



格物致知 聚力安全

2017第五届京东安全峰会

The background is a dark blue field filled with a complex, glowing pattern of blue particles and light trails, resembling a nebula or a high-speed data stream. In the center, there is a bright, circular glow composed of concentric rings of light, with a greenish-yellow outer ring and a more intense, multi-colored inner core. The text is centered over this glowing area.

Cloudjacking for Command and Control



Accenture Security 埃森哲安全



Vincent Yiu 姚旻言

Security Manager, Red Team 安全经理

Advanced Threat Services



@vysecurity





目录 Contents

01

Domain Fronting 101

什么是 domain fronting?

02

Cloudjacking – CDN

介绍 Cloudjacking –

Domain Hijacking Content Delivery Network customers

域名劫持内容分发网络客户

03

Cloudjacking - Storage

介绍 Cloudjacking –

Domain Hijacking Cloud Storage Provider customers

域名劫持云存储提供商客户

04

Benefits, Remediation and Discussion

What are the benefits to threat actors?

对威胁攻击者来说有什么利益?

How do we fix this issue?

我们如何修补这个漏洞?



Domain Fronting 101

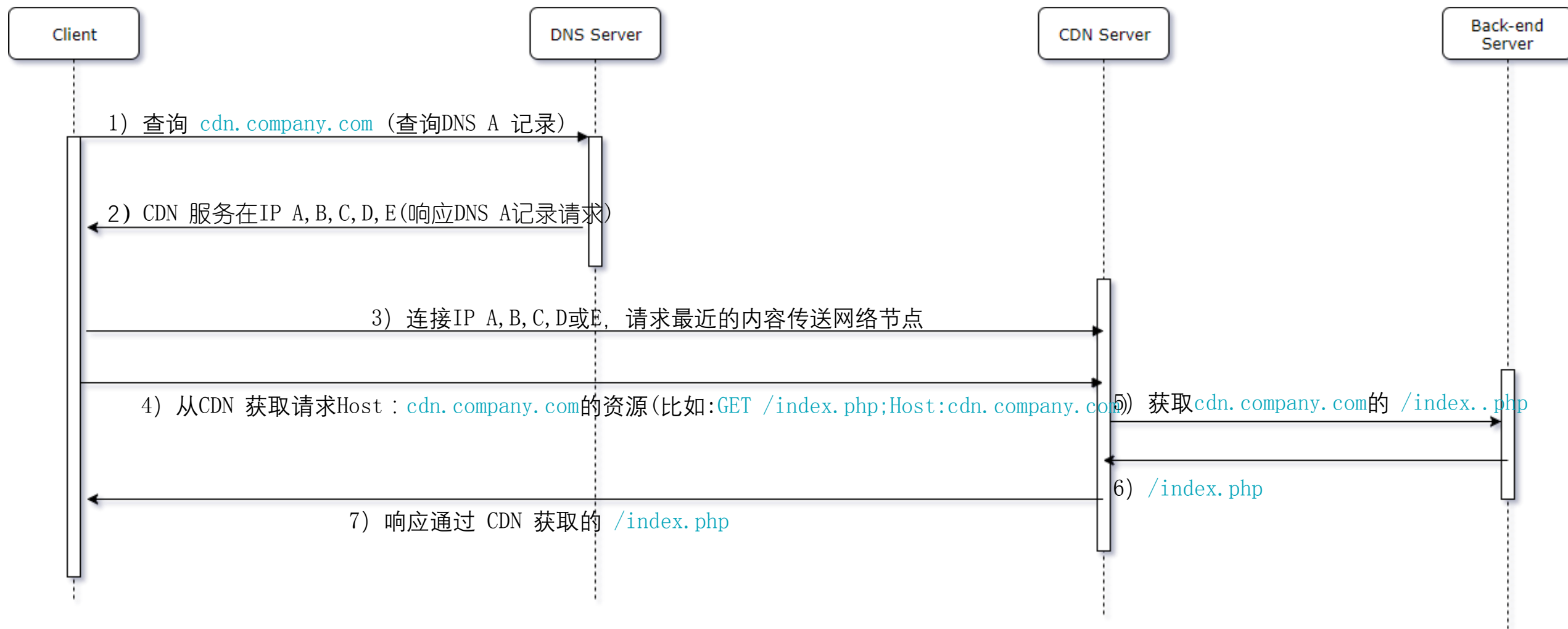
- 近几年来被TOR研究并使用来绕过审查
- 2016年在攻击行为中作为武器来使用
- 这个技术在2017年初成为主流

