫持跳转到非法网站了。 目前官方已经处理： 主机吧根据自己以往经验，告诉大家，被网站被劫持后应该怎么办？ 删除掉 …

JIKE
https://jike.info/topic/21243/51la统计存在劫持-谨慎使用

51LA统计存在劫持，谨慎使用 | JIKE

网页 前一段时间官方在自己的官网承认 不过文章已经被删了 尊敬的51LA用户： 针对部分用户反馈网站统计JS异常问题，现已有基本证据证明系DNS劫持，具体原因还在进一步调查，我 …

腾讯新闻
https://new.qq.com/rain/a/20221022A006FA00

51.la宣布将停运“优站计划”活动 称存在大量违规作弊行为 - 腾讯网

网页 2022年10月22日 · 站长之家（ChinaZ.com）10月21日 消息: 近日，免费流量统计技术服务提供商51.la宣布，因发现活动存在恶意传播和大量违规作弊行为，决定对“优站计划”活动运 …

谷子部落
https://www.xgiu.com/zztj_js

关于近期51.la无忧啦网站统计JS代码疑似被劫持跳转非法网站-关 …

网页 关于近期51.la无忧啦网站统计JS代码疑似被劫持跳转非法网站 近期，有站长朋友发现了使用51.la的网站统计业务后出现跳转到菠菜和色站APP。 站长们经过检测，发现是51.la...

hostloc.com
https://hostloc.com/thread-1187854-1-1.html

51LA有毒！ -美国VPS综合讨论-全球主机交流论坛 - Powered by …

网页 我用的也是51，没发现 用户少很难发现，通常可能是部分51la节点或者是根据画像分发的广告，而且这种ad通常针对半夜，地区等投放，我就没问题，但是确实有问题，都录屏发 …

最新发布时间: 2023年7月14日

soso365.com
https://www.soso365.com/blog/archives/2030

知名网站统计工具51啦统计代码疑被非法被劫持 – 搜搜365博客

网页 2023年9月6日 · 知名网站统计工具51啦统计代码疑被非法被劫持. 手机端访问本站，会被劫持至菠菜网站，是因为本站使用51啦统计代码所致。. 早在今年5月份我就发现，本站网站 …

(https://cdn.54yt.net/usr/uploads/2024/07/742121885.webp)
通过天眼查对紫田科技股东 徐征 进行查询，发现其曾担任 郑州帝恩爱斯网络科技有限公司 法定代表人及高管，也曾担任 河南云打包网络科技有限公司 高管和股东。

曾担任法定代表人1

天眼查

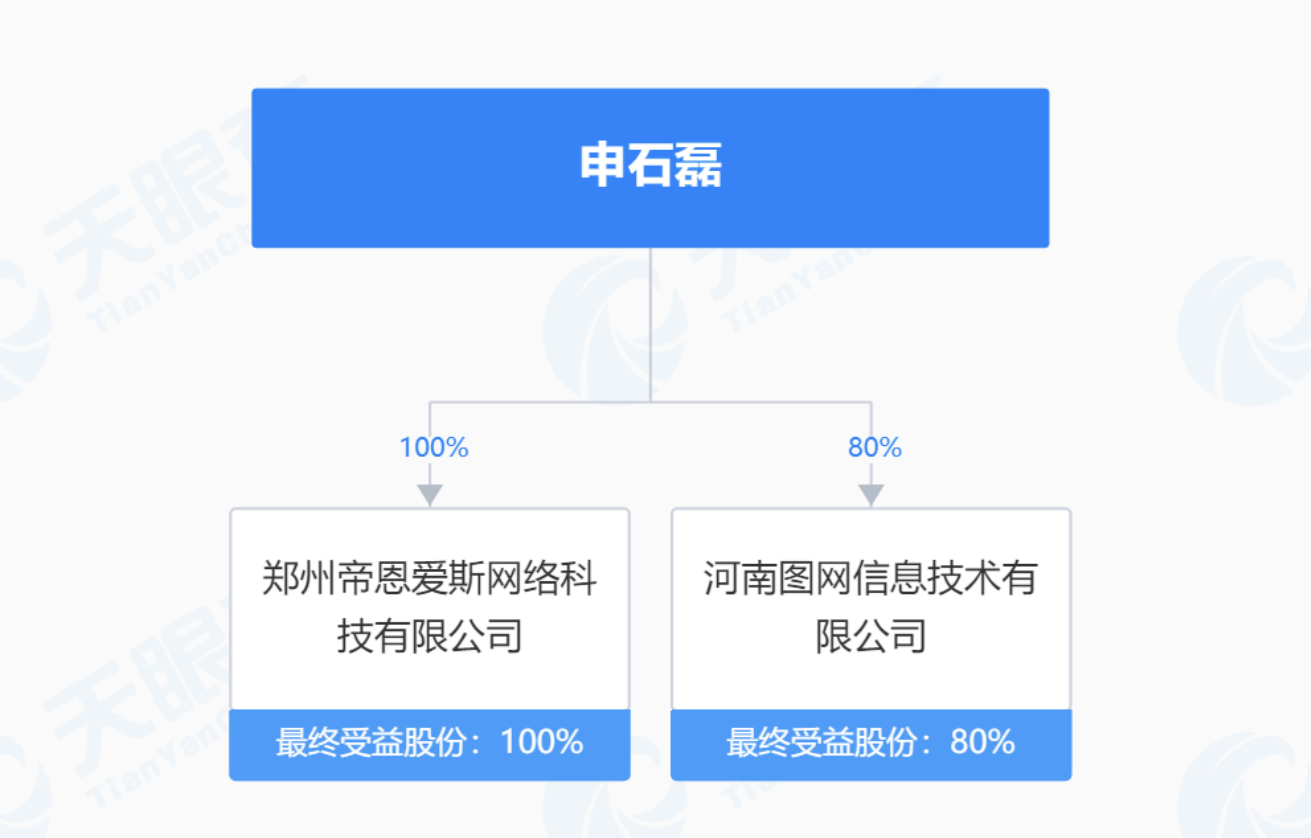
序号	企业名称	现任法定代表人	注册资本	成立日期	登记状态
1	郑州帝恩爱斯网络科技有限公司	申 申石磊 任职 2 家企业 >	100万人民币	2015-03-04	存续

