


# 针对DNS的随机域名DDoS攻击综述： 特性、攻击方法、检测和阻断

Hongliang Liu  
Principal Data Scientist, Nominum

PSC 2017, Beijing March 2017



如果每天你有全球范围1000亿条实时DNS数据，你能拿来干什么？



我们谈谈随机域名(PRSD) DDoS攻击吧

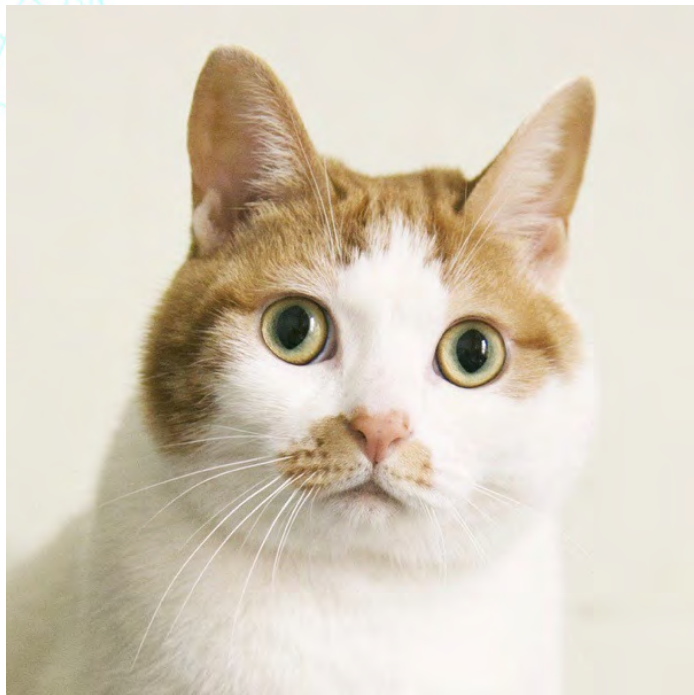


“You might say that DNS is in our DNA. Nominum invented DNS, has written 90% of the world’s DNS code, and was the first to scale, secure, and leverage DNS to deliver a whole new set of services. We are passionate about great Internet experience, high quality code, and straightforward approaches to solving complex provider challenges. Now we have harnessed DNS to allow providers to deliver extraordinary value to their subscribers.”

<https://nominum.com/company/>

# 关于我

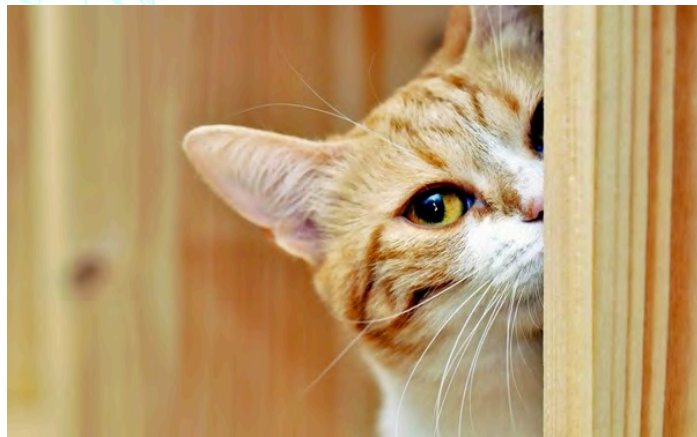
- Nominum 首席数据科学家
- 用机器智能研究解决安全问题
- @phunter\_lau on weibo.



@dudulee的浪里格朗 的猫，她叫杨泥泥

# 摘要

- 随机域名 (PRSD) 攻击是什么?
- 分类讲解A、B、C、X型和其他杂鱼
- 云服务和网络提供商的正确检测和阻断方法：细粒度规则系统



<https://www.pinterest.com/pin/311874342919696035/>

# 你见过它们么？

uec0vakqfmw.air-force.biz.  
60srufutupaq.air-force.biz.  
n16g8pvgwj3.air-force.biz.  
cbert8pa8c7u.air-force.biz.  
2i117grhej3t.air-force.biz.  
i4tita87hkes.air-force.biz.  
a611bjuob2if.air-force.biz.  
skgihwjcnhrc.air-force.biz.  
a5qq26fid5mf.air-force.biz.  
8ger0i49btecqm.oasgames.com.  
h0tb3gpmv3j711e.oasgames.com.  
6yipzhtdbjvswkd47.oasgames.com.  
6yipzhtdbjvswkd47.oasgames.com.  
yeyxqo1vzdox2puux2xzrlz.oasgames.com.  
yeyxqo1vzdox2puux2xzrlz.oasgames.com.  
hmdg78ribgb7.oasgames.com.  
6yipzhtdbjvswkd47.oasgames.com.  
gq3ocdo9vq5u.oasgames.com.

bnBT8BaX.iphop.info.  
boW7u9yC.iphop.info.  
BZHUJZfa.iphop.info.  
CH7eJiL4.arkhamnetwork.org.  
cHbPvNn9.iphop.info.  
d8JR09za.iphop.info.  
dCMz.mc.arkhamnetwork.org.  
Dgvpi2ls.iphop.info.  
DKaGi691.iphop.info.  
e6ylLo4I.arkhamnetwork.org.  
epRIhim6.iphop.info.  
eQv16v3N.iphop.info.  
F8bN7CHc.iphop.info.  
f9WqoEk8.arkhamnetwork.org.  
faggot.extronus.net.  
FGhwML2G.iphop.info.  
fUKFGlE5.arkhamnetwork.org.  
GAtOCGUj.iphop.info.



