McAfee Labs
威胁报告

2014 年 11 月

intel Security

关于 McAfee Labs

McAfee Labs 是威胁研究、威胁情报和网络安全先进理念的全球领先来源之一。McAfee Labs 跨主要威胁媒介（文件、Web、消息和网络）利用数百万个传感器获取数据，提供实时威胁情报、评论分析和专家意见，以增强保护并降低风险。迈克菲现在是英特尔安全的一部分。

www.mcafee.com/cn/mcafee-labs.aspx

关注 McAfee Labs

简介

假日季日益临近，恶意用户又要准备故技重施了。迈克菲近期发布了 ***12 Scams of the Holidays（12 种节日诈骗）***，这份列表对其中部分危险行为进行了重点介绍。文章很有趣，强烈建议大家仔细阅读。另外，我们还开始对 2015 年进行全面预测，从全球经济发展方向到哪些好莱坞明星将红遍全球无一遗漏。

在过去的数年中，McAfee Labs 一直在专业知识领域开展预测。在**去年的预测报告**中，我们提出了多项相关预测。例如，我们精准地预测到勒索软件将会激增（包括移动平台恶意软件！）、政治动机攻击将会增加，而且企业将会积极采用威胁智能服务和分析工具识别日趋增多的隐匿威胁。但是，当然，我们还不够完善，漏掉了一些问题。这正是预测的本质。

今年，我们决定继续发布 2015 年威胁预测报告，并在本报告中提出相关预测。这样，我们的客户将有更多的时间全面考量 2015 年的工作，做好准备应对最严峻的威胁。当然，我们还会一如既往地在每个季度的报告中提供关键主题和威胁统计信息。

本季度首屈一指的关键主题讨论的是 BERserk，一种 RSA 签名验证软件漏洞，网络犯罪分子可以采取数不清的方式利用这种漏洞。迈克菲披露 BERserk 虽不及宣布发现 **Shellshock** 那样引人注目，但前者的潜在危害同样十分值得注意。有关该 BERserk 的更多信息可参阅**此处**。我们将在一个相关示例中对网络犯罪分子滥用用户信任的各种手段进行讨论。这提醒我们，在打击这种类型的威胁的过程中，认知与训练至关重要。

在本报告中，大家将会发现，我们不仅增添了一些新的图表，而且还对“威胁统计信息”部分正在使用的一些图表进行了调整。读者反馈提示我们增添一些对大家有益的统计信息。此外，我们开始利用自身系统提供的更出色的报告功能，提高一些图表的准确性。希望大家喜欢这些调整和新增内容。

对于在 ***August Threats Report（8 月威胁报告）***中对读者调查做出回复的用户，在此我们表示感谢。我们一直认真听取意见，上文列举的威胁统计信息改进就是最好的证明。若要分享您对本报告的看法，请单击**此处**完成一份有关本期“威胁报告”的五分钟快速调查。

祝您和您的至友亲朋节日快乐。

—Vincent Weafer，McAfee Labs 高级副总裁

目录

McAfee Labs 威胁报告
2014 年 11 月

此报告的研究及编写人员：

Cedric Cochin
Benjamin Cruz
Michelle Dennedy
Aditya Kapoor
Dan Larson
Haifei Li
Chris Miller
Igor Muttik
François Paget
Eric Peterson
Mary Salvaggio
Craig Schmugar
Ryan Sherstobitoff
Rick Simon
Dan Sommer
Bing Sun
Vinoo Thomas
Ramnath Venugopalan
James Walter
Adam Wosotowsky
Stanley Zhu

执行摘要

McAfee Labs 2015 年威胁预测

本威胁报告首先将会对 2015 年有望见证的威胁活动进行介绍。我们的预测范围广泛，包括围绕物联网、网络间谍、移动设备、隐私、勒索软件等在内的各种观点。

走进 BERserk 时代：受信任连接将遭受重创

BERserk 可以利用 RSA 的签名验证软件缺陷，为网络犯罪分子大开方便之门，从而在用户毫不知情的情况下发动中间人攻击。

9 月，**英特尔安全**发布的影响深远的所谓 BERserk 漏洞的详细信息，对构成漏洞来源的底层代码进行了首肯。在编写之时，人们并未意识到 BERserk 的各种影响，但它其实非常危险。BERserk 可以利用 RSA 的签名验证软件缺陷，为网络犯罪分子大开方便之门，从而在用户毫不知情的情况下发动中间人攻击。通常首先在 URL 开头使用 "https" 在访问网站时建立信任，再通过友好挂锁完成勾当。BERserk 会破坏这个链接，从而使恶意用户能够利用用户与网站间的信息流随心所需地查看信息及执行操作。

滥用信任：利用在线安全防护的软肋

McAfee Labs 相信，很多形式的在线交互信任均通过电子邮件来实现，这会使人们对其真实性产生怀疑。

用户是绝大部分安全设置的软肋。我们的大部分信息依赖设备提供；如果设备以安全的方式提供准确信息，我们就会选择信任。攻击者往往会集中攻击我们在设备上提供的信任机制，并用它来发动攻击窃取信息。这项关键主题将对信任滥用进行深度剖析，通过近期发生的几个例子重点阐释网络犯罪分子利用信任关系的若干手段。McAfee Labs 相信，很多形式的在线交互信任均通过电子邮件来实现，这会使人们对其真实性产生怀疑。

McAfee Labs 2015 年威胁预测

网络间谍
物联网
隐私
勒索软件
移动设备
销售点
恶意软件 - 突破 Windows 限制
漏洞
逃离沙盒

分享反馈意见

网络间谍

网络间谍攻击频率仍将继续增加。长期攻击者将转型为更加隐秘的信息收集者，而新晋攻击者则竭力设法窃取钱财及打击竞争对手。

小型民族国家和境外恐怖组织将利用网络空间发动战争打击敌方。他们将通过发动毁灭性分布式拒绝服务攻击或者运用清除主引导记录的恶意软件开展攻击，从而破坏敌方的网络。与此同时，长期网络间谍分子还会运用更有效的方法在受害者的网络上继续隐藏行迹，并运用更高级、更精密的隐匿技术和其他手段，持续隐藏在操作系统深处而不被发现。

值得注意的是，McAfee Labs 发现东欧高级网络犯罪分子纷纷从最初对金融机构客户凭据实施快速直接攻击（目的在于开展金融盗窃），转向更精密的高级持久性威胁 (APT) 方法，以便收集可供出售或在日后使用的情报。这样一来，犯罪分子的外观和行为模式开始向高级民族国家网络间谍分子靠拢，观望静待时机收集情报。

类似的方法也开始在零售业崭露头角。许多零售商构建了丰富的客户资料，包括购买习惯和产品兴趣、信用记录、位置记录、详细联系信息等等。此外，成功零售商的战略、运营和财务计划对于吸引适当的买方可能颇具价值。一些网络犯罪分子似乎利用基于 APT 的网络间谍方法入侵零售商的系统，以便暗中收集信用卡信息以外的其他情报，转售给高价竞买人。

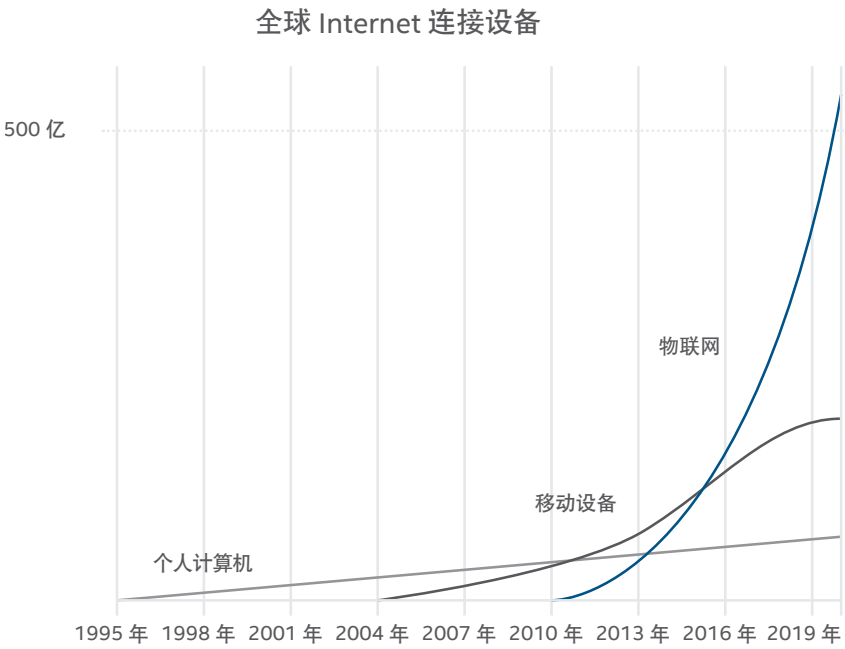
—Ryan Sherstobitoff

物联网

由于连接对象数量高速增长、安全防护意识差，而且设备数据价值高昂，物联网设备攻击势必将迅速增加。

物联网（IoT）家族的设备数量和种类飞速增长。在消费领域，这一趋势已在家用电器、汽车、家庭自动化乃至照明用品领域有所显现。商业领域也涌现出很多应用程序，并且在农业、制造业和医疗保健领域得到广泛应用。构建 IoT 设备的软件和硬件构建块不断增加，从而带来了极大的复杂度，非常不利于保持安全性。

这些组件乃至设备本身通常在构建时并未以安全性作为基本设计原则。IoT 设备的部署规模日益庞大，加之缺乏有力的安全防护，因而个人和公司的隐私性和安全性面临的威胁也不断增加。



资料来源：迈克菲，基于 BI Intelligence、IDC 和英特尔研究。

IoT 设备攻击已然十分常见 - 从安全控制力度薄弱的 IP 摄像机到具有基础加密缺陷的智能计量器再到为全球关键基础设施提供技术支持的 SCADA 设备纷纷沦为攻击目标。例如，在西班牙，数百万家庭安装的联网电表包含漏洞，攻击者可以利用漏洞开展收费欺诈，甚至人为导致停电。在去年的白帽黑客会议上，研究人员对如何轻松自如地攻破一些联网安保摄像机进行了演示，这样不仅可以窃取摄像机视频，还能访问摄像机所在的网络。

一种威胁尤其令人担忧：随着医疗保健 IoT 设备的日益盛行及其在各大医院的应用的日渐广泛，这些设备所含的信息面临的信息丢失威胁也越来越大。医疗保健数据甚至比信用卡数据价值更高，因为**据路透社研究**发现，健康凭据被盗产生的平均损失高达 10 美元，约为美国信用卡号盗窃价值的 10 到 20 倍。

这一度是民族国家和雄心勃勃的网络犯罪组织的乐土，而今则可能成为所有蓄意攻击者的战场。我们预计，2015 年将会出现与 IoT 设备漏洞直接相关的大规模攻击。

—Chris Miller 和 Ramnath Venugopalan

隐私

随着政府和企业在究竟什么是对定义本就不够完善的“个人信息”的公平授权访问问题上争执的持续白热化，数据隐私仍将不断受到攻击。

我们将数据隐私定义为对个人身份信息进行公平授权处理。虽然隐私实践和问题或许可以用一个简单的句子进行表述，但与隐私事件有关的复杂度和风险仍将不断攀升，并在 2015 年继续呈指数级增长。

深入剖析这个定义，“公平”这个概念取决于系统用户、企业客户或员工或者民族国家的公民。公平性可通过一组公平信息实践原则进行进一步定义，早在 20 世纪 60 年代这组公平信息实践原则业已获得国际认可。透明、通知、选择、适当收集、跨国界数据共享和处理、安全、有限访问和处置是其中的部分原则。

