# 思科安全如何防御加密勒索软件

吴清伟
中国区安全技术顾问

# 议题

- 认识加密勒索软件
- 加密勒索软件的演化趋势
- 思科安全如何防御加密勒索软件
- 最佳实践与建议
- 问题与讨论

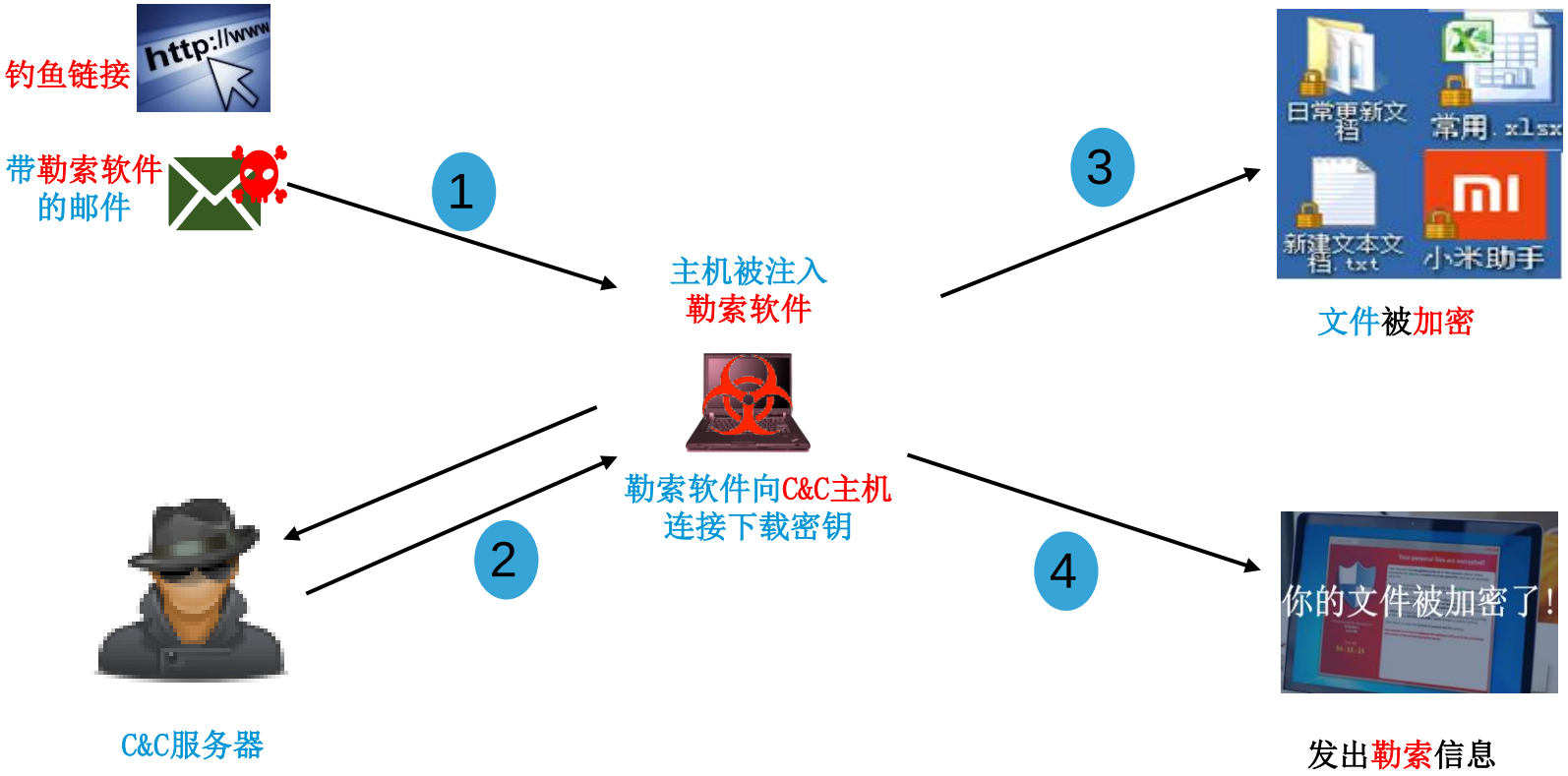
# 加密勒索软件的危害在蔓延

## 思科2016年安全报告显示：勒索软件已经成为史上最赚钱的恶意软件

# 何为加密勒索软件

- 勒索软件是一种恶意软件，其通过邮件或钓鱼网站等方式，利用主机或应用存在的漏洞，感染用户主机或重要服务器。
- 勒索软件侵入电脑后，对文件系统进行遍历和查找，然后对图片，视频和文档类型的文件进行加密处理，造成使用者无法访问和使用。
- 勒索软件通常不会去加密系统文件，保证系统可以正常启动，显示勒索信息。
- 受害者若想打开被加密文件，必须通过支付赎金的方式，下载解密程序并获取解密的密钥，才有可能将文件解密。


