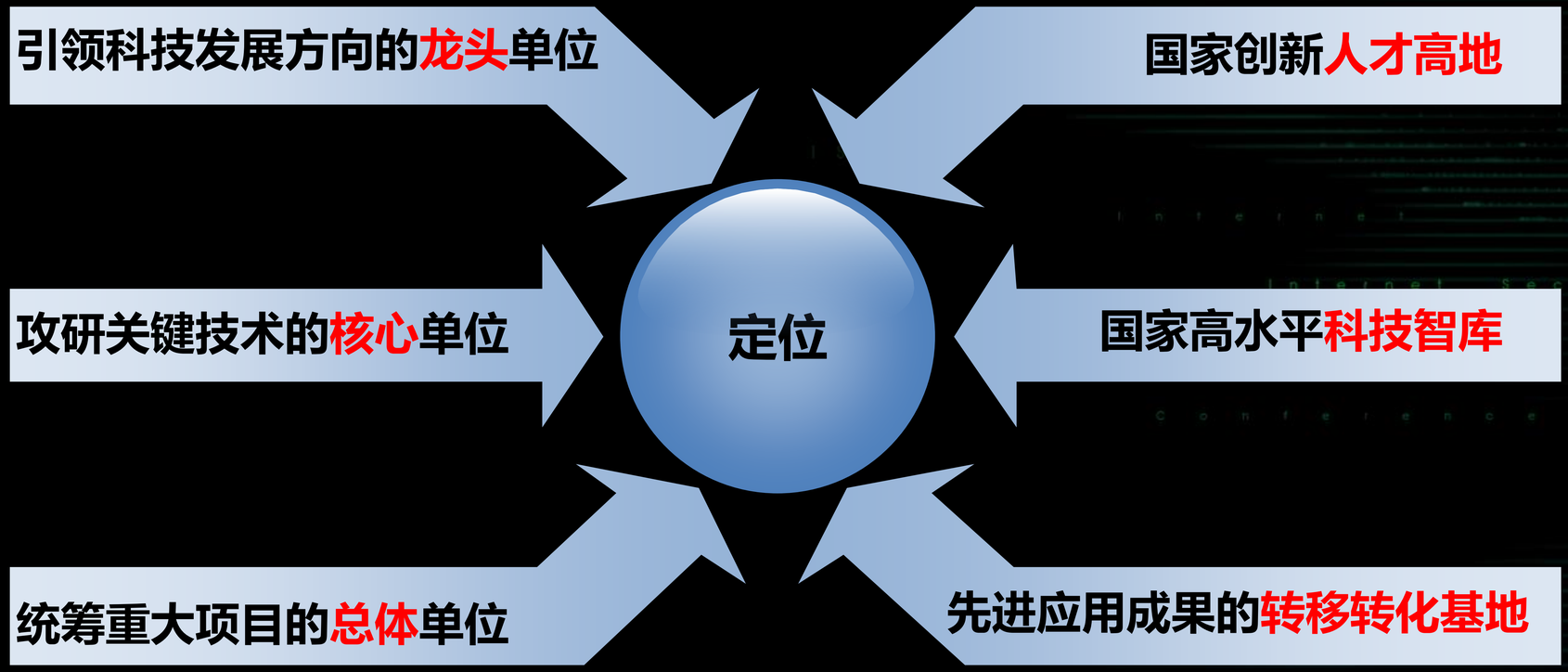
第七届互联网安全大会 360互联网安全中心

加密数据流量测量与行为分析

熊刚
中国科学院信息工程研究所
信息内容安全技术国家工程实验室
中国科学院大学网络空间安全学院
xionggang@iie.ac.cn

中国科学院信息工程研究所

中国科学院信息工程研究所是2011年批准成立的中国科学院直属科研机构。研究所面向国家战略需求，在网络空间安全科技领域，开展基础理论与前沿技术研究，开发应用技术与系统，为国家网络空间安全和信息化发展提供核心关键技术支撑与系统解决方案。研究所的定位：



口 第二实验室（信息内容安全技术国家工程实验室）

国家发改委首批批复的国家工程实验室之一，依托于中国科学院信息工程研究所是国家级科研创新基地。面向国家网络信息安全重大战略需求，研究突破相关理论与关键技术，研制重大系统，为国家网络空间信息安全保障提供技术支撑。

口信息内容安全技术国家工程实验室 简介

科研成果

项目支持：近五年承担科研项目253项，项目总经费累计达5.14亿元，来源包括科技部、发改委、工信部、国家自然科学基金委、广电总局、中科院、总参等。

理论技术：近五年发表论文共发表论文526篇，其中SCI收录/EI收录319篇，论文曾获顶级学术会议最佳论文等多项奖项；申请国家发明专利100余项，申请软件著作权30余项；制定标准7项。

应用及获奖：成果用于多个国家级重大工程项目中，为解决国家信息安全重大战略问题做出了显著贡献；成果曾获国家科技进步一等奖、国家科技进步二等奖和省部级以上科技奖励10 余项。

口 实验室简介

研究方向

- 内容计算信息过滤
- 数据挖掘与保密防护
- 网络靶场与态势感知
- 网络处理架构与测绘
- 网络行为分析与对抗
- 信息存储与异构计算

科研平台

信息内容安全技术国家工程实验室

第七届互联网安全大会 360互联网安全中心

目录

CONTENTS

第七届互联网安全大会 360互联网安全中心

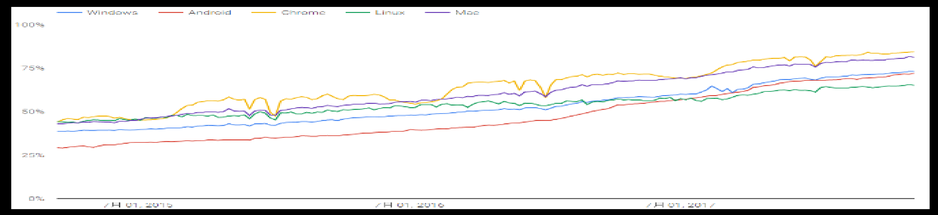
01

章节 PART

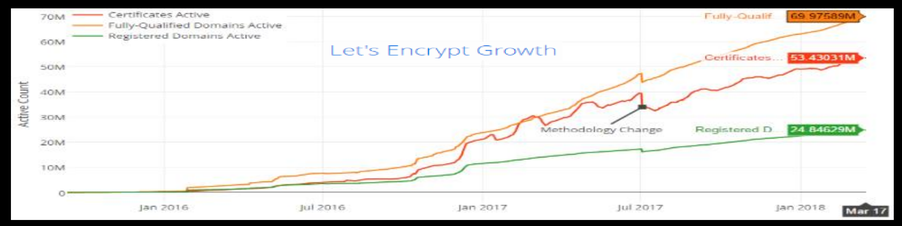
背景意义

网络数据流量全面加密化承载

人们的网络安全意识不断提高，在安全和隐私保护需求的驱动下，网络通信加密化已经成为**不可阻挡的趋势**，加密网络流量呈现**爆炸增长**。

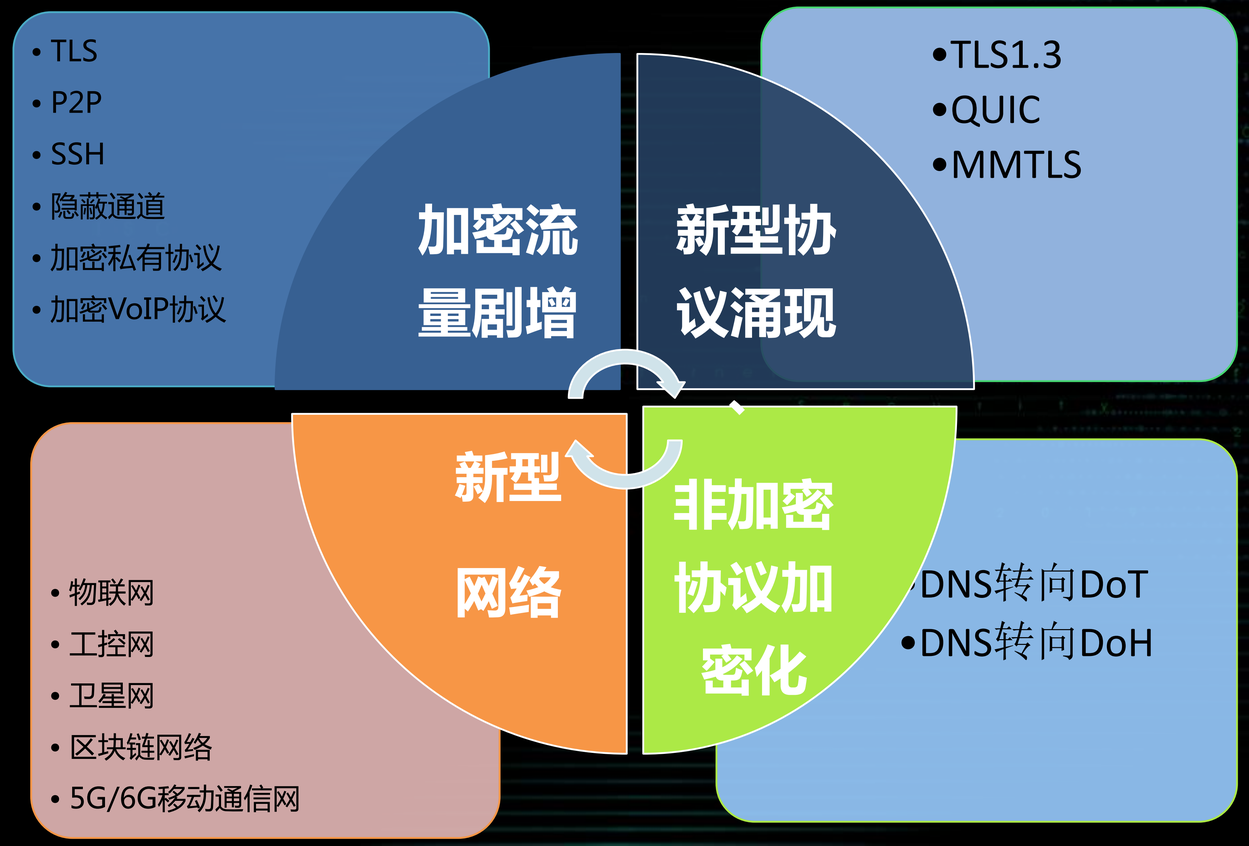


Chrome 中通过 HTTPS 加载的网页所占的百分比（按平台）



免费数字证书对加密的推动

CDN & 云服务的SSL/TLS加密支持



网络主流加密网络服务被滥用

□ 无处不在的网络黑产——爬虫、刷量、薅羊毛

1. 《新闻直播间》和《新闻30分》接连曝光网络黄牛集团背后的黑产链，仅10分钟刷走1245张的车票，几乎垄断一趟列车。
2. 支付宝扫码领红包被薅羊毛，高端玩家赚了几十万。

□ 恐袭当前，如何看待通信APP加密这把“双刃剑”

1. 2017年3月22日，英国首都伦敦的议会大厦外发生恐怖袭击事件，共造成5人死亡，40人受伤，其中7人伤势严重； 不法分子之间联系使用 Whatsapp。
2. 2017年4月，俄罗斯圣彼得堡地铁的自杀式爆炸袭击令15人丧生； 暴恐分子之间使用Telegram联系.

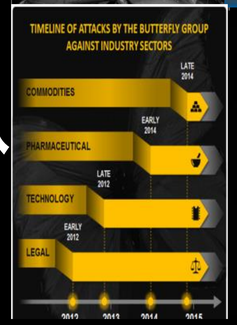
恶意网络服务大量加密化

- 越来越多的恶意网络服务通过**加密和隧道**技术绕过防火墙和入侵检测系统

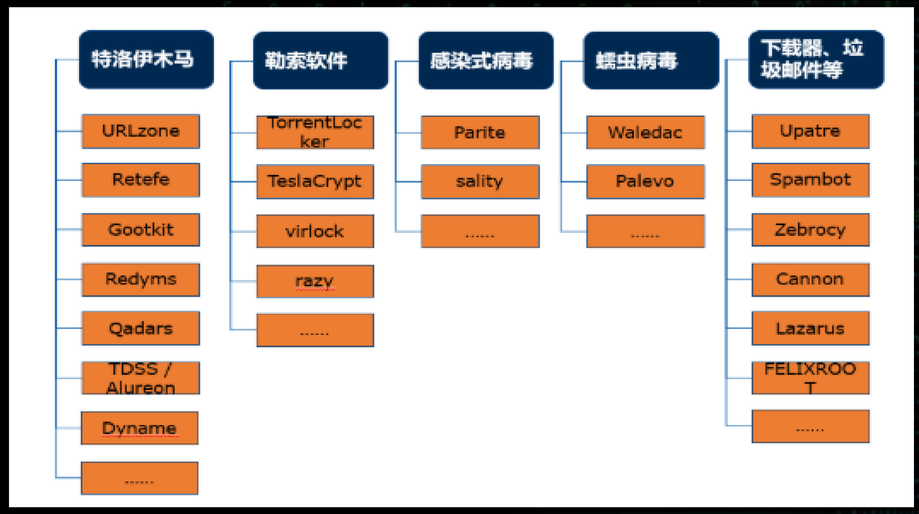
网络间谍
Black
Vine

情报收集
Waterbug

APT攻击团队
Butterfly



暗网
Darkweb



加密流量正在成为恶意服务的温床

据Gartner预测，到2019年，**80%**的网络流量将被**加密**，**半数**的**恶意软件活动**将利用某种类型的**加密**来隐藏交付、命令、控制活动以及数据泄露。

第七届互联网安全大会 360互联网安全中心

02

章节 PART

当前进展

关注加密网络流量数据的各方

国家层面

- 美国目前具备相当成熟完善的网络流量监控体系
- 我国具有相当深厚的技术储备和数据积累

工业界

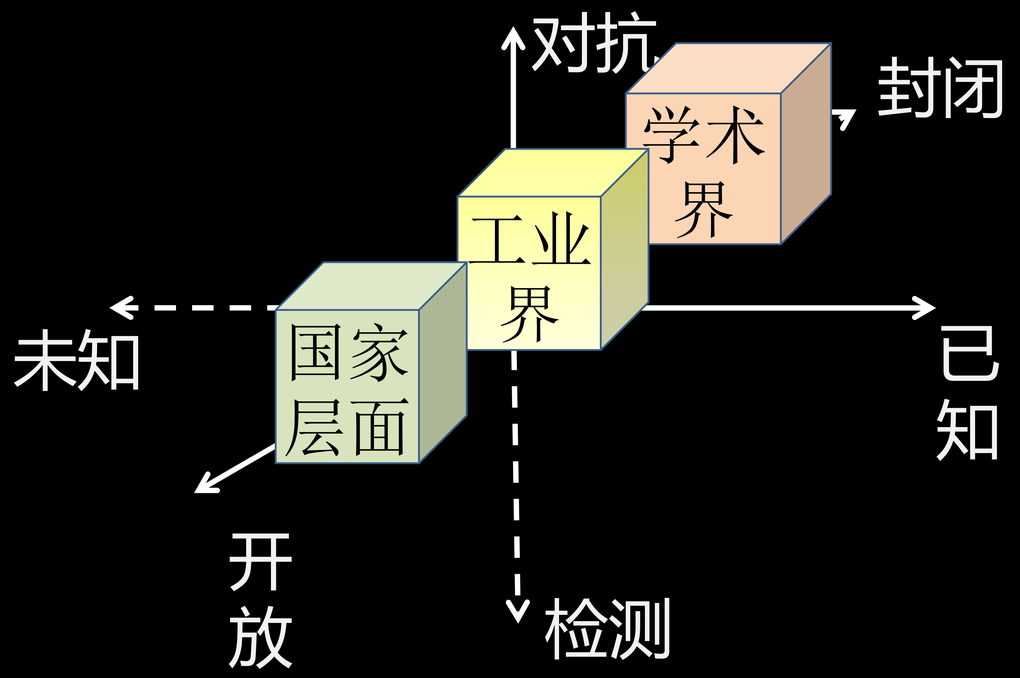
- 国外的Cisco、Palo alto、Sandvine等推出识别加密流量服务
- 国内数家企业也拟公开推出针对加密流检测量的设备

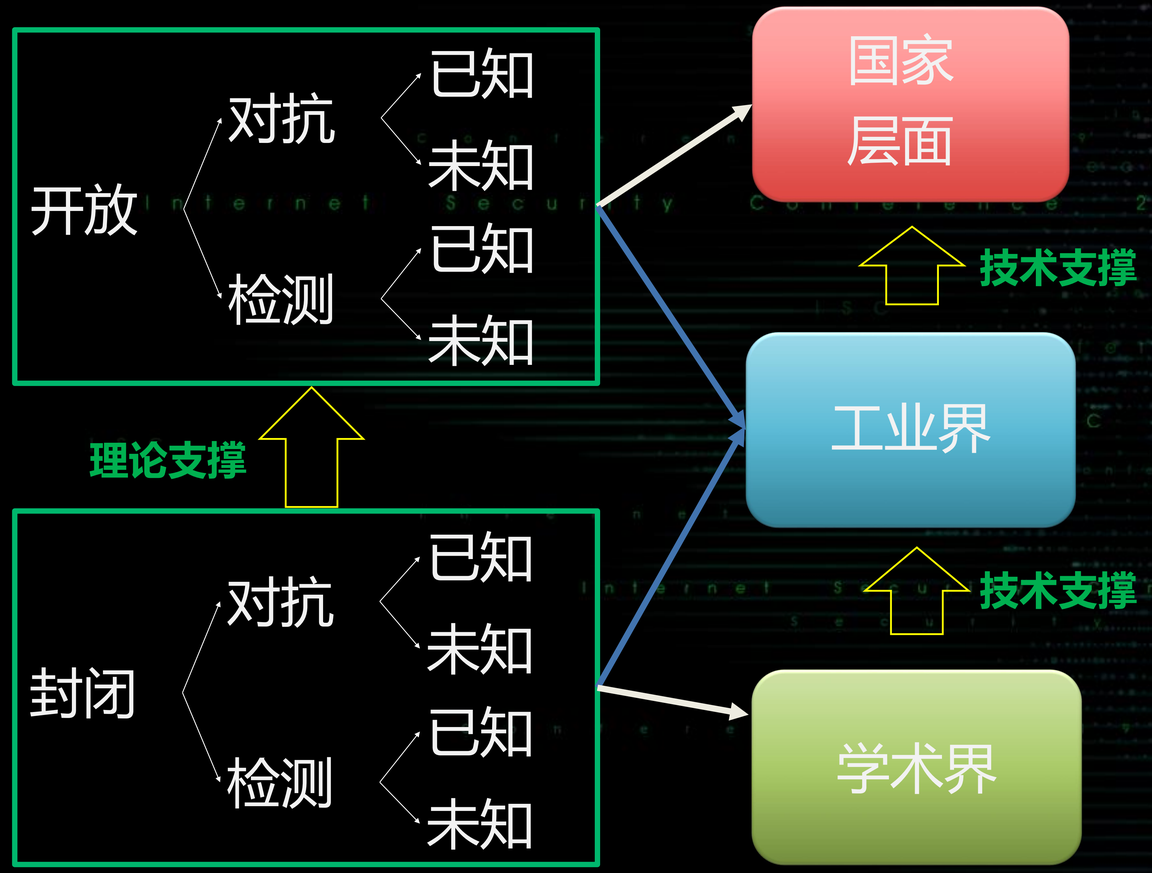
学术界

- 国外研究团队包括密歇根州立大学、加州大学伯克利分校ICSI、Cisco公司、英国牛津大学等
- 国内研究团队包括中科院信工所、清华、北邮、东南大学、西安交大等

各方关注的角度

□ 加密数据流量测量与行为分析

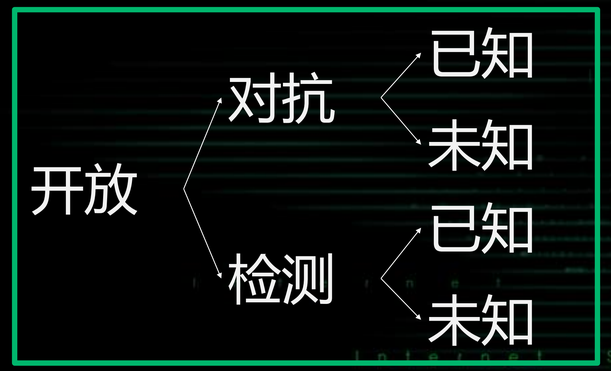




各方关注的角度

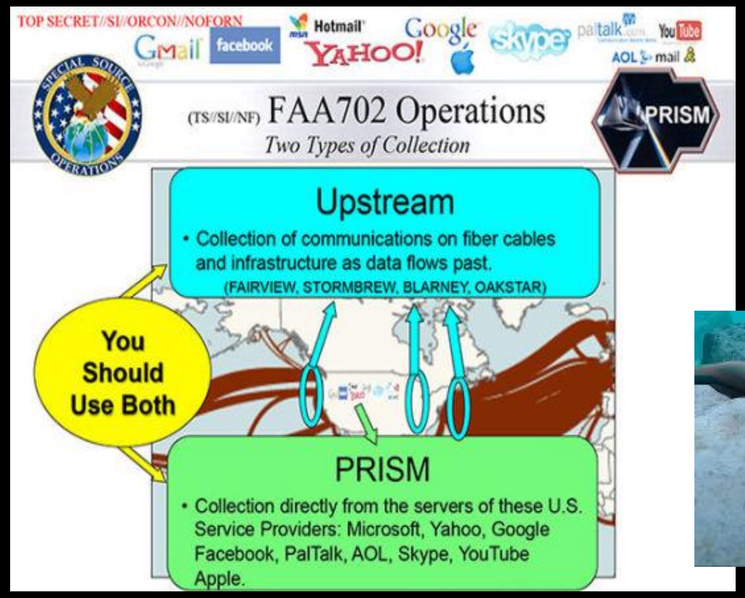
□ 加密数据流量测量与行为分析

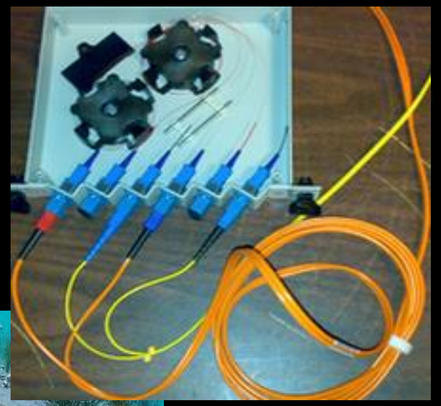
国家层面

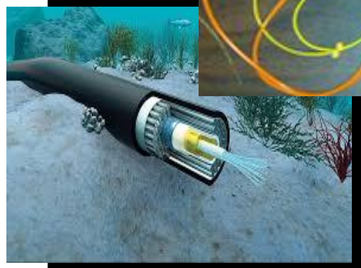


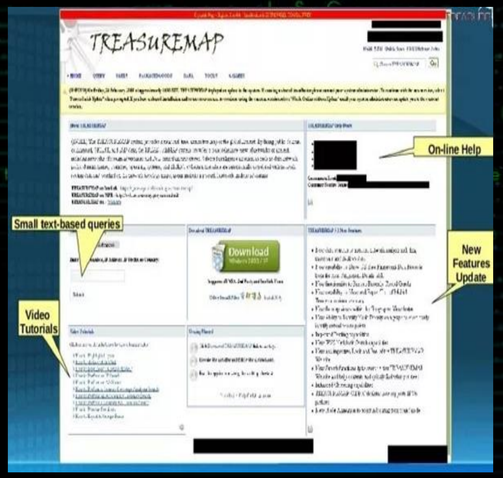
国家层面

- Upstream
- 爱因斯坦
- .....



