Cisco电子邮件安全：了解上下文可适应扫描引擎(案件)

目录

[简介](#)
[了解案件，检测被混和的威胁在上下文](#)
[谁？](#)
[在哪里？](#)
[如何？](#)
[什么？](#)
[在操作的案件](#)
[高性能，低成本](#)
[摘要](#)

简介

在音量的增加被混和的威胁大量。许多最重大的病毒爆发在过去两年关联与垃圾邮件交付–含义病毒有效负载创建“使用发送垃圾邮件、网络钓鱼、间谍软件和更加病毒的僵死”计算机army –。电子邮件出生的间谍软件每六个月加倍，并且安装“窃取用户名和密码的keyloggers”发送消息到新闻组的URL是不不常见的。当Mydoom.B变量采取了上海合作组织的网站脱机与被协调的攻击，病毒可能均等用于创建僵死网络启动一次大量分布式服务拒绝攻击，例如。

什么驱动在被混和的威胁的突然的增加？简而言之，它是金钱。当第一代反垃圾邮件技术(类似黑名单和内容过滤器)广泛部署，传统方法(类似发送从包含一次“提供”在消息的文本的服务器一个已修复内存段的垃圾邮件)变得较没有益。使用更多网络使用反垃圾邮件技术，少量“简单”垃圾邮件消息做它通过垃圾邮件过滤器和成收件人的收件箱。这损害垃圾邮件发送者的边际利润和迫使他们适应这些更改。

垃圾邮件发送者处理了此情况用两种明显的方式：

1. 他们发送垃圾邮件以希望什么他们在交付速率丧失，他们在音量将组成。
2. 他们转向被混和的攻击假装他们的消息和增加他们的利润每个消息。

第二个技术经常变为犯罪活动。组织犯罪网络建立执行攻击和从病毒、网络钓鱼和其他威胁赢利。在2004年，个人名为John多弗在贩卖被拘捕了两百万个信用卡号以后，通过网络钓鱼攻击窃取。

用于被混和的攻击的技术也变得越来越复杂。Sober.N病毒被使用的电子邮件、Web下载、特洛伊人和僵死。传统内容分析过滤器是没有对手对于这些智能威胁。第一代反垃圾邮件过滤器的许多用户发现需要度过增加几小时“培训”他们的过滤器或写入新建的规则的他们。然而，尽管这些努力，他们的渔获率和吞吐量是拒绝的两个。结果是开销升级，当更多系统要求跟上负载，而更多管理时间用于管理每个系统。

Cisco电子邮件安全寻址与叫作上下文可适应扫描引擎的一个唯一被混和的威胁防御技术的这些威胁(案件)。Cisco电子邮件安全的案件技术用于终止传统垃圾邮件和复杂的基于僵死的攻击。此同样扫描技术也用于防止病毒和恶意软件多达在签名可用性前的42个小时–与效率的单个统一的扫描。

了解案件，检测被混和的威胁在上下文

第一代过滤器设计查看消息的内容和做确定。例如，如果“自由”的词在消息比两次出现更多，与草本的词一起“”它很可能是垃圾邮件。此方法是相对容易为了垃圾邮件发送者能击败通过使用隐藏的字符或编号而不是字母，例如“您的f0r y0u”在位置“”。第二代技术，类似贝叶斯过滤器，尝试通过区分垃圾邮件特性和自动地使电子邮件合法的学习寻址此限制。但是这些技术证明太挑战培训，太后起反应和太减慢扫描。

给先进的迷惑技术与今天垃圾邮件一起使用，科技目前进步水平过滤器在全双工上下文需要检查流入的邮件。案件使用模拟逻辑使用由人类评估消息的合法的先进的机器学习技术。一个人的读者，以及Cisco电子邮件安全的案件技术，询问四个基本问题：

1. 谁发送我消息？
2. 在消息的链路在哪里采取我？
3. 消息如何被修建了？
4. 消息包含什么？

要跟随是被评估的每个逻辑区域的考试。

谁？

作为陈述的前，第一代垃圾邮件过滤器主要在关键字检索取决于识别垃圾邮件。在2003年，介绍(IronPort)改革的电子邮件证券业Cisco名誉过滤的概念。当内容过滤询问问题时，“什么在消息？”，名誉过滤询问问题，“谁传送了信息？”。此简单，但是强大的概念扩展了威胁评估的上下文。在2005年之前，接近每个主要商业安全供应商采用某种名誉系统。

