Symantec | 赛门铁克安全解决方案

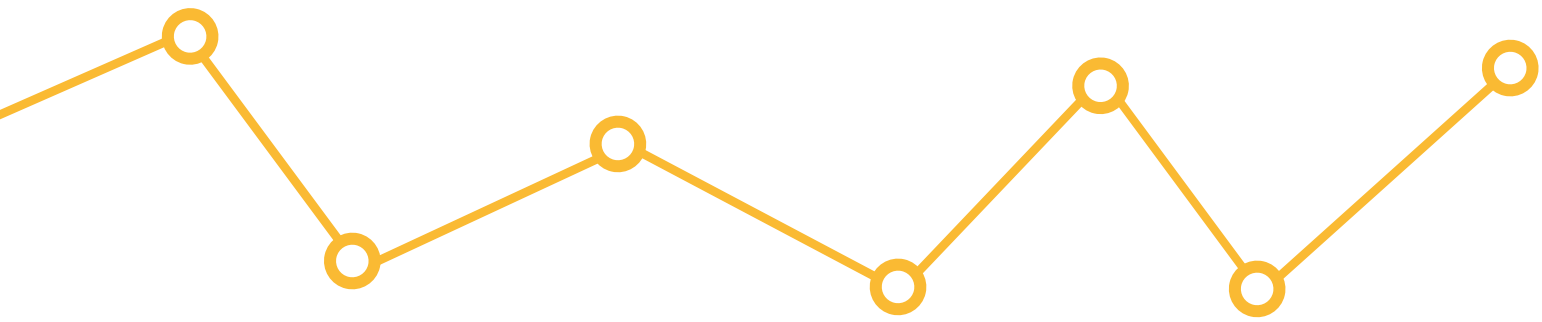
Norton SECURED powered by Symantec


# 网站安全威胁报告

## 第 1 部分

# 目录





# 简介

赛门铁克通过其全球智能网络拥有全球最全面的网络威胁数据资源。该智能网络由超过 4,150 万个攻击感应器组成，每秒钟可记录数以千计的事件。

通过结合以下赛门铁克产品和服务，该网络可以监控超过 157 个国家和地区的威胁活动：

- 赛门铁克 DeepSight™ 威胁管理系统
- 赛门铁克托管安全服务
- 诺顿产品
- 赛门铁克网站安全解决方案
- 其他第三方数据资源

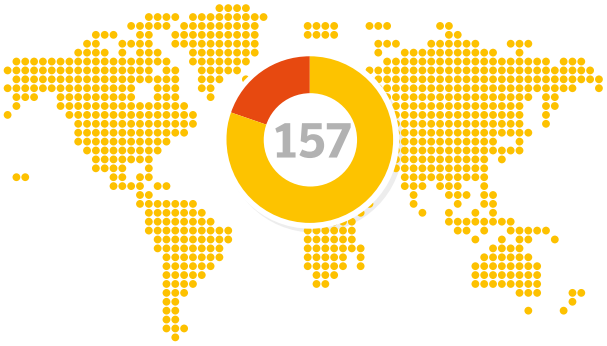
此外，赛门铁克所维护的漏洞数据库是世界上最完整的漏洞数据库之一，涉及超过 19,000 家供应商提供的 54,000 多款产品的 60,000 多条有记录的漏洞。

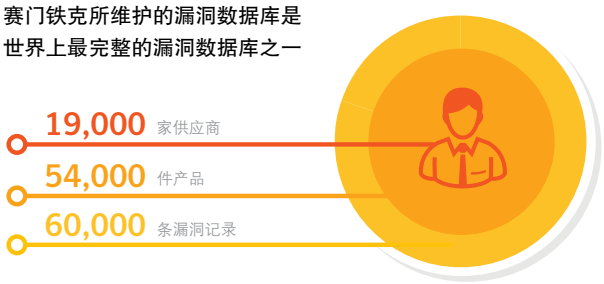
**赛门铁克通过以下来源检测垃圾邮件、网络钓鱼和恶意软件数据：**

- 拥有超过 500 万个诱骗帐户的赛门铁克探查网络
- Symantec.cloud（赛门铁克云服务）
- 赛门铁克网络安全解决方案
- 防止恶意软件与漏洞攻击产品
- 其他众多赛门铁克安全技术

Skeptic™ 是 Symantec.cloud（赛门铁克云服务）专有的启发式技术，能在复杂的新型目标性威胁抵达客户网络之前侦测到。每月可处理超过 84 亿封电子邮件，每天可过滤 14 个数据中心超过 17 亿的 Web 请求。

赛门铁克网站安全解决方案提供 100% 的可用性，并且每天可处理超过 60 亿次的在线证书状态协议 (OCSP) 查找，该查找服务可用于获取全球 X.509 数字证书的撤销状态。这些资源可为赛门铁克的分析人员提供无可比拟的数据来源，供其对攻击、恶意代码活动、网络钓鱼和垃圾邮件的新趋势进行识别和分析，并做出知情评论。





《赛门铁克网站安全威胁报告》由此诞生，为企业、小型公司和个人用户提供重要信息，在现在和将来有效地保护他们的系统安全。

# 执行摘要

2014 年最轰动的业内事件当然要属撼动了互联网安全的基础的 Heartbleed（心脏出血）漏洞。这一漏洞的重点不是罪犯的狡诈，而是人类制造的软件固有的缺陷。它提醒所有人必须提高警惕、更好地实施安全措施，并更加努力地保障网站安全。

当然，当 Heartbleed 登上头条时，罪犯们仍然在拼命创造利用、盗窃和破坏的机会。2014 年，罪犯危害企业和个人的手段变得更加专业、复杂、咄咄逼人。

### 漏洞让我们所有人都像被暴露在外

Heartbleed 并不是 2014 年出现的唯一漏洞。Poodle 和 Shellshock 也为罪犯提供了利用网站访问服务器、盗窃数据和安装恶意软件的途径。

有趣的是，在 2014 年发现的存在恶意软件的网站数量锐减一半，降到了 1/1126。不过，四分之三被扫描的网站存在漏洞，与去年的比例相同。这也许在一定程度上归结于网络安全的提高，但也可能是因为罪犯专注于利用其他方式投放恶意软件，例如社交媒体和恶意广告。

遗憾的是，很多人没有为自己的设备和服务器上运行的软件安装漏洞修补程序，这等于为那些利用漏洞的罪犯打开方便之门。攻击者往往使用一种专门的“安放工具”。这种工具可能会通过偷渡式 (drive-by) 攻击或社交媒体欺诈来投放，它会扫描一系列已知漏洞，一旦发现未安装修补程序的安全漏洞就会加以利用。

### 网络罪犯的手段更趋高明

2014 年，网络罪犯的手法更趋复杂，在专业划分、服务提供者和波动的市场方面都借鉴了合法的技术行业。

例如，只需每周 100 至 700 美元的价格，就能租到一个包含更新和全天 24 小时支持的网络偷渡式下载工具包。分布式拒绝服务 (DDoS) 攻击的订购价为每天 10 至 1000 美元不等[1]；至于买方市场，信用卡信息的售价是每张卡 0.50 至 20 美元，而 1000 个社交网络关注者的价格仅需 2 至 12 美元。

### 攻击手段没有道德、咄咄逼人

网络罪犯素来对受害者冷漠无情，但是在 2014 年，他们的恶意行为更是变本加厉。

仅五月至九月期间，赛门铁克就发现加密恶意软件 (cryptoware) 增加了 14 倍。[2] 这种软件是勒索恶意软件的变种，可对受害者的文件（包括照片、合同、发票等各种文件）进行加密，并持有解密所需的密钥，继而进行勒索。受害者往往会被要求使用 Tor 网页以比特币支付，因此几乎不可能追踪和封锁骗局背后的罪犯。

社交媒体和网络钓鱼骗局还试图利用人们对黑客攻击和健康恐慌事件的恐惧来引诱他们点击；骗徒获得的好处是加入按点击量、注册量和恶意软件下载量获取酬金的联盟营销计划，这些伎俩进一步利用受害者或他们上当后在链接指向的钓鱼网站上填写信息时收集到的数据。

[1] http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services

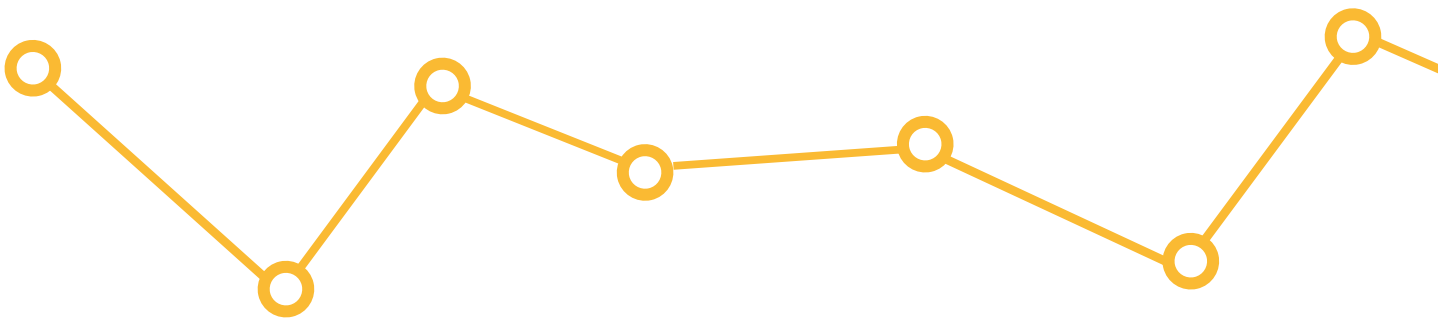
[2] http://www.symantec.com/connect/blogs/australians-increasingly-hit-global-tide-cryptomalware

# 网络威胁

# 一览

| | |
|---|---|
| 1 | Heartbleed 漏洞导致大约五十万个受信任的网站在四月份陷入严重的数据泄露风险中。[3] |
| 2 | 令人恐慌的 Heartbleed 事件引起了许多人的注意，并促使了 SSL 和 TLS 实施标准的提高。 |
| 3 | 罪犯正在利用合法广告网络创建的技术和基础架构，以传播恶意攻击和欺诈。 |
| 4 | 2014 年，匿名网站占受影响网站总数的比例猛增 5%，使这类网站成为全年受影响的主要十类网站之一。 |
| 5 | 发现存在恶意软件的网站总数比 2013 年几乎减少了一半。 |

[3] http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

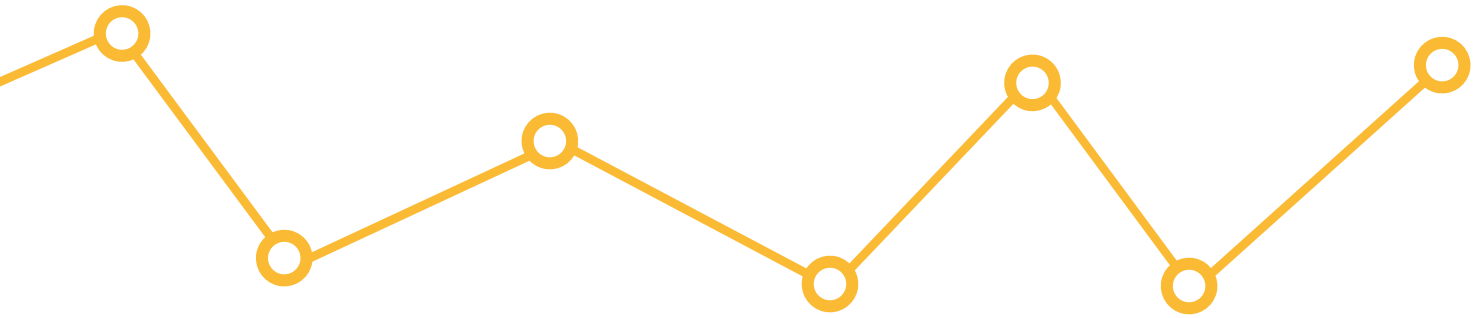


# 简介

2014 年，因为常用工具和加密协议中的漏洞纷纷暴露，罪犯的狡猾手法导致受害者更加难逃其魔掌，所以网络威胁的规模变得更大，势头也更凶猛。

2014 年的网络威胁呈现出极其严峻的形势，这一趋势将在 2015 年延续。漏洞和新的恶意软件变种突显出网络安全值得关键业务级的充分注意。

在撰写本文时，一个被称为 “FREAK” 的 SSL/TLS 新漏洞于 2015 年被几位安全研究员发现[4]。FREAK 使中间人可以攻击网站访问者和网站之间的加密通信，这最终使得攻击者能够截取和解密受影响的客户端与服务器之间的通信。在加密被攻击者破坏后，他们就能盗取密码和其他个人信息，并可能进一步攻击受影响的网站。



[4] http://www.symantec.com/connect/blogs/freak-vulnerability-can-leave-encrypted-communications-open-attack

# 著名漏洞

### Heartbleed 漏洞

Heartbleed 漏洞在 2014 年 4 月成为轰动新闻，该事件揭示了 OpenSSL 加密软件库中的漏洞意味着，攻击者能够访问在一段加密会话的过程中存储在网络服务器内存里的数据。该会话数据可能包括信用卡资料、密码，甚至是可以解锁整个加密交换的私钥。[5]

据估计，当时 Heartbleed 漏洞影响了 17% 的 SSL 网络服务器，这些服务器使用受信任证书颁发机构颁发的 SSL 证书和 TSL 证书。[6] 该漏洞对企业和个人造成了巨大的影响。

不仅有大量敏感数据陷入风险之中，而且必须向公众普及对该漏洞的教育，以便他们了解何时应当更新密码。网站所有者必须首先将服务器更新为安装了修补程序的 OpenSSL 版本，然后安装新的 SSL 证书，最后撤销旧的证书。只有这样，针对威胁而进行的密码更改才会有效，而向普通大众传达这些知识却颇有难度。

幸运的是，当时的响应相当迅速。在五天之内，Alexas 排名 1000 之内的网站没有一个受到 Heartbleed 漏洞的威胁，而排名 50000 以内的网站只有 1.8% 没有摆脱该漏洞的威胁。[7]

### ShellShock 和 Poodle

Heartbleed 并不是 2014 年网络生态系统中出现的唯一漏洞。同年 9 月，有人发现，一个名为 Bash Bug 或 ShellShock 的漏洞影响了大多数版本的 Linux 和 Unix，以及 Mac OS X。ShellShock 是一个很好的例子，它突显了对网站所有者而言安全形势的变化之快：今天，他们的服务器很安全地安装了修补程序，并且处于最新状态，但到了第二天突然就变得不再安全，原本的许多修补程序不再完整，需要重新安装。

网络服务器是最容易下手的攻击途径，因为攻击者可以利用通用网关接口（一种广泛用于生成动态网络内容的系统，简称 CGI）将恶意命令添加到环境变量中，包含漏洞的服务器组件 Bash 会解读和运行这个变量。[8]

大量威胁利用了 ShellShock，使服务器及其连接的网络暴露于可以感染和窥探多台设备的恶意软件。

然后，随着 Google 发现了一个名叫 Poodle 的漏洞，人们在十月份将目光再次投向加密。该漏洞有可能导致罪犯能够利用仍然支持较旧 SSL 协议（即 SSL 3.0）的服务器，利用的方式是干扰协议“握手”阶段（该阶段验证服务器可以使用哪一种协议），迫使它使用 SSL 3.0，即使服务器支持更新的协议。[9]

一旦成功利用，攻击者就能发动中间人攻击，以解密安全的 HTTP cookie，继而盗取信息或控制受害者的在线账户。幸运的是，该漏洞的严重程度不及 Heartbleed。为了利用 Poodle 漏洞，攻击者必须能够访问客户端和服务器之间的网络，例如通过公共 Wi-Fi 热点进行访问。

[5] http://www.symantec.com/connect/blogs/heartbleed-bug-poses-serious-threat-unpatched-servers
[6] http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html
[7] http://www.symantec.com/connect/blogs/heartbleed-reports-field
[8] http://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability
[9] http://www.symantec.com/connect/blogs/poodle-vulnerability-old-version-ssl-represents-new-threat

# 著名漏洞

### 著名漏洞和安装修补程序的时间

上述漏洞被公布之后随即发生的攻击本身也是轰动新闻，只不过在方式上有别于那些引人瞩目的零时差漏洞。Heartbleed 和 ShellShock 可一起被视为不同类的漏洞，更多地被用来危害服务器而不是终端。这两个著名漏洞的关键因素是它们影响的软件十分广泛，涉及多种系统和设备。这两个漏洞因为广泛存在而立即成为攻击者热衷的目标，而且都在被透露之后的若干小时内即遭到利用。

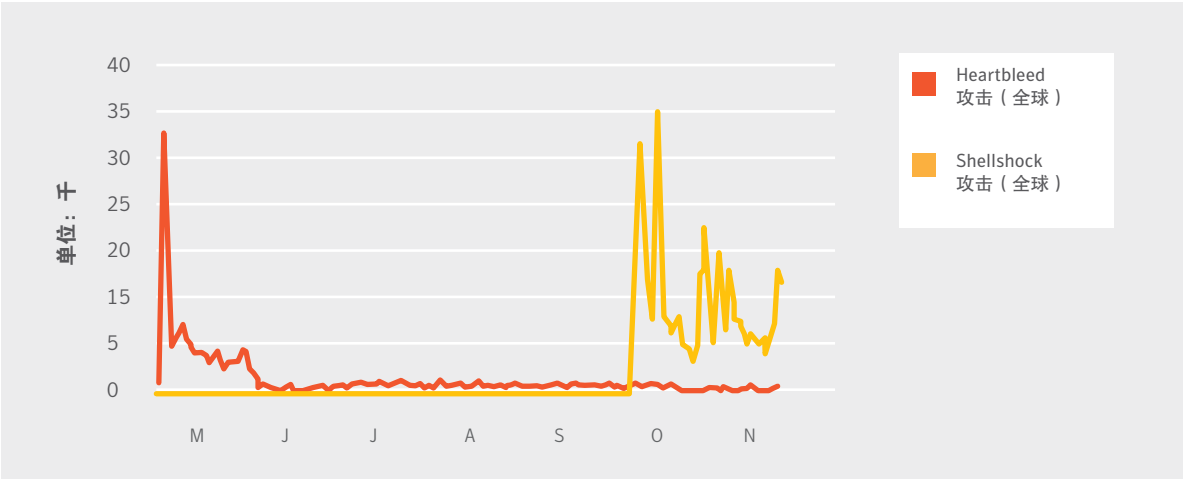
这些攻击的剧增表明，虽然采用赛门铁克签名来检测和阻止几乎在透露之后立刻发生的攻击，但是已经有大量攻击正在进行中。攻击者在 Heartbleed 漏洞被公布之后的 4 小时内就能够对其加以利用。

