Web Base网络参与(WBNP)和发件人基础网络参与(SBNP)

目录

简介

思科网络和邮件内容安全产品可向思科和Talos提供遥测数据，以提高网络安全设备(WSA)中网络分类和连接邮件安全设备(ESA)IP信誉的效力。

遥测数据以“选择加入”的方式提供给WSA和ESA。

数据通过二进制编码的SSL加密数据包传输。 下面提供的附件将提供对所传输数据的数据、特定格式和说明的深入了解。 WebBase网络参与(WBNP)和SenderBase网络参与(SBNP)数据不能以直接日志或文件格式查看。 此数据以加密形式传输。 此数据不是“静止”的。

WSA - WebBase网络参与

思科认识到维护隐私的重要性，不会收集或使用用户名和密码等个人或机密信息。此外，主机名后面的文件名和URL属性经过模糊处理，以确保机密性。

当涉及解密的HTTPS事务时，SensorBase网络仅接收证书中服务器名称的IP地址、Web信誉分数和URL类别。

有关完整信息，请查看WSA用户指南，了解设备上当前运行的AsyncOS for Web Security版本。 请参阅《用户指南》中的“The Cisco SensorBase Network”。

ESA - SenderBase网络参与

参与SenderBase网络的客户允许思科收集有关其组织的汇总电子邮件流量统计信息，从而提高所有使用该服务的用户的效用。参与是自愿的。思科仅收集有关消息属性的摘要数据以及有关思科设备如何处理不同类型的消息的信息。例如，思科不收集邮件正文或邮件主题。个人身份信息和标识贵组织的信息将保密。

有关完整信息， p租赁审查ESA用户指南 适用于设备上当前运行的AsyncOS for ESA Security的版本。 请参阅《用户指南》中的“SenderBase网络参与”一章。

一般安全问题常见问题

问题： 收集的数据存储在何处？
答案： 设备遥感勘测存储在思科美国数据中心。
问题： 谁有权访问收集和存储的数据？
答案： 访问仅限于Cisco SBG人员，他们分析/使用数据以创建可操作的情报。
问题： 收集的数据的保留时间是多少？
答案： 没有有关设备遥测的数据保留/过期策略。数据可以无限期保留，也可以由于各种原因被删除，包括
问题： 客户序列号或公有IP地址是否存储在Talos分类数据库中？
答案： 否，仅保留URL和类别。WBNP数据包不包含源IP信息。

操作

在下面详细介绍操作、数据类型（按说明）和示例数据，以演示要传输的信息：

- SBNP — 与邮件安全相关的特定数据类型（字段）和样本数据
- WBNP — 与网络安全相关的特定数据类型（字段）和样本数据
- 威胁检测操作 — 从操作角度对威胁检测的概述

SenderBase（电子邮件）网络参与

每封邮件共享的统计信息设备

项目	示例数据
MGA标识符	MGA 10012
时间戳	2005年7月1日上午8点到
软件版本号	MGA版本4.7.0
规则集版本号	反垃圾邮件规则集102
防病毒更新间隔	每10分钟更新一次
隔离区大小	500 MB
隔离区邮件计数	隔离区中当前有50封邮件
病毒分数阈值	将邮件发送到威胁级别3或

进入隔离区的邮件的病毒分数总和	120
进入隔离区的邮件计数	30（平均得分为4）
最大隔离时间	12 小时
爆发隔离区邮件计数（按其进入和退出隔离区的原因划分），与防病毒结果相关	50人因.exe规则30而进入
按离开隔离区时采取的操作细分的爆发隔离区邮件计数	10封邮件在离开隔离区后
邮件在隔离区中保留的时间总和	20 小时

