All Your DNS Records Point to Us

Understanding the Security Threats of Dangling DNS Records

2016.11

❑所有你的DNS记录指向我们

1. 介绍	INTRODUCYION
2. DNS概览	DNS OVERVIEW
3. DNS悬挂记录	DALING DNS RECORDS
4. 测试方案	MEASUREMENT METHODOLOGY
5. 测试结果	MEASUREMENT RESULTS
6. 威胁分析	THREAT ANALYSIS

❑所有你的DNS记录指向我们

7. 解决方案	MITIGATIONS
8. 相关工作	RELATED WORK
9. 结论	CONCLUSION
10. 致谢	ACKNOWLEDGMENTS
11. 参考文献	REFERENCES

1 简介

- New Threat
- Large-scale measurement study
- Mitigations
- Roadmap

1 简介

New Threat

A DNS record(a tuple):

<name, TTL, class, type, data>

- 4种Dare
  - Dare-A
  - Dare-CN
  - Dare-MX
  - Dare-NS
- 3种攻击途径：
  - 云端IP地址分配
  - 第三方服务
  - 域名失效

1 简介

Large-scale measurement study

-vector 1

IPScouter工具来获取云端IP地址

Amazon EC2

Microsoft Azure

-vector 2

测试了9个最常用的第三方服务

-vector 3

反复核对WHOIS数据和域名登记者来明确失效域名

- 4个数据库：
  - Alexa top1million跨度7年的顶级域名
  - Alexa top10000子域名
  - 2700个edu子域名
  - 1700个gov子域名

Mitigations

- 3种机制
  - 允许aDNS服务器来认证A记录指向的主机
  - 通过给每一个服务用户都采用安全的独立命名空间来切断悬挂的CNAME记录的解析链
  - 建议aDNS服务器定期检查DNS记录指向的失效的域名

2 DNS 概览

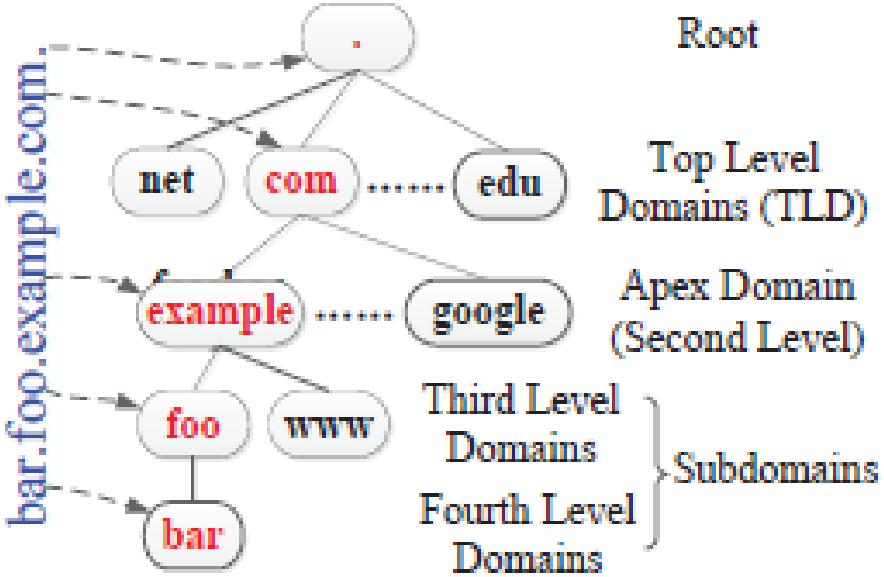


Figure 1: The hierarchy of DNS.