# 勒索软件的典型入侵过程




1. 用户收到含有勒索软件的邮件，或者点击了钓鱼链接，导致主机被注入勒索软件。

2. 勒索软件注入成功后，控制了被感染主机，然后试图连接C&C主机获取用于加密程序或加密密钥。

3. 勒索软件在后台查找文件，并进行加密处理。

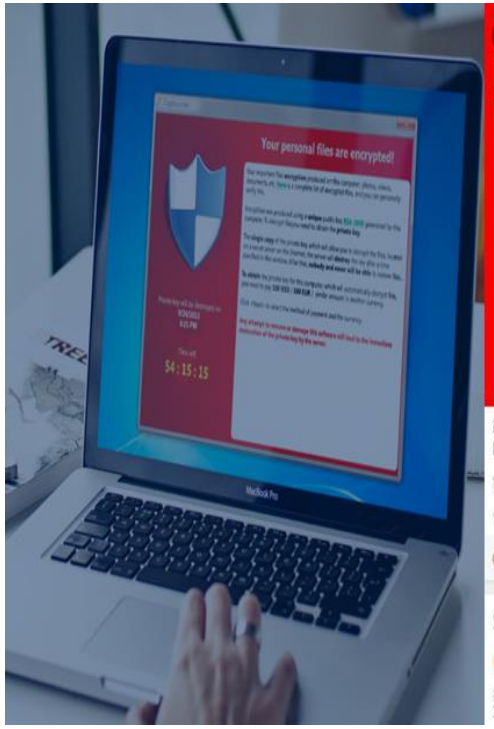
4. 攻击者发出勒索信息，通知用户支付赎金换取解密程序。

# 电脑的文件被加密后。。。


- 加密勒索软件的运行和加密的操作都是在后台完成，使用者常常没有感知。
- 使用者在文件无法访问时，才发现加密行为已经完成了。
- 攻击者通过修改桌面，或者其他通知方式，告知使用者需要支付赎金，获取解密程序和密钥来完成文件解密。

# 受害者收到的勒索信息

- 受害者会收到各种形式的勒索金钱的提示
- 支付赎金并不能确保对加密的文件进行解密

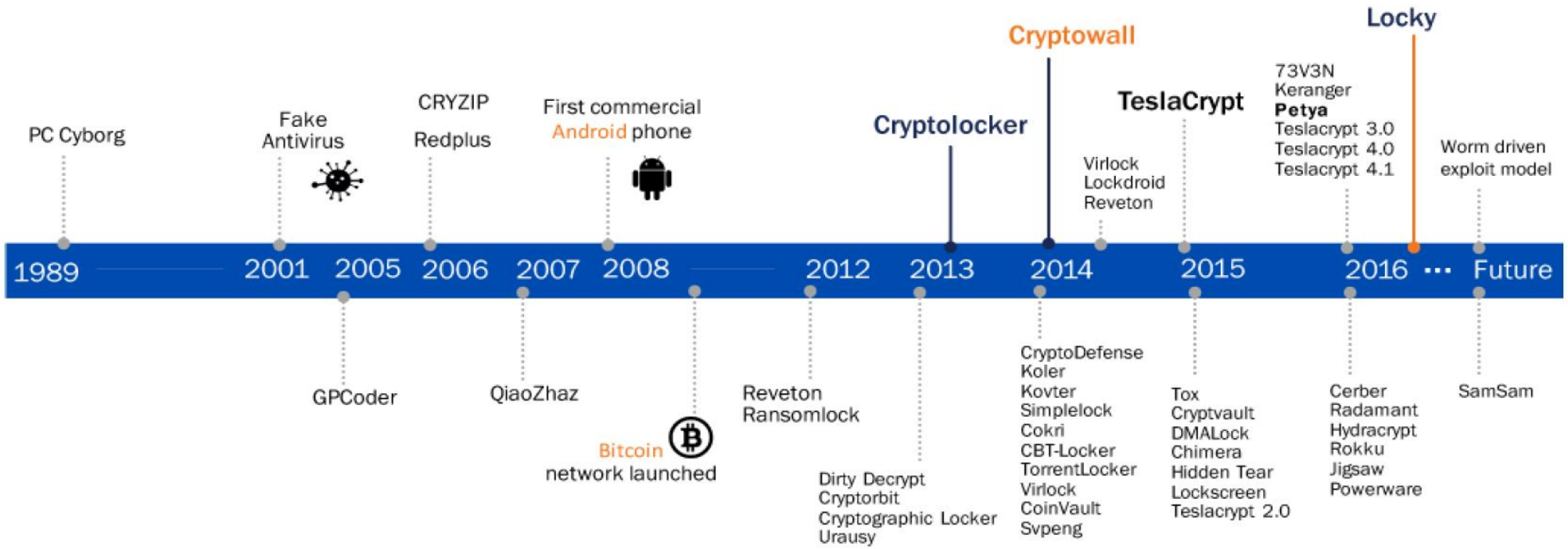


# 议题

- 认识加密勒索软件
- 加密勒索软件的演化趋势
- 思科安全如何防御加密勒索软件
- 最佳实践与建议
- 问题与讨论

# 勒索软件在不断演化

- 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、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。
- 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。

