KCon

纵横

利用AI检测隐蔽的C2通信
AI for Detecting Covert C2 Communication

演讲者：郑荣锋 腾讯企业IT安全研究员

背景

C2技术发展

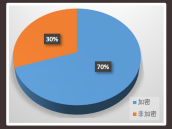
明文传输

公共协议(如TLS)

加密混淆

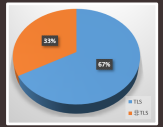
正常服务(如Twitter)

行业统计



2020年，加密的C2通信已达70%。

——Cisco



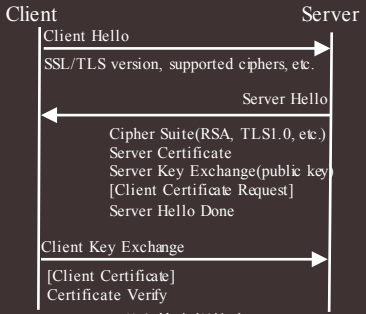
2020年Q1，67%的加密C2采用的TLS协议

——WatchGuard

防的策略

应用AI的难点

Cisco的成功经验



明文的密钥协商

问题分析

C2通信

差异

正常通信

观察对象

- 网络数据包 — 数据包载荷
- 网络会话流 — 数据包出现的顺序
反映出代码执行的流程
- 通信信道 — ？

分析思路

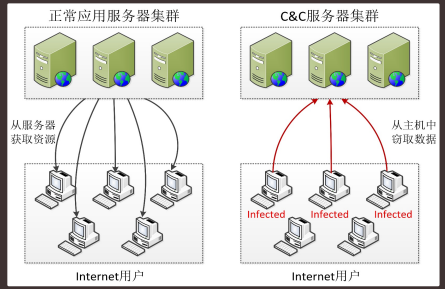
从服务端
视角考虑

三点假设：

1.应用数据载荷主要传输的方向上的差异

2.服务器被有效访问频次的差异

3.用户数量的差异



Internet用户访问正常服务器和C&C服务器的差异

解决思路

以通信信道为观察对象

TLS通信信道：{目的IP, 目的端口}

Flow	Src	Sport	Dst	Dport
1	192.168.9.11	5289	A.B.C.D	443
2	192.168.9.15	4183	E.F.G.H	443
3	192.168.9.15	7618	A.B.C.D	443
4	192.168.9.13	2590	E.F.G.H	443
5	192.168.9.11	9101	E.F.G.H	443
6	192.168.9.13	3180	E.F.G.H	443
…	…	…	…	…

Channel A

Src	Sport	Dst	Dport
192.168.9.11	5289	A.B.C.D	443
192.168.9.15	7618	A.B.C.D	443
…	…	…	…

Channel E

Src	Sport	Dst	Dport
192.168.9.15	4183	E.F.G.H	443
192.168.9.13	2590	E.F.G.H	443
192.168.9.11	9101	E.F.G.H	443
192.168.9.13	3180	E.F.G.H	443
…	…	…	…