### SSL 证书和 TLS 证书仍然对安全至关重要

值得注意的是，虽然在线安全在 2014 年曾被撼动，但是 SSL 证书和更现代的 TLS 证书仍然行之有效，而且不可或缺。实际上，Heartbleed 事件恰恰证明了在线安全行业能够迅速应对这些威胁。

由于 CA 浏览器论坛（赛门铁克是该论坛的成员之一）等组织的努力和警觉，行业标准也在不断改善。换言之，为您的网站和网站访问者提供安全保障的互联网安全的根基仍然强大，并将越来越强。

## 全球 HEARTBLEED 和 SHELLSHOCK 攻击（2014 年 4–11 月）



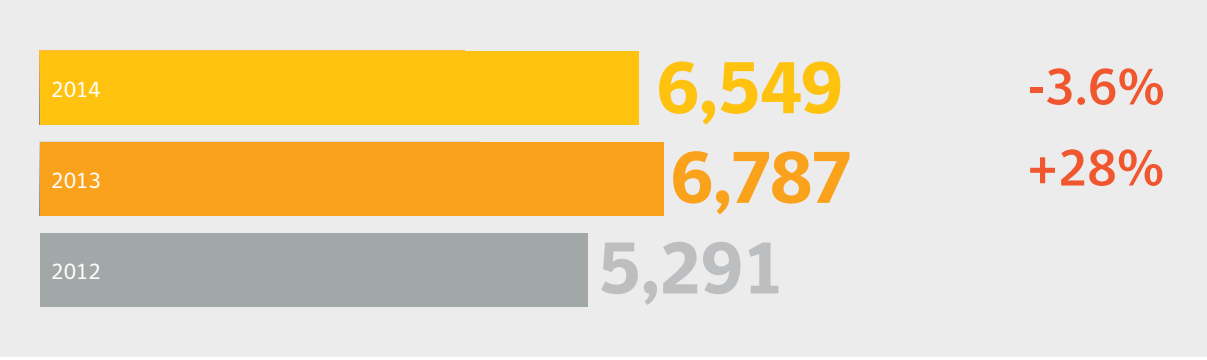

来源：赛门铁克

# 漏洞纵览

虽然每年的浮动幅度较小，但漏洞数量继续呈上升趋势。绝大多数被报告的漏洞都有补救办法、变通方法或修补程序。然而，恶意软件的制作者知道很多人不会去应用这些更新，因此他们在攻击当中可以利用那些记载充分的漏洞。在许多情况下，专门的“安放工具”用来扫描多种已知漏洞，并利用未安装修补程序的安全漏洞作为安装恶意软件的后门。当然，这突显了应用更新的重要性。

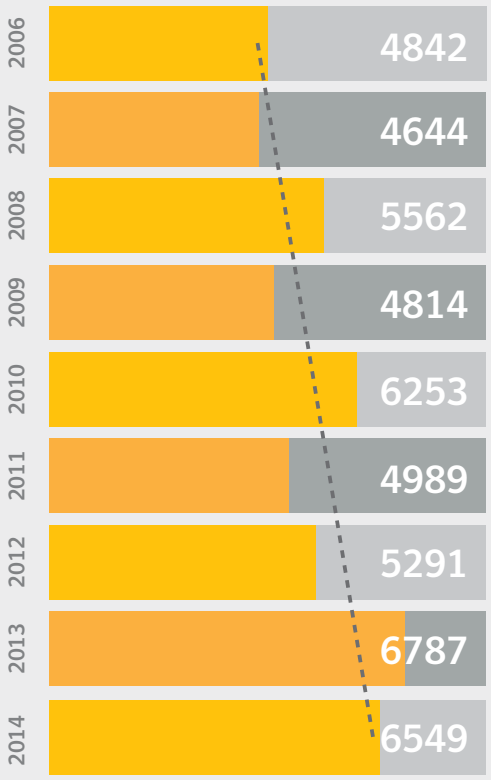
Sakura、Blackhole 等网络漏洞利用工具包就是这样让攻击者更容易利用数月前甚至几年前发布的未安装修补程序的漏洞。对于每个漏洞，攻击者可以利用多次，而网络攻击工具包首先会对浏览器进行漏洞扫描，以确定可能存在漏洞的插件以及最适合发动的攻击。如果使用旧的漏洞利用工具就足以利用新的漏洞，很多工具包不会使用最新的漏洞利用工具。针对零时差漏洞的利用工具并不常见，深受攻击者追捧，尤其是用于水坑式 (watering hole) 目标性攻击。

## 新漏洞



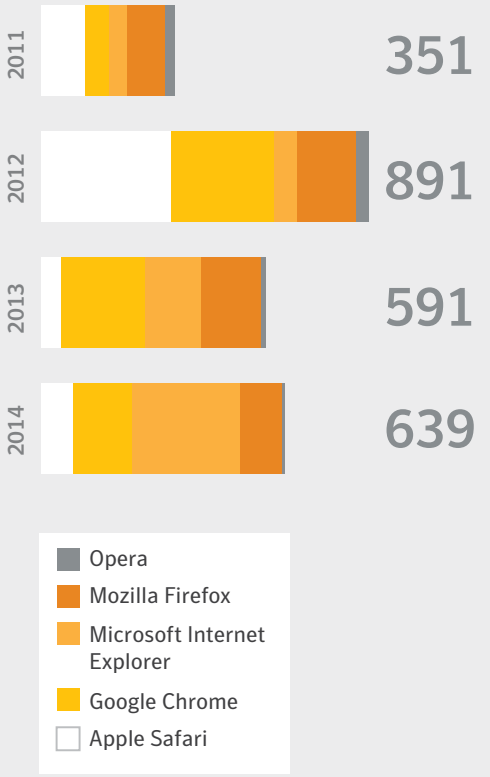

来源：赛门铁克 | Deepsight

## 漏洞总数（2006–2014 年）



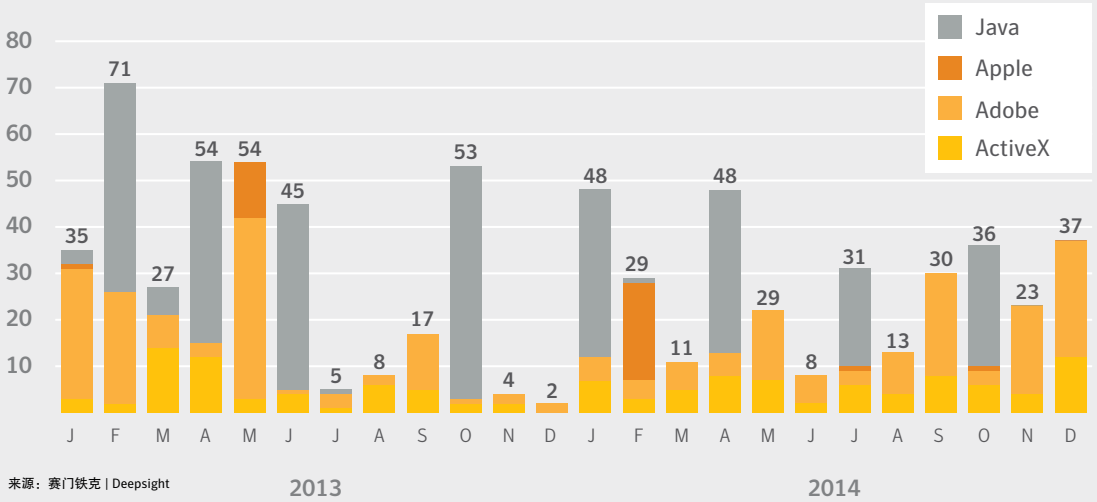

来源：赛门铁克 | Deepsight

## 浏览器漏洞（2011–2014 年）




来源：赛门铁克 | Deepsight

## 各个月份的插件漏洞（2013–2014 年）




来源：赛门铁克 | Deepsight

虽然被报告的漏洞存在一般风险，但零时差漏洞的危害可能要严重得多。这种漏洞只有在被攻击者利用之后才会被发现。请查看“目标性攻击”章节，了解关于零时差漏洞的更多介绍。

# 受害网站

在 2014 年被赛门铁克扫描的所有网站中，大约四分之三被发现存在漏洞，这一比例与前一年相同。然而，被划分为“关键”(critical) 级别的漏洞比例从 16% 上升到了 20%。

与前一年相比，实际发现存在恶意软件的网站数量大大减少，比例从 1/566 降低到 1/1126。这似乎对每天阻止的网络攻击数量产生了连锁效应。每天阻止的网络攻击数量也减少了，但降幅仅 12.7%，说明 2014 年平均每个受影响网站对应的攻击数量增加了。其中一个原因是，某些网络攻击工具包被设计成用于云端，如软件即服务 (SaaS)。例如，受害网站可能使用 HTML iframe 标签或一些混乱的 JavaScript 注入基于 SaaS 的漏洞利用工具包的恶意代码，而不是通过受害网站上的漏洞利用代码直接发动恶意攻击。这种基于 SaaS 的漏洞利用工具包的增加还体现在用于寄存恶意软件的恶意域名新增数量减少，从 2013 年的 56,158 个减到 2014 年的 29,927 个，降幅为 47%。

网络攻击工具包对受害者的电脑进行扫描，查找易受攻击的插件来发动最有效的攻击。此外，这些基于 SaaS 的工具包通常位于防御严密的主机服务上，IP 地址可以迅速改变，域名可以动态生成，因此更难找到恶意 SaaS 基础架构的位置并将其关闭。攻击者还可以控制如何实施漏洞利用，例如只在最初受害网站已设置 cookie 的前提下实施攻击，让恶意代码避开搜索引擎和安全研究员的窥探。网络攻击工具包将在本章稍后详细讨论。

关于最常遭到利用的网站类型，有一个耐人寻味的现象：匿名网站也包括在今年的十大网站类型之中。这也许是罪犯追随大流的又一个实例，因为越来越多的人尝试规避互联网服务供应商 (ISP) 和其他人的追踪，并提高浏览隐私。

## 网络服务器上未安装修补程序的十大漏洞

| 级别 | 名称 |
|---|---|
| 1 | SSL/TLS POODLE 漏洞 |
| 2 | 跨站点脚本 |
| 3 | 检测到支持 SSL v2 |
| 4 | 支持 SSL 弱密码套件 |
| 5 | SSL 证书链无效 |
| 6 | 加密会话 (SSL) Cookie 中缺少安全属性 |
| 7 | SSL 和 TLS 协议重新谈判漏洞 |
| 8 | PHP 'strrchr()' 函数信息泄露漏洞 |
| 9 | http TRACE XSS 攻击 |
| 10 | OpenSSL 'bn_wexpend()' 错误处理未指定漏洞 |

来源：赛门铁克 | 可信服务

## 扫描到存在漏洞的网站

**76%**
2014

-1%

**77%**
2013

+25%

**55%**
2012

来源：赛门铁克 | 可信服务

## “关键”级别的比例

**20%**
2014

+4%

**16%**
2013

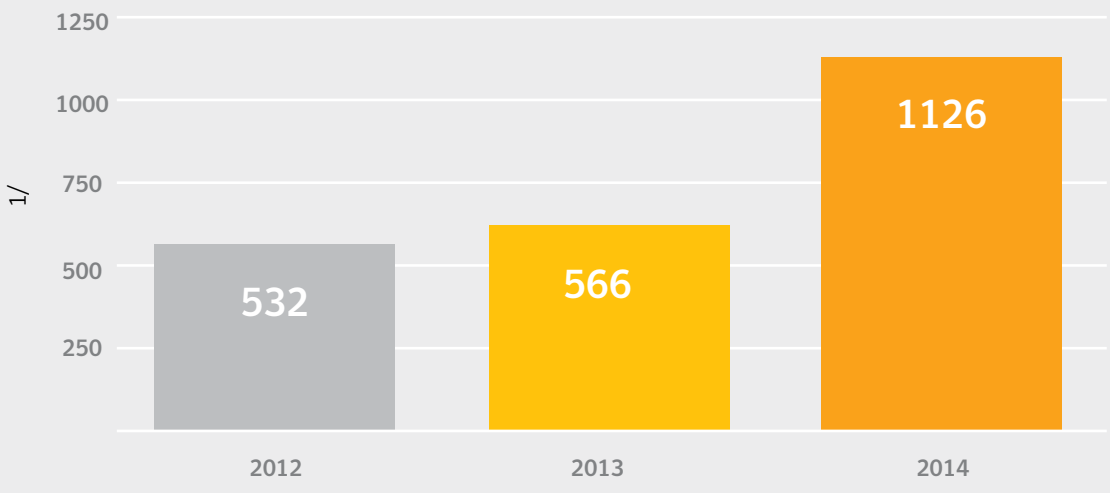
+8%

**24%**
2012

来源：赛门铁克 | 可信服务

*2014 年，在合法网站上发现的所有漏洞中，平均每 5 个漏洞就有一个（即 20%）被认定为关键漏洞，这些漏洞让攻击者可访问敏感数据、篡改网站内容或损害访问者的电脑。*

## 发现存在漏洞的网站



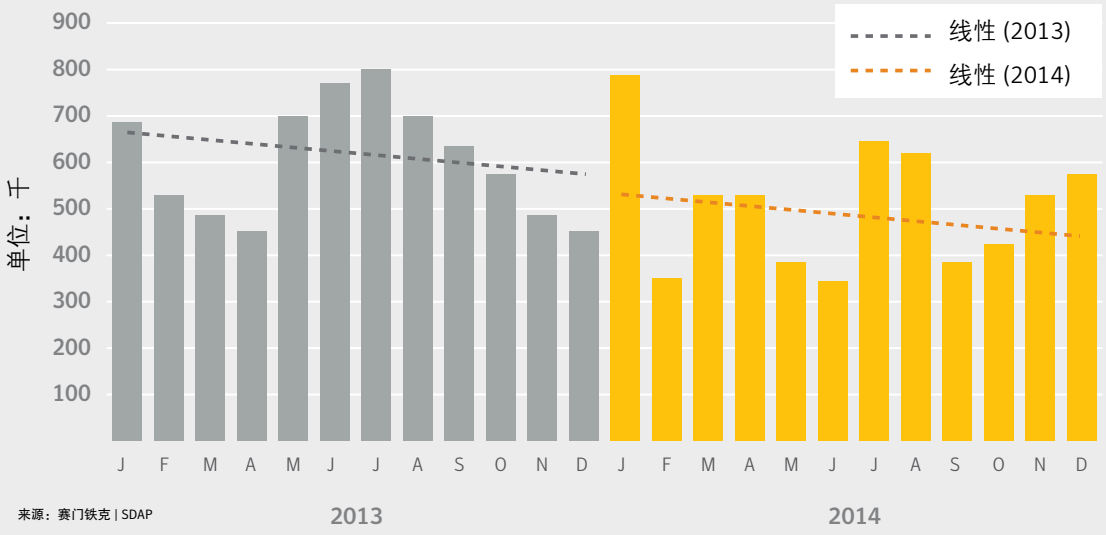

来源：赛门铁克 | 可信服务

## 2013-2014 年最常遭到利用的网站分类

| 排名 | 2014 年最常遭到利用的 10 大网站类型 | 占 2014 年受感染网站总数的百分比 | 2013 年最常遭到利用的 10 大网站类型 | 占 2013 年受感染网站总数的百分比 |
|---|---|---|---|---|
| 1 | 技术 | 21.5% | 技术 | 9.9% |
| 2 | 托管 | 7.3% | 商务 | 6.7% |
| 3 | 博客 | 7.1% | 托管 | 5.3% |
| 4 | 商务 | 6.0% | 博客 | 5.0% |
| 5 | 匿名 | 5.0% | 非法 | 3.8% |
| 6 | 娱乐 | 2.6% | 购物 | 3.3% |
| 7 | 购物 | 2.5% | 娱乐 | 2.9% |
| 8 | 非法 | 2.4% | 汽车 | 1.8% |
| 9 | 占位符 | 2.2% | 教育 | 1.7% |
| 10 | 虚拟社区 | 1.8% | 虚拟社区 | 1.7% |

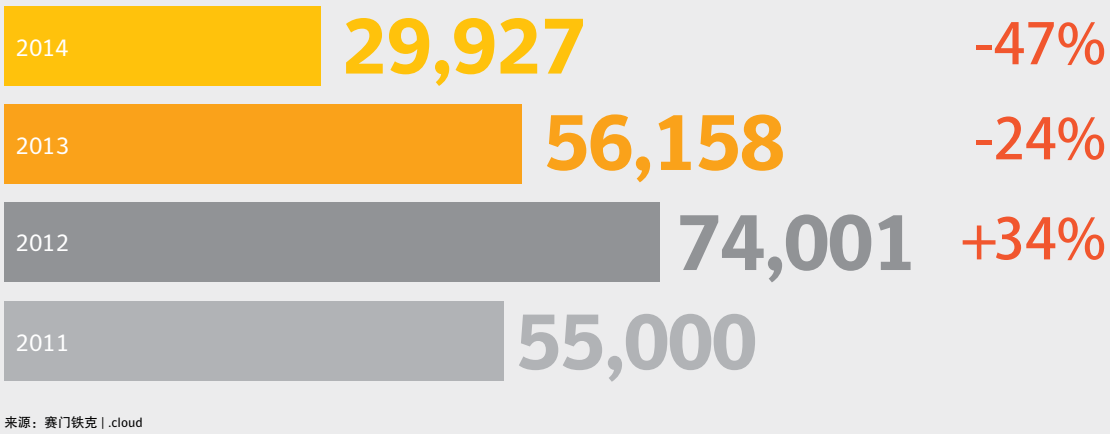
来源：赛门铁克 | SDAP, Safe Web, Rulespace

## 各个月份的被阻止网络攻击（2013–2014 年）




来源：赛门铁克 | SDAP

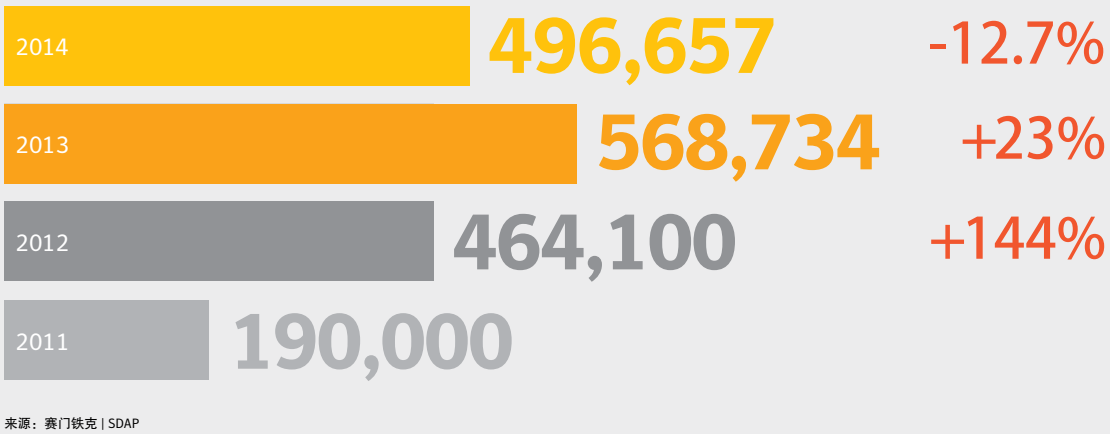
## 全新的恶意网域




来源：赛门铁克 | .cloud

*2014 年，恶意网域减少 47% 说明了基于云的软件即服务 (SaaS) 类工具包使用量的增加。*

## 每天阻止的网络攻击



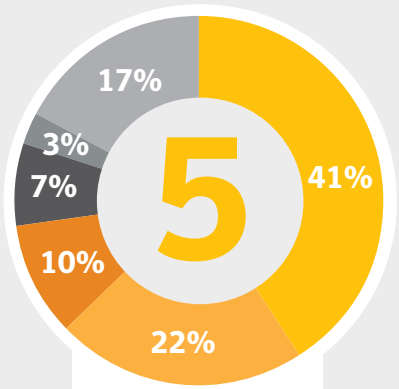

来源：赛门铁克 | SDAP

*在大多数情况下，平均每天阻止的攻击数量减少 12.7% 在很大程度上是因为 2013 年下半年的降幅，因为整个 2014 年的降幅小得多。*

大多数网站仍然存在漏洞，可见许多网站所有者没有掌握漏洞扫描的情况。不过，他们可能会更加留心那些有可能揭示恶意软件的恶意软件扫描。然而，这种恶意软件往往是在早前的漏洞利用之后安放的，所以预防总是胜于“治疗”。

