思科安全如何应对勒索软件攻击

吴清伟David Wu

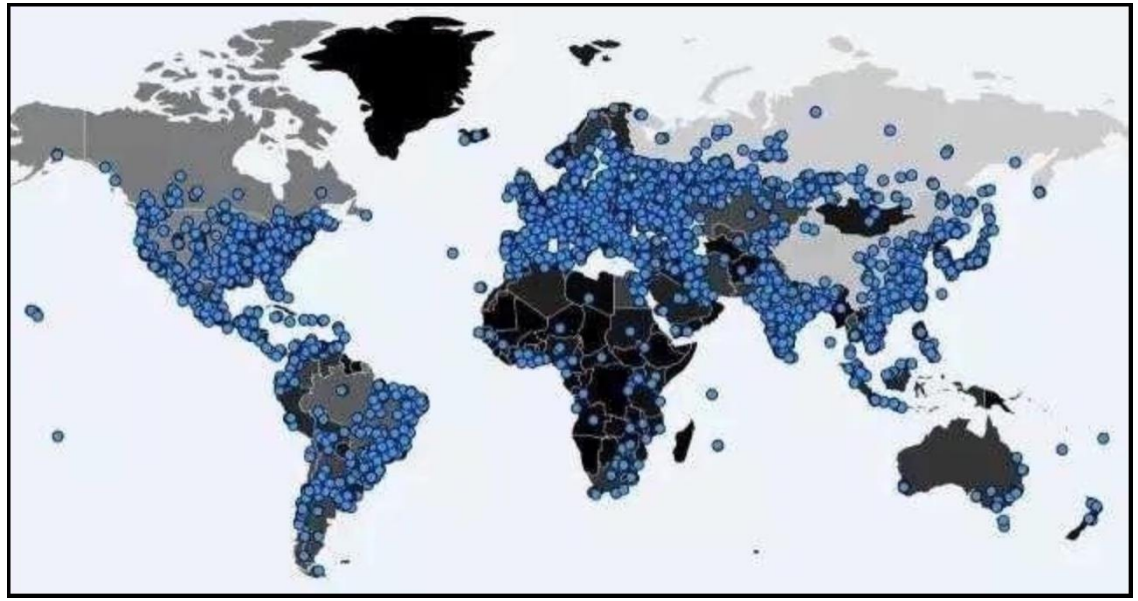
思科安全技术顾问

议题

- WannaCry与Jaff勒索软件解析
- 重新认识勒索软件的危害与演化趋势
- 思科安全如何应对勒索软件
- 最佳实践与建议
- 问题与讨论

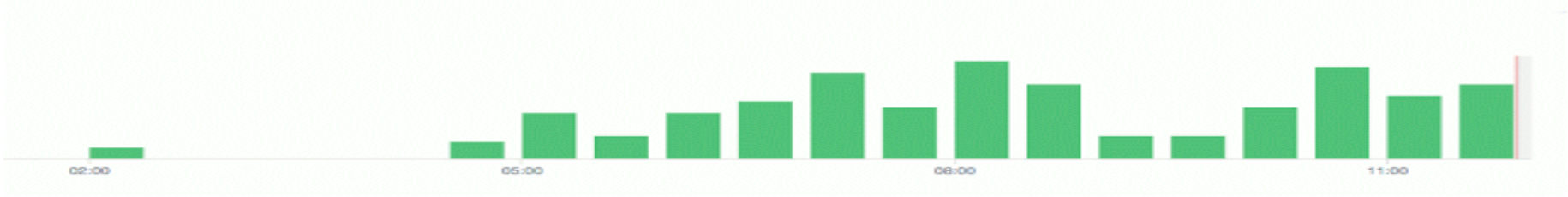
勒索软件WannaCry爆发事件回顾

- 2017年5月12日，勒索软件WannaCry开始在全球范围内传播，包括西班牙的Telefonica、英国的National Health Service、以及美国的FedEx等企业纷纷中招。
- 国内部分高校开始发现了WannaCry的感染事件，随后迅速波及其他企业用户，包括加油站、政府办事终端、制造业、金融、教育等行业。
- 思科Talos威胁情报团队，在第一时间发布了分析报告，详细介绍了WannaCry的特征与传播方式，并给出了用户的应急处理方案

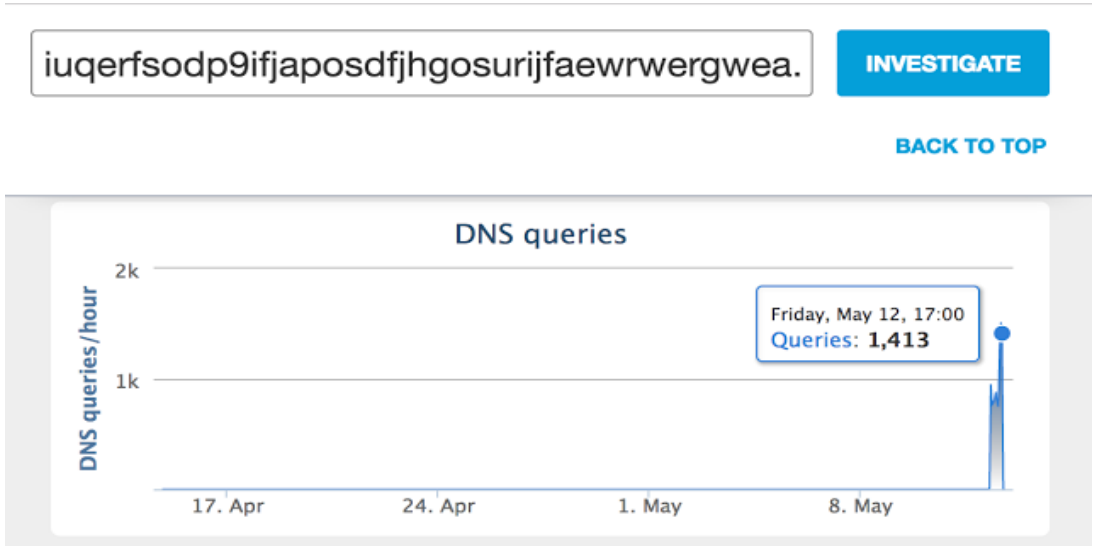


思科Talos对勒索软件WannaCry的分析报告

1、思科Talos研究人员注意到从东部标准时间早上5点（世界标准时间上午9点）前开始，网络中针对联网主机的扫描开始急速攀升。



2、我们研究人员在UTC时间07:24，观察到来自WannaCry的kill switch长域名的第一个请求，此后在短短10小时后，就上升到1400次/秒的峰值。



思科Talos对勒索软件WannaCry的分析报告

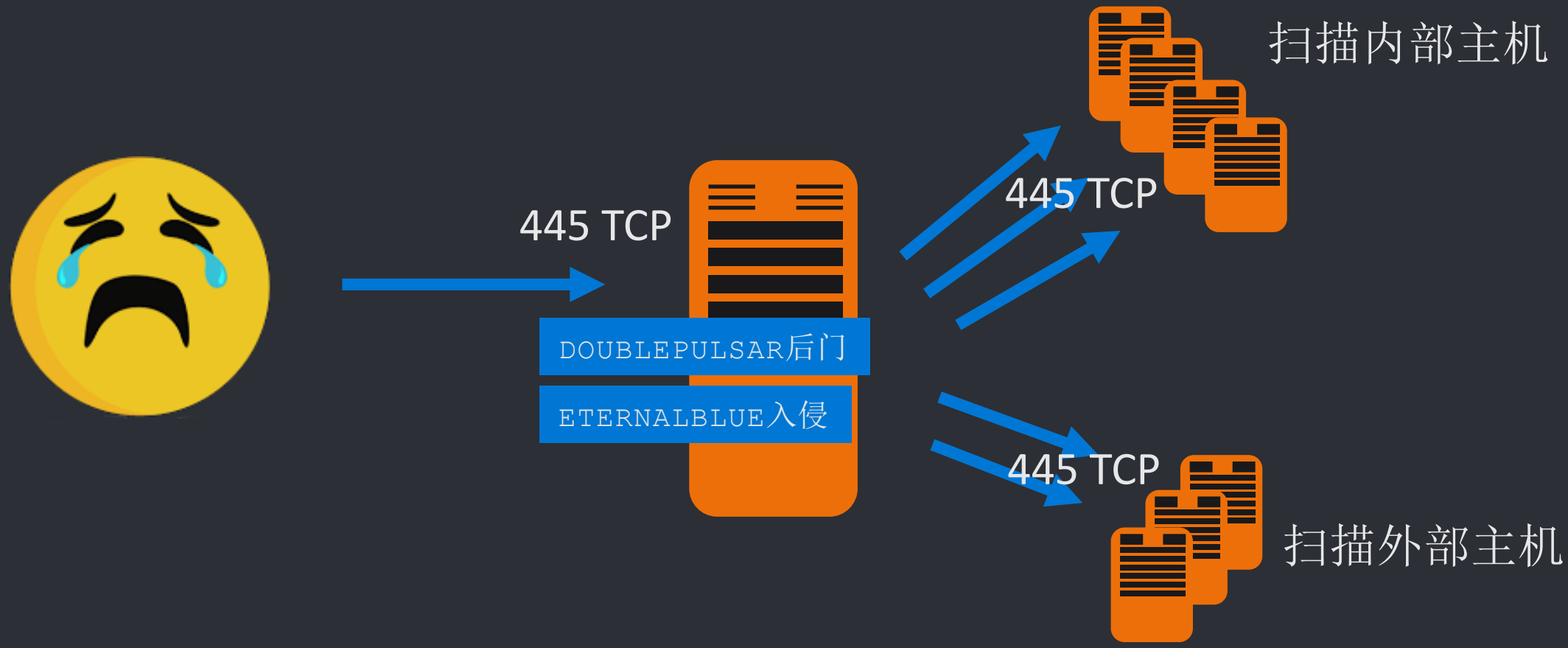
3、思科Talos研究人员通过逆向工程，发现恶意程序会尝试对kill switch域名执行HTTP GET操作，如果失败，它会继续进行感染操作；然而，如果成功，该恶意程序将会结束。

```
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// : "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
if ( v5 )
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
else
{
  InternetCloseHandle(v4);
  InternetCloseHandle(0);
  sub_408090();
  result = 0;
}
return result;
```