按通信信道聚合TLS流

验证假设

以通信信道为观察对象的统计对比

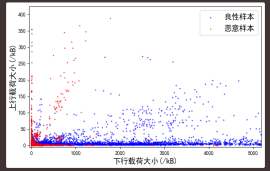


图 1 正负样本上/下行流量统计图

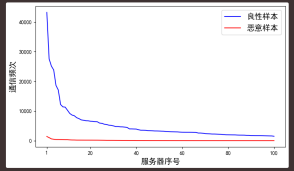


图 2 通信频次排名前100的对比图

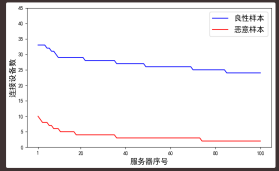


图 3 连接服务器数排名前100的对比图

数据载荷传输方向上的差异

通信频次上的差异

用户数的差异

基于粒度计算的特征表示方法

解决统计特征数值差异大的问题

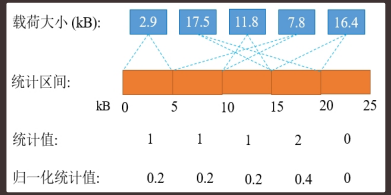


图 1 统计值映射过程图

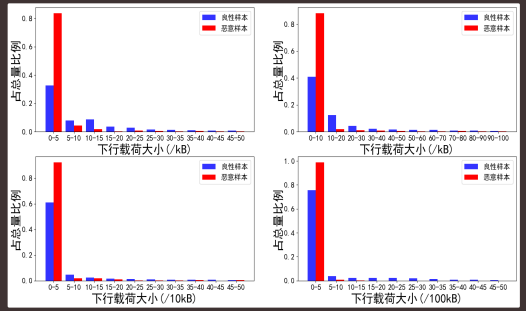


图 2 不同区间下的正负样本比例图

基于粒度计算的特征表示方法

解决统计特征数值差异大的问题

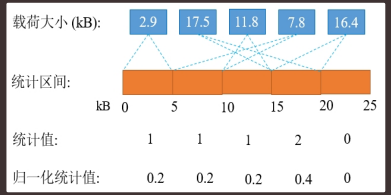


图 1 统计值映射过程图

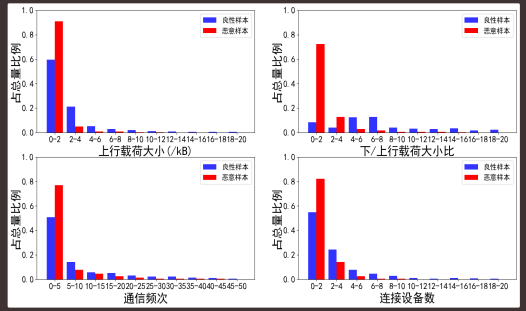


图 3 其他特征字段下的正负样本比例图

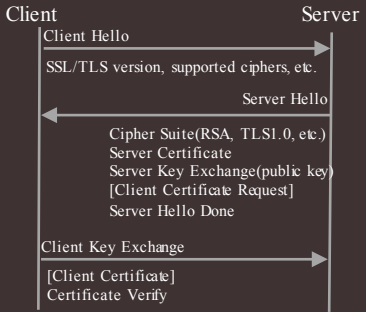
TLS信道特征工程

TLS流在信道上的分布特征设计

特征名	描述	特征数量
下行流载荷	以2,3,5,10,20,50,100,200,500,5000kB划分区间粒度	100
上行流载荷	以2,3,5,10,20,50,100,200,500,5000kB划分区间粒度	100
下/上行流量比	以2,3,5,10,20,50,100,200,500,5000kB划分区间粒度	100
连接频次	以2,3,5,10,20,50,100,200,500,5000划分区间粒度	100
连接设备数	以2,3,5,10,20,50,100,200,500,5000划分区间粒度	100

TLS信道特征工程


TLS握手
字段差异
Web服务端兼容性
握手字段
不一致


Client
Server
Client Hello
SSL/TLS version, supported ciphers, etc.
Server Hello
Cipher Suite(RSA, TLS1.0, etc.)
Server Certificate
Server Key Exchange(public key)
[Client Certificate Request]
Server Hello Done
Client Key Exchange
[Client Certificate]
Certificate Verify
明文的密钥协商

TLS信道特征工程

计算样本一致性比例：

$$Consistency(F) = \frac{\sum_{i=0}^{i=N} C_i(F)}{N}$$

TLS握手字段一致性统计

字段名称	正常信道	C2信道
客户端Hello长度	26.43%	57.63%
客户端HelloSession ID长度	41.11%	68.85%
加密算法数量	16.53%	63.70%
客户端Extension数量	27.68%	79.41%
客户端Session ticket长度	41.11%	68.86%
客户端交换密钥长度	28.86%	79.24%
客户端应用层协议协商长度	52.53%	89.73%
客户端签名算法个数	51.18%	86.44%
客户端签名算法	48.07%	86.39%

TLS信道特征工程

基础信息统计特征

TLS通信信道基础特征

特征描述	描述
上下行信道特征	上行总载荷大小 下行总载荷大小 上下行载荷比
上下行流特征	上行流最小长度 上行流最大长度 上行流平均长度 上行流长度标准差 下行流最小长度 下行流最大长度 下行流平均长度 下行流长度标准差
流的时间间隔特征	流之间的最大时间间隔 流之间的最小时间间隔 流之间的平均时间间隔 流之间的时间间隔标准差

AI算法中的特征选择

实验：样本收集

良性样本：来自于内网样本

恶意样本来源：

1）Malware Traffic (MT)

2）Stratosphere IPS (SIPS)

3）Canadian Institute for Cybersecurity (CIC)

恶意TLS信道样本数据集

样本来源	TLS流	TLS通信信道
MT	37210	8303
SIPS	40100	2242
CIC	582884	5679

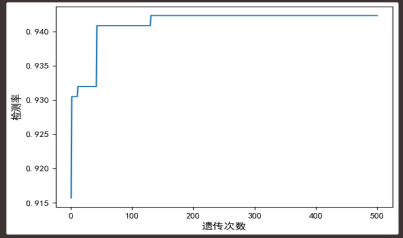
- MT和SIPS：普通的恶意TLS流样本
- CIC：深度协议伪装的恶意TLS流样本