2 DNS 概览

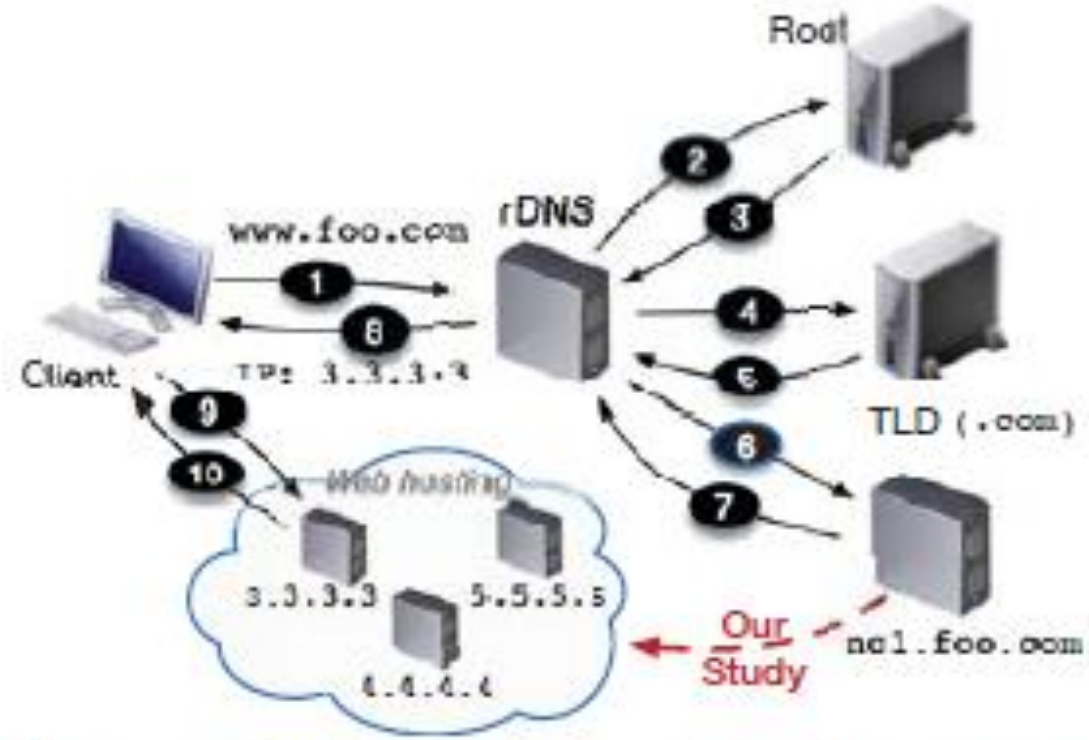


Figure 2: The workflow of DNS resolution for www.foo.com.

3 DNS悬挂记录

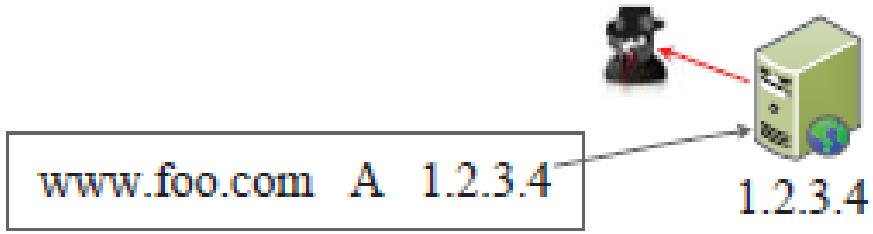


Figure 4: An example of a dangling A record.

Dare	RR	Description
Dare-A †	A	Returns an IPv4 address
Dare-CN ‡	CNAME	Alias of a name to another
Dare-MX	MX	Maps to a list of message transfer agents
Dare-NS	NS	Delegate to an authoritative name server

Table 1: Types of security-sensitive dangling DNS records. †Our work currently covers IPv4 only. ‡DNAME is semantically similar to CNAME, so we do not consider DNAME separately.

3 DNS悬挂记录

- 3.1安全相关的Dares
- 3.2云端IP
- 3.3遗弃的第三方服务
- 3.4失效域名
- 3.5总结

3 DNS悬挂记录

3.1安全相关的DNS

- 4种Dare
  - Dare-A
  - Dare-CN
  - Dare-MX

    foo.com. 60 MX 10 a.mail.com
    foo.com. 60 MX 10 b.mail.com
    foo.com. 60 MX 20 c.mail.com
  - Dare-NS

3 DNS悬挂记录

3.2 云端IP

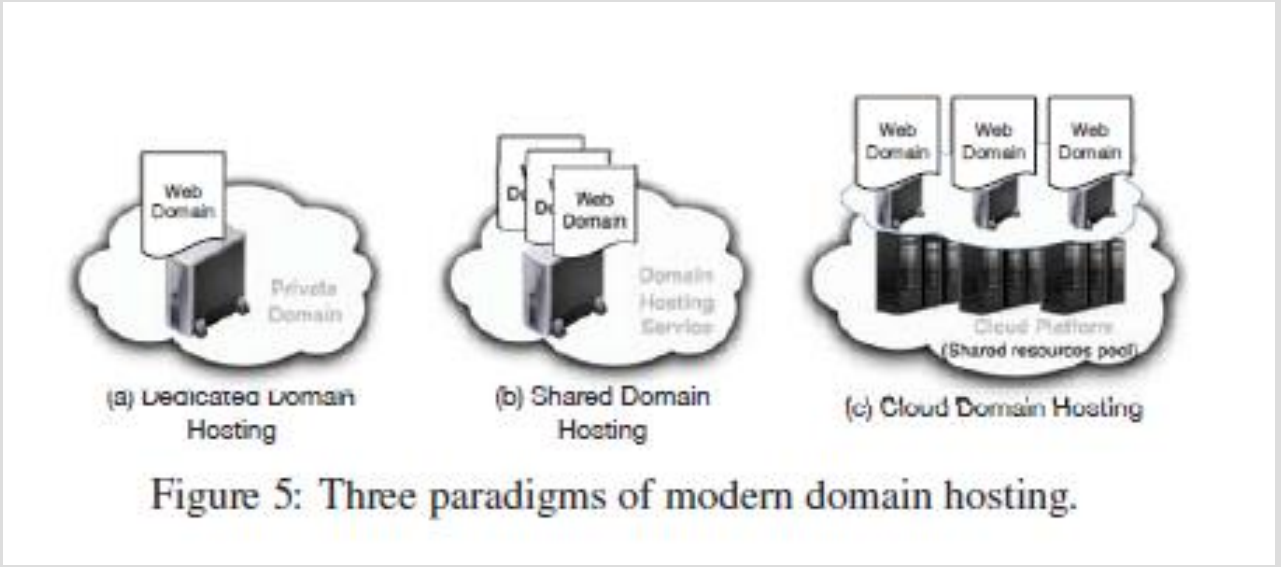


Figure 5: Three paradigms of modern domain hosting.