易受攻击的网站为数众多，罪犯已经屡次得逞。很多罪犯还迅速利用了同样在 2014 年暴露的部分 SSL 漏洞和 TLS 漏洞。此外，2014 年社交媒体诈骗和恶意广告发生率的提高表明，罪犯已经开始从散播恶意软件改为采用其他方法。

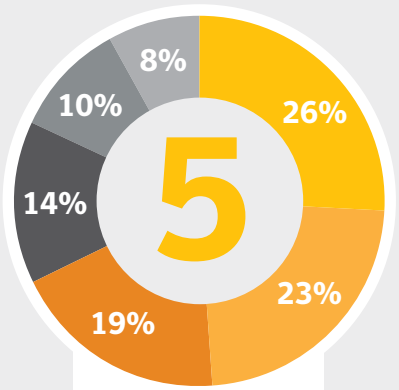
## 2012 年
## 五大网络攻击工具包




- Blackhole
- Sakura
- Phoenix
- Redkit
- Nuclear
- Others

来源：赛门铁克 | SDAP, Wiki

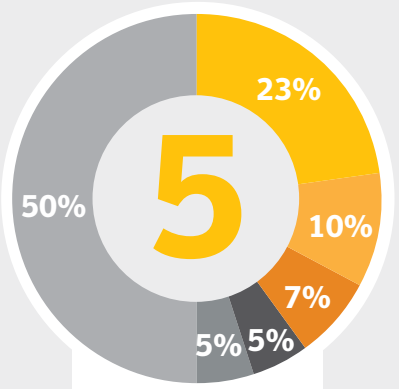
## 2013 年
## 五大网络攻击工具包




- Others
- G01 Pack
- Blackhole
- Sakura
- Styx
- Coolkit

来源：赛门铁克 | SDAP, Wiki

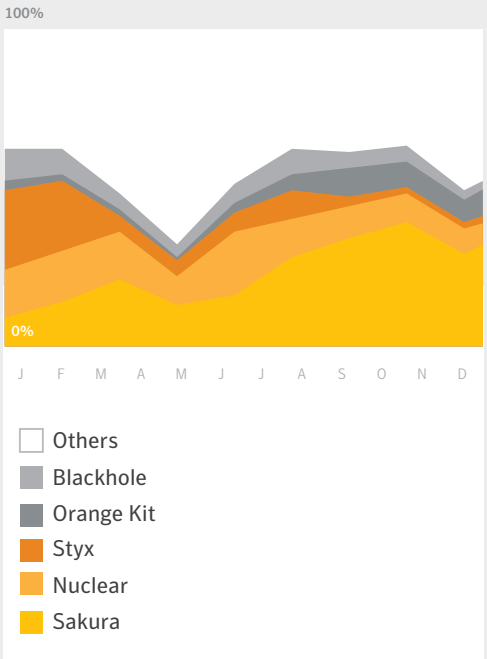
## 2014 年五大网络攻击
## 工具包




- Sakura
- Nuclear
- Styx
- Orange Kit
- Blackhole
- Others

来源：赛门铁克 | SDAP, Wiki

## 2014 年五大网络攻击
## 工具包使用时间线




- Others
- Blackhole
- Orange Kit
- Styx
- Nuclear
- Sakura

来源：赛门铁克 | SDAP, Wiki

# 恶意广告

踏入 2014 年，我们看到勒索软件和恶意广告产生了交集，被重新定向至 Browlock 网站的受害者人数达到了新高。

Browlock 本身是勒索软件攻击性较小的变种。它不是运行在受害者电脑上的恶意代码，而是利用 JavaScript 手段阻止受害者关闭浏览器选项卡的网页。该网站确定受害者的位置，然后呈现针对特定位置的网页，声称受害者因访问色情网站而违反了法律，并要求受害者向当地警方缴交罚款。

Browlock 攻击者似乎会向合法网络购买广告，从而为他们的网站吸引流量。广告被定向到成人网页，然后重定向到 Browlock 网站。Browlock 攻击者购买的流量来自若干来源，但是主要来源是成人广告网络 [10]。

受害者只要关闭浏览器就能逃离，但是罪犯为吸引流量而投入资金说明了人们选择付款了事。也许这是因为在进入 Browlock 网页之前，受害者点击了色情网站广告：愧疚心理可发挥强大的作用。

**恶意广告逍遥法外**

恶意广告帮助扩散的不仅仅是勒索软件，恶意广告还会重定向到安装特洛伊木马的网站。某些恶意广告能利用偷渡式攻击 (drive-by) 感染受害者的设备，哪怕用户并没有点击广告。

吸引罪犯的是，恶意广告可以命中大型合法网站，从而吸引到巨大的流量。广告网络在选择目标时往往还会是高度本地化的，这意味着罪犯可以针对具体的受害者（如搜索金融服务的人）量身打造他们的骗局。合法广告网络有时候会在无意中帮罪犯做好各方面的工作。

罪犯还会变换战术来避开检测。例如，他们会先连续几星期投放合法广告，制造出光明正大的假象，然后再转换成恶意广告。为了应对这些现象，广告网络需要定期扫描，而不是仅仅在新广告上传时扫描。

对网站所有者而言，恶意广告难以防范，因为他们无法直接控制广告网络及其客户。然而，网站管理者可以选择限制广告功能的网络，让广告商无法在促销广告中嵌入恶意代码，从而降低风险。当然，在选择广告网络时，进行尽责调查会大有帮助。


*Browlock 网页示例，要求为非法浏览色情网站而缴交罚款* [11]

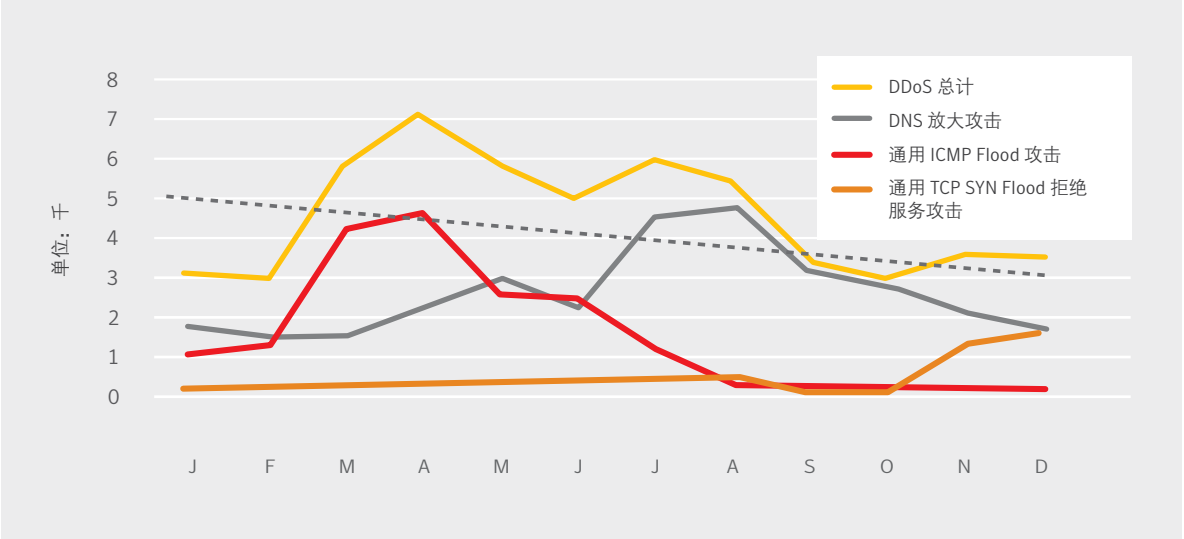
[10] http://www.symantec.com/connect/blogs/massive-malvertising-campaign-leads-browser-locking-ransomware
[11] Ibid

# 拒绝服务

拒绝服务攻击是攻击者针对个别组织发动攻击的又一种手段。通过让网站或电子邮件等关键系统服务超载来阻止对这些系统的访问，拒绝服务攻击可引发财务混乱、破坏正常运作。

分布式拒绝服务攻击 (DDoS) 早已不是新鲜事物，但如今愈演愈烈，并且更加频繁[12]。例如，赛门铁克发现，在 2014 年 1 月至 8 月期间，DNS 放大攻击次数增加了 183%[13]。Neustar 的一份调查显示，60% 的公司在 2013 年受到 DDoS 攻击的影响，其中 87% 不止一次遭到袭击[14]。攻击动机包括勒索金钱、掩护其他形式的攻击、黑客行动主义和报复。蓄谋发动拒绝服务攻击的人越来越容易在网上黑市以 10 至 20 美元的低价发动特定时长和特定强度的攻击。

**赛门铁克全球智能网络的 DDOS 攻击流量**




来源：赛门铁克 I DeepSight Symantec Global Intelligence Network

[12] http://www.symantec.com/connect/blogs/denial-service-attacks-short-strong
[13] http://www.symantec.com/connect/blogs/denial-service-attacks-short-strong
[14] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf

# 漏洞增加

**文：Tim Gallo**

在过去的几年里，漏洞管理这一概念是经常被讨论的话题，但它往往被视为令人烦恼的流程，或虽然有趣但不如漏洞响应或对手追踪那么重要。然而，2014 年生动地说明了漏洞的重要性。三大漏洞成为新闻，不仅是安全行业的新闻，还被大型媒体机构争相报道。这些漏洞的俗称分别是 Poodle、ShellShock 和 Heartbleed。

这些漏洞都是在当时多数漏洞管理流程一向没有覆盖的地方发现的。这些流程最近特别关注笔记本电脑和服务器，因为 Adobe 和 Microsoft 经常公布漏洞并且迅速发布修补程序。虽然我们已经看到并将继续看到新的漏洞在这些应用程序中出现，但是在修补程序部署、漏洞披露和整体的修补程序管理流程方面已经制定了可靠的流程。

操作系统和应用程序供应商采取的修补程序部署自动化迫使攻击者在战术上作出一定的转变。攻击者已改用新的漏洞利用方法，更准确的说法也许是，重拾漏洞研究的把戏。攻击者重新对应用程序进行更加彻底的梳理，结果是在以前被认为安全的地方发现了漏洞。

让我们以其中一个漏洞 ShellShock 为例，来探讨一下今后几年我们可能见到的情况。在 Bourne Again Shell (BASH) 里，[15]Shellshock 在最好的情况下是有缺陷的功能，在最差的情况下是设计缺陷。在被忽略了至少 25 年之后，BASH 被发现是可以利用的，并在随后被公之于众。对互联网上存在的大部分内容来说，Shellshock 一直是互联网的组成元素。实际上，Shellshock 的目标并不是只有路由器或 Linux 网络服务器，还有电子邮件服务器，甚至包括利用外壳程序 (shell) 的 DDoS 机器人程序 —— 也就是说，一切利用 BASH 的基于 Unix 的对象都可以成为它的目标。

*Heartbleed 漏洞甚至还有专门的标志。*

[15] 对于不熟悉 UNIX 术语的读者，“外壳程序”是用于与操作系统交互的命令行用户界面。这里提及的 BASH 是 UNIX 和 LINUX 世界里使用最广泛的外壳程序。

我们可能会继续看到类似这样的漏洞在未来几年里成为新的常态，原因包括以下几点。首先，现在已经很明显，攻击者不会依赖于反复使用同样的旧方法和旧的漏洞利用工具，而是会投资研究那些攻击面较广的常用旧基础架构中的新漏洞。

这三个重大漏洞的有趣之处还在于它们不仅暴露了互联网基础架构重要组件的缺陷，还突显了应用程序开发的其中一个不光彩的秘密：代码重用。代码重用是指开发人员复制既有应用程序中的部分代码，用在新应用程序的开发中。这种几乎从编码出现以来就一直存在的做法可能会导致也许完全不相关的系统里出现漏洞。

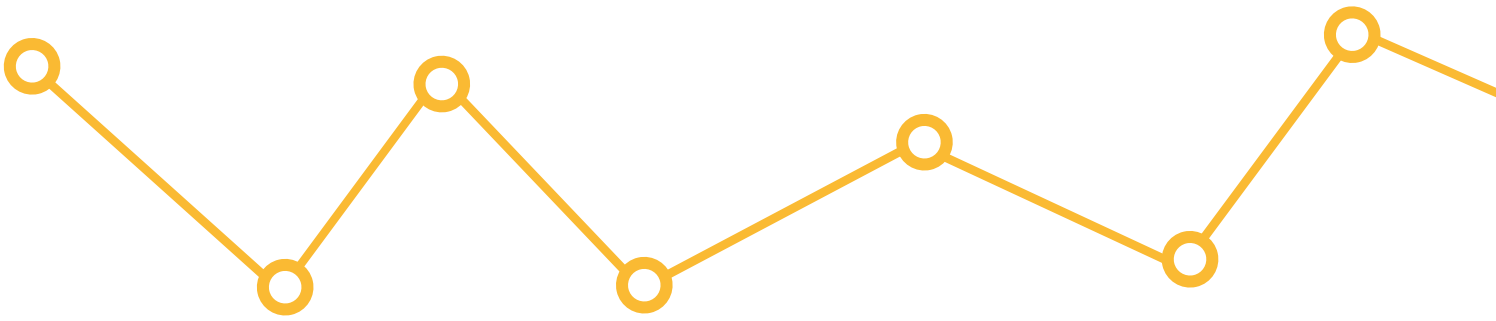
回顾当初引向发现 Heartbleed 漏洞的情形，对 OpenSSL 库的合法使用就是代码重用很好的例子。这种代码一直被视为可靠代码，而且常常未经测试，因为它被当成了“已经解决的问题”。然而，库里陆续发现新的漏洞，世界各地的开发人员不得不急急忙忙地去查明他们实施代码重用的地方有无漏洞。

此外，我们发现漏洞报告奖励计划增多，而政府也不再像多年以前那样威胁将漏洞研究者判刑入狱。[16] 因此，漏洞研究的诱因增加，而研究者也不再惧怕不负责任的泄露或完全唯利是图的行为造成的后果。

然而，我们也希望看到补救措施和更好的安全实践变得更加普遍。一般 IT 专业人员只需通宵工作几个星期就能确定提前计划会有利得多。在整个基础架构中更好地执行配置、政策并安装修补程序将大有帮助。将基础架构向云端转移也有助于工作负担过重的 IT 专业人员管理这些问题。

从安全性的“检测和补救”周期可以看出，漏洞重现是了解威胁态势的要点。如果我们想成为更加高效的安全专业人员，就必须另外考虑如何“保护和响应”以及“通知和评估”。这意味着我们需要更好地计划、测试，需要借助情报来帮助我们掌握信息，需要对我们的环境有足够的认识，以便了解情报是否具有切实可行的意义。

我们需要更好地理解互联网的结构可能仍然布满漏洞，而我们有责任保持警惕，以便在新漏洞被披露时以流程为导向、有计划地做好应对这些漏洞的准备。如果不这样做，就会对我们的未来产生不利影响。

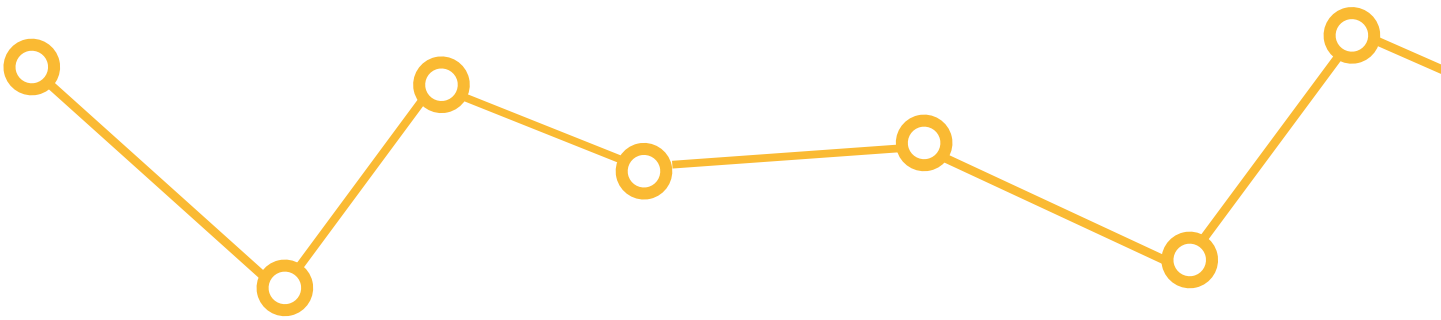


[16] http://www.wired.com/2013/03/att-hacker-gets-3-years

# 电子犯罪和恶意软件

# 一览

| | |
|---|---|
| 1 | 地下经济价格稳定，说明对被盗身份、恶意软件和电子犯罪服务的需求依然强劲。 |
| 2 | 漏洞数量比 2013 年有所下降，但整体仍然呈上升趋势。 |
| 3 | 2014 年新出现的恶意软件变种数量比 2013 年增加了 317,256,956 个，增长率为 26%。 |
| 4 | 勒索软件更趋卑劣，并且数量也在增加。加密勒索软件的数量也比 2013 年增加了 45 倍有余。 |
| 5 | 机器人程序数量在 2014 年下降了 18%。 |