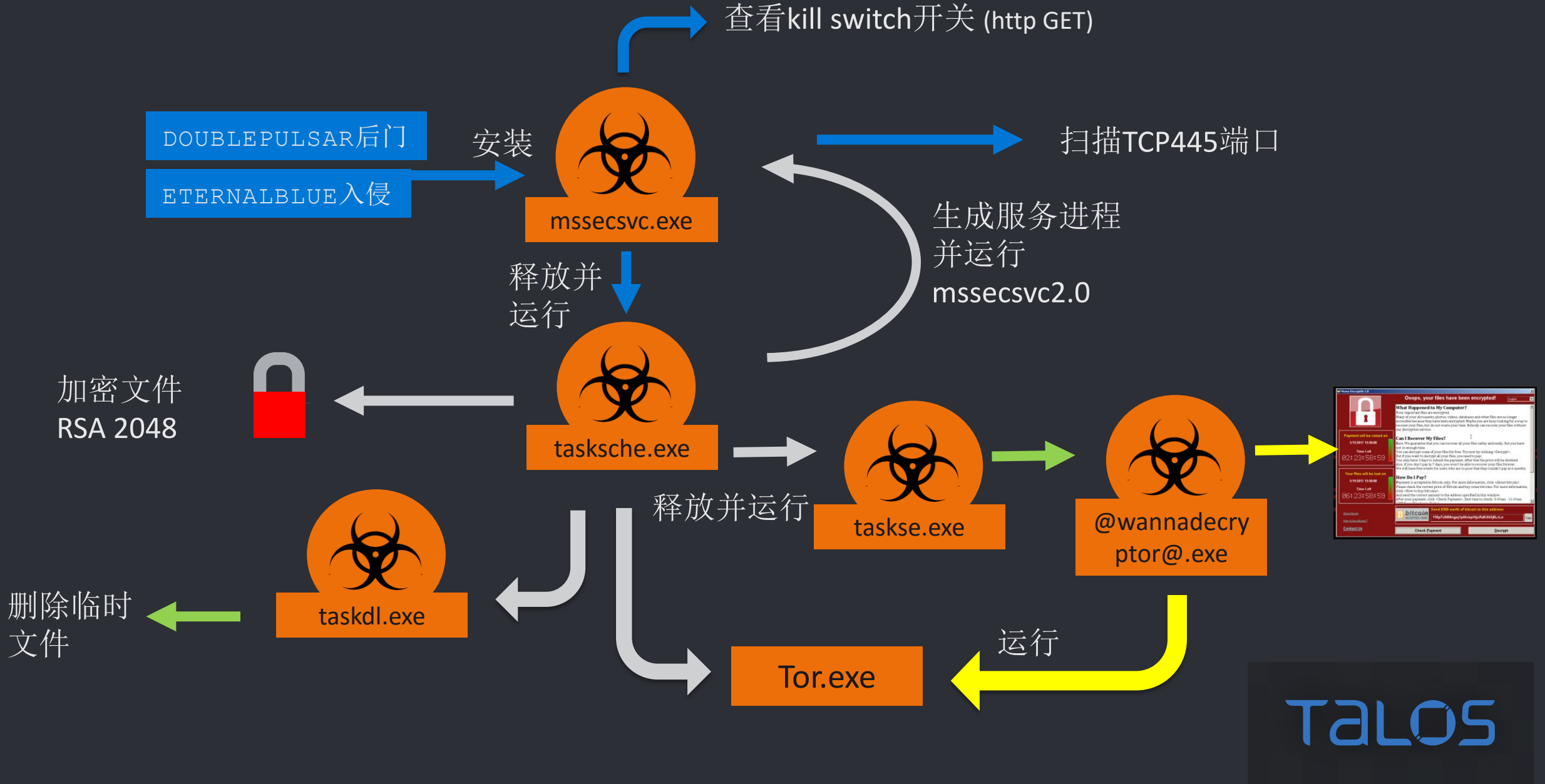
4、思科研究人员发现该长域名被注册到一个已知的sinkhole，有效的减缓了勒索软件的活动。验证域名注册信息证明了这一点，其注册日期为2017年5月12日。

```
Domain Name: IUQERFSODP9IFJAPOSDFJHGOSURIJFAEWRWERGWEA.COM
Registrar: NAMECHEAP INC.
Sponsoring Registrar IANA ID: 1068
Whois Server: whois.namecheap.com
Referral URL: http://www.namecheap.com
Name Server: NS1.SINKHOLE.TECH
Name Server: NS2.SINKHOLE.TECH
Name Server: NS3.SINKHOLE.TECH
Name Server: NS4.SINKHOLE.TECH
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Updated Date: 12-may-2017
Creation Date: 12-may-2017
Expiration Date: 12-may-2018
```

WannaCry的传播过程

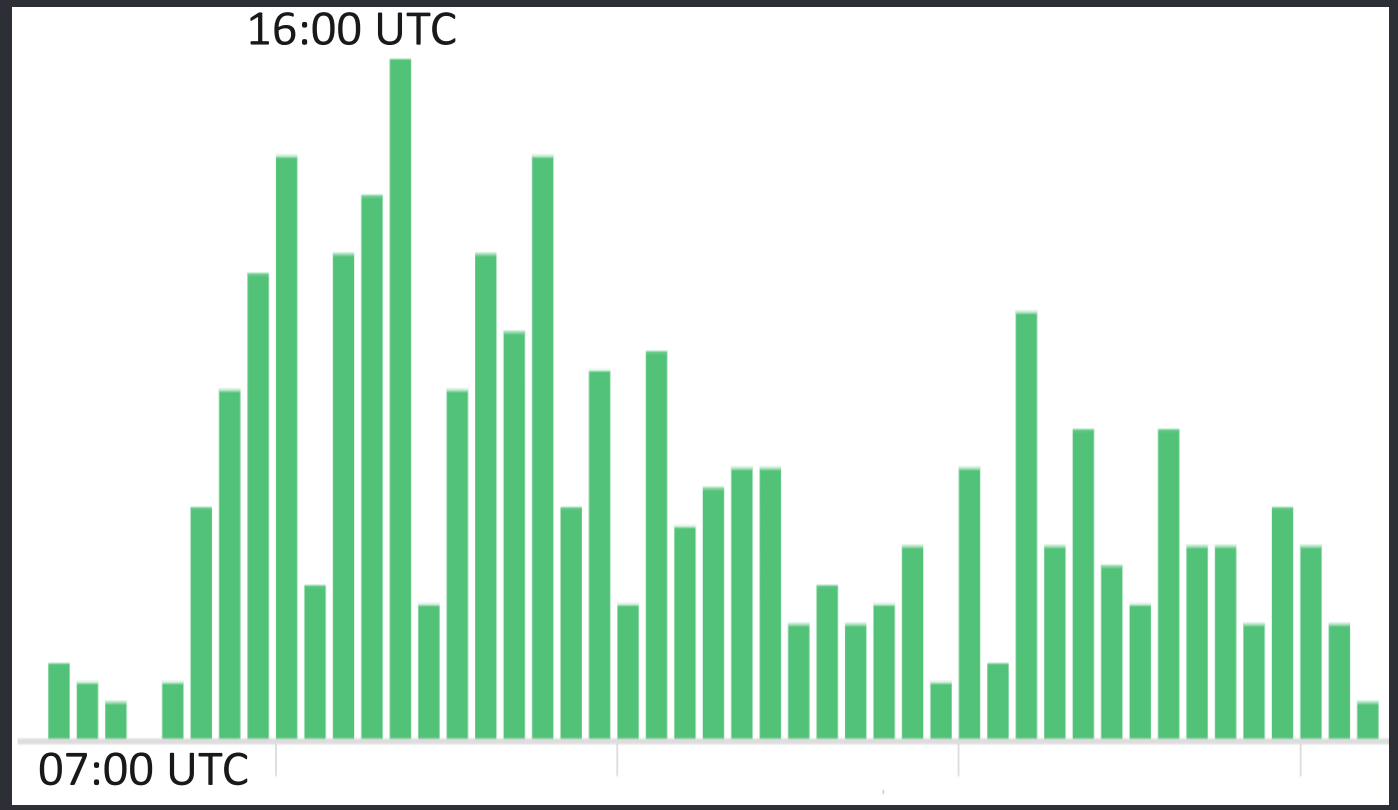


WannaCry的感染过程

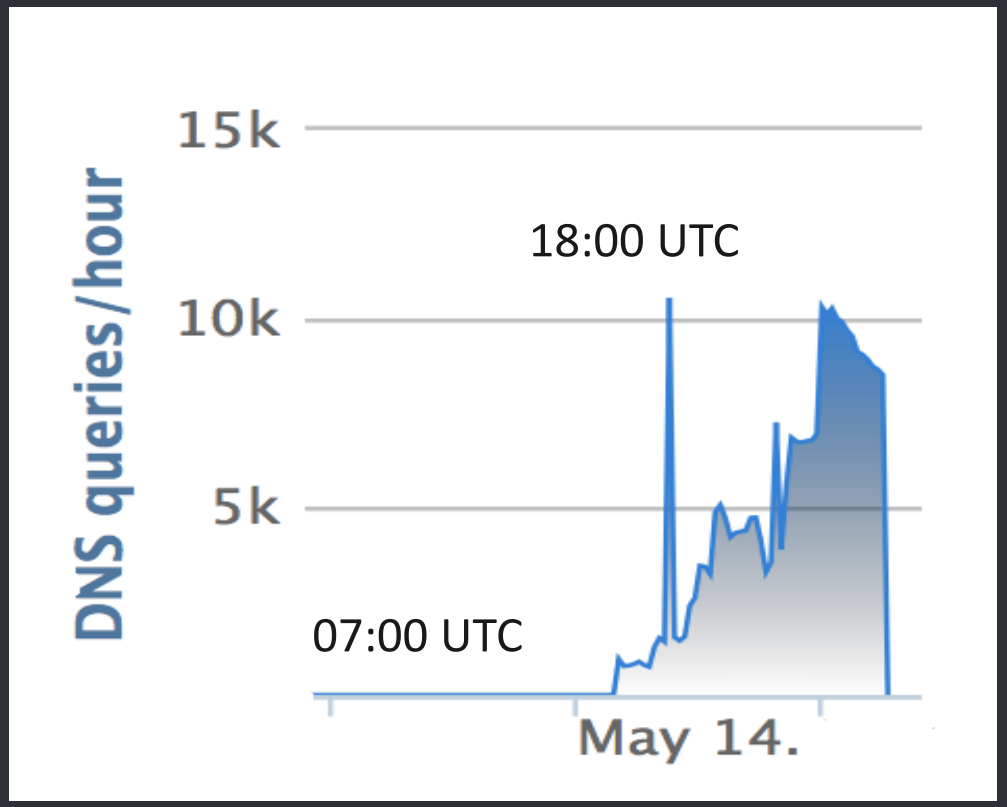


Talos跟踪WannaCry的爆发过程

蜜罐网站记录445端口的TCP连接数



Umbrella统计Kill switch域名的查询数



Talos第一时间建议用户采取措施

- 补丁更新

  安装MS17-010 (微软3月14日发布)

- 阻断SMB连接

  端口 139和445

- 阻断TOR流量

  在Firepower设备上启用安全智能security intelligence更新

- 入侵防御设备更新Snort规则

  42329-42332 DoublePulsar (April 25)
  42340 Anonymous SMB (April 25)
  41978 Samba buffer overflow (March 14)

- AMP防护监控

  监控是否发现恶意执行文件

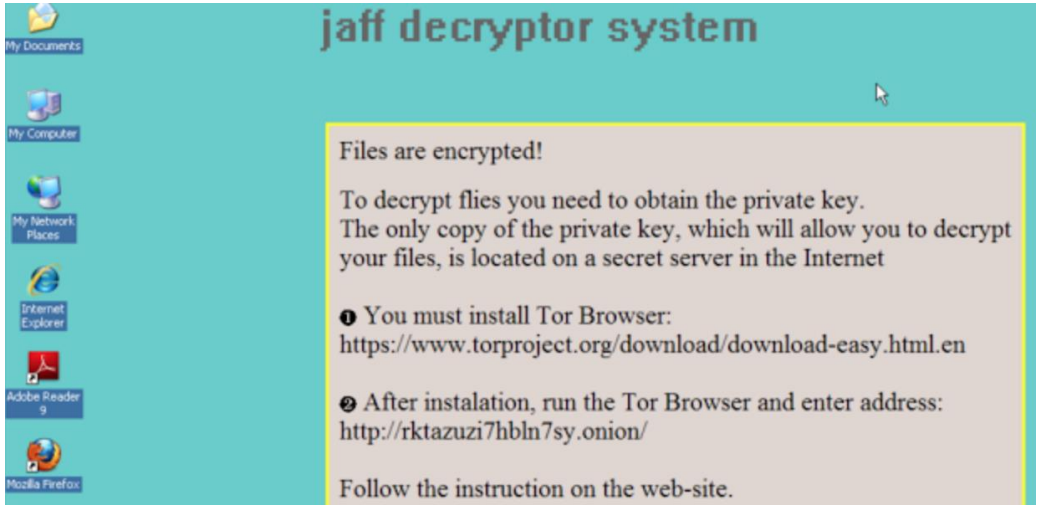
- Cisco Umbrella

  识别恶意域名解析行为并实施保护

TALOS

Talos提醒-WannaCry后面是Jaff，攻击没有停止

- 思科Talos威胁研究团队发现，紧随WannaCry，另一个勒索软件的变种Jaff也开始出现了大规模爆发。
- 勒索软件Jaff包含在钓鱼邮件中，通过PDF格式的附件，附件中嵌入了自动下载勒索软件的工具，一旦打开将下载并安装勒索软件。
- WannaCry与Jaff采用了不同的传播方式：
  - 勒索软件WannaCry，利用Windows主机的SMB服务漏洞，进行入侵攻击并安装勒索软件。
  - 勒索软件变种Jaff，借助于钓鱼邮件也开始大规模传播。



思科Talos关于WannaCry和Jaff的详细信息

- 勒索软件WannaCry的详细分析：
  http://blog.talosintelligence.com/2017/05/wannacry.html

- 勒索软件Jaff的详细分析：
  http://blog.talosintelligence.com/2017/05/jaff-ransomware.html