# 攻击者想要什么

- 消耗所有DNS查询资源
  - 随机域名迫使运营商缓存 (cache server) 实效
  - 转发递归查询攻打权威服务器 (auth server)
  - 权威服务器还不能封运营商缓存服务器IP
- 效果
  - 用户输入网址比如 example.com 浏览器返回该域名不可用。

DNS查询失败错误页面，使用 Chrome 浏览器为例



This webpage is not available

[Hide details](#)

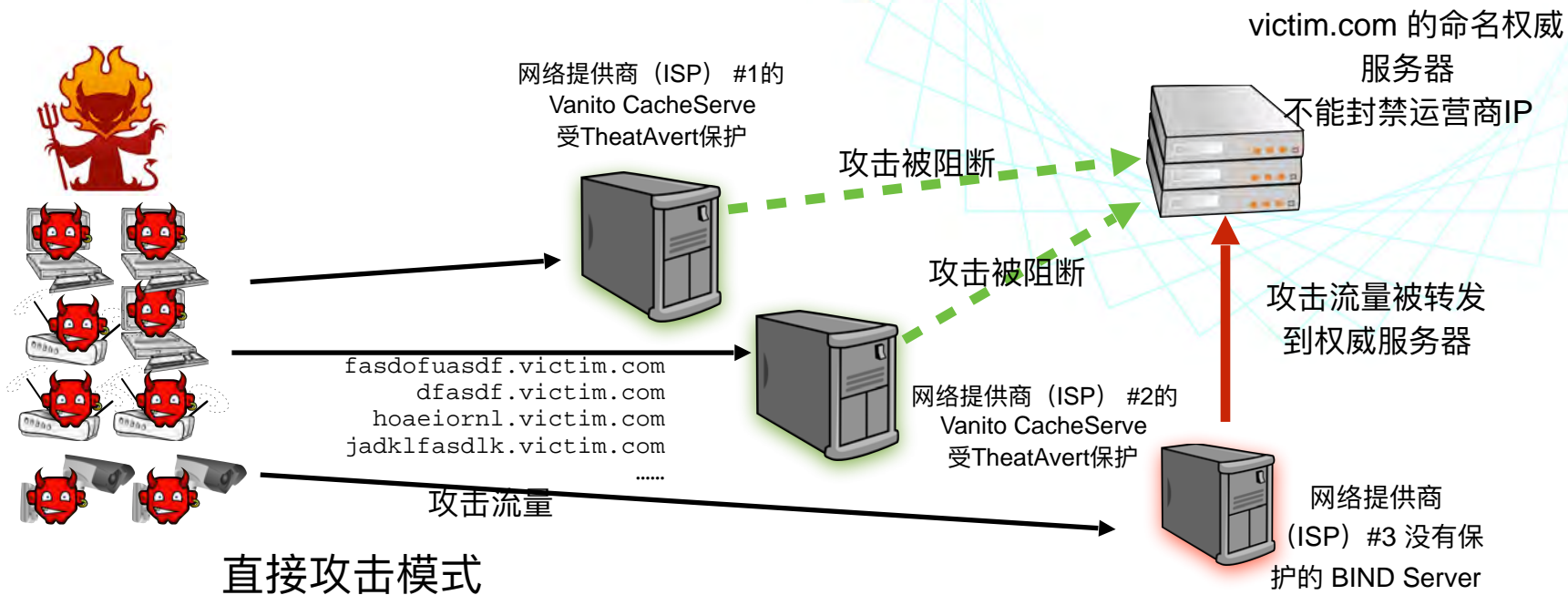
Reload

The server at **example.com** can't be found, because the DNS lookup failed. DNS is the network service that translates a website's name to its Internet address. This error is most often caused by having no connection to the Internet or a misconfigured network. It can also be caused by an unresponsive DNS server or a firewall preventing Google Chrome from accessing the network.

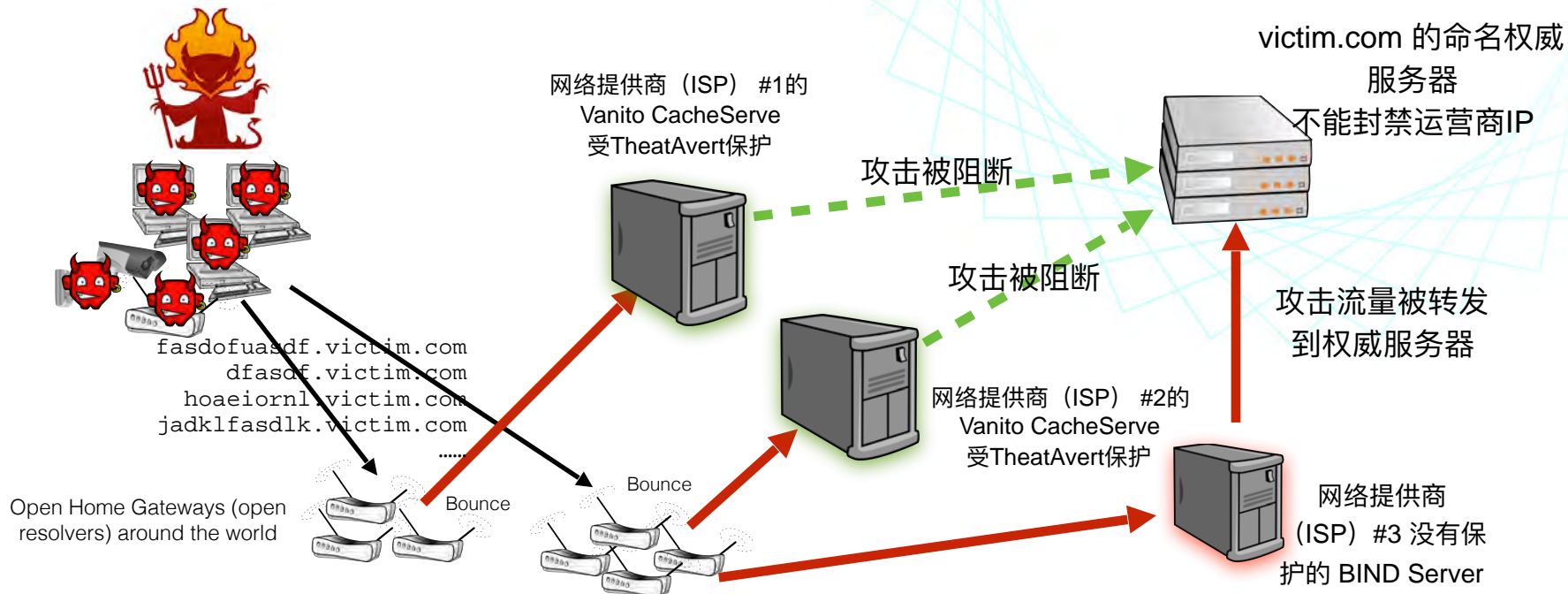
Error code: DNS\_PROBE\_FINISHED\_NXDOMAIN