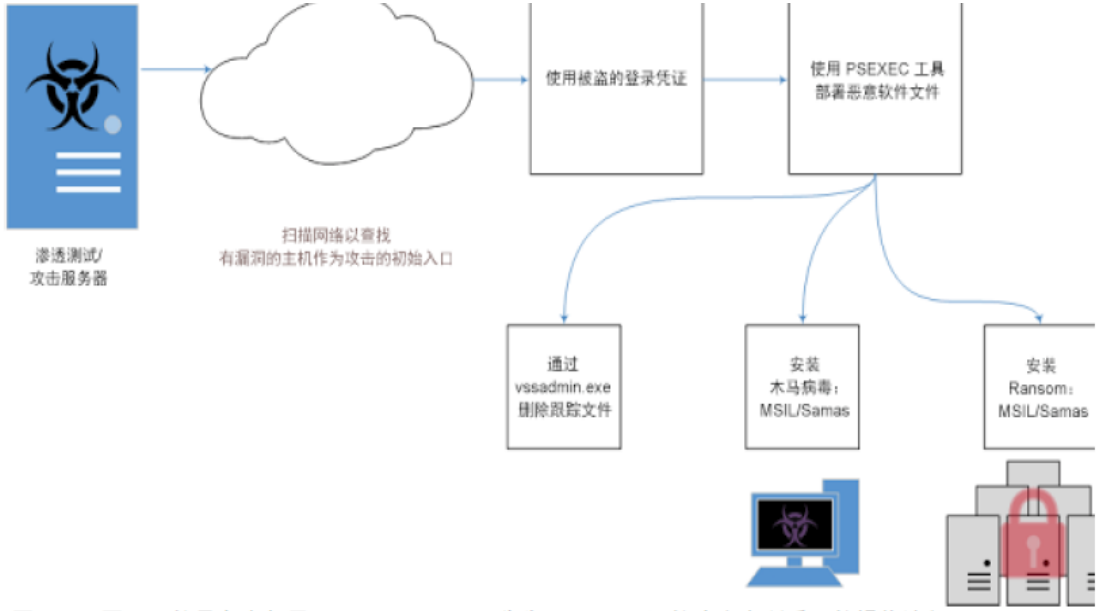



图 9：下图显示的是负责部署 MSIL/Samas（又称为“samsam”）的攻击者所采取的操作流程，

# 攻击目标转向企业用户-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。

# 勒索软件对企业的巨大危害

- 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，经济损失和社会压力导致加快了勒索时间，成为勒索软件的下一个主要目标。
- 医疗行业：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。
- 公共交通：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。
- 金融行业：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。
- 零售行业：影响交易系统的正常工作，消费者无法进行商品买卖，造成巨大经济损失。

# 议题

- 认识加密勒索软件
- 加密勒索软件的演化趋势
- 思科安全如何防御加密勒索软件
- 最佳实践与建议
- 问题与讨论

# 勒索软件的典型传播途径


用户点击恶意链接或者恶意广告

被Angler等恶意工具入侵

用户连接到黑客基础架构

用户被植入勒索软件

勒索软件更新密钥，加密文件

含有恶意附件的邮件

用户被植入勒索软件

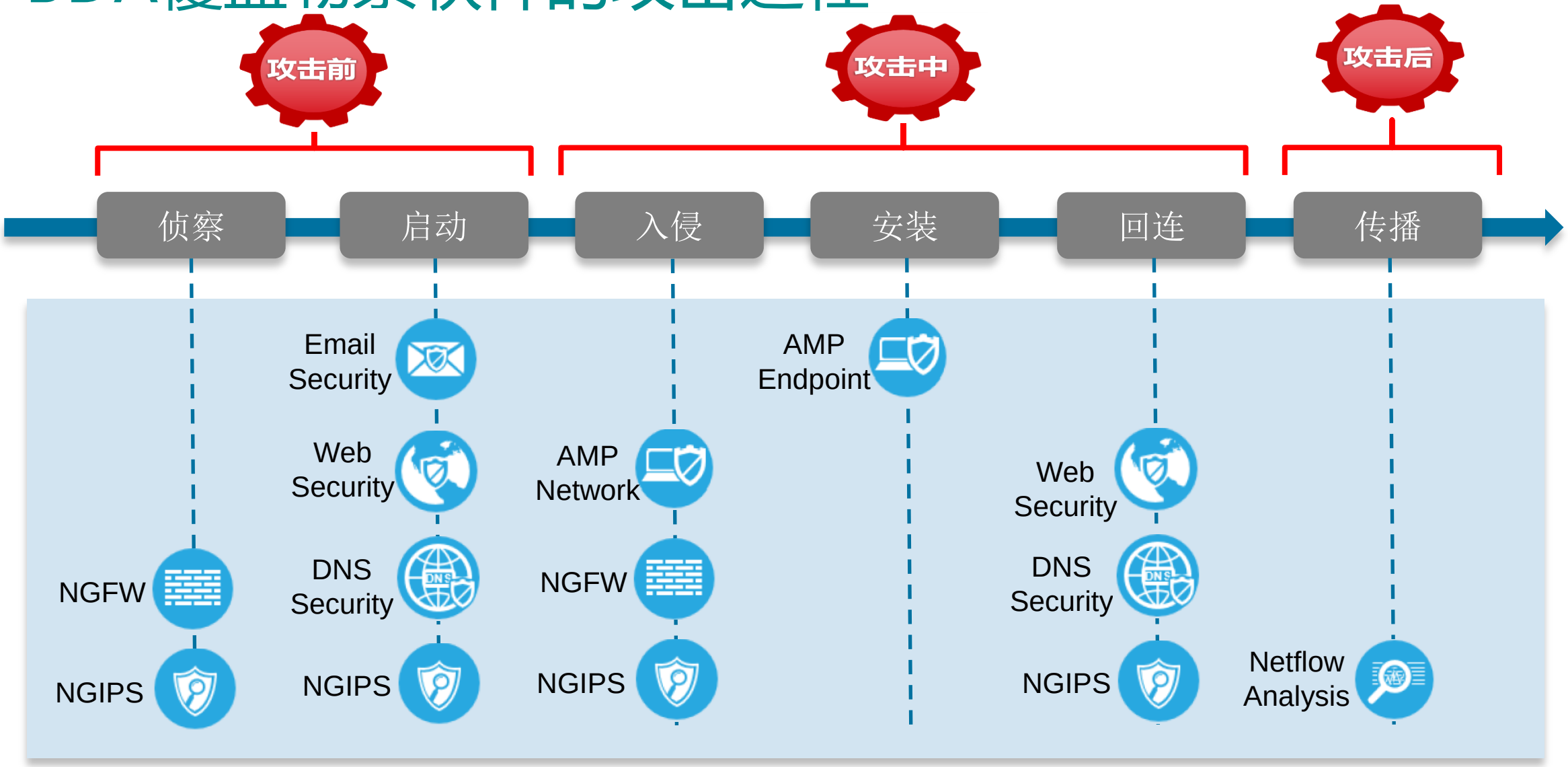
勒索软件更新密钥，加密文件

# 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


| 攻击前 | 攻击中 | 攻击后 |
| --- | --- | --- |
| 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 | 风险报告分析 |
| 自动化防御策略 | 联动策略告警 | 恶意代码的轨迹跟踪 |

