恶 意 域 名 识 别 与 分 析

预测发现未知威胁的能力

美国2013年国防预算法案

Sec.932 国防部下一代主机网络安全系统

1. 为克服现有系统能力的问题和局限，(下一代)系统应不依赖于(会导致下列问题的)技术：

   a) 不能应对新的或快速变形的威胁；

   b) 消耗大量通信带宽，以保证更新至最新已知威胁库，并报告最新状态；

   c) 消耗大量资源，以存储高速增长的威胁库。

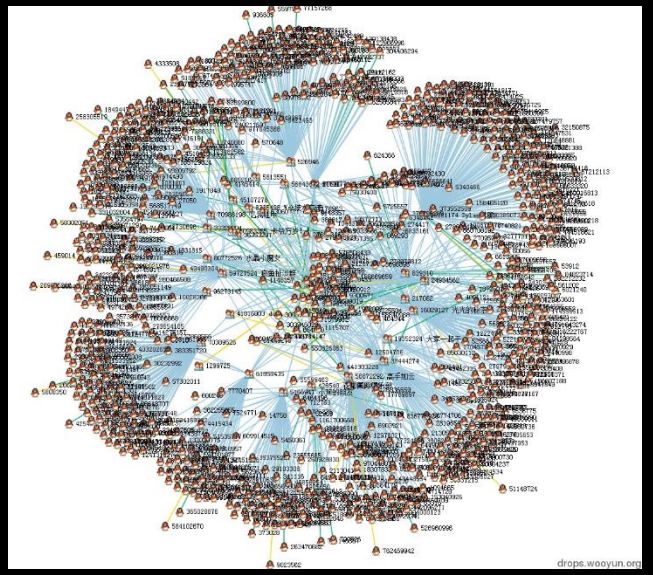
美国众议院军事委员会对国防预算法案的异议

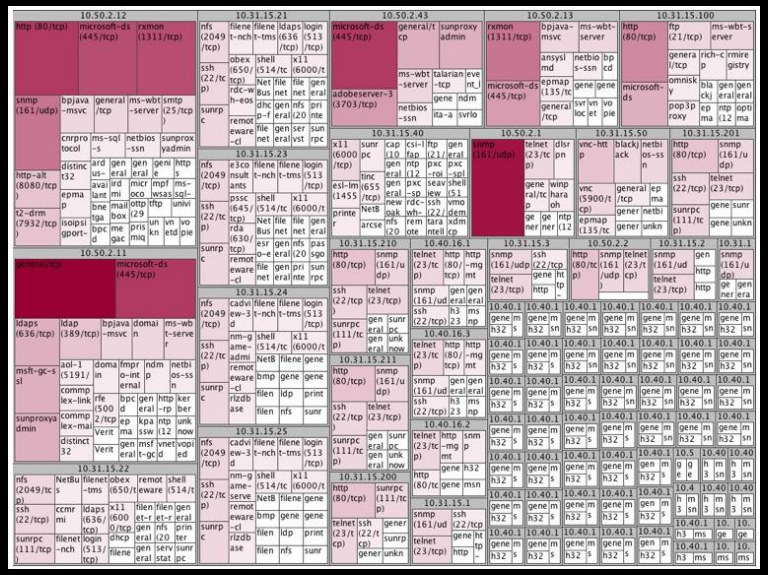
检测尚无识别特征的网络威胁

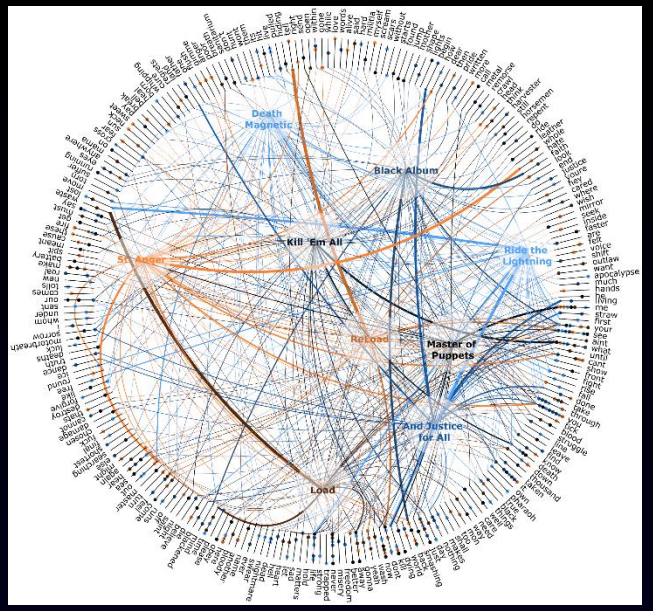
委员会担忧，国防部没有提供充足的资源，以获取检测和防护尚未取得识别特征的网络威胁的能力。实时检测并防御尚无识别特征的威胁的需求一直存在，且应能运行于高带宽的网络，也应能评估网络流量以发现恶意活动。委员会注意到，现在已有能满足此需求的技术出现，但需要额外的开发和测试，以及运营评估。委员会建议国防部迅速建立一个流程，以发现、测试、和评估潜在解决方案，并加速这些技术的采纳和实施，以满足这一迫切需求。