Dare-A

- Amazon EC2
- Microsoft Azure

3 DNS悬挂记录

3.2 云端IP

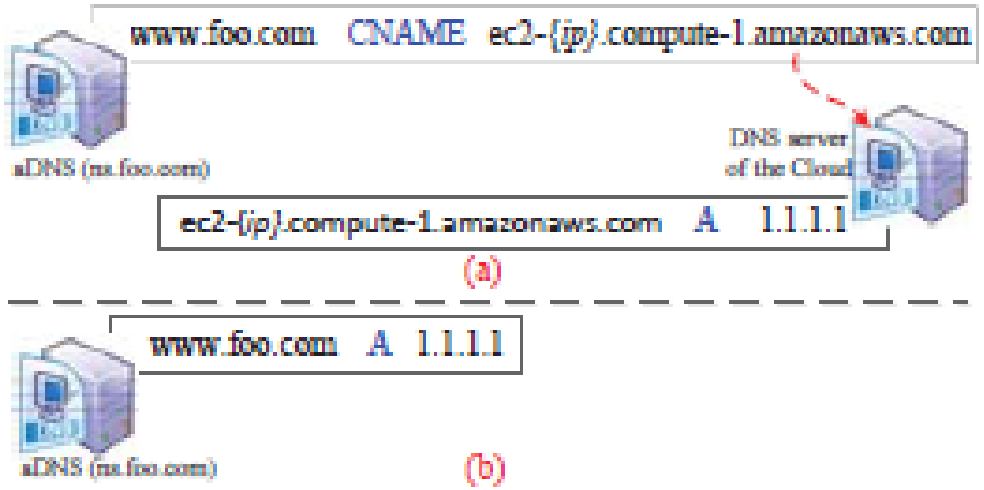


Figure 6: aDNS setups for a domain hosted in the cloud.

3 DNS悬挂记录

3.3被遗弃的第三方服务

Mailgun email 传送
Shopify 建立网上商城
提供子域名alice.myshopify.com

- Alice 配置：
- shop.Alice.com A 23.227.38.32
- (or) shop.Alice.com CNAME alice.myshopify.com

- 一个独立域名：
- *.myshopify.com CNAME shops.shopify.com

成功的攻击需要：

- 易受攻击的域名可以被解析到一个通用的目标（也就是IP地址或者是域名）并且第三方服务不核查这个域名的所有权，或者
- 这个易受攻击的域名解析到一个可用时可以由任何用户收到的自定义目标

3 DNS悬挂记录

3.4 失效的域名

攻击者可以重新注册并滥用失效的域名

以前的研究工作主要是研究滥用失效域名的残留的人们的信任，

我们主要研究滥用人们对未失效子域名的信任。

这样的旧记录普遍被域名管理者忽视，因为：

（1）有第二个记录作为一个失效备援的工具（大量的MX和NS记录）

（2）链接到失效域名的服务不再使用所以没人关心更新它们。

3.5总结

攻击途径总结

Dares	IP in Cloud	Abandoned Services	Expired Domains
Dare-A	√	√	
Dare-CN	√	√	√
Dare-MX	√	√	√
Dare-NS	√		√

Table 2: Summary of the attack vectors to which each type of Dare is vulnerable.

4 测试方案

Figure 7: Methodology overview.

4 测试方案

- 1 每种Dare在自然状态下有多普遍？
- 2 Dare有什么安全影响？

- 4.1域名收集
- 4.2域名数据检索
- 4.3查询DNS悬挂记录（Dare）

4 测试方案

4.1域名收集

Dataset	Data Space
D	Unexpired apex domains in Alexa top 1M during 2010 $\sim$ 2016
S_t	Subdomains of top 10,000 general
S_e	Subdomains of top 2,700 .edu
S_g	Subdomains of top 1,700 .gov

Table 3: Evaluation set of domains.

4 测试方案

4.1域名收集

- 顶级域名数据集记为D
- 成功收集到320个域名
- 在此基础上进行一个20000个规模的强力扫描
- 288million请求
- 570thousand 接收
- 子域数据集记为：
- $S = St \cup Se \cup Sg$

4.2域名数据检索

- 我们使用DNS工具dig检索数据集D和S的每一个域名
- 除了A记录之外，所有类型的Dare我们都在data域递归地发布请求直到到达A记录或者不可达
- 因此每一个域名都有一个解析链
- $RCd = \{rtype0(d, data0), \ldots, rtypei(datai-1, datai)\}$
- 这个数据集记为DREC = *RCd*

4 测试方案

4.3查询Dare

Algorithm 1 Search for Dares.

Input: DREC, ALLOCIP
Output: Dares (DARES) and potential Dares (PDARES)

```
1:  procedure DAREFINDER(DREC, ALLOCIP)
2:      for RC ∈ DREC do
3:          daretype ← RC.rtype_0
4:          for rec ∈ RC do
5:              hostname, rtype, data ← unpack(rec)
6:              if rtype == "A" then
7:                  if data ∈ ALLOCIP then
8:                      DARES ← [daretype, rec, data]
9:                  else if likely_dareA(data) then
10:                     PDARES ← [daretype, rec, data]
11:             if rtype ∈ ["CN", "MX"] then
12:                 if domain_expired(data) then
13:                     DARES ← [daretype, rec, data]
14:                     break
15:                 if abandoned_service(data) then
16:                     DARES ← [daretype, rec, data]
17:                     break
18:             if rtype == "NS" then
19:                 if domain_expired(data) then
20:                     DARES ← [daretype, rec, data]
21:                     break
```