“授权”是数据隐私的另一个要素。我是谁？在管理数据资产时，我需要做些什么？在数字化和公平性不断上升的全球经济形势下，您是客户、员工还是公民？2015 年，我们将继续见证基于角色的旧系统，密码架构沦陷，被恶意或者至少行为草率的用户所接管。上下文生物特征和 ID 或许是最佳的存在和意图指标，必将成为巨大的创新领域。我们预计，身份、时间和地点将继续推动创新和漏洞利用风险飞速发展。

隐私定义的最后一个要素是“个人身份信息”。2015年，我们将会发现更多讨论，但仍然无法明确究竟什么是“个人”信息，哪些信息可供国家或隐私机构合理检测。很多地区的法律定义如下：个人信息是指直接识别特定个体的数据，或者与其他数据组合后很可能识别特定个体的数据。虽然统计学家和经济学家往往将大量趣闻轶事称为“数据”，而从技术角度，人们倾向于将使用大量信息的现象称为“大数据”。大数据规模越宏大，真正保持匿名的概率也就越低。因此，2015 年以后，人们将会发现越来越多的数据隐私规章制度及各种违规要求和安全规范涌入先前匿名的数据集王国。

我们预计，及至 2015 年底，欧盟将出台《数据保护条例》(2016) 全面更新 **1995 年颁布的《数据保护指令》**，该条例将在各欧盟成员国推广，并广泛应用于各国际组织。在欧盟看来，这一举措或许是一次声势浩大的公共政策策划，但拉美国家、澳大利亚、日本、韩国、加拿大及许多其他国家则在数据隐私法规制度方面表现得更加积极也更具区域性。

—Michelle Dennedy

勒索软件

勒索软件将对传播、加密和目标寻找方法进行演变。越来越多的移动设备将会遭受攻击。

我们预计，设法规避系统上安装的安全软件的勒索软件变体将专门攻击订阅基于云的存储解决方案（如 Dropbox、Google Drive 和 OneDrive）的终端。一旦这些终端受到感染，勒索软件将尝试利用登录用户的云访问凭据继续感染云中备份的数据。

如发现终端数据经过加密，当勒索软件受害者尝试访问云存储还原数据时将会受到猛烈攻击 - 结果发现勒索软件已对备份进行加密。

虽然经过勒索软件加密的文件自身无法传播也无法感染其他设备，但可以想象一下战术演变：通过将目标文件转换为可执行文件，并将原始数据文件存储到恶意软件中，每份加密文件都成为勒索软件本身的载体。文件感染病毒运用这项技术接管合法可执行文件并将它们转化为载体。勒索软件作者可以复制同一模型进行文件加密。

与去年的预测结果相同，我们预计针对移动设备的勒索软件将继续增加。由于手机和平板电脑托管大量珍贵图片和个人数据，因而成为恶意软件作者感兴趣的目标。我们预计，以云备份数据为目标的勒索软件技术将在移动领域再次发挥作用。随着支持大量无管制付款方式的移动平台的盛行，攻击者将可以寻求多种途径向受害者索要赎金，而后再释放其加密数据。

—Vinoo Thomas

移动

随着新型移动技术的攻击面不断扩大，加之几乎并未采取任何措施阻止应用商店滥用，移动攻击将继续迅速增长。

PC 恶意软件素来追随重大事件的脚步而发展，如恶意软件生成包兴起（允许不具备编程知识的用户制造威胁）、恶意软件源代码发布（允许编程经验极少的用户修改威胁），以及常见功能、应用程序或脚本引擎滥用。2015 年，我们将会在移动恶意软件领域见证类似的影响。开放式商业移动恶意软件源代码持续增加，很可能不久就会遭受相关影响。移动恶意软件生成包的崛起只是一个时间问题，这将降低潜在窃贼的进入门槛。

Apple iPhone 6（采用近场通信 (NFC) 芯片和集成数字钱包）将使利用 NFC 进行数字支付实现合法化。2015 年，其他移动设备供应商也会很快采用这些技术，用户将开始利用这些技术有效办理业务。由于是销售点 (POS) 交易，并且网络窃贼喜欢进行 POS 盗窃，因而将成为恶意用户的重大目标。2015 年，研究人员很可能会发现 NFC 硬件和数字钱包软件漏洞，网络窃贼势必会尝试利用这些漏洞。

移动恶意软件安装方法大致保持不变。受信任的应用商店（如 Apple App Store 和 Google Play Store）在防止恶意软件应用程序上架方面表现得相当不错，但仍然不免发生意外。此外，还有很多不受信任的应用商店和应用程序直接下载网站，其中的应用程序往往包含恶意软件。这些恶意应用商店和站点通信往往由“恶意广告”驱动，并且在移动平台上增长迅速。2015 年，我们将继续发现针对移动用户的恶意广告快速增长，移动恶意软件也会随之持续增加。

另外，由于攻击者竭力设法从 PC 世界移植有效的勒索方法，我们预计移动勒索软件将会有所增长。一旦在移动平台上臻于完善，对于网络窃贼而言，勒索软件甚至比在 PC 上更加有利可图，因为移动用户在很大程度上依赖自身设备即时访问联系人、计划和方位等关键信息。鉴于移动设备中存储了如此大量的宝贵信息，用户势必会不惜代价（包括支付赎金）重新获取访问权限。

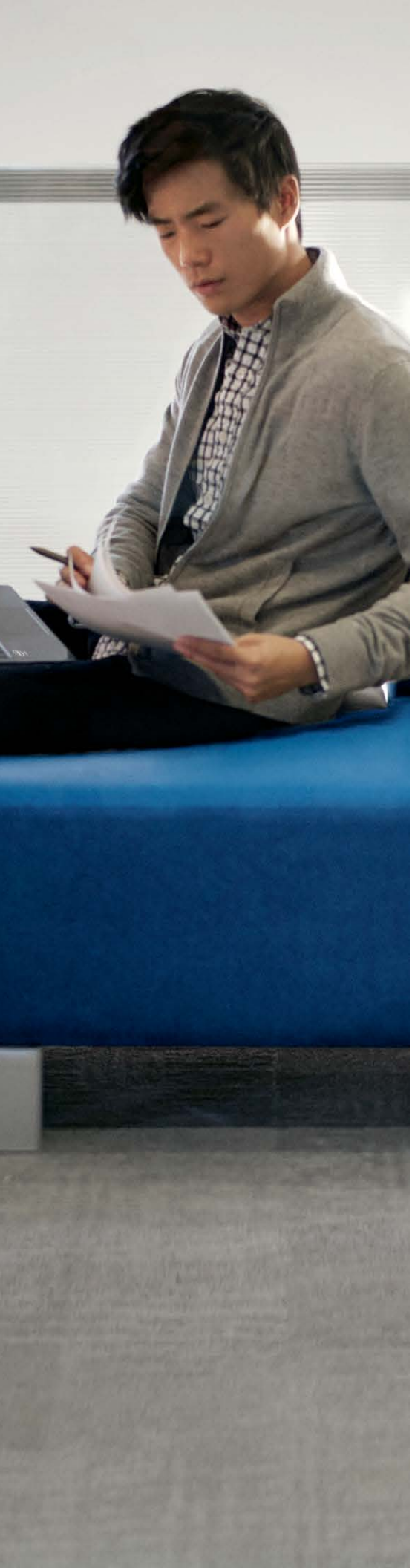
—Craig Schmugar 和 Bing Sun

销售点

销售点 (POS) 攻击仍然有利可图，越来越多的消费者在移动设备上采用数字支付系统，这就为网络犯罪分子提供了新的有机可乘的攻击面。

据一篇《**福布斯**》**文章**报道，2013 年的零售交易额高达 15 万亿。这也促使有关交易支付系统成为摆在网络犯罪分子面前的诱人目标。2014 年，我们发现此类系统攻击出现大幅上扬，Home Depot 就曾发生大规模违规事件。一如既往，信用卡刮录器仍在继续危害消费者。今年的表现更为猖獗，从用餐卡刷卡器到 ATM 再到气泵无一幸免。POS 攻击十分常见，因而业已成为相关行业从业人员日常工作的重要组成部分。然而，人们几乎未采取任何措施增强 POS 安全性，据此我们预计 2015 年 POS 系统违规将继续呈上升趋势。但是，我们可能会发现美国威胁形势将在 2015 年末有所缓解，因为零售商纷纷开始部署芯片密码卡和读卡器。

我们预计，明年数字支付系统应用将大幅增加。Apple 对 iPhone 进行了更新，纳入了 NFC 技术。它将营造一项全新的 iWallet 功能，即将信用卡信息纳入支付系统，无需消费者进行刷卡。一些 Android 设备还支持 NFC，运用所谓的 Host Card Emulation 进程简化移动支付。Visa 和 MasterCard 均已采用这项技术，目前提供可以在支持 NFC 的设备上使用的移动支付应用程序。鉴于相关基础设施现已部署妥当，我们预计消费者必将广泛采用。这意味着，我们还会见证针对这些系统的大量成功攻击。



数字支付系统可以消除信用卡刮录器风险，但其自身却也不乏风险。一些风险来源于基础 NFC 技术漏洞。其中一些漏洞已经在 DEF CON 2013 期间突出强调，**NFC Awareness Project** 还会继续追踪相关情况。根本问题在于，人们目前通过无线方式发送敏感信息，攻击者很可能会利用此类连接。此类攻击历史悠久，包括 2005 年发动的 Bluetooth Sniper Rifle 攻击，以及 2009 年发动的 Radio Frequency Identification (RFID) Passport 远程克隆攻击。由于目前已有很多**漏洞记录在案**，很可能还会发生针对 NFC 设备的类似攻击。鉴于消费者目前通过具有已知漏洞的协议发送支付信息，2015 年很可能会涌现出以此类基础设施为目标的攻击。

—Dan Larson

恶意软件 - 突破 Windows 限制

在 Shellshock 漏洞的推动下，非 Windows 恶意软件攻击将全面爆发。

2014 年下半年，我们发现了 **Shellshock 漏洞**：它是 Bash（Unix、Linux 和 OS X 计算机的一种常见命令行外壳）的一大缺陷。攻击者可以借助它在受害者的计算机上执行任意命令，从而使其成为最危险的漏洞 - 被**美国国家漏洞数据库**评为 10 级漏洞（严重性共分 10 级）。

在未来的几年中，人们将充分感受到这种新发现的漏洞带来的巨大冲击。很多设备会运行某种形式的 Unix 或 Linux，从路由器到 TV、工业控制系统、飞行系统和重要基础设施无所不在。我们只是刚刚开始对这种漏洞的范围进行了解。

这种攻击媒介将作为从消费者设备访问严重依赖非 Windows 系统的企业的基础设施切入点。因此，我们有望在 2015 年见证非 Windows 恶意软件大幅增长，因为攻击者希望加以利用：泄露数据、攫取系统赎金、添加垃圾邮件僵尸程序，继而开展其他恶意行为。Shellshock 将在攻击者利用易受攻击的新旧设备开展攻击时掌控局面。