- 利用内容分发网络中的核心设计缺陷
- 不只是针对于一个云或基础架构服务提供商
- 被威胁行为者利用



Domain Fronting基础

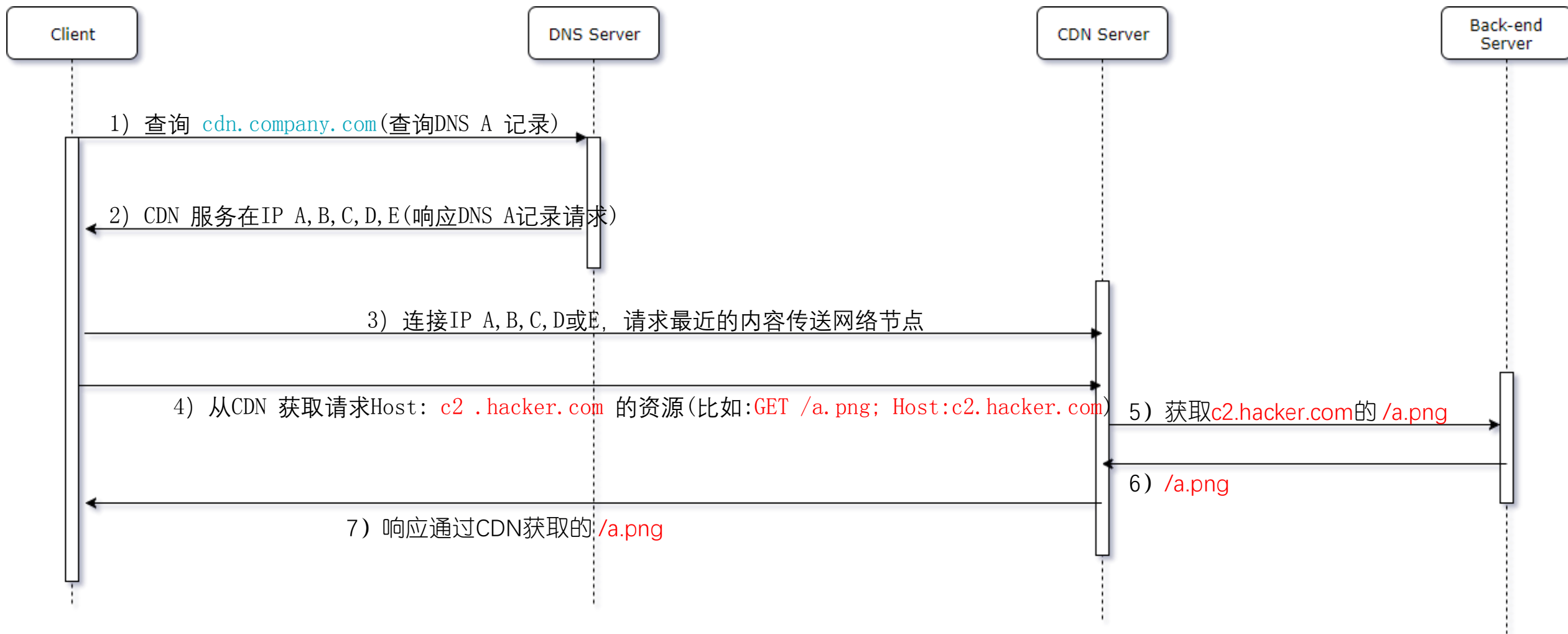
访问 `cdn.company.com`





Domain Fronting基础

通过cdn.company.com获c2.hacker.com/a.png





可以使用什么 Domains?