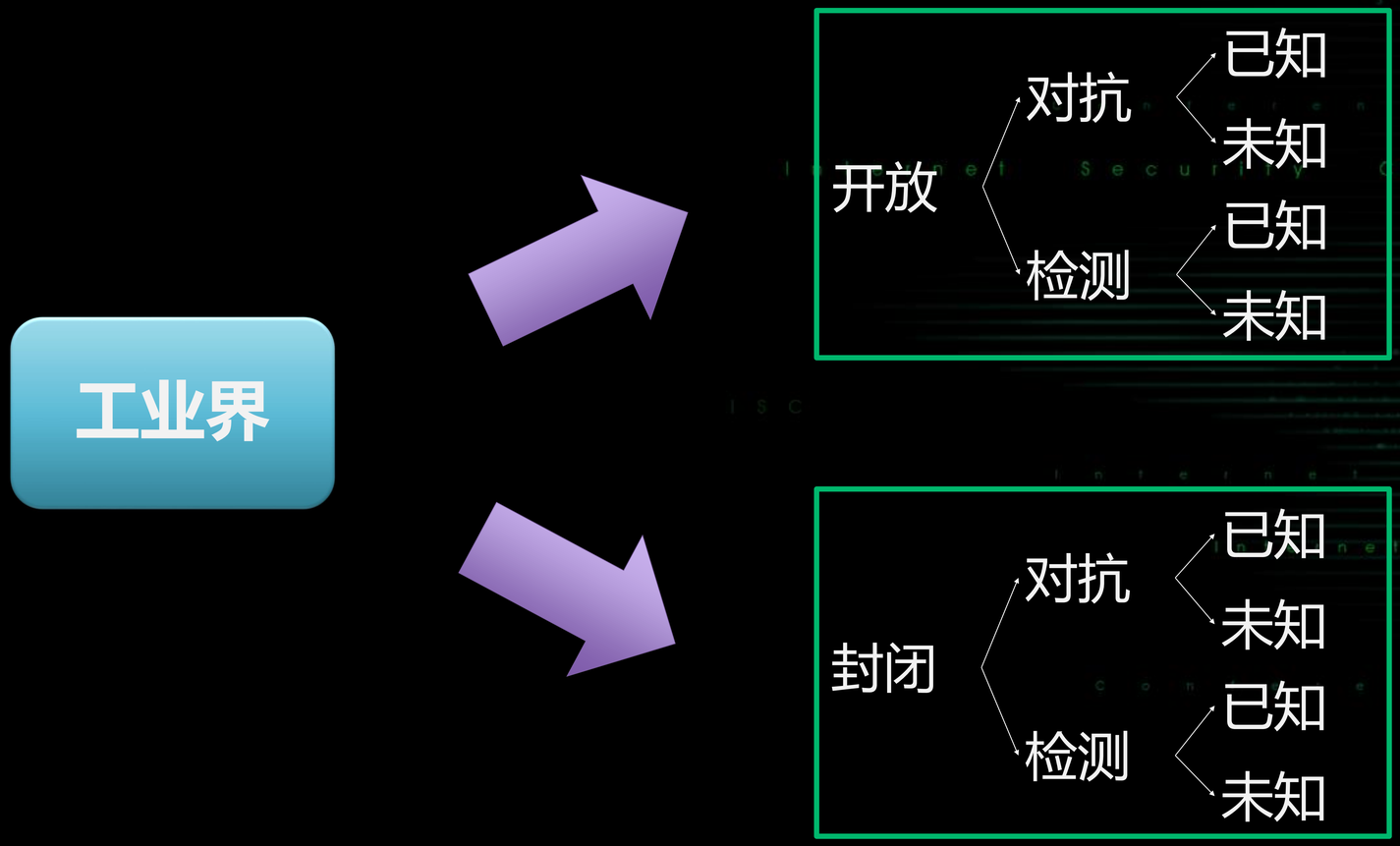






各方关注的角度

□ 加密数据流量测量与行为分析

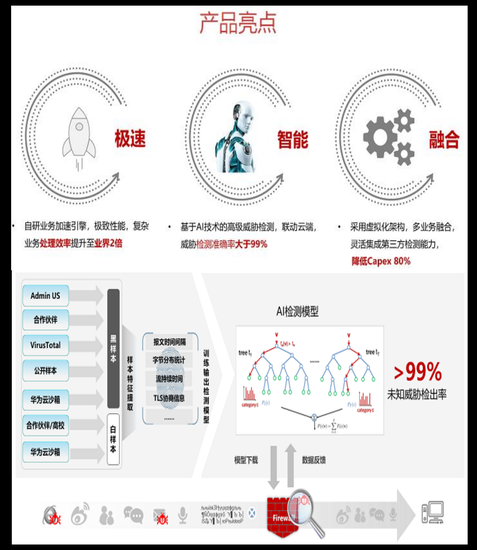


工业界的网络流量检测与分析

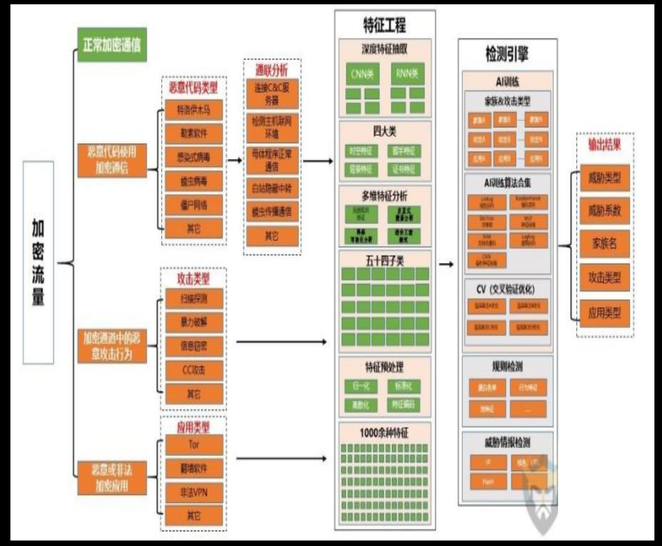
- 工业界中网络流量分析（NTA）大多结合使用机器学习、高级分析和基于规则来检测企业网络上的可疑活动。
  - 国内厂家包括华为、绿盟科技、安天、观成科技、上海观安、科来软件、东华软件、网鼎芯睿、上海纽盾、恒安嘉新、Panabit、亚信安全等；
  - 国外厂家包括Cisco、ENEA、Vectra、Awake Security、Bricata、Corelight、Corvil、Darktrace、ExtraHop、FireEye、GREYCORTEX、Lastline、allot等。

工业界的网络流量检测与分析

口国内部分产品

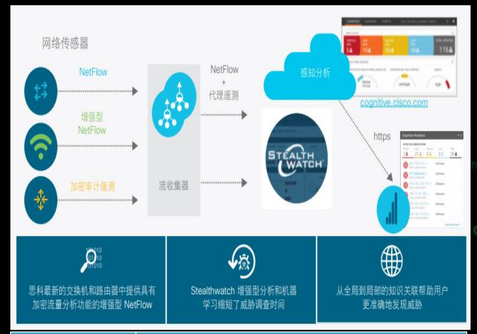


盒式防火墙



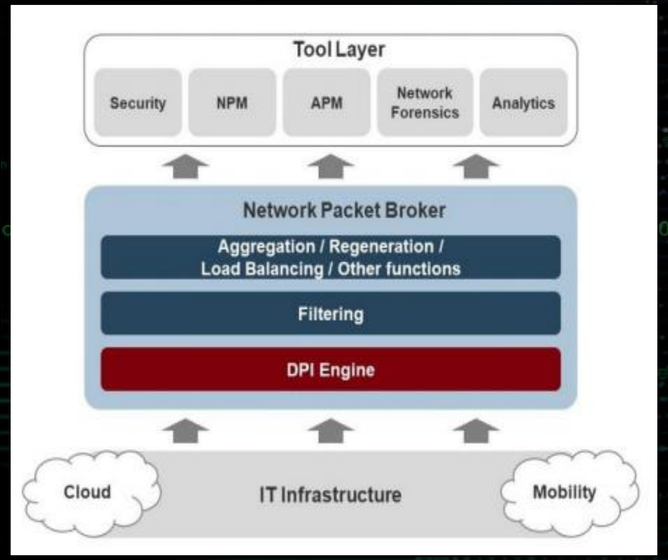
恶意加密流量AI检测引擎

口国外部分产品



安全可视化	通过网络分析洞悉加密流量中的威胁，与用户和设备信息关联的实时分析获取情景威胁情报。
加密评估	确保复合加密协议标准，并提供网络中已加密或未加密内容可视性和相关信息
更快响应	快速遏制受感染的设备和用户
节省时间和成本	将网络作为维护安全状态的基础

路由器、交换机等



加密流量分类引擎

产品大多可检测并防御隐藏在SSL加密流量中的威胁，包括入侵防御、反病毒、内容过滤、URL过滤等应用层防护，也可对使用加密通信的恶意样本、非法应用等进行深度分析。

监控传入和传出网络流量，检测零日恶意软件、内部威胁、高级持久性威胁、分布式拒绝服务等。部分产品可识别多种协议，实时分析流量，对加密流量分类。

工业界的网络流量检测与分析

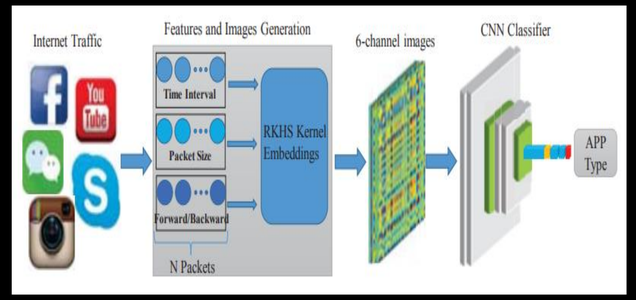
口国内厂家部分学术产出

	C features			CT features			CS features		
	precision	recall	F1	precision	recall	F1	precision	recall	F1
no stalling	0.931	0.900	0.915	0.937	0.925	0.931	0.958	0.980	0.969
stalling	0.528	0.625	0.572	0.607	0.652	0.628	0.871	0.760	0.812
weighted avg.	0.870	0.859	0.863	0.887	0.883	0.885	0.945	0.947	0.945

	CTS features	
	no stalling	stalling
no stalling	130969	2424
stalling	5768	18010

	CTS features		
	precision	recall	F1
no stalling	0.958	0.982	0.970
stalling	0.881	0.757	0.815
weighted avg.	0.946	0.948	0.946

加密流量中流媒体QoE分析



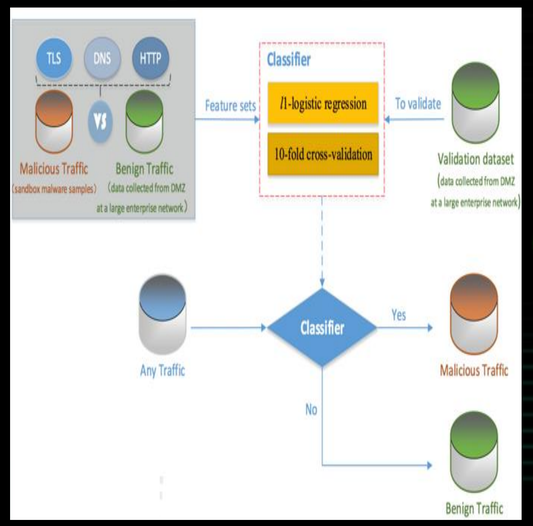
	SVM	MLP	NB	DT	Seq2Img
raw features	96.78	91.49	88.5	98.24	99.84
processed features	97.21	85.28	96.25	99.63	

卷积神经网络在流量分类中的应用

通过基于流的机器学习方法从加密网络流量中实时分析流媒体的停顿问题。

采用非参数内核嵌入法将流序列转换为图像，再将其输入CNN中分类。

口国外厂家部分学术产出



利用背景流信息检测加密恶意流量

通过TLS背景流信息如DNS响应、HTTP头部等辅助检测恶意流量。

Malware Family	Meta+SPLT +BD	TLS Only	Meta+SPLT +BD+TLS	All+SS
Bergat*	100.0%	100.0%	100.0%	100.0%
Kazy*	98.5%	99.5%	99.8%	100.0%
Parite*	99.3%	97.8%	99.6%	99.6%
Sality*	95.0%	94.1%	97.7%	98.0%
Tescrypt*	89.8%	95.6%	97.6%	97.6%
Upatre*	99.9%	98.7%	100.0%	100.0%
Virtob*	99.2%	98.8%	99.4%	99.4%
Yakes*	88.7%	98.5%	99.7%	99.7%
Zbot*	98.9%	99.6%	99.7%	100.0%
Zusy*	98.6%	88.7%	99.9%	99.9%
Deshacop	93.0%	63.6%	96.1%	96.1%
Dridex	16.5%	68.7%	78.5%	97.9%
Dynamer	95.4%	78.8%	95.7%	96.5%
Razy	91.5%	77.1%	95.9%	96.8%
Skeeyah	95.9%	82.1%	98.6%	98.6%
Symmi	99.1%	92.4%	99.8%	99.8%
Toga	100.0%	100.0%	100.0%	100.0%
Virlock	100.0%	100.0%	100.0%	100.0%

根据TLS加密流分析恶意软件

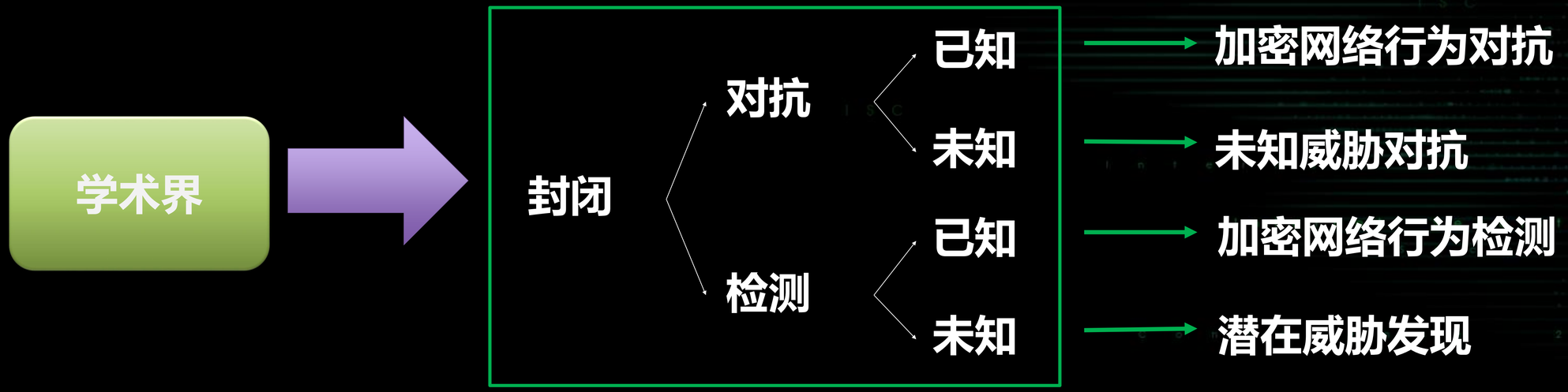
通过TLS背景流信息如DNS响应、HTTP头部等辅助检测恶意流量。

分析TLS流和恶意软件，发现恶意软件中TLS的使用区别于企业环境，这些差异可用于分类器。

学术前沿

□ 加密数据流量测量与行为分析

加密数据流量测量与行为分析是可以为网络管理和网络空间安全管控提供有效技术支撑，从学术角度，国内外不端涌现相应的理论创新成果。



学术前沿

□ 加密数据流量测量与行为分析

（检测-已知） 加密网络行为检测

学术前沿

□ （检测-已知）加密网络行为检测

网络流量加密后，基于规则的流量检测问题变得更加困难；许多研究引入机器学习算法，取得良好的研究成果，但目前的研究对特征的人工选取已达瓶颈，很难再有新特征的突破；而深度学习可以提取更本质、更有效的检测特征，因此最近的研究工作开始探索深度学习在加密流量检测领域的应用。

基于规则的加密流量检测

- 基于证书
- 基于字段匹配
- 基于通讯模式的正则表达

流量加密后

基于机器学习的加密流量检测

- 多源信息
- 时空统计特征
- 结合朴素贝叶斯、支持向量机(SVM)等算法

基于深度学习的加密流量检测

- 原始流量信息作为输入
- 结合CNN、LSTM等方法

学术前沿

□ （检测-已知）加密网络行为检测

- 基于规则的加密流量检测

主要思想：利用加密流量的字段组合、排序或者固定模式等作为指纹进行模式匹配。

- **优点**：轻量级的识别加密流量。
- **缺点**：
  1. 需要**人工分析**海量级流量，选择具有区分性的字段特征或组合。
  2. 仅可以对**已提取的规则**进行匹配识别。
  3. 容易被人工拼接或恶意伪造字段的流量**绕过**，导致**高误报率**。

- 典型研究
  - [Kim, APNOMS 2015]: 构建Certificate、session ID和IP对应关系列表。
  - [Shbair, ICDCSW 2016]: 对比SNI和IP对应的域名信息。
  - [Husák., EURASIP JIS 2016]: 采用ciphersuite list和HTTP中的user-agent。
  - [Papadogiannaki, RAID2018]:正则匹配固定模式，如包出现频率或包所在的位置。

学术前沿

口（检测-已知）加密网络行为检测

- 基于机器学习的加密流量检测

主要思想：构建加密流量的统计属性联合作为指纹进行分类识别。

- **优点**：面对**具体的应用场景**，选取**合适**的特征作为指纹，保证分类的**精度**。
- **缺点**：
  - 特征需要**人工设计和构建**，依赖**专业的知识和经验**
  - **如何构造**的统计特征成为难点。

- 典型研究
  - [Anderson. SIGKDD 2017]和[Anderson, JCVHT 2016]: C2S、S2C包长和时间的最大最小均值方差、等分包长度块构建马尔科夫链，握手阶段的原信息包括ciphersuite list extension等构建指纹。
  - [Yan, TrustCom 2018]: 根据通讯字节的突变情况切分成burst，统计每个burst内部的统计特征（包括进出方向包的负载和包数、包序列特征等）结合传统特征构建指纹。

学术前沿

口（检测-已知）加密网络行为检测

- 基于深度学习的加密流量检测

主要思想：研究将深度学习模型的表示学习思想逐步应用到加密流量分类的问题上，可以从加密的原始信息中自动提取关键信息并生成有区分性的加密流量指纹。。

- **优点**：输入不需要人工构建，可以自动化提取有效特征。
- **缺点**：考虑信息不全面。仅面对单一分类任务构建特征，没有考虑指纹的普适性。

- 典型研究
  - [Wei, ICISC 2017]: 融合特征提取，特征选择和分类为一个端到端的框架，采用一阶卷积神经网络对不同行为的前784个负载字节进行计算，构建指纹。
  - [Lotfollahi, CoRR 2017]: 将payload从tcp/udp层开始对其填充，保证协议头部分20字节和8字节对齐，对于负载部分，采用前1480个字节，对于不足的负载进行0填充，保证维度一致性，使用ANN和SAE进行特征提取生成指纹。
  - [Rimmer, NDSS 2018]:利用匿名化网络tor的特性，采用长度序列的方向序列作为深度学习网络SAE、CNN、LSTM的输入，从而分类访问的网页。

学术前沿

□ 加密数据流量测量与行为分析

（对抗-已知） 加密网络行为对抗

学术前沿

口 （对抗-已知）加密网络行为对抗

加密流量分析的目标是根据通信特征构造可区分性的加密流量指纹。因此对抗加密流量的对加密信道的通信特征修改。从实现角度分为两类，基于标准传输协议特性的通用对抗和基于应用层协议的定制对抗。修改的通信特征的属性主要包括流传输的包长序列特征、方向序列特征和时间序列特征。

- 基于通用协议特性的加密对抗
  - 可利用的协议特性包括：IP层分片及转发；TCP MSS、拥塞窗口、重传、多TCP连接；SSH、TLS和IPSec 字节填充;HTTP层 range, pipelining；
  - 优点：通用，支持多种加密传输信道，无需对应用层协议进行修改。
  - 缺点：通信特征混淆能力有限
- 典型工作
  - Luo等人提出HTTPOS通过修改TCP MSS及HTTP range等选项控制包长度防御网页分类攻击[NDSS 11]
  - Dyer等人验证了加密协议字节填充的加密流量分类对抗的效果[S&P 12]

学术前沿

□ （对抗-已知）加密网络行为对抗

加密流量分析的目标是根据通信特征构造可区分性的加密流量指纹。因此对抗加密流量的对加密信道的通信特征修改。从实现角度分为两类，基于标准传输协议特性的通用对抗和基于应用层协议的定制对抗。修改的通信特征的属性主要包括流传输的包长序列特征、方向序列特征和时间序列特征。

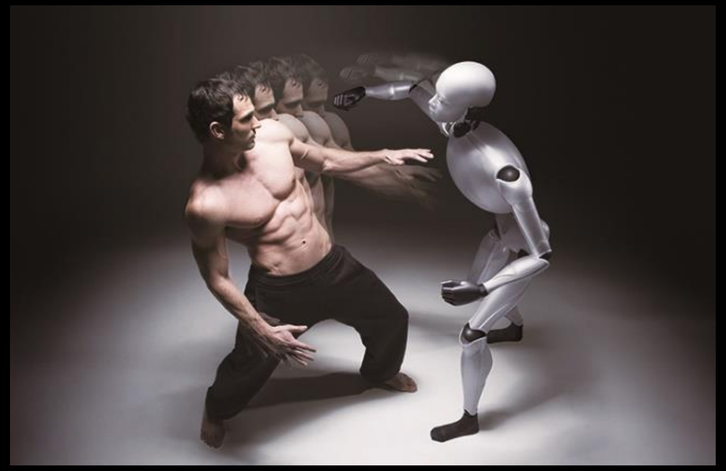
- 基于基于应用层协议的定制对抗
  - 定制化的内容主要包括：加载背景流量、无目标的传输特征混淆、有目标的模仿其他网站分布特征等
  - 优点：修改灵活, 混淆伪装能力强
  - 缺点：不通用
- 典型工作
  - Luo等Panchenko等人提出了加载背景流量的防御方法，并在Tor和JAP匿名网络进行验证。[WPES11]
  - Wang等人提出Walkie-talkie以单工方式加载网站来混淆burst特征。[USENIX 16]

学术前沿

□ （对抗-已知）加密流量AI对抗展望

对抗人工智能技术的研究在加密网络流量检测领域还处在探索阶段，主要原因：

- 现有的针对加密流量的AI模型不成熟，难以实际应用；
- 人工智能技术应用到加密网络流量分类领域时间较短，基于AI的加密流量分类技术的安全问题尚未暴露出来；
- 缺乏对AI加密流量分类系统的敌手流量构造方法的深入研究。