# BDA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

识别用户到用户的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

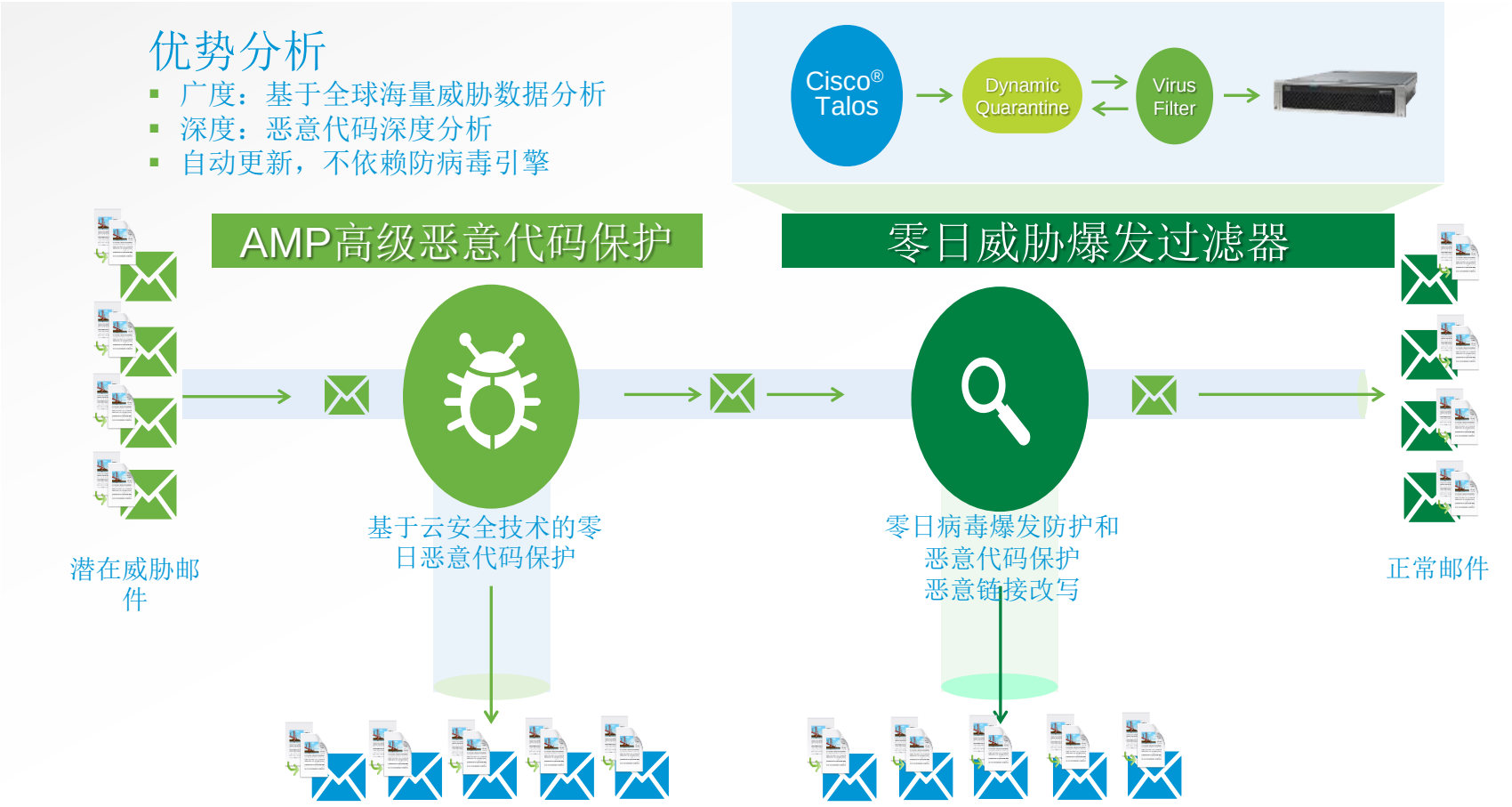
## StealthWatch(Lancope)

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

# 方案之一：ESA切断恶意邮件传播途径




- 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。

# 方案之一：切断恶意邮件传播途径-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 |

# 方案之二：NGFW/NGIPS阻挡恶意代码的植入

Firepower NGNW和NGIPS提供业界领先的威胁防御


- 检测并且阻挡针对内部主机的攻击，减少勒索软件被植入的可能性。
- 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。