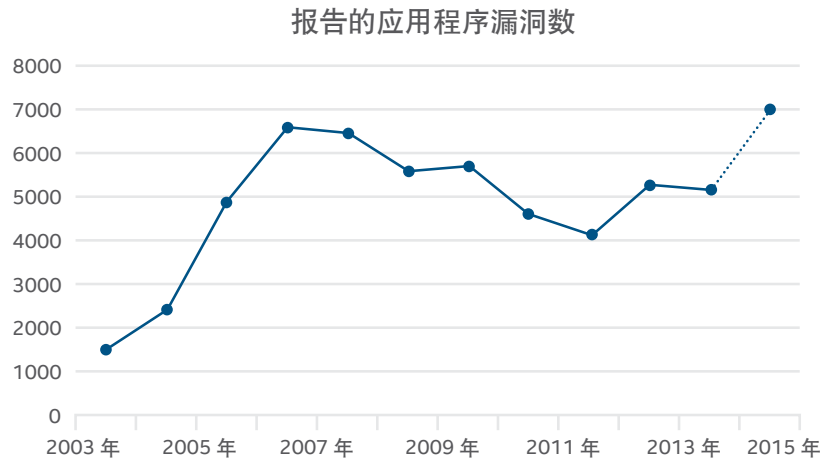
—Craig Schmugar

漏洞

随着常见软件缺陷数量的持续增加，漏洞也将不断增加。

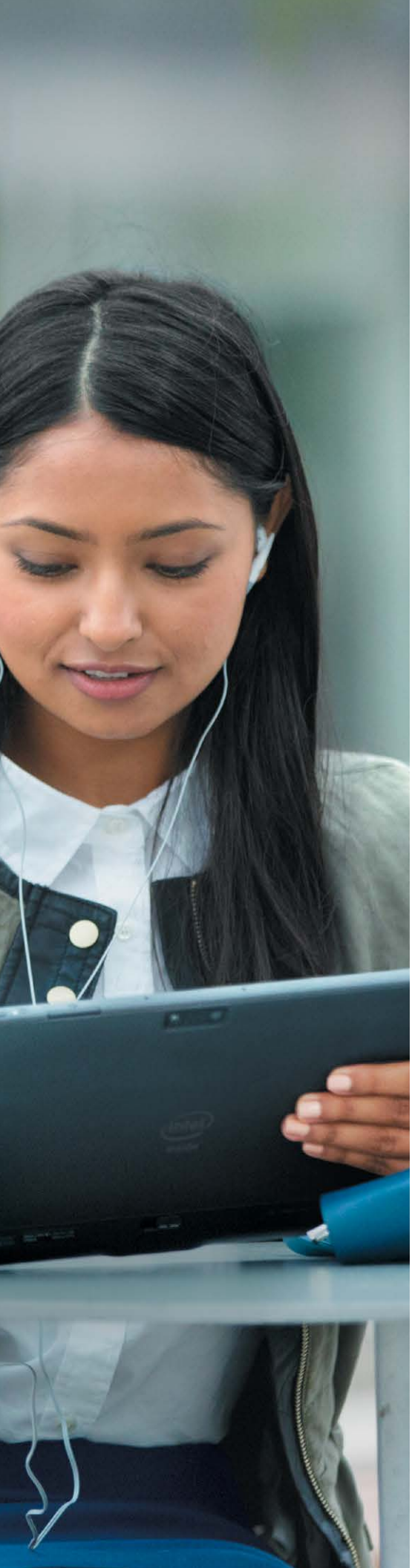
美国政府国家漏洞数据库数据显示，过去三年的漏洞数量不断增加。据对 9 月 30 日前记录的约 5200 个条目的研究发现，2014 年的漏洞总量很可能已经超过 2006 年创造的历史记录。

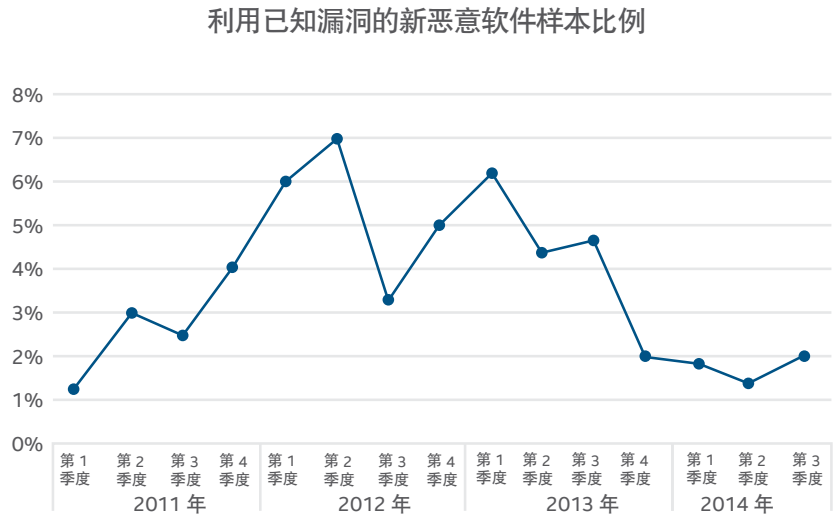
漏洞计算并非直接风险指标，因为还有很多相关因素也会带来影响，包括修补速度和覆盖面、各种漏洞的严重性、攻击面以及许多其他因素。但是，这些数字可以让我们对生态系统的整体健康状况有所认识。



资料来源：美国国家标准与技术研究院 - 国家漏洞数据库。

我们发现，自 2006 年到 2011 年，漏洞数量有所下降，但情况将有所改变。这种下降或许要归功于 64 位软件的编译器堆栈检查、数据执行保护和地址空间布局随机化技术。近期出现的上升趋势很可能表明存在新的漏洞利用技术，如堆栈透视及返回和跳跃性编程，同时黑帽和白帽漏洞猎人很可能对 64 位软件有了更深入的了解。





资料来源：McAfee Labs。

McAfee Labs 对我们的恶意软件库进行分析，确定了恶意软件利用已知漏洞的频率。按季度计算，有介于1%到6%之间的新恶意软件样本利用已知漏洞。本季度的统计数字约为 2%，相当于 821000 个新恶意软件样本利用已知漏洞。随着运用漏洞利用技术的样本绝对数量的增长，恶意软件量也随之增长；因此，“漏洞相关”样本的比例仍然相对稳定。

2015 年，我们预计应用程序或操作系统开发人员采用的漏洞缓解技术不会出现任何重大变化。此外，现行和新兴最佳实践的采用率也很可能会增加。因此，我们预计新发现的漏洞数量将持续攀升，这意味着利用这些新发现漏洞的恶意软件数量也会增加。

—Igor Muttik 和 François Paget

逃离沙盒

逃离沙盒将成为重要的 IT 安全战场。

许多重要的常见应用程序（包括 Microsoft Internet Explorer、Adobe Reader 和 Google Chrome）纷纷实施自身的沙盒技术来限制恶意行为。由于应用程序沙盒可以有效阻止很多类型的攻击，恶意软件作者一直设法绕开这道安全机制。

我们以 Internet Explorer 为例进行说明。无法绕过沙盒的恶意软件不会对用户构成威胁，因为这种漏洞利用技术不可能对系统做出持久性更改。尽管如此，目前共有两个版本的 Internet Explorer 沙盒技术 - 保护模式 (PM) 和增强保护模式 (EPM)。目前，Internet Explorer 10 和 11 默认采用 PM，但据我们的研究发现，PM 比较容易绕过。虽然我们并未发现用于绕过 PM 或 EPM 的流行漏洞利用技术，但构建块已然摆在面前，因此我们很可能会在 2015 年发现一些 Internet Explorer 沙盒逃离及并发零日攻击案例。

目前，人们已经在许多主要客户端应用程序中发现并披露了可能导致应用程序沙盒逃离的漏洞。我们已经在 Adobe Reader 和 Flash、Chrome、Apple Safari、Oracle Java 及 Internet Explorer 中发现了一些有据可循的漏洞。这些漏洞促使研究人员和攻击者纷纷投身开展进一步的调查。例如，BlackHat 2014 期间，研究人员列举了四项应用程序沙盒绕过技术，这些技术已在今年举办的 Pwn2Own 黑客大赛获奖作品中得到成功应用。事实上，在今年大赛中胜出的几乎所有 “pwns” 均在攻击的最后阶段成功完成了沙盒逃离。

我们已经发现可以利用漏洞逃离应用程序沙盒的技术。黑客市场终究会向网络犯罪分子提供此类技术，这仅仅是一个时间问题。我们相信，2015 年将会变为现实。

另外一项预测：迄今为止，网络犯罪分子主要致力于逃离应用程序沙盒。但是，随着安全软件供应商提供的独立沙盒系统的日益盛行，必然会为网络窃贼设置新的障碍。作为回应，网络犯罪分子开始设法使自身的恶意软件逃离这些沙盒系统。而今，已有数量可观的恶意软件家族可以识别和规避基于沙盒的检测。但是，迄今为止我们还未发现任何恶意软件能够成功利用管理程序漏洞突破独立沙盒系统。预计这种情况将在 2015 年有所改观。

—Haifei Li, Rick Simon, Bing Sun, 和 Stanley Zhu

关键主题

走进 BERserk 时代：受信任连接将遭受重创

滥用信任：利用在线安全防护的软肋

分享反馈意见

走进 BERserk 时代：受信任连接将遭受重创

—James Walter

在关键主题“**滥用信任：利用在线安全防护的软肋**”中，我们对目前面临的在线网站信任挑战进行了概括介绍。在这个关键主题中，我们将讨论会深刻影响信任的特定漏洞。

英特尔安全高级威胁研究团队专注影响在线交易和信息流安全的若干重要领域。其中一个重要领域是安全通信基准。该领域包括在 SSL/TLS 中实施深度威胁和泄露分析、TPM 2.0、加密通道及其他各个领域，倘若假设现有的信任模型十分“牢固”，则往往会忽略其他领域。

9 月，英特尔安全高级威胁研究团队发布了漏洞 BERserk 的详细信息。该名称衍生自特定编码序列（遵循 RSA 签名验证实现的基本编码规则 (BER)）分析发现的薄弱条件。英特尔安全与安全研究人员 Antoine Delignat-Lavaud 披露了这个 Mozilla 漏洞，提醒公司为多款产品发布更新，包括 Firefox、Thunderbird、SeaMonkey 和 NSS。Google 还更新了 Chrome 浏览器和 OS，因为这些产品采用了 NSS 加密库。

缺陷位于 RSA 签名验证，特别是序列验证期间 ASN.1 编码序列的解析错误。此漏洞是 Bleichenbacher PKCS#1 v1.5 RSA 签名伪造漏洞（在 **CVE-2006-4339** 中定义）的一个变体。易受攻击的实现会扫描编码消息确定是否存在填充字节 0xFF，直至发现分隔符字节 0x00 为止。该进程可在未确保编码消息 (EM) 的 DigestInfo 和信息摘要右对齐的情况下，继续对照预期值验证 DigestInfo 和信息摘要，这样将保证信息摘要不会多出任何额外字节。若不执行这项检查，EM 可能会在信息摘要后包含多余的垃圾字节，只有这样，此 EM 才能满足以下签名验证要求：

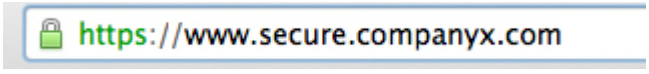
EM’ = 00 01 FF FF FF FF FF FF FF FF 00 DigestInfo MessageDigest Garbage

其他 EM 垃圾可能会允许对手生成 RSA 签名：EM 等于 RSA 模数的立方：

EM’ = (s’)^3 mod N

恶意用户无需知道 RSA 私钥 {p,q,d} 即可创建 RSA 签名，从而伪造 RSA 签名。

结果，攻击者无需搞清对应的 RSA 私钥，即可伪造 RSA 证书。这是什么意思？我们会遭受怎样的影响？

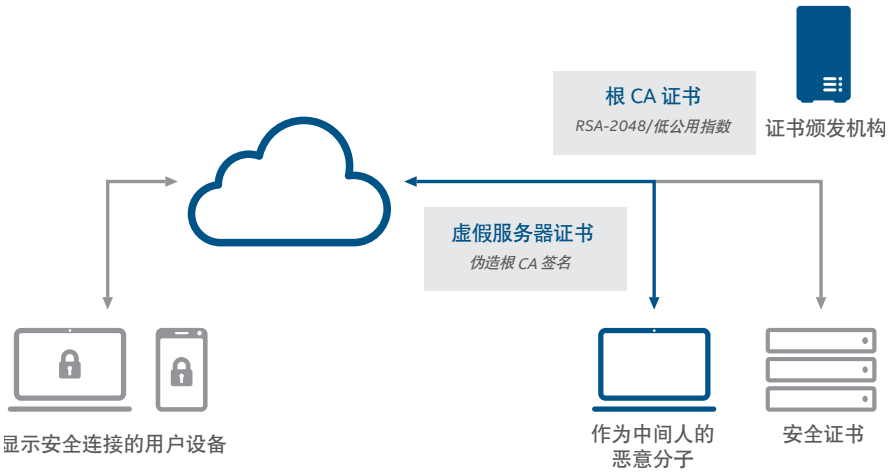


BERserk 为网络犯罪分子大开方便之门，从而在用户毫不知情的情况下发动 Internet 会话中间人攻击。这可能会成为竞争对手 Shellshock 的潜在威胁。