# 随机域名攻击方法



# 随机域名攻击方法



开放解析反射攻击模式

# DNS：DDoS防护的阿喀琉斯之踵

- DDoS防护：木桶效应的典型例子。
- 高防服务器：流量打击的有效清洗。
  - 但仅贡献了木桶里比较高的木板。
- DNS服务器是软肋：查询资源比带宽更脆弱
  - 一个权威服务器服务多个域名
  - 运营商解析服务器承载所有域名缓存和递归。
    - 部分运营商还在DNS架构上节省必要费用
- 组合套路：随机域名攻击伴随其他攻击



“在一出生之时其女神母亲便将其捉住脚踝放入冥河斯堤克斯里浸泡，但由于抓住的脚踝没有沾水而使其成为日后的弱点，除去此处之外阿喀琉斯全身近乎刀枪不入，更是有著超越凡人的战争智慧与强大力量，只要他出战希腊联军在他的领导下就战无不胜。”

“阿喀琉斯最后被赫克托耳的弟弟特洛伊王子帕里斯在太阳神阿波罗指点下用箭射中脚踝，希腊人的第一勇士因此而死去。” <https://zh.wikipedia.org/zh-hans/阿喀琉斯>

# 攻击目标和连带损失

- DNS基础设施最不受保护。
- 攻击目标：权威命名服务器 Authoritative Server
  - 消耗查询资源而非带宽，迫使终止域名解析
  - 同服务器上的其他域名都被牵连
- 连带损失：运营商DNS递归缓存
  - 利用网络运营商DNS递归缓存服务器当跳板
  - 消耗递归资源，拖慢或阻止所有域名查询
- 域名所有者和用户：效果等于断网
  - “我付了你几百万你还让我断网？”
  - 断网远比速度慢更可怕。



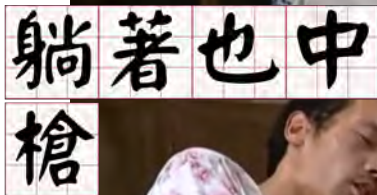
<https://www.pinterest.com/pin/487514728382523487/>

# 攻击目标和连带损失



Credit: Instagram GrumpyCat

Auth Server 提供商  
(云服务商)



Credit: 情景喜剧《我爱我家》

网络服务提供商  
(ISP)

域名所有者



Credit: 电影《少林足球》

用户



Credit: 百科“断网”词条



# PRSD引起的几次重大事故

- 2014年12月初，全球各地DNS解析失败
  - 记得那天连淘宝和百度首页都上不去吧？
- 2015年3月，Rutgers大学全校网络瘫痪
- 2016年12月，德意志电信瘫痪
- 2017年1月，英国劳埃德银行网络银行瘫痪