# 方案之二：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：

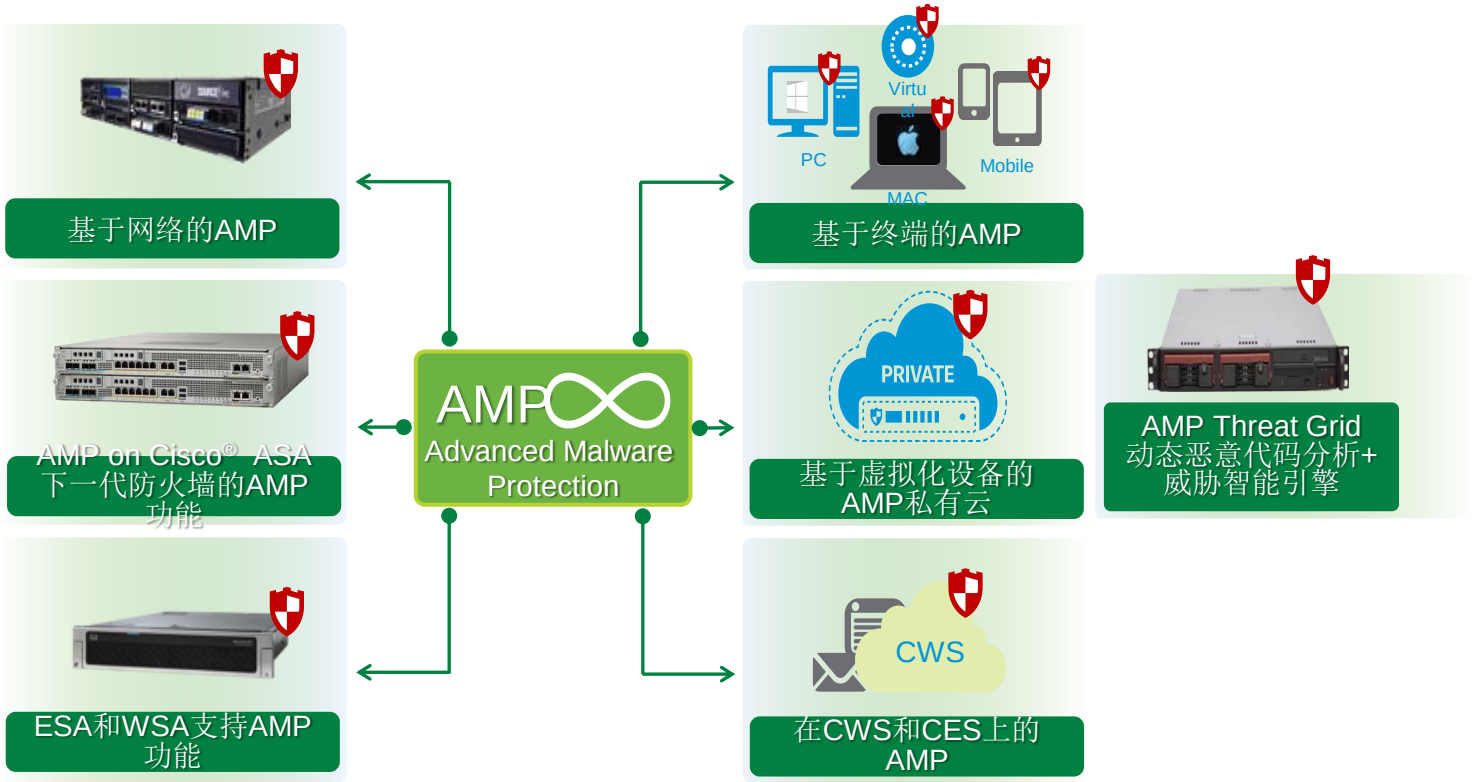
| Event Type | Event Subtype | Threat Name | File Name | File SHA256 |
|---|---|---|---|---|
| Threat Detected in Network File Transfer (Retrospective) | | W32.E5F66F6536.Locky.tht.Talos | | e5f66f65...63f55024 |
| Threat Detected in Network File Transfer (Retrospective) | | W32.E5F66F6536.Locky.tht.Talos | INVOICE_huangyang.zip | e5f66f65...63f55024 |
| Threat Detected in Network File Transfer (Retrospective) | | W32.E5F66F6536.Locky.tht.Talos | INVOICE_gulili.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_gulili.zip , INVOICE_huangyang.zip , INVOICE_zhengyi.zip (+1 more) |
| **File Type** | |
| **File Category** | |
| **Current Disposition** | Malware |