4 测试方案

4.3.1查询A记录（7/9行

- 搜索IP池
  - IPScouter 工具
  - EC2
    - EC2-Classic
    - EC2-VPC
  - Azure
- 自然状态下的潜在的Dare（9行）
  - 一组A 记录$R = \{r1, r2, \cdots, rn\}$
  - ri = <namei, IPi>，$i \in [1, n]$
- 算法1里的第九行
  - Step1 如果IPi不在云里，就移除它
  - Step2 移除所有不可能悬挂的记录
  - Step3 用Zmap扫描所有剩下的记录
  - Step4 剩下的记录都是可能成为Dare的

4 测试方案

4.3.2搜索被遗弃的服务

- 搜索被遗弃的服务(15行)
  - 把所有的CNAME和MX归类
  - 检查所有的email和top200的非email服务
  - 进一步选择（1个email和8个non-email）
    - 满足3.3成功攻击的要求时
    - 免费帐户
  - Non-email：google和aliyun强制进行所有权审核
  - 只有一个email服务不强制进行所有权审核

Type	Service List
CN	Azure cloud service (`cloudapp.net`), Shopify, Github, Wordpress, Heroku, Tumblr, Statuspage, Unbounce
MX	Mailgun

Table 4: Evaluated third-party services.

4 测试方案

4.3.3搜索失效域名

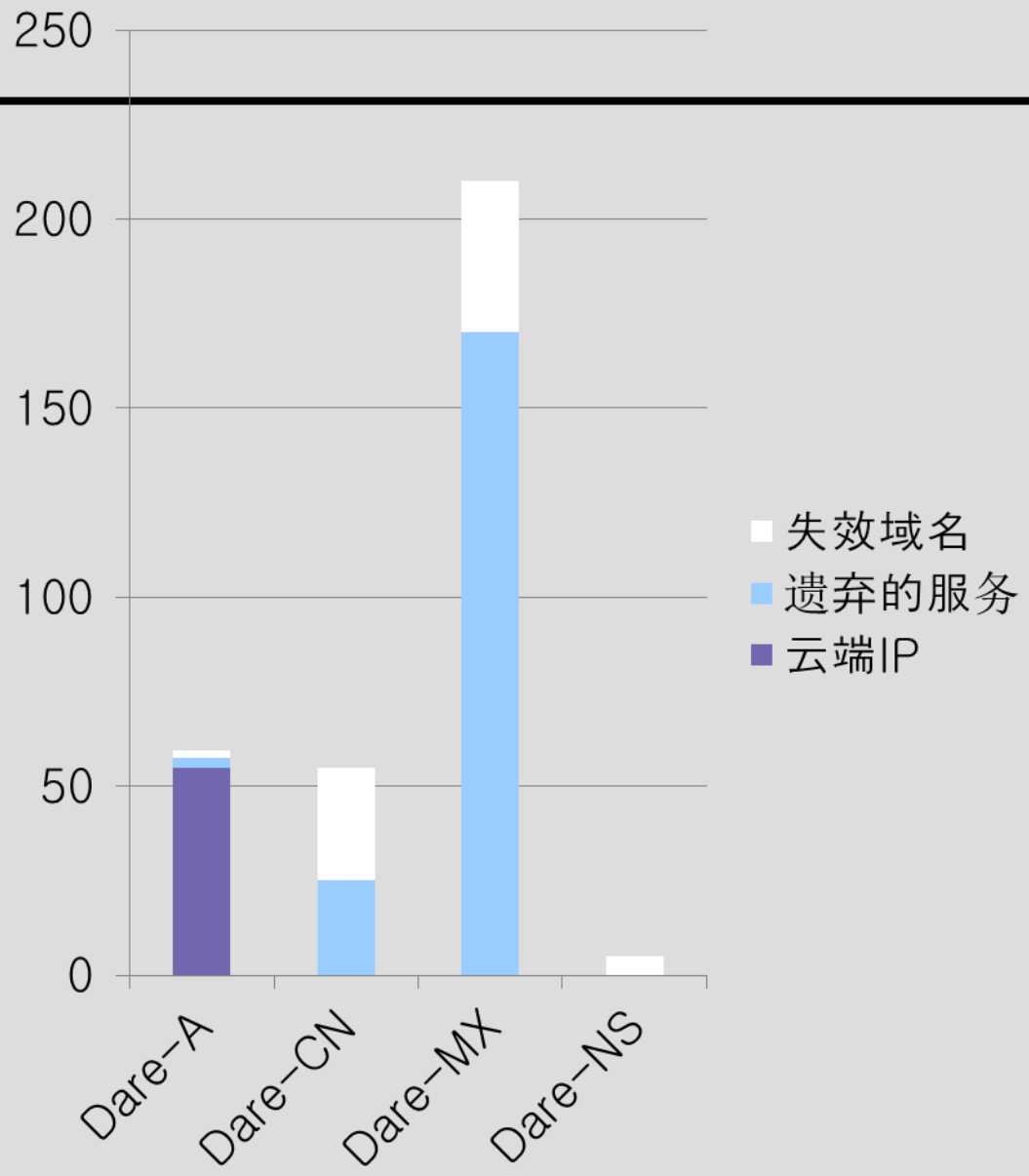
- 搜索失效域名(12/19行)
  - WHOIS回应
    - （null=失效）
  - 审核常用网络域名注册商如GoDaddy
    - （可重新注册=失效）

