2011 年 6 月

邮件攻击：这次的问题是个性化

执行摘要

近来，网络犯罪的商业模式已经开始向低攻击量但有针对性的攻击模式转变。这类攻击仍以邮件为首要攻击媒介，但攻击频率及其对目标组织的经济影响均有所提升。思科安全智能运营中心（SIO）的研究发现，源自大规模无差别邮件攻击的网络犯罪业务活动年均减少了一半以上。与此同时，源自高度个性化的针对性攻击的业务活动量正在快速增长，甚至在去年增至原来的三倍。除了受到的经济影响将导致资金损失和凭证遭窃外，受此类攻击危害的组织还必须承担补救受感染主机的费用，以及对其品牌声誉产生的负面影响。

此类攻击的越发盛行，加上移动性和不受控终端的发展趋势，无一不要求今天的组织实施一种能够利用网络保障安全的新方法。虽然许多组织都会培训用户辨别危险邮件和避免点击可能引至不安全网站或下载恶意软件的 URL，但用户培训并不能完全使企业免受这些威胁。组织需要的其实是一种高度分布式的安全架构，能够使用具有情景感知能力的高级策略语言来管理防火墙、网络代理和入侵防御传感器等实施要素。

本文的目的就是研究攻击发展趋势和探讨此类攻击活动的影响。本文中的调查结果均基于思科同全球各行各业组织共同开展的研究。

网络犯罪业务：邮件的角色

去年，网络犯罪业务模式的转变导致威胁活动发生了显著的变化。大规模攻击有所减少，从垃圾邮件总量下降了 80% 便可见一斑。取而代之的是，网络犯罪分子正越来越专注于更高附加值的活动，包括越来越多的诈骗攻击和恶意攻击、鱼叉式网络钓鱼攻击和针对性攻击。

大规模攻击的减少

随着越来越多的网络犯罪分子转而使用针对性攻击，Cisco SIO 估算，通过传统大规模邮件攻击攫取的网络犯罪年收益降低了 50% 以上：从 2010 年 6 月的 11 亿美元降低到 2011 年 6 月的 5 亿美元。这一变化也体现在垃圾邮件日均数量的减少，从 2010 年 6 月的 3000 亿封减少到 2011 年 6 月的 400 亿封。

这种数量上的减少与持续用户转化率较低的情况相符，并且因用于用户转化的平均支出的提高而略有抵消。

这种减少也因诈骗和恶意攻击而有所抵消，这是大规模攻击中一个小的子类别，只占大规模攻击总量的 0.2% 左右，但由此攫取的网络犯罪收益却较高。通过使用更多的个性化工具，精心设计的诈骗和恶意攻击的用户转化率在去年显著提高。此外，由于信息共享，恶意软件或所采用的诈骗攻击所造成的用户平均损失有所增加。

在估算总损失时（见表 1），Cisco SIO 按每个受害组织用户损失 250 美元的保守估计进行计算。此金额与最近公开披露的诈骗和恶意攻击估算值的较低值相符。例如，2011 年 6 月，美国联邦调查局（FBI）曾公布过一种诈骗邮件，声称收件人需交付 350 美元以获得结清证明，否则将面临法律制裁。按这种估算值计算，诈骗和恶意攻击（大规模攻击中的一个子类别）获得的年均不法收益在过去一年已经从 5000 万美元增长到 2 亿美元。