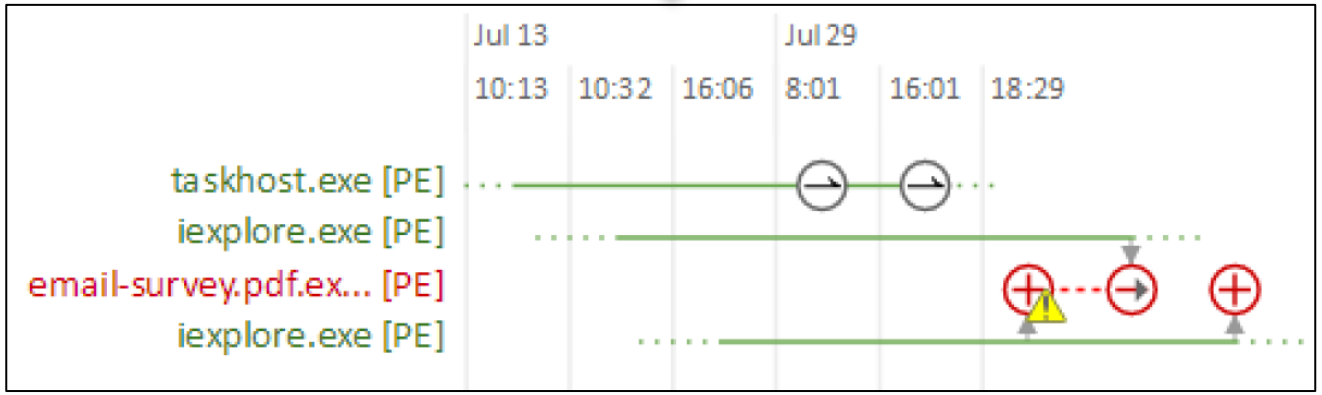
# 方案之三：AMP技术检测恶意代码




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

# 方案之三：AMP技术检测恶意代码-拦截记录

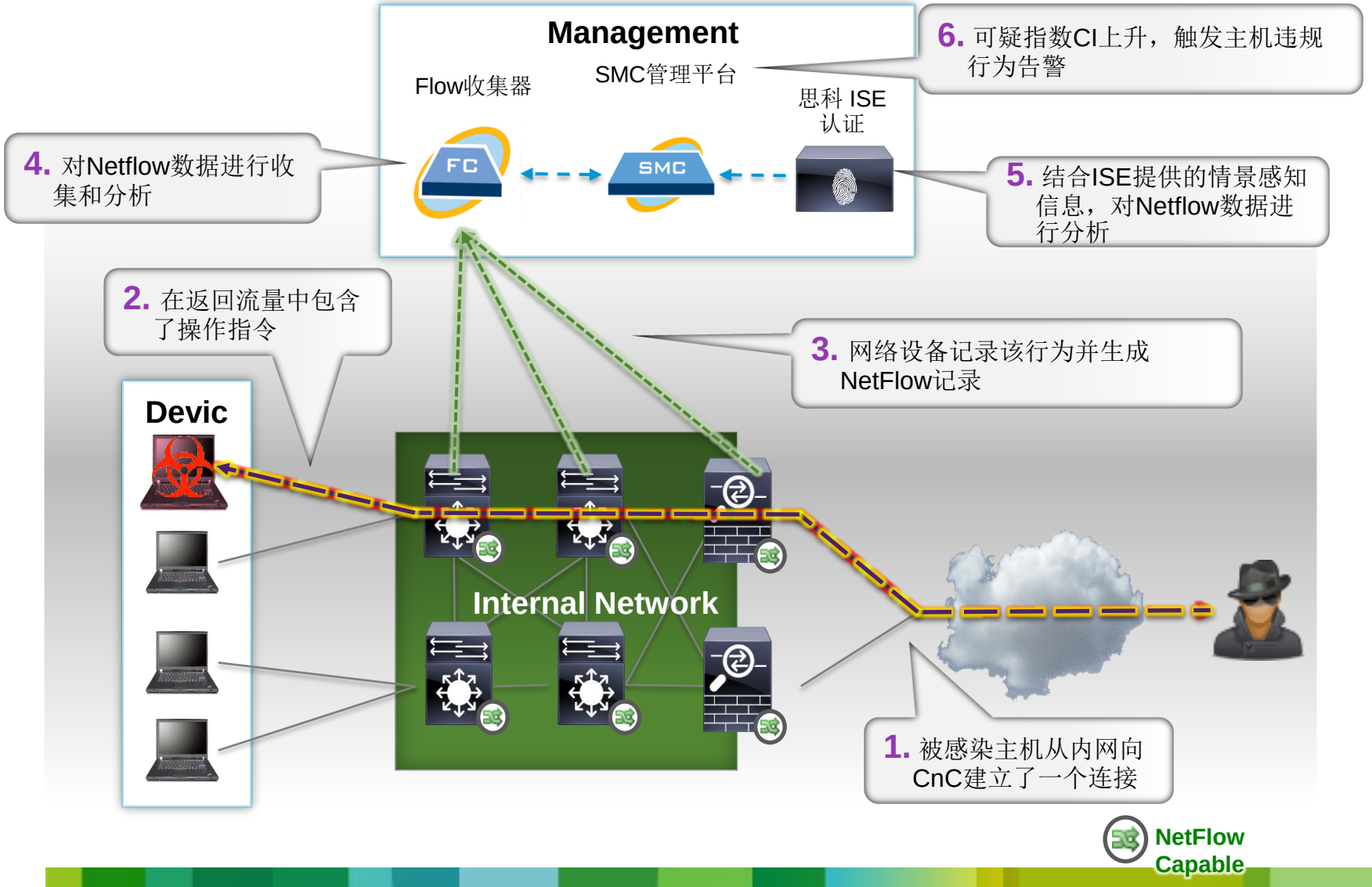




恶意文件轨迹跟踪

AMP记录恶意文件传播轨迹：

- 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。

# 方案之四：Stealthwatch检测终端异常连接




Stealthwatch对勒索软件的防御：

- 收集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异常访问，减少内部传播勒索软件的可能性
- 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。