学术前沿

□ 加密数据流量测量与行为分析

（检测-未知） 潜在威胁发现

学术前沿

口 （检测-未知）潜在威胁发现

潜在威胁发现首先需要获得其流量数据，但在实际中采集到的往往是几种流量的混合，如何将未知流量进行分离， 按特征进行归类，从而发现威胁流量是学术届近几年的关注热点。

具体框架

背景流量中未知流量的抽取

↓

未知的流量的种类细分

↓

潜在威胁流量的识别

核心思想：通常利用三元组扩展标签流量(服务器ip和端口, 协议) ，采用无监督的方式聚类发现部分未知，训练（N+1）分类器识别背景流的未知流量后进行无监督聚类，根据不同行为特征发现潜在的威胁流量。

- **优点**：简单、易于实现，并且具有较好的实验结果；
- **缺点**：未充分利用流的相关性; 未知类别不能保证完全正确细分

典型工作

- Zhang J等训练N+1分类器识别未知判别是否为威胁流量[TON 2015]
- Lin R等利用半监督和集成学习模型识别未知检测其类型[ICCS 2015]
- Cesare S等在聚类过程中增加了算法约束，防止未知流量落入已知标签流量中[ICCC 2017]
- Zhang Y等提出利用深度编码器和PCKeans实现未知流量类别更精准的识别方法[ICCS 2019]

学术前沿

□ 加密数据流量测量与行为分析

（对抗-未知） 未知威胁对抗

学术前沿

口 （对抗-未知）未知威胁对抗

基于静态分析、动态分析、行为分析的未知威胁对抗方法层出不穷，攻击者想要绕过检测系统实属不易，网络行为分析和混淆伪装对抗逃逸一直处于动态对抗过程中。未知威胁对抗近几年来一直是匿名通信、隐私保护、抵御网络审查等领域的研究热点，也是勒索软件、木马、僵尸网络等恶意软件逐渐实用化的技术来源。

目前来看，对抗未知威胁对抗方法的技术主要包括三个方面，分别是：

- **流量伪装与混淆，**包括对抗签名或规则、对抗流量统计分析、流量模糊随机化。
- **新型私有协议应用，**主要思路是由于业界缺少对新型私有协议的认识与分析，利用新型私有协议的通信能更好地逃避系统的检测。
- **消除痕迹防溯源分析，**在攻击完成后及时消除攻击痕迹、不留线索，以防研究人员对攻击活动进行溯源分析。

学术前沿

口 （对抗-未知）未知威胁对抗

典型工作：

- **流量伪装与混淆**

  - 对抗签名或规则：Li F等人提出了黑盒分析流量分类规则的方法，从而可以通过多次测试推断出流量分析识别规则从而修改通信包进行逃逸（IMC 2016）

  - 对抗流量统计分析：SkypeMorph（CCS 2012）

  - 流量模糊随机化： Tor的流量混淆插件OBFS，已经从obfs到obfs4，其原理通过多次加密变换使得原有协议特征消除，从流量分析层面来看通信流量字节随机化，难以找到特征

- **新型私有协议应用**

  - APT攻击活动组织Wild Neutron使用的恶意软件与C&C服务器的通信都是使用自定义的协议进行加密， 逃避检测

- **消除痕迹防溯源分析**

  - 恶意软件在执行之前对系统进行全面扫描，确认是否有安全防护产品正在运行，如果发现有运行中的安全防护产品，恶意软件将不会执行，并清除相关痕迹

第七届互联网安全大会 360互联网安全中心

03

章节 PART

研究成果

第七届互联网安全大会 360互联网安全中心

团队研究方向简介

□ 大数据网络行为分析与对抗

- 研究方向：
  - 网络流量分类（高速网络流量分类，加密流量分析，协议自动分析）
  - 网络测量与资源服务识别（基础/加密/私有服务测量与IP综合测绘）
  - 海量数据网络行为分析（知识库、多源融合、机器学习及应用）
  - 信息对抗理论与技术（网络信息对抗模型架构、方法与技术）
  - 隐蔽式网络攻击检测（协议伪装混淆对抗，未知威胁检测）
  - 网络取证
  - 网络态势感知
- 授课情况（中国科学院大学）
  - 专业普及课《网络行为学导论》，40学时
  - 博士生课程《网络测量与行为分析》，40学时

网络行为学

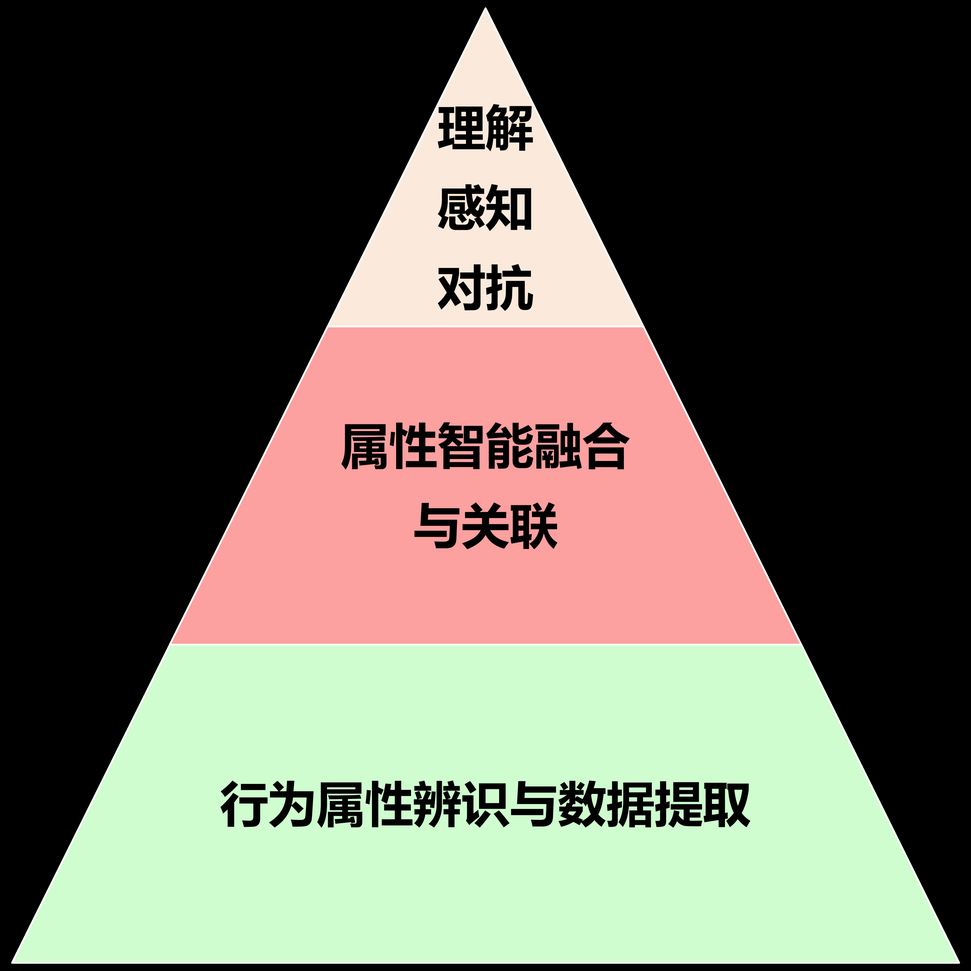
网络行为学

- **网络行为**

  即网络空间主体的行为，包括交易行为、消费行为、娱乐行为、政治行为、 违法行为等。这些行为无疑是法学、经济学、管理学、社会学、心理学等 人文社会科学学科的研究对象。 它们也是信息科学与技术学科的研究对象。

- **网络行为学**
  - 网络行为学 是研究网络运行规律的科学。
  - 网络行为学是研究网络发展、进化规律的科学。
- **主要研究方向**
  - 网络测量技术：主动和被动
  - 数据分析和预测技术：定性和定量
  - 网络管理技术等
- **主要研究方法**
  - 通过建立模型进行网络行为分析;
  - 通过仿真模拟进行研究;
  - 通过测量分析对网络的运行管理以及网络行为进行研究

网络行为学基本思路



对抗溯源：伪装识别，跨越时空追踪源头路径

感知与理解：全局历史跨度，态势立体深度解析

已知到未知：智能学习进化，提升威胁感知能力

构建基准行为与场景合规动态标准

时空数据智能关联融合，形成知识库

由点到面，属性聚合形成实体综合刻画

关联行为：网络、连接、交互、时空

实体行为：人、机、物三元刻画属性

微观行为：声、光、电磁、指令……

行为分析通过行为属性辨识与数据提取，实现属性智能融合与关联分析，支撑理解、感知、对抗等安全应用，有效筛选出可疑行为和有害信息。

第七届互联网安全大会 360互联网安全中心

加密数据流量测量与行为分析

1. （检测-已知）加密网络行为检测

2. （对抗-已知）加密网络行为对抗

3. （检测-未知）潜在威胁发现

4. （对抗-未知）未知威胁对抗

加密数据流量测量与行为分析

1、（检测-已知）加密网络行为检测

1、（检测-已知）加密网络行为检测

- 标准加密协议：X.509数字证书分析恶意加密行为
- 标准加密协议：加密流量分类
- 新型加密协议：加密协议升级 TLS1.3

1、（检测-已知）加密网络行为检测

□ 标准加密协议：X.509数字证书分析恶意加密行为

□ 标准加密协议：加密流量分类

□ 新型加密协议：加密协议升级 TLS1.3

1、（检测-已知）加密网络行为检测

□ X.509数字证书分析恶意加密行为

1. X.509数字证书

随着人们网络安全意识的增强及HTTPS的普及，与X.509证书相关的安全问题日益突出。

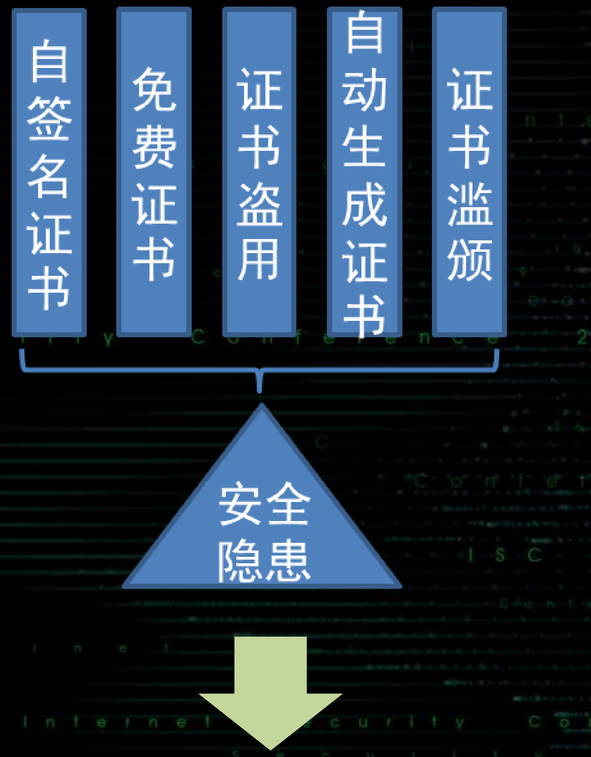
Mozilla列举沃通CA的诸多问题

赛门铁克向Blue Coat签发了一个中级证书

沃通用 FUD 恐吓 Let's Encrypt 用户

Let's Encrypt CA已被所有主流浏览器信任

加密網攻惡意軟體暴增60倍 SSL成企業資安防護新盲點



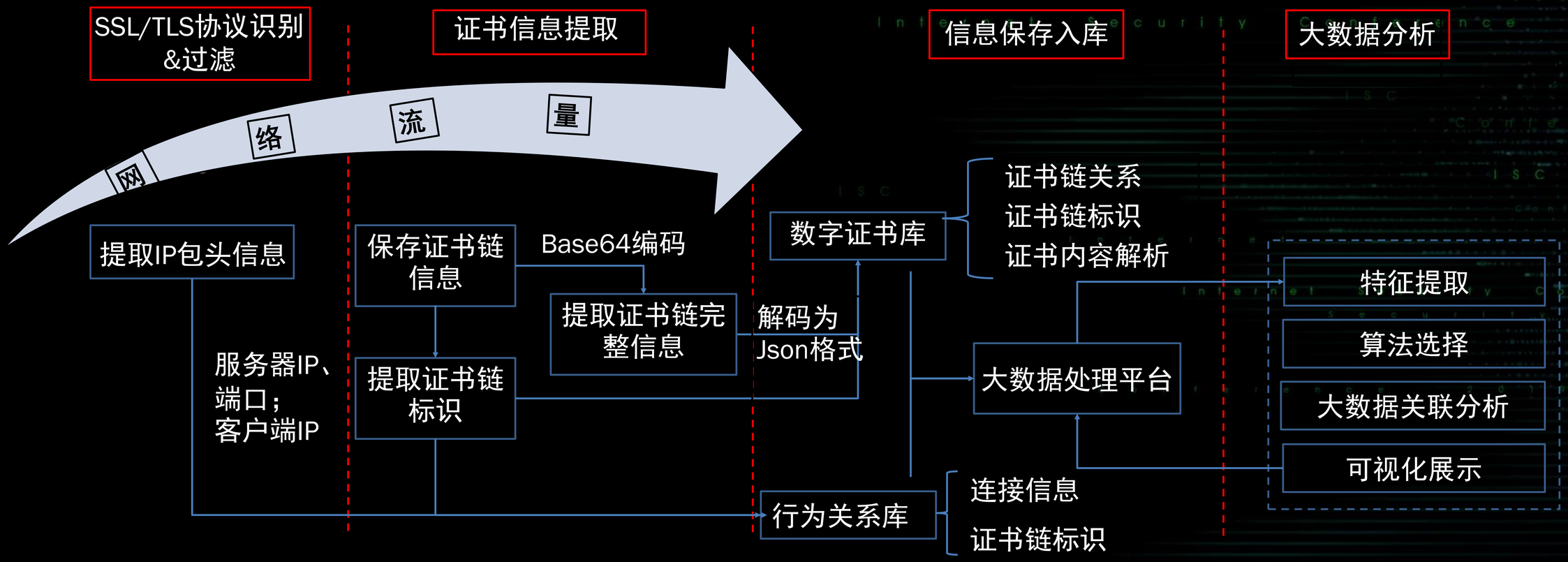
越来越多的恶意软件使用SSL加密其通信流量，以绕过防火墙和IDS系统

通过被动检测获取**证书**，结合相应的**流量行为分析**，对**恶意/异常**加密网络流量进行识别与检测

1、（检测-已知）加密网络行为检测

□ X.509数字证书分析恶意加密行为

2. X.509数字证书获取和分析框架



1、（检测-已知）加密网络行为检测

□ X.509数字证书分析恶意加密行为

3. 恶意加密流量增长迅猛

SSL Blacklist数据集中，用于恶意软件/僵尸网络的证书从**2014年**的**1,454**个增长到**2016年**的**13,456**个，不到**3年**内增长了**近10倍**。

- 低成本
- 更新频繁
- 证书属性相似
- 网络行为相似

大多数恶意软件使用自动部署的自签名证书或者Let's Encrypt等签发的免费DV证书来加密。

为了逃避基于黑名单的检测，大部分恶意软件会频繁更新所使用的证书，因此与正常的加密其通信流量，以绕过检测。在增强了生存能力的同时，其增加的成本可以忽略不计。

网络服务相比（如Google），恶意加密流量对在证书属性方面，基于证书的自动部署，同一僵尸网络更新更加频繁。

在网络行为方面，SSL流量在连接统计特征、数据包统计特征等方面与正常的SSL加密恶意软件的大部分属性相同或相似，可以作为检测特征。

服务流量存在着差异。

1、（检测-已知）加密网络行为检测

□ X.509数字证书分析恶意加密行为

4. 恶意证书更新频繁

表1 – 恶意证书的更新频率

Malicious Reasons	server : port	Update frequency
KINS C&C	37.25.102.37 : 443	2.7
	31.128.74.100 : 443	4.3
	average	*3.5*
TorrentLocker C&C	144.76.251.60 : 443	5.5
	62.213.67.152 : 443	8
	average	*6.75*
Redyms C&C	213.111.203.203 : 443	1.8
	173.71.98.228 : 443	2.7
	188.230.84.45 : 443	2.7
	93.127.119.6 : 443	1.7
	176.110.22.247 : 443	2.7
	average	*2.32*
Dridex C&C	200.49.169.94 : 443	1
	42.117.2.85 : 443	3.6
	78.47.203.94 : 4493	5.75
	202.69.40.173 : 243	5.7
	173.45.192.173 : 443	1.5
	188.126.116.26 : 443	1.7
	94.73.155.12 : 2448	2
	78.47.66.169 : 7447	4.75
	221.132.35.56 : 8843	4.25
	46.22.134.78 : 4493	6.5
	94.73.155.11 : 2448	3.3
	203.158.193.83 : 444	1.25
	89.32.145.12 : 8443	1
	202.129.57.130 : 443	5.7
	94.73.155.10 : 2448	1.1
	average	*3.27*

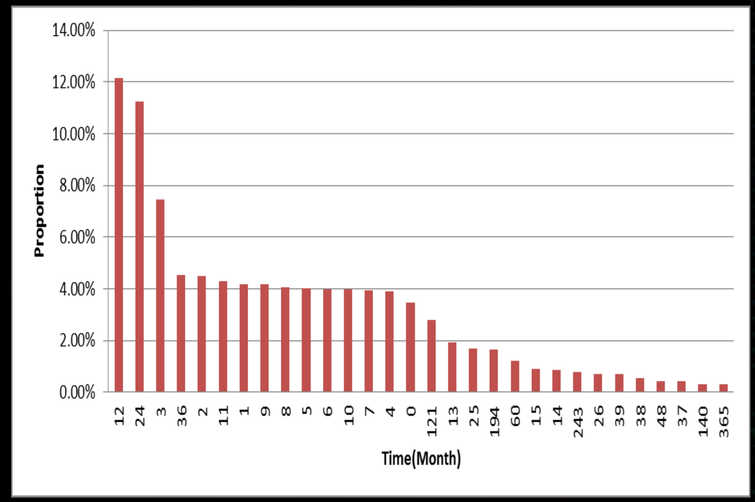


图1 – 非自签名证书的有效期

对facebook、google、淘宝等10个大型网站的服务器进行追踪，在300天内，有**3个**服务器更新过**5次**证书，**2个**服务器更新过**1次**证书，**5个**服务器**没有更新**过证书。

正常的证书更新频率远小于恶意证书

1、（检测-已知）加密网络行为检测

□ X.509数字证书分析恶意加密行为

5. 恶意服务连接频率相似

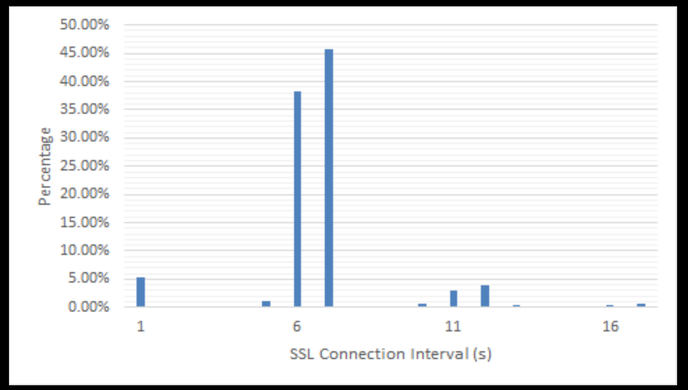


图2 – 恶意服务SSL连接间隔

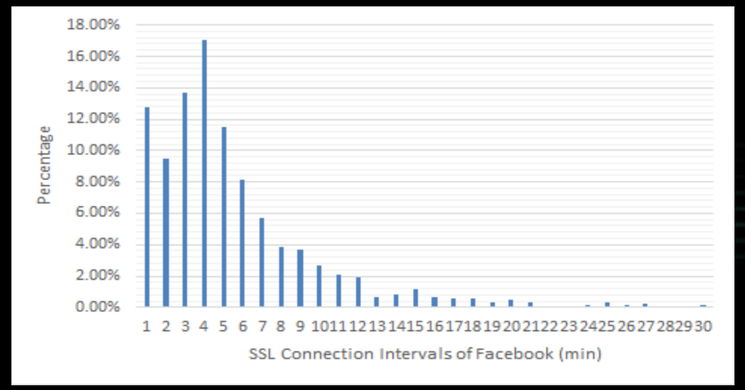


图3 – Facebook SSL连接间隔

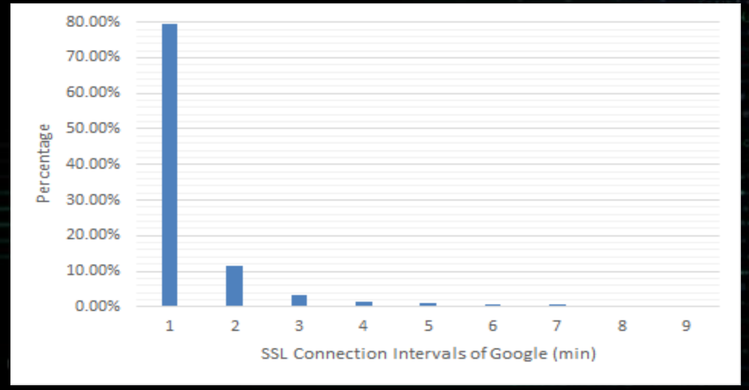


图4 – Google SSL连接间隔

- 通过对恶意服务的SSL连接行为分析，发现其**连接间隔**（保活/心跳机制）与正常服务（如Facebook、Google等）SSL连接间隔存在着较大的差异性。
- 结合**其他统计特性**，可以很好的区分恶意SSL服务于正常SSL服务。