议题

- WannaCry与Jaff勒索软件解析
- 重新认识勒索软件的危害与演化趋势
- 思科安全如何应对勒索软件
- 最佳实践与建议
- 问题与讨论

2016安全报告-Ransomware已经进化到2.0

报告指出，勒索软件攻击方式在不断演化，已经具备自我复制和大规模传播的能力

自我复制和传播

- 利用漏洞大范围传播
- 复制到所有可用设备
- 文件感染
- 有限制的暴力破解行动
- 弹性的C2连接
- 利用各种系统后门

模块化

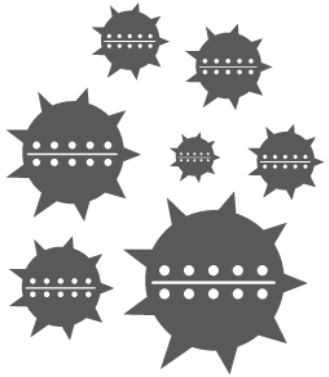
- Autorun.Inf/USB大容量存储介质传播
- 利用认证基础架构的漏洞入侵
- C2报告感染统计
- 攻击速率控制
- RFC1918目标地址限制

2017安全报告-勒索软件攻击已经成为常态

报告指出，勒索软件的攻击工具愈加自动化，减少漏洞和加强安全保护才能降低被攻击风险

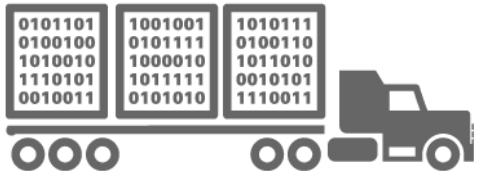
Recon

分析，筛选和确定目标



Weaponization

利用远程访问代码和漏洞攻击入侵配合使用



Delivery

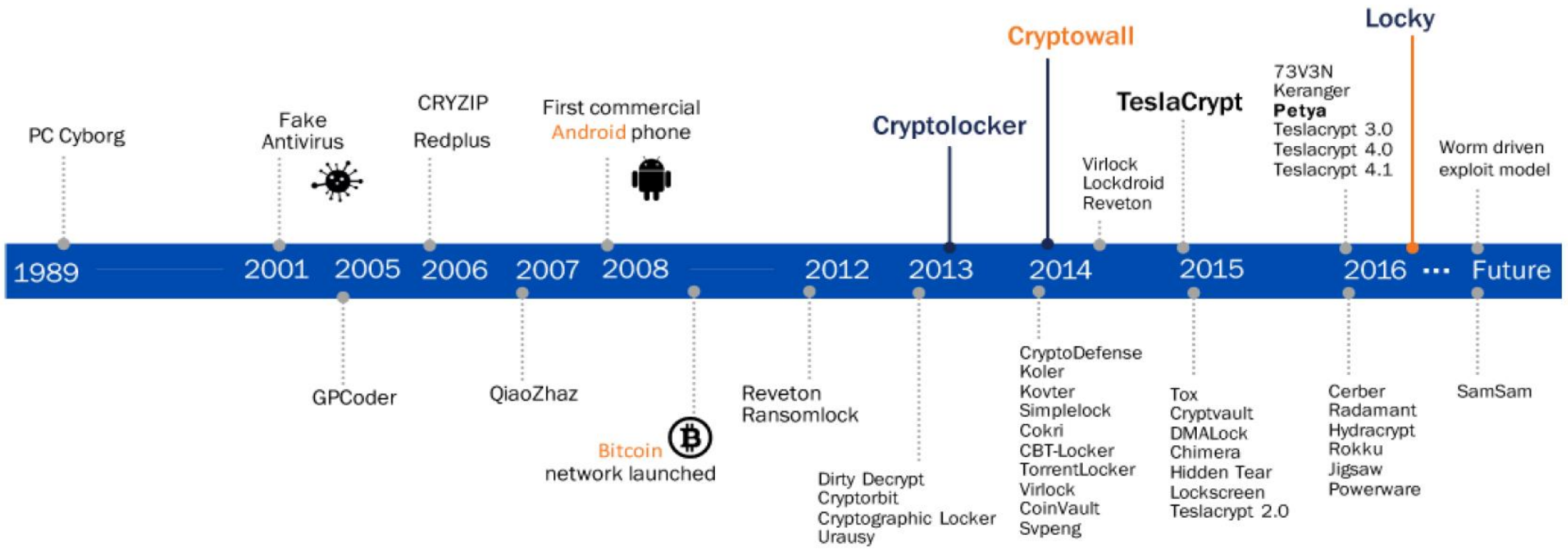
利用邮件，网站和附件散播恶意代码

Installation

安装恶意代码，驻留和传播

勒索软件的演变历史

- 采用对称加密方式，加密文件名，隐藏文件夹，影响用户访问文件系统，如PC Cyborg,QiaoZhaz等。
- 采用非对称加密方式，针对文档、图片、音频，视频等文件加密，如GPCoder,CRYZIP等。
- 采用强加密算法，利用Trojan-Downloader从C&C主机获取密钥，通过Bitcoin方式支付赎金，如Cryptolocker, Locky等。
- 思科Talos预测,未来可能会以蠕虫传播的方式，在网络内部有关联的应用系统之间传播，更大范围勒索金钱。



专门针对企业的勒索软件-Samsam

- 攻击者的目标转向企业用户，专门针对关键数据或应用服务器，甚至是IoT设备。
- 攻击者探测某些应用系统存在未打补丁的漏洞，入侵成功后安装Samsam软件，感染Web应用服务器。
- 勒索软件会逐步在网络中传播，寻找企业用户的重要数据，甚至包括映射的网络共享和备份数据。

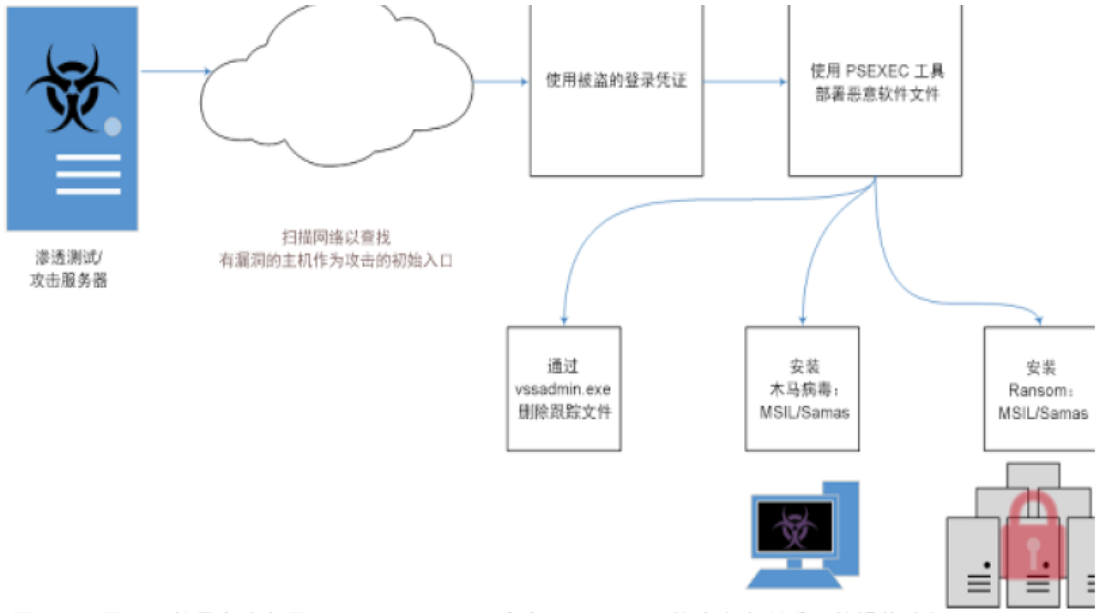


图 9：下图显示的是负责部署 MSIL/Samas（又称为“samsam”）的攻击者所采取的操作流程，

企业用户被感染的案例

- 2016年2月，国外某医院的病人数据被加密，造成医疗应用系统无法访问病人资料；攻击者勒索300万美金。

- 2016年11月，国外某地铁公司的应用系统被加密，造成售票机无法提供售票业务，乘客免费乘坐地铁运营两天；攻击者勒索7.5万美金。

勒索软件对企业的危害更大

- 由于企业数据被加密后，造成业务无法正常运营，甚至业务中断，经济损失和社会舆论压力迫使受害者快速支付赎金，缩短了勒索时间，因此企业成为攻击者的下一个主要目标。
- 医疗：医院可能无法访问或丢失重要的病人信息，治疗系统无法正常工作，影响对患者进行及时的救治。
- 交通：公共交通的关键控制系统无法正常运行，售票系统的瘫痪，造成整个运营系统的混乱，运营方遭受巨大损失和公众压力。
- 金融：网上银行系统或者柜员系统被控制，导致关键信息泄露，或无法提供正常交易，带来造成巨大经济损失。
- 制造：影响生产线的正常工作，造成生成停滞，供货延期，制造商违约，损失巨大。
- 教育：教育与科研系统无法工作，科研资料无法访问，科研活动中断，研究成果无法找回。