5 测试结果

- 5.1DNS悬挂记录的特征
- 5.2云端IP
- 5.3遗弃的第三方服务
- 5.4失效域名
- 5.5DNS悬挂记录的篡用
- 5.6道德性考虑

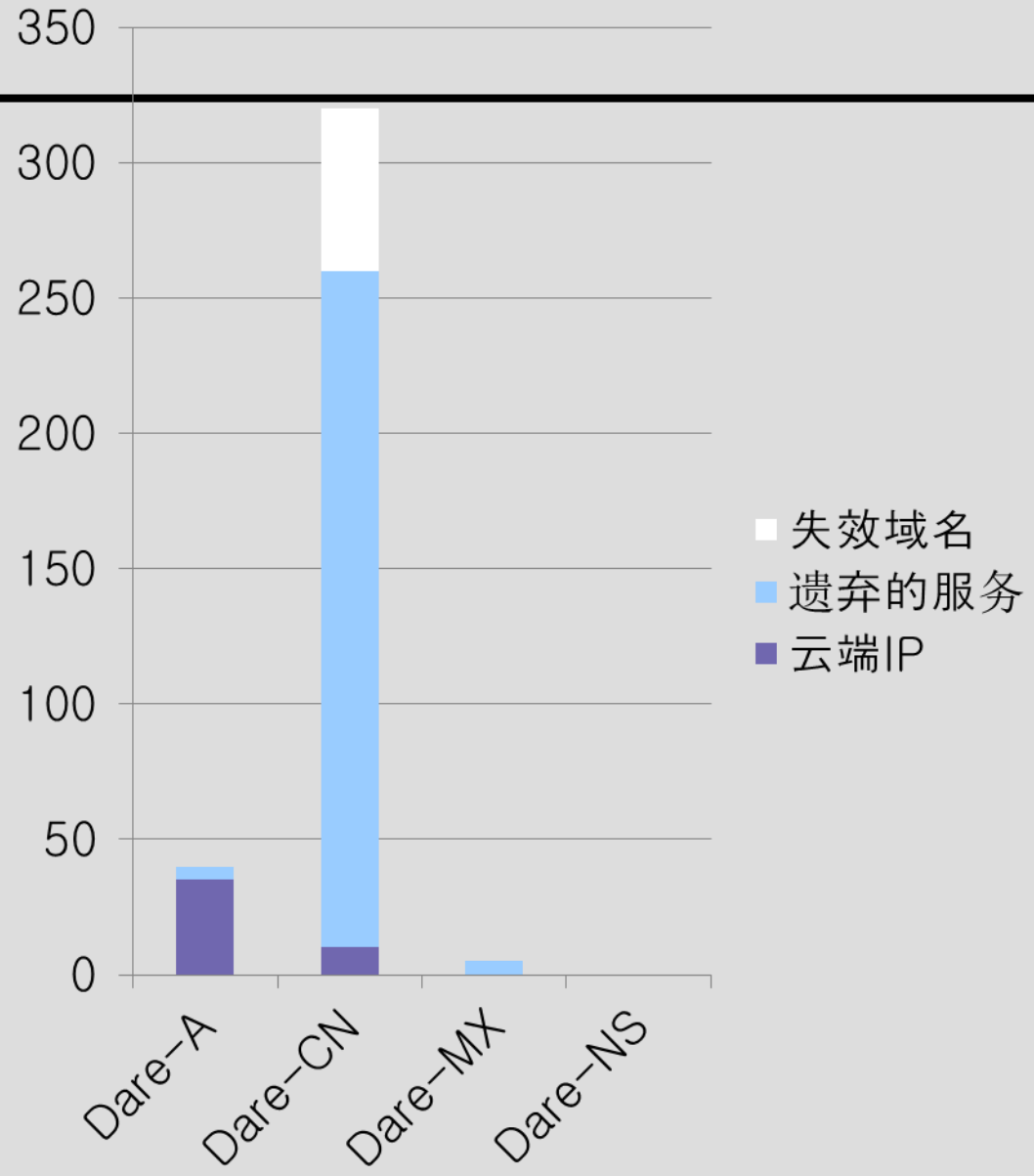
数据集确认是Dare的数量

(a) Alexa top 1M顶级域名



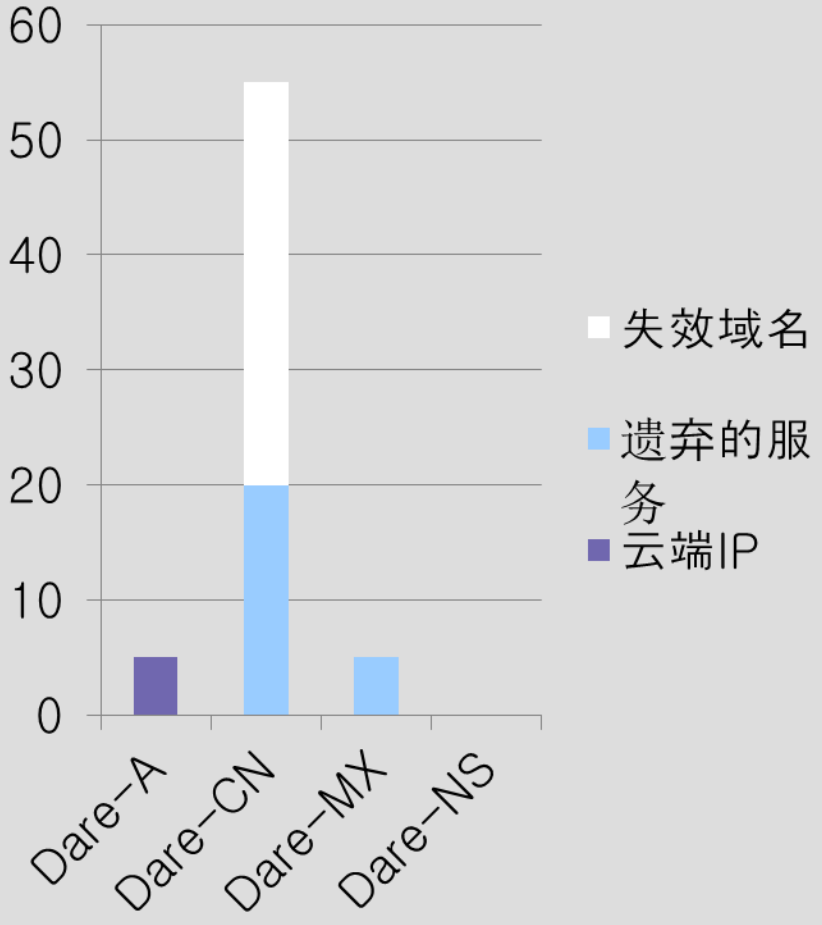