表 1：通过大规模攻击攫取的网络犯罪收益

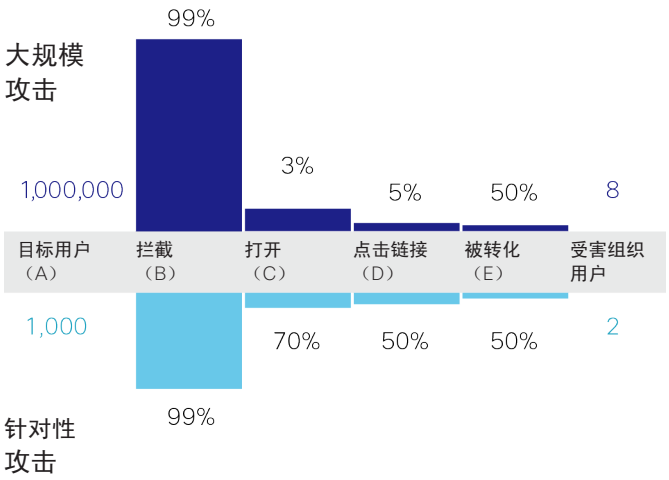
网络犯罪收益（百万美元）	1 年前	目前
垃圾邮件攻击	1,000 美元	300 美元
诈骗和恶意攻击	50 美元	200 美元
总计	1,050 美元	500 美元

从 2010 年开始到 2011 年，犯罪生态系统一直在发生翻天覆地的变化。全球的执法机构及安全和行业组织展开合作，关闭或限制了最大规模的垃圾邮件发送僵尸网络及相关威胁的活动。大型垃圾邮件发送联盟网络 SpamIt，就是在 2010 年 10 月其数据库泄露，并且俄罗斯警方对其所有者提起控诉后，停止了运营。主要僵尸网络的力量被大幅削减，有的甚至被关闭，其中包括 Rustock、Bredolab 以及 Mega-D。由于主要同业联盟的经济和技术业务模式被瓦解，威胁活动数量有所下降，转向获利更多的活动。

我们来简单了解下大规模攻击和针对性攻击在转化过程和业务模式方面的差异。

过去，垃圾邮件的转化渠道是先收集一系列邮件地址，相关僵尸网络将利用这些地址发送邮件（请参阅图 1 中的阶段 A）。收到邮件后，反垃圾邮件引擎会正确识别和拦截绝大多数的威胁邮件（阶段 B）。通过了垃圾邮件过滤器的邮件将被视为合法的邮件，最终进入用户的邮箱。具备相关知识的用户通常会忽略垃圾邮件，只会打开其中一小部分（阶段 C）。在这之中，只有很少一部分用户会点击邮件中的链接（阶段 D）并最终被“转化”（阶段 E），毫无戒心的用户才会购买产品或下载恶意软件。

图 1：威胁转化渠道



这种传统垃圾邮件渠道仍然存在，但随着个性化程度的不断提高，它也在发生变化，在针对性攻击中表现最为明显。在整个渠道中，针对性攻击通常存活率更高，因为邮件和网站链接会被发送到有效用户，而且面向安全引擎和收件人均表现得像合法邮件。尽管攻击量较低，但针对性攻击的转化率要高出很多。提高转化率的代价则是更多的投入，例如：

- 列表中仅包含具有指定属性的有效邮件地址
- 让邮件表面看起来合法，通常伪装成来自认识的联系人，且内容对于收件人有针对性
- 使用质量更高且通常尚未被发现的恶意软件
- 往往专门为某一种针对性攻击实例建立新网站（此前未见过）

这是犯罪进化论在作祟：网络犯罪分子保持其活动与时俱进，以便提高自己的持久力。

攻击分类

随着网络犯罪活动的不断进化，各种攻击及其对组织的影响也在相应发生变化。

大规模攻击

自分布式网络形成以来，大规模攻击一直是各种威胁的基础。自我传播式蠕虫、分布式拒绝服务（DdoS）攻击和垃圾邮件均为实现经济利益或业务干扰的惯用方法。不法分子会创建常见的有效负载并将其置于受害者一不留神便会访问的位置。例如：感染网站、以 PDF 等文件格式利用安全漏洞、发送邮件骗取用户购买，以及批量钓鱼银行证书。

传统的防威胁方法依赖于几个因素，包括在网络中首次发现威胁或收到报告后快速进行识别，并且在日后拦截类似的威胁。如果不法分子渗透到足以达到他们目标的安全层深度，他们将会得到预期的结果，足以让此业务模式有利可图。