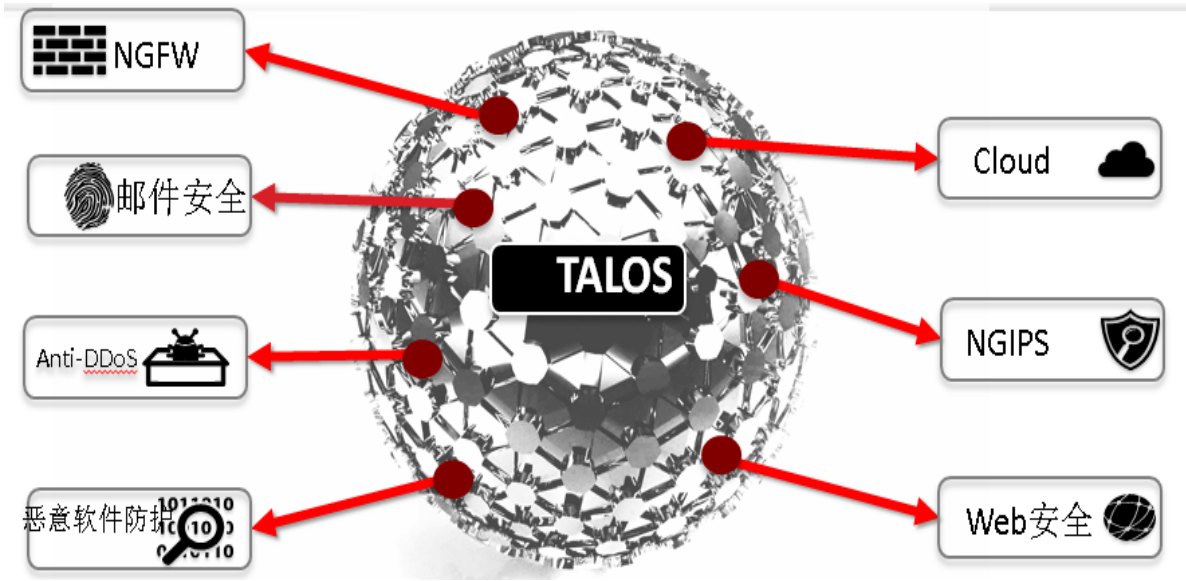
议题

- WannaCry与Jaff勒索软件解析
- 重新认识勒索软件的危害与演化趋势
- 思科安全如何应对勒索软件
- 最佳实践与建议
- 问题与讨论

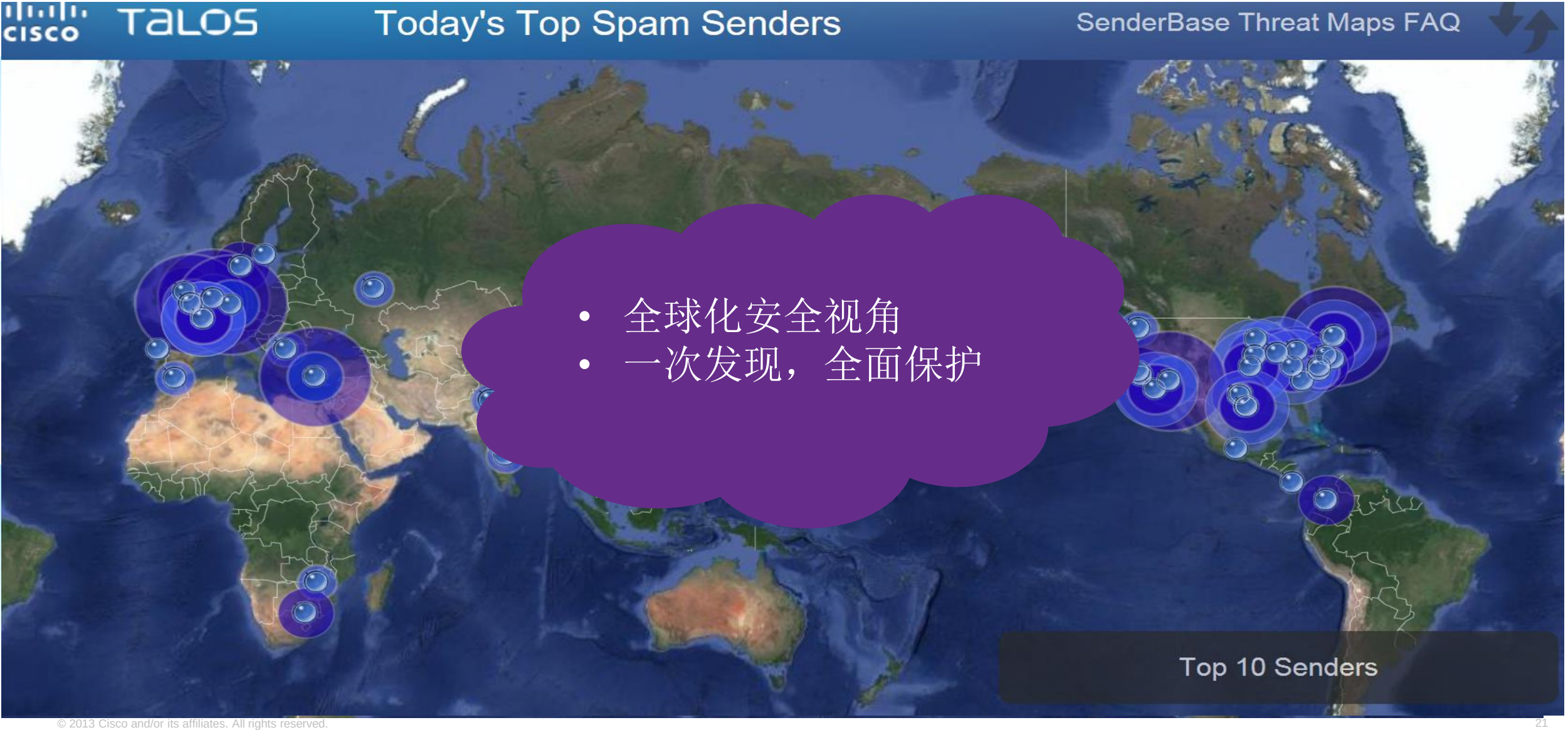
思科Talos威胁情报研究中心

TALOS是业界最大的威胁情报研究团队

- 业界领先的网络安全专家组成
- 分析评估黑客活动，入侵企图，恶意软件以及漏洞的最新趋势
- 来自Snort、ClamAV、Senderbase.org和Spamcop.net等丰富的资源支持
- 为思科安全产品和服务提供了强大的后盾支持

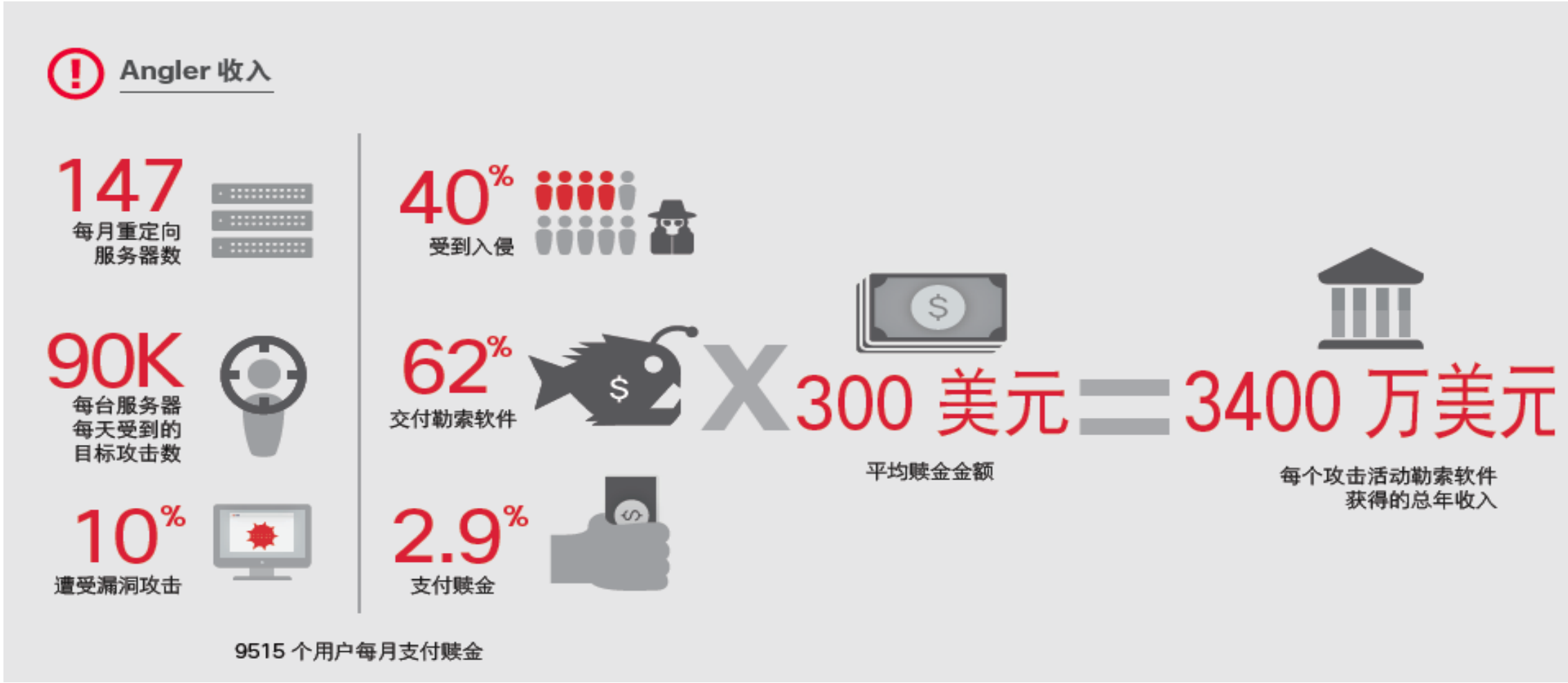


思科Talos – 实现全球化安全视角



思科Talos帮助运营商挽回3400万美元损失

2016年阻止勒索软件Angler在Limestone和hertzner两个服务托管运营商的爆发

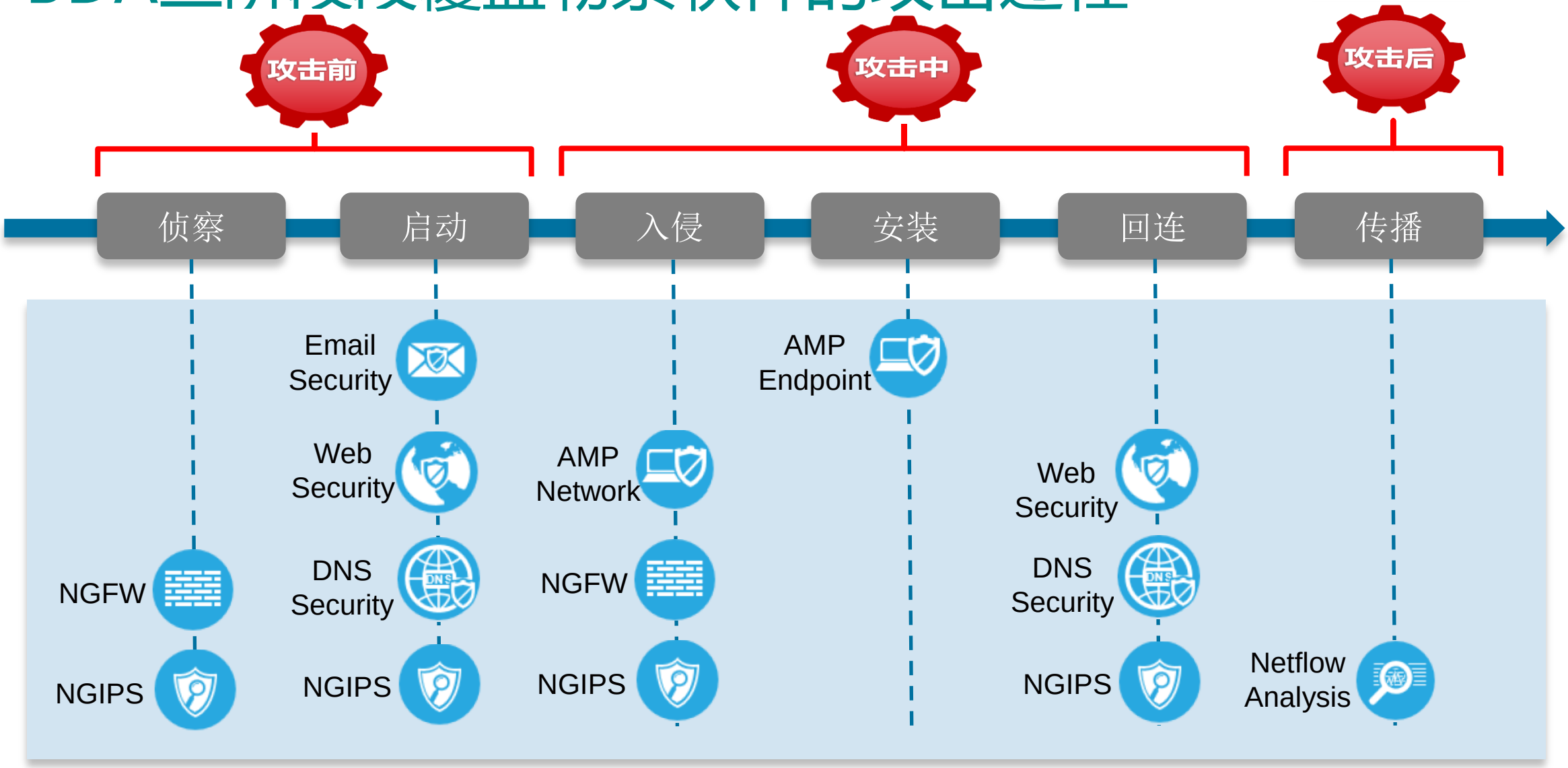


思科动态威胁防御模型-Before,During,After

涵 盖 威 胁 防 御 的 的 完 整 周 期

主机与应用可视化	威胁智能防御	威胁影响日志
AVC访问控制策略	IoC感染指数	风险评估报告
自动化防御策略	联动策略告警	恶意代码的轨迹跟踪

BDA三阶段段覆盖勒索软件的攻击过程



思科应对勒索软件的产品和方案

ASA NGFW/NGIPS和Email防护

识别终端主机的C&C连接

拦截含有恶意附件的邮件

识别或改写邮件的URL钓鱼链接

零日威胁爆发过滤

集成AMP防护

OpenDNS与Web防护

防止恶意网站的DNS解析

拦截超过95%的C&C域名解析请求

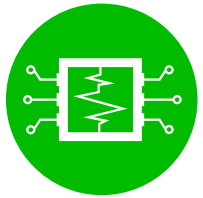
URL信誉过滤拦截C&C网站访问

AMP高级恶意代码保护

利用云智能分析技术

恶意代码一旦被发现后，则实现后续的检测和拦截

对已知的恶意文件拦截最有效



StealthWatch(Lancope)