曾担任股东2

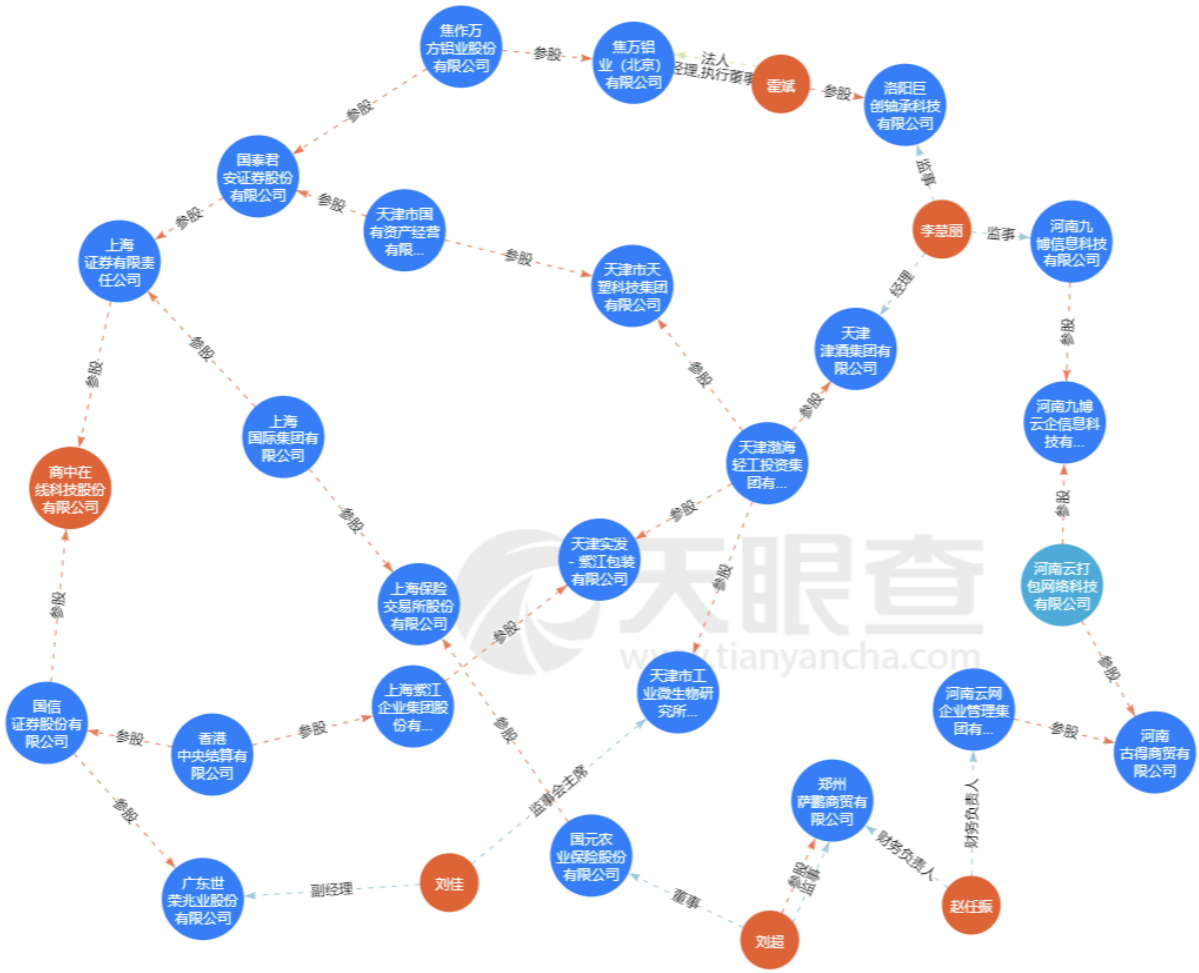
天眼查

序号	企业名称	注册资本	法定代表人	成立日期	登记状态
1	河南云打包网络科技有限公司	500万人民币	徐 徐浩 任职 10 家企业 >	2015-03-19	存续
2	郑州帝恩爱斯网络科技有限公司	100万人民币	申 申石磊 任职 2 家企业 >	2015-03-04	存续

(https://cdn.54yt.net/usr/uploads/2024/07/1731231198.webp)
而Staticfile域名持有公司 河南图网信息技术有限公司 的法人 申石磊 同时任职 郑州帝恩爱斯网络科技有限公司 法定代表人。



(https://cdn.54yt.net/usr/uploads/2024/07/353149248.webp)
而Staticfile的域名注册商商中在线也与紫田科技关联的公司存在着说不清道不明的关系。



(https://cdn.54yt.net/usr/uploads/2024/07/3944715471.webp)

自此可以确定这两个原本由不同云厂商所赞助的静态资源加速服务已经被同一组织所控制，与上述 `Ze-Zheng Wu` 的调查一致。

看似似乎这只是一个名不见经传的小公司所为，然而这只不过是挡在云层前的迷雾。

通过查阅可以发现 郑州紫田网络科技有限公司 总经理 李跃磊 同时担任 河南亿恩科技股份有限公司 股东。

担任法定代表人1

导出 天眼查

序号	企业名称	持股比例	注册资本	成立日期	省份地区	登记状态
1	郑州紫田网络科技有限公司	4%	1000万人民币	2005-06-03	河南省	存续