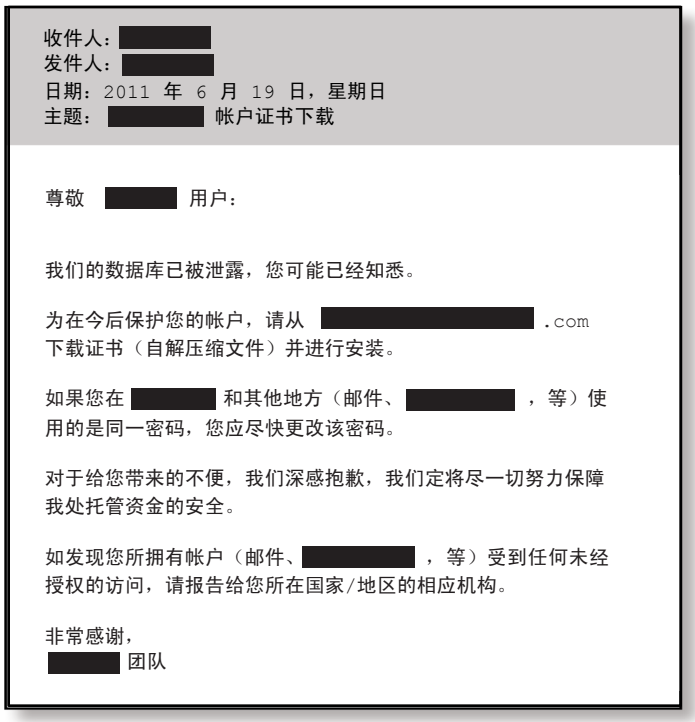
此类攻击中很大一部分是迅速增多的诈骗和恶意攻击。作为犯罪生态系统演进的一部分，这些攻击的针对性越来越高。短信服务（SMS）、电子邮件、社交媒体，无论使用的是哪种媒介或传送引擎，不法分子都会使用用户的地理位置或职位等个性化信息更谨慎地选择自己的攻击目标。此类诈骗攻击的示例包括：

- 发往具体区域位置的 SMS 金融诈骗攻击
- 使用 URL 缩短服务的营销邮件诈骗
- 不法分子伪装成用户或用户组友人以攫取经济利益的社交媒体诈骗

如果只发送少量攻击威胁，这些策略可能会有效地危及受害者，但对于不法分子而言并不总是具成本效益。然而，为了能骗取高价值受害者，这种方法正日益受到有头脑、有组织、唯利是图的不法分子的青睐。如果不法分子的攻击是专门针对受害者的简档，那么这些威胁便称为鱼叉式网络钓鱼攻击。

鱼叉式网络钓鱼攻击针对的是特定的用户简档，通常以有权访问商业银行帐户的高级组织用户为攻击目标。鱼叉式网络钓鱼攻击通常经过精心设计，使用真实情景信息使用户相信与其进行交互的是合法内容。鱼叉式网络钓鱼邮件的内容可能是有关个人的重要事项或有关公司的相关事宜，例如，讨论薪酬差异或法律问题。根据 Cisco SIO 的研究，80% 以上的鱼叉式网络钓鱼攻击都包含指向含有恶意内容的网站的链接。但是，链接的网站通常经过特殊设计且之前从未见过，因此很难检测出来。

