报告

迈克菲威胁报告：2009 年第一季度

作者：McAfee® Avert® Labs

目录

《迈克菲威胁报告》为您提供了有关基于电子邮件和 Web 威胁的最新统计和分析信息。此报告由 McAfee Avert Labs 的研究人员编写，每季度发布一次。McAfee Avert Labs 研究人员遍布世界各地，他们以独特的视角分析当前存在的威胁，这些威胁可能来自美国乃至世界各地，并将影响个人及企业用户。我们将分析过去三个月中出现的主要安全问题，请立即加入我们吧。您加入后便可以在迈克菲威胁中心查找更多信息：http://www.mcafee.com/us/threat_center/default.asp 或 www.trustedsource.org。

与一年前甚至几个月前相比，我们发现 2009 年第一季度出现的威胁发生了很多重大变化。没有人能够在十二个月前预测到垃圾邮件数量会下降，但是 2008 年 11 月 McColo 关闭后，这种情况确实发生了。现在垃圾邮件数量仍比峰值水平低 30%，与历史同期相比，我们并没有发现三月份的垃圾邮件数量出现增长。问题并不在于垃圾邮件数量**是否**会恢复到以前的水平，而在于**何时**会恢复到以前的水平。有关新搭建的僵尸网络的数据表明，恐怕用不了多久就将达到这一数量。

随着恶意网站数量的增加，提供恶意软件的网站也会增加，每天都会新增数千个这样的网站。每天都会出现新形式的恶意软件，本报告将详细说明最流行的恶意软件。

与最近出现的所有安全威胁一样，Conficker 蠕虫（正式名称为 W32/Conficker.worm）受到了广泛关注。本报告将从多个角度分析这种威胁是媒体炒作，还是确实存在的。我们还将着重介绍一些并未获得媒体同等关注的威胁。事实上，这些威胁可能比那些备受关注的威胁更加危险。

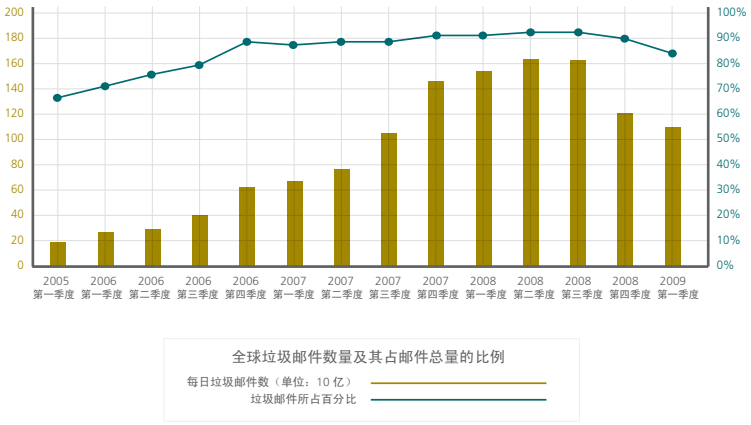
威胁的地域分布情况也在不断发生变化。本报告将分析威胁的地域分布情况，其中包括垃圾邮件源、僵尸网络搭建、恶意软件网站位置以及如何识别刚出现的新威胁。本报告还披露了一些有趣的细节，可以从中看出制造这些威胁的国家/地区并不吝于对其本土用户散布这些威胁。

最后，讨论重点转回到我们自身。我们将浏览一月份所发布的《2009 年威胁预测》报告中的一些预测结果，看看这些预测是否变为现实，或者它们与现实有多大差距。本报告将重点介绍利用当前发生的事件和社交网站向毫不设防的用户传播威胁的情况。

垃圾邮件：仍然是一个全球性问题

下降原因

在 2009 年第一季度，电子邮件和垃圾邮件总量几乎降到两年前的水平。难道垃圾邮件制造者也随着其他行业遭受到了金融危机的影响？事实并非如此。实际情况是：2008 年 11 月关闭 McColo 后，垃圾邮件数量还没有完全恢复。与去年同期相比，2009 年第一季度垃圾邮件数量下降了 20%；与 2008 年第三季度相比，则下降了 30%（去年第三季度的垃圾邮件数量达到了历史最高点）。自垃圾邮件主机被关闭后，垃圾邮件数量恢复了约 70%，但还没有达到以前的水平。