# 简介

每天都有个人银行资料被虚假邮件和虚假网站以网络钓鱼的方式窃取。受恶意软件感染的电脑被用来发送垃圾邮件，或被利用来发动分布式拒绝服务攻击。最不走运的受害者会发现自己的文件被勒索软件加密、电脑被勒索软件影响到无法使用。

电子邮件继续充当垃圾邮件、网络钓鱼和恶意软件的有效传播渠道，而在整体上，含有恶意软件的电子邮件比例正在上升。网络罪犯依靠地下网络经济来购买和售卖服务和恶意软件，以及非法买卖被盗信用卡和僵尸网络。

执法机关与包括赛门铁克在内的安全机构合作，继续瓦解僵尸网络和逮捕犯罪分子。这明显改善了网络犯罪的整体状况，哪怕只是暂时的改善。

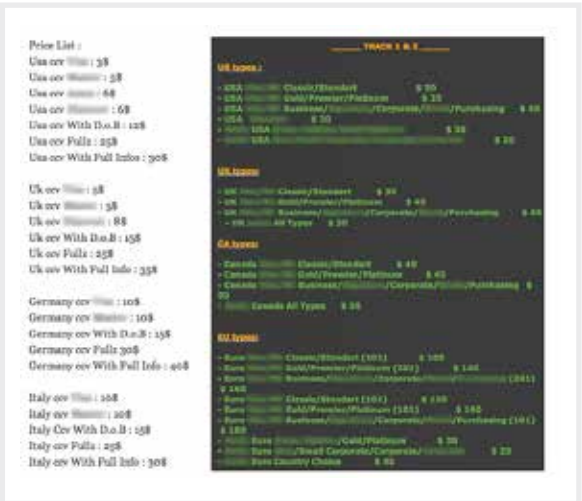
### 地下经济

地下黑市十分猖獗。在互联网的阴暗角落里，大量交易肆无忌惮地进行着，包括被盗数据、恶意软件和攻击服务的买卖[17]。犯罪分子把非法市场转移到更加远离公众视野的地方，例如使用匿名 Tor 网络、以邀请制限制访问等[18]。价格的变化在一定程度上反映了供求状况。整体上，电子邮件的价格已大幅下降，信用卡信息的价格稍微下降，而网上银行账户资料的价格仍然保持稳定。

网络罪犯还可以购买现成的恶意软件、攻击工具包和漏洞信息。他们甚至还可以购买“犯罪软件即服务”，这种服务包含用于进行网上诈骗的整个基础架构。

这些市场分工明确。有人专门编写特洛伊木马和病毒，有人专门散播恶意软件、僵尸网络或贩卖被盗的信用卡资料。其中有些市场已存在至少十年之久，但是赛门铁克发现各方面都变得更加专业化。任何与买家的金钱收益有直接关联的产品或服务都保持着稳定的市场价[19]。

只需每周 100 至 700 美元的价格，就能租到一个包含更新和全天 24 小时支持的网络偷渡式下载工具包。网上银行恶意软件 SpyEye（作为 Trojan.Spyeye 被检测到）为期六个月的租赁费是 150 至 1250 美元，而分布式拒绝服务 (DDoS) 攻击的订购价为每天 10 至 1000 美元不等[20]。




*信用卡在各国地下经济的价格。*

[17] http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services
[18] http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services
[19] http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services
[20] http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services

## 在黑市上售卖的信息的价值

| | | |
|---|---|---|
| *1000 个被盗的电子邮件地址* | **0.50 至 10 美元** | 垃圾邮件、网络钓鱼 |
| *信用卡资料* | **0.50 至 20 美元** | 购物欺诈 |
| *真实护照扫描件* | **1 至 2 美元** | 身份盗用 |
| *被盗的游戏账户* | **10 至 15 美元** | 获取有价值的虚拟物品 |
| *定制恶意软件* | **12 至 3500 美元** | 付款转移、比特币盗取 |
| *1000 个社交网络关注者* | **2 至 12 美元** | 引发观看者的兴趣 |
| *被盗的云账户* | **7 至 8 美元** | 托管命令与控制 (C&C) 服务器 |
| *100 万封被核实为发出的垃圾邮件* | **70 至 150 美元** | 垃圾邮件、网络钓鱼 |
| *注册并激活的俄罗斯手机 SIM 卡* | **100 美元** | 欺诈 |

来源：赛门铁克

# 恶意软件

2013 年年底，俄罗斯当局逮捕了 Paunch。Paunch 被指控为 Blackhole（黑洞）漏洞利用工具包的作者，该工具包导致世界各地的大量感染 [21, 22]。这是一次与各种形式的恶意软件长期斗争的小型胜利。

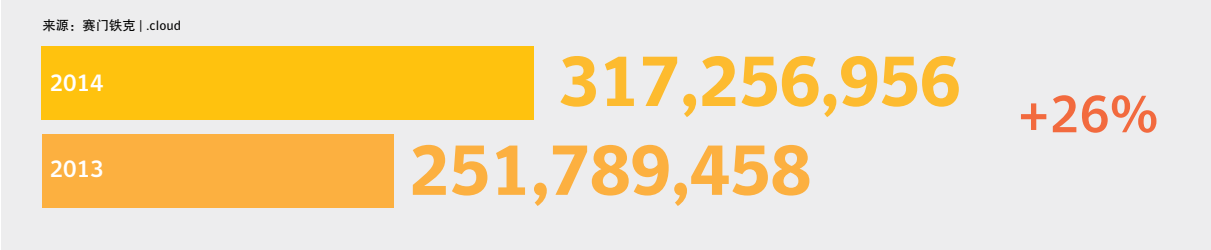
无可避免的是，其他攻击工具包取而代之。为盗窃银行资料而设计的恶意软件仍然继续泛滥。2014 年还出现了针对新“市场”的恶意软件。银行木马 Snifula 攻击了日本的金融机构 [23]，中东也出现了一组本土攻击，使用的是一种叫做 njRAT 的恶意软件 [24]。

在十月份，仅有百分之七的垃圾邮件含有 URL 链接。这一比例在十一月飙升到 41%，并在十二月初继续攀升，原因是包括恶意传真和语音信箱通知电子邮件在内的社交骗局主题的信息激增。

这些电子邮件里的链接利用被劫持的域名，邮件包含的 URL 路径指向 PHP 登陆页面。如果用户点击这些链接，就会被引向一个恶意文件。特别是，我们发现 Downloader.Ponik 和 Downloader.Upatre 被用在这些电子邮件里。它们是广为人知的特洛伊木马，被用来向受害电脑下载更多恶意软件，包括 Trojan.Zbot（又名 Zeus）等盗取信息的恶意软件。[25]

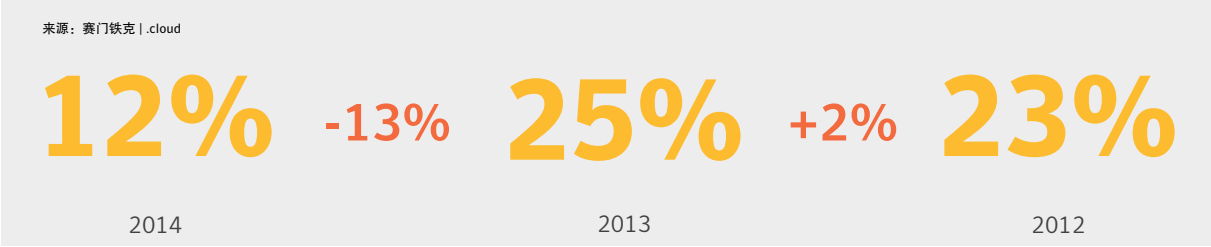
整体上，经过 2013 年的高峰期后，散播恶意软件的电子邮件数量在 2014 年已经下降。

### 新的恶意软件变种（每年新增）



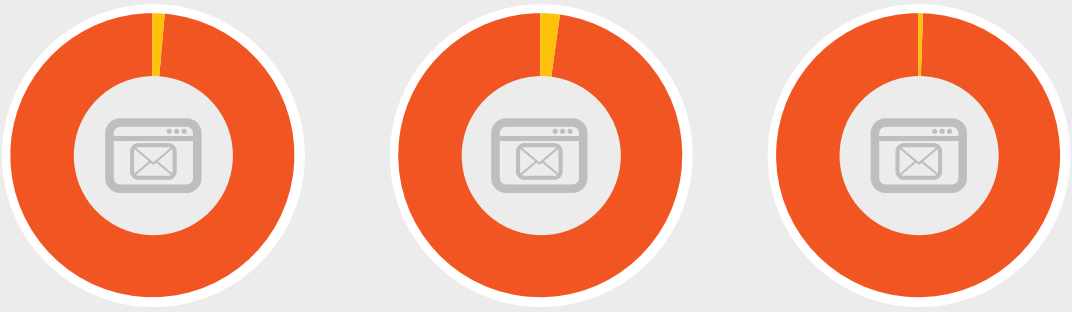

*2014 年制造的新恶意软件超过 3.17 亿个，相当于每天新出现近一百万个恶意软件；恶意软件的整体总数目前直逼 20 亿（17 亿）。*

### 电子邮件恶意软件比例（整体）




[21] http://en.wikipedia.org/wiki/Blackhole_exploit_kit
[22] http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/
[23] http://www.symantec.com/connect/blogs/snifula-banking-trojan-back-target-japanese-regional-financial-institutions
[24] http://www.symantec.com/connect/blogs/simple-njrat-fuels-nascent-middle-east-cybercrime-scene
[25] http://www.symantec.com/connect/blogs/malicious-links-spammers-change-malware-delivery-tactics

## EMAIL MALWARE RATE (OVERALL)



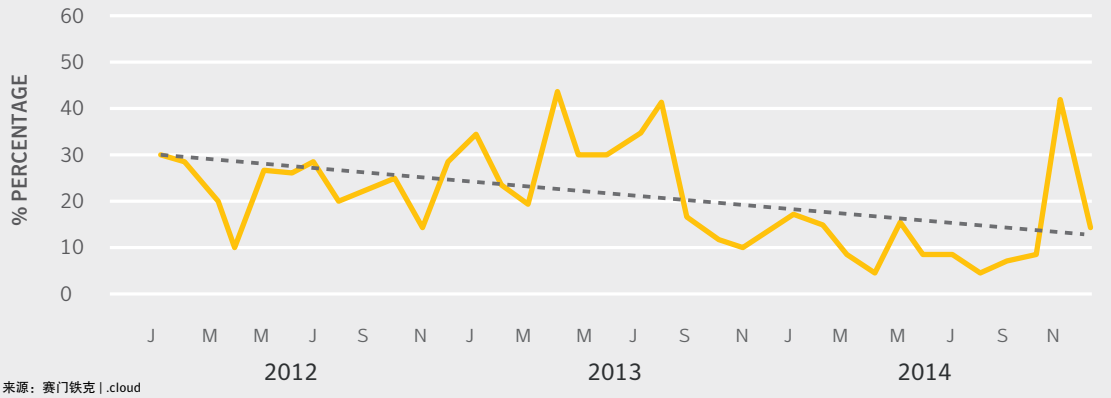
**1 IN 244** — 2014

**1 IN 196** — 2013

**1 IN 291** — 2012

来源：赛门铁克 | .cloud

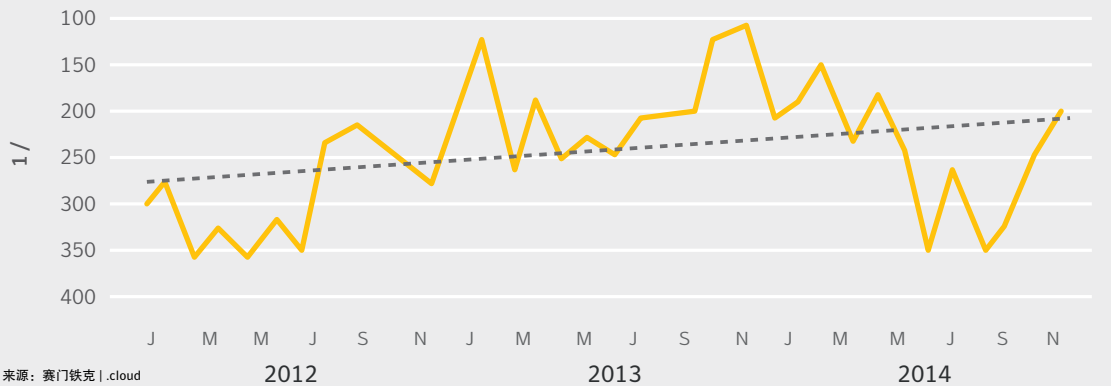
## 各个月份的 URL 式和附件式电子邮件恶意软件比例比较




来源：赛门铁克 | .cloud

*2014 年，在以电子邮件为载体的恶意软件中，12% 含有恶意链接（而不是将恶意软件作为邮件附件），在 2013 年这一比例为 25%。*

## 2012–2014 年检测到病毒的电子邮件通信比例




来源：赛门铁克 | .cloud

# 勒索软件

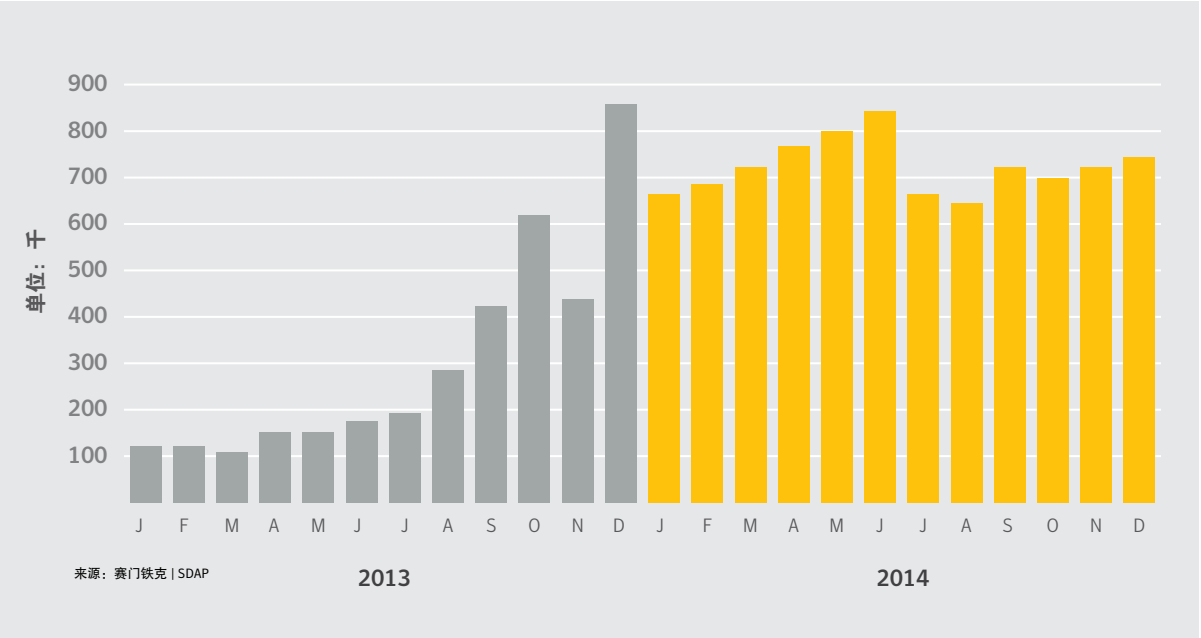
勒索软件攻击在 2014 年不止翻了一番，从 2013 年的 410 万次增加到 880 万次。更令人担忧的是文件加密勒索软件（赛门铁克称之为“加密勒索软件”）的增长，从 2013 年的 8274 个增加到 2014 年的 373342 个。

也就是说，在威胁环境中，加密勒索软件的数量在短短一年内增加了 45 倍。2013 年，加密勒索软件相当罕见，占勒索软件的 0.2% (1/500)；然而到了 2014 年年底，这种软件已经占所有勒索软件的 4% (1/25)。

从人类的角度来看，勒索软件是对受害者最卑劣的攻击形式。犯罪分子用恶意软件加密受害者硬盘上的数据，如家庭照片、作业、音乐、未完稿的小说等等，然后索取付款作为解锁这些文件的条件。最好（也许也是唯一）的防御方法是另外备份您的文件，最好是离线备份，以便在必要时进行恢复。

勒索软件存在多种变体，没有一个操作系统可以保证免受其害。[26] 虽然一直以来的建议都是不要付款给犯罪分子，但是很多企业和个人只想或需要取回文件。所以，他们为此付款，这种诈骗方式也因而利润可观。

### 2013–2014 年随时间推移的勒索软件




来源：赛门铁克 | Response

[26] http://www.symantec.com/connect/blogs/windows-8-not-immune-ransomware-0

# 加密勒索软件

令人担忧的是，赛门铁克发现，在 2013 至 2014 年之间，在威胁环境中，勒索软件的数量翻了一番，而且加密勒索软件的数量增加了 45 倍有余。[27]

加密勒索软件有几个不同的分支，例如 Cryptolocker[28]、Cryptodefense[29] 和 Cryptowall[30]，但它们的漏洞利用手段都是相同的。加密勒索软件并不是躲在勒索之墙的后面锁定您的桌面，而是远程加密您的个人文件，并持有解密私钥以便勒索。这种攻击的恶意程度远远超过传统的勒索软件。

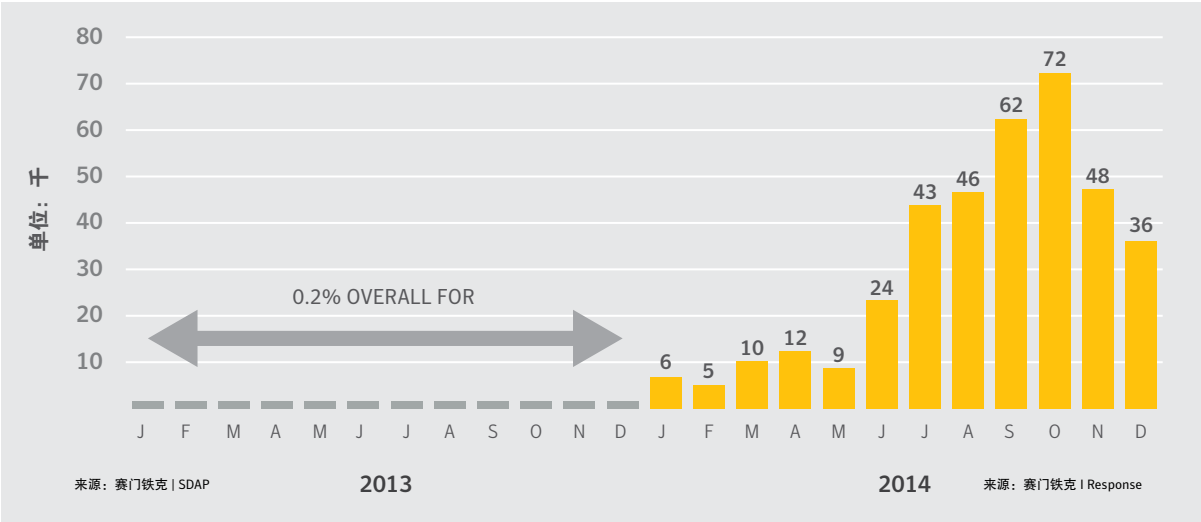
感染方式不尽相同，但常见途径是作为恶意邮件附件伪装成发票、水电煤气费账单或图片。这种恶意软件的投放往往构成“服务”的一部分，实际提供这种服务的人是执行加密勒索软件的不同罪犯。这仅仅是地下经济的其中一个黑暗面，里面的罪犯提供“本人可感染 x 台电脑，价格为 y”之类的服务。