第七届互联网安全大会 360互联网安全中心

1、（检测-已知）加密网络行为检测

- 标准加密协议：X.509数字证书分析恶意加密行为
- **标准加密协议：加密流量分类**
- 新型加密协议：加密协议升级 TLS1.3

1、（检测-已知）加密网络行为检测

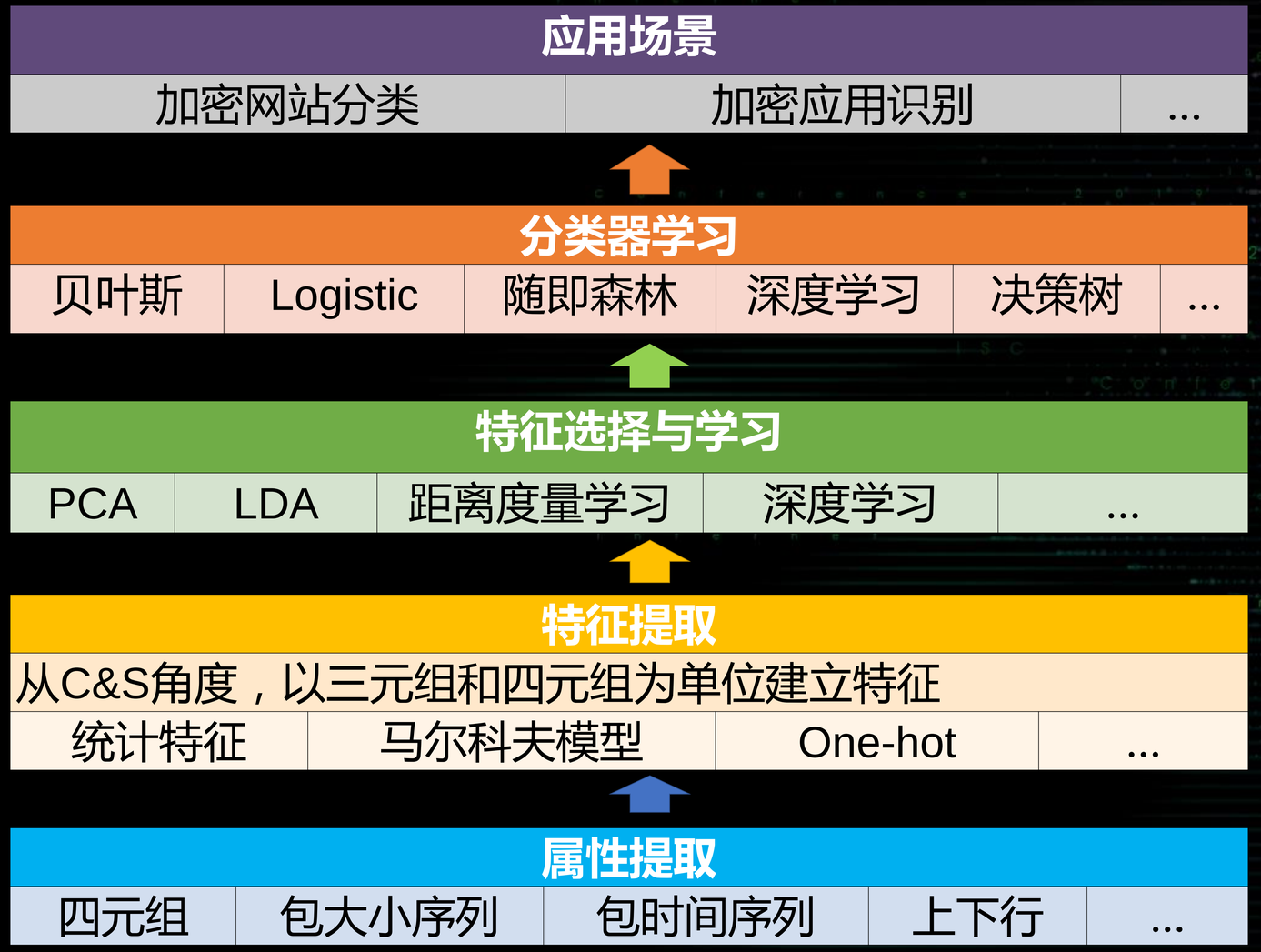
□ 加密流量分类

◆挑战1 ：公有云迅猛发展

- 2017年度上半年公有云服务市场同比增长28.6%；
- 中国市场同比增长55.6%。

◆挑战2：加密用户量剧增

- Google所有的产品和服务产生的流量中，90%以上均已被加密；
- Firefox提供的数据也显示，2019年4月通过Firefox浏览器加载的网页有超过87%都是加密的。



1、（检测-已知）加密网络行为检测

口 加密流量分类

关键技术1：面向加密流量的多模态统计特征

随着对抗的加剧，仅靠握手特征已难以满足加密流量的识别需求。基于此，我们提出使用包长度和包间隔构造**多模态、多角度统计特征**，然后使用不同的机器学习算法对流量分类。

贡献： 在IP五元组失去作用、原始统计特征有限的情况下，**利用上下包的关联属性**，构造基于**一阶马尔科夫模型**的包大小、包间隔**多模态统计特征**；结合高斯概率模型和直方图构造**多角度统计特征**。在时间和空间上挖掘出具有较好判别性能的**特征融合方式**，充分发挥出有限特征的判别能力。

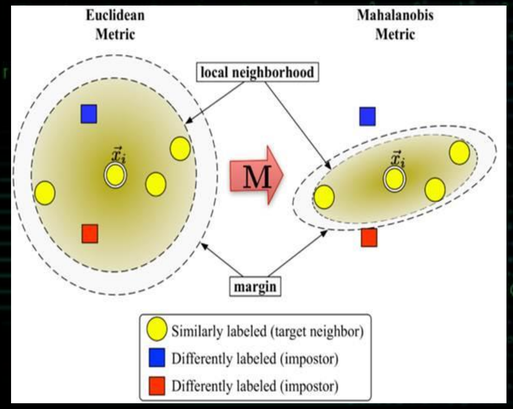
元数据 flow metadata	the number of inbound packets, the number of outbound packets, the number of inbound bytes, the number of outbound bytes, total duration of the flow
sequence of packet lengths	马尔科夫 MRF feature 10x10 高斯、直方图 等
sequence of packet times	马尔科夫 MRF feature 10x10 高斯、直方图 等
Byte distribution	Statistical probability of bytes256
TLS information	Cipher-suites lists Public key length

1、（检测-已知）加密网络行为检测

口 加密流量分类

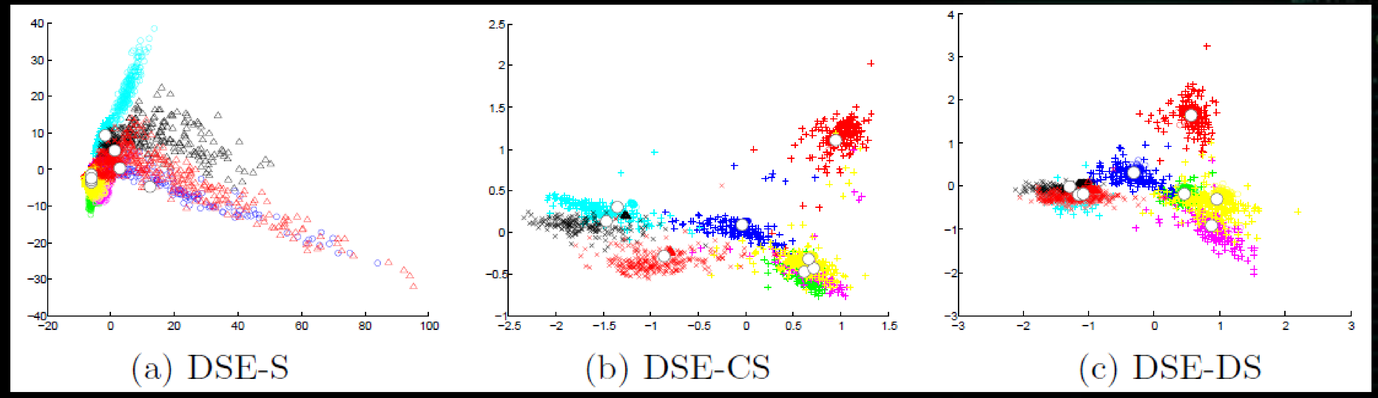
关键技术2：面向大数据与开放环境的算法研究

贡献：针对流量分类模型在大数据环境中的泛化性问题，提出基于**距离度量学习**和**低秩约束**的子空间学习算法。通过学习特征的**自适应度量矩阵**进行特征选择和关联；采用**APG加速梯度逼近算法**计算最优解，解决了流量特征的离散性问题和数据不平衡问题，还具有良好的泛化能力。



关键技术3：基于深度学习的特征融合与分类

贡献：采用深度信念神经网络和卷积神经网络对流量进行识别；提出**基于距离的Softmax交叉熵**取代Softmax，更好地降低类内距离，更适用于匹配问题。



第七届互联网安全大会 360互联网安全中心

1、（检测-已知）加密网络行为检测

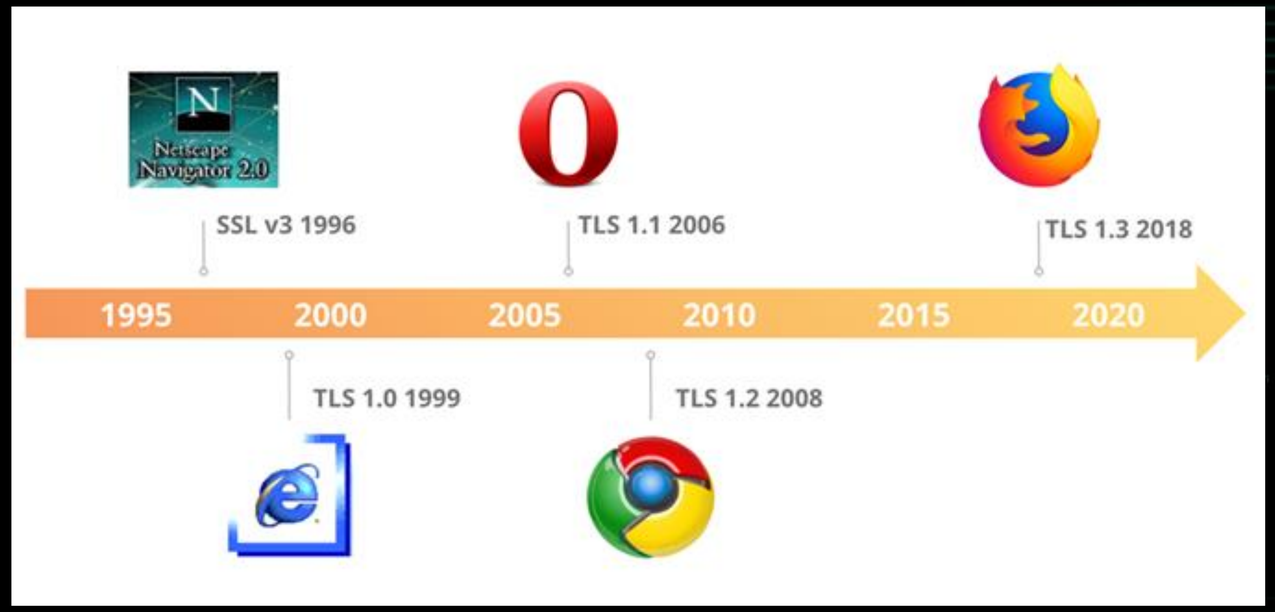
- 标准加密协议：X.509数字证书分析恶意加密行为
- 标准加密协议：加密流量分类
- **新型加密协议：加密协议升级**

1、（检测-已知）加密网络行为检测

口 加密协议升级

TLS1.3简介

2018年8月，IETF正式发布TLS1.3协议的最终版本 (RFC 8446)，在安全性、性能和隐私等方面有重大改进，同时大大提升了HTTPS连接的速度。



1、（检测-已知）加密网络行为检测

□ TLS1.3的改进

1. 证书加密

TLS1.3在TLS1.2的基础上做了改进，通过加密更多的握手过程 (如证书交换) 来保护其免受窃听者的侵害，从而为数据交换提供更强的隐私性。

TLS1.2

```
 4 0.585331    192.168.1.153   104.18.131.189  TLSv1.2   264 Client Hello
 5 1.189184    104.18.131.189  192.168.1.153   TCP        54 443 → 62174 [ACK] Seq=1 Ack=211 Win=30720 Len=0
 6 1.206937    104.            .168.1.153      TLSv1.2  1514 Server Hello
 7 1.208550    104.            .168.1.153      TLSv1.2   979 Certificate, Server Key Exchange, Server Hello Done
 8 1.208613    192.168.1.153   104.18.131.189  TCP        54 62174 → 443 [ACK] Seq=211 Ack=2386 Win=261184 Len=0
 9 1.209132    192.168.1.153   104.18.131.189  TLSv1.2   147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake
10 1.214721    192.168.1.153   104.18.131.189  TLSv1.2   147 Application Data
```

TLS1.3

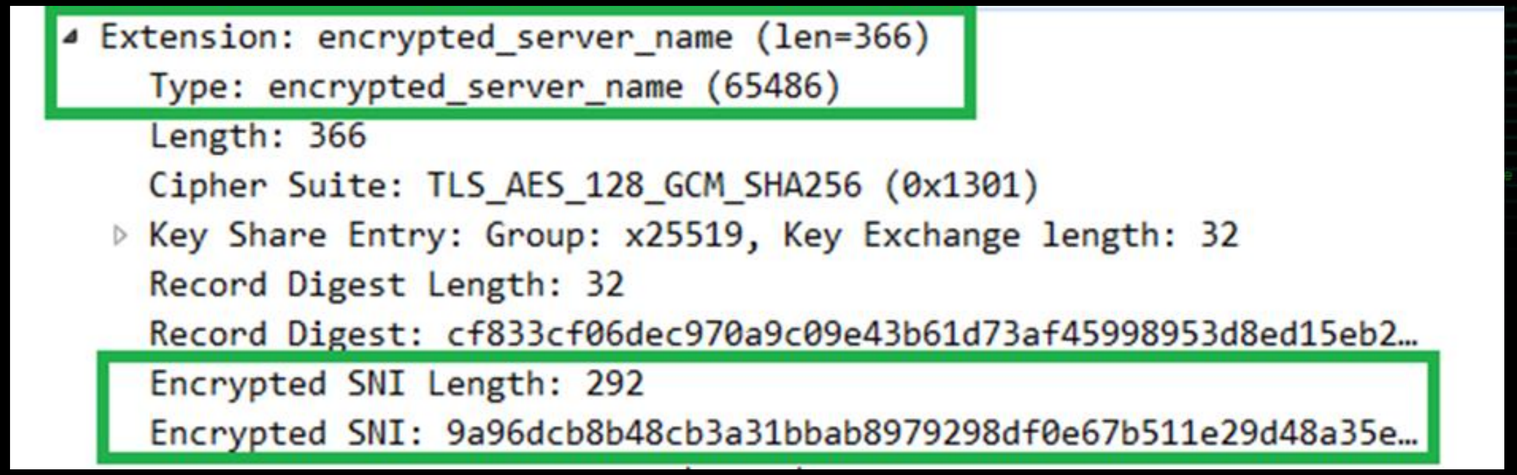
```
 4 1.020808    192.168.1.153   216.239.32.116  TLSv1.3   583 Client Hello
 5 1.701922    216.239.32.116  192.168.1.153   TCP        66 443 → 61209 [ACK] Seq=1 Ack=518 Win=61440 Len=0 TSval=566
 6 1.727669    216.239.32      .153            TLSv1.3  1484 Server Hello, Change Cipher Spec
 7 1.752568    216.239.32      .153            TCP      1484 443 → 61209 [ACK] Seq=1419 Ack=518 Win=61440 Len=1418 TSv
 8 1.752639    192.168.1.153   216.239.32.116  TCP        66 61209 → 443 [ACK] Seq=518 Ack=2837 Win=129600 Len=0 TSval
 9 1.784370    216.239.32.116  192.168.1.153   TLSv1.3   289 Application Data
```

1、（检测-已知）加密网络行为检测

□ TLS1.3的改进

2. ESNI

ESNI（加密SNI）是TLS1.3协议的扩展，它可以阻止ISP、WiFi和其他监控者拦截TLS扩展模块中的SNI，防止用户访问网站的浏览记录被泄露，ESNI让使用HTTPS的互联网用户更难被跟踪。



1、（检测-已知）加密网络行为检测

口 加密协议升级

HTTP/2流量分类

据W3Techs称，截至2019年1月，前1000万网站中有32.5%支持HTTP/2。在HTTP/1.1中，只有前一个响应收到后才能发送下一个请求。为提高效率，HTTP/2提出**复用和并发**。浏览器不需等待接收上一个响应就可以启动下一个请求。服务端可以根据接收到的请求，发送任意一个响应数据包。这使同方向上连续非零负载数据包等**burst特征**失效。

为此我们提出**局部请求和响应序列（LRRS）**作为特征。包括pcap包统计信息，基于时间片的请求和响应序列，局部请求和响应序列。从不同层面描述HTTP/2协议流量。

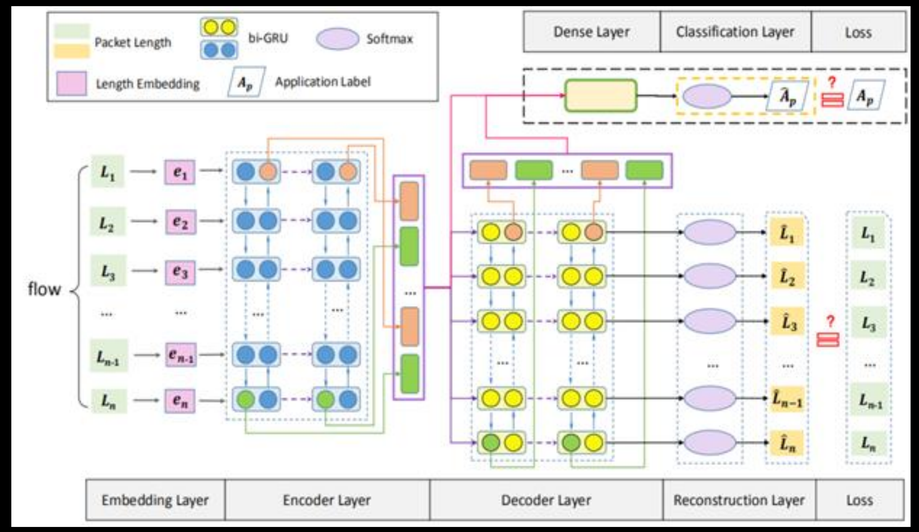
Feature Type	Description	Feature Number
part1	the total size of incoming[1] packets, the total size of outgoing[2] packets, the packet number of incoming packets, the packet number of outgoing packets, the total size of first 30 incoming packets, the total size of first 10 outgoing packets, the packet number of first 30 incoming packets, the packet number of first 10 outgoing packets, the total size of last 10 outgoing packets and the packet number of last 10 outgoing packets	10
part 2	The duration of the whole pcap is first divided equally into 20 time slices. Then we obtain the total size of incoming packets, the total size of outgoing packets, the packet number of incoming packets and the packet number of outgoing packets in each time slice.	80
part 3	the first 20 incoming packet size, the first 20 outgoing packet size and the last 20 incoming packet size.	60

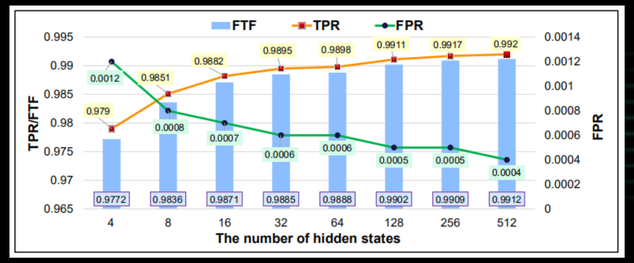
第七届互联网安全大会 360互联网安全中心

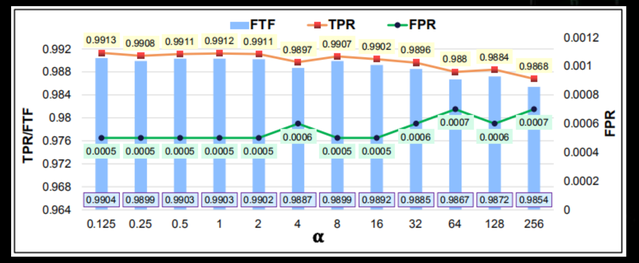
团队研究成果

INFOCOM 2019-基于流序列网络的加密流量分类算法

提出了一种基于表示学习的流序列网络，以双向GRU为基本单元，编码-解码为整体结构，同时采用重构机制增强加密流量指纹的表现能力。该网络可以自动化的从原始流量信息中学习有效特征，并保证识别精度







困难挑战：针对加密流量的特征构建需要大量人工成本，并且特征需要人工验证。

技术路线：从原始流量信息中提取对分类最有效的特征，从而保证分类精度。

在真实流量数据下，识别不同应用的TPR为99.14%，FPR在0.05%。

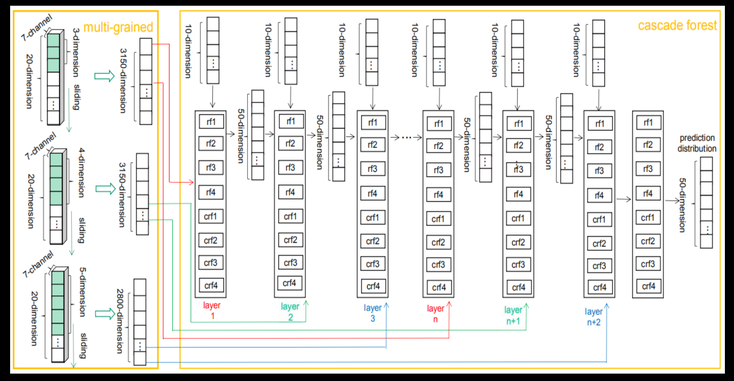
C. Liu, L. He, G. Xiong, Z. Cao and Z. Li, "FS-Net: A Flow Sequence Network For Encrypted Traffic Classification," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, Paris, France, 2019.