答案很简单。我们这些遵纪守法的 Internet 公民和用户已经习惯特定的信任模式。当处理在线交易（要求提供个人数据的银行、医疗或其他交易）时，我们知道该如何检查会话是否安全。我们一直以来学到的方法是在 URL 中查找 "https" 以及有益的挂锁图片。这些信息有助于我们确定站点或应用程序是否安全，确保并未向任何非法团体暴露任何数据。

BERserk 及相关漏洞改变了这一惯例，对我们的信任度和通过 SSL/TLS 传输会话的安全性提出了挑战。由于能够精确伪造 RSA 签名，攻击者可以在任意数量的场景下建立中间人会话。

BERserk 漏洞可能会导致中间人攻击



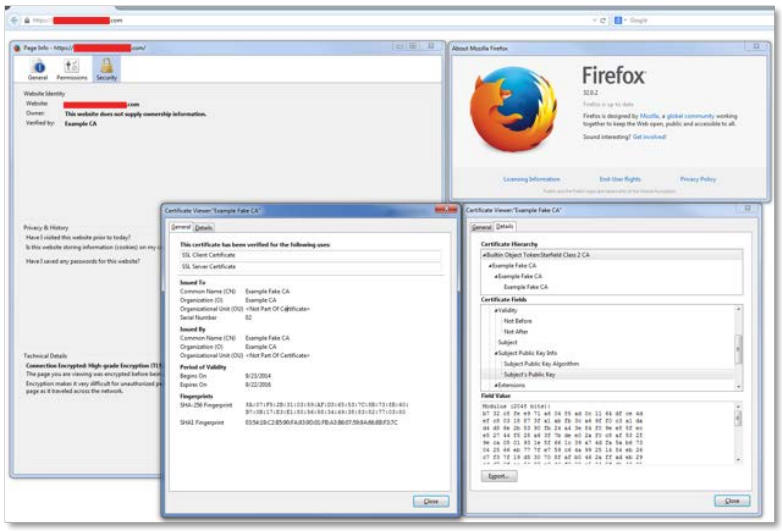
例如，客户与其银行网站间的会话机密性和完整性可能会遭到破坏。通过安装虚假证书，用户可以访问站点，甚至查看证书确认其真实性。一切看似有效，但其实根本无效。同样，登录医生网站查看检查结果的用户也可能会沦为该缺陷的受害者。在线缴税及许多其他场景下的用户也会面临同样的威胁。

除 Web 威胁和软件威胁以外，硬件设备（如手机）内部使用的加密库会存储敏感数据，应用程序有权根据需要访问这些敏感数据。想象一下，如果某部手机或平板电脑包含安全记忆体和执行，以便为设备软件提供加密功能。那么，设备中势必包含一个经过数字签名的固件，从而防止通过恶意软件或手动用户干预进行未授权修改。但是，由于 BERserk 缺陷的影响，他们很可能会攻破固件，继而破坏安全硬件要素负责监管的数据的完整性和机密性。

了解迈克菲如何帮助抵御这种威胁。

该模型的常见用途是存储用于专业供应商或终端（如 NFC 支付系统，所有卡数据均存储在设备之上）支付的金融帐户数据。在此场景下，攻击者可通过多种方式操纵会话，包括劫持及操控输入和输出，或者简单收集和窃取敏感数据。

在我们的研究中，我们最多可以伪造 1024 位和 2048 位的 RSA 证书。这很可能使攻击者受益。尤其是 Mozilla NSS，攻击者可以伪造证书，并且证书链能够获得 Mozilla NSS 的信任。



Firefox 中发现的一份伪造证书。

英特尔安全高级威胁研究团队将继续检查这些问题，并确定浏览器行为以外的其他场景会受到怎样的影响。我们的团队还与 CERT 和受影响的供应商合作解决相关问题。

受影响的加密库供应商将继续发布更新并提供指导。Mozilla 和 Google 一直对产品进行更新。受影响的用户应遵循供应商指导，确保系统保持最新状态。

有关 BERserk 的更多信息：

- BERserk 漏洞：**Part 1: RSA signature forgery attack due to incorrectparsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5（第 1 部分：PKCS#1 v1.5 ASN.1 编码 DigestInfo 解析错误引发的 RSA 签名伪造攻击）**
- BERserk 漏洞：**Part 2: Certificate forgery in Mozilla NSS（第 2 部分：Mozilla NSS 证书伪造）**
- Intelsecurity.com：**BERserk**
- 计算机紧急响应小组：**VU#772676**
- 美国国家漏洞数据库：**CVE-2014-1568**

滥用信任：利用在线安全防护的软肋

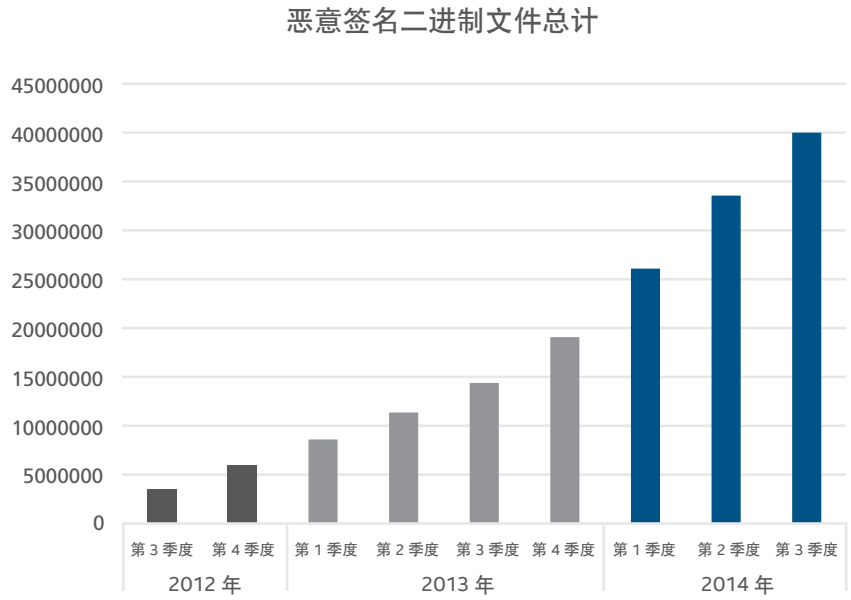
—Cedric Cochin 和 Craig Schmugar

每一天，世界上都有很多人在依赖电子设备，无论是个人设备、手机、电视还是汽车。我们一直依赖这些设备，并且在大部分情况下相信它们可以提供精确信息。

但是，信任必须通过通过努力营造和建立，这个过程往往需要时间和财力支撑。每年企业都要耗费数百万美元加强品牌效应，它们明白，有效的品牌投资将会带来数倍的回报。它们明白，倘若产品声誉卓著，消费者势必更愿意购买产品。

攻击者也十分清楚这一点，但往往缺乏与受害者建立信任关系所需的时间、资源和耐心。他们退而求其次，想法设法利用信任投资以及与他人之间的关系。

每天都会发生数起信任滥用事件，而且形势每况愈下。例如，McAfee Labs 会跟踪恶意签名二进制文件，恶意签名二进制文件是一种信任滥用形式，因为攻击者会通过冒充合法认证文件来伪装恶意软件。自 2007 年开始执行相关跟踪以来，恶意签名二进制文件有增无减。

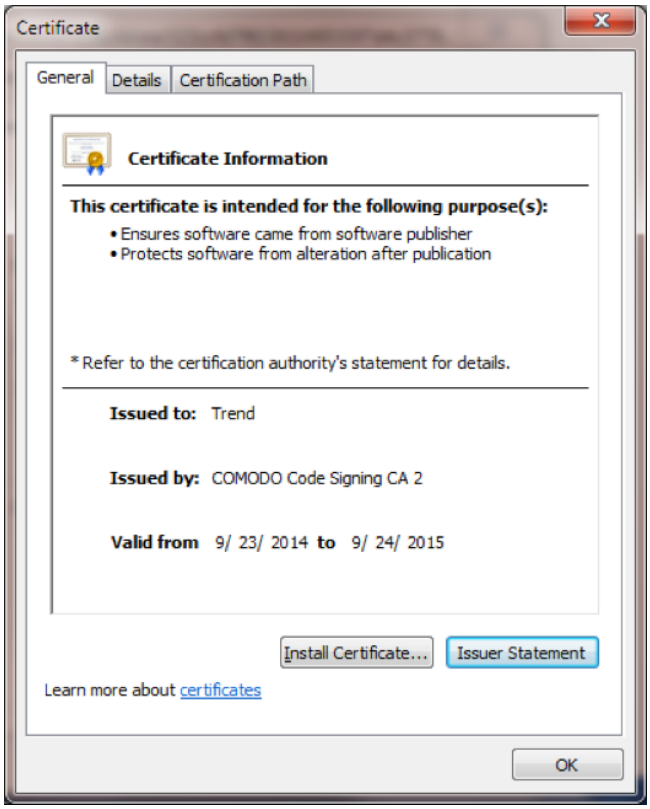


恶意软件作者对威胁进行数字签名，以期滥用用户、产品和操作系统信任。
资料来源：McAfee Labs。

继承信任利用品牌在用户心中的价值。网站往往会模糊受信任品牌与站点中显示的其他品牌之间的关系。

继承信任

多年来，人们只是通过确认品牌，在交易期间与商业品牌建立信任。而今，消费者还必须确定受信任品牌是否反过来信任通过受信任品牌的在线踪迹表示的其他品牌。9 月，**"Kyle and Stan" 恶意广告网络**被发现通过大众网站（如 Amazon.com、ads.yahoo.com 和 youtube.com）以及**主要广告网络（如 Double-Click 和 Zedo）**分发“恶意广告”。据报道，通过 Zedo 广告网络发动的一项恶意活动对 Alexa 热门网站**用户造成恶劣影响**，借此分发经过签名的 CryptoWall 特洛伊木马变体。使用的数字签名被分发到 "Trend"，很可能是为了模拟安全供应商 Trend Micro。初期遥测显示，北美用户遭受的影响最为剧烈。遗憾的是，很多消费者凭空臆断“关联无害”信任，因而往往陷入彀中无法自拔。



用于签署 CryptoWall 的证书。

消费者与商业品牌之间的信任关系通常会被滥用。例如，在某款山寨应用程序中，病毒或特洛伊木马会被视作合法而且往往广受欢迎的程序。在过去的一个季度中，垃圾邮件制造者企图将 Adobe 仿冒 "FlashPlayer11" 作为正品出售。据 Google Play 下载计数和 McAfee Mobile Security 检测遥测显示，垃圾邮件制造者在欺骗用户方面取得了一定的成效。

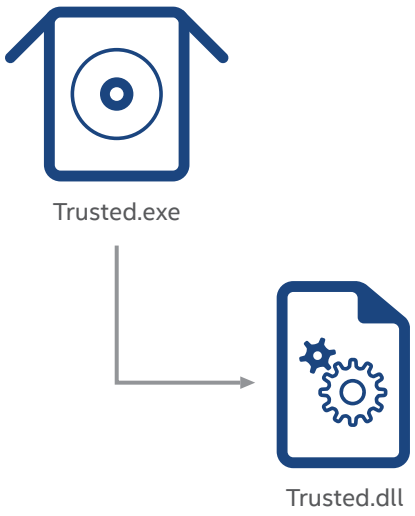
Google Play 中的若干山寨 "FlashPlayer11" 应用程序之一。