<http://www.bbc.com/news/business-38594058>

# 技术细节





# PRSD A、B、C、X型和其他杂鱼

PRSD-A

2014年初至今  
变长二级域名  
肉鸡+反射结合  
多攻打国内目标  
规模很大

PRSD-B

2014年底至2015年中  
大小写混合二级域名  
摄像头等物联网设备  
多攻打国外游戏站  
规模很大

PRSD-C

2016年夏天至今  
固定长二级域名  
摄像头路由器等物联网设备  
规模很大  
它叫Mirai

PRSD-X

2015年至今  
变长二级域名  
攻击高排名域名  
规模小

PRSD-copycat

2014年至今  
变长二级域名  
肉鸡  
规模小

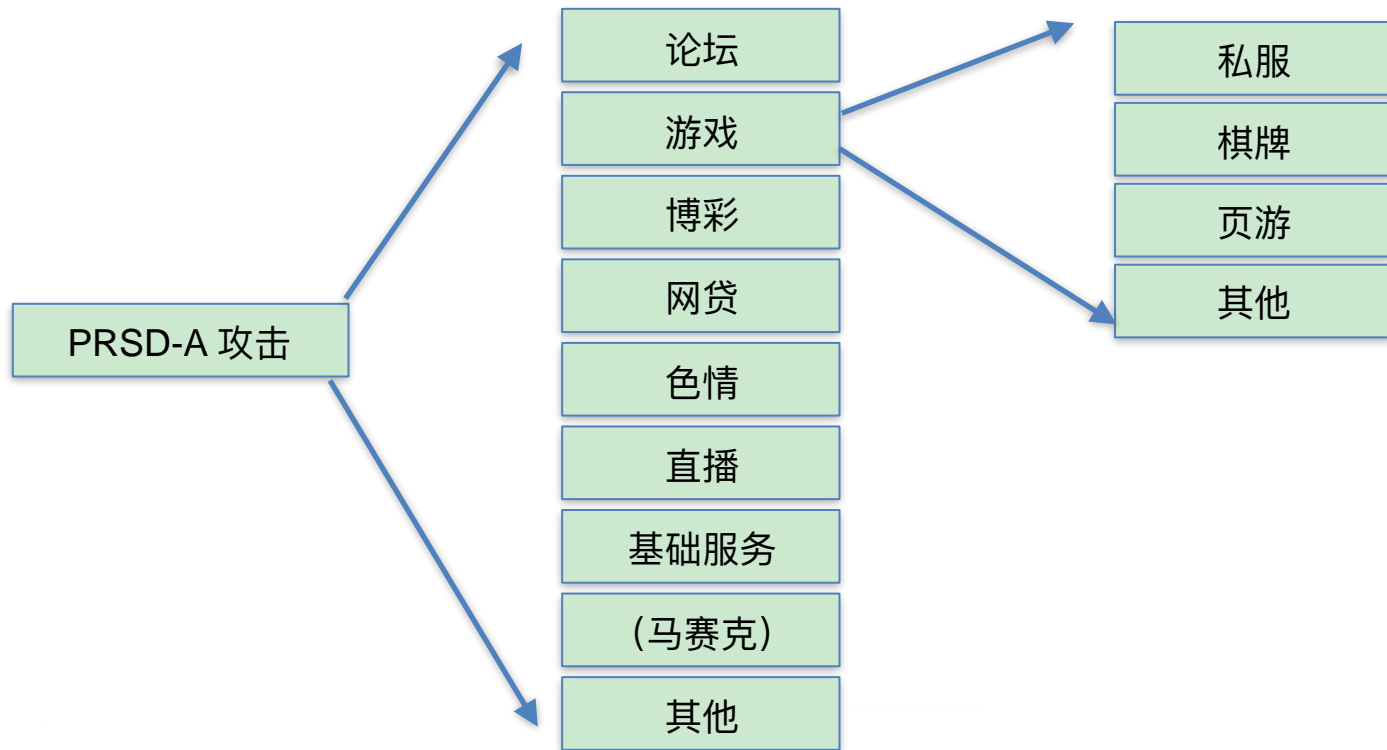
# PRSD-A

- 攻击目标：游戏、博彩、直播、保健品、色情等。
- 攻击特性
  - 全球范围僵尸网络加开放解析反射
  - 持续时间较长（几小时到几周）
  - 全球同步攻击
- 随机域名
  - 变长随机域名，2-16个英语字符
  - 随机生成器效率较低，有实现漏洞导致随机序列可快速检测
  - 我们称之为伪随机域名攻击 Pseudo Random Subdomain attack



<https://www.pinterest.com/pin/54606214207071359/>

# PRSD-A的攻击目标细分



# 攻击开始第一分钟的流量变化

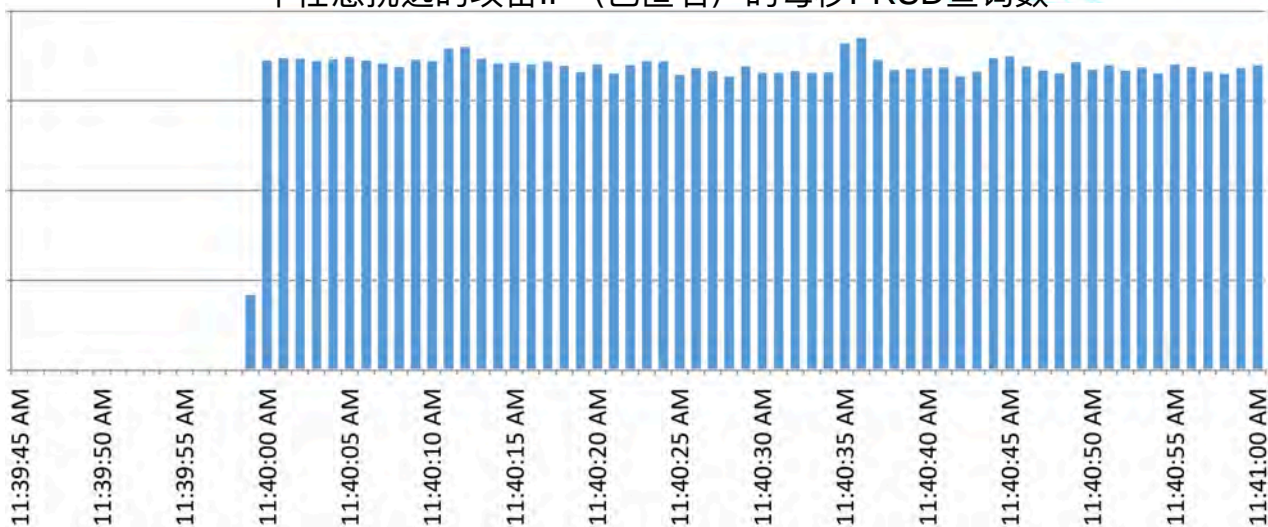
\* 利用Nominum全球观测流量获得

\* Nominum Security Report

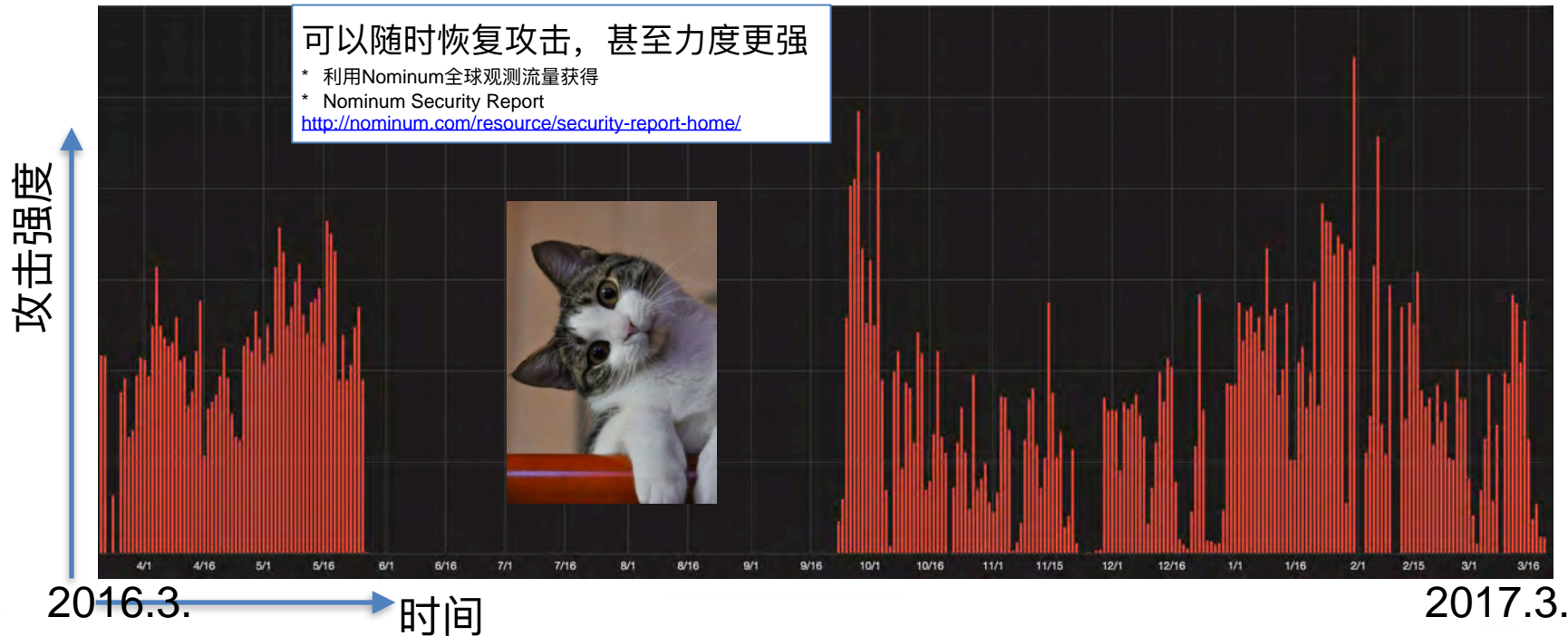
<http://nominum.com/resource/security-report-home/>