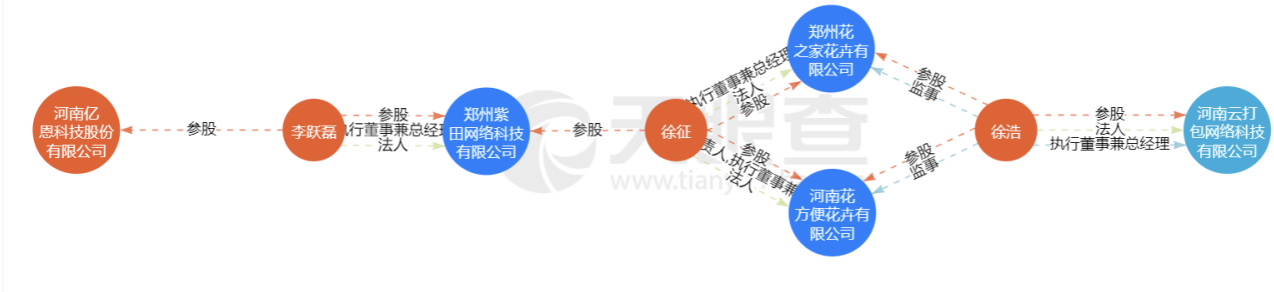
担任股东2

导出 天眼查

序号	企业名称	职位	投资比例	注册资本	法定代表人	成立日期	省份地区	登记状态
1	郑州紫田网络科技有限公司	执行董事兼总经理	4%	1000万人民币	李 李跃磊 任职 2 家企业 >	2005-06-03	河南省	存续
2	河南亿恩科技股份有限公司	-	-	1000万人民币	陈 陈文东 任职 3 家企业 >	2003-08-20	河南省	存续

(https://cdn.54yt.net/usr/uploads/2024/07/2423598592.webp)

通过天眼查透视链可以查看到企业彼此之间的关联信息。



(https://cdn.54yt.net/usr/uploads/2024/07/1172296499.webp)
故事到这里似乎就结束了，然而还有收购polyfill服务的那家公司 `Funnull` 需要进行调查。通过查询域名注册和备案信息可以发现背后的公司为 南京妙彩文化传播有限公司 。

苏ICP备2022000111号

备案类型	企业
备案主体	南京妙彩文化传播有限公司

子备案号

子备案号	网站名称	备案域名
苏ICP备2022000111号-3	-	mikinj.cn
苏ICP备2022000111号-1	-	mcwangl.cn
苏ICP备2022000111号-4	-	miaocwh.cn
苏ICP备2022000111号-2	-	shopingmc.cn

(https://cdn.54yt.net/usr/uploads/2024/07/132754244.webp)
这家公司的主营业务则是为博彩网站提供国内优化CDN服务，与上述的劫持行为不谋而合。