McAfee Mobile 的 "FlasherPlayer11" 恶意软件检测结果 (Android/Fladstep.B)。

攻击者通过 DLL 旁加载（一项用于插入恶意代码的常见技术）滥用产品或操作系统信任。

产品和操作系统信任

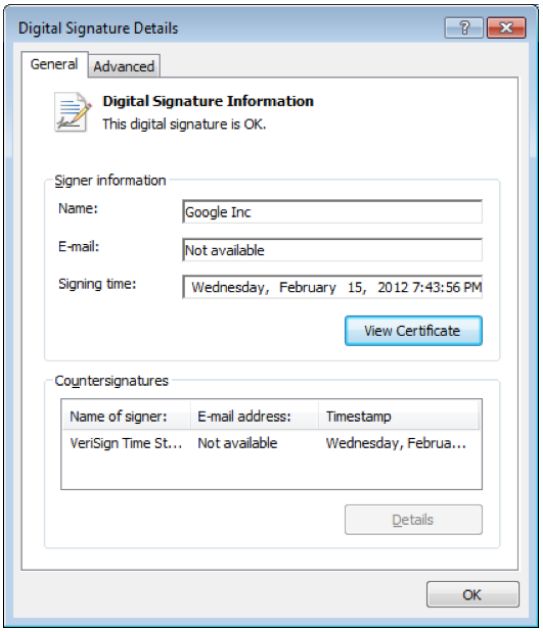
目前的安全产品往往根植于信任。为提高性能及减少误报，系统清单会确定无害应用程序，并且不会对其行为祥加检查。攻击者明白，如果他们的代码可以借受信任应用程序之便，那么势必会大大提高成功几率。多年来，恶意软件一直利用这一因素，采用所谓的 DLL 旁加载方法。这项技术包括执行实施外部库代码的合法应用程序。攻击者巧妙利用负载充当预期 DLL 角色，从而使清洁应用程序执行恶意代码。



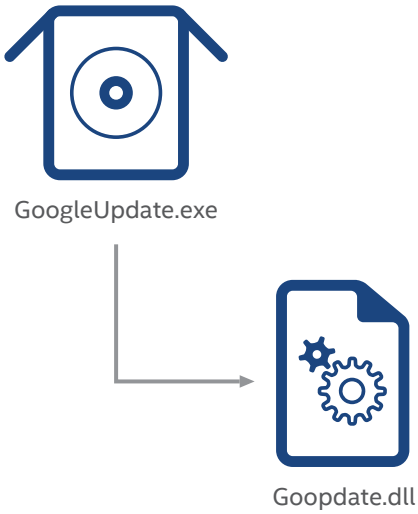
典型场景：受信任的可执行文件加载受信任的库。

恶意场景：受信任的可执行文件加载未知恶意软件库。

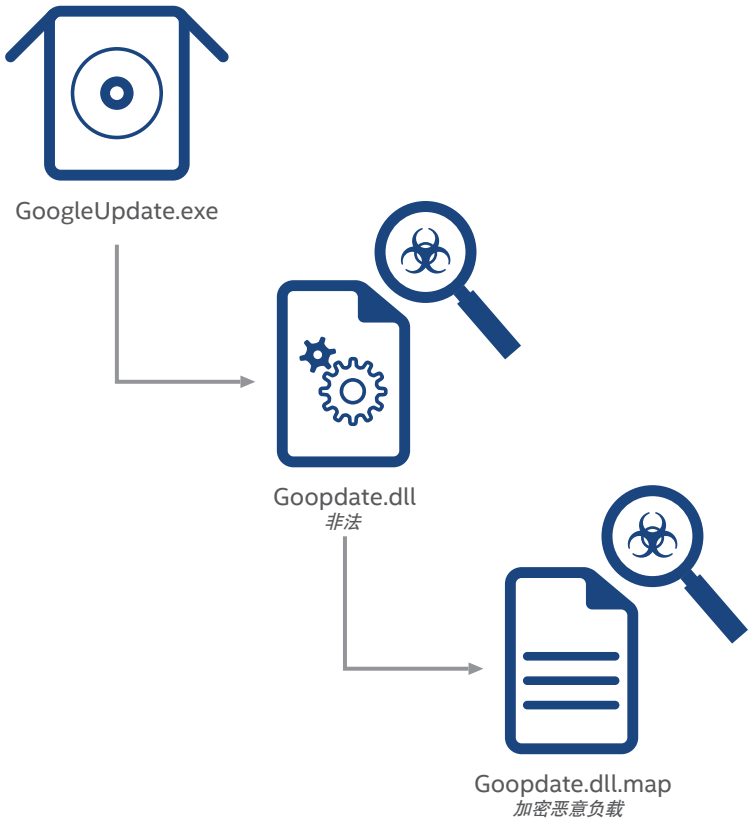
第三季度，McAfee Labs 观测到 DLL 旁加载滥用一个相对较新的目标 - 签名 Google Updater 应用程序。新 PlugX 恶意软件变体充当导入 goopdate.dll 的角色，但 PlugX 则进一步隐藏行迹。goopdate.dll 模块不过是担任中间人，负责读取加密数据文件 goopdate.dll.map 的内容，将内容解密到内存，然后对这些代码实施执行控制。这种方法的优势在于，可以模仿中间 DLL 文件的功能。攻击中涉及的三个组件本身都没有恶意，单独分析这些文件可能很容易得出错误的结论。但结合其他因素不难看出，恶意意图昭然若揭。信任经合法 Google Inc. 证书签署的文件的产品将会被运用这项技术的攻击者滥用。



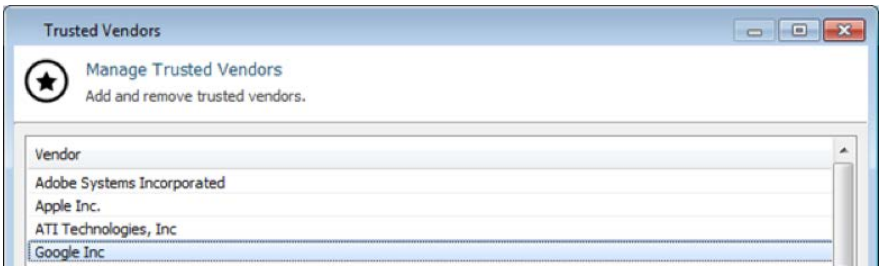
合法签名 Google Updater 应用程序。



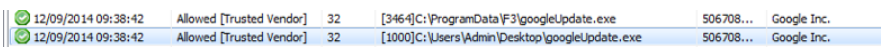
合法 Google Updater 加载 Google 库。



合法 Google 可执行文件加载恶意模块，该恶意模块可加载负载。
Google Updater 加载 Google 库。



默认情况下，该白名单应用程序毫无保留地信任有效 Google 应用程序。

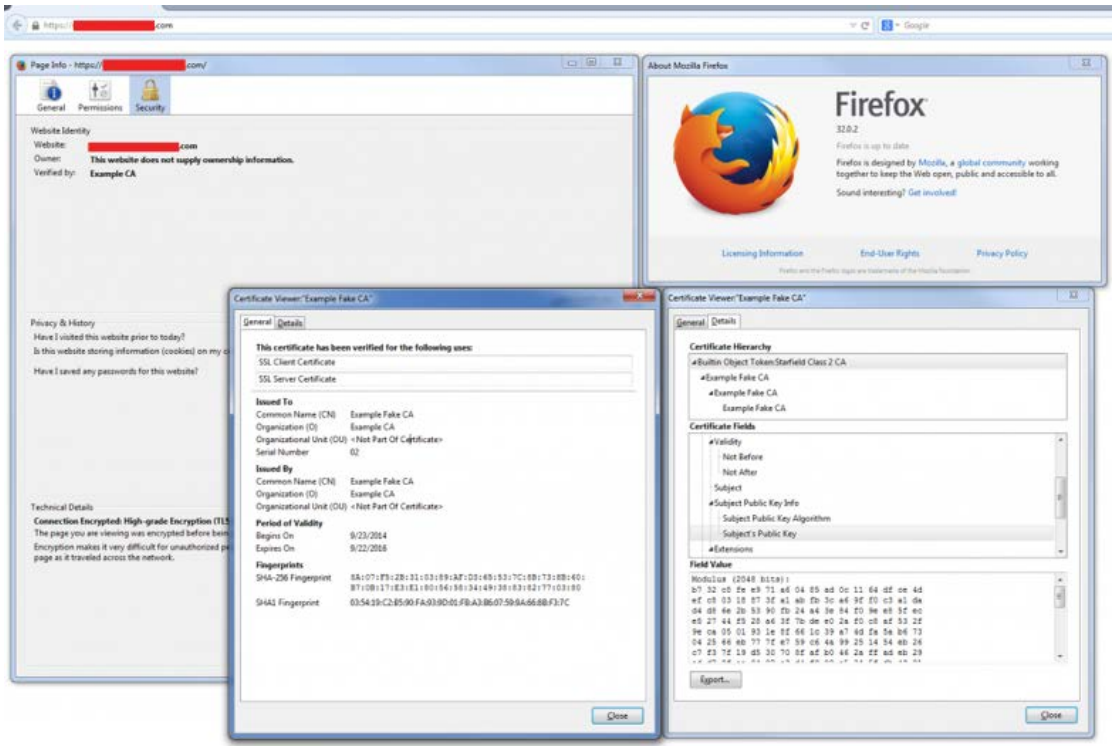


默认允许的 [受信任的供应商] 应用程序。

在最近的一个 **Angler Exploit Kit 变体**中，我们发现产品信任滥用取得了巨大的进步。该攻击无需将负载事先写入磁盘即可直接执行，因而白名单应用程序没有机会允许或拒绝新交付的代码，再确定是否执行代码。另外，这一步骤还可以绕过文件防病毒检查，因为在攻击之时不会扫描任何文件。

另一种形式的信任滥用涉及操作系统与网络路由控件交互。应用程序依赖操作系统提供安全可信的通信模式。例如，应用程序假设其流量将会安全正当地路由至预期接收者。一个非常知名的恶意软件系列是 DNS Changer。此类恶意软件的唯一目的是改变操作系统的 DNS 配置，迫使所有 DNS 查询进入攻击者控制的 DNS 服务器。虽然浏览器表现得很像在与受信任的银行网站进行通信，其实却是在与捕获用户数据的虚假站点或恶意透明代理交换数据。

确定用户是否在与虚假站点交互并没有想象的那么轻松。"BERserk" ASN.1 **漏洞由英特尔于 9 月 24 日报告**，并在本报告的关键主题**“走进 BERserk 时代：受信任连接将遭受重创”**中进行讨论，出色地说明了如何破坏浏览器，使其相信它们正在与受信任站点进行通信。该漏洞可让攻击者伪造 RSA 签名，从而绕过使用 SSL/TLS 执行的网站身份验证。鉴于能够伪造任何域的证书，这个问题会在我们访问自认为安全的网站时引发严重的完整性和机密性隐患。



"BERserk" ASN.1 漏洞利用程序。

了解迈克菲如何帮助抵御这种威胁。

名称解析滥用还会损害操作系统。通过将系统指向恶意升级服务器以及在预期范围外使用受信任证书，攻击者就可以部署恶意软件了。**Flame 间谍恶意软件**就是一个著名的案例，这款间谍恶意软件于 2012 年首次发现。Flame 包含用于感染目标计算机的代码，通过劫持分发安全补丁程序的 Microsoft Windows 更新机制达到攻击目的。

类似攻击可能会损害网络元素（如消费者路由器），这样攻击者不仅可以捕获来自台式机和笔记本电脑的通信，还能捕获来自电视、控制台及其他连接设备的通信。8 月，当 Synology 网络附加存储用户报告感染 SynoLocker（一种挟持数据的勒索软件特洛伊木马）时，发生过此类攻击。