攻击者没有留给运维任何反应时间，必须自动化阻断

一个任意挑选的攻击IP（已匿名）的每秒PRSD查询数



# PRSD-A 的趋势变化（最近一年）



# PRSD-B

- 攻击目标：不定，多为接单打Minecraft等游戏网站，但是攻击过高价值目标比如学校、著名电子商务等。
- 攻击特性
  - 2014年出现的第一个大规模用物联网打PRSD的僵尸网络
  - 利用 Shellshock + busybox，多为摄像监控设备
  - 攻击力度极大，远超过PRSD-A四五倍
  - 大规模打击可以造成全球断网（2014年12月）
- 随机域名
  - 数字大小写混合英语字符
  - 随机效率很高，随机数生成均匀
  - 但是忘了DNS基本知识导致模式可预测

```
{random}.proxypipe.net.
{random}.93ERBlfD.iphop.info.
{random}.util.proxypi.pe.
{random}.extronus.net.
{random}.vdos-s.com.
{random}.arkhamnetwork.com.
{random}.getfastinstagramfollowers.net.
{random}.arkhamnetwork.org.
```



**DNSPod** V: #DNSPOD公告# 广大用户朋友们，目前全网的运营商正在遭受来自僵尸网络的反射攻击，造成全网用户的DNS解析成功率降低，包括使用DNSPod进行解析的域名，还望周知！ @乌云-漏洞报告平台 @36氪 @互联网的那点事 @七牛云存储 @安全宝 @奶罩 @墨猫Caroline @Fengng @caoz