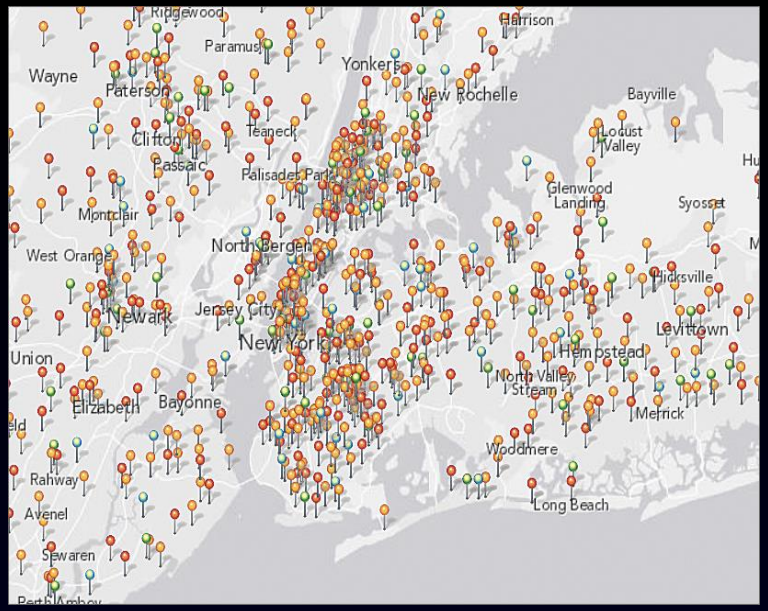
cirrusgate.com

有大数据就足够了吗？









只见森林大海捞针

发现未知威胁，你需要一条线索

nfcxhxdttc.cn

nfcxhxdttc.cn

2015年6月21日 - 内网DNS解析请求

Conficker

2008年11月

.A

- 随机生成 250 个域名/天
- 5 个TLD
- 尝试连接所有域名

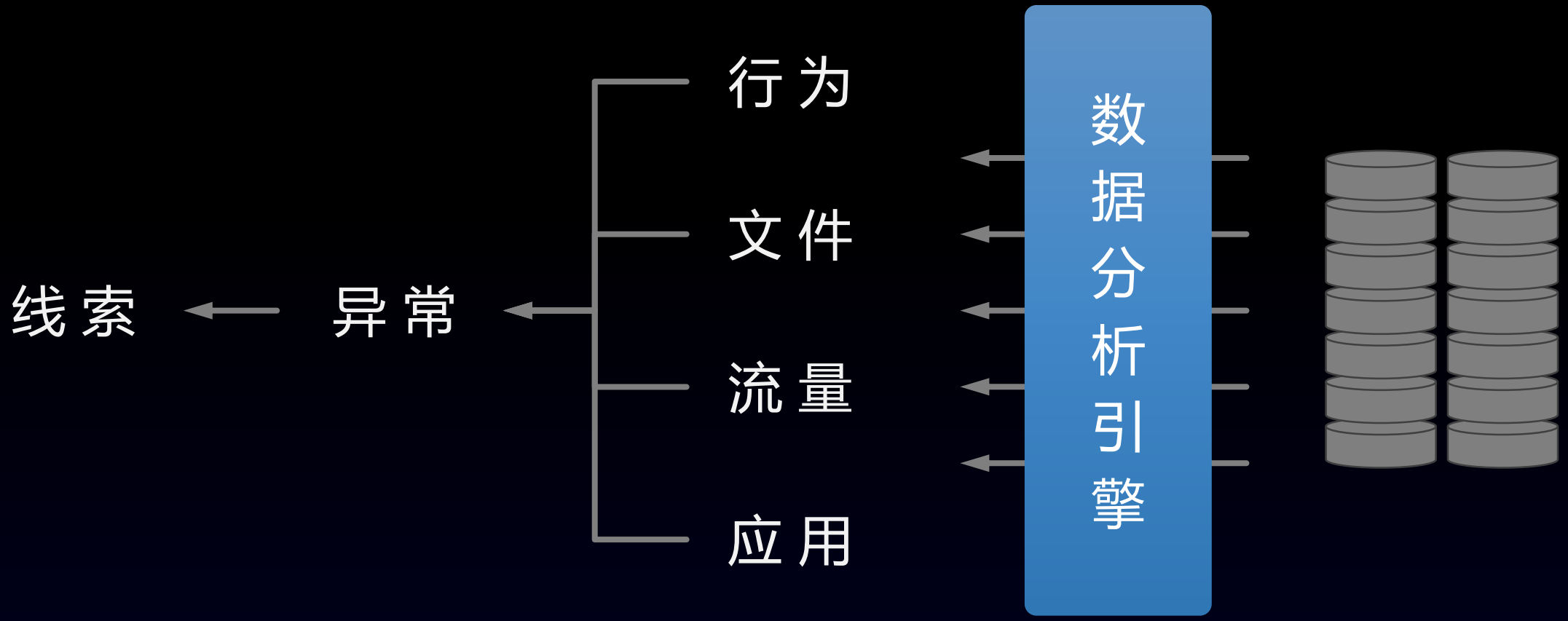
.D

- 随机生成 50,000 个域名/天
- 110 个TLD
- 随机尝试连接 500 个/天

跟踪线索定位威胁


域名解析请求
nfcxhxdttc.cn
DNS日志
192.168.20.157
CSIRT检测
确定Conficker感染
终端Z

发现未知威胁，你需要一条线索



线索与威胁情报

Domain Name Object

nfcxhxdttc.cn

域名生成算法DGA用于C&C联络

Cryptolocker	Gameover Zeus
qnqgkouekldintl.net	il6ytoywktgp8xv3ve1j3av1v.net
eppgftqgclxcnpk.biz	t5rr78orl5hw12yheez187kkui.com
rosfjxmtnwxynff.ru	9x8t00yk5xhfaw0s0a149r2xk.biz
fqrfedivfwsseom.org	knvqi4fh8yyx13dja5p10mwpww.com
spvkivucmxqfcee.co.uk	gcsqzp1nybe4ssw2hzrwructz.com