按IP地址共享的统计信息

项目	示例数据	标准参与	有限参与
设备内不同阶段的邮件计数	防病毒引擎可见：100 反垃圾邮件引擎可见：80		
反垃圾邮件和防病毒分数和判定的总和	2,000（所有发现邮件的反垃圾邮件分数之和）		
达到不同反垃圾邮件和防病毒规则组合的邮件数	100条消息符合规则A和B 50条消息仅符合规则A		
连接的数量	20个SMTP连接		
收件人总数和无效收件人数	总共50个收件人 10个无效收件人		
散列文件名：(a)	在名为<one-way-hash>.zip的存档附件中找到了文件<one-way-hash>.pif。	未混淆的文件名	散列文件名
模糊文件名：(b)	在文件aaaaaaaa.zip中找到文件aaaaaaa0.aaa.pif。	未混淆的文件名	模糊文件名
URL主机名(c)	在发往www.domain.com的邮件中找到一个链接	未混淆的URL主机名	模糊URL主机
模糊URL路径(d)	在发往主机名www.domain.com的消息中找到一个链接，其路径为aaa000aa/aa00aaa。	未混淆的URL路径	模糊URL路径
按垃圾邮件和病毒扫描结果划分的邮件数	10个垃圾邮件 10个垃圾邮件否定 5垃圾邮件可疑 4病毒阳性 16病毒阴性 5病毒无法扫描		
按不同反垃圾邮件和防病毒判定的邮件数	500个垃圾邮件，300个火腿		
大小范围中的邮件计数	3万至3万5千范围内125个		
不同分机类型的计数	300个“.exe”附件		
附件类型、真文件类型和容器类型的关联	有100个附件，其扩展名为“.doc”，但实际上是“.exe” 50个附件是zip中的“.exe”扩展		
扩展名和真文件类型与附件大小的关联	30个附件在50-55K范围内为“.exe”		
随机抽样结果的消息数	14条消息已跳过采样 25条消息排队等待采样 从采样中扫描50封邮件		
DMARC验证失败的邮件数	34封邮件未通过DMARC验证		

注意：

(a)文件名将以单向哈希(MD5)编码。

(b)文件名将以模糊形式发送，所有小写ASCII字母([a-z])替换为"a"，所有大写ASCII字母([A-Z])替换为"A"，任何多字节UTF-8字符替换为"x"（为其他字符集提供隐私），所有ASCII数字

([0-9])替换。

(c)URL主机名指向提供内容的Web服务器，与IP地址一样。不包括用户名和密码等机密信息。

(d)对主机名后面的URL信息进行模糊处理，以确保不泄露用户的任何个人信息。

每个SDS客户端共享的统计信息

项目	示例数据
时间戳	
客户机版本	
向客户端发出的请求数	
从SDS客户端发出的请求数	
DNS查找的时间结果	
服务器响应时间结果	
与服务器建立连接的时间	
建立的连接数	
与服务器的并发打开连接数	
向WBRS发送的服务请求数	
到达本地WBRS缓存的请求数	
本地WBRS缓存的大小	
远程WBRS的响应时间结果	

AMP SBNP遥测数据

格式	示例数据
amp_carvents':{("verdict"、"spyname"、"score"、"uploaded"、"filename"),	
（"裁定"、"spyname"、"score"、"uploaded"、"filename"），	
（"裁定"、"spyname"、"score"、"uploaded"、"filename"），	
.....	
（"裁定"、"spyname"、"score"、"uploaded"、"filename"），	
}	
描述	
判定 — AMP信誉查询	恶意/干净/未知
Spyname — 检测到的恶意软件的名称	[特洛伊木马测试]
得分 — AMP分配的信誉得分	[1-100]
上传 — 指示上传文件的AMP云	1
文件名 — 文件附件的名称	abcd.pdf

WebBase(Web)网络参与

按Web请求共享的统计信息

项目	示例数据	标准参与	有限参与
version	coeus 7.7.0-608		
Serial Number			
SBNP采样系数（体积）			
SBNP采样因子（速率）	1		
目标IP和端口		未混淆的URL路径段	散列URL路径段
选择的反间谍软件恶意软件类别	已跳过		
WBRS分数	4.7		
McAfee恶意软件类别判定			

引用者URL	未混淆的URL路径段　散列URL路径段
内容类型ID	
ACL决策标记	0
传统Web分类	
CIWUC Web类别和决策源	{'src':'req'、'cat':“1026”}
AVC应用名称	广告和跟踪
AVC应用类型	广告网络
AVC应用行为	不安全
内部AVC结果跟踪	[0,1,1,1]
通过索引数据结构跟踪用户代理	3