团队研究成果

- CIKM2019-基于LRRS和深度森林的SSL/TLS网站指纹细粒度分类

使用本地请求和响应序列（LRRS）作为特征。LRRS使用局部包序列，既可以表示基于HTTP/1.1加密流量，也可以表示基于HTTP/2加密流量。引入深度森林学习原有特征子序列，提取细粒度网站指纹特征并增强特征表示能力。

Feature Type	Description	Feature Number
part1	the total size of incoming[1] packets, the total size of outgoing[2] packets, the packet number of incoming packets, the packet number of outgoing packets, the total size of first 30 incoming packets, the total size of first 10 outgoing packets, the packet number of first 30 incoming packets, the packet number of first 10 outgoing packets, the total size of last 10 outgoing packets and the packet number of last 10 outgoing packets	10
part 2	The duration of the whole pcap is first divided equally into 20 time slices. Then we obtain the total size of incoming packets, the total size of outgoing packets, the packet number of incoming packets and the packet number of outgoing packets in each time slice.	80
part 3	the first 20 incoming packet size, the first 20 outgoing packet size and the last 20 incoming packet size.	60



困难挑战：HTTP/2复用和并发带来的数据包无序性以及细粒度的网站指纹分类。

技术路线：为了在同一个网站上指纹不同的网页，我们引入深度森林提取细粒度特征。它使用卷积结构上充分利用了LRRS序列特征和多层结构，增强了特征表示的能力。

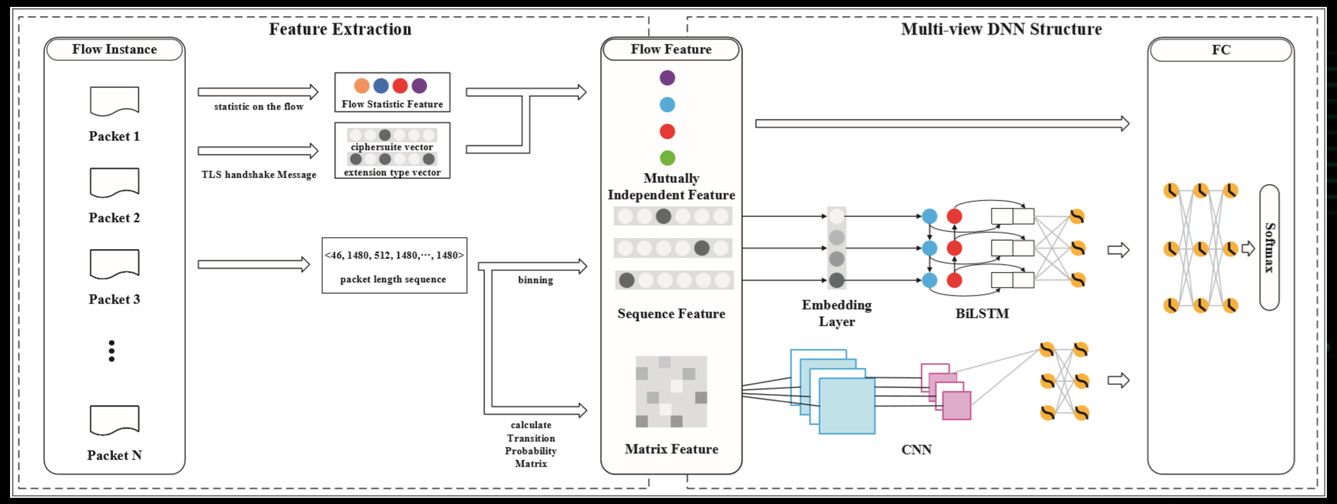
在HTTP/2细粒度分类双向流场景下，LRRS+DF比传统方法F1值高出55%。

Ziqing Zhang, Cuicui Kang, Gang Xiong, Zhen Li,"Deep Forest with LRRS Feature For Fine-grained Website Fingerprinting with Encrypted SSL/TLS" ACM CIKM 2019 - ACM International Conference on Information and Knowledge Management, Beijing, China, 2019

团队研究成果

- GlobeCom 2019-基于多类型特征的深度学习加密网站服务分类模型

  提出了一种充分利用加密流量不同类型特征的深度学习模型。对于不同类型的特征使用特定类型的深度学习算法进行处理。并且将该模型应用于网站服务分类中，一个网站服务可能包含多个网页，为用户提供该网站下的一种特定服务。

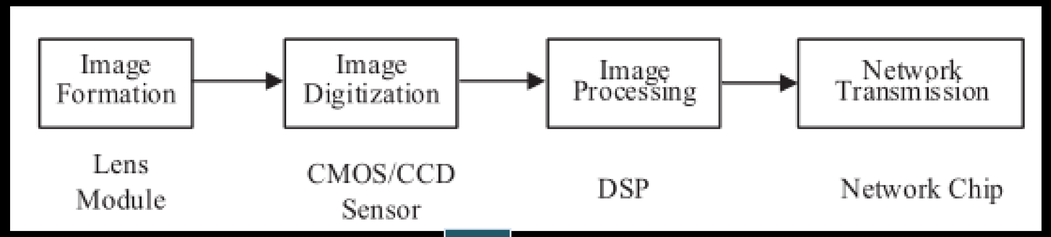


在腾讯公司的真实流量下，针对30中网站服务识别的准确率为93.74%，召回率为93.71%

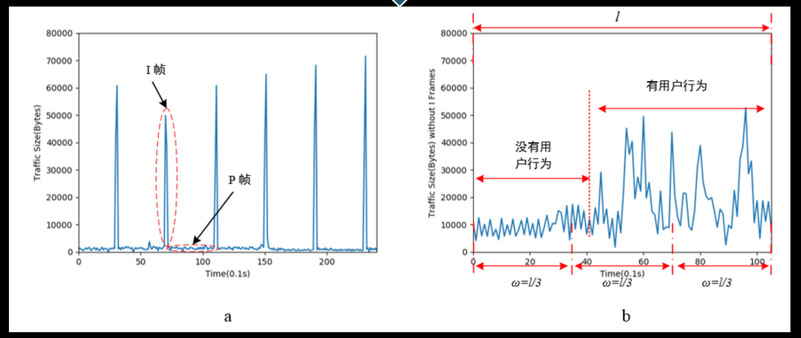
K. Liang, G. Gou, C. Kang, C. Liu, M. Yang and Y, Guo. "A Multi-view Deep Learning Model For Encrypted Website Service Classification," *2019 IEEE Global Communications Conference*, 2019.

团队研究成果

- HPCC 2019-基于加密摄像头流量的用户行为推测

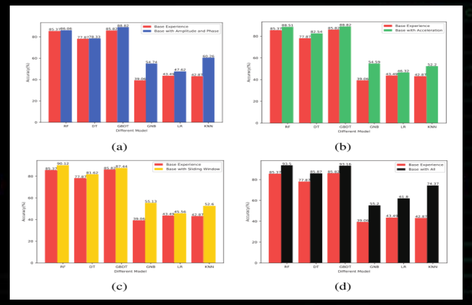


图片处理中差分压缩模块，导致用户不同行为产生不同流量分布



特征提取：提取有效特征表示流量变化

mean, variance, skewness,
kurtosis, duration time
k DFT coefficients
amplitude and phase
acceleration
sliding window.



不同特征组合的识别结果

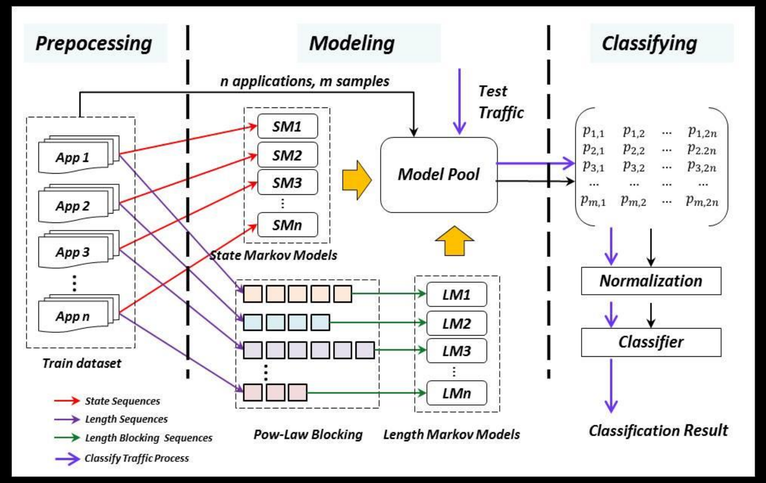
X. Liu, J.Wang, Y. Yang and G. Xiong, " Inferring Behaviors via Encrypted Video Surveillance Traffic by Machine Learning," IEEE HPCC 2019 - IEEE High Performance Computing and Communications, Zhangjiajie, China, 2019.

第七届互联网安全大会 360互联网安全中心

团队研究成果

IWQoS 2018-基于包长度和包间传递关系的加密应用分类

提出了一种融合包多维时间序列属性的加密流量分类方法，在考虑流中包之间的传递关系的基础上，将多个应用的马尔科夫概率作为流的特征，增强了分类识别的鲁棒性和精确性。



困难挑战： 针对加密流量的特征工程构建的有效性难以保证。

技术路线： 利用马尔科夫考虑包之间的传递关系，融合包长度和状态序列构建模型，并采用不同应用的输出概率作为特征。

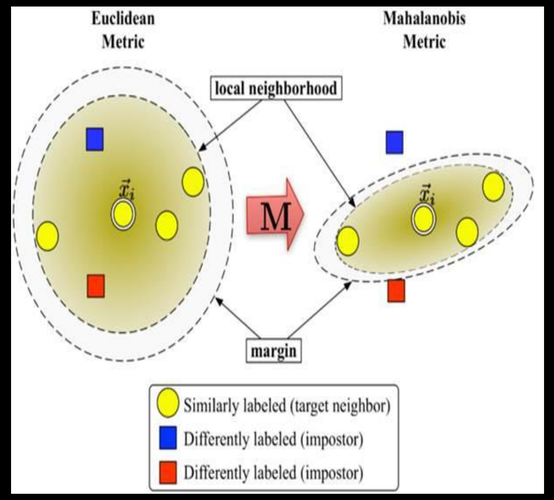
在真实流量数据下，识别不同应用的TPR为96.4%，FPR在0.2%。

C. Liu, Z. Cao, G. Xiong, G. Gou, S. Yiu and L. He, "MaMPF: Encrypted Traffic Classification Based on Multi-Attribute Markov Probability Fingerprints," *2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS)*, Banff, AB, Canada, 2018.

团队研究成果

IPCCC 2017-基于度量学习的开放环境加密流量分类

提出了基于统计特征和距离度量学习的子空间学习模型，通过学习特征的自适应度量矩阵，进行特征选择和关联，解决了流量特征的多属性融合问题，取得了优异的是识别效果。



困难挑战：IP五元组失去作用，具备统计属性的元素有限，如何在时间和空间上挖掘具有判别性能的统计特征。

技术路线：提出使用基于距离度量学习和低秩约束的子空间学习算法，通过低秩约束挖掘特征的关联特性并去除噪声，达到更好的鲁棒性；采用APG加速梯度逼近算法，得到算法的最优解。

同样实验环境下，该算法准确率比RF高了12%，比决策树高了9%。

Zhang Z , Kang C , Fu P , et al. Metrie learning with statistical features for network traffic classification[C]// 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC).

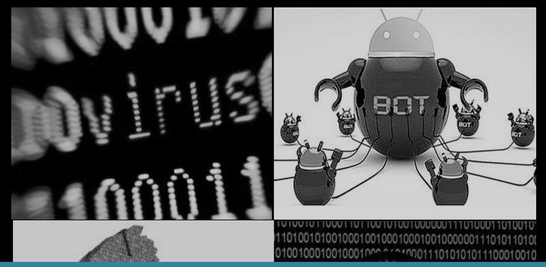
加密数据流量测量与行为分析

2、（对抗-已知）加密网络行为对抗

2、（对抗-已知）加密网络行为对抗

□ 网络流量加密化：SSL/TLS加密流量正在成为恶意服务的温床

勒索病毒
Ransomware



僵尸网络
ZeuS、KINS

木马
Dyre、Dridex

据Gartner预测，到2019年**半数**的**恶意软件活动**将利用某种类型的**加密**来隐藏交付、命

“云”+“加密”使得加密流量分析呈现对抗趋势，如何与之进行有效对抗，是加密网络行为分析中急需解决的难题。

□ 网络

加困难

据Gartner预测，2019年全球公有云服务市场将增长17.3%

单个节点上承载**多种**网络服务
恶意服务混杂其中
云上加密服务的监管更加困难

2、（对抗-已知）加密网络行为对抗

- 节点发现：基于IDC的恶意云节点发现
- 服务发现：基于证书的恶意云服务发现
- 服务细分：云上加密web服务指纹构建

2、（对抗-已知）加密网络行为对抗

- 节点发现：基于IDC的恶意云节点发现
- 服务发现：基于证书的恶意云服务发现
- 服务细分：云上加密web服务指纹构建

2、（对抗-已知）加密网络行为对抗

□ 基于IDC的恶意云节点发现

IDC

- 名称：互联网数据中心（Internet Data Center）。随着移动互联网、云计算、大数据等技术的发展，产业规模高速增长。
- 特点：高带宽，低延迟，服务质量高，规模大，安全可靠。
- 应用：大型互联网企业如Amazon，Google，Akamai，阿里云，腾讯云，都采用自建或租用数据中心作为基础设施。

主机托管	主机租用	机房空间出租	DNS域名解析	虚拟主机

2、（对抗-已知）加密网络行为对抗

□ 基于IDC的恶意云节点发现

IDC与恶意机器流量

- 网络攻击：
  - 僵尸网络、DDoS
- 黑产盈利：
  - 恶意爬虫
  - 领券、刷票、刷广告
  - 视频刷量
  - 游戏挂机
  - 恶意注册

电商	视频直播	游戏	金融
领券	僵尸粉	代练	信用卡刷卡礼
秒杀	刷礼物	工作室练号	银行卡用户回馈
拼团	刷人气	装备奖励	开户奖励
红包抵扣	刷排名	经验升级	新手理财红包

报告1：Distil Networks发布的《2018 Bad Bot Report》显示，在2017年，**恶意机器流量**占到web流量的21.8%。而恶意机器流量中，**82.7%**来自**IDC**。

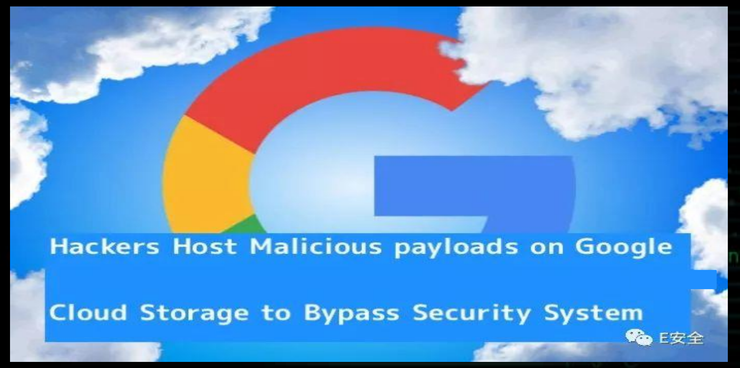
报告2：威胁猎人发布的《在线视频流量欺诈黑灰产研究报告》显示，**在线视频刷量**从业人数十万，年产值十亿，**25%**刷量流量来自**IDC**。

2、（对抗-已知）加密网络行为对抗

□ 基于IDC的恶意云节点发现

IDC与恶意应用

- 托管应用：
  - Amazon云，Zeus C&C，SpyEye木马
  - Google云，4600个钓鱼网页
  - Amazon云， 被恐怖分子所用的 Telegram
- 隐藏应用流量：
  - Tor



支持多种加密协议，采用**domain fronting**技术

利用IDC**转发**自身流量

隐藏自身流量于正常流量中

2、（对抗-已知）加密网络行为对抗

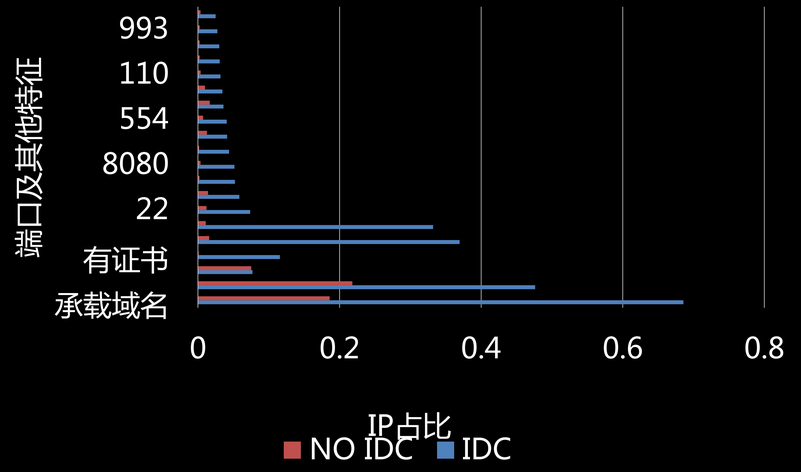
□ 基于IDC的恶意云节点发现

网络攻击　黑产盈利　托管恶意应用　隐藏应用流量

识别IDC，防范网络攻击与黑产行为，提升业务安全能力
理解应用行为，帮助识别应用

识别特定应用，净化网络环境，维护网络安全

- **主动扫描**
- **被动测量**



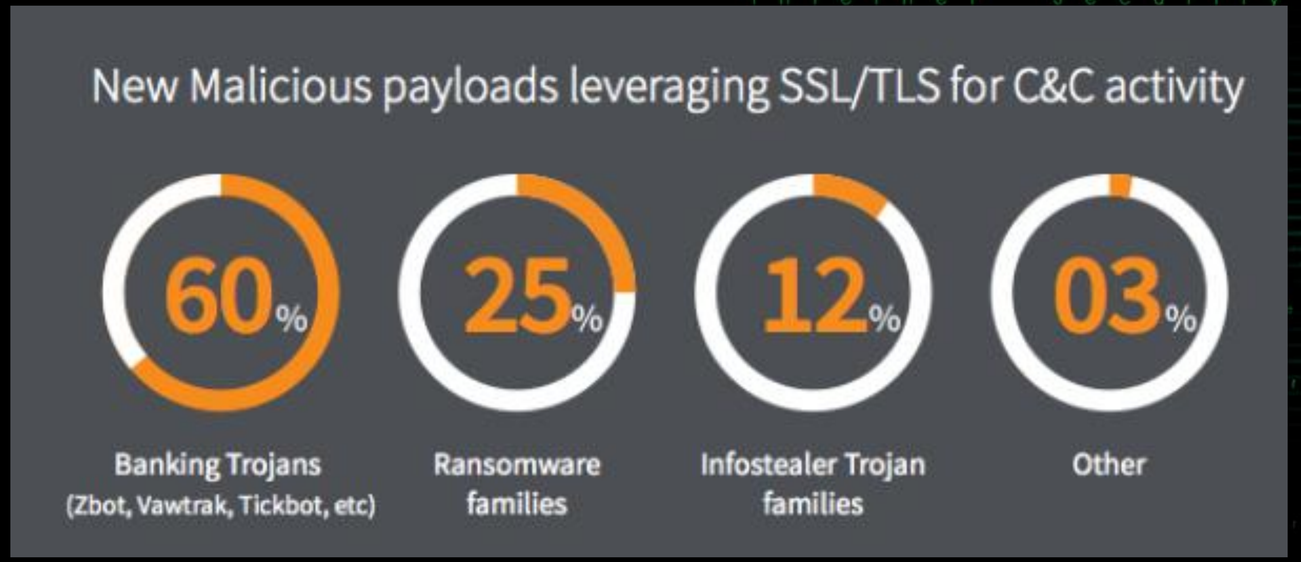
2、（对抗-已知）加密网络行为对抗

- 节点发现：基于IDC的恶意云节点发现
- **服务发现：基于证书的恶意云服务发现**
- 服务细分：云上加密web服务指纹构建

2、（对抗-已知）加密网络行为对抗

□ 基于证书的恶意云服务发现

大量恶意服务利用SSL加密和云躲避安全检测

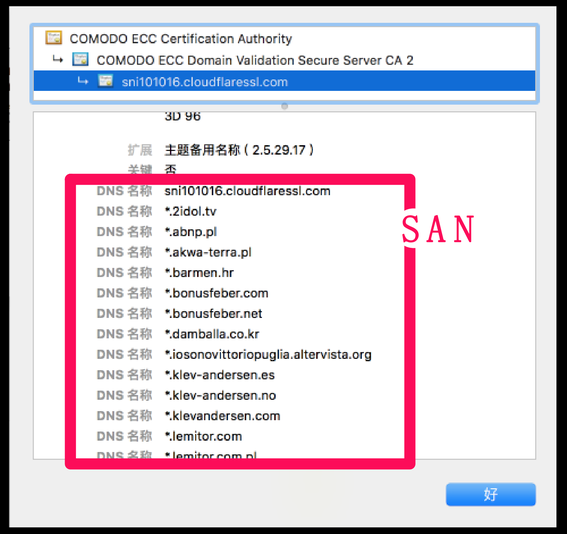


图：使用SSL进行C＆C通信的恶意软件家族分布情况。分别为银行木马、勒索、信息窃取、其他。

2、（对抗-已知）加密网络行为对抗

□ 基于证书的恶意云服务发现

部分恶意网站可以利用**cloudflaressl**等CDN平台颁发的**共享证书**提供SSL服务。



部分非HTTPS网站会返回**其他网站的证书**（访问中华网 返回 chinacenter的证书）

C&C 通信恶意服务的**自签名证书**（相对随意的Subject、Issuer、部分采用过时的TLS版本）

Subject Common Name:	3Vefommmenolfo.realty
Subject:	C=KE, ST=Osesu ticuedec8, L=Nairobi, O=Ttsefs Fevofrs Oyj, CN=3Vefommmenolfo.realty
Issuer Common Name:	3Vefommmenolfo.realty
Issuer:	C=KE, ST=Osesu ticuedec8, L=Nairobi, O=Ttsefs Fevofrs Oyj, CN=3Vefommmenolfo.realty
SSL Version:	TLSv1
Fingerprint (SHA1):	0e1f2ef3c459c74c6d8e76ebbfbf54c3c69354de
Status:	**Blacklisted** (Reason: Dridex C&C, Listing date: 2017-12-17 12:53:29)

第七届互联网安全大会 360互联网安全中心

2、（对抗-已知）加密网络行为对抗

- 节点发现：基于IDC的恶意云节点发现
- 服务发现：基于证书的恶意云服务发现
- **服务细分：云上加密web服务指纹构建**

2、（对抗-已知）加密网络行为对抗

□ 云上加密web服务指纹构建

目前，大部分云平台都提供免费的SSL证书，并且随着云计算的普及，**云上单IP多网站**(图一)现象日趋普遍，使得诸多不良网站的加密通信流量可以**藏匿于正常流量**中(图二)。同时，该类网站经常具有多个域名或克隆站点，使得客户端难以及时获得完整列表进行过滤。

```
Ping www.51dotnet.com [47.90.50.201] 具有 32 字节的数据
47.90.50.201 的回复: 字节=32 时间=41ms TTL=47
Ping www.cdjzyszy.com [47.90.50.201] 具有 32 字节的数据:
47.90.50.201 的回复: 字节=32 时间=41ms TTL=47
```

图一：单IP多网站现象

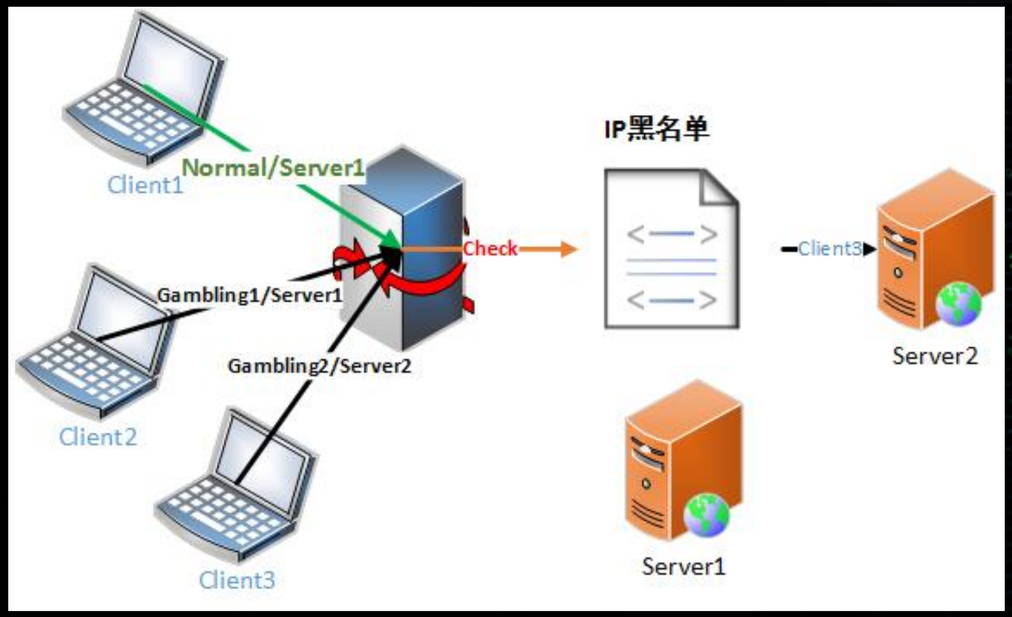
1	y919.com	bet365官网
2	www.xnxx-sextube.com	查询失败!『重试』
3	www.gavbus3.com	Gavbus-老司机AV磁力連結分享 - 日本成人影片資料庫
4	www.lukaskaiser.com	查询失败!『重试』
5	2887k.com	澳门新葡京
6	1.bp.blogspot.com	查询失败!『重试』
7	xv127.xvideos.com	查询失败!『重试』
8	1408kk.com	LNMP一键安装包 by Licess