grukdbqeexlychh.info	1qtkve01cjzsju1hvcsi9d4mmvv.org
tqxjhfmrpjlvjih.com	tqms0g1rr25lmsf61hhseu3jc.com
hswjckithjgpays.net	ch9quv19fwudc114755d3anvbg.org
ugywcyndspvscaq.biz	4czl1m1iarfcz1o4ssl6cz3eb6.biz
vtxlfehkkmeikgx.ru	dvs9mfhuhphv1jxw4ovdwqv7r.net
vhbvbifsvbqjcws.org	dbz9th1udt7i310igjatir5c85.com
wuakenyanxyybtr.co.uk	e5pfzy16huhygttl5w0sj3wky.net
wiebagnbucjpceq.info	2dn4pf1fqa6ivsqm2vx19j9knh.biz

DNS隐蔽隧道上传关键数据

杀毒软件合法回传样本特征

16-0.19-a3000000.10082.1644.976.3ea3.410.0.6bq4kprjdsbmpkj2kvtanwl1db.avts.mcafee.com

FrameworkPOS木马上传信用卡数据

[Unique ID].beacon.[Encoded IP].[Encoded Hostname].[C&C Server].[TLD]

[Unique ID].alert.[Encoded App Name].[C&C Server].[TLD]

[Unique ID].[Encoded Credit Card Data].[Encoded Credit Card Data].[C&C Server].[TLD]