确定名誉介入检查关于一给的发送方的行为的一个清楚的数据集(发送方定义作为发送邮件)的IP地址。Cisco随着时间的推移考虑120个不同的参数，包括电子邮件音量，“垃圾邮件编号由此IP，原产地，主机是否被攻陷和许多设陷井”命中数。Cisco有开发并且维护算法，处理此数据生成名誉分数统计学家的团队。此名誉分数然后安排可用接收的Cisco电子邮件安全工具(ESA)，能然后节流根据他们的可信赖性的发送方。在短“spammy”发送方出现，越怠工。也过滤的名誉涉及问题关联与涌起的电子邮件音量由，在消息接受前，因而大量地改善邮件系统的性能和可用性的拒绝或限制的连接。Cisco ESA名誉过滤器近似两次终止超过流入垃圾邮件的80百分比，竞争的系统渔获率。

在哪里？

当电子邮件内容分析和名誉的组合在2003年时是科技目前进步水平，垃圾邮件发送者的和病毒作家的战术的优雅继续增长。合情合理Cisco (IronPort)介绍Web名誉的饰物–一关键新建的矢量扩展消息被评估的上下文。类似于用于计算电子邮件的名誉的方法， Cisco Web名誉查看超过45个服务器相关参数估计所有给的URL的名誉。参数随着时间的推移包括音量HTTP请求对URL， URL是否在与一个恶劣的名誉分数的一个IP地址主机，此URL是否关联与已知“僵死”或被感染的PC主机和URL使用的域的年龄。使用一个粒状分数，如同电子邮件名誉，此Web名誉被测量，允许系统处理复杂的威胁二义性。

如何？

对Cisco电子邮件安全的上下文分析的另一种新方法将检查消息的建筑。使用MIME编码、HTML，或者其他相似的平均值，合法邮件客户端，例如Microsoft Outlook，修建消息用唯一方式–。消息的建筑的考试能非常显示关于其合法。当垃圾邮件服务器设法模拟一个合法邮件客户端的建筑，一告诉此的示例发生。这是很难执行，并且不完美的仿真是一个非法消息的一台可靠指示器。

什么？

一充分的上下文分析需要考虑消息的内容，但是，如注释前，单独的内容分析不是一满足的方法对识别非法邮件。使用科技目前进步水平机器学习技术， Cisco电子邮件安全的案件技术执行全部内容分析。这些技术检查消息的内容并且计分它以多种类别–是否是财务的，色情，或者是否包含知道关联与其他垃圾邮件的内容？此内容分析析因到案件与其他属性一起–，其中，如何，并且什么–评估消息的全双工上下文。

在操作的案件

由于案件分析的数据广度，技术用于各种各样的安全应用程序–包括IronPort反垃圾邮件(IPAS)，Graymail和病毒爆发过滤器(VOF)。示例下面的优点案件如何用于终止垃圾邮件。消息内容是几乎完全相同的对获得的组织phished，因此消息的内容分析不会识别任何威胁。到基于内容的过滤器，此消息看来是一合法通信。确定此消息是否是垃圾邮件，依靠主要“的过滤器什么”可能容易地被唬弄到认可消息如合法。然而，消息的全双工上下文的分析绘一幅不同的画。

- 发送的邮件服务器的IP地址是可疑的–在音量有一突然的电涌，并且域，反回，不接受邮件。
- 电子邮件的URL指向看来在用户宽带网络的服务器。
- 在消息通告的URL是与“实际” URL不同用户导航对，当单击在链路时。

当全部三这些要素在上下文时设想，变得清晰，这不是一个合法消息，但是，实际上，垃圾邮件攻击。

传统“内容过滤器”
什么内容过滤器查找

什么？ 合法的消息内容。



判决：未知

上下文可适应扫描
什么案件查找

什么？合法的消息内容。
如何？消息建筑模拟Microsoft Outlook客户端。
谁？
1)在发送的音量的一突然的电涌电子邮件。
2) 反回，邮件服务器不接受邮件。
3) 在乌克兰查找的邮件服务器。

在哪里？
1)在显示&目标URL网站域之间的上午ismatch注册
天前。
2)在用户宽带网络主机的网站。
3) “Whois”数据显示域所有者作为已知垃圾邮件发
。