检测和发现感染主机与C&C僵尸网络的通信

对连接C&C的通信企图进行告警

借助网络设备作为探针来发现和降低风险

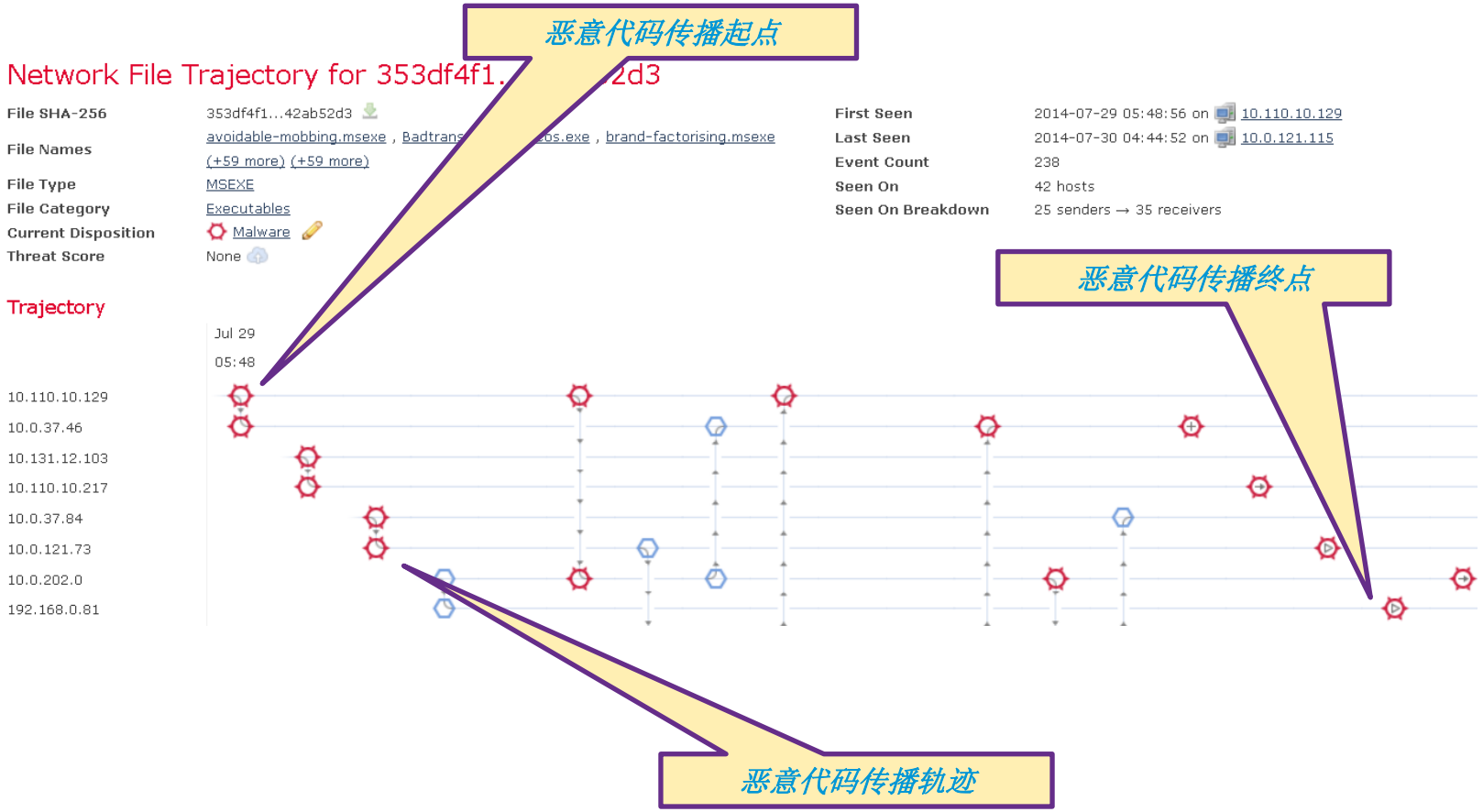
应对之一：网络边界安全保护内部主机

思科Firepower NGFW和NGIPS阻止端口扫描和漏洞探测

- 阻断攻击者对内部主机的端口扫描，缩小暴露在外网的攻击面。
- 拦截外部的入侵和攻击，保护内网有漏洞的主机免受威胁。
- 整合AMP恶意软件检测和防护功能。
- 检测内网中的C&C连接，切断下载勒索软件和加密密钥的通路。

Firepower NGFW/NGIPS记录恶意代码传播轨迹

AMP基于网络设备与终端设备协作与共享威胁事件信息



- 支持基于网络/终端/云/网关等，多个位置进行全方位安全防护。
- 完整记录恶意文件的传播的起点、过程和终点。
- 实现持续性的的威胁检测与防护。
- 回溯整个攻击发生的过程
- 保存威胁发生的证据与记录，用于事后追踪和审计。

Firepower NGFW/NGIPS发现勒索软件-拦截记录

- 发现加密勒索软件Locky的入侵行为：

Event Type	Event Subtype	Threat Name	File Name	File SHA256
Threat Detected in Network File Transfer (Retrospective)		W32.E5F66F6536.Locky.tht.Talos		e5f66f65...63f55024
Threat Detected in Network File Transfer (Retrospective)		W32.E5F66F6536.Locky.tht.Talos	INVOICE_huangyang.zip	e5f66f65...63f55024
Threat Detected in Network File Transfer (Retrospective)		W32.E5F66F6536.Locky.tht.Talos	INVOICE_qulili.zip	e5f66f65...63f55024
Threat Detected in Network File Transfer (Retrospective)		W32.E5F66F6536.Locky.tht.Talos	INVOICE_changyi.zip	e5f66f65...63f55024
Threat Detected in Network File Transfer (Retrospective)		W32.E5F66F6536.Locky.tht.Talos	INVOICE_huangyang.zip	e5f66f65...63f55024
Threat Detected in Network File Transfer (Retrospective)		W32.E5F66F6536.Locky.tht.Talos	INVOICE_huangyang.zip	e5f66f65...63f55024

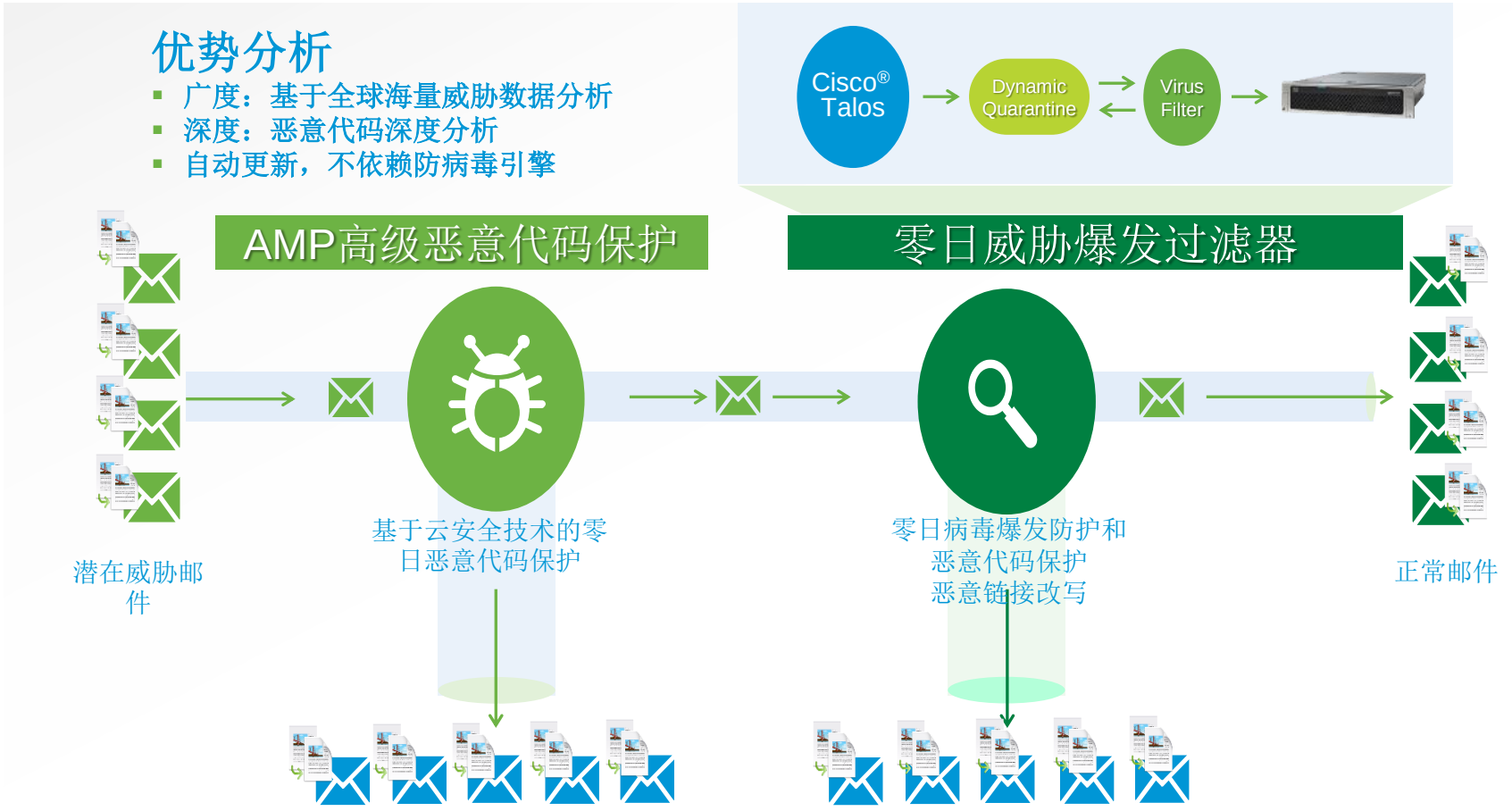
- 记录加密勒索软件的详细信息：

Network File Trajectory for e5f66f65...63f55024

File SHA-256	e5f66f65...63f55024
File Names	INVOICE_changyi.zip , INVOICE_qulili.zip , INVOICE_huangyang.zip , INVOICE_zhengyi.zip (+1 more)
File Type	
File Category	
Current Disposition	Malware

应对之二：切断钓鱼邮件传播途径

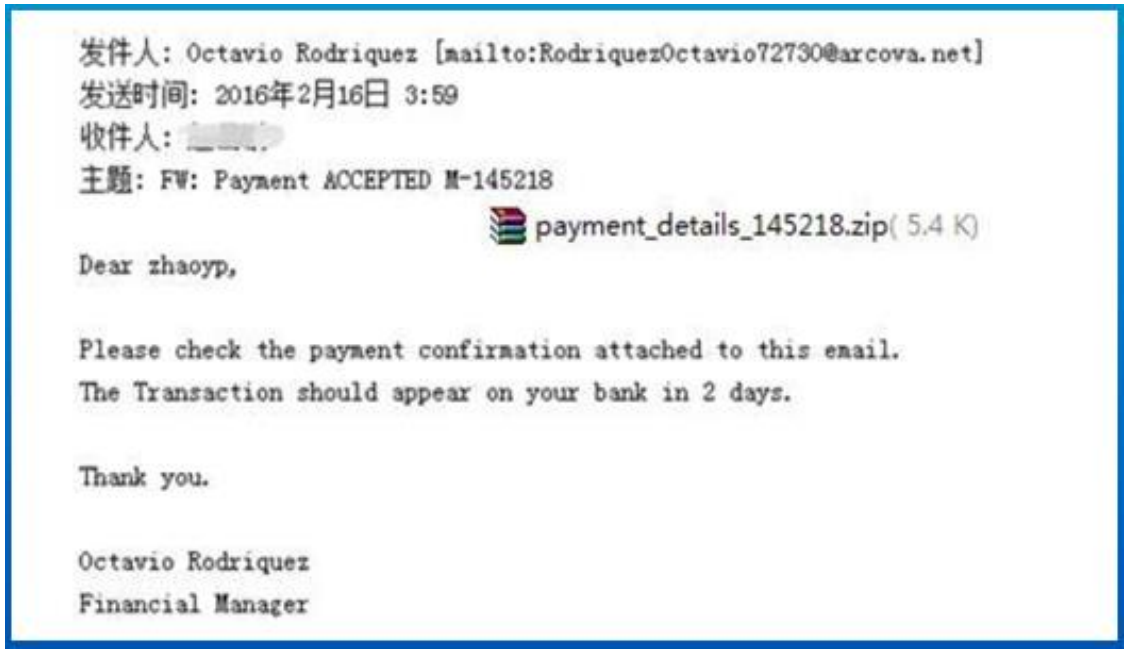
思科ESA邮件安全网关过滤钓鱼邮件和拦截恶意代码



- 恶意邮件过滤集成恶意软件防护，切断恶意软件/勒索软件的传播。
- 对邮件中存在的恶意链接，可以进行防护或者改写。
- 基于最新的零日威胁威胁，提供过滤恶意邮件。