上传关键数据的线索

dacsjmxlt7p53j8p775hc.nam9hi6nqcc4j6e6wo7d25.56.85h5.com

onmg5rfhnrvam7554qxue5p55n.9i9jpu9uc96ovgbpebog8up69a.56.nbgtr.com

x8p3ux2hao7ngoi9vrinr445k8.l2os599igokrhlire5uiofx2oa.56.vcxde.com

Domain Shadowing

> 域名阴影，利用失窃口令的正常域名账户，大量创建子域名进行钓鱼攻击。此恶意攻击手法非常有效且难以遏止。因为防御方无法获悉下一个被黑客利用的账户，所以几乎没有办法预测下一个受害者。

www.taiyangchengyulechengweiyibo.386jg.z[redacted].gov.cn	太阳城娱乐城伟易博
www.tangrenjieyulechengxianshangduchang.3g9sk.z[redacted].gov.cn	唐人街娱乐城线上赌场
www.zuixindianyingzaixianguankan.s8z1n.z[redacted].gov.cn	最新电影在线观看
www.zhifubaotikuandecaipiaowang.l[redacted].gov.cn	支付宝提款的彩票网
www.shuangseqiuyucezhuanjiashahaocaijing.l[redacted].gov.cn	双色球预测专家杀号彩经

采用混淆手法的钓鱼域名

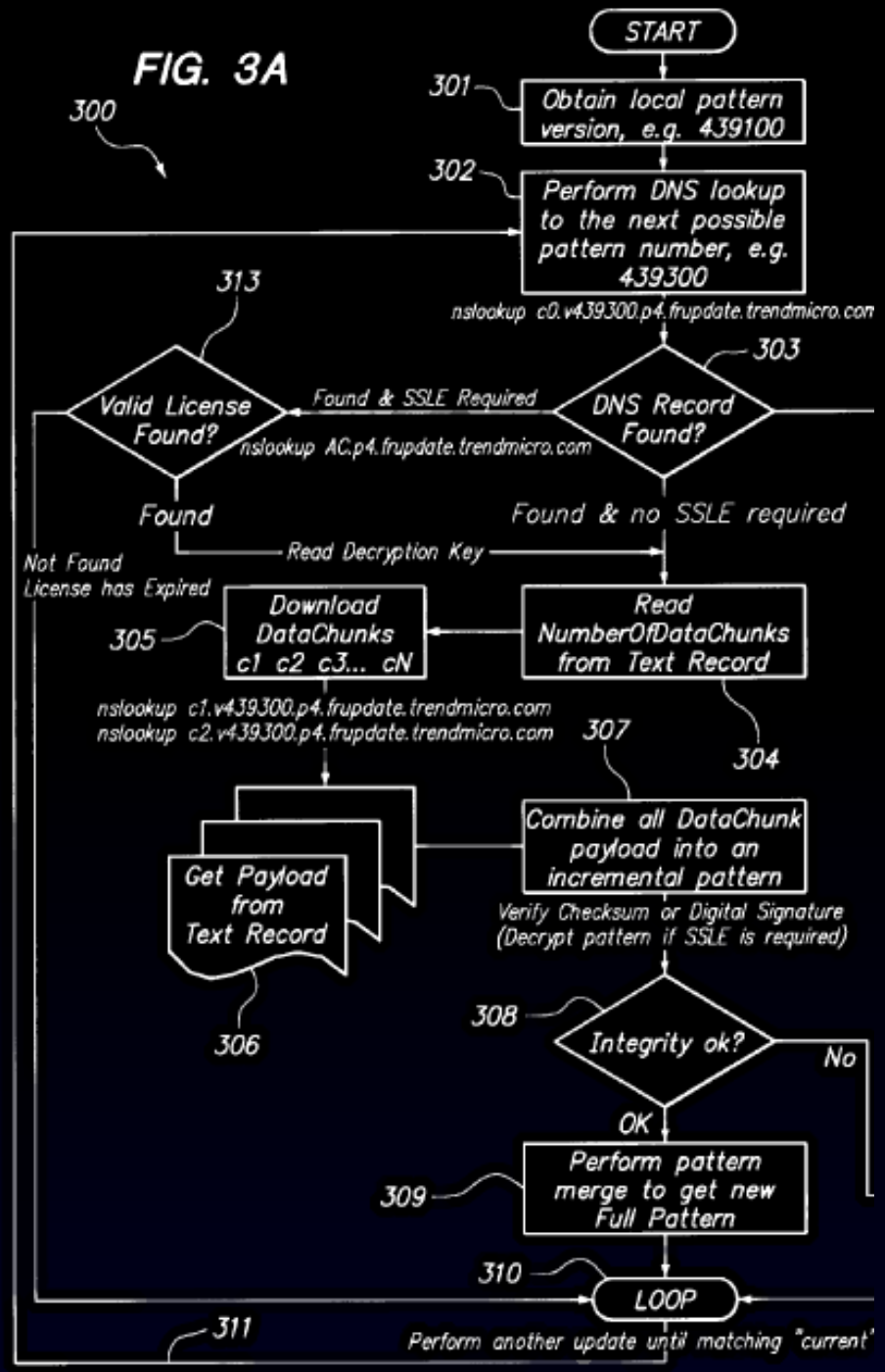
www.taobao.com.4q7p1.ejwir.**alipey-nnc**.com
www.taobao.com.smdb6.uo68z.**alipey-nna**.com
www.taobao.com.wudn0.gb6kc.**alipey-ncc**.com
www.taobao.com.e8cmh.5a7o2.**alipey-crc**.com
www.taobao.com.i067z.1czwf.**alipey-ccc**.com
www.taobao.com.i37l8.1xwla.**alipey-cvc**.com