数据集确认是Dare的数量

(b) Alexa top 10k的子域名



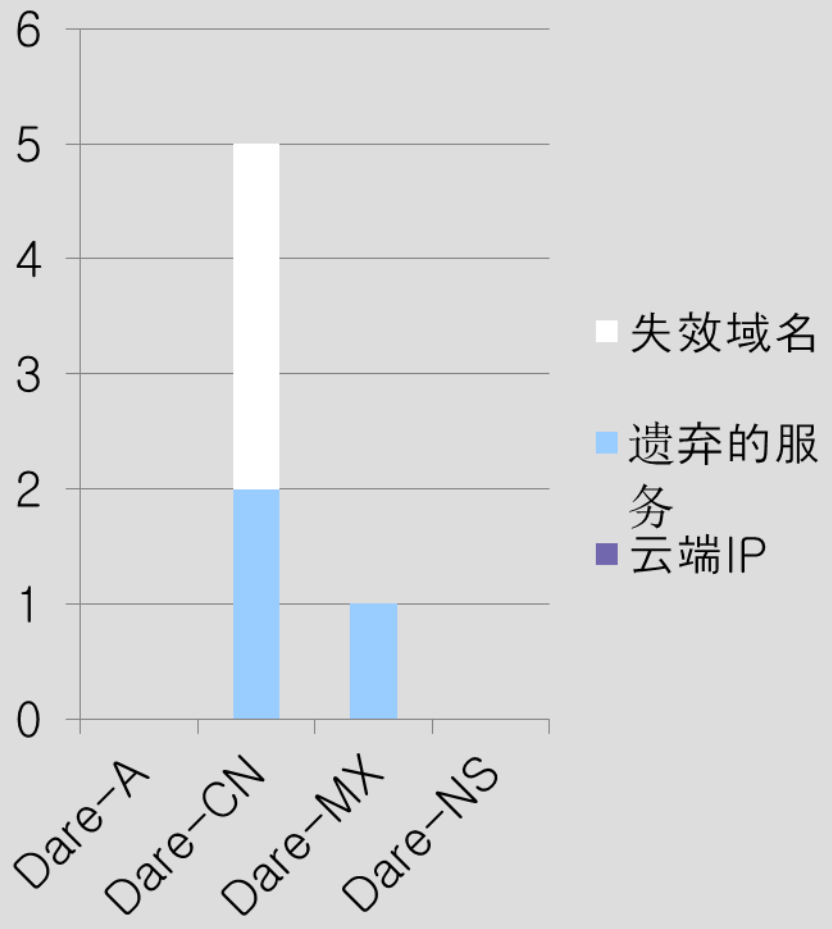
数据集确认是Dare的数量

(c) Edu的字域名



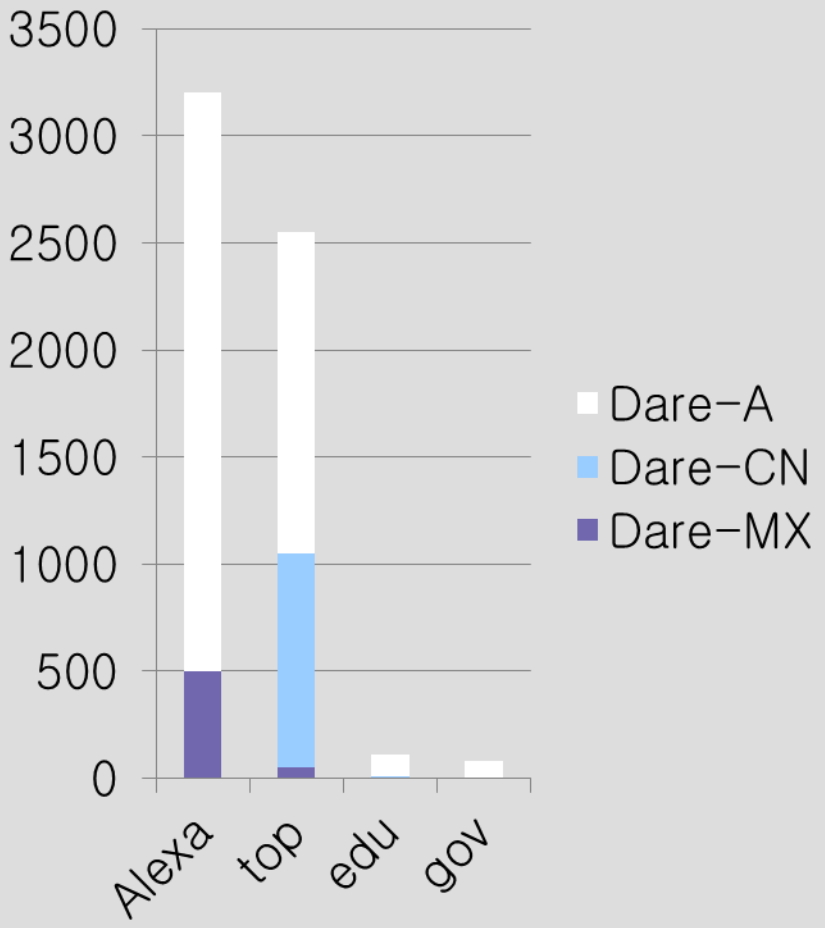
数据集确认是Dare的数量

(d) Gov的子域名