Discovering front-able domains



<https://github.com/vysec/DomainFrontingLists>

01

找到云服务提供商

02

找到两个使用同一个云服务的网站

03

使用指定的 Host:website-b.com
链接 <http://website-a.com>

04

如果请求到website-b的资源,
那么就可以domain fronting。



2017第五届京东安全峰会

Domain Fronting in Command and Control

使用Domain Fronting作为C2的演示视频

演示给我们看！



<> Code

! Issues 0

🔗 Pull requests 0

📁 Projects 0


📊 Insights

Branch: master ▼

DomainFrontingLists / Cloudfront.txt

Find file

Copy path

 Vincent Yiu First push

8283107 on Sep 4

0 contributors

14381 lines (14381 sloc) | 271 KB

Raw

Blame

History



```
1 a792b6aae928.incms.net
2 abrakam.com
3 accountancyagejobs-edge.madgexhosting.net
4 admin.3docean.net
5 admin.abemafresh.tv
6 admin.activateden.net
7 admin.agilixbuzz.com
8 admin.airmap.com
9 admin.allego.com
10 admin.amplitude-studios.com
11 admin.assignar.com.au
12 admin.audiojungle.net
13 admin.aws.prod.flixster.com
14 admin.beachbodyglobal.com
15 admin.beepsend.com
```

我们一起演示Domain Fronting



Cloud Domain Hijacking!

2018年的下一代技术！



Domain Hijacking 不是一个新概念



利用DNS的核心设计



使用当前域名的声望



传统的 Domain Hijacking

在过去的20年里，它是如何被利用的？



- 1) static.company.com CNAME static.companystorage.global
- 2) static.companystorage.global 已经被遗弃了
- 3) 攻击者注册了static.companystorage.global，所以可以控制 static.company.com 的内容



基于云的Domain Hijacking

现在和将来！

DOMAIN HIJACKING
USING THE CLOUD!

01

CONTENT DELIVERY
NETWORKS

02

CLOUD
STORAGE

03

- 1) 主要的云服务提供商！
- 2) 重新创建废弃的内容交付网络实例！
- 3) 重新创建废弃的云存储实例！



云A – 内容分发网络 (CDN) Domain Hijacking

澄清



劫持以前使用过云A的CDN服务的域名



劫持废弃的域名



这不是domain fronting



01

DNS

获取大量个
DNS
CNAME记录

02

找目标

针对特定云
提供商筛选
出域名列表

03

研究

通过运行
Hijack.py来发
现那些可能被
劫持的域名

04

利用/攻击

验证或攻击
这些可能被
劫持的域名



什么是 Hijack.py ?