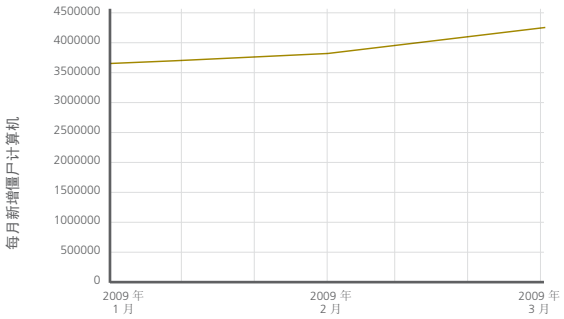
在最近几年里，电子邮件数量往往在三月份达到最高点，但今年三月份没有出现这种情况。去年，平均每天有 1530 亿封邮件，而今年三月份平均每天只有大约 1000 亿封邮件。

自 2006 年以来，垃圾邮件占电子邮件总量的比例首次降到了 90% 以下。在 2008 年全年，电子邮件总量的 90% 是垃圾邮件，而上一季度这个比例只达 86%。虽然电子邮件帐户及其活动千差万别，但我们还是可以估算出每个帐户每天比去年少收到 6-12 封电子邮件。

我们相信垃圾邮件数量必定会恢复到 2008 年的水平，但垃圾邮件制造者在 McColo 关闭后重新搭建指挥中心和僵尸网络的时间比很多人最初预测的要长。从根本上讲，对于垃圾邮件制造者来说，这是一个投资回报问题，与其他行业并无两样。

新的僵尸网络正在搭建

在本季度，我们检测到将近有 1200 万个新 IP 地址是以“僵尸计算机”（受垃圾邮件制造者或其他人控制的计算机）的形式存在的。与 2008 年第四季度相比，这一数字已显著增加，增幅接近 50%。2008 年第三季度新增的僵尸计算机数量就已创下历史记录，但仍比本季度少 100 万台。虽然垃圾邮件数量还没有从 McColo 关闭中恢复，但新僵尸计算机的活动程度表明，垃圾邮件制造者正在开足马力重建所拆掉的架构。不久，垃圾邮件数量就会恢复到以前的水平。



我们可以按国家/地区划分被感染的系统。上一季度，63% 的新僵尸计算机来自前 10 个国家/地区。与之前的两个季度相比，这一数字略有下降。这表明垃圾邮件制造者正将魔爪伸向更多国家/地区的计算机，以达到他们的最终目的。

2009 年第一季度		2008 年第四季度		2008 年第三季度	
国家/地区	**IP 数所占比例**	**国家/地区**	**IP 数所占比例**	**国家/地区**	**IP 数所占比例**
美国	18.0	中国	15.8	中国	20.4
中国	13.4	美国	15.4	美国	16.5
澳大利亚	6.3	德国	6.5	德国	6.8
德国	5.3	英国	6.0	英国	6.0
英国	4.7	巴西	4.9	巴西	4.8
巴西	4.0	西班牙	4.3	西班牙	3.7
印度	3.1	澳大利亚	4.1	印度	2.5
西班牙	3.0	意大利	3.5	俄罗斯	2.4
韩国	2.8	俄罗斯	3.1	韩国	2.4
俄罗斯	2.5	韩国	2.4	意大利	2.2
总计	**63.3**	**总计**	**66.0**	**总计**	**67.5**

在过去三个季度里，中国和美国一直占据着榜首位置，受垃圾邮件制造者控制的僵尸计算机数量一直居高不下。另一个值得注意的国家是澳大利亚，该国在 2008 年第三季度还没有进入前 10 位。可在随后的两个季度里，僵尸计算机数量快速攀升到第 3 位，在新增僵尸计算机总量中占到 6%。南方大陆真可谓是一块“沃土”，为僵尸计算机提供了赖以滋生的温床。

2009 年第一季度		2008 年第四季度	
国家/地区	**占总量比重**	**国家/地区**	**占总量比重**
美国	35.0	美国	34.3
巴西	7.3	巴西	6.5
印度	6.9	中国	4.8
韩国	4.7	印度	4.2
中国	3.6	俄罗斯	4.2
俄罗斯	3.4	土耳其	3.8
土耳其	3.2	韩国	3.7
泰国	2.1	西班牙	2.4
罗马尼亚	2.0	英国	2.3
波兰	1.8	哥伦比亚	2.0
	70.0		**68.3**

按国家/地区划分的垃圾邮件：美国再次成为全球领跑者

美国汽车厂商可能遇到了生产和销售问题，但美国的垃圾邮件制造者继续成为全球领跑者，其制造的垃圾邮件占全球垃圾邮件输出量的 35%。虽然垃圾邮件指挥和控制操作的基础设施是全球性的，但是垃圾邮件制造者仍然偏爱使用美国境内的计算机来制造垃圾邮件。前 10 个国家/地区在垃圾邮件生产方面遥遥领先，几乎占到垃圾邮件总量的 70%，远高于世界其他 200 多个国家/地区的总和。