图 2：鱼叉式网络钓鱼邮件


收件人：[redacted]
发件人：[redacted]
日期：2011 年 6 月 19 日，星期日
主题：[redacted] 帐户证书下载

尊敬 [redacted] 用户：

我们的数据库已被泄露，您可能已经知悉。

为在今后保护您的帐户，请从 [redacted] .com 下载证书（自解压缩文件）并进行安装。

如果您在 [redacted] 和其他地方（邮件、[redacted] ，等）使用的是同一密码，您应尽快更改该密码。

对于给您带来的不便，我们深感抱歉，我们定将尽一切努力保障我处托管资金的安全。

如发现您所拥有帐户（邮件、[redacted] ，等）受到任何未经授权的访问，请报告给您所在国家/地区的相应机构。

非常感谢，
[redacted] 团队

针对性攻击

针对性攻击属于高度定制化的威胁，针对特定用户或用户组，通常是为了盗用知识产权。这些攻击的数量极少，并且可以通过帐户信息无意中泄露的熟知实体或专业僵尸网络传播渠道中的匿名身份进行伪装。针对性攻击通常使用某种形式的恶意软件，而且通常使用零日漏洞攻击，以便在第一时间侵入系统，在一段时间内收集到所需数据。在此类攻击中，不法分子通常使用多种方法接近受害者。针对性攻击很难防范，并且很可能对受害者产生最严重的负面影响。

尽管结构上可能类似，但针对性攻击相较鱼叉式网络钓鱼攻击，最大的不同在于对骗取对象的关注度。针对性攻击锁定的是特定用户或用户组，而鱼叉式网络钓鱼攻击通常锁定的是具有共同点的一群人，例如同一家银行的客户。针对性攻击者通常会针对目标人群建立一份档案，从社交网络、新闻稿和上市公司通讯信函中收集信息。鱼叉式网络钓鱼攻击可能包含一部分个性化信息，而针对性攻击则可能包含大量高度个性化的信息，而且通常对于锁定目标具有独特的吸引力。

表 2：针对性攻击与鱼叉式网络钓鱼攻击之间的比较

属性	针对性攻击	鱼叉式网络钓鱼攻击
意图	知识产权盗用	经济利益
恶意软件	使用，通常通过零日漏洞攻击	可能使用
目标侦察	是	否
个性化程度	极高	中等

Stuxnet 攻击是为公众所熟知的一种针对性攻击，它是于 2010 年 7 月发现的一种计算机蠕虫病毒，专门针对工业软件和设备。Stuxnet 以 Windows 处理快捷方式文件的方法进行漏洞攻击，从而使蠕虫传播到新系统中。这种蠕虫被认为是目的性非常强的一种病毒，专门攻击监控和数据采集（SCADA）系统，或者攻击用于管理复杂工业网络的系统，如发电站和化工生产工厂中的系统。Stuxnet 的聪明之处在于能够穿越非联网系统，也就是说，甚至连未连接到网络或互联网的系统都会面临风险。操作人员认为供应商无法在不为客户带来任何重大麻烦的前提下更改默认的 Siemens 密码（多年前已在网络上公开）。SCADA 系统操作人员可能一直处于一种错误的安全感之下，因为他们的系统并未连接到公共互联网，所以他们可能认为自己不易受到感染。联邦新闻广播的网站称 Stuxnet 为“史上最聪明的恶意软件”。

2011 年 1 月，Cisco SIO 侦测到一份发送给一家大型公司高管的针对性攻击邮件。此次攻击活动非常复杂，因为它使用了之前未见到过的资源。邮件由一个未知方通过位于澳大利亚的一台合法但已受感染的服务器发送。该邮件看似合法（图 3）。嵌入的行动链接托管在一个合法但已受感染的法律博客上。点击链接时，用户的浏览器将转到之前未知的一个 Phoenix 漏洞攻击工具副本。漏洞攻击成功后，会在受害者的计算机上安装宙斯木马。

图 3：针对性攻击邮件

发件人：[redacted]
日期：2011 年 1 月 19 日，星期三
收件人：[redacted]
主题：商业诉讼传票

我们通过本信函特此通知您 [redacted] 营销有限责任公司提起了针对您所代表公司的诉讼程序。您需要根据本“传票安排”中列出的说明，准备完全对应或部分对应的所有文档和其他项目的原件（无论原件位于何处，是由您所有、保管或控制，还是由您的合作伙伴、同事、员工、代理人、代表、会计人员或律师所有、保管或控制），还需准备因任何部分（包括背面）存在添加、删除、更改、注释或题词而与原件不同的文档的所有复印件。