域　　名: alipey-crc.com
注册日期: 2015-06-19
发现日期: 2015-06-20

利用TXT记录
下载指令和payload

Updating Of Malicious Code Patterns
Using Public DNS Servers

United States Patent US8171467



恶意域名作为线索

正常

- 符合语言习惯
- 容易记忆
- 有语义特征
- 使用记录符合通常习惯
- 时间长，使用稳定

异常

- 难以发音阅读
- 无法记忆
- 内容无意义
- 恶意使用记录的特征明显
- 创建时间短，使用不频繁

企业内发现恶意域名的价值极高

- 直指被入侵设备
- 发现未能防御的未知威胁
- 关联性和及时性完胜信誉库

基于已知特征的信誉库
的实际效果如何？

恶意网址识别率

APWG

14 %

28 %

Bit.ly 对流行信誉库的实际测试

利用先进技术
在海量DNS数据中发现恶意域名

自然语言处理

机器学习

数据挖掘

算法组合与特征选取

- N-grams
- Random Forest
- Levenshtein Distance
- 自有算法库
- C4.5
- Adaboosting
- Word Segmentation

发现异常域名就结束了吗？

4000万

某省24小时唯一域名数量

60万

发现异常域名数量

帮助安全人员更好地使用线索：

恶意域名分类分析

分类标准

- 威胁机制
- 相同来源
- 攻击品牌
- 创建特征

目的

- 线索的易用性
- 直观可视化
- 与其它系统关联分析
- 更深入数据挖掘的基础

数量级要降到安全人员可以分析

4000万

某省24小时唯一域名数量

60万

发现异常域名数量

~100

异常域名分类线索

发现DNS隐蔽信道下载payload

- TXT记录长度有限，需要多次查询才能拼接payload
- 同一终端频繁发送同源恶意域名解析请求
- 自动批量查询同源恶意域名组TXT记录
- 是否存在多个下载数据长度超过100字符情景
- 与正常记录不同的字符使用组合

应用场景广泛才能成功

高性能

- 单线程性能：>20万条/秒

嵌入式

- 模块化嵌入SIEM、NGFW、AV 、Sandbox等
- 小型化、轻资源消耗

易扩展

- 计算节点横向扩展配置简单
- 算法和规则库升级快速便捷

产品化中的工程难点

- 拼音和数字域名（360、51、kaixin001）
- 白名单的稀缺和不可靠
- 缺少可供机器学习的国内样本
- 不规范的域名滥用现象（xshzzxx.net）
- 易用的人机交互界面

复杂的域名生态环境：经验与知识的积累

login.live.com.nsatc.net

cdn.marketplacecontent.windowsphone.com.nsatc.net
www.update.microsoft.com.nsatc.net
login.passport.com.nsatc.net
v4windowsupdate.microsoft.nsatc.net
eds-anon.xboxlive.com.nsatc.net
r.msn.com.nsatc.net
clientconfig.microsoftonline-p.net.nsatc.net
advertising.microsoft.com.nsatc.net
mobileads.msn.com.nsatc.net

应对高级DGA算法带来的新挑战

statement
account
transaction
live
mobile
secure
report
fraud
app
update
+ PayPal +
c1ient
transfer
manager
login
service
sh0p
feedback
checking
content
apis
customer

那些来不及讲的...

- 实时阻断与警告
- 与其它来源线索交叉定位入侵
- 揭示入侵路径和时间
- 威胁情报生产
- 安全服务