图二：单IP上的多服务流量混杂现象

2、（对抗-已知）加密网络行为对抗

□ 云上加密web服务指纹构建

针对层出不穷的不良网站，传统的防火墙利用黑名单实现快速过滤，但是该方法在云场景下容易造成误伤，如图三所示。



图三：使用黑名单对加密流量进行分类的困境

Zakir的研究成果（NDSS2017）指出，许多防火墙将**自签发证书注入浏览器**已达到加密流量管理的目的，但是极大的侵害了用户权益。

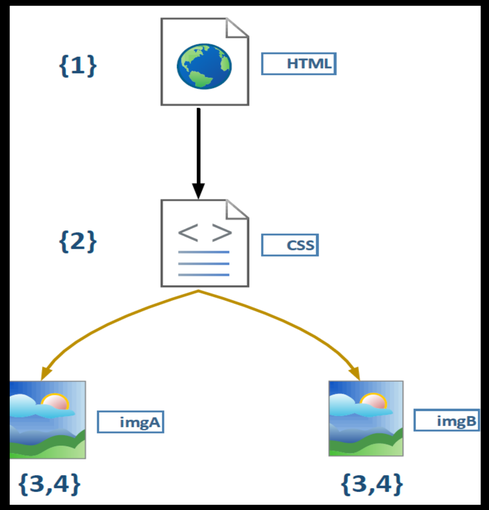
因此，需要研究针对云上加密网站的精细化分类问题。

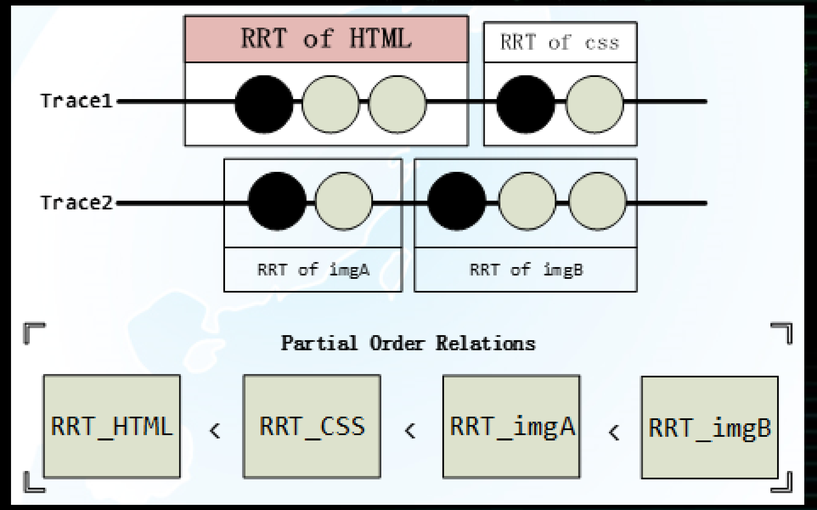
2、（对抗-已知）加密网络行为对抗

口 云上加密web服务指纹构建

- **RRT特征模型**

RRT（Request-Response Tuple）特征模型基于HTTP 1.1协议中的**单连接内串行请求的特征**设计，用于具体刻画每个Web资源的**局部统计特征**。同时，利用**Web资源依赖关系在时间偏序关系上的体现**，依照时序关系选取**前K个RRT**表示整体的网络行为特征。基于局部统计特征的RRT能够避免基于全局视野抽取特征时，采用粗粒度指纹刻画不精确，而细粒度指纹特征维数庞大计算低效的问题。



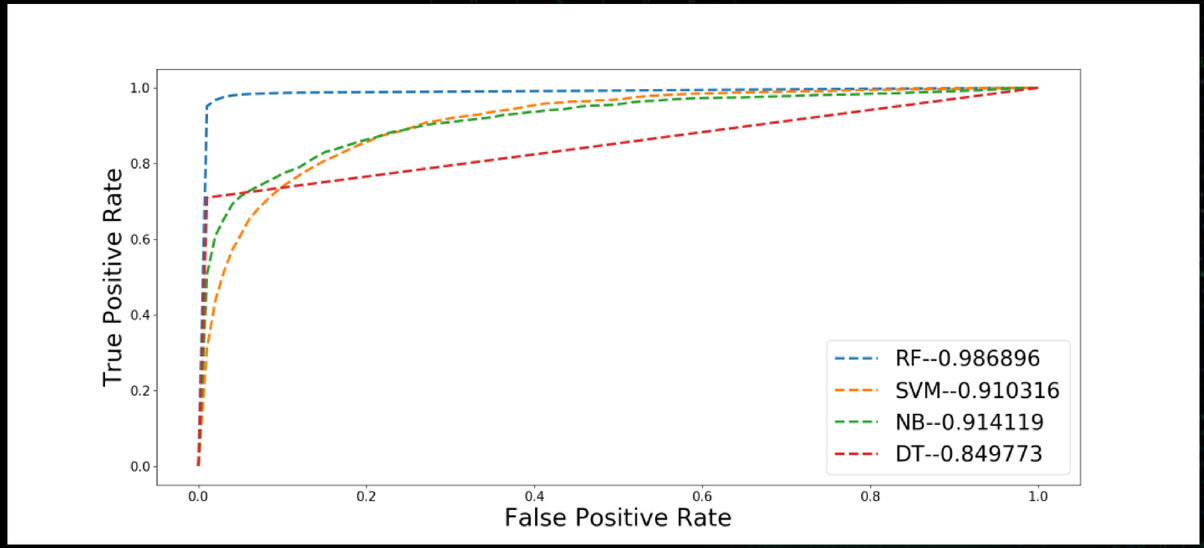


加密网络行为对抗

口 云上加密web服务指纹构建

- **模型效果**

RRT特征模型在不同的机器学习分类算法上达到的效果如右图所示；和已有方法k-fingerprinting (2016 USENIX)相比，如下表所示，我们提出的RRT-RF也明显更为优越。

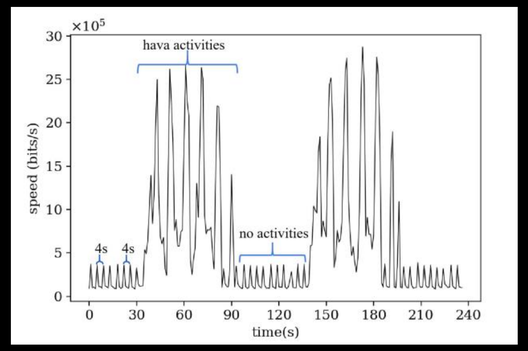


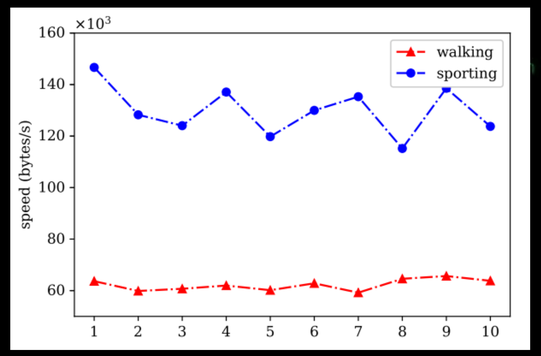
数据集	TPR		FPR	
	RF-RRT	KFP	RF-RRT	KFP
BAE	98.62%	94.24%	0.95%	0.65%
CDN-200	84.85%	62.89%	0.45%	5.25%
BET+CDN-1000	99.34%	89.62%	0.05%	0%

团队研究成果

Globecom 2019-加密云监控摄像头流量中的用户行为分类

提取加密摄像头流量中的统计特征并使用机器学习方法对其进行分类，证实根据流量特征可识别用户行为进而构建日常生活行为规律，用户的隐私安全性受到威胁





监控画面中有人活动和无人活动其数据传输速率存在很大差异，并且不同动作的幅度大小也会对流量传输速率产生一定的影响。根据上下行速率、包数与包长分布、概率转移等特征，可对用户行为进一步细化分类。

Classifier	360's PTZ Camera				Hikvision's EZVIZ C6C			
	$Precision_{ma}$	$Recall_{ma}$	F_{1ma}	Time	$Precision_{ma}$	$Recall_{ma}$	F_{1ma}	Time
Decision Tree	89.37%	89.31%	89.29%	2.5s	82.00%	81.82%	81.82%	2.3s
Gradient Boosting DT	96.41%	96.36%	96.35%	592.9s	94.39%	94.29%	94.28%	458.2s
K-NearestNeighbor	66.76%	58.38%	53.00%	15.4s	69.85%	48.96%	45.31%	12.5s
Logistic Regression	93.62%	93.53%	93.44%	22.1s	92.86%	92.87%	92.77%	11.8s
Perceptron	92.91%	92.87%	92.80%	815.6s	91.33%	91.33%	91.21%	647.4s
Random Forest	97.28%	97.24%	97.23%	3.3s	95.10%	94.93%	94.91%	3.6s
Multilayer Perceptron	94.38%	94.31%	94.27%	329.6s	92.14%	92.16%	92.06%	185.9s
AlexNet	97.97%	97.89%	97.89%	9.15h	95.20%	95.11%	95.10%	8.95h

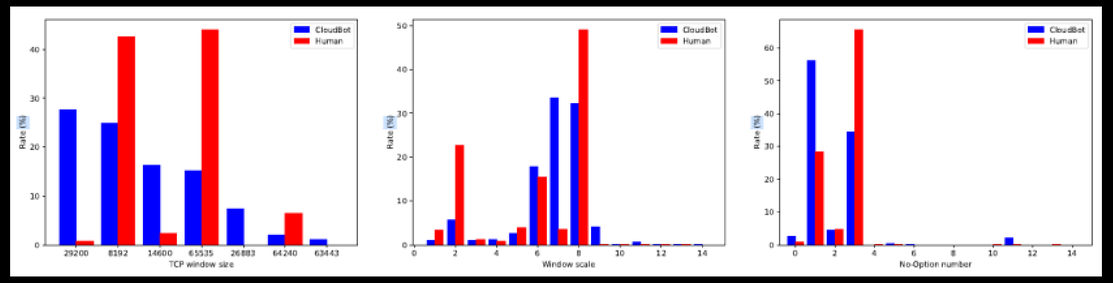
随机森林可兼顾识别精度与速度，以较快的速度达到97.28%的准确率和97.24%的召回率

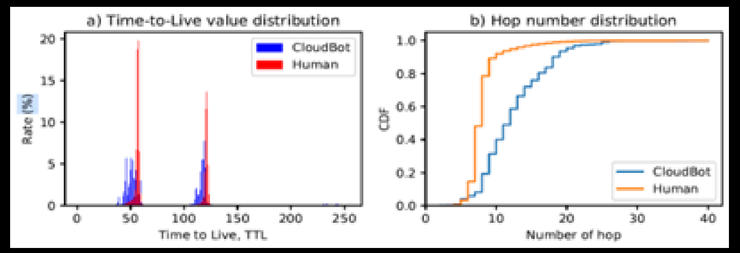
J. Wang, Z. Cao, C. Kang and G. Xiong, "User Behavior Classification in Encrypted Cloud Camera Traffic," IEEE GLOBECOM 2019 - IEEE Global Communications Conference, Waikoloa, USA, 2019.

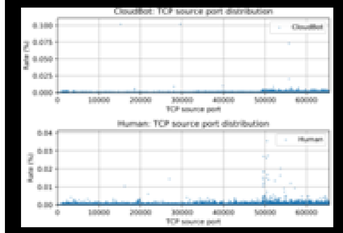
团队研究成果

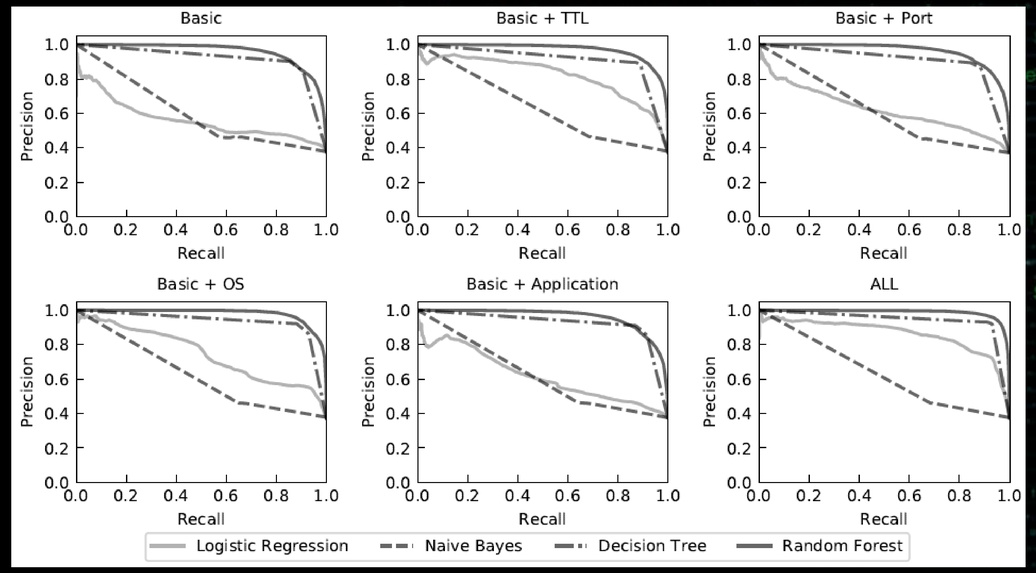
HPCC 2019-基于多层流量信息的恶意网络机器人检测

基于多层流量信息的恶意网络机器人检测









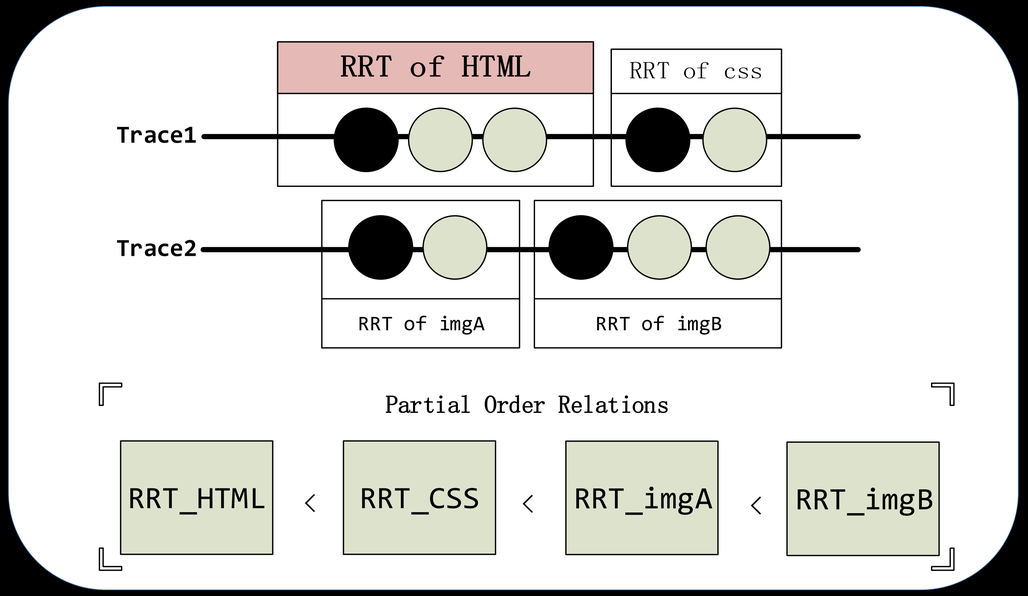
在真实世界数据集的评估上仍能达到90%以上的准确率和召回率。而且不涉及任何具体的应用层字段信息，保护了用户隐私

Y.Guo, J.Shi, Z. Cao , ,C. Kang ,G. Xiong , and Z.Li ,"Machine Learning Based CloudBot Detection Using Multi-layer Traffic Statistics" IEEE HPCC 2019 - IEEE High Performance Computing and Communications, Zhangjiajie, China, 2019.

团队研究成果

ICCS 2018-基于网页加载多流汇聚行为的加密网站指纹

提出了基于网页加载模式的网站指纹模型，通过刻画网页加载所产生的网络行为特征，进行网站指纹分类，解决了云上单IP多网站难精细化区分的问题，取得了良好的分类效果。



困难挑战：可用信息分布于多个TCP流中，实际环境下难以完整汇聚，如何从部分流量上提取出具有代表性的统计特征。

技术路线：提出使用基于HTTP 1.1协议单连接内串行请求特性刻画单个Web资源的局部特征模型，通过时间偏序关系的串联，提取前K个局部特征集，结合随机森林算法，实现指纹分类。

实验环境下，该算法对比k-fingerprinting，TPR提升20%。

Zeng X, Kang C, Shi J, et al. Old Habits Die Hard: Fingerprinting Websites on the Cloud[J]. 2018.

加密数据流量测量与行为分析

3、（检测-未知）潜在威胁发现

3、（检测-未知）潜在威胁发现

- 基于明文：不一致性恶意发现
- 基于密文：匿名网络追踪溯源

3、（检测-未知）潜在威胁发现

- 基于明文：不一致性恶意发现
- 基于密文：匿名网络追踪溯源

3、（检测-未知）潜在威胁发现

口 研究背景

- HTTP流量中存在35%的content-type与实际内容类型不一致的现象。
- 许多恶意软件采用HTTP文件类型伪装的方式绕过检测。
  - APT30将可执行文件伪装成txt文件的方式进行传播；
  - QQ盗号木马将木马样本伪装成图标文件，提高隐蔽性；

不一致进行测量对于隐蔽式网络攻击检测、未知恶意发现具有重要意义

/ForZRLnk3z/bak.txt	Switch to backup stage one C2 server (BACKSPACE is typically configured with main and backup first-stage C2 servers).
/ForZRLnk3z/app.txt	Download and execute the file.
/ForZRLnk3z/myapp.txt	Download and execute the file (if victim appears in hostlist.txt).
/ForZRLnk3z/ver.txt	Perform version check.
/ForZRLnk3z/exe.txt	Download and execute the file if the version check fails (self-update).
/ForZRLnk3z/SomeUpVer.txt	Backup URI for version check.
/ForZRLnk3z/SomeUpList.txt	List of hostnames that should perform self-update if backup version check fails.
/ForZRLnk3z/SomeUpExe.txt	Backup URI for self-update.
/ForZRLnk3z/dizhi.gif	Second-stage C2 information (IP address and port(s)).
/ForZRLnk3z/connect.gif	List of victims to connect to second-stage C2 controller.

3、（检测-未知）潜在威胁发现

不一致性测量内容

为绕开检测，恶意软件通过如下伪装行为：

伪造文件类型：文件类型不一致
- Content-type, URI声明的类型与实际载荷类型不同

伪造文件大小：文件大小不一致
- Content-length声明的大小与实际载荷大小不相等

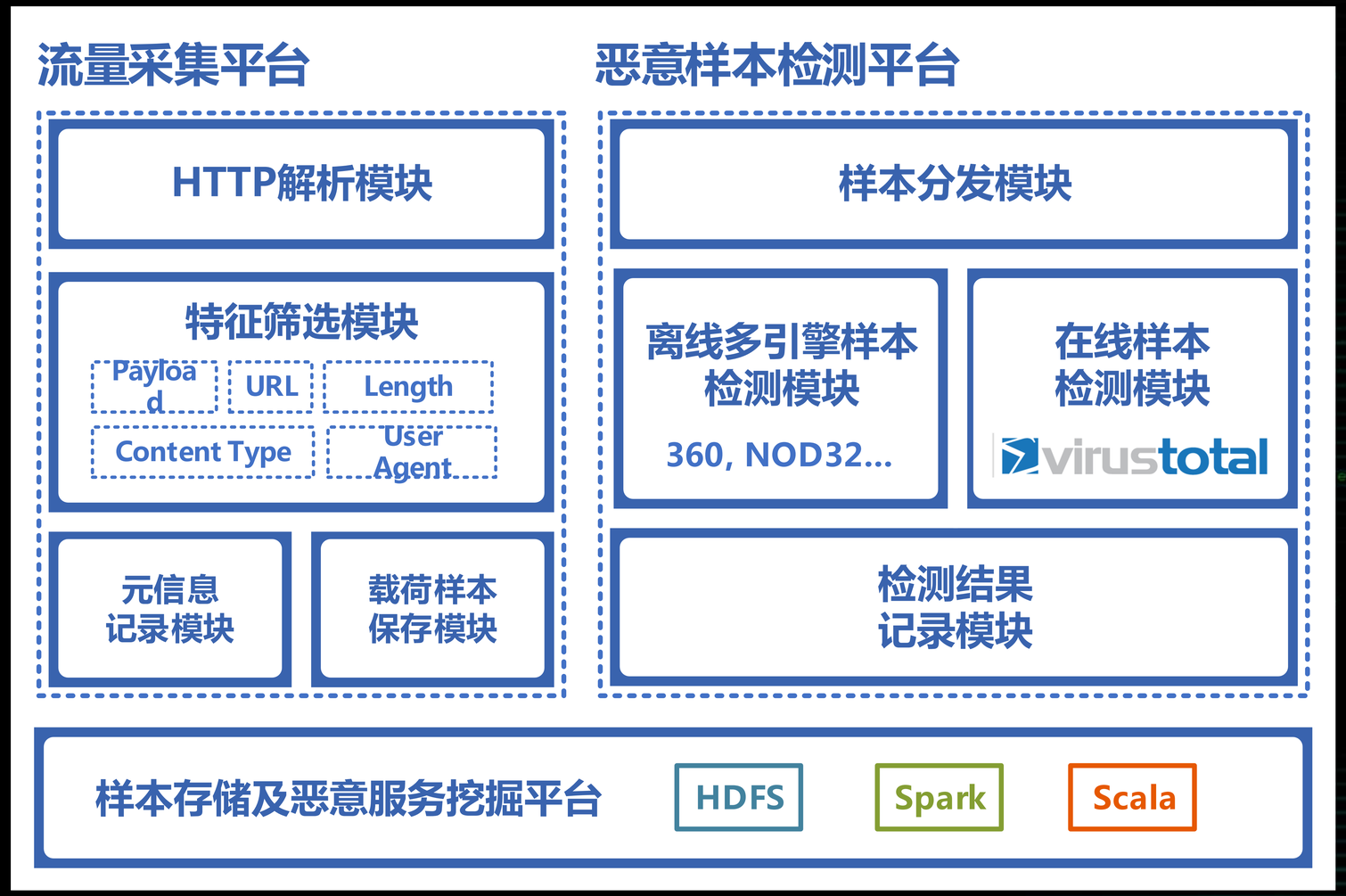
伪装目标主机：目标主机不一致
- Host声明的目标主机与目标IP不属于同一个机构