所需文档的完整列表位于：
http://www.officialarticles.com/subpoena_files/

其中还包括营销有限责任公司的法律代表于 2010 年 12 月 21 日针对贵公司 [redacted] 侵犯版权行为的申诉编号。如果未能准备和呈交所需文件，您将面临法庭的罚款。

[redacted]
高级律师
[redacted] 法律事务所

攻击的经济效益

从典型活动的经济效益，我们可以看出大规模攻击与针对性攻击业务模式之间的差异。为了展示这种差异，表 3 利用大规模钓鱼攻击与鱼叉式网络钓鱼攻击的示例，对转化渠道中的产出及网络犯罪的相对经济效益进行了比较：

表 3： 大规模钓鱼攻击与 鱼叉式网络钓鱼攻击

典型攻击活动示例	大规模钓鱼攻击（单次活动）	鱼叉式网络钓鱼攻击（单次活动）
（A）攻击活动中发送的邮件总数	1,000,000	1,000
（B）拦截率	99%	99%
（C）打开率	3%	70%
（D）点击率	5%	50%
（E）转化率	50%	50%
受害者	**8**	**2**
从每个受害者处攫取的收益	2,000 美元	80,000 美元
从攻击活动中获得的总收益	**16,000 美元**	**160,000 美元**
攻击活动的总成本	2,000 美元	10,000 美元
从攻击活动中获得的总利润	**14,000 美元**	**150,000 美元**

对单次攻击活动，鱼叉式网络钓鱼攻击的经济效益比大规模攻击更明显。成本相对高很多，但是产出和收益也同样高很多。Cisco SIO 估计，考虑到所需的目标清单的质量、租赁的僵尸网络、邮件生成工具、购买的恶意软件、创建的网站、攻击活动管理工具、订单处理后端基础设施、订单履行提供商和用户背景调查活动，鱼叉式网络钓鱼攻击的成本是大规模攻击成本的五倍。如此高昂的成本基数和大量的工作都需要高度专业化的技能。还需要较高的产出率来保证成本效益。

网络犯罪分子也在平衡相互冲突的优先项：是感染更多用户还是让攻击数量少到足以躲过安全供应商的检测雷达？ 鱼叉式网络钓鱼攻击活动在数量上非常有限，但用户打开和点击率却较高。由于存在这些限制，网络犯罪分子越来越看重拥有企业银行帐户访问权限的企业用户，确保每次感染均能得到足够的回报。这就是为什么从每个受害者处攫取的收益平均值能够达到大规模攻击的 40 倍。综合来看，使用此方法合情合理：从单次鱼叉式网络钓鱼攻击活动中获得的利润能够达到大规模攻击的 10 倍以上。

这种潜在的回报导致网络犯罪业务模式发生了转变。目前，由于反垃圾邮件效力和用户认识的提升，回报率可能不足以负担垃圾邮件攻击的机会成本。取而代之的是，网络犯罪分子将更多的时间和精力放在了不同类型的针对性攻击上，其目的通常是获取更有利可图的公司和个人银行帐户以及有价值的知识产权。

为使自己的攻击更具个性化，某些网络犯罪分子专门入侵邮件营销供应商的网络，因为他们拥有有效的姓名、邮件地址以及其他属性信息。用在诈骗攻击和恶意攻击中时，无论是大规模攻击还是鱼叉式网络钓鱼攻击，此类个性化信息都会提高用户打开攻击邮件的可能性。

较小规模垃圾邮件攻击与最近的数据外泄之间的关系非常微妙，但从中得出的真正要点是如今的攻击正在变得越来越个性化。

个性化攻击的影响

鱼叉式网络钓鱼攻击的影响

尽管相对于其他类型的威胁，鱼叉式网络钓鱼攻击在数量上较少，但它会给当今企业造成非常严重的后果。大多数鱼叉式网络钓鱼攻击最终都会导致经济损失，对于受害者来说非常危险，而对于网络犯罪分子来说则非常有利可图。