连带损失：攻击目标域名均不在DNSPod上，但是它躺着中枪了，因为运营商中枪了。

2014-12-9 23:14 来自 微博 weibo.com

124 43 7

<http://weibo.com/1644913943/BAbK7C4b0>

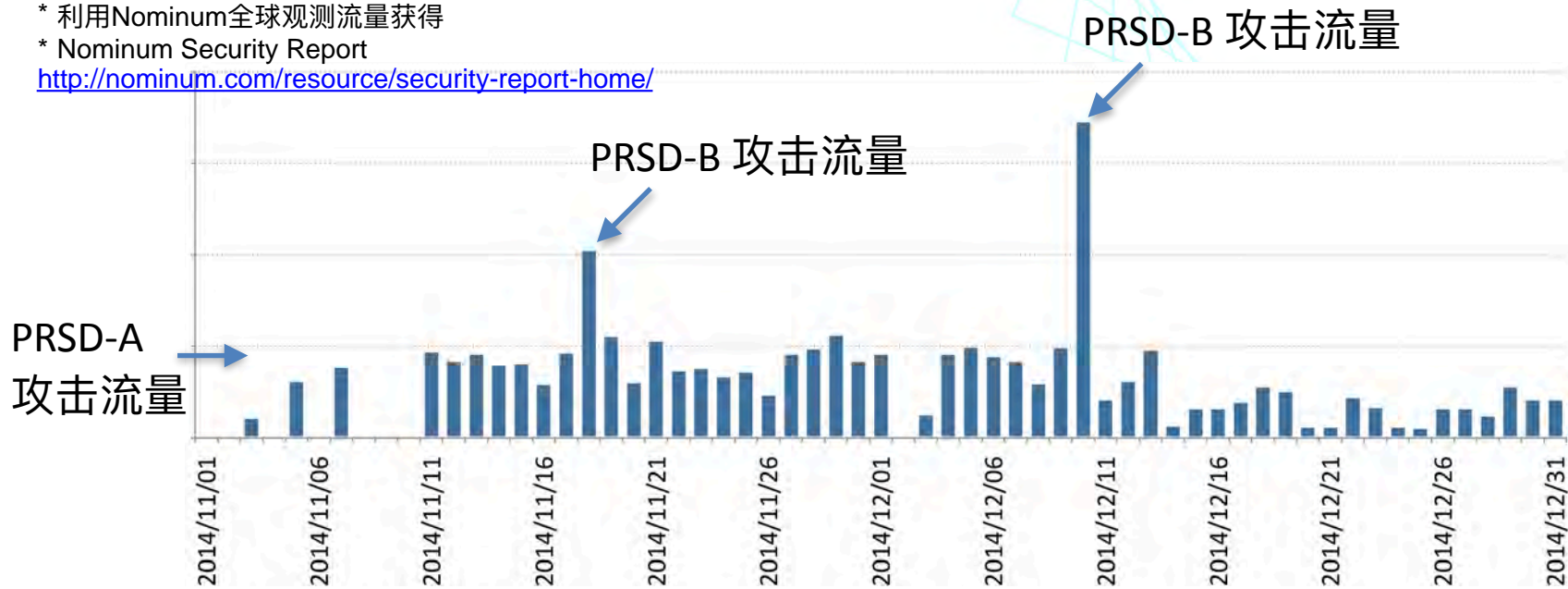


# A型和B型的攻击强度对比

\* 利用Nominum全球观测流量获得

\* Nominum Security Report

<http://nominum.com/resource/security-report-home/>





# PRSD-C

- 它就是著名的 Mirai 僵尸网络若干攻击方法之一。
- 攻击特性
  - 物联网设备攻击，B型继承者
  - 攻击效率很高，力度很大
  - 发起大规模攻击需要的IP远少于A型。
- 随机域名
  - 重用了部分PRSD-B代码
  - 自创固定长度随机域名 `[a-w0-8]{12}`
  - 随机效率较高，随机数生成较均匀
- Nominum 数据科学组在Mirai开源前三个多月观测并阻断PRSD-C



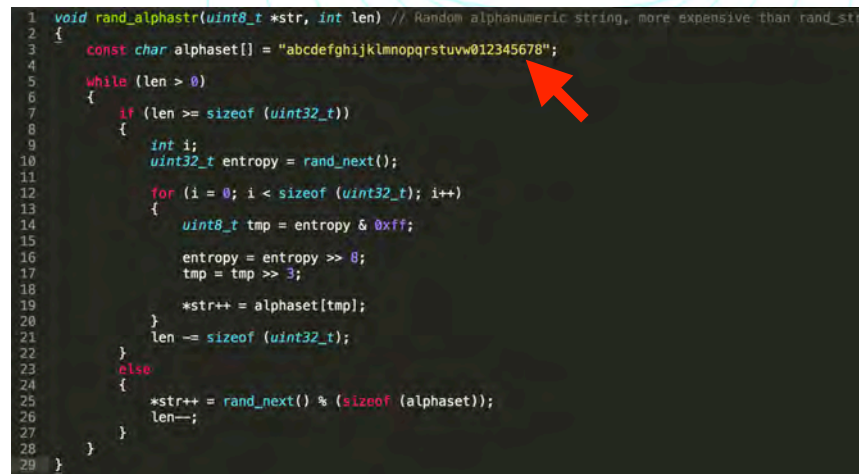
<http://www.boredpanda.com/cat-kimonos-japan/>

# 深入谈谈 PRSD-C

- 2016年7月中旬, Nominum数据科学组首先在数据中观测到 mc.arkhamnetwork[.]org viperhcf[.]com 等随机域名攻击并通过 N2 ThreatAvert 阻断。
- 2016年9月底, 观测并阻断 air-force[.]biz kladka[.]biz xxx24[.]biz 大规模攻击。
- 2016年10月底Mirai公开源代码, 对照确认PRSD-C攻击源。

## PRSD-C 攻击查询范例

uec0vakqfmuw.mc.arkhamnetwork.org.  
 60srufutupaq.mc.arkhamnetwork.org.  
 n16g8pvgwj3.mc.arkhamnetwork.org.  
 cbert8pa8c7u.mc.arkhamnetwork.org.  
 2i117grhej3t.mc.arkhamnetwork.org.  
 i4tita87hkes.mc.arkhamnetwork.org.  
 a611bjub2if.mc.arkhamnetwork.org.  
 skgihwjcnhrc.mc.arkhamnetwork.org.  
 a5qq26fid5mf.mc.arkhamnetwork.org.  
 ...



```

1 void rand_alphastr(uint8_t *str, int len) // Random alphanumeric string, more expensive than rand_str
2 {
3     const char alphasets[] = "abcdefghijklmnopqrstuvwxyz012345678";
4     while (len > 0)
5     {
6         if (len >= sizeof (uint32_t))
7         {
8             int i;
9             uint32_t entropy = rand_next();
10            for (i = 0; i < sizeof (uint32_t); i++)
11            {
12                uint8_t tmp = entropy & 0xff;
13                entropy = entropy >> 8;
14                tmp = tmp >> 3;
15                *str++ = alphasets[tmp];
16            }
17            len -= sizeof (uint32_t);
18        }
19        else
20        {
21            *str++ = rand_next() % (sizeof (alphasets));
22            len--;
23        }
24    }
25 }
    
```

<https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/rand.c>

# PRSD-X

- 攻击特性
  - 攻击效率很低，力度很小，攻击IP数很少
  - 多攻击高排名域名及后端服务域名
  - 疑似子域名爆破
    - 目标并非阻止查询而是其他
- 随机域名模式
  - 字典+短随机字符串
  - 常见汉语拼音组合
  - 字典创造者的英语可能不太好

## PRSD-X 攻击查询范例

34tp.instagram.com.  
aomenlvyouquangongglue.instagram.com.  
3ka2.instagram.com.  
2try.instagram.com.  
3flc.paypal.com.  
888zaixianzhenrenyule.paypal.com.  
44538.paypal.com.  
315175.paypal.com.  
ardec-sit.uber.com.  
3vks.uber.com.  
alexanderbobadilla.uber.com.  
9g35.uber.com.  
998guanfang.uber.com.  
aeroflot.uber.com.  
am5a.netflix.com.  
3jse.netflix.com.  
88yulechengbocaiwangzhan.netflix.com.  
39-7.netflix.com.  
39zk.netflix.com.  
8586d.netflix.com.

# PRSD其他杂鱼

- 一些局部地区的小规模攻击
  - 攻击力度较小，使用IP较少
  - 也被检测并阻断。
- 仅简单列举当作参考，不作深入讨论。

## PRSD-copycat 攻击查询范例

vwoe.hao0039.com.  
xcsj.hao0039.com.  
hbgr.hao0039.com.  
peeh.hao0039.com.  
dohqyw.hao0039.com.  
cfdbdr.hao0039.com.  
iuwaws.hao0039.com.  
qwktbv.hao0039.com.  
vzzuer.hao0039.com.  
uysrvh.hao0039.com.