第3步到底是什么？

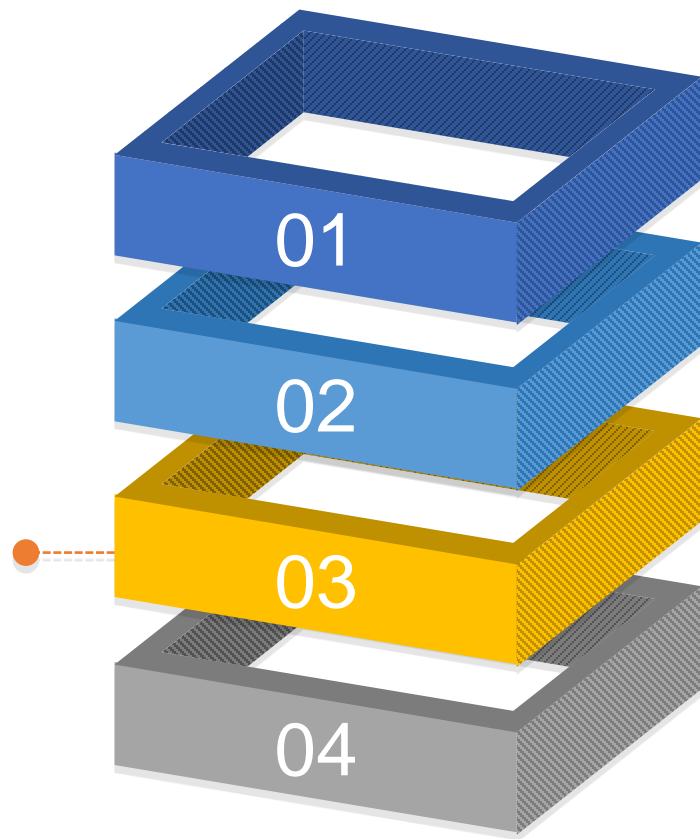
Hijack.py

连接到指定的目标域，并检查是否可以劫持一些已知的可劫持云服务

云A的CDN: "Bad Request, the Request could not be satisfied"

云A的Storage: "The specified bucket does not exist"

云B的Storage: "The specified key does not exist"





2017第五届京东安全峰会

云A – CDN Domain Hijacking方法

劫持云A客户群的域名

演示给我们看！



Benefits of Domain Fronting, CDN Domain Hijacking and Cloud Storage Domain Hijacking

为什么这些技术会被采用？



1

Bypass
Categorisation

网络代理可以配置为只允许流量到某些允许的网站 – 这个技术可以绕过它



2

Masquerade

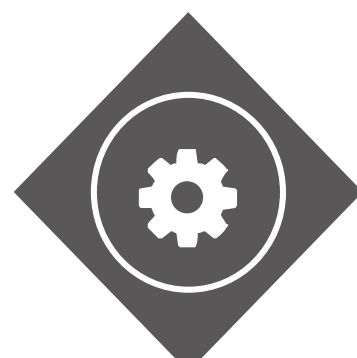
为了绕过检测通常会伪装成一个合法的网站 – **WHOIS**指向银行，政府或者其它行业