实验：三类通信信道特征效果对比

目标：评估提出的三类信道特征的有效性

- 分布特征（Distribution feature, DF）
- 一致性特征(Consistency feature, CF)
- 统计特征(Statistic feature, SF)

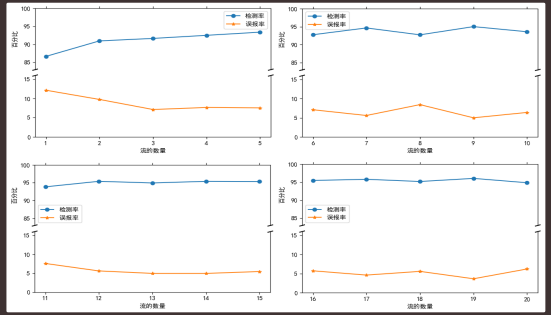
特征集	Precision	Recall	F_1 score
DF	79.78%	67.93%	73.29%
CF	89.59%	89.75%	88.63%
SF	87.34%	87.77%	88.51%
BF+HF+SF	92.57%	88.10%	90.23%



迭代次数：131

特征数量：864 ⟶ 304

实验：评估通信信道中流的数量对检测模型的影响



20个
通信信道

结论

1个通信信道：9条TLS流

实验：与其他恶意TLS通信检测方法的对比

实验对比

数据集	Cisco方法		非监督方法		本方法	
	检测率	误报率	检测率	误报率	检测率	误报率
MT	92.42%	5.56%	81.86%	20.20%	90.24%	8.42%
SIPS	96.00%	4.10%	84.43%	11.55%	92.29%	9.71%
CIC	84.05%	17.03%	71.23%	31.33%	**91.62%**	**1.33%**

本方法在深度协议伪装的样本集上表现得更好

基于HTTP协议的C2检测

目标：基于HTTP协议
验证本方法的普适性

HTTP信道中：

- 统计特征与TLS通信信道的一致
- 分布特征与TLS通信信道的一致
- 一致性特征利用HTTP头的请求字段

HTTP请求头字段一致性特征设计

编号	请求头字段
1	Accept：能够接受的回应内容类型
2	Accept-Charset：能够接受的字符集
3	Accept-Encoding：能够接受的编码方式列表
4	Accept-Languate：能够接受的回应内容的自然语言列表
5	Authorization：用于超文本传输协议的认证信息
6	Connection：该浏览器想要优先使用的连接类型
7	Content-Length：以八位字节数组表示的请求体的长度
8	Content-Type：请求体和多媒体类型
9	User-Agent：浏览器的浏览器身份标识字符串
10	Expect：表明客户端要求服务器做出特定的行为

实验：HTTP流量样本收集

良性样本：来自于内网样本

恶意样本来源：

1）Malware Traffic (MT)

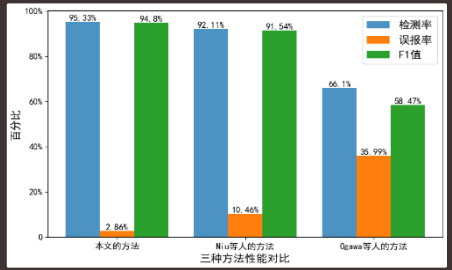
2）Stratosphere IPS (SIPS)

3）Canadian Institute for Cybersecurity (CIC)

恶意HTTP信道样本数据集

样本来源	HTTP流	HTTP信道
MT	41515	14352
CIC	35528	2906
SIPS	189653	2695

实验：与其他恶意HTTP通信检测方法的对比



测试样本：

1000个良性通信信道，32657条良性HTTP流

1000个恶意通信信道，28332条恶意HTTP流

训练算法：

本文：随机森林

2019, Niu等人： XGBoost算法

2017, Ogawa等人：*k*-Means + SVM

经验总结

方法总结

假设 -> 验证 -> 特征设计 -> 建模

经验分享

样本 70%

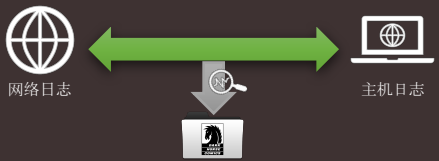
\>

特征 20%

\>

算法 10%

未来研究方向

1. 信道特征  单流特征
2. 其它通信协议 FTP SSH
3. 

感谢观看！

KCon 汇聚黑客的智慧

知道创宇 | KCon