鱼叉式网络钓鱼使用的定制化方法比大规模诈骗攻击和恶意攻击使用的方法更胜一筹，因此用户打开率和转化率都要高得多。这些成功因素使鱼叉式网络钓鱼攻击感染的效率得以提升，因此使用更加普遍，经联邦贸易委员会证实，每年估计有 900 万美国人的身份信息遭到窃取。

通过鱼叉式网络钓鱼攻击从每个受害者处攫取的收益可能会千差万别，但平均值和中间值都非常高。例如，根据 Javelin 战略与研究机构开展的初级消费者调查，2010 年从每个受害者处获得的平均身份信息欺诈金额达到了 4607 美元。如果按照 400 美元的用户损失保守估计，2010 年 6 月，通过鱼叉式网络钓鱼攻击获得的年犯罪所得总金额达到了 1.5 亿美元（见表 4）。此数额是一年前的 5000 万美元的三倍；而且由于网络犯罪活动又恢复到之前的企业级别，因此预计未来几个月还会继续增长。

针对性攻击的影响

针对性攻击的恶意性质使其对于社会整体以及每个具体组织的危害都极大。通过针对性攻击攫取的网络犯罪收益虽然巨大，但同时也不易估计，因为受害者和攫取到的知识产权不同，获得的收益多少也千差万别。不过，网络犯罪收益只是受害组织总体成本的一部分，后者很大程度上也取决于组织的声誉和经营状况。

组织因受到针对性攻击而产生的成本可能千差万别。据 FBI 的调查显示，这些成本从数千到数亿美元不等。同样，Ponemon 研究所也估计，每个组织数据外泄可能产生的成本从 100 万美元到 5800 万美元不等。举个例子，一家大型游戏平台提供商报告，2011 年 2 季度其网络遭受的未经授权的访问，目前已知产生的相关成本大约高达 1.72 亿美元。这些成本包括设置个人信息防盗程序、身份信息窃取损失保险、“客户召回”计划费用、客户支持费用、网络安全增强费用、法律和专家费用，以及由于未来收入可能下降带来的利润影响。

再举一例，一家公共付款处理程序公司遭受数据外泄，导致数百万用户帐户凭证受影响。一年后，该公司报告，产生的相关费用达到 1.05 亿美元。根据其向美国证券交易委员会提交的 10-Q 报表文件显示，“此类费用约达 9080 万美元，大部分与以下几项费用相关：（i）万事达卡和维萨信用卡针对我们以及我们的担保行进行的评估，（ii）我们向特定卡品牌提出的解决提议，用于解决对我们的担保行（根据我们之间的协议，担保行有权向我们寻求保护）主张的索赔，以及（iii）与正在与之进行结算探讨的索赔人结算的预计成本。”从遭受入侵到提交 10-Q 结果的时间段里，该公司标准普尔 500 指数痛失 30% 的价值，即大概 3 亿美元的股东利益。

最终，该公司的声誉也遭受重创，这比资金损失和补救工作加在一起产生的成本还要高昂。

攻击的整体影响

表 4 汇总了这些预估值并显示出不同类型攻击每年带给网络犯罪分子的经济收益总额。

表 4：网络犯罪年经济收益总额

网络犯罪收益（百万美元）	1 年前	目前
大规模攻击	1,050 美元	500 美元
鱼叉式网络钓鱼攻击	50 美元	150 美元
针对性攻击	不固定，请参见上文	不固定，请参见上文
总计	1,100 美元	650 美元

很明显，网络犯罪业务模式的转变使不法分子通过较少的威胁活动产生了过渡性收益。虽然网络犯罪活动有所减少，但组织也未能因此而完全放松，因为由此产生的成本比经济损失要多得多。要估计此类总损失，Cisco SIO 对位于全球范围的 361 家组织展开了初步调查，以便了解他们的看法。

攻击对组织的影响可分类如下：

1. 经济
2. 补救
3. 声誉

经济：根据具体攻击的不同，直接转移到网络犯罪分子的经济损失可能相差很多；因此，组织无法估计此损失。

补救：鱼叉式网络钓鱼攻击和针对性攻击产生的补救成本由受害组织承担。管理团队必须辨别和补救受影响的主机；由于欺骗性应用的使用不断增加，这一工作颇具挑战性。鉴于当今针对性攻击和基础恶意软件的复杂性，补救成本可能非常高。