3

Difficult Attribution

在使用内容分发网络的主机中找到潜在的恶意主机需要云提供商帮助



4

Easy Deployment

利用这项技术需要相对较少的时间



5

Core Design Flaw

这就是利用了内容分发网络的一个核心设计缺陷来改进传统**C2**的方法



2017第五届京东安全峰会

云A – 存储 Domain Hijacking方法

劫持使用云A的域名

演示给我们看！

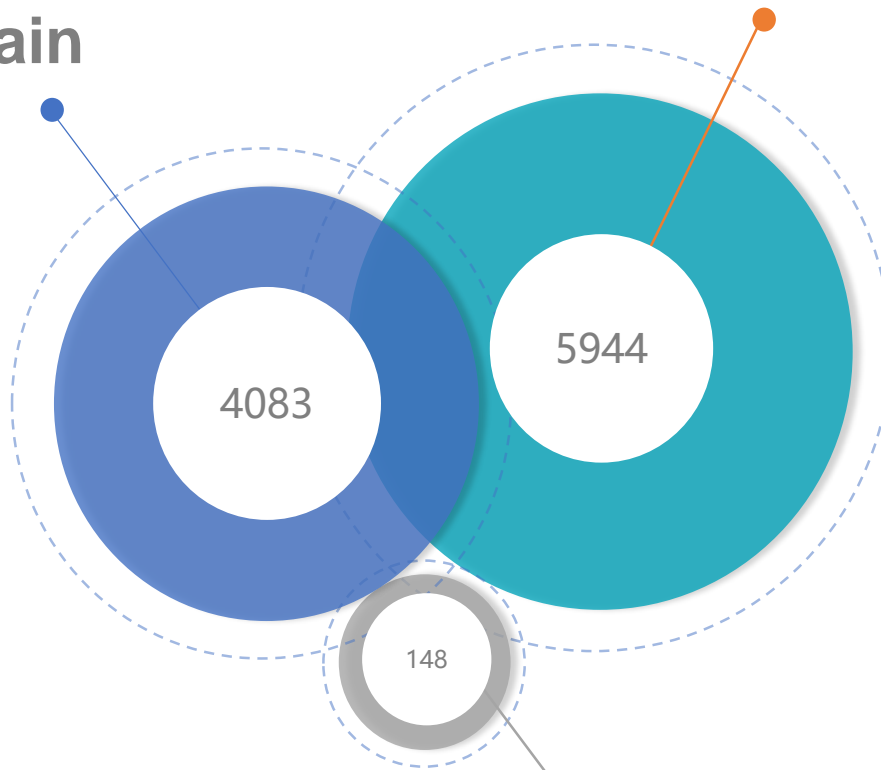




24小时 – 研究的结果！

云A内容分发网络Domain Hijacking

云A存储Domain Hijacking



云B存储Domain Hijacking



整治

如何修补？



禁用废弃的云实例



删除该实例的CNAME记录



不要删除实例！



2017第五届京东安全峰会

提问环节



R

FusionX – Washington DC
Me? – U.K.

)

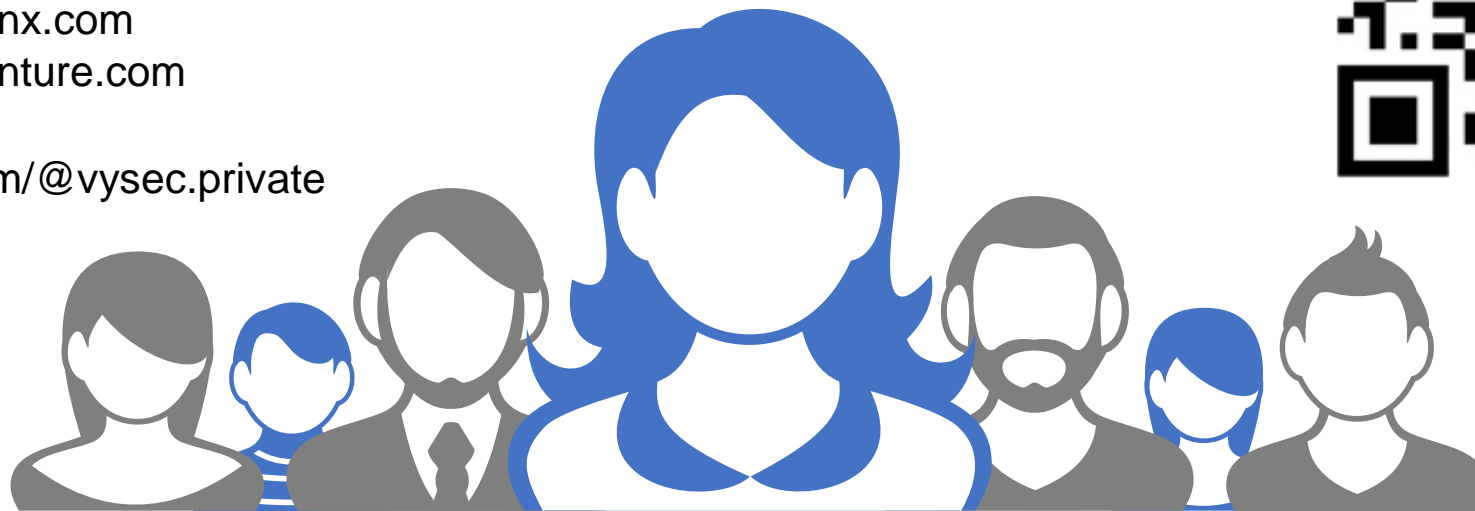
Vincent.Yiu@fusionx.com
Vincent.Yiu@accenture.com

E

<https://medium.com/@vysec.private>

L

@vysecurity





THANK YOU!