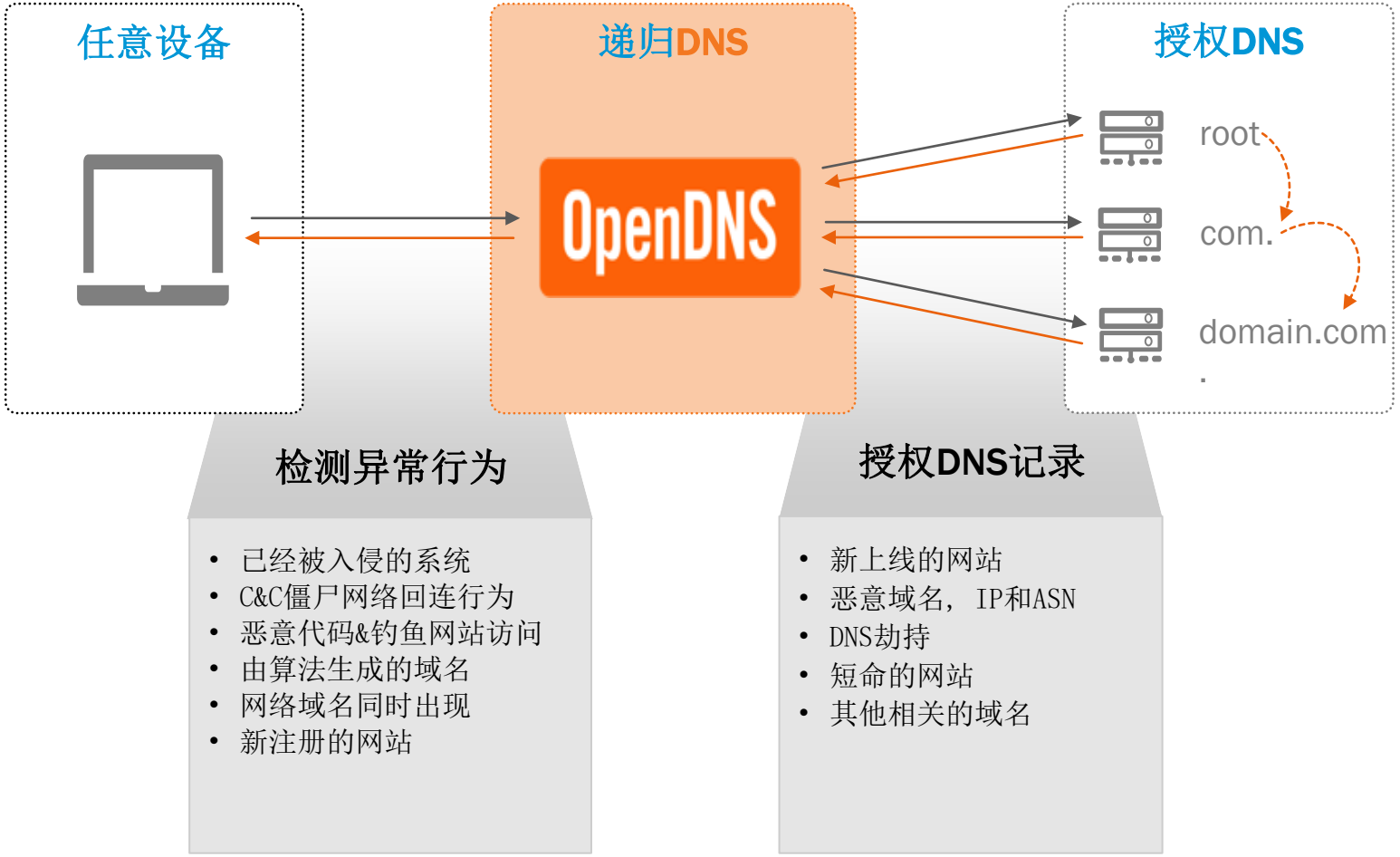
# 方案之五：WSA拦截钓鱼网站访问和恶意代码下载


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。

# 方案之六：OpenDNS切断恶意域名解析

OpenDNS通过DNS解析结果的智能分析切断访问C&C主机的行为



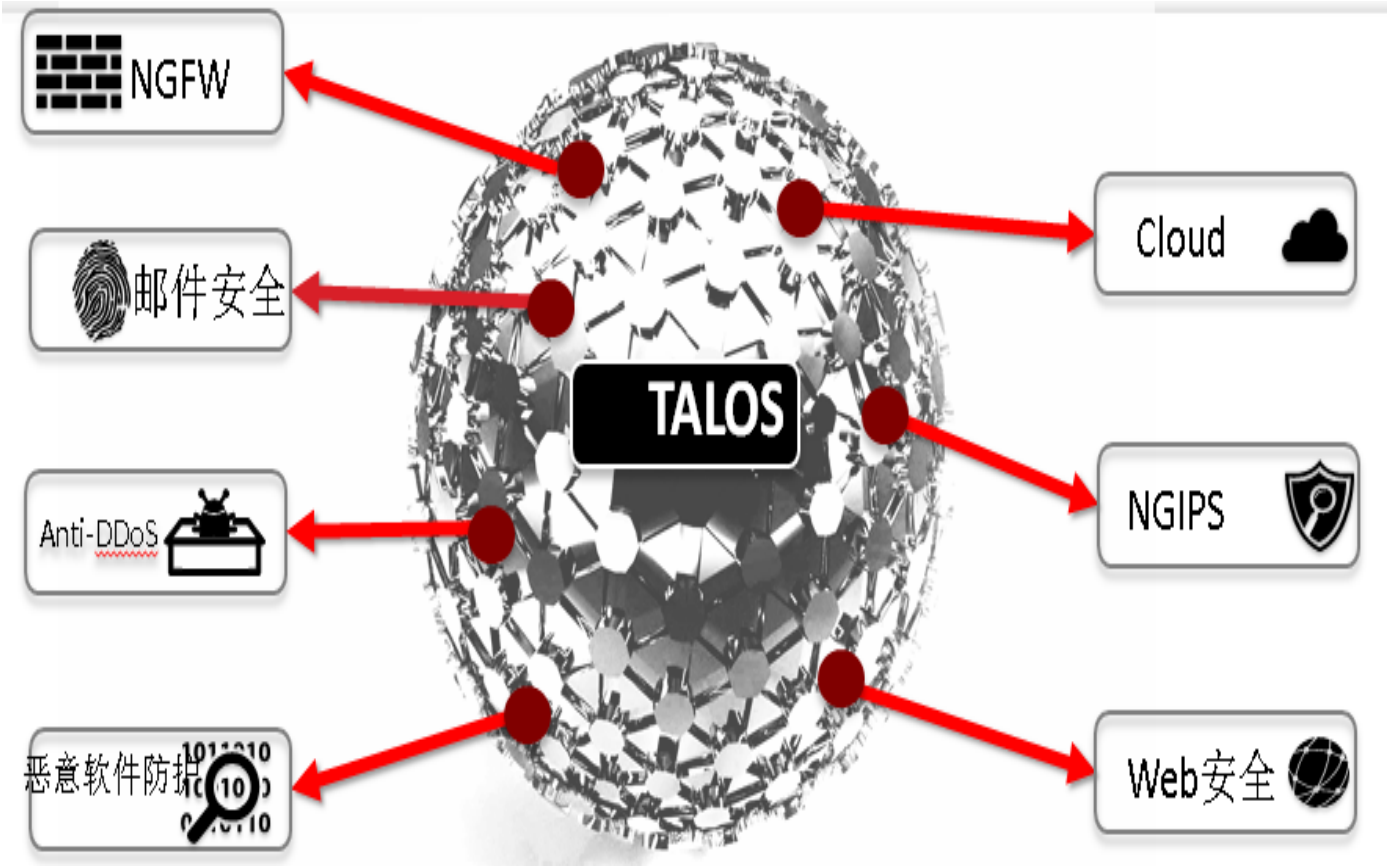

OpenDNS对勒索软件的防御：

- 分析DNS的解析结果，替换或更新恶意网站的IP地址记录
- 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

# 思科Talos情报中心提供实时威胁信息

TALOS是业界领先的安全情报中心

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



# 议题

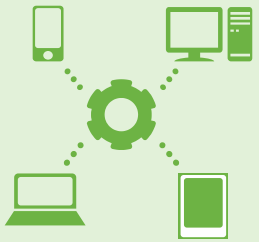
- 认识加密勒索软件
- 加密勒索软件的演化趋势
- 思科安全如何防御加密勒索软件
- 最佳实践与建议
- 问题与讨论