在三月被揭露的 CryptoDefense 充分说明了加密勒索软件的严重性和追踪其幕后黑手的难度。它的投放途径是恶意邮件附件，通过公钥加密算法将受害者的文件加密，这种算法使用强大的 RSA 2048 位加密。

为了支付赎金，受害者必须访问 Tor 网络上的网页。[31] 然后，他们会被要求用比特币进行支付。这些是加密勒索软件罪犯的典型伎俩，导致这类骗局极其难以追踪和封锁。

然后，我们来看一看整个骗局的关键所在：利益。赛门铁克估计 CryptoDefense 背后的网络罪犯在短短一个月内就赚了超过 34000 美元。[32] 难怪加密勒索软件被视为目前存在的最有效的网络犯罪行为。

## 2013–2014 年加密勒索软件




*2013 年，加密勒索软件大约占所有勒索软件攻击的 0.2%。到 2014 年年底，这个数字增长到了 4%。*

[27] http://www.symantec.com/connect/blogs/australians-increasingly-hit-global-tide-cryptomalware

[28] http://www.symantec.com/security_response/writeup.jsp?docid=2013-091122-3112-99

[29] http://www.symantec.com/security_response/writeup.jsp?docid=2014-032622-1552-99

[30] http://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99

[31] Tor 是软件和开放式网络的结合，可保护用户不被纳入流量分析，有助于保持用户在网上的匿名性和隐私。虽然它本身并没有违法犯罪，但在这种情况下却帮助保护了罪犯的匿名性。

[32] http://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month

# 机器人程序和僵尸网络

相比前一年，机器人程序的数量在 2014 年下降了 18%。在很大程度上，这是因为美国联邦调查局 (FBI)、欧洲刑警组织 (Europol) 下属的欧洲网络犯罪中心 (EC3) 以及其他国际执法机关与赛门铁克和其他技术公司携手合作，积极地瓦解和封锁机器人程序和僵尸网络。其中最引人注意的是在 2014 被封锁的 Gameover Zeus 僵尸网络。自 2011 年出现以来，该僵尸网络感染了世界各地数百万台电脑 [33, 34]。这是过去几年来被瓦解的一系列僵尸网络之一，[35, 36] 是 IT 公司和执法机关通力合作的成果。

## 不同源头的恶意活动：机器人程序，2012–2014 年

| 国家 / 地区 | 2014 年机器人程序排名 | 2014 年机器人程序百分比 | 2013 年机器人程序排名 | 2013 年机器人程序百分比 |
|---|---|---|---|---|
| 中国 | 1 | **16.5%** | 2 | **9.1%** |
| 美国 | 2 | **16.1%** | 1 | **20.0%** |
| 台湾 | 3 | **8.5%** | 4 | **6.0%** |
| 意大利 | 4 | **5.5%** | 3 | **6.0%** |
| 匈牙利 | 5 | **4.9%** | 7 | **4.2%** |
| 巴西 | 6 | **4.3%** | 5 | **5.7%** |
| 日本 | 7 | **3.4%** | 6 | **4.3%** |
| 德国 | 8 | **3.1%** | 8 | **4.2%** |
| 加拿大 | 9 | **3.0%** | 10 | **3.5%** |
| 波兰 | 10 | **2.8%** | 12 | **3.0%** |

来源：赛门铁克 | GIN

*作为互联网用户最集中的两个人口大国，美国和中国在 2014 年交换了第一名和第二名的位置。这种转变可能是因为 Gameover Zeus 的瓦解。*

[33] http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network
[34] http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/
[35] http://www.computerweekly.com/news/2240185424/Microsoft-partnership-takes-down-1000-cybercrime-botnets
[36] http://www.computerweekly.com/news/2240215443/RSA-2014-Microsoft-and-partners-defend-botnet-disruption

## 机器人程序的数量


来源：赛门铁克 | GIN

*2014 年机器人程序减少，这在一定程度上是因为国际执法联合行动 Operation Tovar 瓦解了 GameOver ZeuS 僵尸网络。该僵尸网络主要被用于银行欺诈和 CryptoLocker 勒索软件的散播。*[37]

## 发送垃圾邮件的十大僵尸网络，2014 年

| *垃圾邮件/僵尸网络名称* | 僵尸网络垃圾邮件比例 | 估计每日垃圾邮件量 | 僵尸网络垃圾邮件的主要来源 | | |
|---|---|---|---|---|---|
| | | | 排名第 1 | 排名第 2 | 排名第 3 |
| *KELIHOS* | 51.6% | 884,044 | 西班牙 10.5% | 美国 7.6% | 阿根廷 7.3% |
| *未知/其他* | 25.3% | 432,594 | 美国 13.5% | 巴西 7.8% | 西班牙 6.4% |
| *GAMUT* | 7.8% | 133,573 | 俄罗斯 30.1% | 越南 10.1% | 乌克兰 8.8% |
| *CUTWAIL* | 3.7% | 63,015 | 俄罗斯 18.0% | 印度 8.0% | 越南 6.2% |
| *DARKMAILER5* | 1.7% | 28,705 | 俄罗斯 25.0% | 乌克兰 10.3% | 哈萨克斯坦 5.0% |
| *DARKMAILER* | 0.6% | 9,596 | 俄罗斯 17.6% | 乌克兰 15.0% | 中国 8.7% |
| *SNOWSHOE* | 0.6% | 9,432 | 加拿大 99.9% | 美国 0.02% | 日本 0.01% |
| *ASPROX* | 0.2% | 3,581 | 美国 76.0% | 加拿大 3.4% | 英国 3.3% |
| *DARKMAILER3* | 0.1% | 1,349 | 美国 12.7% | 波兰 9.6% | 韩国 9.1% |
| *GRUM* | 0.03% | 464 | 加拿大 45.7% | 土耳其 11.5% | 德国 8.5% |

来源：赛门铁克 | .cloud

[37] http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network

# OSX 沦为目标

近年来，Apple 注意到一些针对 OSX 操作系统的威胁，并陆续推出了该操作系统亟需的几个安全功能。XProtect 会扫描已下载文件有无恶意软件的迹象，并在用户下载了 Apple 已知的恶意文件时警告用户。GateKeeper 用代码签名来限制可在 OSX 电脑上运行的应用程序。GateKeeper 可提供不同程度的保护，包括仅限安装来自官方 Mac App Store、Apple 认定为可信任的开发者或对应用程序进行签名的开发者的应用程序。

尽管这些安全功能提高了入侵 OSX 的难度，威胁却成功摆脱了这些功能的限制。和所有基于签名的安全解决方案一样，应用程序已经能够在采用签名加以屏蔽之前感染电脑。带有合法开发人员签名的恶意应用程序也出现了，这些签名是通过盗取合法凭据或伪造而得到的。

2014 年最常见的威胁在行为上与其他操作系统上的发现相似。有些特洛伊木马通过利用浏览器漏洞而入侵。臭名昭著的威胁仍然肆虐横行，例如曾在 2012 年感染超过 60 万台 Mac 电脑的 Flashback，它的不同变种在 2014 年分别排名第三和第十。在 OSX 电脑上改写设置（如 DNS、浏览器或搜索设置）的威胁也登上了较高的排名。

两个著名的威胁突显了 OSX 威胁环境中的重大问题：含有恶意软件的盗版 OSX 应用程序。

**OSX.Wirelurker** 是一种双重威胁特洛伊木马，它会影响运行 OSX 的 Mac 电脑和任何连接到受害电脑的 iOS 设备。这一威胁在托管于中国某第三方 OSX 应用商店的 467 个 OSX 应用程序内被发现，引起了重大关注。这些恶意应用程序在下载 356,000 次后，被 Apple 介入和阻止。

**OSX.Luaddit（又名 iWorm）**是一种将受害电脑添加到 OSX 僵尸网络的威胁。这一威胁捆绑了商用产品（如 Adobe Photoshop、Microsoft Office、Parallels 等）的盗版。[38] 这些应用程序被发布到 torrent 站点，被下载了成千上万次。

其他著名的 OSX 威胁包括 OSX.Stealbit.A 和 OSX.Stealbit.B，这两种盗窃比特币的威胁会监控浏览流量，并搜寻大型比特币网站的登录凭据。OSX.Stealbit.B 是 2014 年发现的五大 OSX 威胁之一。

**OSX.Slordu** 是一种后门特洛伊木马，它似乎被用来收集关于受害电脑的信息。这种威胁的有趣之处在于它似乎是一种流行的 Windows 后门的 OSX 端口。

**OSX.Ventir** 是一种模块威胁，它带有的选配组件可以打开后门、记录按键或包含间谍软件功能。取决于攻击者试图从受害电脑中获取的信息，不同的模块会被下载和安装在 OSX 里。

**OSX.Stealbit.A** 是一种盗窃比特币的威胁，它会监控浏览流量，并搜寻大型比特币网站的登录凭证。


[38] http://www.thesafemac.com/iworm-method-of-infection-found/

## OSX 终端屏蔽的十大 MAC OSX 恶意软件，2013-2014 年

| 排名 | 恶意软件名称 | 2014 年 Mac 威胁百分比 | 恶意软件名称 | 2013 年 Mac 威胁百分比 |
|---|---|---|---|---|
| 1 | OSX.RSPlug.A | **21.2%** | OSX.RSPlug.A | **35.2%** |
| 2 | OSX.Okaz | **12.1%** | OSX.Flashback.K | **10.1%** |
| 3 | OSX.Flashback.K | **8.6%** | OSX.Flashback | **9.0%** |
| 4 | OSX.Keylogger | **7.7%** | OSX.HellRTS | **5.9%** |
| 5 | OSX.Stealbit.B | **6.0%** | OSX.Crisis | **3.3%** |
| 6 | OSX.Klog.A | **4.4%** | OSX.Keylogger | **3.0%** |
| 7 | OSX.Crisis | **4.3%** | OSX.MacControl | **2.9%** |
| 8 | OSX.Sabpab | **3.2%** | OSX.FakeCodec | **2.3%** |
| 9 | OSX.Netweird | **3.1%** | OSX.Iservice.B | **2.2%** |
| 10 | OSX.Flashback | **3.0%** | OSX.Inqtana.A | **2.1%** |

来源：赛门铁克 | SDAP

# 虚拟化系统上的恶意软件

面对恶意软件，虚拟化无力抵御。越来越多的恶意软件能够检测是否正在虚拟机上运行。这些恶意软件不会放弃入侵，反而会改变自身行为来降低被检测到的风险[39]。以往会检测是否运行在 VMware 上的恶意软件的比例一直徘徊在 18% 左右，但在 2014 年年初飙升到 28%[40]。

但这种功能并不仅仅是用来避开安全研究员。在安装到虚拟机上之后，恶意软件就可以跳到同一硬件的其他虚拟机上，或感染虚拟机监控程序，大大提高风险和移除的难度[41]。在实际环境中已经发现了这种行为：W32.Crisis 恶意软件试图感染存储在主机计算机上的虚拟机映像[42]。

对 IT 经理而言，这种攻击构成了特别的风险：它不太可能被入侵检测系统或使用虚拟机检测虚拟“沙盒”中的威胁的防火墙等周边安全机制检测到；虚拟机可能无法获得与传统客户端或服务器同等程度的保护，因为人们（误）以为恶意软件不会攻击虚拟机。企业需要将网络硬件、虚拟机监控程序和软件定义网络之类的技术纳入安全计划和修补程序周期的考虑范围内。

[39] http://www.symantec.com/connect/blogs/does-malware-still-detect-virtual-machines
[40] Ibid
[41] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/threats_to_virtual_environments.pdf
[42] Ibid

# 网络敲诈：勒索软件简史

**文：Peter Coogan**

在 2014 年，关于加密勒索软件的新闻几乎未曾中断。在长期以来一连串的勒索软件中，出现了一种最新也最致命的趋势 —— 不是像常见的勒索软件那样仅仅锁定设备，而是在受害设备上加密数据文件，让受害者在大多数情况下无法挽救他们的数据。不过，新旧勒索软件都是为了向受害者勒索赎金，作为解除感染的条件。

这种恶意软件已经诞生超过十年，但在近年来却大有泛滥之势。这种发展势头的原因是网络罪犯从伪造防病毒软件改为炮制更加有利可图的勒索软件。虽然从虚假防病毒软件到勒索软件再到加密勒索软件的演变过程是有迹可循的，但是恶意软件的作者并不会原地踏步。我们可以清楚地看到这些网络敲诈勒索者在威胁领域的新走向。

虚假防病毒软件或流氓安全软件是一种具有误导性的应用程序，会蒙骗或误导用户付款卸除恶意软件。这种软件至今为止已存在多时，但它最盛行的时期是 2009 年左右。当年的一份赛门铁克报告指出，大约有 4300 万个流氓安全软件通过超过 250 种不同的程序试图让用户安装，给购买这些软件的用户造成的金钱损失为 30 美元至 100 美元不等。[43]

勒索软件是一种对受感染电脑进行锁定和限制访问的恶意软件。然后，勒索软件会显示一条使用社交骗局主题的敲诈消息，要求支付赎金来换取解锁。赛门铁克在 2012 年报告了勒索软件日益增长的威胁，指出欧洲的敲诈者索要的解锁赎金为 50 至 100 欧元，美国的敲诈者索要的赎金最高达 200 美元。[44]

如今，在臭名昭著的 Trojan.Cryptolocker[45] 于 2013 年出现并取得“成功”之后，恶意软件的作者已转移注意力，去制造新的加密勒索软件式威胁。由此导致了 2014 年的加密勒索软件家族激增的现象，其中包含新的创新、平台和入侵手段，以及新旧伎俩的运用，目的都是为了向受害者勒索钱财。

2014 年里其中一个较为高产的新加密勒索软件是 Trojan.Cryptodefense[46]（又名 Cryptowall）。这个威胁出现在 2014 年 2 月末，起初在市面上的名称是 Cryptodefense。它采用的伎俩包括使用 Tor 和比特币保持匿名性、对数据进行强大的 RSA 2048 位加密，以及施加压力恐吓受害者付款。它开始索要的赎金是 500 美元或欧元，如果没有收到付款就在不久后涨到 1000 美元或欧元。然而，有人在分析后发现，这款恶意软件的作者没有很好地实施加密功能，私钥留在了系统里，所以被要挟者可以借助这把“钥匙”自救。在公布这一情况后，恶意软件作者解决了这个问题，并将这款软件改名为 Cryptowall 重新面世。此后，Cryptowall 通过进一步加强自身武装而不断演变，其中包括漏洞利用权限提升、抗分析检查以及利用隐形互联网计划 (I2P) 实现匿名通信。Cryptowall 产生的已知收入在第一个月至少有 34,000 美元 [47]，而研究人员判断它在六个月里赚得金额超过 100 万美元。[48]

Windows 个人电脑对勒索软件作者而言一直是利润可观的领域，今后可能继续如此。然而，这些网络敲诈工具背后的攻击者在 2014 年开始摸索新的平台。我们看到 Reveton 团伙发布了安卓勒索软件 Android.Lockdroid.G[49]（又名 Koler）。通过使用流量分配系统 (TDS)，Reventon 团伙目前可以实施三叉式勒索软件攻击。根据特定的条件，例如用于浏览被该团伙控制的网站的浏览器，流量将被重定向到合适的勒索软件。

[43] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_exec_summary_20326021.en-us.pdf
[44] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf
[45] http://www.symantec.com/security_response/writeup.jsp?docid=2013-091122-3112-99
[46] http://www.symantec.com/security_response/writeup.jsp?docid=2014-032622-1552-99
[47] http://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month
[48] http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/
[49] http://www.symantec.com/security_response/writeup.jsp?docid=2014-050610-2450-99

勒索软件突然具备了平台无关性。安卓用户会被重定向去下载 Android.Lockdroid.G，Internet Explorer 用户会被重定向去下载提供 Trojan.Ransomlock.G 有效载荷的 Angler Exploit 工具包[50]，而在 Windows、Linux 或 Mac 上使用的其他浏览器会被重定向到另一种形式的勒索软件 —— Browlock[51]，它会试图锁定电脑，然后用网页浏览器中的工具来勒索用户。

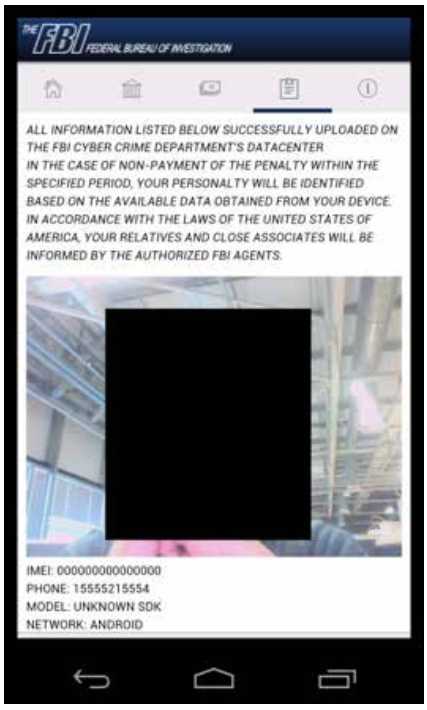
2014 年 6 月，第一款针对安卓的文件加密勒索软件 Android.Simplocker[52] 被发现。该软件起初以俄语索要赎金，后来在 2014 年 7 月发现了英语更新版 (Android.Simplocker.B[53])，英语版本采用了 FBI 社交骗局主题。2014 年 10 月出现了 Android.Lockdroid.E[54]（又名 Porndroid），它再次使用虚假的 FBI 社交骗局主题。但是，这个威胁还会利用设备的摄像头进行拍照，然后将照片与勒索信息一并显示。Android.Lockdroid 进一步衍生出新的变种，包括蠕虫功能，从而可以通过向受感染设备上的通讯录联系人发送手机短信进行自我复制，设下社交骗局圈套。