每个Web请求的高级恶意软件统计信息

AMP统计信息

判定 — AMP信誉查询	恶意/干净/未知
Spyname — 检测到的恶意软件的名称	[特洛伊木马测试]
得分 — AMP分配的信誉得分	[1-100]
上传 — 指示上传文件的AMP云	1
文件名 — 文件附件的名称	abcd.pdf

最终用户反馈统计信息源

每个最终用户共享的统计信息 分类错误 反馈

项目	**示例数据**
引擎ID（数字）	0
传统Web分类代码	
CIWUC Web分类源	'resp' / 'req'
CIWUC Web类别	1026

提供的示例数据 — 标准参与

```
# categorized
"http://google.com/": {    "wbrs": "5.8",
   "fs": {
         "src": "req",
         "cat": "1020"
   },
}

# uncategorized
"http://fake.example.com": {    "fs": {
     "cat": "-"
   },
}
```

提供的示例数据 — 参与有限

- 来自客户端的原始请求：www.gunexams.com/Non-Restricted-FREE-Practice-Exams
- 已记录的消息（在遥测服务器中）：http://www.gunexams.com/76bd845388e0

完全WBNP解码

每个思科设备共享的统计信息

项目	示例数据
version	coeus 7.7.0-608
序列号	0022190B6ED5-XYZ1YZ2
型号	S660
已启用Webroot	1
已启用AVC	1
已启用Sophos	0
已启用响应端分类	1
已启用反间谍软件引擎	default-2001005008
反间谍软件SSE版本	default-2001005008
反间谍软件Spycat定义版本	default-8640
反间谍软件URL阻止列表DAT版本	
反间谍软件URL网络钓鱼DAT版本	
反间谍软件Cookie DAT版本	
已启用反间谍软件域阻止	0
反间谍软件威胁风险阈值	90
已启用McAfee	0
McAfee引擎版本	
McAfee DAT版本	default-5688
WBNP详细级别	2
WBRS引擎版本	freebsd6-i386-300036
WBRS组件版本	categories=v2-1337979188,ip=default-1379460997,keyword=v2-1312487822,prefixcat=v2-1379460670,rule=default-1358979215
WBRS阻止列表阈值	-6
WBRS允许列表阈值	6
已启用WBRS	1
支持安全移动	0
L4流量监控器已启用	0
L4流量监控阻止列表版本	default-0
L4流量监控器管理阻止列表	
L4流量监控器管理阻止列表端口	
L4流量监控允许列表	
L4流量监控允许列表端口	
SBNP采样因子	0.25
SBNP采样系数（体积）	0.1
SurfControl SDK版本（旧版）	default-0
SurfControl完整数据库版本（旧版）	default-0
SurfControl本地增量累积文件版本（旧版）	default-0
Firestone引擎版本	default-210016
Firestone DAT版本	v2-310003
AVC引擎版本	default-110076
AVC DAT版本	default-1377556980
Sophos引擎版本	default-1310963572
Sophos DAT版本	default-0
已启用自适应扫描	0
自适应扫描风险分数阈值	[10、6、3]
自适应扫描负载因子阈值	[5、3、2]
SOCKS已启用	0
事务总数	

事务总数	
允许的事务总数	
检测到的恶意软件事务总数	
管理员策略阻止的事务总数	
被WBRS分数阻止的事务总数	
高风险交易总数	
流量监控器检测到的事务总数	
与IPv6客户端的事务总数	
与IPv6服务器的事务总数	
使用SOCKS代理的事务总数	
来自远程用户的事务总数	
来自本地用户的事务总数	
使用SOCKS代理允许的事务总数	
允许使用SOCKS代理的本地用户的事务总数	
允许使用SOCKS代理的远程用户事务总数	
使用SOCKS代理阻止的事务总数	
使用SOCKS代理阻止的来自本地用户的事务总数	
使用SOCKS代理阻止的来自远程用户的事务总数	
自上次重新启动以来的秒数	2843349
CPU利用率(%)	9.9
RAM利用率(%)	55.6
硬盘利用率(%)	57.5
带宽利用率（/秒）	15307
打开TCP连接	2721
每秒事务数	264
客户端延迟	163
缓存命中率	21
代理CPU利用率	17
WBRS WUC CPU利用率	2.5
记录CPU利用率	3.4
报告CPU利用率	3.9
Webroot CPU利用率	0
Sophos CPU利用率	0
McAfee CPU利用率	0
vmstat实用程序输出(vmstat -z、vmstat -m)	
配置的访问策略数	32
已配置的自定义Web类别数	32
身份验证提供程序	基本，NTLMSSP
身份验证领域	身份验证提供程序主机名、协议和其他配置元素