从过去的两个季度看，我们发现印度的增长比例最大，现在占到全球垃圾邮件的 7% 左右。与上一季度相比，他们输出的垃圾邮件增加了一倍。这也许是印度产业外包所尝试的最新行业。

除印度之外，泰国、罗马尼亚和波兰也跻身到前 10 位。这些数据印证了垃圾邮件制造者正在四处寻找新的源头，以便为其垃圾邮件引擎提供动力。

	2009 年第一季度		2008 年第四季度		2008 年第三季度
处方药	25.0	处方药	37.0	男性保健品	31.2
广告	21.9	广告	19.3	广告	19.3
仿制品	18.8	男性保健品	16.8	处方药	10.7
男性保健品	17.5	DSN	9.5	Storm	8.0
DSN	7.1	约会	3.9	DSN	7.7
Storm	1.6	仿制品	2.6	最新消息	6.7
文凭证书	1.1	就业	1.7	仿制品	6.0
软件	1.1	软件	1.5	债务贷款	1.6
债务贷款	1.0	债务贷款	1.2	银行	1.1
其他	4.9	其他	6.5	其他	7.7
	100.0		**100.0**		**100.0**

按类型划分的垃圾邮件：性、毒品和其他

在发送的垃圾邮件类型中，男性保健品、处方药和一般广告一直名列前茅。在过去的三个季度里，这三类垃圾邮件约占发送的垃圾邮件总量的 60%。好象曾经流行一时的文化口号“性、毒品和摇滚乐”又回来了，但只是好像。可能我们已经发展到一定程度，所以现在的口号更像是“性、毒品和经济”。

仿制品垃圾邮件（大多是仿制手表）的数量在本季度大幅攀升，大约占到垃圾邮件总量的 19%。这种仿制品垃圾邮件过去就十分流行，但本季度仍然涨幅明显。这表明，在经济形势非常恶劣的情况下，垃圾邮件制造者正在通过销售价格低廉的冒牌货来扩大我们的购买力。

发送状态通知垃圾邮件数量保持稳定，占到垃圾邮件总量的 8%。这些邮件大多与网络钓鱼攻击有关，在骗取受害人的电子邮件地址后将向受害人发送退信通知。很明显，网络钓鱼仍然十分猖獗。其中的很多邮件与财务有关，并试图获取受害人的个人信息。

垃圾邮件制造者无视任何国家/地区的主权，即使是他们自己的国家/地区

网络安全社区流传着这样一种说法，网络犯罪分子更愿意将西方国家作为攻击目标，而避免攻击受本地司法管辖的个人或公司，据称这些网络犯罪分子大多居住在东欧国家。但是我们逐渐发现与这一说法并不相符的数据。互联网没有地域界限。很显然，网络犯罪分子会攻击他们发现的任何目标。我们已经找到一些证据，表明俄罗斯和东欧国家的一些重要政府机构和公司及其高级官员饱受网络骗子的侵扰。

McAfee TrustedSource™ 最近发现，来自俄罗斯的很多政府部门和银行机构的电子邮件和垃圾邮件含有恶意软件。根据我们的分析，饱受侵扰的俄罗斯银行包括：

- Rusfinance Bank
- OGO Bank
- Tusarbank
- Link Capital Investment Bank
- The Maritime Bank
- Vladivostok Alfa Bank
- Bank Eurotreid
- Bank Voronezh
- Bashcreditbank
- Enisey's United Bank
- Inter-Svayz Bank

我们的数据还表明，以下俄罗斯政府办公室的计算机系统也被网络犯罪团伙控制：

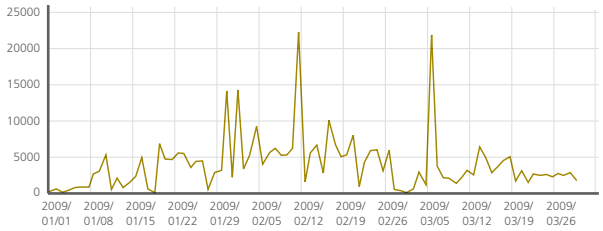
- 纳兹兰地区税务局
- 俄罗斯国家互联网
- 地区财经学院
- 联合核研究所
- 俄罗斯联邦总统办公厅医疗中心
- 俄罗斯联邦养老金协会
- 俄罗斯联邦法院的个人网络
- JSC 车臣蜂窝通信系统