伪装服务端口：服务端口不一致
- 如目标端口与HTTP协议常用端口（80，8080）不同

变化传播路径：传播路径不一致
- 主动下载与被动监测不一致

3、（检测-未知）潜在威胁发现

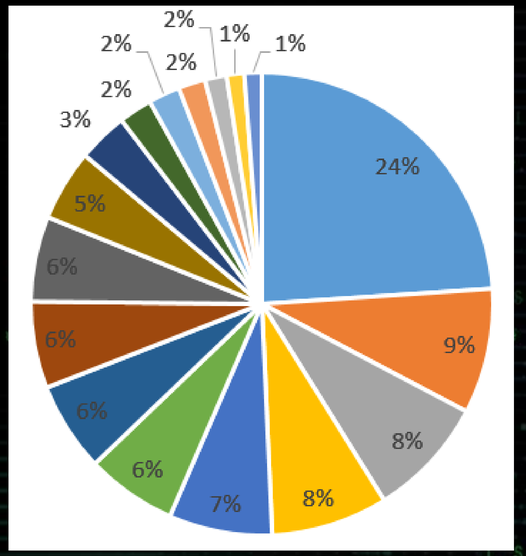
体系架构

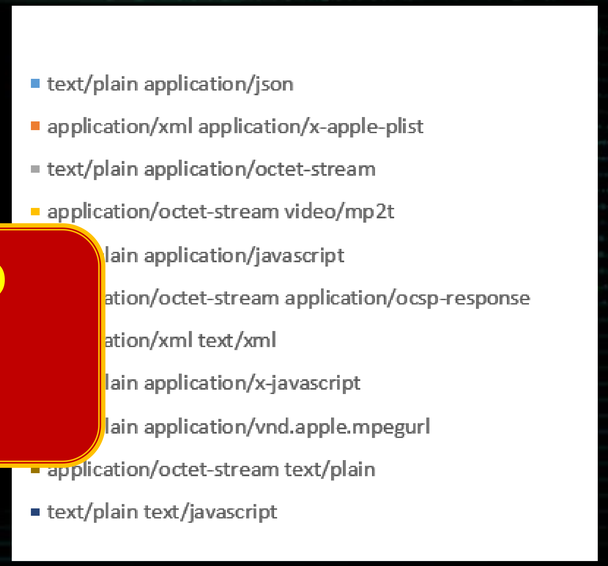


3、（检测-未知）潜在威胁发现

Content-type不一致测量

- 数据来源：
  - 科研网测量，共发现1604种HTTP内容与载荷不一致的现象
- 对1604种不一致进行分析，发现通过恶意软件主要是PHP和PE文件，因此缩小不一致的范围



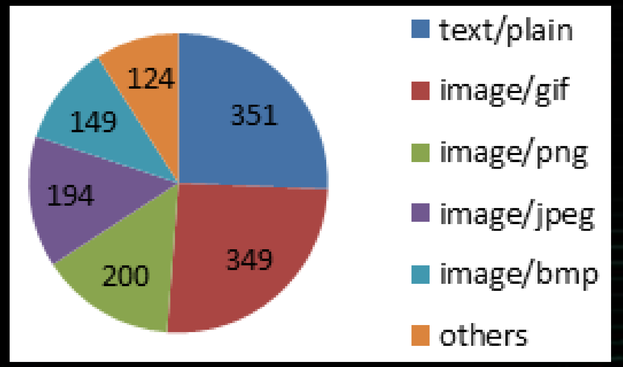


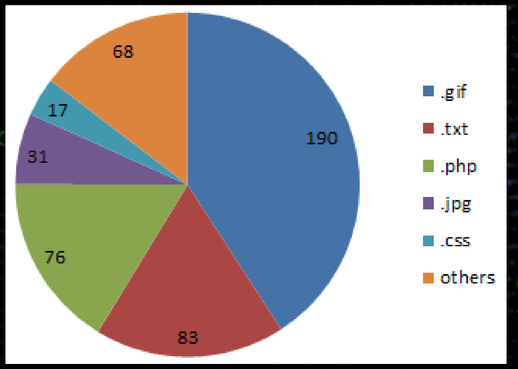
攻击者通过不一致手段隐蔽式地传播PHP和PE攻击文件

3、（检测-未知）潜在威胁发现

文件类型不一致测量结果

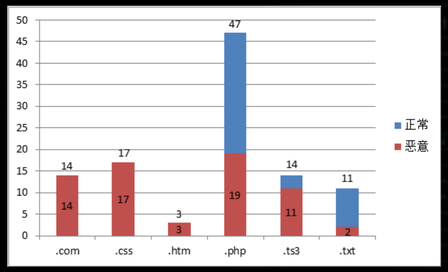
- 数据集：
  - 1484个类型不一致的PE文件
  - 1367个Content-Type不一致的PE文件
  - 465个URI扩展名不一致的PE文件
- 3个类别的不一致的数量及比例如下：





文件类型不一致的类别	所有数量	恶意的数量
Content-Type不一致 extension不一致	336	293(87.20%)
Content-Type不一致，extension一致	1031	753(73.04%)
Content-Type一致，extension不一致	117	108(92.30%)

3、（检测-未知）潜在威胁发现



Content-Type_extension不一致测量结果

- 文件类型声明值只有图片和文本两种类型
- 声明成图片：几乎100%恶意
  - （227/230）为已知恶意，2个为未知恶意（rescan by VirusTotal），余下一个行为特征可疑
- 声明成文本：特定扩展名为恶意的概率高，但样本数量少

Content-Type不一致测量结果

	恶意	正常
URI的形式	无后缀，形式为“http://IP:PORT/MD5”	有文件后缀
URI的级数	<3	>3
Host的形式	IP	域名
主动访问（两周后）	失效	有效

- 声明值只有图片和文本两种类型
- 几乎都是恶意的
- 对Content-Type为“text/html”的PE文件进行分析，发现正常文件和恶意文件具有以下差异，可用于辅助恶意检测：

extension不一致测量结果

- 声明值只有文本类型
- 声明成文本：**特定扩展名为恶意的概率大，但样本数量少**

3、（检测-未知）潜在威胁发现

Host不一致测量

- Host不一致定义：
  - Host头域与目标IP地址所属组织不同
- 测量结果：
  a) 比例关系：测试数据集中恶意比例为12.31%（1000/8123），而不一致中恶意比例为10.11%（433/4285）；
  b) 暂无有效特征用于恶意检测

```
GET /d/conh11.jpg HTTP/1.1
Accept: */*
Host: www.google.com
User-Agent: Mozilla/5.0
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx
```

Malware:TROJ_RODECAP.SM
伪造Host域，真实域名非google

服务端口不一致测量

- 端口不一致定义：
  - 服务端口为非IANA规定的常规端口（80,8080）
- 测量结果：
  - 服务端口不一致中恶意比例为96.55%（3527/3653）
  - 常用端口中恶意比例为5.93%（7991/134479）

3、（检测-未知）潜在威胁发现

文件大小不一致测量

- 经测量，发现能应用于恶意行为检测的结果：
  - 声明值小于0的恶意比例达到40.52% (94/232)
  - 其他方面没有看到明显的区分特征

主被动下载不一致测量

- 主被动下载不一致定义：
  - 恶意软件通过变换传播路径或者仅在特定时间段有效，导致主动下载失效（主动下载失败或者主动下载的文件不是PE文件）。
- 测量结果：
  - **89.57%**（6946/7755）为恶意
  - 另外，发现**未知**恶意软件52个

3、（检测-未知）潜在威胁发现

文件类型不一致之PHP文件分析

- 发现存在**伪装成图片**的PHP shell恶意脚本代码
  - Content-type为“image/jpg”，实际类型为“text/x-php”
  - 具有查询服务器文件及文件夹信息，修改文件、上传下载等功能
  - 具有暴力破解ftp、sql密码、窃取文件并上传到恶意服务器的功能

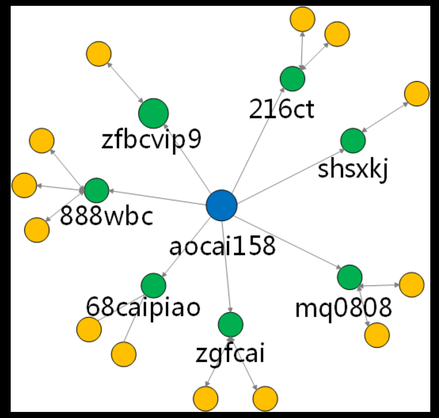
对PHP文件中不一致的分析可以发现隐蔽式Webshell攻击

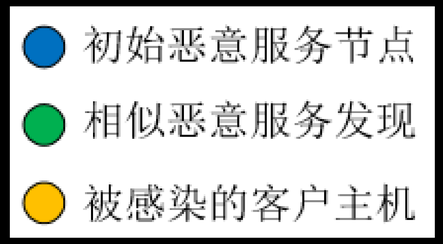
- 发现**伪装成图片**的PHP测试攻击
  - Content-type为“image/jpeg”，实际类型为“text/x-php”
  - 功能为根据某路径下的已有6个图片生成新图片，设置content-type类型
  - 猜测是攻击者对该网站服务器进行的测试攻击
- 发现服务器配置/宕机问题导致PHP解析失效泄露源码

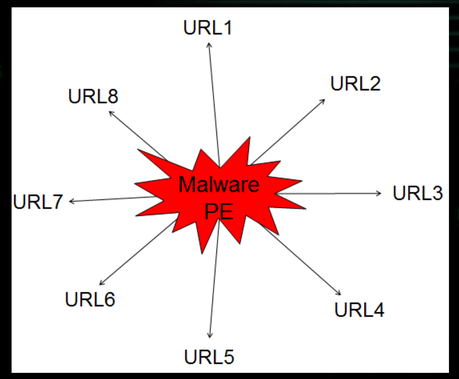
3、（检测-未知）潜在威胁发现

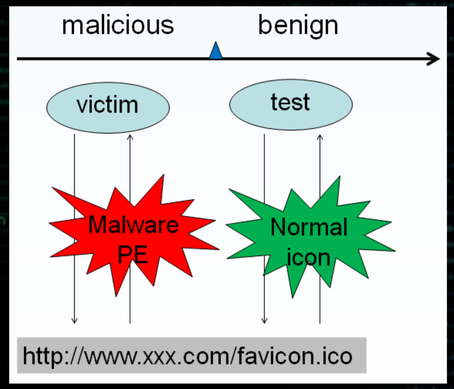
典型攻击事件分析挖掘

- 通过**关联分析**挖掘出针对博彩网站的隐蔽式挂马攻击 [Journal of Super-computing (**SUPE, CCF C**)]
  - 通过样本检测发现样本favicon.ico (host: aocai158) 存在恶意行为
  - 通过MD5、URL(*/favicon.ico)**关联分析**发现7个相似的隐蔽式网络攻击









- 基于URL失效性进行恶意检测，准确率89.04%，发现未知52个[S&P 2016（CCF A，poster)]
  - 攻击者采用变换URL的方式进行恶意样本传播，导致URL失效
  - 存在隐蔽式网页挂马攻击只在特定时间活跃，隐藏挂马攻击行为

第七届互联网安全大会 360互联网安全中心

3、（检测-未知）潜在威胁发现

- 基于明文：不一致性恶意发现
- **基于密文：匿名网络追踪溯源**

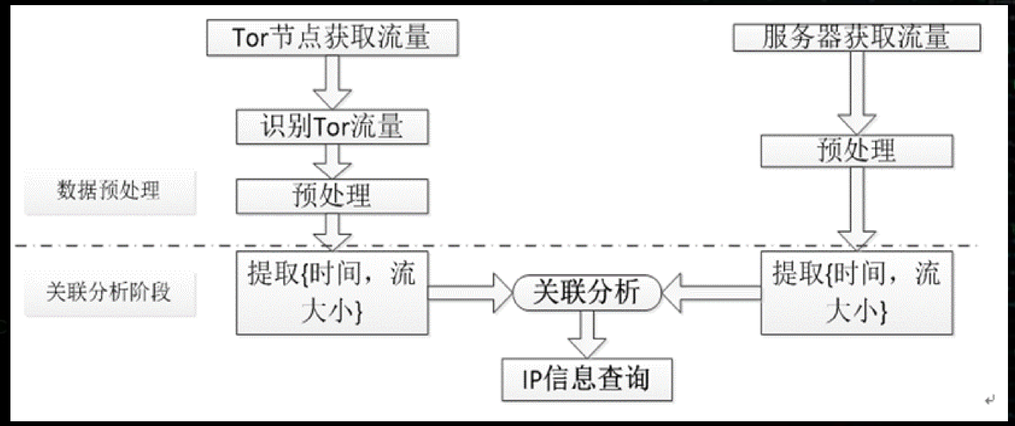
3、（检测-未知）潜在威胁发现

□ 匿名网络追踪溯源

1. 基于网络流量的信息溯源关键技术研究

在流量分析的基础上，尝试破除匿名网络的不可关联性。对获取到的匿名网络入口和出口流量进行关联、去匿名化分析，达到追踪溯源的效果。在网络犯罪监管和调查方面有很大的意义。

溯源过程包括针对匿名网络Tor的流量识别、已识别流量的重组和过滤、出入口流量关联、对关联到的IP地址进行信息查询。



信息溯源关键技术流程

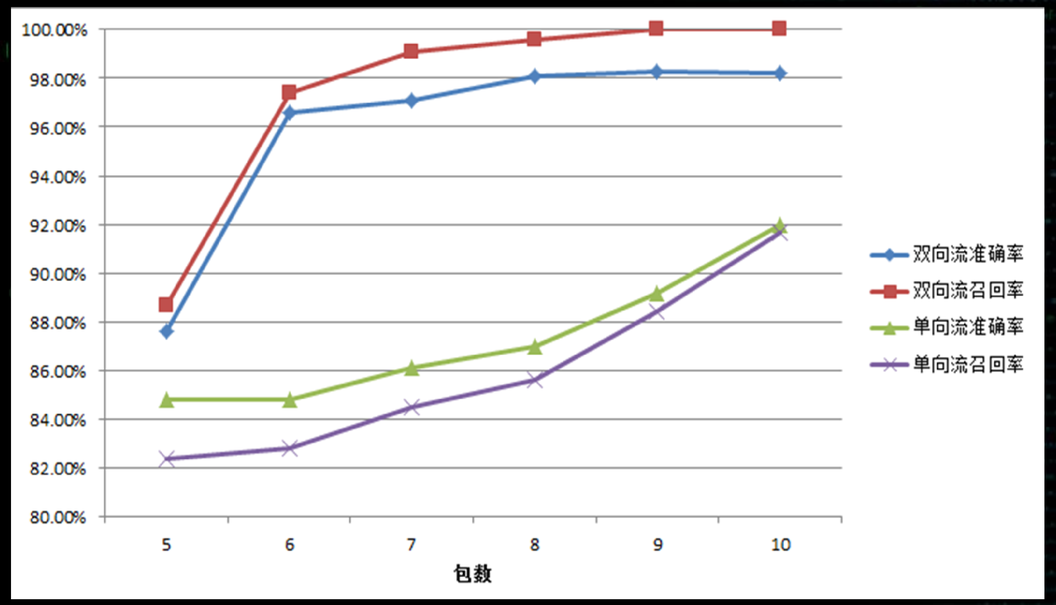
3、（检测-未知）潜在威胁发现

匿名网络追踪溯源

信息溯源关键技术研究——流量识别、重组与过滤

考虑到匿名性强弱与匿名集合的大小直接相关，在对Tor流量进行关联溯源之前，首先以包长、方向为特征，从全部流量中识别出Tor流量，缩小匿名集合、降低溯源难度。

对识别流量，按五元组将数据包还原为流，同一五元组如果超过60秒没有新数据包到达，则认为流已结束。流重组完成后过滤出满足一定字节数的数据流。



识别率随统计包数的变化

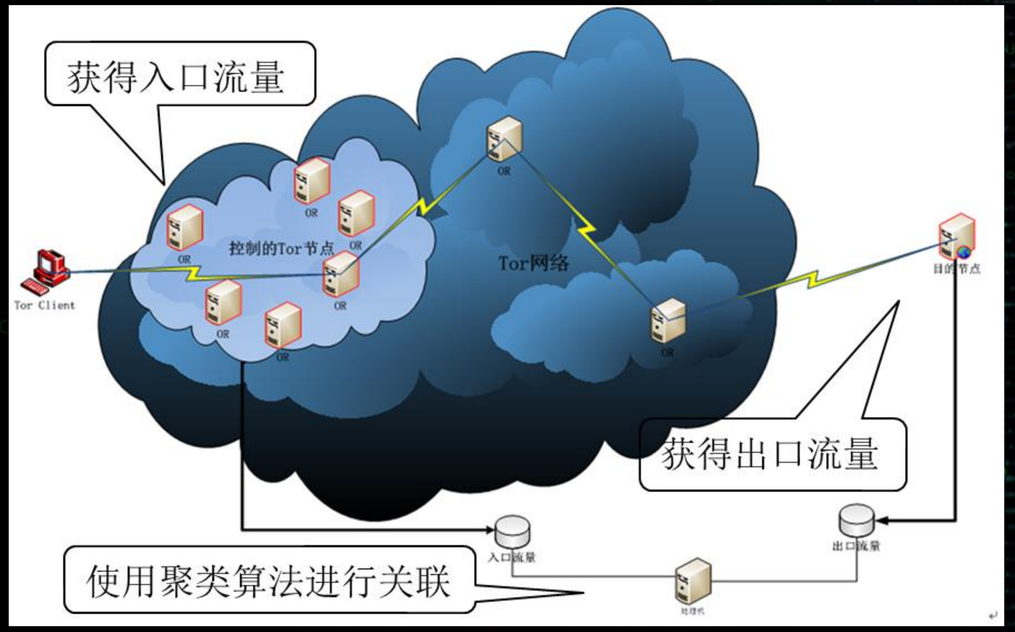
3、（检测-未知）潜在威胁发现

匿名网络追踪溯源

信息溯源关键技术研究——流量关联

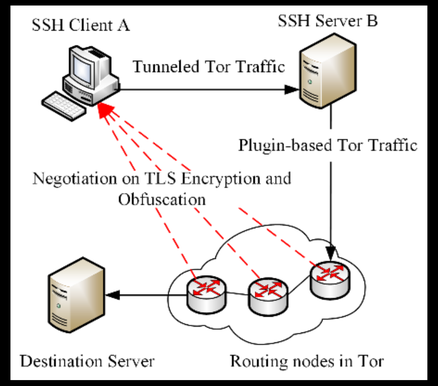
关联依据：低延迟的特性决定了Tor不会对数据流进行大程度变换，因此出口与入口的流量增长模式差异不会很大，如某段重叠时间内同时出现突发流量。

基于k-means的关联分析：由于增长模式相似，使用聚类算法后，那些与特定出口流聚类到同一类中的入口流，很可能是与此条出口流对应的入口流，由此获取可疑入口IP集合。



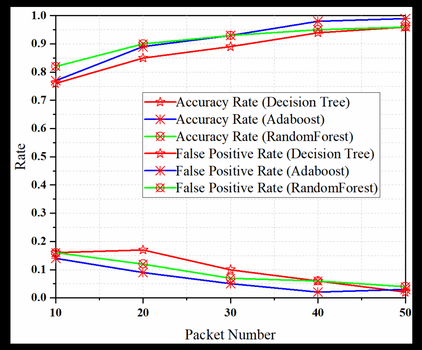
团队研究成果

Milcom2019-加密隧道中匿名网络流量的识别及关联



SSH动态转发将匿名流量封装在隧道中

匿名网络用户面临两方面安全威胁：内部节点监听和外部流量分析。将匿名流量封装在加密隧道中传输(如配置SSH代理动态转发匿名流量)可以抵御恶意节点，但在面对流识别、流关联等分析手段时能否保证匿名服务持续可用且不被溯源，还需实验验证。



部分识别结果

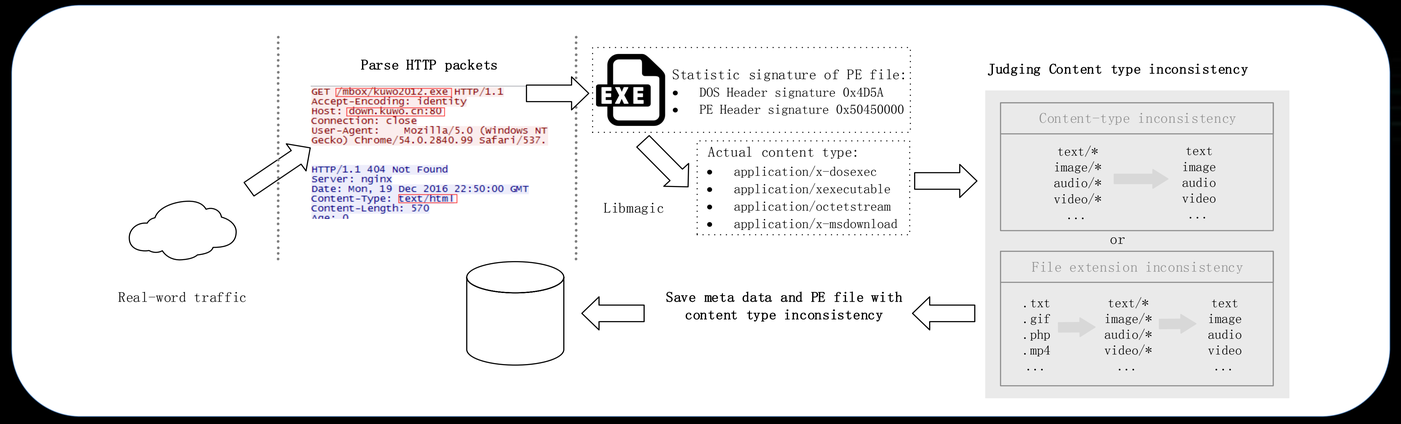
论文构建流量的外部特征转移矩阵，利用机器学习方法实现流量的识别和关联，评估经过加密隧道封装后匿名网络流量的可用性和不可追溯性。在实验环境下得到较高的识别和关联准确率，证明即使经过插件混淆和加密隧道的封装，匿名网络流量仍表现出一定的可区分性。

Zhong Guan, Gaopeng Gou, Yangyang Guan, Bingxu Wang, "An Empirical Analysis of Plugin-Based Tor Traffic over SSH Tunnel" IEEE MILCOM 2019 - International Conference on Military Communication, Norfolk, America, 2019

团队研究成果

IPCCC 2017-基于不一致性测量与分析的网络恶意行为检测

目前HTTP协议占据网络流量中很大的一部分，将恶意代码隐藏于正常HTTP流量中传播是常用的逃逸检测手段。通过对多种HTTP不一致进行测量，提取恶意软件隐蔽式传播的特征，借助机器学习的方法进行网络恶意行为检测。



Xu F , Pan H , Cao Z , et al. Identifying malware with HTTP content type inconsistency via header-payload comparison[C]// 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC). IEEE, 2017

技术路线：对HTTP文件类型声明与实际不一致、Content-Length与实际载荷大小不一致、服务端口与IANA规定的常规端口不一致、Host声明与实际通信服务器不一致、主动下载与被动捕获文件不一致五种不一致场景的可执行程序进行测量。

加密数据流量测量与行为分析

4、（对抗-未知）未知威胁对抗

4、（对抗-未知）未知威胁对抗

- 新型化：区块链网络测量与行为分析
- 混淆化：隐蔽信道

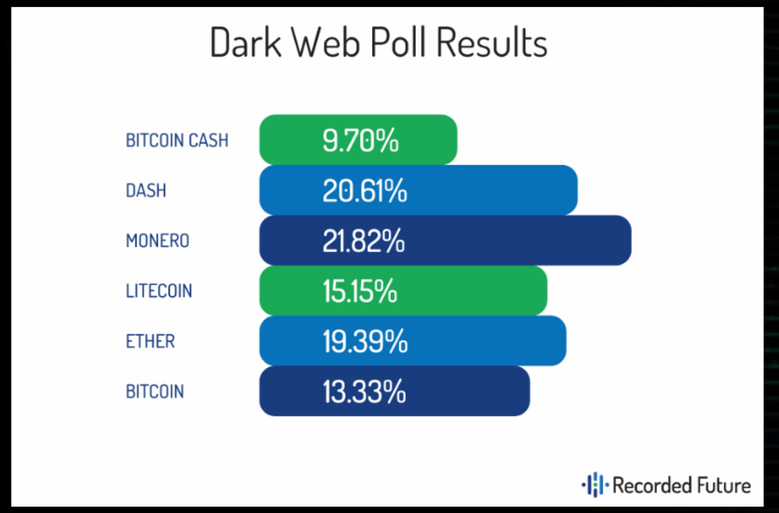
4、（对抗-未知）未知威胁对抗

- 新型化：区块链网络测量与行为分析
- 混淆化：隐蔽信道

未知威胁对抗

口 区块链网络测量与行为分析

1. 区块链安全



德国亚琛工业大学和德国法兰克福大学一组研究人员对比特币区块链信息进行量化分析发现，添加到比特币区块链的1600份文件中，就有59份文件包含指向非法儿童图片、政治敏感内容或侵犯隐私的链接。