信任为攻击者创造了机会，滥用风潮肆虐全球。用户需要随时保持警惕。安全产品需要允许客户定义应该信任/不信任哪些数据并提供灵活的控件，在限制不受信任用户的同时，给予受信任用户更广阔的权限。倘若无法应对这项挑战，很可能会增加人们对用于访问 Internet 的许多技术的质疑，甚至还可能会降低整体 Web 利用率。

抵制信任滥用

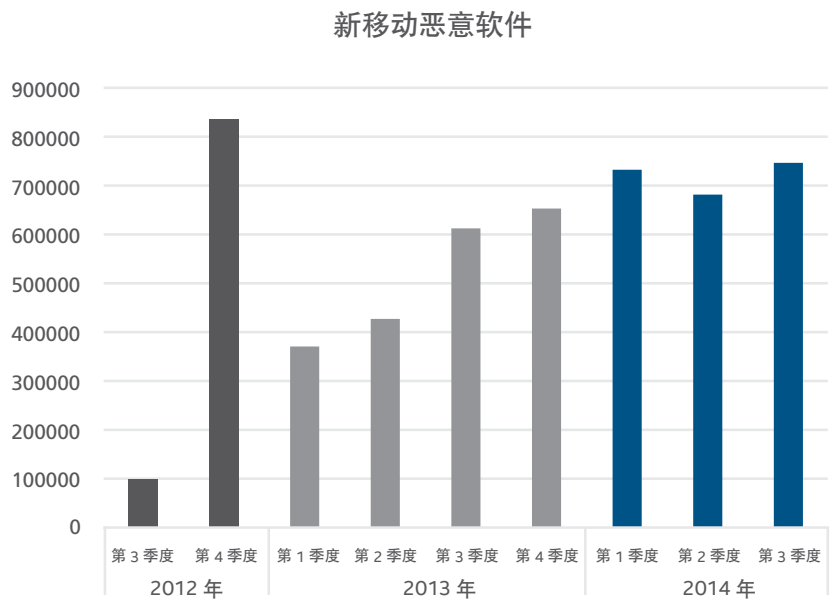
滥用	对策
继承信任（恶意广告）、产品和操作系统信任	始终保证操作系统、应用程序和安全软件处于最新状态。
恶意漏洞利用程序（随看随下）	保证系统处于最新状态。访问信誉良好的网站。将光标悬停在超链接上预览目标。不要点击通过电子邮件或社交网络提供的可疑链接。
品牌滥用（伪造的电子邮件、山寨应用程序和虚假域）	怀疑并验证，手动输入 Web 地址，在受信任站点上搜索应用程序，选择信誉良好的应用程序（下载量大、评价出色），并检查应用程序权限请求。
设备滥用	保证设备安装最新固件。

威胁统计信息

移动恶意软件
恶意软件
Web 威胁
邮件威胁
网络威胁

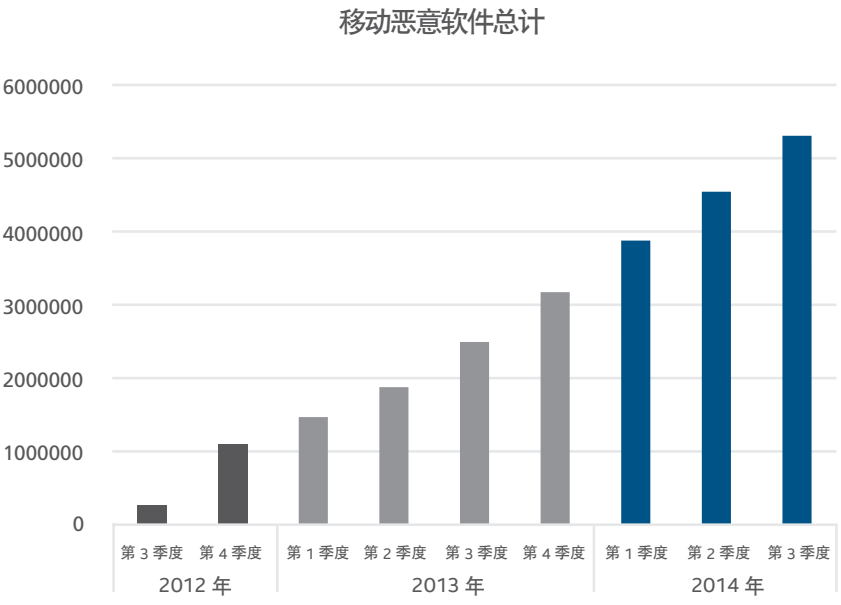
分享反馈意见

移动恶意软件



资料来源：McAfee Labs。

2014 年第三季度，移动恶意软件样本总数超过 500 万个，本季度增长高达 16%，相较于去年同比增长 112%。

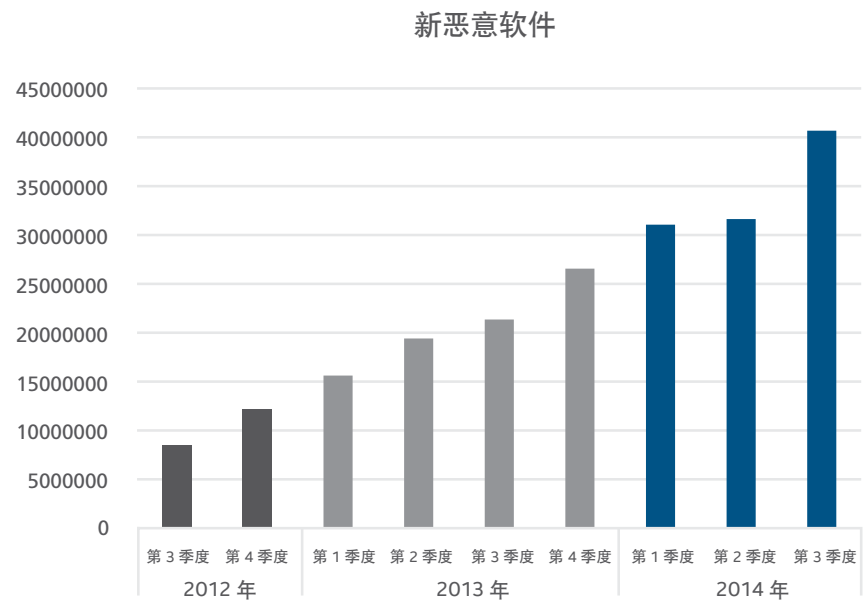


资料来源：McAfee Labs。

分享本报告

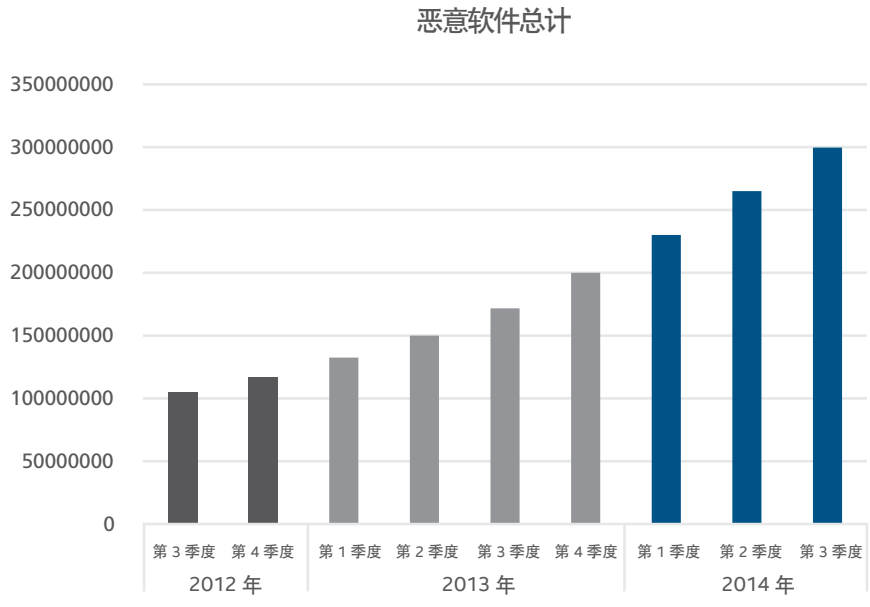
恶意软件

每分钟产生的新威胁超过 307 个，或者说每秒钟超过 5 个。



资料来源：McAfee Labs。

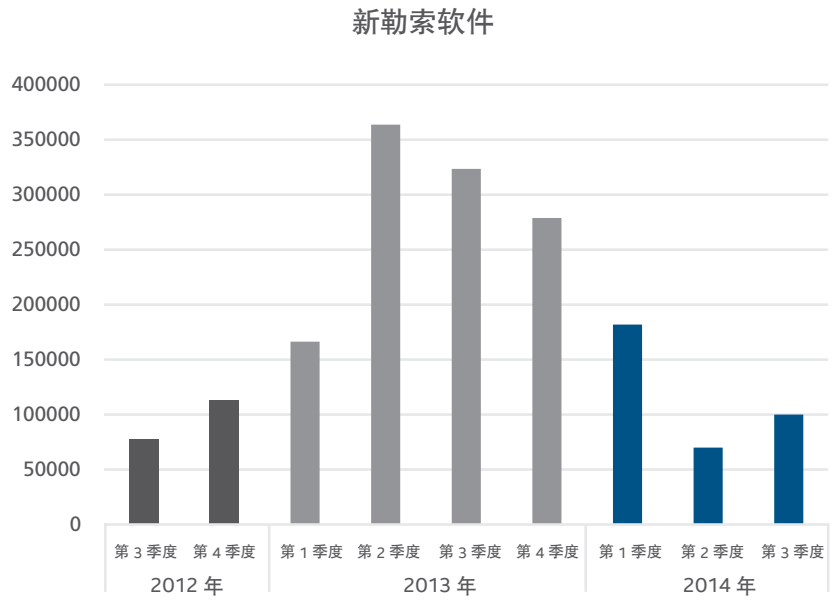
2014 年第三季度，McAfee Labs 恶意软件库样本数突破 300 万大关，相较于去年同比增长 76%。