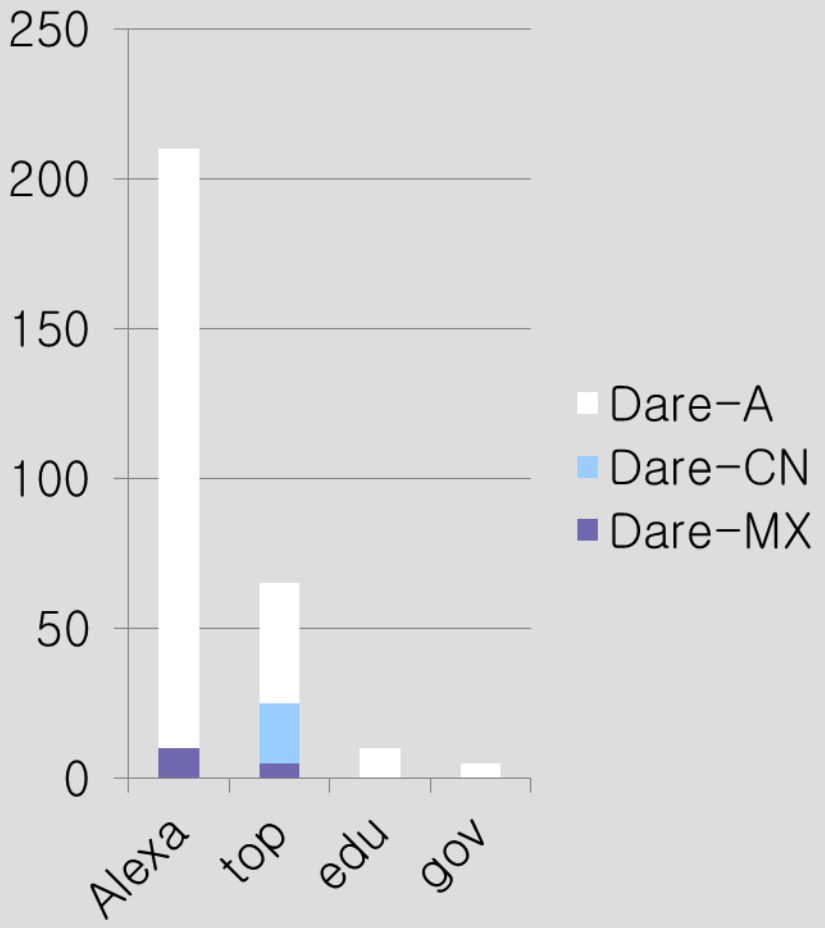
潜在的Dare数量

(a) Amazon EC2



潜在的Dare数量

(b) Microsoft Azure



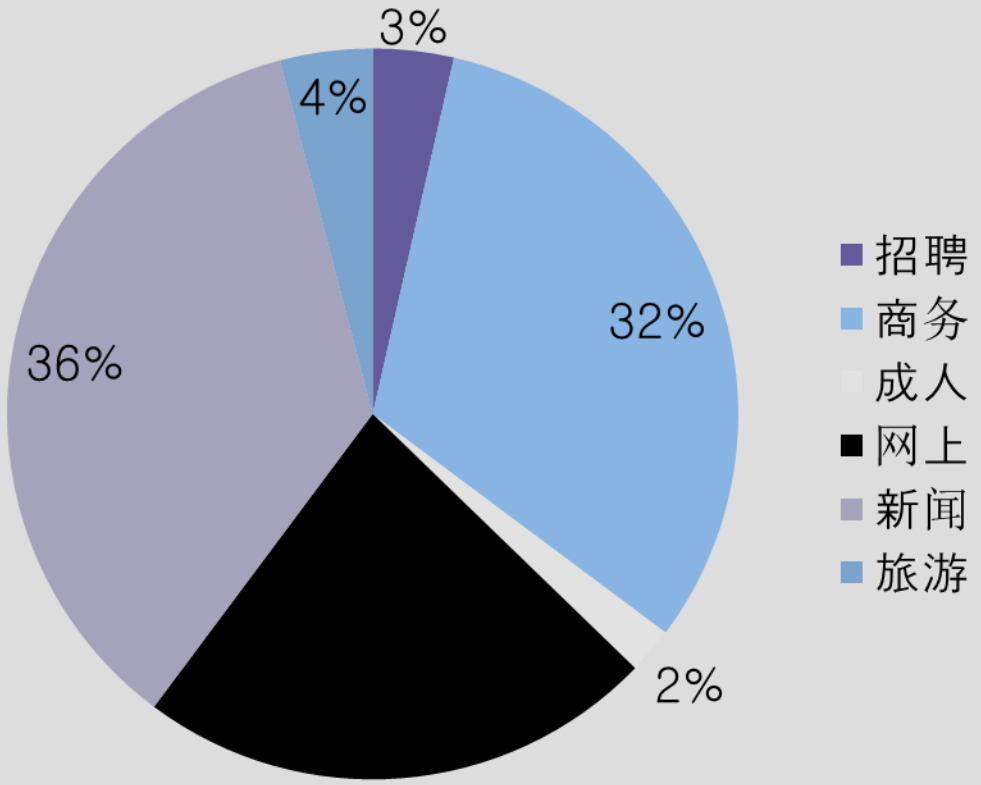
- S数据集确认是Dare的分类统计，其中一些域名重叠了（可能既有Dare-A又是Dare-CN）