判决：块

当案件用于病毒爆发过滤器时，虽然同样计分和计算机学习能力应用–对一个分开被调整的数据集。病毒爆发过滤器是案件技术提供由Cisco和供给动力的一预防抗病毒解决方案。爆发过滤解决方案扫瞄消息“实时”爆发规则(发出由Cisco Talos特定爆发)和“不间断工作的”可适应规则(一直请驻留在案件)，保护用户爆发，在他们有一个机会充分地前形成。案件使病毒爆发过滤器准确地检测和防止受到病毒爆发用几个方式。首先，案件能迅速扫描根据参数的消息例如附件、文件大小、文件名、文件

名关键字、文件魔术(实际分机文件)和被嵌入的URL文件扩展。由于案件技术分析消息对此详细程度， Cisco Talos能发出非常粒状爆发规则，准确地防止受到与最小错误肯定的爆发。案件能动态地接收更新爆发规则，保证防止受到最新的爆发。

除根据爆发规则的消息之外分析，案件技术也扫描根据可适应规则的消息。检查畸形的传入消息和伪装特性预示病毒的可适应规则是细致被调整的推断和算法。除这些参数之外，根据他们的SenderBase病毒分数的可适应规则分数消息(SBVS)。SBVS是分数类似于SenderBase名誉分数(SBRS)，但是与根据可能性的等级发送的当事人发送病毒电子邮件，而不是垃圾邮件。大多数病毒电子邮件由以前被传染的“僵死”机器发送，因此识别和计分这些发送的当事人是在传染性的病毒的一个重要要素。

因为案件检查在多种方式的消息Cisco电子邮件安全的案件技术使病毒爆发过滤器终止病毒爆发在传统抗病毒解决方案之前。它有能力分析消息附件许多特性、消息内容和消息建筑，以及能力分析根据他们的发送方名誉的消息。并且，因为案件也作为IronPort反垃圾邮件和名誉过滤器引擎，仅消息需要永远被扫描这些应用程序。

高性能，低成本

在案件技术后的逻辑能是非常复杂的，并且非常强化中央处理处理。要最大化效率，案件使用一个唯一“早期的退出”技术。早期的退出优先安排案件处理的无数的规则的效力。案件技术运行规则以最高冲击和最便宜第一。如果一个统计判决作出(是否正或负)，另外的规则没有运行，保存系统资源。在此方法的高雅有一好了解每个规则效力。自动地装入监视器并且适应规则执行顺序，效力更改。

早期的退出结果是案件技术比一个传统基于规则的过滤器处理消息大约100百分比快速。这有大ISP和企业的明显的优点。但是它也有中小企业的好处。案件效率，加上Cisco电子邮件安全的AsyncOS操作系统的效果，意味着与AsyncOS和案件技术的ESAs在非常便宜的硬件可以实现–压低资本费用。

另一个方式技术翻译对低成本的案件是通过排除管理开销。盒自动地被调整并且每天更新，千位时期。Cisco Talos提供被培训的工程师，多语种技术人员和统计学家。Cisco Talos分析师有突出显示在所有Cisco电子邮件安全客户网络检测的邮件流量的反常现象的特殊的工具，或者全局电子邮件流量模式。Cisco Talos生成在实时自动地推送到系统的新的规则。Cisco Talos也维护“垃圾邮件和火腿一个大量语科库”，用培训案件使用的多种规则。自动地更新的案件规则意味着不必须是调整和调整过滤器或花费时间趟过通过垃圾邮件检疫的管理员。

摘要

同一个基础动机驱动垃圾邮件、病毒、恶意软件、间谍软件、拒绝服务攻击和目录收获攻击全部–利润。这些利润通过商品信息销售或广播或盗窃获得。从这些销售的利润越来越驱动诡辩的攻击，开发由专业工程师。先进的电子邮件安全系统在最清楚的可能的上下文需要分析一个消息抵抗这些威胁。Cisco电子邮件安全的上下文可适应扫描引擎技术询问四个基本问题：谁，其中，什么和如何清除从被混和的威胁的合法消息。

- “谁”是发送方的电子邮件名誉–谁传送了信息。
- “”是主机网站的来源的名誉–分析的地方链路将采取您的地方。
- “什么”是消息的内容的分析–什么消息包含(经常第一代系统请独自地取决于在”什么”分析的类型)。
- 最后， “如何”是分析消息如何被修建。

此基本框架分析谁，其中，什么和同样好地工作对于终止垃圾邮件，为防止病毒爆发执行，网络钓

鱼如何攻击，电子邮件出生的间谍软件或者其他电子邮件威胁。数据集和分析规则集为每个威胁特别地被调整。案件技术允许Cisco ESA通过处理在单个高性能的引擎的这些威胁终止威胁宽广的范围以最高效率。