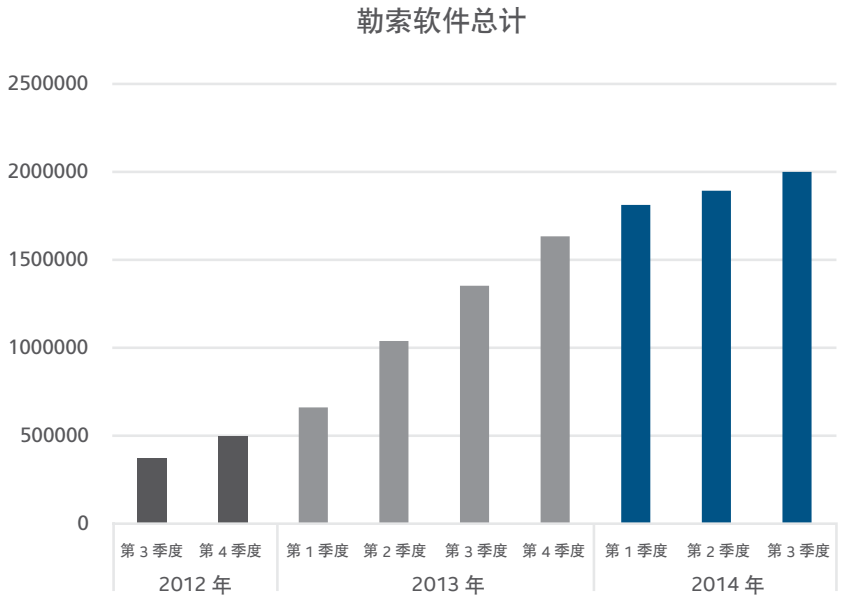
资料来源：McAfee Labs。

分享本报告

四个季度后，新勒索软件样本数停止滑落。我们对滑落趋势感到困惑，但对目前再次恢复增长并不感到惊讶。



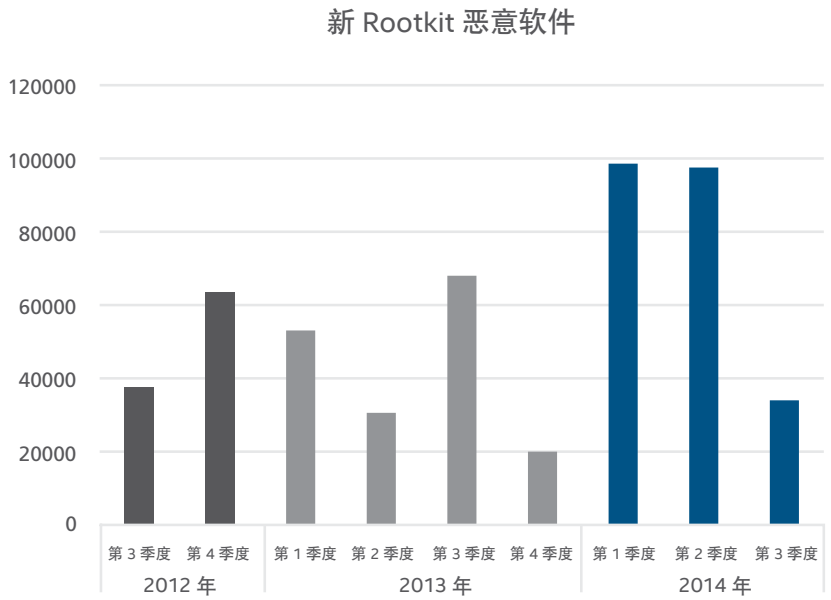
资料来源：McAfee Labs。



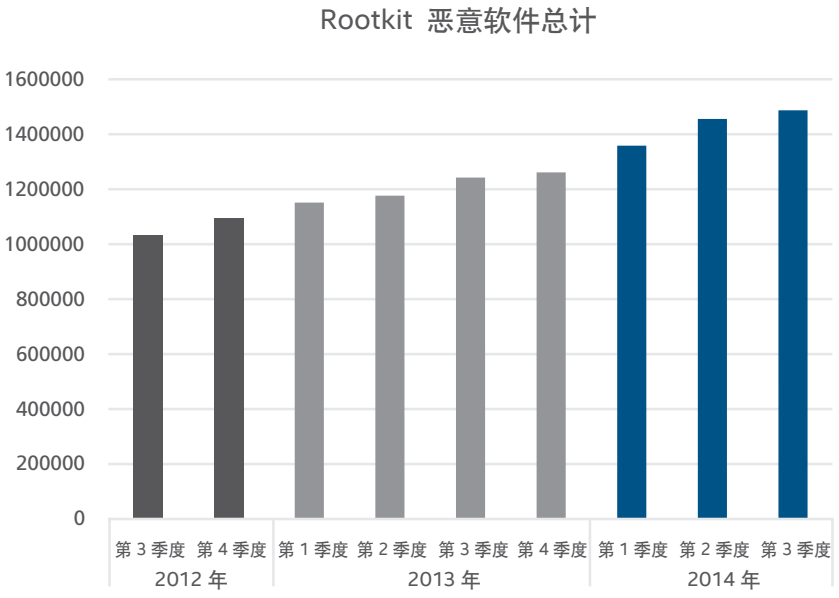
资料来源：McAfee Labs。

分享本报告

第三季度新 Rootkit 下降达 65%，充分反映出这种形式的恶意软件的波动性。



资料来源：McAfee Labs。

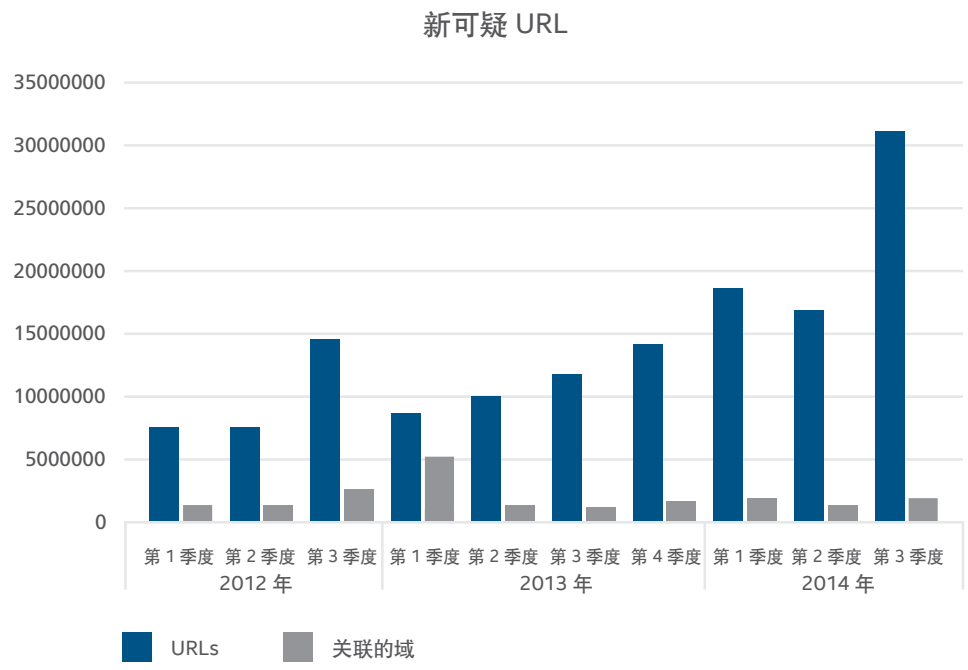


资料来源：McAfee Labs。

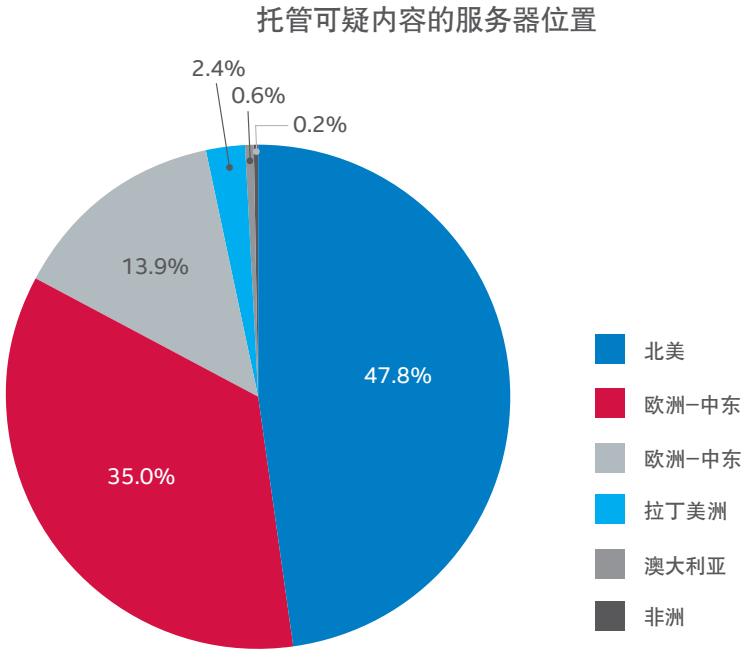
分享本报告

Web 威胁

本季度，新可疑 URL 数量猛增。部分增长可能由新短 URL 数量加倍导致，短 URL 往往会隐藏恶意网站，而网络钓鱼 URL 则急剧增加。



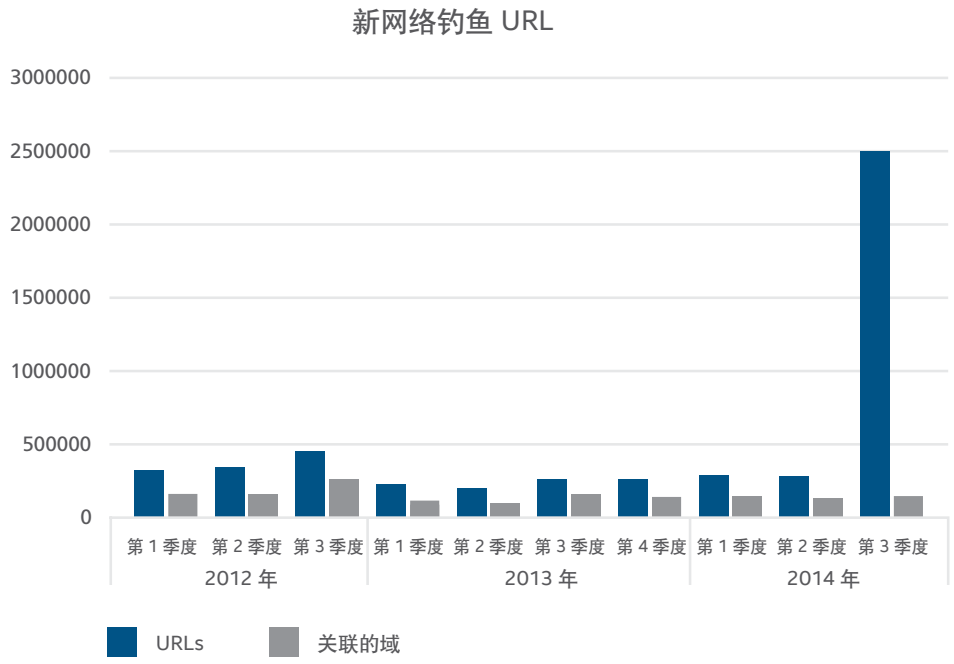
资料来源：McAfee Labs。



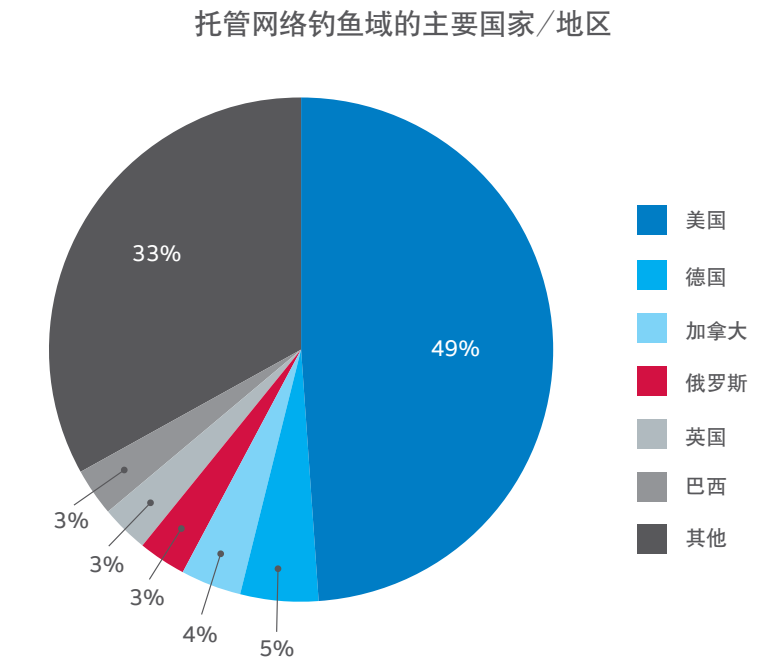
资料来源：McAfee Labs。

分享本报告

我们将本季度出现的极速增长态势主要归咎于俄罗斯药品垃圾邮件网络钓鱼活动，该活动会为每个接收者创建单独的子域。我们的数据收集功能将计入每一个子域。



资料来源：McAfee Labs。

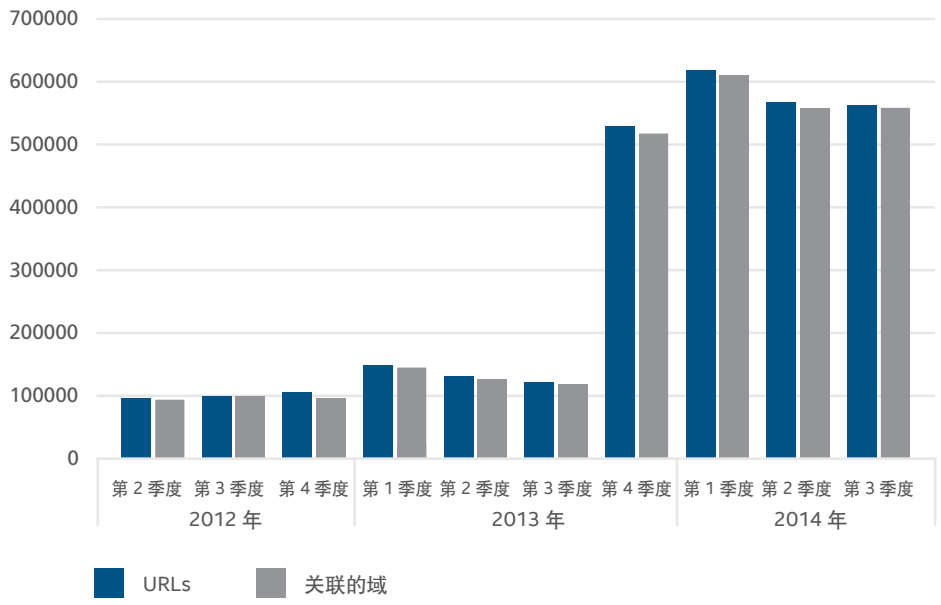


资料来源：McAfee Labs。

分享本报告

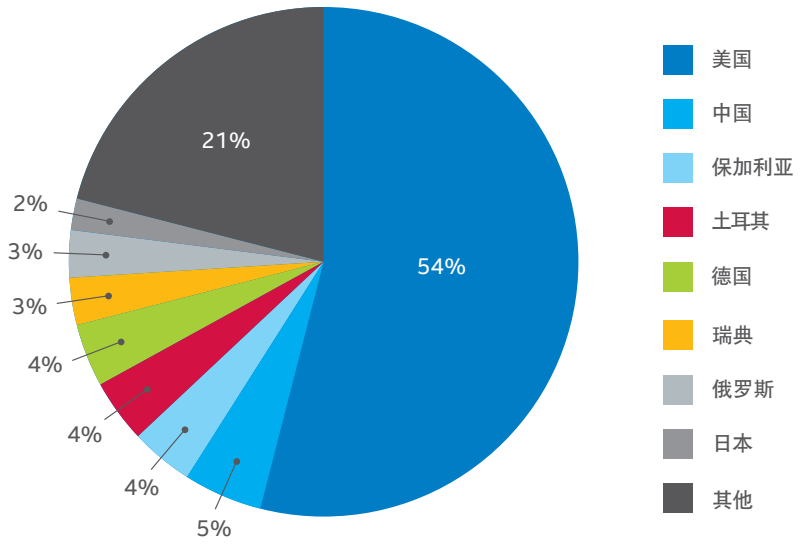
自本季度开始，我们将会统计全球新垃圾邮件 URL 计数。相较于第二季度，第三季度的新 URL 数量略微下降。由于我们对数据收集程序进行了改进，去年第四季度显现巨大飞跃。

新出现的垃圾邮件 URL



资料来源：McAfee Labs。

托管垃圾邮件域的主要国家／地区

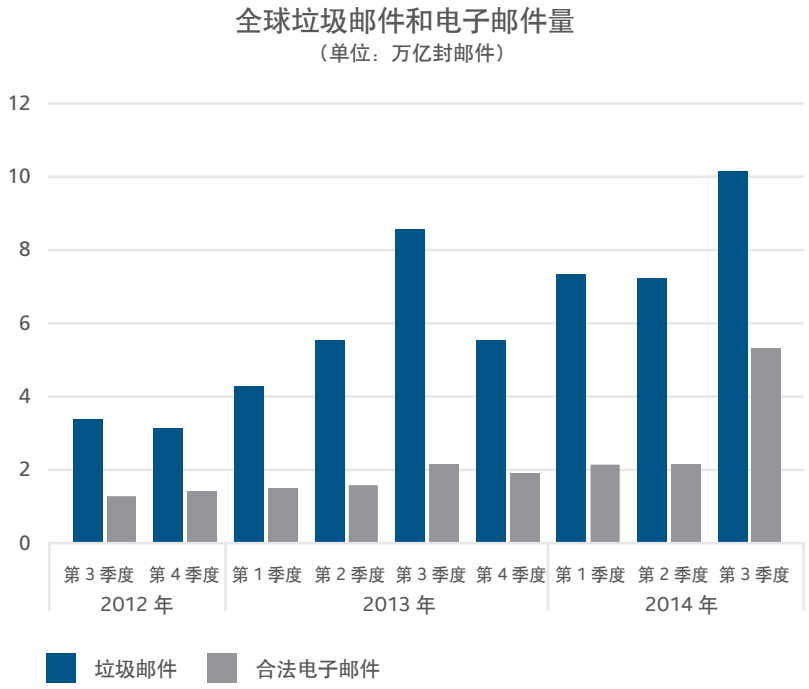


资料来源：McAfee Labs。

分享本报告

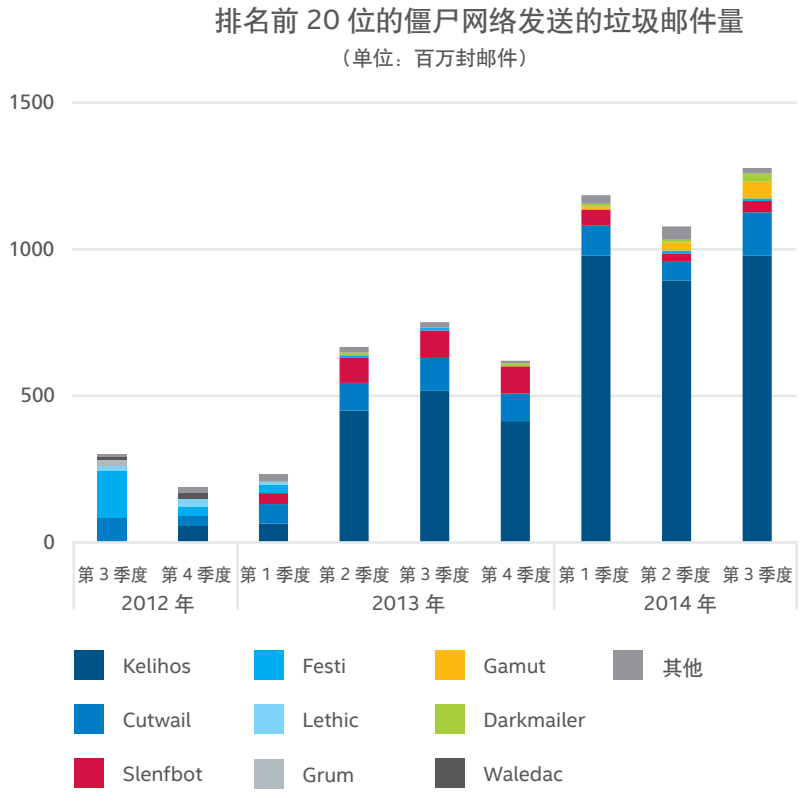
消息传递和网络威胁

由于对数据收集方式进行了改进，本季度的合法电子邮件增长高达 148%。该数字与过去几个季度的数据没有直接可比性，但我们可以在图中对邮件量进行更精确的历史评估。与此同时，垃圾邮件量增加了 40%。我们将部分增长归咎于数据收集方式，同时与客户群不断增长、僵尸网络日益猖獗及雪鞋垃圾邮件日渐增多脱不开干系。