(https://cdn.54yt.net/usr/uploads/2024/07/2137386275.webp)
不过更为危险的是这家公司同时还提供诈骗、钓鱼、色站等令人发指的服务，将供应链攻击提升到了新的高度。

(https://cdn.54yt.net/usr/uploads/2024/07/799859749.webp)

答案

这就像一张巨大的关系网，串联起了利益链中的彼此。每一家公司都看似运营者合规可靠的服务，背后进行的确实见不得人的勾当。

```
郑州紫田网络科技有限公司
商中在线科技股份有限公司
河南亿恩科技股份有限公司
南京妙彩文化传播有限公司
河南图网信息技术有限公司
河南云打包网络科技有限公司
北京新网互联软件服务有限公司
郑州帝恩爱斯网络科技有限公司
```

镇痛

从来没有什么疼痛能够有效缓解，更何况是这种绝症。
目前最为可靠的同类服务为字节跳动静态资源公共库 (https://cdn.bytedance.com/)
你可以将以下地址进行修改

```
cdn.bootcss.com
cdn.bootcdn.net/ajax/libs
cdn.staticfile.net
cdn.staticfile.org
```

替换为

```
//zstatic.net 又拍云赞助
s4.zstatic.net/ajax/libs
//本站提供，回源南科大，使用火山云CDN
cdnjs.snrat.com/ajax/libs
```

或者你可以尝试其他的提供商

```
//7ED
use.sevencdn.com/ajax/libs
//Web缓存网
cdnjs.webstatic.cn/ajax/libs
///字节跳动 最后更新于2022年
lf3-cdn-tos.bytecdntp.com/cdn/expire-1-M
lf6-cdn-tos.bytecdntp.com/cdn/expire-1-M
lf9-cdn-tos.bytecdntp.com/cdn/expire-1-M
lf26-cdn-tos.bytecdntp.com/cdn/expire-1-M
//360奇舞团，长期未更新
https://lib.baomitu.com/
//晓白云
sf.akass.cn
//泽瑶网络 jsDelivr镜像
cdn.jsdmirror.com
```

[1]https://www.bleepingcomputer.com/news/security/polyfillio-bootcdn-bootcss-staticfile-attack-traced-to-1-operator/ (https://www.bleepingcomputer.com/news/security/polyfillio-bootcdn-bootcss-staticfile-attack-traced-to-1-operator/)
[2]https://www.v2ex.com/t/950163 (https://www.v2ex.com/t/950163)
[3]https://web.archive.org/web/20121206014141/http://www.bootcss.com/ (https://web.archive.org/web/20121206014141/http://www.bootcss.com/)
[4]https://ip.sb/whois/bootcss.com (https://ip.sb/whois/bootcss.com)

[5]https://www.icpapi.com/%E4%BA%ACICP%E5%A4%8711008151%E5%8F%B7/ (https://www.icpapi.com/%E4%BA%ACICP%E5%A4%8711008151%E5%8F%B7/)
[6]https://web.archive.org/web/20131103022433/http://open.bootcss.com/ (https://web.archive.org/web/20131103022433/http://open.bootcss.com/)
[7]https://web.archive.org/web/20171230183848/http://www.bootcdn.cn/ (https://web.archive.org/web/20171230183848/http://www.bootcdn.cn/)
[8]https://global.v2ex.com/t/494375 (https://global.v2ex.com/t/494375)
[9]https://web.archive.org/web/20190119210705/https://www.bootcdn.cn/ (https://web.archive.org/web/20190119210705/https://www.bootcdn.cn/)
[10]https://web.archive.org/web/20220208201547/https://www.bootcdn.cn/ (https://web.archive.org/web/20220208201547/https://www.bootcdn.cn/)
[11]https://whoisfreaks.com/tools/whois/history/lookup/bootcss.com (https://whoisfreaks.com/tools/whois/history/lookup/bootcss.com)
[12]https://www.v2ex.com/t/950163 (https://www.v2ex.com/t/950163)
[13]https://github.com/Tencent/vConsole/issues/683 (https://github.com/Tencent/vConsole/issues/683)
[14]https://www.icpapi.com/staticfile.net/ (https://www.icpapi.com/staticfile.net/)
[15]https://x.com/mdmck10/status/1806349965733544160 (https://x.com/mdmck10/status/1806349965733544160)

最后修改：2024 年 07 月 13 日 01 : 58 AM

下一篇 (https://www.54yt.net/426.html)

1 条评论

hack

July 17th, 2024 at 07:22 pm

支持一下

回复 (https://www.54yt.net/435.html?replyTo=1207#respond-post-435)

发表评论

评论 *

说点什么吧.....

表情

私密评论

名称 *

姓名或昵称

邮箱 *

邮箱 (必填,将保密)

地址

网站或博客

发表评论