勒索软件作者甚至开始越过移动设备而试图挖掘其他可以进行敲诈勒索的渠道。他们发现存储了大量文件的网络存储 (NAS) 设备也是一个可以下手的目标。Trojan.Synolocker[55]（又名 Synolocker）盯上了群晖科技的网络附加存储设备，它的方法是利用群晖科技的 DiskStation 管理软件中原先不为人知的漏洞来取得设备的访问权限，然后加密所有文件，并挟持这些文件进行勒索。此后，这些设备安装了修补程序，以防进一步攻击，但是这个案例突出说明了勒索软件攻击者不断寻找新的攻击领域。

那么，勒索软件为什么会如此快速地变化呢？勒索软件对网络罪犯而言是一个利润可观的行当，赎金从 100 美元至 500 美元不等。2014 年，我们还发现比特币成为多数新勒索软件首选的付款方式。由于比特币具有很强的匿名性，网络罪犯可以轻易藏匿和洗白这些不义之财。

在注意到新增大量勒索软件分支的同时，赛门铁克还看到了整体增长路径的提升。与 2013 年相比，我们看到的勒索软件发生率上升了 113%。然而，由于这些威胁利润可观，而且新出现的勒索软件分支数量众多，威胁环境中的勒索软件类欺诈在短期内不太可能消减，在未来更加可能会有增无减。


*图 x.“Porndroid”安卓勒索软件威胁。*

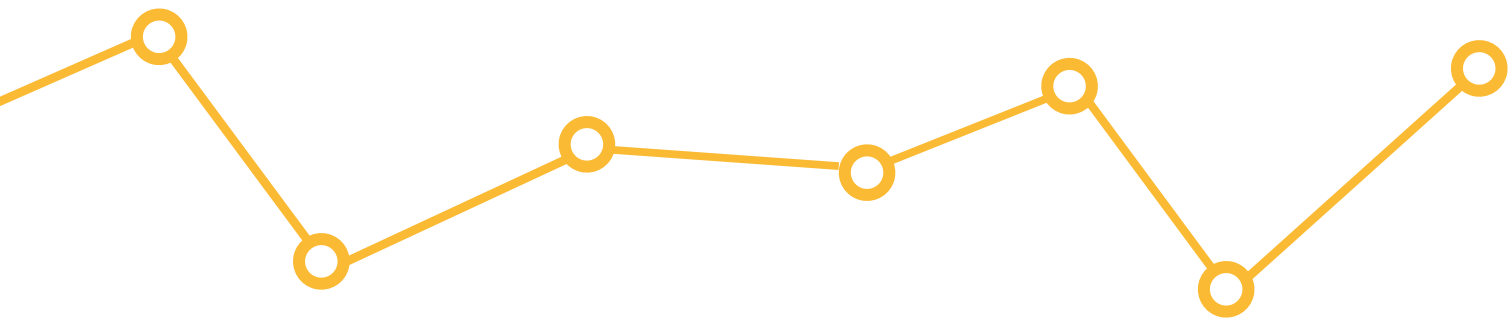



[50] http://www.symantec.com/security_response/writeup.jsp?docid=2011-051715-1513-99
[51] http://www.symantec.com/connect/blogs/massive-malvertising-campaign-leads-browser-locking-ransomware
[52] http://www.symantec.com/security_response/writeup.jsp?docid=2014-060610-5533-99
[53] http://www.symantec.com/security_response/writeup.jsp?docid=2014-072317-1950-99
[54] http://www.symantec.com/security_response/writeup.jsp?docid=2014-103005-2209-99
[55] http://www.symantec.com/security_response/writeup.jsp?docid=2014-080708-1950-99

# 目标性攻击

# 一览

| | |
|---|---|
| 1 | 更多由国家资助的网络间谍活动在 2014 年浮出水面。 |
| 2 | 攻击者使用的恶意软件越来越精良，体现了复杂的软件工程和专业程度。 |
| 3 | Dragonfly（蜻蜓）、Waterbug（水虫）和 Turla 等间谍软件渗透到工业系统、大使馆和其他敏感目标内。 |
| 4 | 鱼叉式网络钓鱼攻击的数量在 2014 年增加了 8%，而每日攻击的数量则有所减少，因为攻击者变得更加耐心，潜伏起来精心酝酿以长期侦察为基础的更为隐秘的攻击。 |



# 简介

2014 年，赛门铁克分析了几场网络间谍攻击，收集了与攻击策略有关的数据。攻击者采用这些策略，渗透到世界各地数以千计防御良好的敏感组织内。这项研究显示了攻击的复杂性已经提升到令人担忧的程度。

想象一下您是某东欧外交使团的首席信息安全官 (CISO)。2014 年，您怀疑贵国在欧洲各地的大使馆的电脑感染了一种后门木马。您请了一家安全公司进行调查，他们证实了您所怀疑的最糟糕的情况。经过调查，您发现某个经过精心部署的目标性鱼叉式网络钓鱼攻击活动向大使馆工作人员发送了电子邮件，而隐含在其中的木马有效载荷感染了电脑。在零时差漏洞利用、精心策划的电子邮件以及狡猾的水坑式网站攻击下，这些攻击长时间避开了检测，并感染了 100 多个国家中超过 4500 台电脑 [56]。

上述情景令人担忧，但并非假设。它所描述的就是水坑式攻击。

它类似于其他目标性攻击（例如 Turla 和 Regin），但是鉴于它所选择的目标以及攻击方法的复杂性，赛门铁克认为 Waterbug[57] 的背后黑手是由国家资助的组织。

由于这些攻击日趋复杂，良好的 IT 安全是必不可少的，广泛的网络安全实践应当成为常态。资金充足的国家行为体并不是唯一的威胁。爱国主义黑客、黑客行动主义者、刑事犯罪勒索者、数据窃取者和其他攻击者也利用类似的技巧，但是他们的资源相对较少，而且可能复杂程度没那么高。

基于电子邮件的攻击基本上继续保持之前的态势。基于 Web 的攻击越来越复杂。网络间谍攻击使用更多的漏洞利用工具包，将多种漏洞利用捆绑起来，而不是单单采用一种攻击。漏洞利用工具包在网络犯罪中的应用已有多年，但是如今很多网络间谍攻击者也在使用这些工具包。

[56] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf
[57] Ibid

# 网络间谍

2014 年，赛门铁克安全专家用了将近八个月的时间剖析有史以来最复杂的网络间谍恶意软件之一。这个被称为 Regin 的网络间谍软件赋予拥有者强大的工具，以监视政府部门、基础设施运营商、企业、研究机构和个人。对电信公司的攻击似乎是为了访问通过这些公司的基础设施传送的电话 [58]。

Regin 相当复杂，有五个隐秘的安装阶段。它还采取模块化设计，允许拥有者增加或删除不同的功能。多阶段加载和模块化设计在以前也曾出现过，但是 Regin 体现了高水平的工程能力和专业开发。例如，它带有数十个模块，这些模块的功能包括远程访问、屏幕截图、密码窃取、网络通信监控和恢复已删文件等 [59]。

它的开发需要耗时数月甚至数年，这说明投入了大量资源。它十分适合长期监视行动，而其复杂性说明它是由某个国家研制的。

在另一项网络间谍攻击活动中，赛门铁克也看到类似的投入，这项攻击活动被称为 Turla[60]。攻击者采用鱼叉式网络钓鱼和水坑式攻击（见下方），其目标是前“东方集团”国家的政府和大使馆。一旦安装，攻击者即可远程访问受感染的电脑，从而可以复制文件、删除文件、连接服务器等等。鉴于这个恶意软件所选择的目标以及它的复杂程度，赛门铁克认为这些攻击的背后也存在着一个由国家资助的组织 [61]。

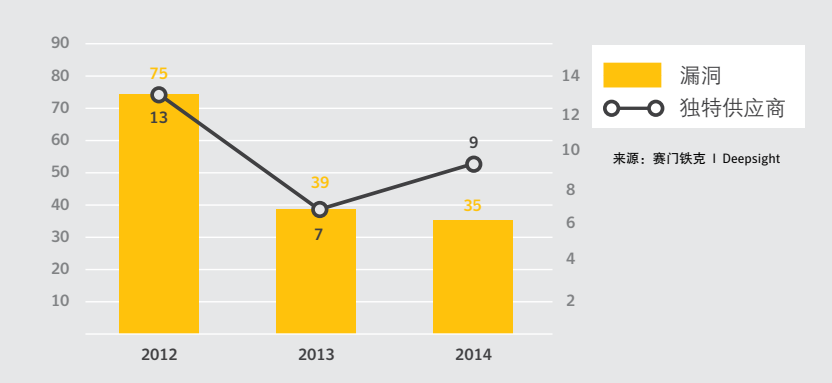
最近，一个被称为“方程组”(Equation Group) 的资源雄厚的攻击团体被曝光 [62]，揭示了前几年（包括 2014 年）的网络间谍攻击可能已经采取了高度专业化的攻击。此外，由于网络间谍攻击团体不断改进技术，他们还能利用漏洞攻击、零时差攻击、定制代码等黑市。方程组的曝光进一步突显了这些专业化攻击的开发背后的职业性。和合法的软件公司一样，网络间谍攻击团体也受益于传统的软件开发实践。

[58] http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance
[59] http://www.symantec.com/en/uk/outbreak/?id=regin
[60,61] http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats
[62] http://www.symantec.com/connect/blogs/equation-advanced-cyberespionage-group-has-all-tricks-book-and-more

# 工业网络安全

随着越来越多的设备连接到互联网，新的攻击（可能还有破坏活动）途径也不断出现。对于被称为工业控制系统 (ICS) 的工业设备，情况尤其如此。这些设备通常用于世界各地的工业生产和公用服务。其中，很多设备可连接互联网，因此更容易被监视和控制。

## 2012–2014 年在包括 SCADA 系统在内的 ICS 中披露的漏洞




*下图显示了与工业控制系统 (ICS) 和数据采集与监控系统 (SCADA) 相关的已披露漏洞数量，包括每年涉及的厂商数量。*

赛门铁克发现，2014 年，针对工业控制系统的攻击增多了。例如，网络间谍行动 Dragonfly 攻击了多种目标，包括能源网运营商、电力运营商、石油管道运营商和工业设备制造商[63]。大多数受害者位于美国、西班牙、法国、意大利、德国、土耳其和波兰。

尽管 Dragonfly 对工业控制系统的攻击与之前针对伊朗核计划的 Stuxnet 相似，但它的目标似乎没有那么大的破坏性。起初，它似乎着重于网络间谍活动和持久访问，最终的目标并不是破坏。然而，它让资源雄厚的攻击团体可以了解重要的工业系统，并有可能让他们能够在必要时发动更具破坏力的攻击。

它的散播方式是利用定制编写的恶意软件以及从俄语论坛购买的现成恶意软件，结合基于电子邮件的鱼叉式网络钓鱼和基于网页的水坑式攻击，通过供应链中规模较小、防护较差的公司对其主要受害者进行攻击。

如果公司无力承担安装修补程序所需的停机时间，或者使用专有技术或防护不力的技术，则可能很难保护其旧版系统。例如，用于过程控制的 OLE[64] (OPC) 是广泛用于工业自动化系统的协议。它是一项纪录详实的开放标准，但它几乎不提供加密、身份验证或其他安全措施，因此很容易被流氓软件攻击。Dragonfly 的其中一个目的是收集关于目标公司 OPC 系统的信息。

通过专门利用 ICS 厂商软件更新服务器的漏洞，Dragonfly 攻击呈现了水坑式攻击方法的新面孔。水坑式攻击利用真正的攻击目标会访问的第三方网站中的漏洞，攻击者通过这些网站向目标组织植入恶意软件。通过 Dragonfly，攻击者利用受害者为 ICS 软件采用的软件更新服务器的漏洞，从而感染供应链。这是新型水坑式攻击的又一个里程碑。

[63] http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat
[64] http://en.wikipedia.org/wiki/OLE_for_Process_Control

# 侦察攻击

除了利用鱼叉式网络钓鱼的攻击和水坑式攻击（这些攻击的成功离不开社交骗局中的人为因素）之外，攻击者还继续从其他角度攻击目标组织，以便在这些组织的网络中立足。他们只要攻击网络周边，找到防御漏洞并加以利用，即可达到目的。

如今，在攻击者访问目标组织网络的过程中，侦察的作用比以往更加重要。侦查往往是黑客入侵过程的第一步：获取关于系统的信息，寻找可以利用的漏洞。

从 2014 年位居前列的零时差漏洞利用事件来看，侦察的盛行是显而易见。最常用的零时差漏洞无疑是 CVE-2013-7331。它也不是那种利用脆弱系统中的漏洞获取系统访问权限、平淡无奇的漏洞利用方式。它仅用于攻击者收集关于目标网络的情报。然而，这对策划进一步的攻击十分有用。在掌握了目标内部网络的主机名、IP 地址和各种内部路径名等信息之后，攻击者就能轻易筹谋下一个攻击计划。

对于这种零时差攻击，在相当长的一段时期内没有安装修补程序。这一漏洞的 CVE 早在 2013 年已经部署，直到 2014 年 2 月才被披露；不仅如此，直到 2014 年 9 月才发布了缓解这种漏洞风险的修补程序。于是，在公开泄露与发布修补程序之间有长达 204 天的窗口期供攻击者利用。

至于暴露期如此之长，最好的解释也许是人们对这一威胁的严重性的认识。因为该漏洞利用攻击并没有让攻击者直接控制受害电脑，所以人们可能以为它不像其他漏洞那样亟待解决。攻击者清楚地认识到这一点，成功地利用了漏洞以及由此掌握的关于目标网络的信息，这间接帮助了他们实现恶意企图。

这是在威胁环境中可能值得安全行业加强关注的一部分。相比可导致权限升级的漏洞，仅仅馈送与网络、计算机或设备有关的信息的漏洞可能会被认为不太严重，但是如果后者可以引导攻击者发现本来不会被发现的存在漏洞的系统，那么它的危险程度可能就不亚于前者。

# 水坑式攻击以及零时差攻击的重要性

一支被称为 Hidden Lynx（隐秘山猫）的职业受雇黑客团体最初在 2013 年 9 月被发现，在 2014 年继续开展行动。这一团体通过水坑式攻击利用了一个重大的零时差漏洞 (CVE-2014-0332)[65]。攻击的最终结果是在“水坑”已部署之后访问被感染网站的任何电脑都被打开了后门，继而可以开展后续攻击和数据渗漏。

在针对与法国航空业有关的组织和多种日本网站的水坑式攻击中，还发现了另一种零时差漏洞，即 CVE-2014-0332。但是，我们认为这些攻击与 Hidden Lynx 团体无关，涉及这种漏洞利用的行动者另有其人。[66]

还有一场重大的水坑式攻击利用了 Adobe Flash 中的零时差漏洞 (CVE-2014-0515)，并结合了某家合法厂商生产的一款特定软件。这场攻击似乎极具针对性，因为只有目标组织同时安装了上述两种软件，攻击才会得逞。

还有另一个实例：一个以前在 Microsoft Windows 中未曾发现的漏洞让网络间谍组织 Sandworm 得以在目标组织中安装恶意软件 [67]，这些组织包括北大西洋公约组织 (NATO)、乌克兰和西欧的多个政府组织、能源公司、电信公司等。

Elderwood 平台在 2012 年被首次发现，但得以继续维持。例如，在 2014 年初，它利用三个新的零时差漏洞攻击了受害者 [68]。

在 2014 年发现了 24 个零时差漏洞，与 2013 年的历史高位持平，这说明被发现和利用的零时差漏洞数量出现了新的常态。也许还有更多漏洞被攻击者暂时保留，目前仍然不为人知。

对攻击者而言，零时差漏洞的利用有以下两方面的价值和意义。首先，任何未公布的漏洞都有巨大的价值，前提是攻击者可以利用该漏洞来获取远程访问权限或实施侦察。第二，把握好从厂商意识到漏洞的存在到实际提供修补程序的延迟，可以利用漏洞获得巨大的回报。提供修补程序可能需要几天、几星期甚至几个月的时间，然后还要经过更长的时间才能广泛部署。

对于 2014 年公布的最经常被利用的 5 大零时差漏洞，从厂商公布漏洞到发布修补程序的日期之间相隔的总天数由 2013 年的 19 天延长到了 2014 年的 295 天。从公布漏洞到提供修补程序之间相隔的平均时间也延长到了 59 天，而 2013 年的平均时间只有 4 天。2014 年最经常被利用的零时差漏洞 CVE-2013-7331 在 2013 年首次被发现，因此归类为 2013 年漏洞；但是，它的存在直到第二年才被公之于众。此后又经过 204 天，厂商才终于发布了修补程序。排名第二和第三的最经常被利用的零时差漏洞也经过了漫长的发布修补程序窗口期，分别为 22 天和 53 天。这两个窗口期都超过了 2013 年的平均值。

网络间谍攻击团体正是依赖这个弱点（即漏洞的窗口期）而获得成功。例如，当软件厂商公布关于某漏洞存在的信息之后，即使尚未发布修补程序，被水坑式攻击利用漏洞的受感染网站也可能马上停止利用零时差漏洞。然后，攻击者可能会改为利用另一种尚未被发现的漏洞，这也进一步说明了他们拥有的资源极其充裕。

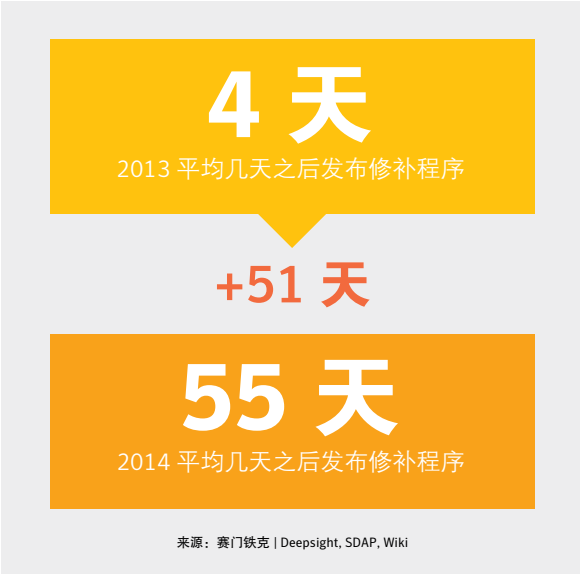
[65] http://www.symantec.com/connect/blogs/emerging-threat-ms-ie-10-zero-day-cve-2014-0322-use-after-free-remote-code-execution-vulnerabi
[66] http://www.symantec.com/connect/blogs/zero-day-internet-vulnerability-let-loose-wild
[67] http://www.symantec.com/connect/blogs/sandworm-windows-zero-day-vulnerability-being-actively-exploited-targeted-attacks
[68] http://www.symantec.com/connect/blogs/how-elderwood-platform-fueling-2014-s-zero-day-attacks