Dare	top 10K (S_t)	edu (S_e)	gov (S_g)	
Dare-A	40	1	0	
Dare-CN	260	50	5	
Dare-MX	5	1	1	
Total	277†	52	6	335

Table 5: Statistics of distinct apex domains in $\mathbb{S}$ with confirmed Dares. † Some domains overlap across the above three lines (e.g., a domain has both Dare-A and Dare-CN).

有Dare的网站分类

5.2云端IP



已经确认的和潜在的Dare

- 在测试中，所有的Dare都来自于EC2
  - 其中92%来自于EC2-Classic

5.3遗弃的第三方服务

表明每一个第三方服务平台都有Dare，包括Yahoo.net以及mit.edu

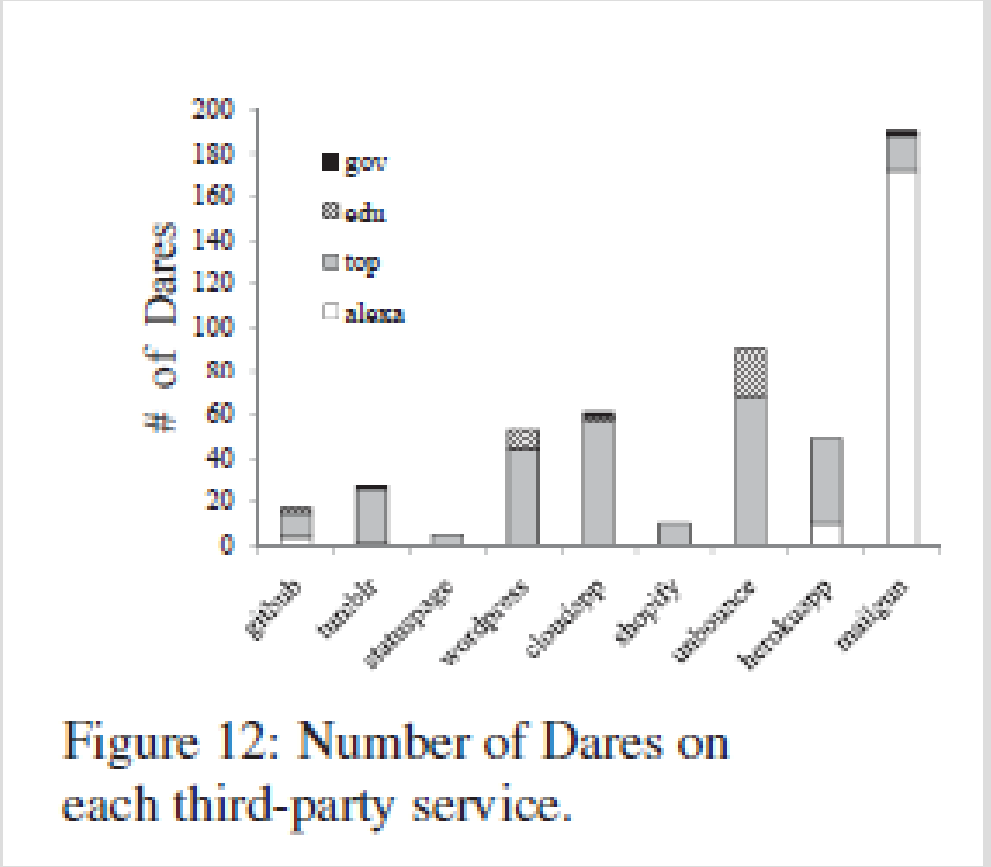


Figure 12: Number of Dares on each third-party service.

5.4失效域名

Pattern	Examples	%
Similar to alias	module.rabobank.nl → rabobank-hoi.nl rps.berkeley.edu → rpsberkeley.org	39%
Expired external services	js.jiayuan.com → 21vcdn.com shopping.segye.com → ticketdamoa.com	21%
Typo	b.ns.trnty.edu → awsnds-18.net customizedgirl.com → shoplattitude.com	7%

Table 6: Patterns of expired domains.

6 威胁分析

- 6.1垃圾邮件、钓鱼网站等
- 6.2活跃的Cookie窃取
- 6.3邮件欺诈

7 解决方案

- 对短暂IP地址进行审核认证
- 通过第三方服务的aDNS破坏解析链
- 失效域名检查

THANKS