ESA切断钓鱼邮件传播途径-拦截记录

带恶意附件的钓鱼邮件：


发件人: Octavio Rodriquez [mailto:RodriquezOctavio72730@arcova.net]
发送时间: 2016年2月16日 3:59
收件人: [redacted]
主题: FW: Payment ACCEPTED M-145218

payment_details_145218.zip(5.4 K)

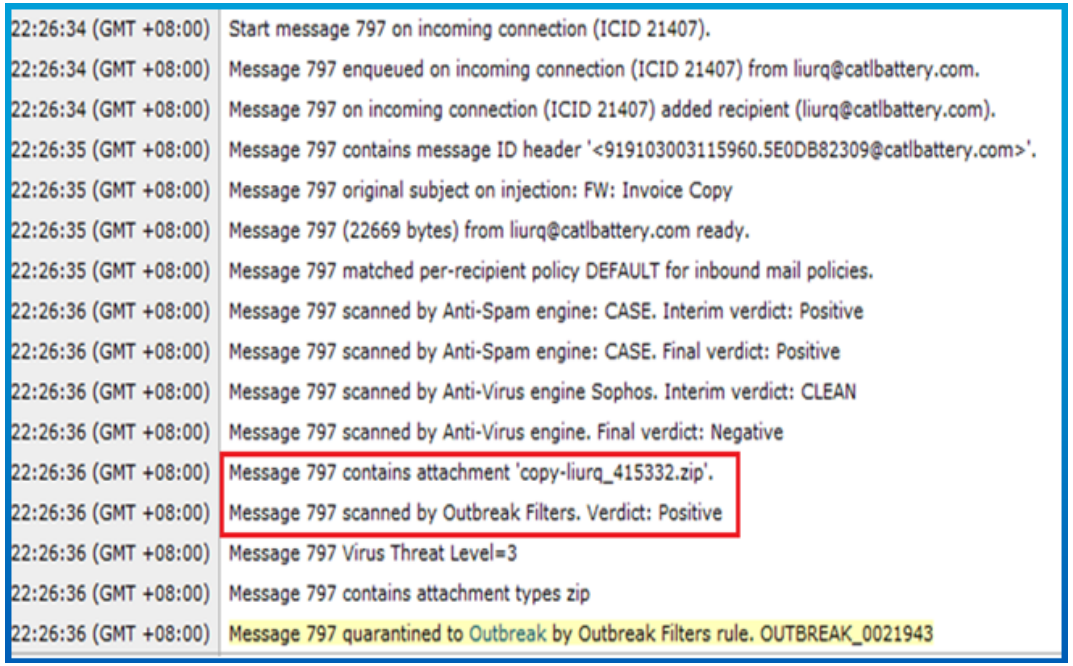
Dear zhaoyp,

Please check the payment confirmation attached to this email.
The Transaction should appear on your bank in 2 days.

Thank you.

Octavio Rodriquez
Financial Manager

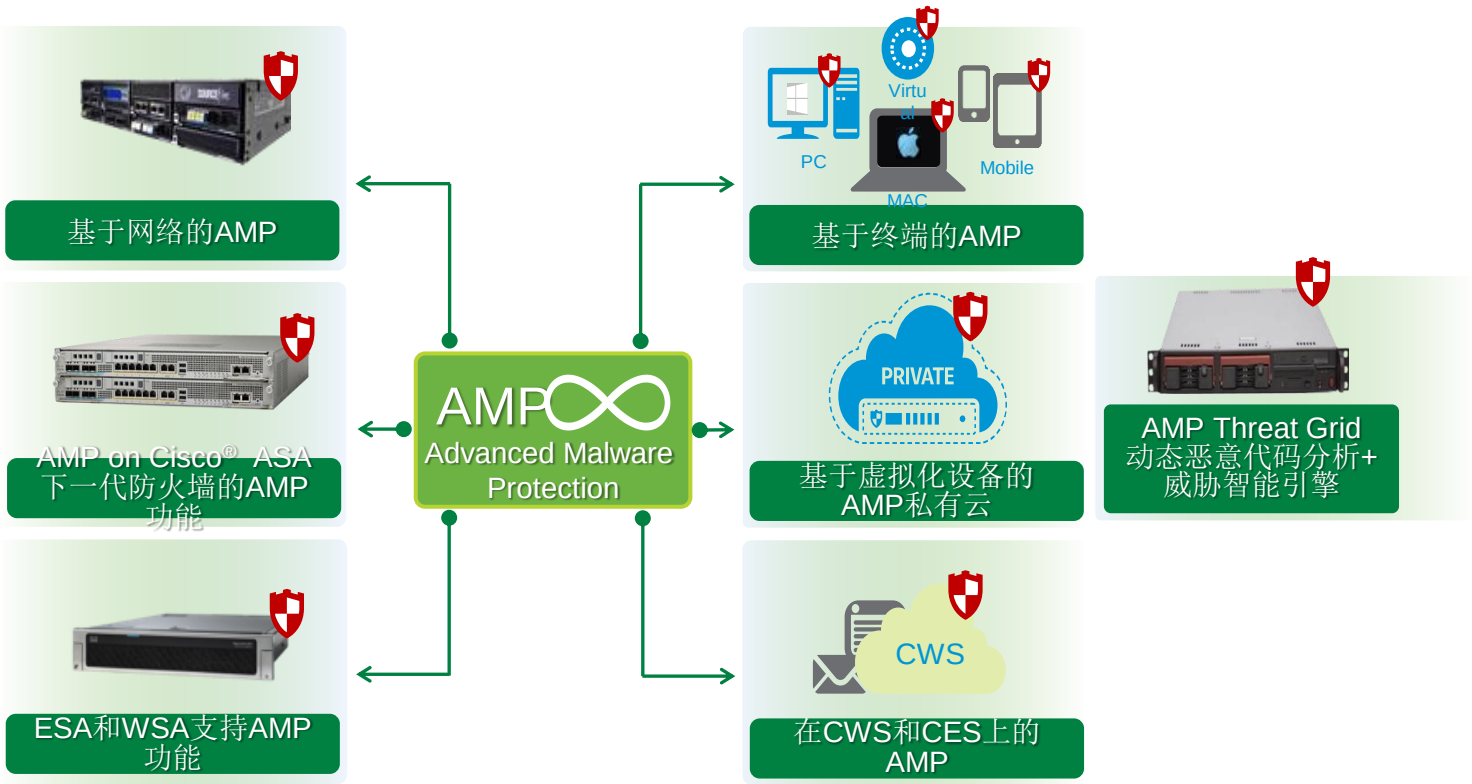
邮件网关拦截记录：



22:26:34 (GMT +08:00)	Start message 797 on incoming connection (ICID 21407).
22:26:34 (GMT +08:00)	Message 797 enqueued on incoming connection (ICID 21407) from liurq@catlbattery.com.
22:26:34 (GMT +08:00)	Message 797 on incoming connection (ICID 21407) added recipient (liurq@catlbattery.com).
22:26:35 (GMT +08:00)	Message 797 contains message ID header '<919103003115960.5E0DB82309@catlbattery.com>'.
22:26:35 (GMT +08:00)	Message 797 original subject on injection: FW: Invoice Copy
22:26:35 (GMT +08:00)	Message 797 (22669 bytes) from liurq@catlbattery.com ready.
22:26:35 (GMT +08:00)	Message 797 matched per-recipient policy DEFAULT for inbound mail policies.
22:26:36 (GMT +08:00)	Message 797 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
22:26:36 (GMT +08:00)	Message 797 scanned by Anti-Spam engine: CASE. Final verdict: Positive
22:26:36 (GMT +08:00)	Message 797 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
22:26:36 (GMT +08:00)	Message 797 scanned by Anti-Virus engine. Final verdict: Negative
22:26:36 (GMT +08:00)	Message 797 contains attachment 'copy-liurq_415332.zip'.
22:26:36 (GMT +08:00)	Message 797 scanned by Outbreak Filters. Verdict: Positive
22:26:36 (GMT +08:00)	Message 797 Virus Threat Level=3
22:26:36 (GMT +08:00)	Message 797 contains attachment types zip
22:26:36 (GMT +08:00)	Message 797 quarantined to Outbreak by Outbreak Filters rule. OUTBREAK_0021943

应对之三：AMP技术检测恶意代码

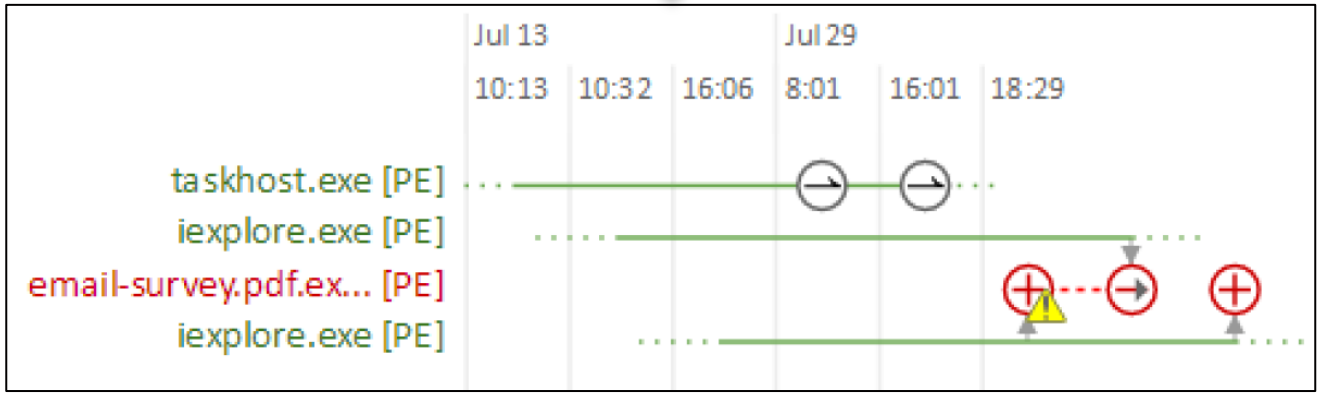
思科AMP技术可以集成在安全设备或者部署在主机终端



AMP对恶意软件的防护：

- 支持基于网络/终端/云/网关等，多个位置进行全方位防护。
- 对文件实施检测，找到恶意软件/勒索软件，进行阻挡和清除
- 通过云智能分析以及ThreatGrid沙盒技术，对可疑的软件进行分析，基于行为，识别出勒索软件