## 零时差漏洞


来源：赛门铁克 | Deepsight, SDAP, Wiki

## 五大零时差漏洞、修补程序和签名


来源：赛门铁克 | Deepsight, SDAP, Wiki



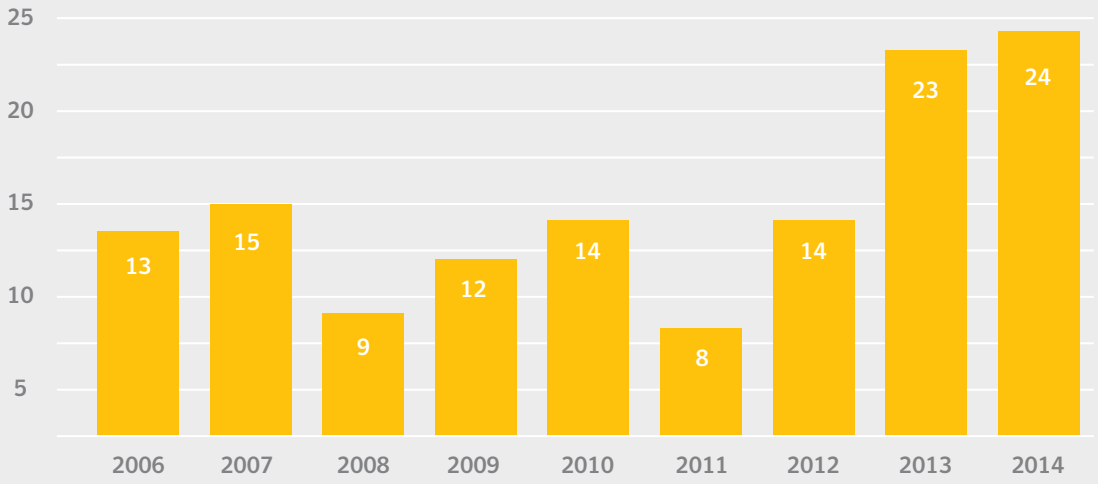

来源：赛门铁克 | Deepsight, SDAP, Wiki

*2014 在添加签名之后（90 天之内）和厂商发布修补程序之前发生的五大漏洞攻击的百分比 57%*


| 排名 | CVE | 2014 年整体比例 |
|---|---|---|
| 1 | Microsoft ActiveX Control CVE-2013-7331 | 81 % |
| 2 | Microsoft Internet Explorer CVE-2014-0322 | 9.5 % |
| 3 | Adobe Flash Player CVE-2014-0515 | 7.3 % |
| 4 | Adobe Flash Player CVE-2014-0497 | 2.0 % |
| 5 | Microsoft Windows CVE-2014-4114 OLE | <1 % |

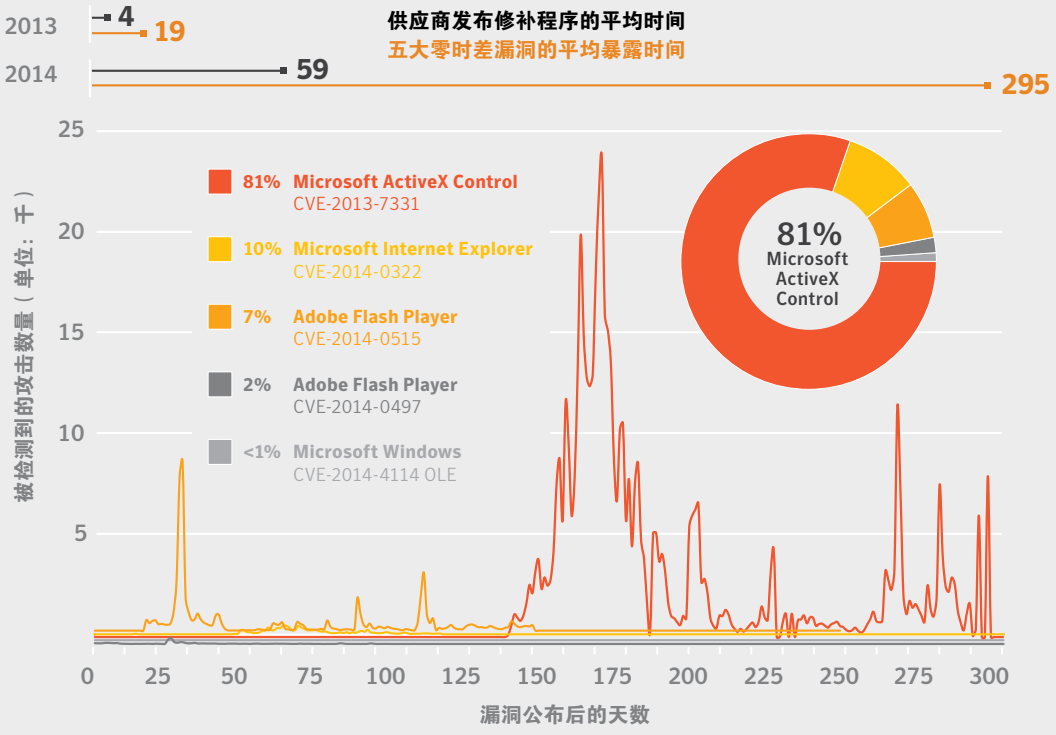
*对于最经常被利用的 5 大零时差漏洞，从厂商公布漏洞到后来发布修补程序的日期之间相隔的总天数由 2013 年的 19 天延长到了 2014 年的 295 天。在利用这五大零时差漏洞的攻击中，有 57% 在最初 90 天内被赛门铁克端点技术阻止，而且往往是在出现可用修补程序之前阻止的。*

## 2006–2014 年全年累计零时差漏洞




来源：赛门铁克 | SDAP

## 五大零时差漏洞



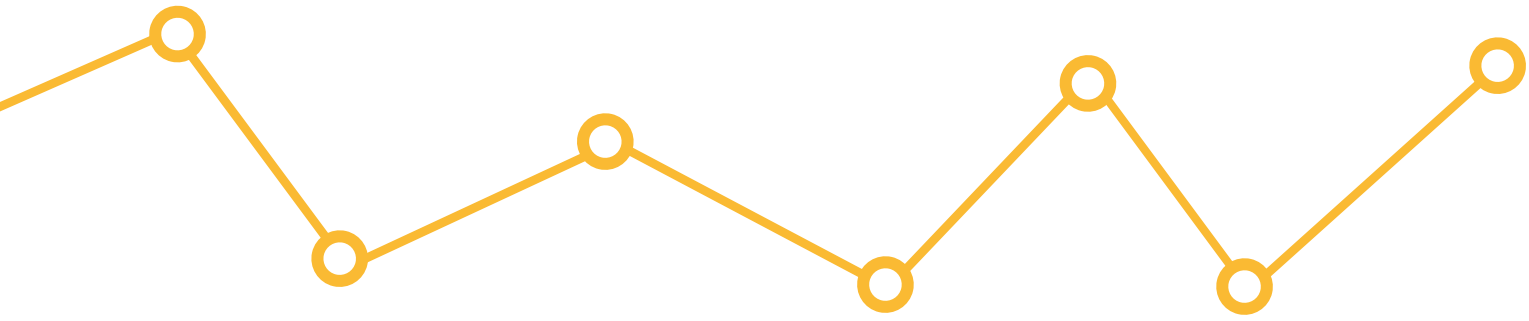

*2014 年最经常被利用的零时差漏洞的窗口期（即公布漏洞至发布修补程序之间相隔的时间）延长了。CVE-2014-0322、CVE-2014-0515 和 CVE-2014-4114 都在 2014 年的多场目标性攻击中被利用，其中包括与 Hidden Lynx 和 Sandworm 有关的攻击。*

# 威胁情报

如今，对任何组织来说，若要了解自身网络面对的潜在威胁，威胁情报已成为至关重要的组成部分。

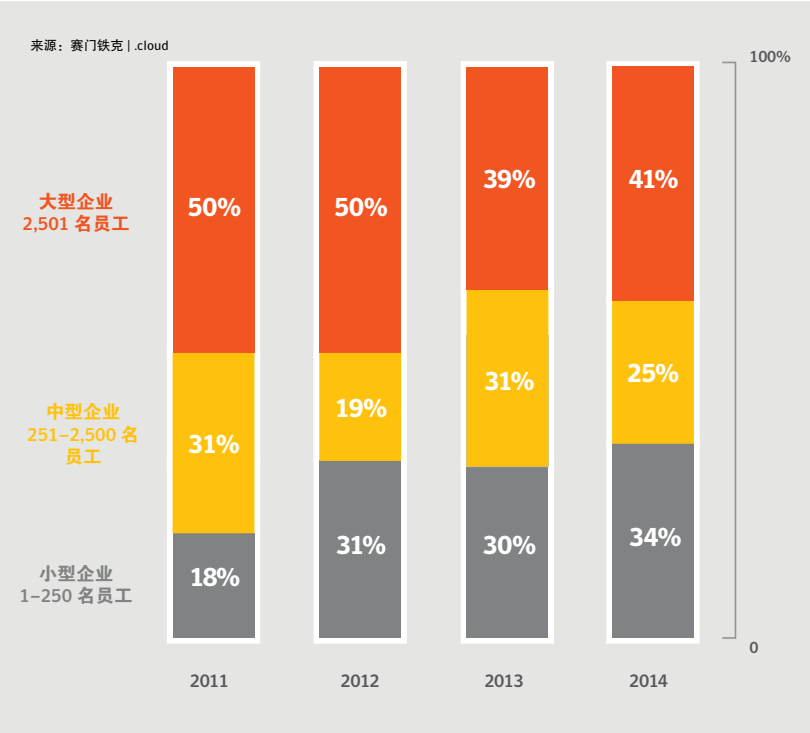
投资于卓越的技术仅仅在部分程度上解决问题，而威胁情报、风险管理和最佳技术解决方案的结合不仅有助于揭示受威胁的目标，还有助于揭示威胁的方式和原因。了解这些威胁是至关重要的，因为当今的企业难免会被攻击 —— 问题不在于是否会被攻击，而在于何时会被攻击。

在漏洞利用工具包的帮助下，技术先进的攻击者不仅针对旧的漏洞，也针对新的零时差漏洞。擅于防御意味着您的防线难以被攻破。威胁情报可以将整个企业的所有可用信息关联起来，由此提供可疑事件的优先级列表。对人员、人员技能以及流程的持续评估将确保遵循最佳响应，并确保流程的不断更新和技能的维持。如果企业可以加强防御能力，那么攻击者就必须更加煞费苦心地寻求突破点。不要成为供应链中最薄弱的环节。



# 目标性攻击采用的技巧

## 2011–2014 年不同规模的企业遭受鱼叉式网络钓鱼攻击的风险比例




*2014 年，41% 的鱼叉式网络钓鱼电子邮件针对的是大型企业。而在 2013 年，针对中小型企业的鱼叉式网络钓鱼攻击说明了规模较小、相对不知名的企业并不能免于威胁。实际上，2014 年的攻击证实了顽固的攻击者往往以攻击目标公司供应链的方式包抄这些公司的安全措施。*

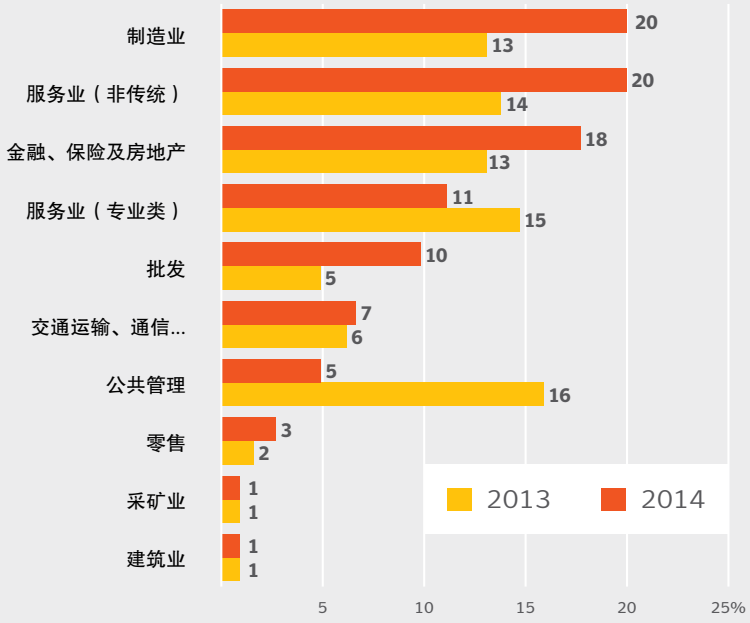
## 不同规模的企业遭受鱼叉式网络钓鱼攻击的风险比例

来源：赛门铁克 | .cloud, SRL

| | 2014 年<br>风险比例 | 2014 年<br>风险比例 (%) | 2013 年<br>风险比例 | 2013 年<br>风险比例 (%) |
|---|---|---|---|---|
| *大型企业<br>员工人数超过 2500* | 1/1.2 | 83% | 1/2.3 | 43% |
| *中型企业<br>251–2,500* | 1/1.6 | 63% | 1/3.5 | 33% |
| *小型企业<br>1–250* | 1/2.2 | 45% | 1/5.2 | 19% |

*2014 年，83% 的大型企业成为鱼叉式网络钓鱼活动的目标，而在 2013 年，该比例为 43%。*

## 2013–2014 年鱼叉式网络钓鱼攻击针对的十大行业




*整体而言，2014 年的鱼叉式网络钓鱼攻击在数量上的最主要目标行业是制造业，其中 1/5（即 20%）的攻击针对的是制造业企业。*

来源：赛门铁克 | .cloud

## 不同行业遭受鱼叉式网络钓鱼攻击的风险比例

| 2014 年行业 | 2014 年风险比例 | 2014 年风险比例 (%) |
|---|---|---|
| 采矿业 | 1/2.3 | 43% |
| 批发 | 1/2.9 | 34% |
| 制造业 | 1/3.0 | 33% |
| 交通、通信、电力、燃气及卫生服务 | 1/3.4 | 29% |
| 公共管理 | 1/3.4 | 29% |
| 金融、保险及房地产 | 1/4.8 | 21% |
| 零售 | 1/4.8 | 21% |
| 服务业（非传统） | 1/6.5 | 15% |
| 服务业（专业类） | 1/6.9 | 15% |

| 2013年行业 | 2013 年风险比例 | 2013 年风险比例 (%) |
|---|---|---|
| 采矿业 | 1/2.7 | 37% |
| 公共管理（政府） | 1/3.1 | 32% |
| 制造业 | 1/3.2 | 31% |
| 批发 | 1/3.4 | 29% |
| 交通、通信、电力、燃气及卫生服务 | 1/3.9 | 26% |
| 金融、保险及房地产 | 1/4.8 | 21% |
| 服务业（非传统） | 1/6.6 | 15% |
| 建筑业 | 1/11.3 | 8% |
| 农业、林业及渔业 | 1/12.0 | 8% |

来源：赛门铁克 | .cloud, SRL

*采矿业是 2014 年最常被攻击的行业，多达 43% (1/2.3) 的采矿企业在这一年里至少被攻击过一次。采矿业这个类别包括能源开采企业以及开采金属和矿物的企业。*

## 每日鱼叉式网络钓鱼电子邮件

| 2014 | 变化 | 2013 | 变化 | 2012 |
|---|---|---|---|---|
| 73 | -12% | 83 | -28% | 116 |

来源：赛门铁克 | STAR Malware Ops

*赛门铁克检测到的鱼叉式网络钓鱼电子邮件的数量略有下降，但是没有迹象表明目标性攻击的力度也在渐弱。电子邮件攻击活动的总体数量有所增加，而鱼叉式网络钓鱼电子邮件变得更为隐蔽，为绕过安全措施而使用自定义编写的恶意软件和精心打造的社交骗局信息。*

## 鱼叉式网络钓鱼电子邮件活动

来源：赛门铁克 | .cloud, SRL

| | 2014 | 变化 | 2013 | 变化 | 2012 |
|---|---|---|---|---|---|
| *活动* | 841 | **+8%** | 779 | **+91%** | 408 |
| *每次活动的接收者* | 18 | **-20%** | 23 | **-81%** | 111 |
| *每次活动的攻击量* | 25 | **-14%** | 29 | **-76%** | 122 |
| *活动的平均时间* | 9 天 | **+13%** | 8 天 | **+173%** | 3 天 |

*在 2014 年，通过鱼叉式网络钓鱼活动发动的目标性攻击增加了 8%，但每日发送的鱼叉式网络钓鱼电子邮件数量整体下降了 12%。2014 年的鱼叉式网络钓鱼攻击在风格上更加不像垃圾邮件，减少了向大量收件人群发的电子邮件。攻击者在发动攻击之前花费了更多时间进行计划和协调，尤其注重侦察。赛门铁克还观察到几场看似由多个攻击者团体协调开展的“分布式目标性攻击”。这些攻击的计划和分发方式导致即使发送的电子邮件数量相对庞大，它们也不会被归为垃圾邮件。*

## 鱼叉式网络钓鱼电子邮件词云


鱼叉式网络钓鱼攻击中最常用的词语

来源：赛门铁克 | .cloud, SRL

## 不同职位遭受鱼叉式网络钓鱼攻击的风险比例

来源：赛门铁克 I .cloud, SRL

| 2014 | 2014 年风险比例 | 2014 年比例 (% ) |
|---|---|---|
| 销售 / 营销 | 1/2.9 | 35% |
| 运营 | 1/3.8 | 27% |
| 财务 | 1/3.3 | 30% |
| 研发 | 1/4.4 | 23% |
| IT | 1/5.4 | 19% |
| 工程 | 1/6.4 | 16% |
| 人力资源及招聘 | 1/7.2 | 14% |
| 其他 | 1/9.3 | 11% |