按Web请求共享的统计信息

项目	示例数据	标准参与	有限参与
version	coeus 7.7.0-608		
Serial Number			
SBNP采样系数（体积）			
SBNP采样因子（速率）	1		
目标IP和端口		未混淆的URL路径段	散列URL路径段
选择的反间谍软件恶意软件类别	已跳过		
WBRS分数	4.7		

McAfee恶意软件类别判定		
引用者URL		未混淆的URL路径段　散列URL路径段
内容类型ID		
ACL决策标记	0	
传统Web分类		
CIWUC Web类别和决策源	{'src':'req'、'cat':“1026”}	
AVC应用名称	广告和跟踪	
AVC应用类型	广告网络	
AVC应用行为	不安全	
内部AVC结果跟踪	[0,1,1,1]	
通过索引数据结构跟踪用户代理	3	

每个Web请求的高级恶意软件统计信息

AMP统计信息

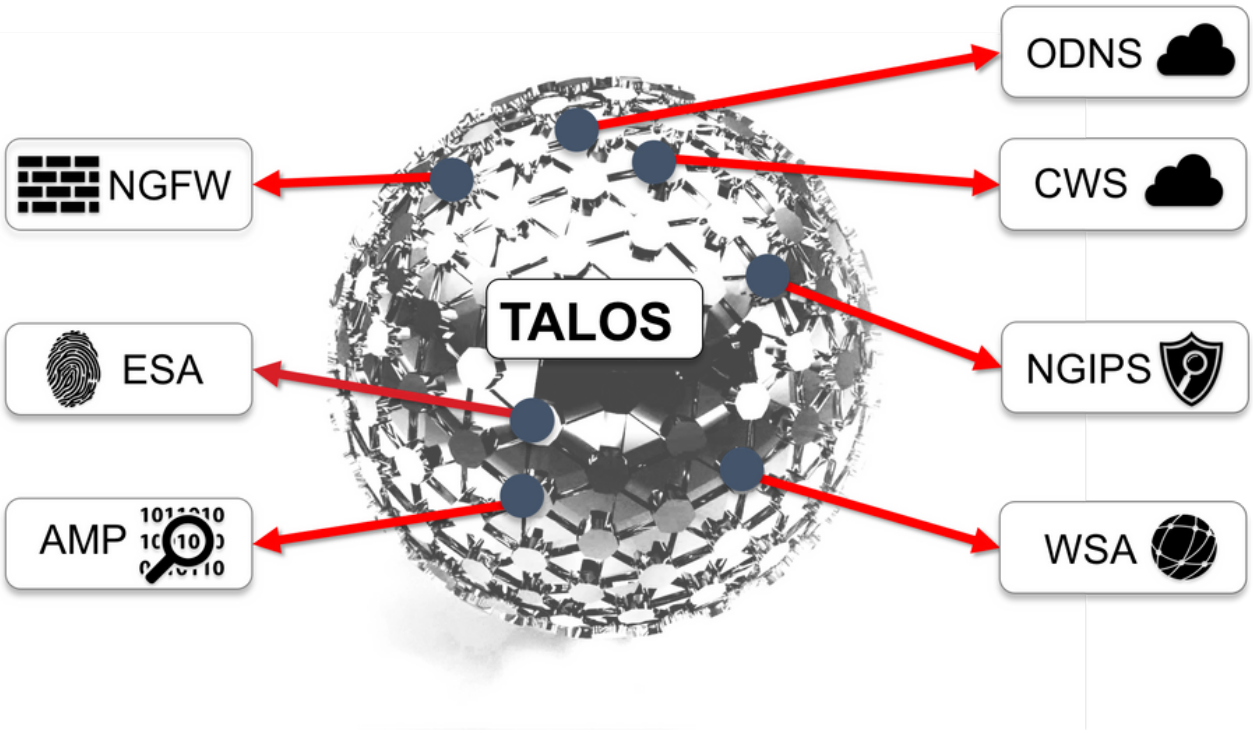
判定 — AMP信誉查询	恶意/干净/未知
Spyname — 检测到的恶意软件的名称	[特洛伊木马测试]
得分 — AMP分配的信誉得分	[1-100]
上传 — 指示上传文件的AMP云	1
文件名 — 文件附件的名称	abcd.pdf