# 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。



URL重写

用户点击改写后的URL链接

**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**

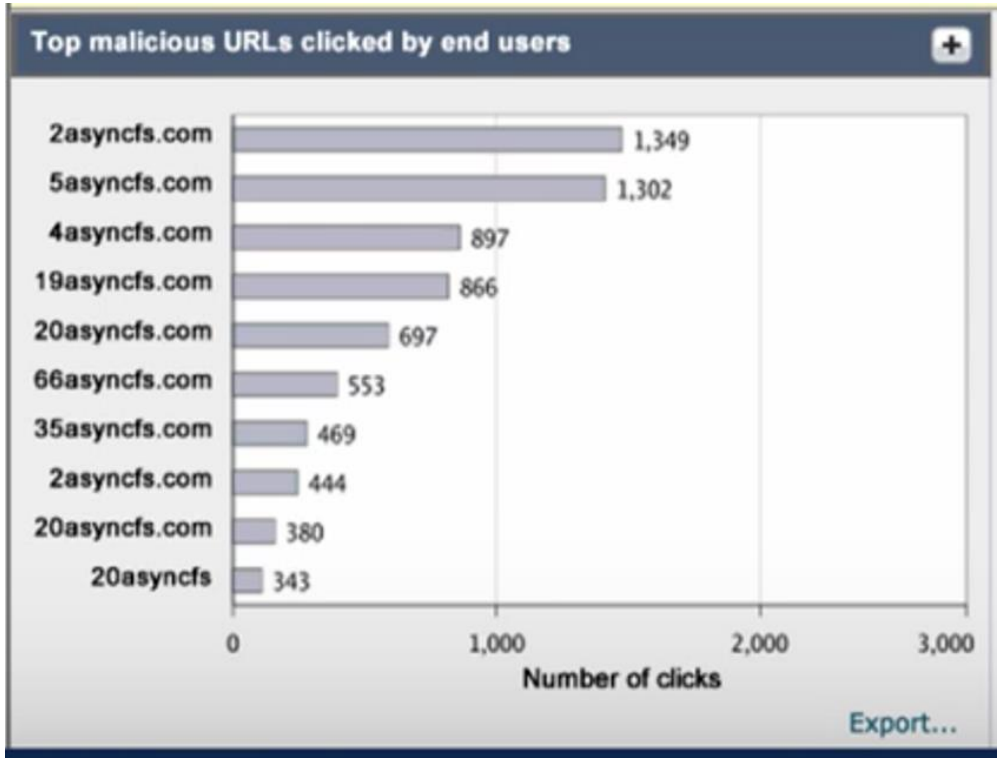
- 按照邮件ID统计
- 按照LDAP分组统计
- 按照IP地址统计

**将恶意URL或钓鱼链接加入到黑名单**

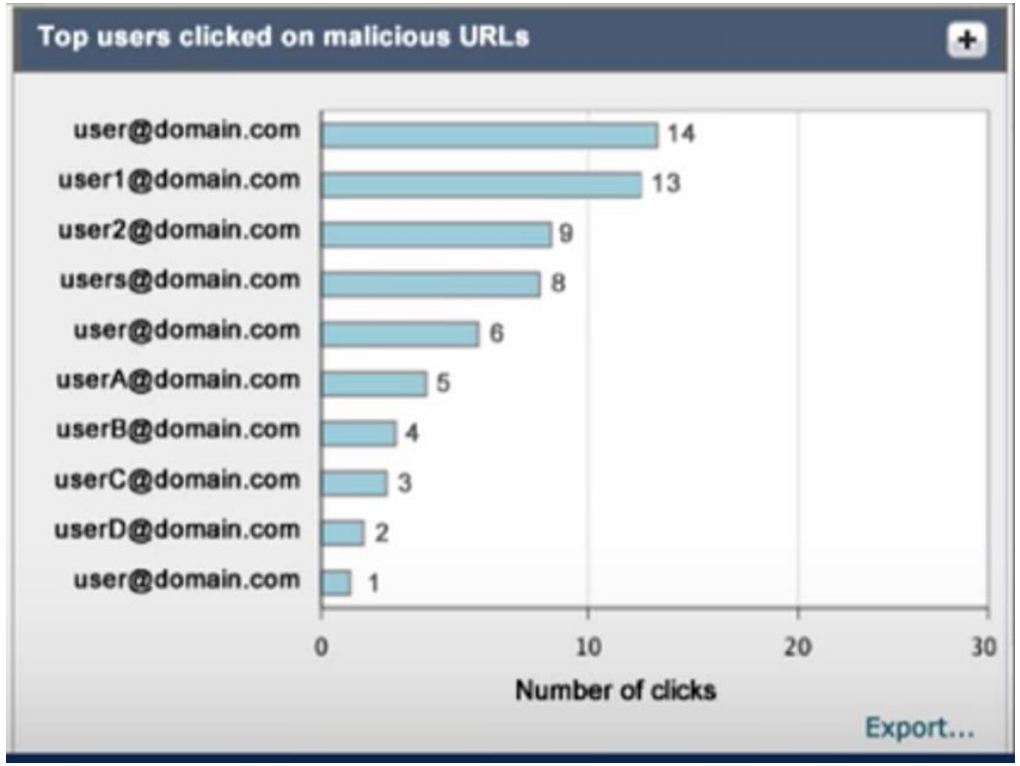
- 阻止零日攻击
- 动态智能
- 用户安全教育

# 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



# 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。
- 思科安全产品与解决方案，帮助可以从各个阶段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：勒索软件的过去、现在和将来
  - 设计指南：思科安全防御加密勒索软件的设计指南

Thank you.