*销售和营销人员是 2014 年最主要的攻击目标，其中每 2.9 人就有 1 人被攻击过至少一次，相当于 35% 的销售和营销人员曾遭到攻击。*

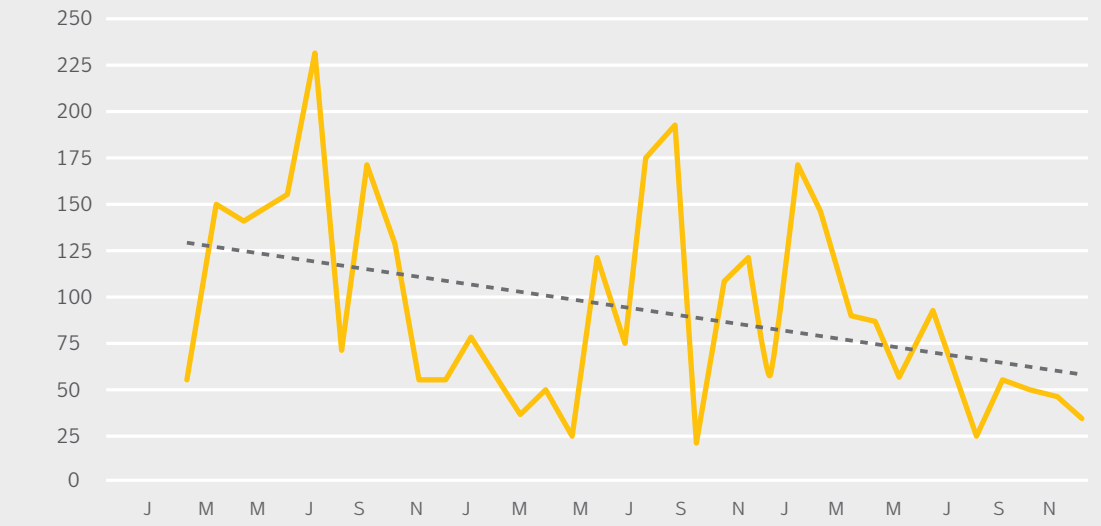
## 不同工作级别遭受鱼叉式网络钓鱼攻击的风险比例

来源：赛门铁克 | .cloud, SRL

| 2014 | 2014 年风险比例 | 风险比例 (%) |
|---|---|---|
| 经理 | 1/3.8 | 26% |
| 独立贡献者 | 1/3.7 | 27% |
| 实习生 | 1/3.9 | 26% |
| 总监 | 1/5.4 | 19% |
| 支持人员 | 1/7.6 | 13% |
| 其他 | 1/9.3 | 11% |

*经理是 2014 年最经常受到攻击的工作级别，其中每 3.8 人就有 1 人被攻击过至少一次，相当于 26% 的管理级别的人员曾遭到攻击。*

## 2012–2014 年鱼叉式网络钓鱼攻击的每天平均数




来源：赛门铁克 | .cloud

## 对 2013-2014 年目标性攻击所用的鱼叉式网络钓鱼电子邮件的分析

| *排名* | 可执行文件的类型 | 2014 年整体比例 | 可执行文件的类型 | 2013 年整体比例 |
|---|---|---|---|---|
| *1* | .doc | 41.2% | .exe | 31.3% |
| *2* | .exe | 24.0% | .scr | 18.4% |
| *3* | .scr | 9.7% | .doc | 7.9% |
| *4* | .au3 | 8.7% | .pdf | 5.3% |
| *5* | .jpg | 4.9% | .class | 4.7% |
| *6* | class | 3.6% | .jpg | 3.8% |
| *7* | .pdf | 3.3% | .dmp | 2.7% |
| *8* | .bin | 2.0% | .dll | 1.8% |
| *9* | .txt | 1.5% | .au3 | 1.7% |
| *10* | .dmp | 1.1% | .xls | 1.2% |

*2014 年，41% 的攻击使用了 Office 文档附件，比例超过可执行文件，成为鱼叉式网络钓鱼攻击中最常用的附件策略。如果公司在电子邮件网关阻止可执行文件附件和屏幕保护程序，那么至少 35% 的鱼叉式网络钓鱼攻击是可以避免的。恶意文档附件还可能被呈现为安全附件，然后通过强大的云过滤功能抵达电子邮件网关（云过滤可以识别和解除鱼叉式网络钓鱼攻击，使其无法进入公司网络）。*

来源：赛门铁克 | .cloud

# 转变目标和技巧

**文：赛门铁克攻击分析托管和威胁情报团队**

赛门铁克多年来努力保障客户的安全，并注意到我们的网络对手表现出相当高的灵活性和适应力。由此导致非政府行为体发动的目标性攻击大量涌现，而在此之前，政府被认为是唯一拥有这种能力和意图的行为体。

这种情况在 2014 年仍然保持不变。赛门铁克通过 DeepSight 安全情报服务，跟踪并报告了我们的网络对手（即开展恶意攻击的行为体），以及他们的工具、技巧和活动。[69] 我们在 2014 年发现的两大变化与转变技巧和目标有关。

网络罪犯越来越多地将恶意活动与善意行为相结合，以此瞄准全球各地的网络。这些行为体在针对环境准备发动攻击时，会限制使用恶意软件和可检测到的攻击工具，以避免防御者的检测和随后作出的安全性改进。虽然涉及含有恶意软件和第二阶段攻击的恶意软件（以保持网络访问权）的鱼叉式网络钓鱼电子邮件的入侵依然是非常盛行的入侵方式，但是利用可产生合法网络活动的工具（如网络管理工具）来使用特权用户帐户已成为普遍现象。赛门铁克已经发现和曝光了这种网络入侵以及今年在零售业企业客户中保持持续访问权限的方法，并预计网络对手群体将越来越多地采用这种技巧。

为了降低这类攻击的风险，除了依靠基于签名的检测之外，防御者还应识别和降低由在他们网络上运行的任何合法但不必要的服务带来的风险。这些服务可能会被攻击者用来进行横向移动、特权提升和向外渗漏。他们还应解决来自不对称攻击向量的风险，例如防御较差的有关方面（如供应商）的网络连接。

对金融和其他高姿态行业的攻击有增无减，而在 2014 年发现多宗网络间谍活动将目标定为通过工业控制系统 (ICS) 技术实现物理流程自动化的重点行业，例如能源和制造业等。在过去的一年里，赛门铁克检测到针对 ICS 技术的若干活动，例如某些行为体使用 BlackEnergy 恶意软件对专业化 ICS 软件程序进行漏洞利用、Dragonfly 团体使用特洛伊木马式 ICS 捆绑软件传播 Backdoor.Oldrea[70]（又名 Havex，被 Dragonfly 团体使用）来侦察 ICS 网络协议和端口。鉴于这些攻击可能会对目标企业和国家产生的影响，我们可以预计某些类别的网络对手将继续增强他们利用 ICS 弱点的能力。

ICS 技术的防御者不应单单依赖这些环境有限的连接性和独特的体系结构。鉴于资产的敏感性，应当实施强力的安全控制措施，并利用环境的确定性，通过安全监控来识别异常行为。

[69] http://www.symantec.com/deepsight-products/
[70] http://www.symantec.com/security_response/writeup.jsp?docid=2013-052817-2105-99

# 为工业控制系统保驾护航

**文：Preeti Agarwal**

目标性攻击已经从乳臭未干的入侵尝试演变成网络间谍的必备武器。工业控制系统 (ICS) 是这些攻击者的主要目标，其动机是在国家安全级别上执行攻击。这些趋势导致多个国家加强投资并制定策略，以提高 ICS 安全。

“工业控制系统”一词是指控制、监控和管理电力、水和废水、石油和天然气、交通运输等工业领域的关键基础架构的设备。不同的 ICS 类型包括监督控制与数据采集 (SCADA)、可编程逻辑控制器 (PLC)、分布式控制系统 (DCS) 等等。

针对 ICS 的攻击已经成为一种普遍现象，并有可能造成严重的社会影响和经济影响。但这些攻击经常会未被公开，从而限制了受害者的公关后果，并低估问题的严重程度。

至今已发生了多次攻击，其意图包括网络间谍、破坏 ICS 中的公用设施等。2010 年，专门攻击特定 SCADA 系统的 Stuxnet 被发现，并破坏了伊朗核系统的实体设施。此后，威胁环境中陆续出现了众多武器化恶意软件，2014 年也不例外。网络间谍活动 Dragonfly 针对一系列目标，但主要针对能源行业，其背后的攻击者成功地破坏了目标组织中具有重要战略意义的多个 ICS。假如这些攻击者使用了他们可以使用的破坏功能，那么他们可破坏或中断受影响国家的能源供应。

最近，Sandworm 发动了复杂的目标性恶意软件活动，感染了数家知名 ICS 厂商的人机界面 (HMI)。攻击者通过连接到 HMI 的互联网利用 ICS 软件中的漏洞。这些入侵有可能是为其他攻击而进行的侦察活动。

2014 年最新增加的一桩攻击事件是德国境内某钢铁厂的工厂网络遭遇网络攻击，对该厂的一座高炉造成巨大损害。[71]

A 针对 ICS 的攻击已经成熟并日趋频繁，导致这些系统的安全性成为至关重要和亟待解决的问题。

很多 ICS 在安装后都会运行多年。这常常会导致植根于“隐晦式安全”这种思路的安全策略，希望通过物理隔离、专有协议和专用硬件来保障系统的安全。在这些系统中，有很多是在企业使用互联网技术之前开发的，其设计侧重于可靠性、易维护性和可用性，很少关注或完全不关注安全性。然而，对于远程访问和企业连接性的迫切需求大大改变了攻击面，使这些系统暴露出新的安全漏洞可供攻击。

如今，这些攻击的主要切入点是防御薄弱的可访问互联网的关键基础架构设备。为了提供远程访问，用于监视和控制工厂及设备的 SCADA 系统元素通过公司网络而连接到互联网。这些 SCADA 元素暴露了控制网络，并构成攻击风险，这些风险包括扫描、探测、暴力破解尝试、未经授权而访问这些设备等。

在攻击中利用这些设备的其中一种方法是通过 HMI，而 HMI 通常从公司网络即可访问。攻击者可以通过利用任何现有的零时差漏洞来感染公司主机，搜寻任何可访问控制网络的主机，并尝试利用这些信息入侵 ICS。

利用 ICS 的另一种方法是通过直接连接互联网的 HMI。借助常用的搜索引擎，攻击者可以在互联网上轻易发现这些面向互联网的设备。在发现控制设备之后，他们就可以通过漏洞利用或不当配置来感染该设备。发动这些攻击对知识水平的要求相当低。

[71] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

除了上述切入点之外，ICS 及其软件还存在多个固有漏洞，这等于向网络敌手敞开了大门。其中很多专有的 Web 应用程序存在安全漏洞，可导致缓冲区溢出、SQL 注入或跨站脚本攻击等。薄弱的身份验证和授权技术可能会导致攻击者获得访问关键 ICS 功能的权限。ICS 协议中薄弱的身份验证可导致中间人攻击，如数据包回放、欺骗等。攻击者最终可能会向 PLC 发送流氓指令或向 HMI 发送虚假状态。

用于 PLC 编程的梯形逻辑是 ICS 环境中的关键资产。用于设计和上传这种 PLC 梯形逻辑的工程工作站一旦遭到感染，就可能导致反向工程，而反向工程可被用来酝酿攻击。

保障 ICS 环境的安全需要制定全面的安全计划，以帮助企业确定其安全目标，包括标准、法规遵从性、潜在风险因素、业务影响以及需要采取的缓解措施。建立一个安全的 ICS 环境需要将安全整合到从计划到日常运作的各个工业过程环节。

应当将控制网络和企业网络之间的网络级隔离作为绝对要求，因为这样能大大降低从企业网络内发起攻击的几率。然而，从实际情况来考虑，需要从企业网络连接 ICS。在这种情况下，应当限制接入点，并使用防火墙提供保护，还应当利用可信的通信渠道（如 VPN）。

ICS 环境不断演变，厂商对通用 SCADA 服务器和工程工作站的控制设备上的安全软件增加了支持。然而，PLC、DCS 等系统仍然使用厂商特定的自定义操作系统。这些控制系统一经安装，就完全不能容许停机时间、有限资源和依赖于时间的代码。这样就限制了部署专为 IT 计算机系统设计的传统企业安全解决方案的机会。鉴于种种挑战，任何解决方案都不是保护 ICS 安全的法宝。相反，必须在每个层面实施端到端安全措施，这些层面包括网络外围、企业内部接入点、外部网络接入点、网络层面以及主机和应用层面。

此外，控制设备本身也应当采取安全设计。制造商有责任确保在出货前就在控制设备中内置安全性。

展望未来，我们可能会看到这样一个趋势：越来越多的人将使用提供 HMI 访问和控制选项的移动技术。尽管移动解决方案从管理效率的角度来看极具吸引力，但是它将揭开与移动使用模式有关的新的攻击面。

我们还可能会看到 ICS 攻击通用技术的形成。因此，我们或许会看到免费提供的 ICS 漏洞利用工具包的增加。毫无疑问，这一趋势将导致 ICS 攻击数量的增长。

就像衍生出多个变种的 Stuxnet 那样，后来出现的主要针对 ICS 的威胁也具有相似的攻击媒介和构件，利用常见 ICS 协议和通用特洛伊木马。ICS 上很有可能存在尚未被检测到的威胁，这些威胁被攻击者鬼鬼祟祟地安装好，暂时按兵不动。攻击者可能随时找到理由激活这些被动的攻击。我们完全有可能会看到更多关键基础架构的漏洞利用事件大爆发，构成重大危险。

# 展望


后见之明 + 深刻洞察 = 前瞻远见

# 展望

**安全游戏化**

15 世纪的安全顾问尼可罗 • 马基亚维利 (Niccolo Machiavell) 说：“人类太单纯，而且很容易屈服于眼下的欲望，所以耍诡计的人总能找到被诡计耍的人。”

互联网安全对人为因素的依赖不亚于对技术的依赖。如果人们更高明一些，就能帮助减少他们面临的风险。消费者避免被骗和政府雇员避免目标性攻击采用的社交骗局都是这个道理。

在这个语境里，利用简单的电脑游戏带来的心理回报和即时满足，可以用“游戏化”[i]将“眼下的欲望”变成持久的行为变化。例如，游戏化可以用来训练人们警惕网络钓鱼电子邮件或生成、记住和使用强密码。

我们看到了这种培训在未来数年里巨大的市场机遇和庞大需求。

**安全模拟**

企业可以通过利用模拟和安全“演习”，做好应对安全漏洞的准备，并加深对自身防御的了解。通过将传统的渗透测试延伸到模拟响应及补救阶段中，企业可以培训员工和改善他们的就绪状态。这一措施同样适用于政府。2015 年 1 月，英国首相戴维 • 卡梅伦和美国总统巴拉克 • 奥巴马达成了两国之间进行网络攻击“演习”的协议[ii]。企业应该会在 2015 年陆续效仿。

**不甘罢休的攻击者可能会成功**

在攻击者和企业 IT 安全人员之间的斗争中，邪恶的一方只要有一次侥幸就能得逞。IT 部门必须每次都把握好运，这样才能立于不败之地。考虑到这一点，IT 管理者（其实消费者也一样）需要做好最坏的打算。没有任何神奇的技术能够保证在互联网犯罪或坚持不懈的目标性攻击前，赋予您金刚不坏之身。所以，不妨假设您已被黑客攻击或者即将被黑客攻击。从“安全 / 不安全”的二元观点转变为细致入微、近乎医学式的观点来看待趋势、症状以及行为预防、诊断和治疗。

在技术层面上，这意味着确保您在每个端点、网关和电子邮件服务器上都具备有效的数据丢失预防软件，以防止数据向外渗漏。这也意味着备份和灾难恢复的重要性大大提高，检测和响应计划也是如此。这不是绝望之中的建议 —— 在任何时候，我们都不应该放弃防范，否则就等于为攻击者大开方便之门。与其事后追悔，不如事前明智[iii]。

**企业之间的数据分享是必不可少的**

企业之间的数据分享对安全而言是必不可少的[iv]。一直以来，企业都不敢与其他企业分享太多信息，于是他们一直都依赖自己的内部资源，与不法之徒单打独斗。我们认为企业有必要共享威胁情报，并分享交流他们打击罪犯的经验。可以帮助他们在分享之余兼顾知识产权保护的工具将变得日益重要。例如，安全电子数据交换可以分享哈希 (hash)、二进制属性、症状等等，同时不会透露企业机密或可能对攻击有用的信息。

**不安全的操作系统**

四分之一的 PC 用户在 2014 年 7 月仍在运行 Windows XP 和 Office 2013[v]，即使他们的软件已经不再受到支持，并且 Microsoft 也终止了相应的更新。许多人仍然对这场改变持怀疑态度[vi]。这使他们在新的威胁出现时处于无修补程序状态。在接下来的一年里，这将构成重大的安全风险。对于运行过时操作系统的嵌入式设备，企业需要找到新的方式来保护它们，直到可以更换或升级这些设备。

**物联网**

越来越多的消费者购买智能手表、活动追踪器、全息耳机以及在美国硅谷和中国深圳横空出世的各种新型可穿戴设备，针对这些设备提高安全性也成了日益迫切的需要。这是一个日新月异的环境。在这个环境里，创新胜过隐私。由于缺乏政府监管和适合媒体报道的恐慌新闻，并且消费者的危险意识也有待提高，安全和隐私不太可能得到应有的重视[vii]。

[i] Gamification from Efrain Ortiz interview
[ii] http://www.bbc.co.uk/news/uk-politics-30842669
[iii] Assume you've been hacked from Efrain Ortiz interview
[iv] Efrain Ortiz
[v] http://www.informationweek.com/software/operating-systems/windows-xp-stayin-alive/d/d-id/1279065
[vi] Candid Wueest interview
[vii] Vaughn Eisler interview

网站安全威胁报告的
第 2 部分即将推出，不容错过

## 第 2 部分：数据泄露、社交媒体骗局、建议与最佳实践


在第 2 部分中，您将掌握网络间谍活动的最新形式，了解最近爆发的数据泄露事件和社交媒体骗局，并展望未来的威胁态势。此外，不要错过赛门铁克的信息图表，整个报告中的关键见解一目了然。

# 关于赛门铁克

Symantec Corporation（纳斯达克：SYMC）是信息保护领域的专家，帮助个人、企业和政府随时随地自由探索技术所带来的机遇。赛门铁克成立于 1982 年 4 月，作为一家财富 500 强公司，运营着全球最大的数据情报网络之一，为重要信息的存储、访问和共享提供一流的安全、备份和可用性解决方案。公司拥有 20,000 多名员工，分布在 50 多个国家。99% 的财富 500 强公司是赛门铁克的客户。在 2013 财政年度，赛门铁克的营收为 69 亿美元。

要了解更多信息，请访问 **www.symantec.com**

或登录 **go.symantec.com/socialmedia** 与赛门铁克联系。

**更多信息**

- 赛门铁克中国：http://www.symantec.com/
- 《互联网安全威胁报告》和赛门铁克情报资源：http://www.symantec.com/threatreport/
- 赛门铁克安全响应中心：http://www.symantec.com/security_response/
- 诺顿安全情报：http://us.norton.com/security_response/threatexplorer/
- 诺顿网络犯罪指数：http://us.norton.com/cybercrimeindex/

如需了解特定国家或地区的办事处和联系电话，请访问我们的网站。

**澳大利亚**：+61 3 9674 5500
**新西兰**：+64 9 9127 201
**新加坡**：+65 6622 1638
**香港**：+852 30 114 683
**中国**：+86 400 010 5880
**台湾**：+886 2 2162 1992
**或发送电子邮件至** ssl_sales_au@symantec.com
ssl_sales_asia@symantec.com


**赛门铁克**
Symantec Website Security Solutions Pty Ltd
3/437 St Kilda Road, Melbourne,
3004, ABN: 88 088 021 603
**www.symantec.com/en/aa/ssl-certificates**