最终用户反馈统计信息源

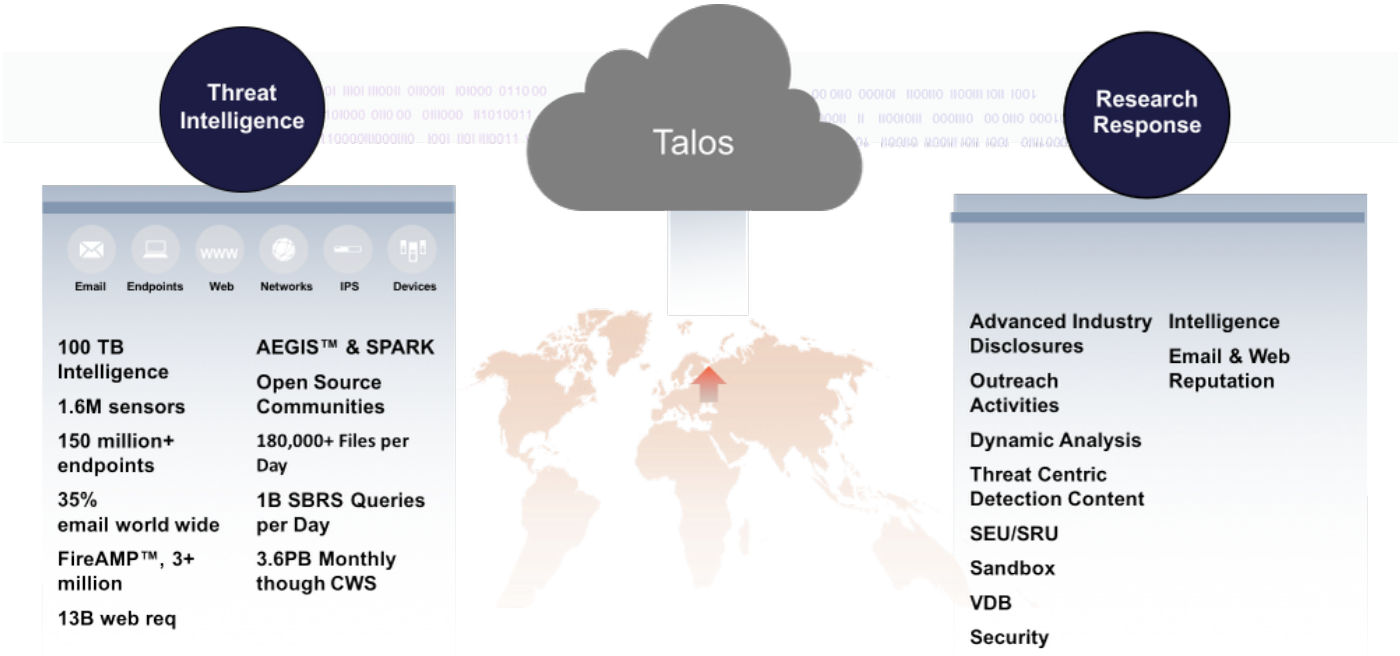
每个最终用户共享的统计信息 分类错误 反馈

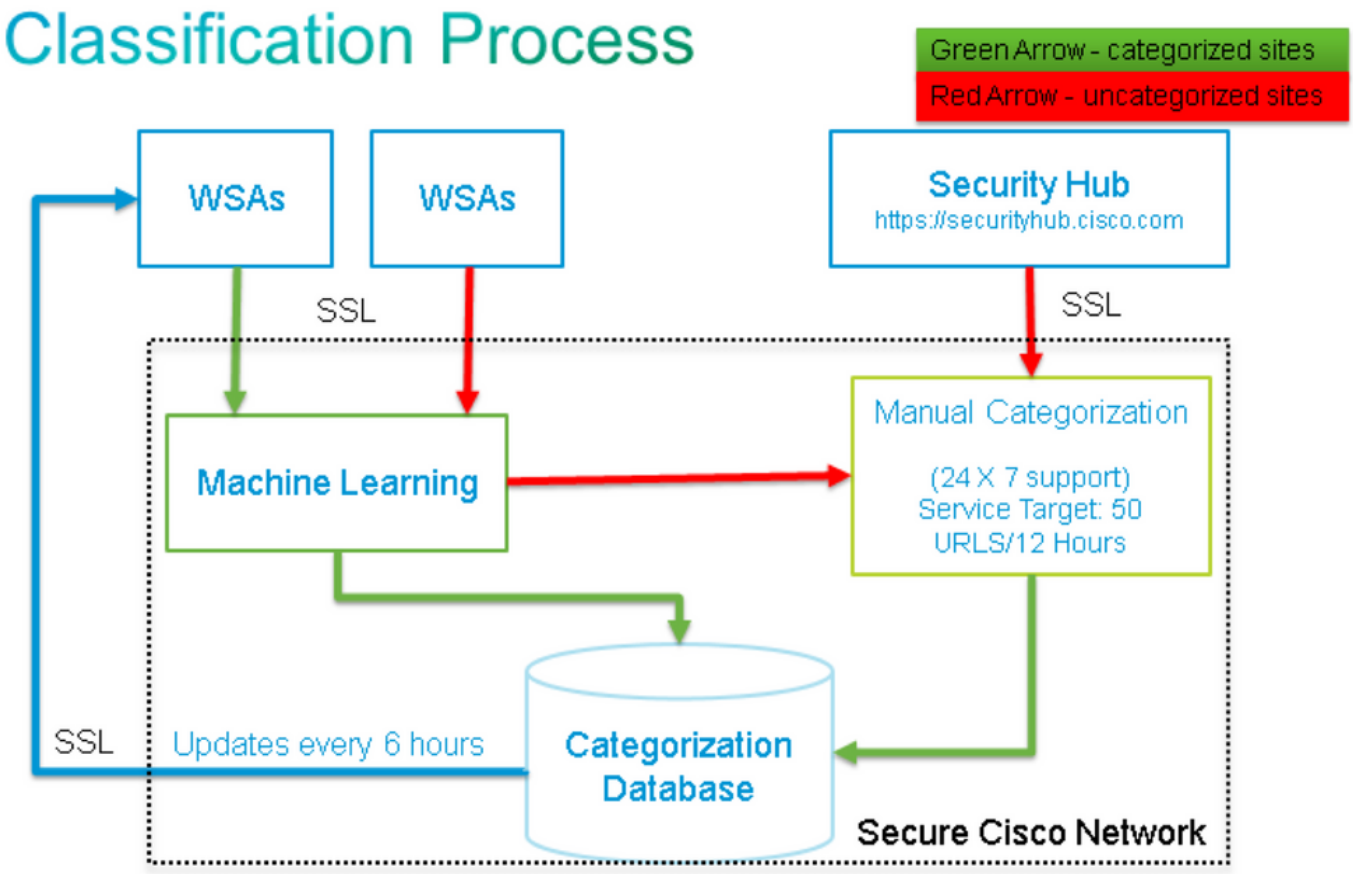
项目	**示例数据**
引擎ID（数字）	0
传统Web分类代码	
CIWUC Web分类源	'resp' / 'req'
CIWUC Web类别	1026

Talos检测内容


ODNS
CWS
NGFW
TALOS
NGIPS
ESA
AMP
WSA

专注于威胁


Threat Intelligence
Talos
Research Response
Email
Endpoints
Web
Networks
IPS
Devices
100 TB Intelligence
1.6M sensors
150 million+ endpoints
35% email world wide
FireAMP™, 3+ million
13B web req
AEGIS™ & SPARK
Open Source Communities
180,000+ Files per Day
1B SBRS Queries per Day
3.6PB Monthly though CWS
Advanced Industry Disclosures
Outreach Activities
Dynamic Analysis
Threat Centric Detection Content
SEU/SRU
Sandbox
VDB
Security
Intelligence
Email & Web Reputation



相关信息

- 思科网络安全设备 — 产品页
- 思科邮件安全设备 — 产品页面
- 技术支持和文档 - Cisco Systems