AMP技术检测恶意代码-拦截记录



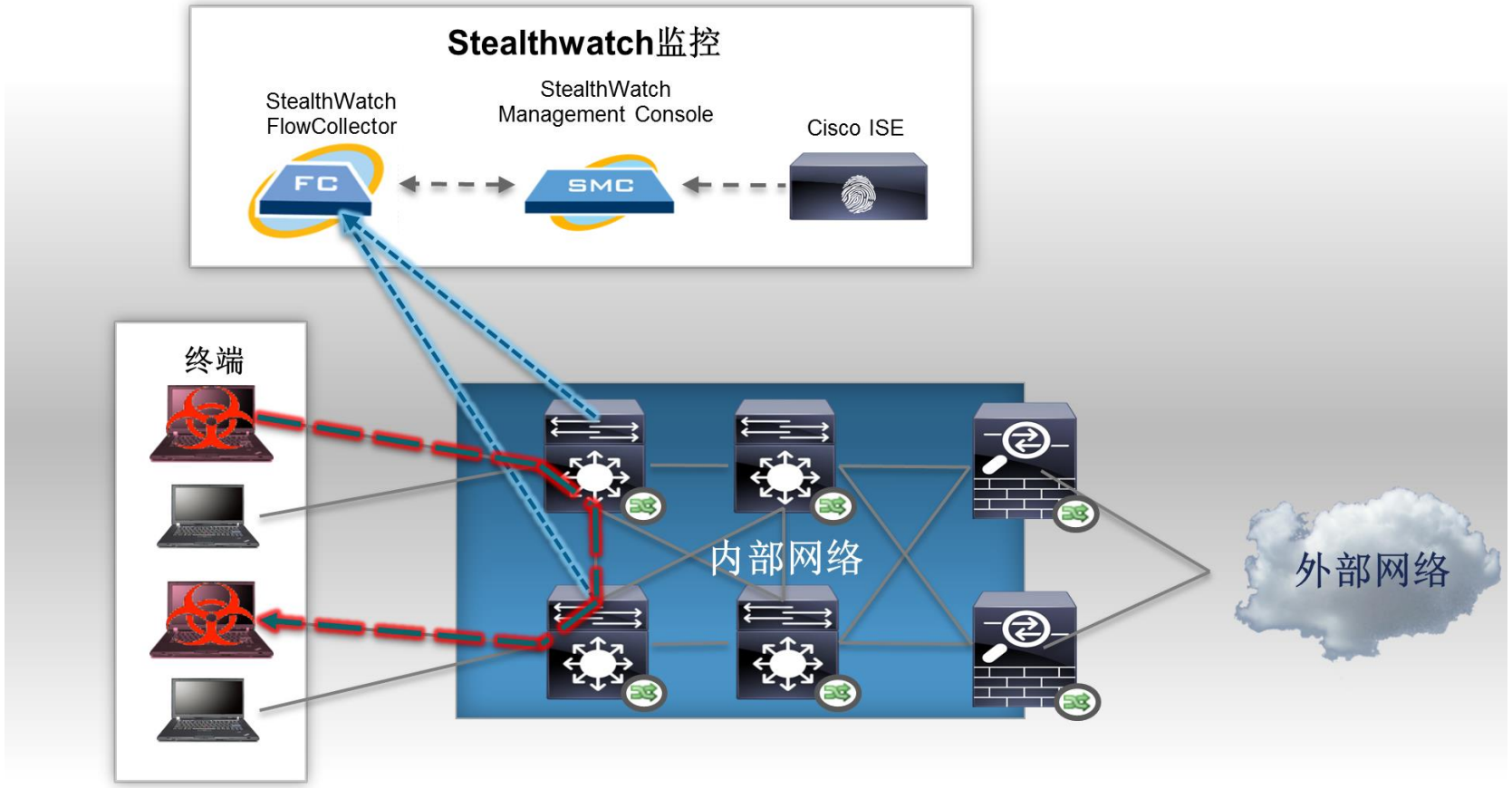
恶意文件轨迹跟踪

AMP检测并拦截恶意文件：

- 基于组合方式分析，包括特征库，文件信誉度，行为分析和沙盒技术。
- 持续分析和跟踪，并记录文件的完整的传播记录。
- 一旦确认是恶意软件，AMP能够采用手工或者自动方式，进行隔离或者修复。

应对之四：Stealthwatch检测内网异常行为

思科Stealthwatch检测内网终端发生蠕虫传播行为



Stealthwatch检测内网异常行为：

- 分析Flow记录，基于机器学习和大数据分析，识别网络中各种异常行为。
- 检测内部主机之间的端口扫描行为，网络传播，发现内部传播勒索软件的行为
- 检测内网主机到C&C的连接请求，切断被感染主机下载加密程序或加密密钥的的通路。

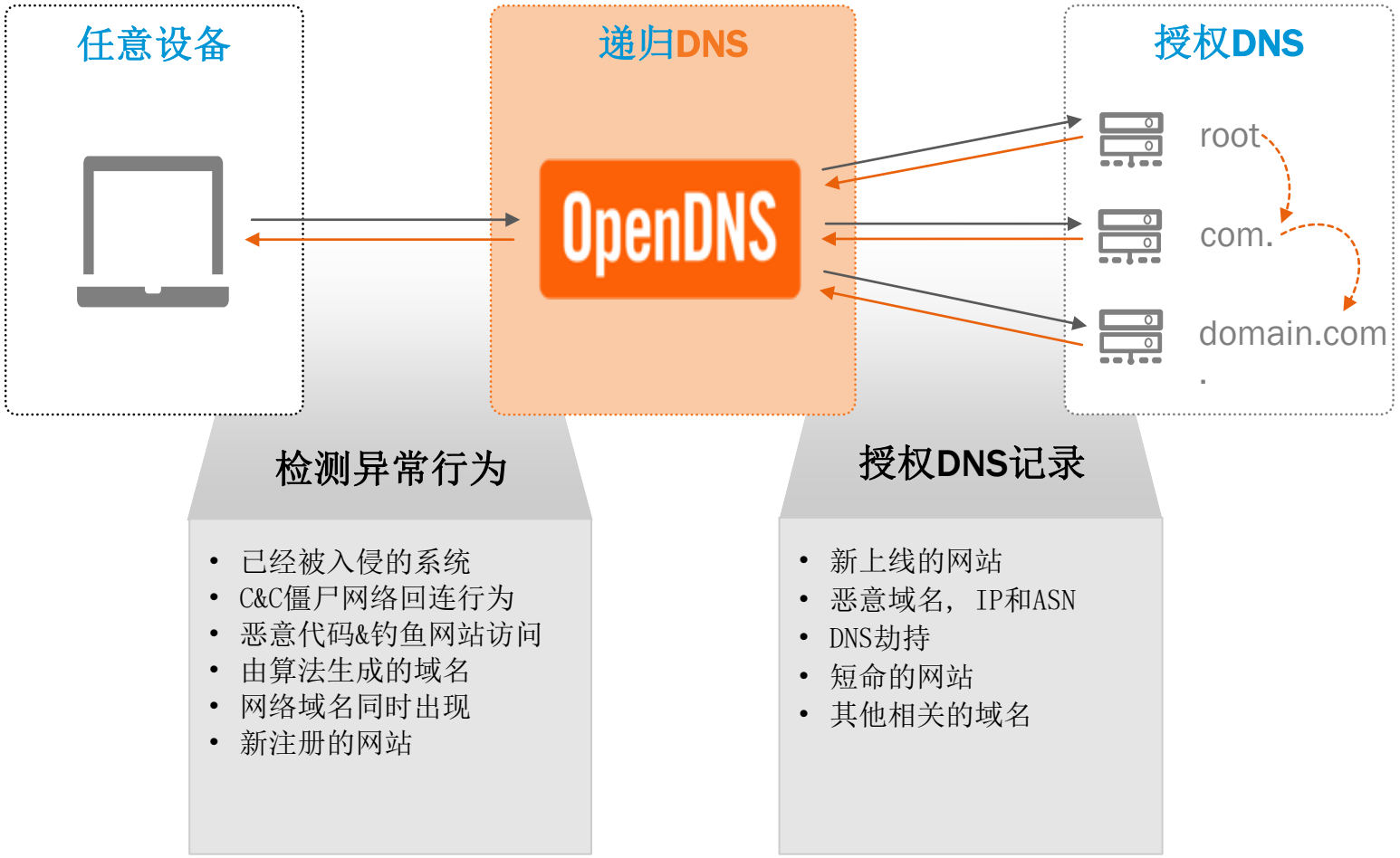
应对之五：WSA拦截钓鱼网站访问和恶意代码下载

WSA对勒索软件的防御：

- URL网站分类库，限制访问与工作无关的网站。
- 网站信誉过滤技术，拦截用户访问各类钓鱼或恶意网站。
- 集成AMP高级恶意代码防护，实现对恶意代码的检测和拦截。

应对之六：Umbrella切断恶意域名解析

Umbrella通过DNS解析结果的智能分析,切断访问C&C主机的行为



Umbrella对勒索软件的防御：

- 分析DNS域名的可信度，将恶意域名的解析结果重定向到安全网址
- 检测通过算法生成的域名
- 阻断对钓鱼或恶意网站的访问
- 阻断对C&C网络的回连行为

应对之七：统一准入控制与分区隔离

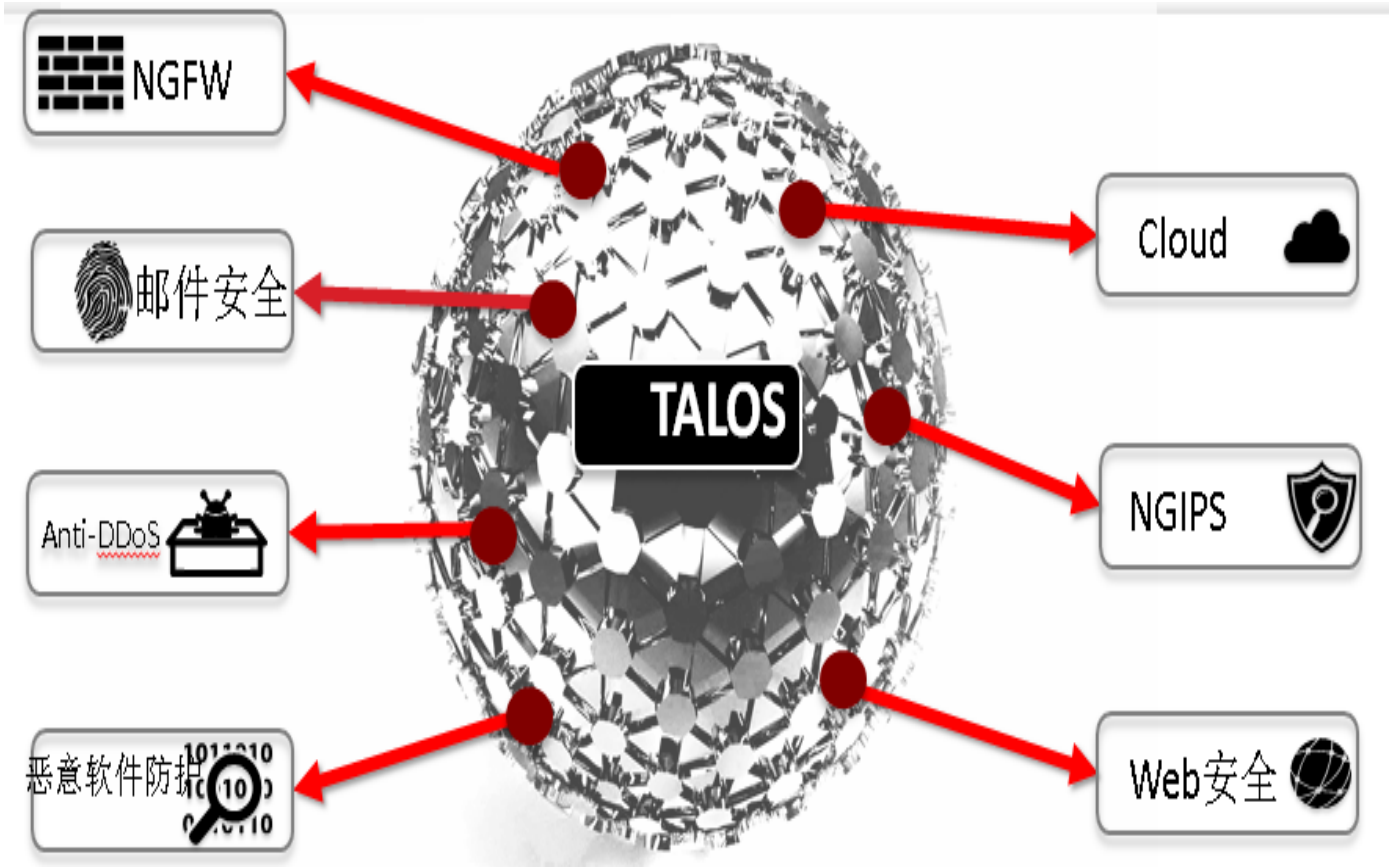
结合统一准入控制与内网分区隔离，阻断勒索软件大范围传播

网络接入场景	用户身份组识别	组合条件	用户授权结果

思科Talos威胁情报中心扮演关键角色

TALOS是业界领先的安全情报中心

- 即时更新针对最新漏洞的攻击特征
- 即时更新最新的Email和URL信誉
- 即时更新最新的恶意软件样本
- 即时更新最新的C&C地址



议题

- WannaCry与Jaff勒索软件解析
- 重新认识勒索软件的危害与演化趋势
- 思科安全如何应对勒索软件
- 最佳实践与建议
- 问题与讨论

企业勒索软件防御的最佳实践 - 人、流程和技术

- 人员
  - 员工安全意识培训，提高对网络威胁的辨识能力。
- 流程
  - 定期进行系统的备份，缩短备份间隔的时间。
  - 完备的灾难恢复计划，确保能够有效实施。
  - 制定涵盖人、流程和技术的应急处理机制，并定期进行演习。
  - 设定安全基线，包括应用软件、系统软件镜像、以及网络性能指标。
- 技术
  - 健壮的应用与系统软件的补丁管理
  - 实行操作系统软件的标准化，快速的系统恢复步骤。
  - 用户终端的准入控制，严格控制访问权限。