# 一些神奇的无效 PRSD 攻击流量

部分攻击目标已匿名马赛克处理

- {random}.http://118.184.[???].2:30001. DNS和http不是一个协议
- {random}.118[??]t.com:80. DNS查询不用端口号
- {random}.\032vmobai.[??.aliyungf.com. DNS查询不允许空格 (\032)
- {random}.v5[??.com\032. DNS查询不允许空格 (\032)
- {random}.104.85.[???].1. DNS查询不能用IP
- {random}.l.root-servers.net. ROOT用PRSD打不下来
- {random}.cpsc.gov. 反射放大攻击不用和PRSD组合
- {random}.akamaiedge.net. Akamai等大厂光用PRSD打不下来

啥叫干一行 爱一行



电影《疯狂的赛车》截图



# 防护措施





# 检测和阻断

- 网络服务提供商（ISP，递归和缓存服务器）与云服务商（auth server）联手阻断。
- 实时检测攻击流量并自动阻断。
  - 想一想攻击开始第一分钟的流量图
- 最重要的：让合法查询通过
  - 细粒度规则是问题的关键。
  - 阻断攻击流量，放行合法查询



<https://www.qwertee.com/product/grumpy-cat-you-shall-not-pass-dog>

# 网络提供商常见问题

## 无视派



假装没看见  
缓存服务器资源耗尽  
所有合法查询被丢弃

## 黑洞派



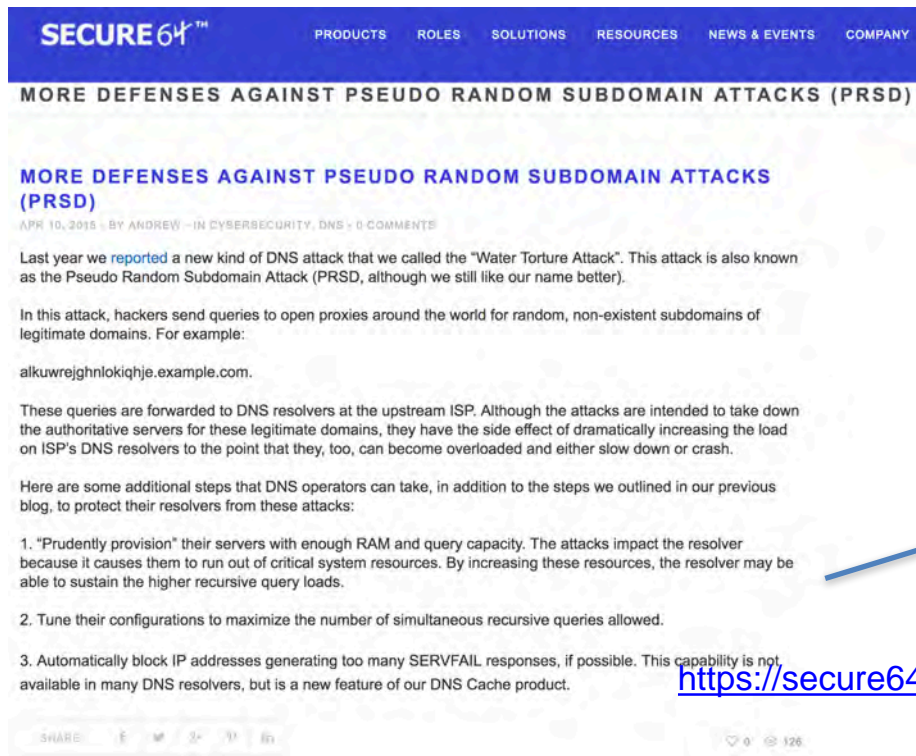
运维24小时轮班监测  
被打域名查询全部丢掉（包含合法），保住小命要紧，  
即使云端权威服务器防护住，运营商被迫中止服务。

## 过滤派



想当个好猫，建立细粒度过滤阻断规则并让合法查询通过，  
但是怎么建呢？

# 我能无视攻击让服务器硬抗么？



抗不住，但是有人还是硬要抗，  
比如Secure64

Secure64的解决方案：加内存，加大递归并发数，自动封禁太多SERVFAIL请求的IP  
(并且自我感觉良好)  
但是这不解决问题，只是拖延

<https://secure64.com/defenses-pseudo-random-subdomain-attacks-prsd/>

# 给黑洞派的提问

如果十一月某天凌晨在报警日志看到 `{random}.alipay.com` 该怎么办？  
我觉得你知道答案了。

# 建立细粒度过滤阻断系统的常见问题

- 当攻击开始时候才分析该域名数据?
  - 太迟了
- 让缓存 / 解析服务器决定?
  - 偏差 (bias) 太大, 覆盖不全可能导致误杀
  - 全球数据才可以保证全面精确判断。
- Nominum 数据科学组从全球数据里实时作细粒度分类分析判断合法查询。



[http://www.funnykittensite.com/pictures/kitten\\_fight.htm](http://www.funnykittensite.com/pictures/kitten_fight.htm)



# 云服务商 (Auth server) 常见问题

- 硬抗：200G? 500 G? 1T? 10 T?
- 不作细粒度过滤
  - 部分云服务商的 auth server没有设计细粒度阻断过滤规则的功能
  - 其实等攻击流量到达 auth server 时，攻击已经完成了
- 和网络提供商 (ISP) 互相独立
  - 必须互相帮助，建立细粒度阻断过滤规则系统