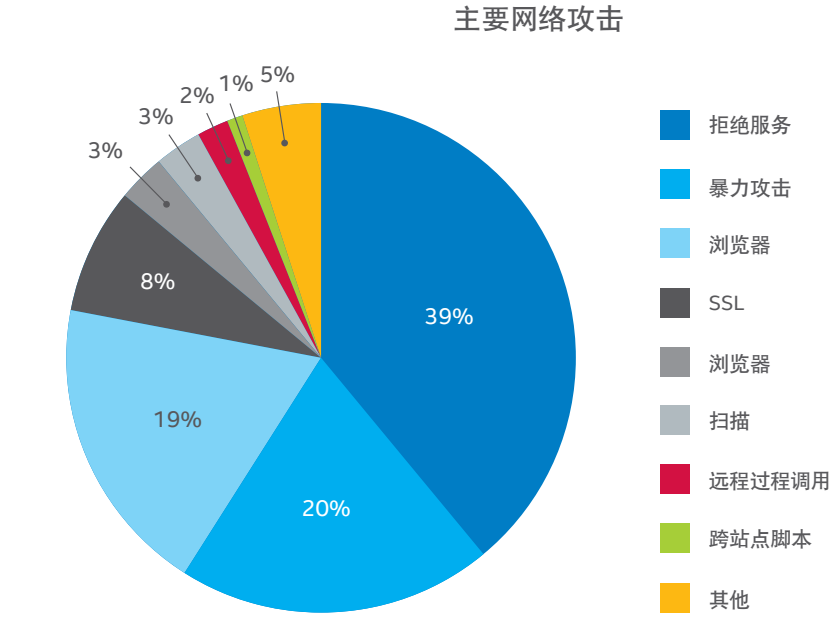
资料来源：McAfee Labs。

自本季度开始，我们将对排名前 20 位的垃圾邮件传播僵尸网络进行全新分解。Kelihos 成为本年度最高产的僵尸网络。第三季度，Kelihos 电子邮件占到前 20 位僵尸网络生成的垃圾邮件总数的76%。最近，Kelihos 逐渐与业务改进垃圾邮件（“8 大简单规则解析 B2B 销售本质”）、药品垃圾邮件（“购买廉价药品，费用节省高达 70%”）和快速致富垃圾邮件（“短短一天赚取 376 美元？是真的吗？立即检验”）。Kelihos 分布广泛，本年度垃圾邮件发送 IP 遍布 226 个国家/地区。



资料来源：McAfee Labs。

本季度最热门的三种威胁占到全部威胁的 78%。第三季度，SSL 攻击跃升至 8%，相较于第二季度增长 5%。这一增长很可能与 Heartbleed 的持续大规模爆发有关。



资料来源：McAfee Labs。

分享本报告

反馈。为帮助指导我们以后的工作，我们殷切希望得到您的反馈意见。如果您愿意分享您的观点，请**单击此处**填写一份五分钟的快速威胁报告调查。

关注 McAfee Labs

关于 Intel Security

迈克菲现在是 Intel Security 的一部分。英特尔安全凭借其 Security Connected 战略（创新型硬件增强安全解决方案和独特的 Global Threat Intelligence）致力于开发具有前瞻性且经实践验证的安全解决方案和服务，保护用作商业或个人目的的全球系统、网络和移动设备。Intel Security 将迈克菲的安全经验和专业知识与英特尔的创新和可靠性能相结合，使安全性成为每种体系结构以及每个计算平台的基本要素。Intel Security 的使命是让每位用户放心地在数字世界中安全可靠地工作生活。

www.intelsecurity.com

McAfee. Part of Intel Security.

北京市朝阳区建国路 91 号金地中心 A 座 37 层 邮编：100022 电话：(8610) 85722000 传真：(8610) 85752299

上海市西藏中路 268 号上海来福士广场办公楼 2006 室 邮编：200001 电话：(8621) 23080699 传真：(8621) 63406606

广州市天河区体育东路 118 号财富广场西塔 15 楼 106 室 邮编：510620 电话：(8620) 38860668 传真：(8620) 38860638

销售热线：800-810-0369 www.intelsecurity.com

61504rpt_qtr-q3-2015-predictions_1214_fnl_PAIR