补救成本包括应对受感染主机所需的时间和该时间对应的机会成本。根据对组织的调查，思科发现，专门用于补救受感染主机需要的时间平均为两小时。每次补救两小时的成本基数视每个组织有具体情况而定，该时间对应的机会成本也如此。

根据 Cisco SIO 的研究，组织估计每个受感染用户的直接补救成本为 640 美元，相当于直接经济损失的 2.1 倍。

声誉：受害组织和用户可能在较长时间内都无法摆脱攻击带来的负面影响。例如，树立品牌通常需要很多年，但是负面事件或新闻报道，尤其是曝光率特别高的事件，可能会在很短的时间内就使企业的形象大打折扣。直接影响可能是业务大幅下滑，有时甚至会导致组织陷入绝境。

判断负面声誉影响造成的实际成本非常困难，就像估算组织的品牌价值一样。但是，组织很清楚负面事件可能会影响他们的声誉，进而可能会带来业务和股东价值的大幅下滑。

根据 Cisco SIO 的研究，组织估计每个受感染用户的声誉成本为 1900 美元，相当于直接经济损失的 6.4 倍。

复合影响：组织因鱼叉式网络钓鱼攻击和针对性攻击产生的总体成本要比转移到网络犯罪分子的直接经济损失多得多。表 5 展示的是 Cisco SIO 研究 361 家组织的结果。

表 5：每次攻击产生的总体组织成本

组织规模	资金损失*	补救成本*	声誉成本*
不超过 1,000 名用户	327 美元	558 美元	2,346 美元
介于 1,000到 5,000 名用户之间	233 美元	484 美元	1,436 美元
5,000 名用户以上	290 美元	833 美元	1,553 美元

*每个受感染用户

尽管根据组织情况和攻击方式的不同，产生的成本可能各不相同，但有一点非常明确：组织的总体成本会非常高。此外，声誉管理和补救工作可能会对组织形成无形压力。

总结

无论所属行业、地理位置和规模如何，低攻击量针对性攻击发生次数的增加，对众多组织中的用户都产生了影响。此类攻击的盛行，导致不法分子的经济收益增加，也对受害组织产生了影响。组织不仅要承担经济损失，而且还要承担补救受感染主机的成本和其品牌声誉遭受到的负面影响。随着针对性攻击数量的不断增加，网络犯罪活动将继续发展，其影响也将持续。

解决方案：思科安全智能运营中心

传统的安全保障方法依赖于产品的分层和多重过滤器的使用，而这已经不足以抵御最新一代恶意软件的攻击，因为它们不仅传播迅速、目标遍布全球，而且能够利用多种载体进行传播。

思科安全智能运营中心（SIO）是世界上规模最大的基于云的安全生态系统，利用其中的实时威胁情报功能，思科能够跟踪最新的威胁。Cisco SIO 使用已部署的思科邮件、网络、防火墙和入侵防御解决方案中的近百万个实时数据源提供的 SensorBase 数据。

Cisco SIO 对数据进行分析和处理，然后自动对威胁进行分类并使用 200 多种参数创建规则。安全研究人员还会针对可能对网络、应用和设备造成广泛影响的安全事件，收集并提供相关信息。每三到五分钟，系统就会为已部署的思科安全设备动态提供安全规则。Cisco SIO 团队还将发布安全防护最佳实践建议，以及抵御安全威胁的战术指导。

思科致力于为世界各地的组织提供一体化、及时、综合且有效的完整安全解决方案，从而实现全方位的安全保障。有了思科，组织可以省下研究威胁与漏洞的时间，集中精力实施主动的安全保障工作。

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太地区总部
Cisco Systems (USA) Pte. Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

Cisco 在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 中列出了各办事处的地址、电话和传真。