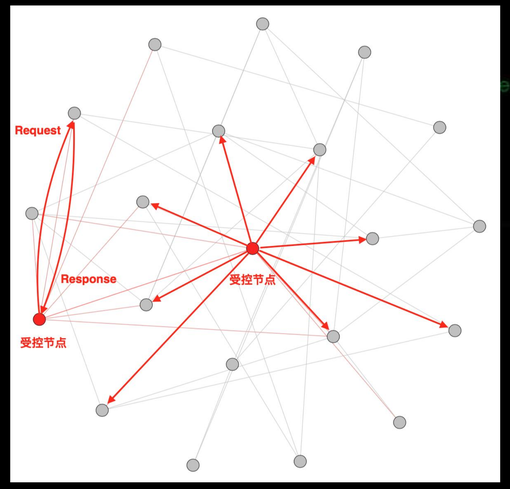
未知威胁对抗

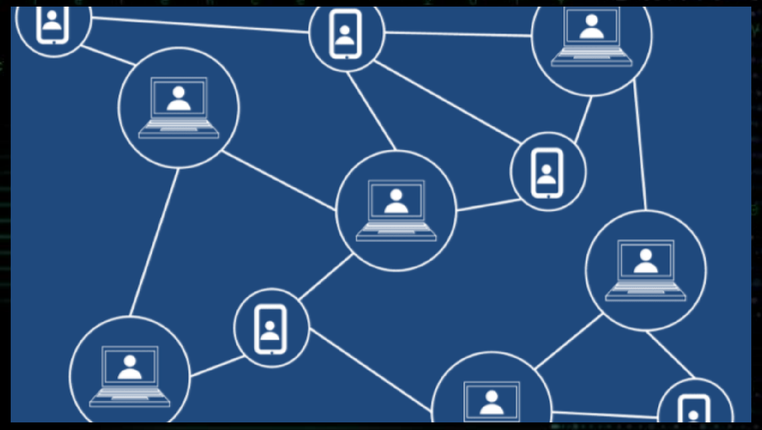
□ 区块链网络测量与行为分析

2. 区块链测量方法总结

SHODAN

ZoomEye





主动扫描

覆盖广、准确率低

植入节点

增加负载、轻节点缺失

网关检测

覆盖轻节点

主动测量

被动测量

未知威胁对抗

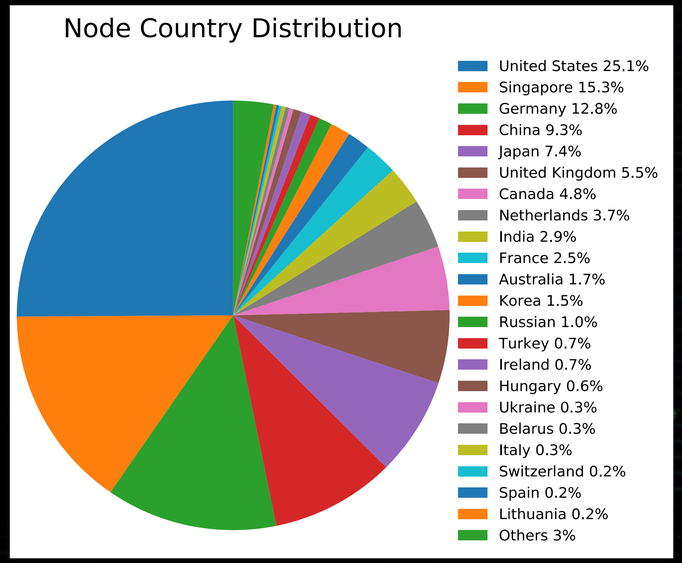
□ 区块链网络测量与行为分析

3. 区块链（以太坊）被动测量

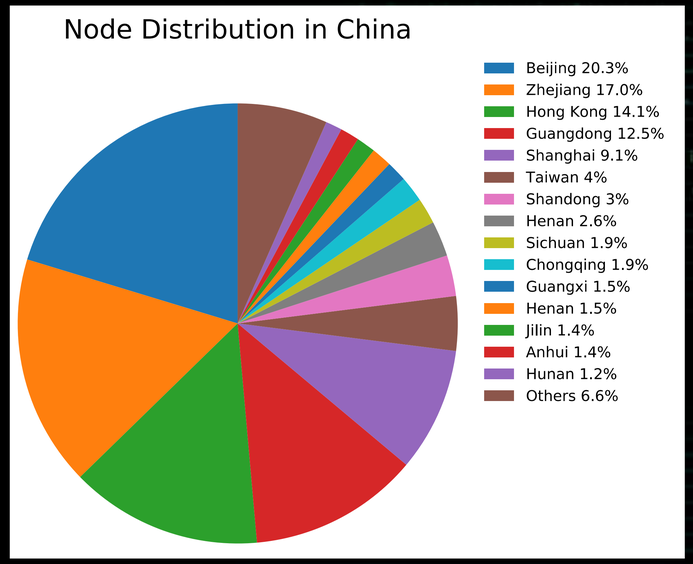
极少数的IP承载了大多数的节点

以太坊日志量18亿-20亿条/天 连接数3亿-4亿条/天

端口主要分布在30000与50000



以太坊节点全球分布



以太坊节点在中国的分布

未知威胁对抗

□ 区块链网络测量与行为分析

4. 区块链行为分析

	行为名称	对应操作	是否加密
比特币-区块链（Bitcoin Core）	发现节点	version；verack	×
	获取节点信息	getaddr； addr	×
	获取区块头	getheaders；headers	×
	获取区块数据	getblocks； inv；getdata；block	×
	创建钱包	createwallet	×
	发送交易	tx	×
	检查交易	checkorder	×
	确认交易	submitorder	×
	测试TCP/IP连接可用性	ping	×
	节点间发送通知	alert	×
	挖矿	miner	×

比特币网络行为分析

	行为名称		对应操作	是否加密
以太坊-区块链(Geth)	创建账号		personal.newAccount()	√
	锁定账号		personal.lockAccount()	√
	解除锁定账号		personal.unlockAccount()	√
	查询账户信息		eth.accounts	√
	查询账户余额		eth.getBalance()	√
	获取区块信息		eth.getBlock()	√
	获取最新区块号		eth.blockNumber	√
	查询交易信息		eth.getTransaction()	√
	部署智能合约			√
	调用智能合约		contract.multiply.call()	√
	挖矿	CPU挖矿	miner.start()	√
		GPU挖矿		
		矿池挖矿		
	停止挖矿		miner.stop()	√

以太坊网络行为分析

	行为名称		对应操作	是否加密
以太坊-区块链2.0代表平台	同步数据	模式：full	geth --syncmode “full”	√
		模式：fast	geth –fast –cache 512	√
		模式：light	geth --light	√
	交易	由钱包发起的交易	eth.sendTransaction()	√
		由合约发起的交易		
	提交交易		把交易加入到交易缓冲池中（txpool）	√
	广播交易		通知EVM执行，把交易信息广播给其他节点	√
	节点发现	ping packet	尝试连接其他节点	×
		pong packet	回应ping包	×
		findnode packet	请求附近节点信息	×
		neighbors packet	邻居节点对findnode包回复	×

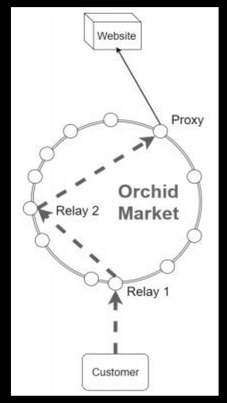
4、（对抗-未知）未知威胁对抗

- 新型化：区块链网络测量与行为分析
- **混淆化：隐蔽信道**

4、（对抗-未知）未知威胁对抗

□ 隐蔽通道

1. 典型技术

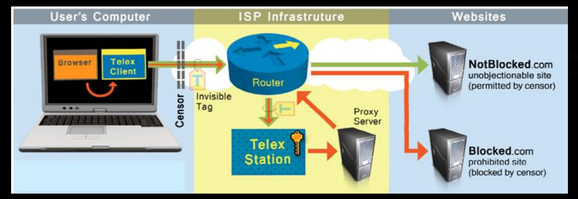


Orchid网络

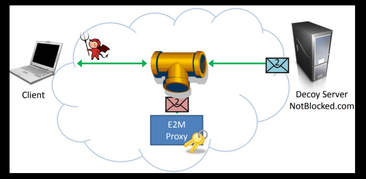
HTTPS网络代理

Web匿名代理

代理转发



Telex架构



Tapdance架构

基础设施整合

Tor网络

i2p网络

JAP网络

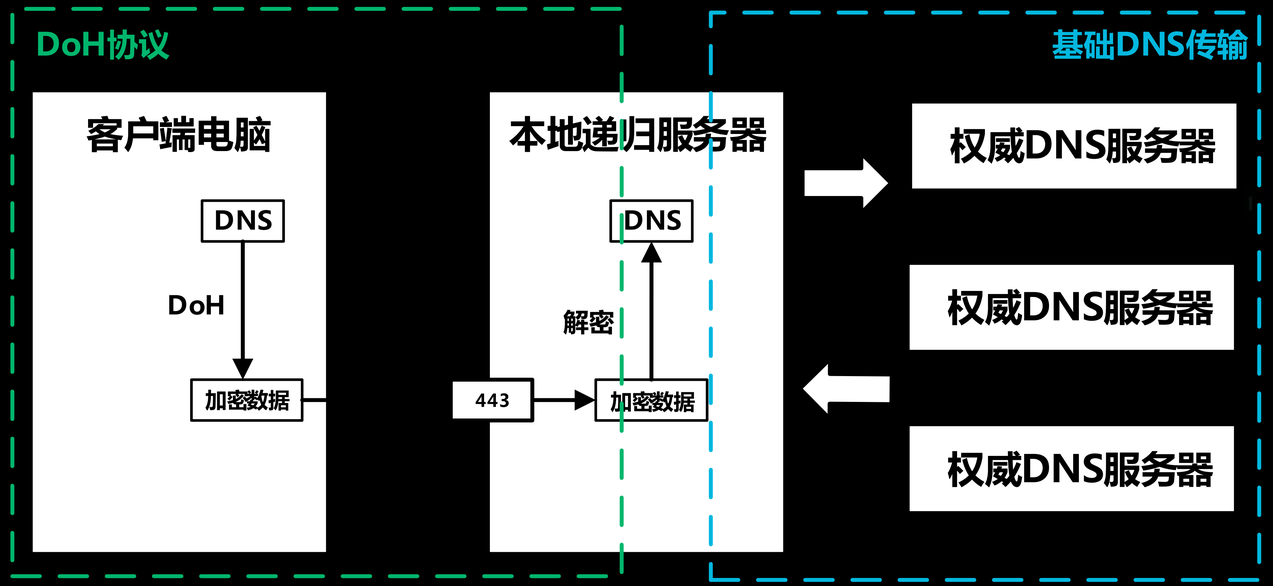
Loopix网络

匿名通信系统

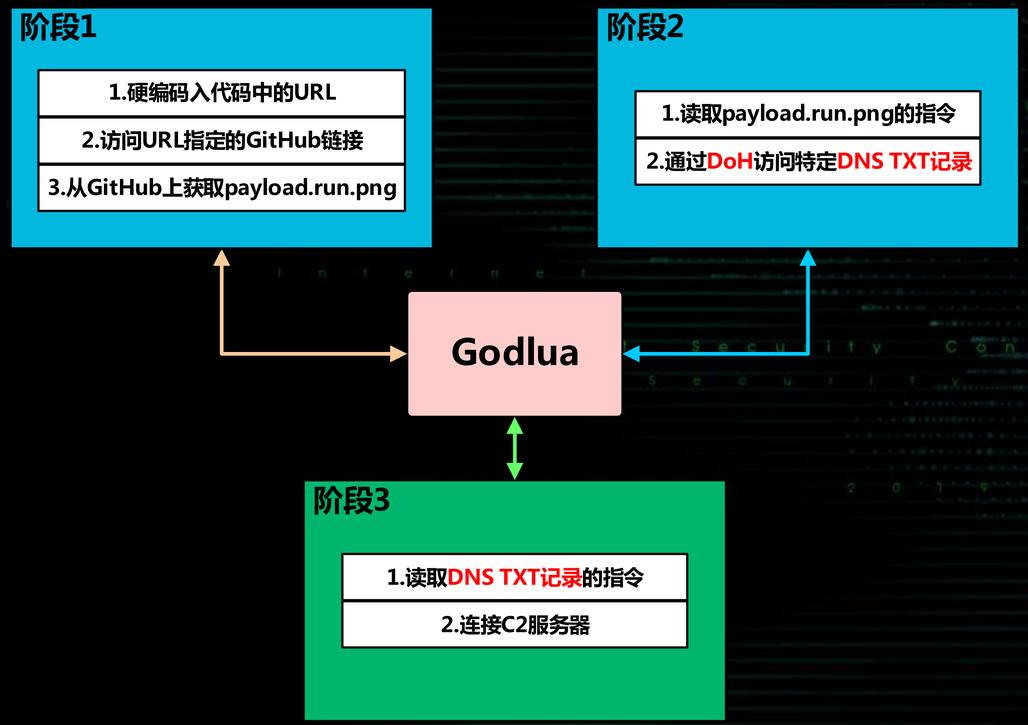
4、（对抗-未知）未知威胁对抗

□ DNS over HTTPS

在整个DNS请求过程中，只有客户端与本地递归服务器之间的DNS报文会被转化为DoH。



基于DoH的DNS请求加密

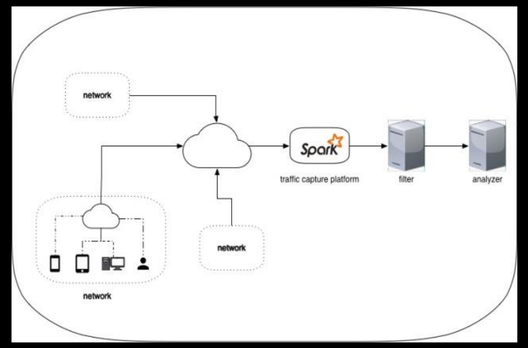


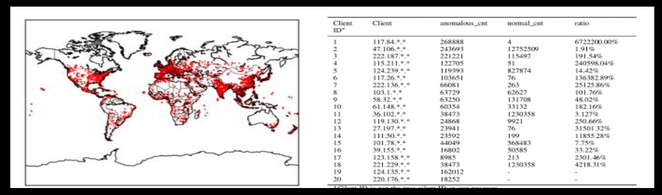
基于DoH的恶意软件Godlua

团队研究成果

HPCC 2019-网络流量中异常用户代理的分析

通过用户代理（UA）中存在异常字符的现象，构建系统使用正则表达式检测异常UA，并且从客户端的角度分析了这些异常UA产生的原因





Client ID*	Client	anomalous_cnt	normal_cnt	ratio
1	117.84.*.*	268888	4	6722200.00%
2	47.106.*.*	243693	12752509	1.91%
3	222.187.*.*	221221	115497	191.54%
4	115.211.*.*	122705	51	240598.04%
5	124.239.*.*	119393	827874	14.42%
6	117.26.*.*	103651	76	136382.89%
7	222.136.*.*	66081	263	25125.86%
8	103.1.*.*	63729	62627	101.76%
9	58.32.*.*	63250	131708	48.02%
10	61.148.*.*	60354	33132	182.16%
11	36.102.*.*	38473	1230358	3.127%
12	119.130.*.*	24868	9921	250.66%
13	27.197.*.*	23941	76	31501.32%
14	111.50.*.*	23592	199	11855.28%
15	101.78.*.*	44049	568483	7.75%
16	39.155.*.*	16802	50585	33.22%
17	123.158.*.*	8985	213	2301.46%
18	221.229.*.*	38473	1230358	4218.31%
19	124.135.*.*	162012	-	-
20	220.176.*.*	18252	-	-

流量捕获平台:使用基于spark的平台捕获流量并以<IP, UA>的格式存储为日志

过滤器: 检测异常UA，并且使用LevenShiten距离计算相似度，收集与这些异常UA的相似度大于0的正常UA

分析器：对收集的UA进行分析

为了避免偶然因素对我们的分析产生影响，我们对含有异常UA数目前20的客户端进行分析。他们产生的异常UA占了所有异常UA的14%，并且产生了大量重复的异常UA

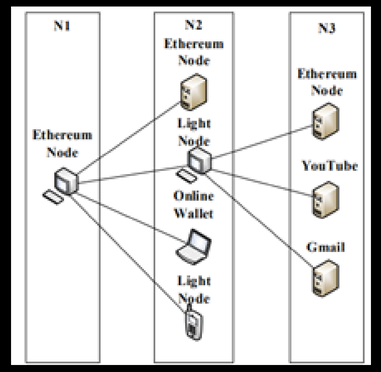
异常UA的产生主要是由客户端自身产生的，这些客户端在网络中进行恶意活动。部分是由于对UA的编码和解码的方法不匹配而产生的

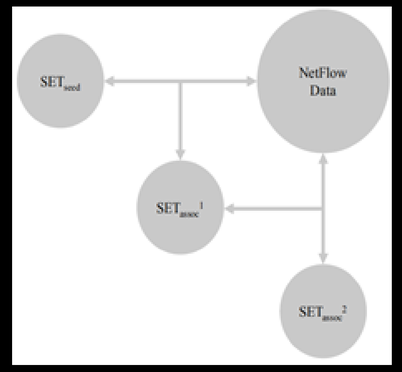
J. Chen, G. Gou and G. Xiong, "An Analysis of Anomalous User Agent Strings in Network Traffic," IEEE HPCC 2019 - IEEE High Performance Computing and Communications, Zhangjiajie, China, 2019.

团队研究成果

APNOMS 2019-基于NetFlow数据的以太坊行为分析

使用被动关联分析的方法在千分之一抽样的NetFlow流量中检测以太坊行为，通过机器学习的方法对关联结果进行收敛，并在收集的以太坊行为数据集合中进行多角度的测量分析。





Algorithm \ Date	12/20/2018		12/21/2018		12/22/2018		12/23/2018		12/24/2018		12/25/2018		12/26/2018	
	precision	recall	precision	recall	precision	recall	precision	recall	precision	recall	precision	recall	precision	recall
LR	81.9	81.3	80.9	80.9	80.9	80.3	80.0	81.1	81.4	80.4	80.9	80.4	81.6	81.6
SVM	82.6	83.5	82.5	84.1	81.5	83.9	82.4	83.8	82.6	83.5	82.8	82.3	82.7	82.5
KNN	80.3	79.7	79.5	80.0	79.3	79.6	80.2	79.2	80.8	80.7	80.7	80.0	80.5	79.8
C4.5	79.4	79.4	80.6	79.6	80.2	79.1	79.3	80.8	80.8	80.9	80.8	79.9	79.3	80.8
Adaboost	84.7	84.2	86.3	85.7	85.1	86.1	85.9	83.7	87.8	84.8	85.0	84.2	85.3	85.9
Random Forest	**89.1**	**90.5**	**89.7**	**90.8**	**90.8**	**90.8**	**91.0**	**90.3**	**90.1**	**90.1**	**89.6**	**90.3**	**90.4**	**90.5**

The seven-day performance of different algorithms in precision rate and recall rate is verified by a ten-fold cross-validation method. Among them, the random forest perform has the best performance.

提出了一种被动关联方法在真实骨干网NetFlow流量中检测以太坊节点，可以获得主动探测方式不能够检测到的轻节点及客户端节点。

比较了几种机器学习经典方法，选择随机森林算法对关联数据进行收敛，提高了以太坊服务发现的效率。

对以太坊服务行为数据集进行分析，测量结果揭示了以太坊网络真实特性，具有良好的连通性及稳定性。

Z. Li, J. Hou, H. Wang, C. Wang, C. Kang and P. Fu, "Ethereum behavior analysis with NetFlow Data“.IEEE APNOMS 2019 -Asia-Pacific Network Operations and Management Symposium 2019.

团队研究成果

- ICCS 2018-基于大规模行为测量知识库的MITM攻击检测

通过实施大规模的SSL被动测量，构建了X.509数字证书知识库，基于知识库对伪造证书进行多维度分析，结合网络行为特征，有效检测SSL MITM攻击。

SERVER IP	LOCATION	ORGANIZATION	DOMAIN
62.*.*.21	France: 48.8582, 2.3387	ONLINE SAS	poneytelecom.eu
195.*.*.44		Iliad-Entreprises	poneytelecom.eu
195.*.*.172		Iliad-Entreprises	poneytelecom.eu
195.*.*.209		Iliad-Entreprises	poneytelecom.eu

困难挑战：伪造证书很多用于安全审计而非恶意行为，如何从中筛选出真正的MITM攻击。

技术路线：提出使用基于HTTP 1.1协议单连接内串行请求特性刻画单个Web资源的局部特征模型，通过时间偏序关系的串联，提取前K个局部特征集，结合随机森林算法，实现指纹分类。

检测出涉及近100万伪造证书的MITM攻击，溯源得到恶意服务器IP

Cui M, Cao Z, Xiong G. How Is the Forged Certificates in the Wild: Practice on Large-Scale SSL Usage Measurement and Analysis[C]//International Conference on Computational Science. Springer, Cham, 2018: 654-667.

第七届互联网安全大会 360互联网安全中心

04

章节 PART

未来展望

未来对加密数据流量测量与行为分析

未来趋势

加密网络流量的激增

•全量检测、抽样测量

加密网络流量检测技术的要求

•更细粒度的用户行为识别

222.162.148.186	122.189.169.225	1573808000	1573810000	21057	2059	2	2194	17
122.190.241.170	119.167.128.13	1573835000	1573839000	57580	80	3	180	6
122.188.141.249	113.204.216.54	1573809000	1573809000	43946	35597	1	1466	6
113.56.88.241	183.95.154.16	2088447000	2088447000	53512	80	1	90	6
122.189.169.91	58.19.245.14	2088446000	2088446000	17776	41345	1	77	17
183.92.144.157	123.114.208.50	2088445000	2088445000	12345	10260	1	90	17
119.36.73.197	27.44.195.235	2088445000	2088445000	26323	45093	1	126	17
175.168.152.95	122.188.137.95	2088444000	2088444000	0	771	1	101	1
183.94.43.156	114.114.114.114	2088443000	2088443000	58547	53	1	71	17
60.24.88.141	113.56.90.206	2088447000	2088447000	42756	11825	1	1097	17

流采样

用户行为判别

“非破密”的检测技术

•从行为层面检测加密网络流量，识别加密的用户行为。

“破密”的角度

•以网络设施和技术手段实现对高优先级加密流量的深度分析。

相关管理手段

•利用授权和安全立法，与主流互联网厂商开展合作。

第七届互联网安全大会 360互联网安全中心

Thank You