思科建议：有针对性的员工安全意识培训

利用ESA邮件网关设备，统计哪些用户点击了带有钓鱼链接的网站，对这些用户进行针对性的安全意识培训。

被重写的URL统计报告

- 恶意URL链接排名
- 用户点击了链接日期/时间，
- 重写原因，URL动作

访问过重写URL的用户列表

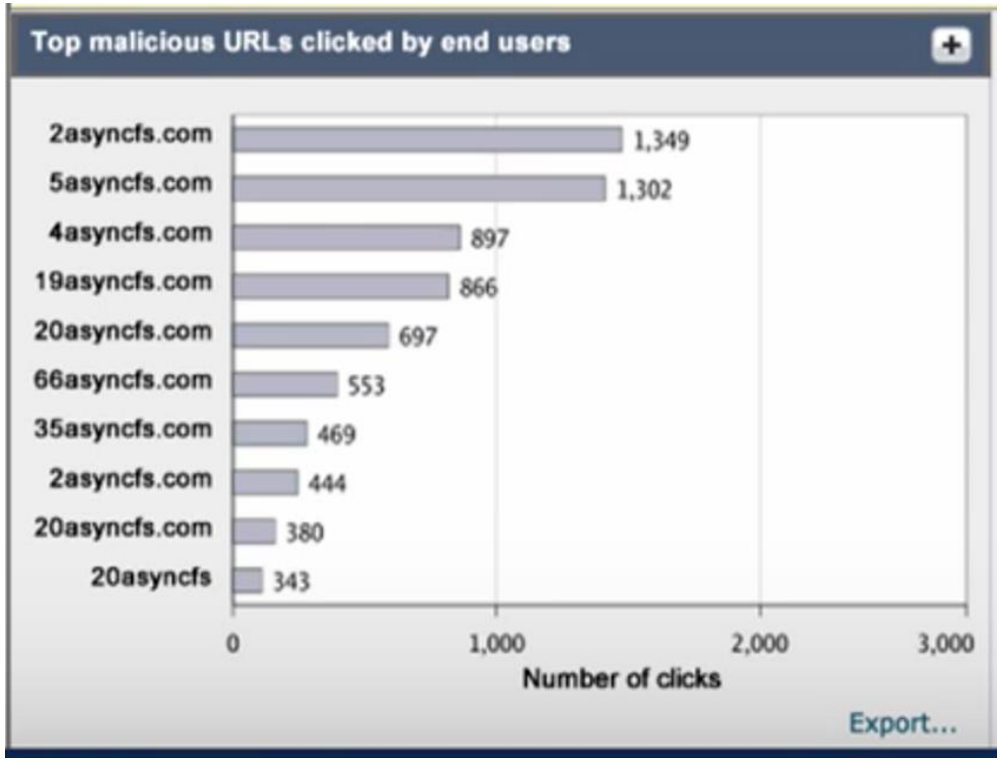
- 按照邮件ID统计
- 按照LDAP分组统计
- 按照IP地址统计

将恶意URL或钓鱼链接加入到黑名单

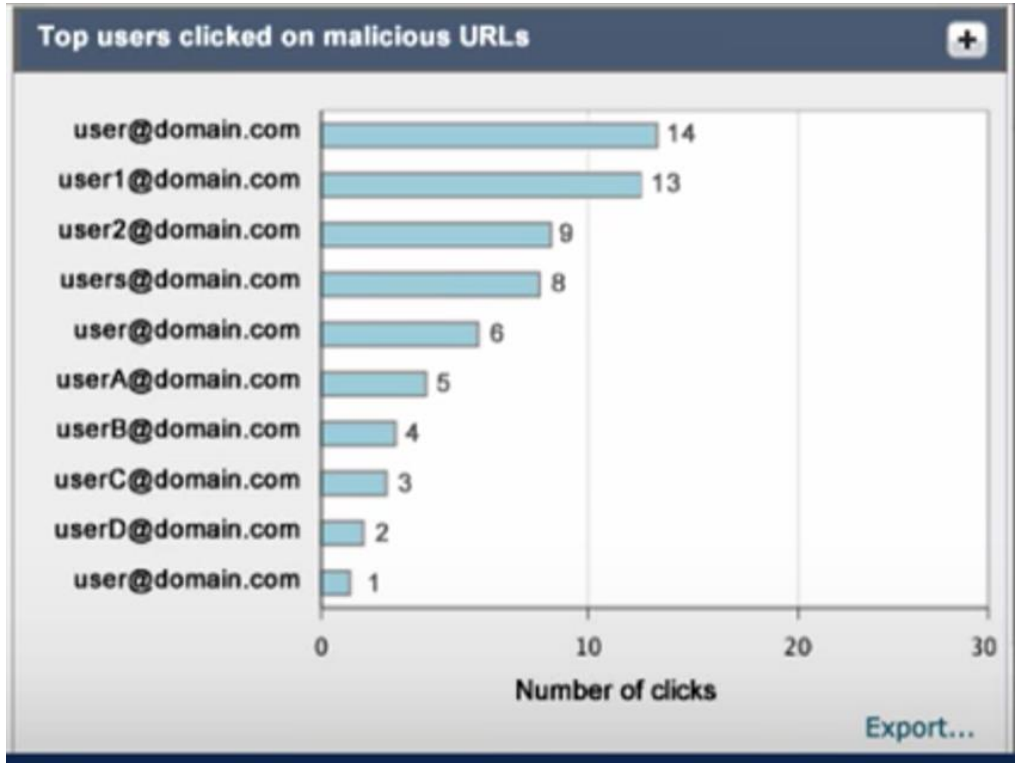
- 阻止零日攻击
- 动态智能
- 用户安全教育

思科建议：有针对性的员工安全意识培训

- 被点击的恶意网站的排名统计



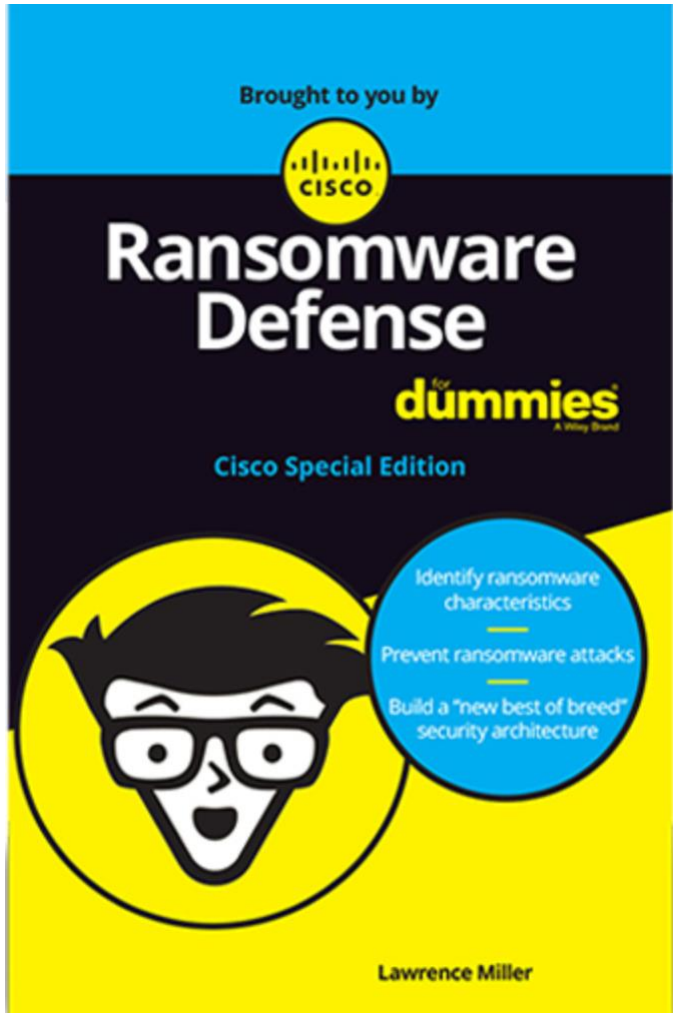
- 点击恶意链接的用户排名统计



员工防范勒索软件的几个建议

- 确保个人电脑系统安装了最新的补丁。
- 确保安装了防病毒或者防恶意软件程序，并保持定期的到最新。
- 定期备份电脑中的重要文件。
- 访问邮件时，确认邮件发件人是真实的邮箱地址，如果发件人地址不认识或者不确认发件人是谁，就不要打开任何附件，或者点击邮件中的链接因为这有可能是恶意文件或者钓鱼链接。
- 安装软件一定要通过正规途径，尽量不要通过免费网站下载各类软件，这些软件很可能已经被嵌入了恶意代码。

思科安全资源-勒索软件防御傻瓜书



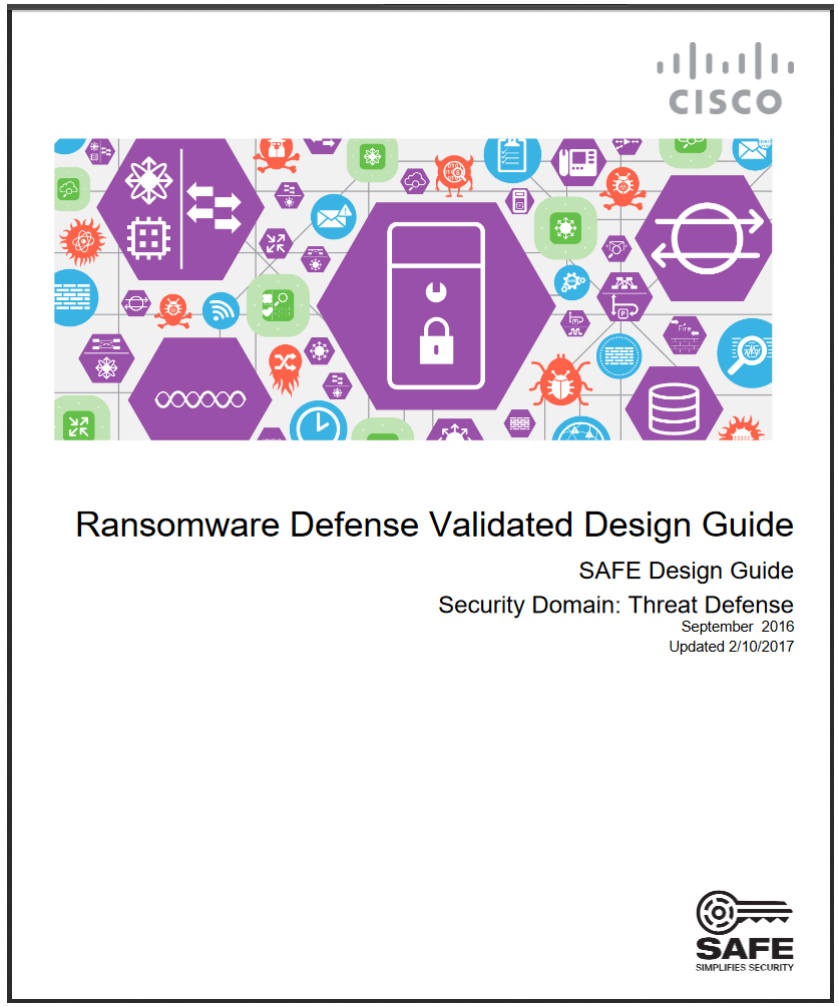
通过本书您可以了解：

- 勒索软件是如何工作的
- 勒索软件的有哪些特点
- 降低勒索软件的最佳实践
- 什么是架构式安全防御
- 思科勒索软件防御解决方案
- 勒索软件防御的关键点

- 下载链接

https://resources.umbrella.com/ransomware-for-dummies/

思科安全资源-勒索软件防御设计指南



通过本书您可以了解：

- SAFE架构介绍
- 勒索软件概览
- 什么是架构式解决方案
- 如何实施架构式解决方案
- 如何进行验证测试

- 下载链接

http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/ransomware-defense-dig.pdf

关键点回顾

- 由于直接经济利益的驱动，使勒索软件的危害在不断蔓延。
- 勒索软件逐渐转向企业用户，目的是追求勒索更大规模的赎金。
- 思科架构式安全产品与解决方案，帮助用户从各个阶段、各个层面有效防御加密勒索软件。
- 关注思科安全资源：
  - 意识培养：利用社会工程散播勒索软件视频
  - 技术博客：思科Talos持续跟踪和研究威胁演变和防御
  - 设计指南：思科安全防御加密勒索软件的设计指南

Thank you.