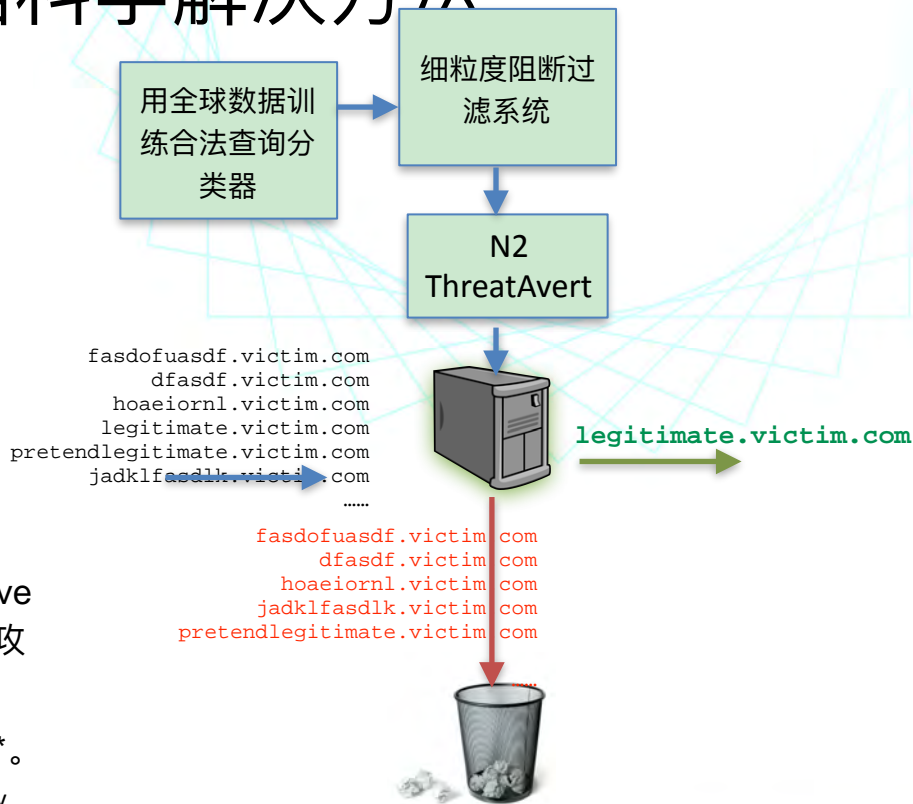


<http://favim.com/image/3753087/>

# Nominum 的数据科学解决方法

- 检测：Kafka实时全球DNS查询数据流检测
  - 实时记录每个域名的独立子域名数
  - 秒级检测PRSD攻击
  - 不需要利用任何预设随机字符模式。
- 细粒度阻断过滤系统：精确阻断攻击和释放合法请求
  - 实时分类器判断合法DNS请求
  - 拥有全球数据，全面覆盖
- 推送并自动作出细粒度阻断和过滤
  - 结合 N2 ThreatAvert, Nominum Vantio CacheServe 能在网络提供商（ISP）服务器端阻断所有 PRSD 攻击流量并通过合法流量。
  - 细粒度阻断过滤系统可以单独提取供其他服务使用\*。

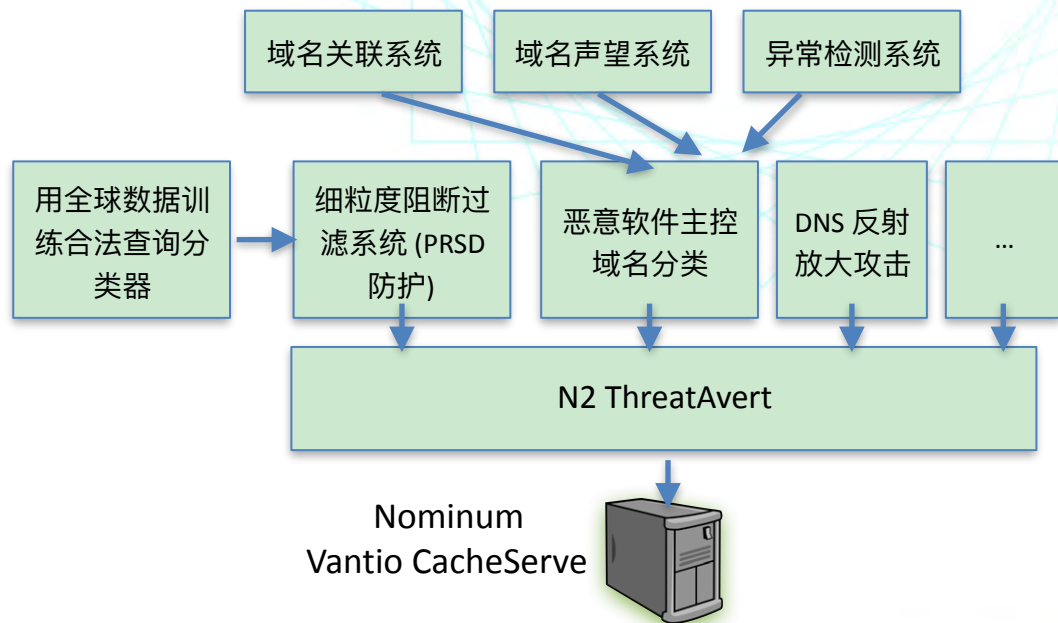
\* conditions may apply





# 简单点：用 N2 ThreatAvert

- 给网络服务提供商最简单的解决方案。
- Nominum 数据科学组全面支持。
- 从全球实时数据里检测各种威胁并自动推送到运营商缓存 / 解析服务器作实时阻断。
  - 包含 PRSD 等多种威胁。
- 正全面保护全球多家大型主要网络提供商的DNS服务和用户安全。



# 总结

- 随机域名攻击DDoS防护中的软肋：DNS
  - 多种形态的攻击并存于市场，攻击随时发生
  - 云服务商和网络提供商都需要做好防护
- 检测和阻断方法
  - 通过独立子域名计数检测随机域名攻击
  - 利用全球数据建模的细粒度阻断和过滤系统精确打击攻击流量
    - 拥有全球全面数据的重要性
- N2 ThreatAvert 提供本议题提到的保护方法
  - 实时检测并推送细粒度阻断过滤规则
- 本议题提到的方法已申请多项专利。
- Nominum 期待和各位的商业及研究合作。



\* Nominum Security Report

<http://nominum.com/resource/security-report-home/>

# 联系我们

- Email: hongliang.liu@nominum.com
- Company website: <http://nominum.com/>





用好手上数据，做一些微小的贡献