俄罗斯的这些数据表明，网络犯罪分子大多对其目标一视同仁，他们会攻击任何金融机构或其他感兴趣的机构。虽然这种活动主要集中在俄罗斯（并且他们制造的垃圾邮件的绝对数量也最多），但我们的分析表明这种活动在前苏联国家中也非常猖獗，其中包括乌克兰、白俄罗斯、亚美尼亚、阿塞拜疆、格鲁吉亚、哈萨克斯坦、吉尔吉斯斯坦、摩尔多瓦、塔吉克斯坦、土库曼斯坦和乌兹别克斯坦。

Web：每天都会出现新的恶意网站

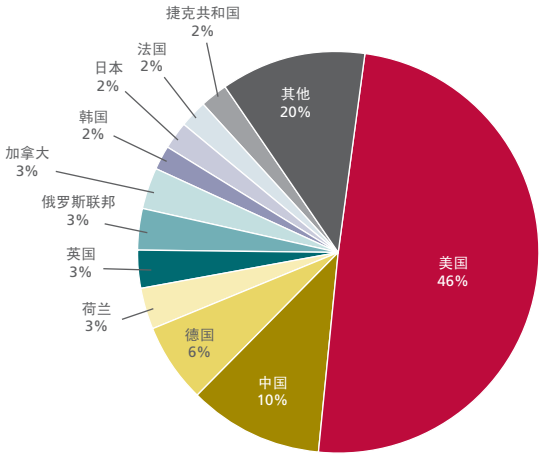
在本季度的研究中，我们发现 2008 年第四季度出现的很多威胁仍然存在，并且呈明显上升趋势。虽然大多数媒体宣传和关注的是 Conficker，但这绝不是本季度流行的唯一威胁。即使忽略 Conficker 活动，我们仍会看到各类威胁在逐年增加，每个季度都必定高于前一季度。恶意反病毒应用程序是 Web 上一个很受关注的问题，与此同时，涉及诈骗和网络钓鱼的活动也有一定的增加。

除了“恶意网站分布”这幅图外，本节中的日常图表和数据并不包括 Conficker 所触及的恶意域。虽然 Conficker 数据是威胁图表的重要组成部分，但它会分散我们关注全部恶意活动的注意力。有很多其他威胁正在变得越来越流行。恶意软件作者和垃圾邮件制造者正在利用我们对经济形势的担忧和恐慌，推出各种各样的诈骗网站。他们的广告包括避免丧失抵押赎回权和各种各样的网络钓鱼网站；他们甚至还提供信誉奖励卡。恶意防病毒网站依然将毫不设防的用户作为攻击目标，并且吸引用户访问网站的手法也在不断翻新。甚至所有 Conficker 活动还推出打折服务，与 2008 年最后两个季度相比，越过“底线”（或“红线”）而划到“恶意”网站的 URL 数量显著增加。



每日新增的恶意网站

这些网络信誉较差的 URL 位于哪里？大多数人肯定回答不出来。



恶意网站分布

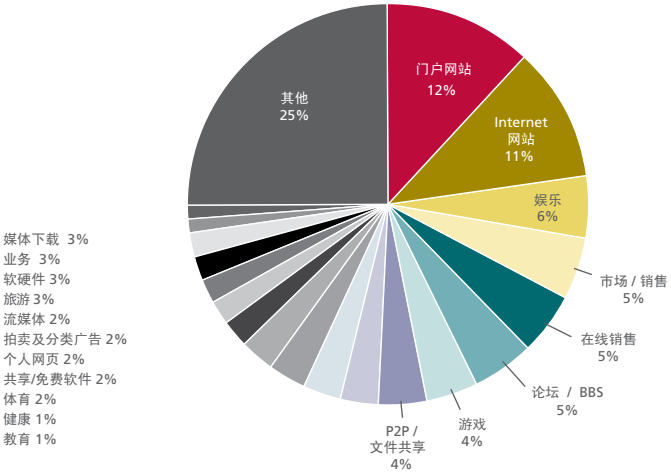
为什么我们之前视为“准则”的恶意网络活动分布（其中美国、中国和俄罗斯排在前三位）会突然发生变化呢？[1] 这并不能说明某些国家/地区的恶意 URL 数量减少了。更确切的说，是其他国家/地区的恶意 URL 数量增加了。在很大程度上，这种增长与 Conficker 将触及或已触及的某些域不无关系。事实上，只此一点便将荷兰推到了第四位。尽管荷兰长期以来一直因托管网络钓鱼 URL 而饱受诟病，但这种增长主要归因

1. 2008 年第三季度的排名顺序为：美国占 41%，中国占 12%，俄罗斯占 7%，德国占和荷兰各占 5%，韩国占 4%，香港占 3%，台湾、加拿大和捷克共和国各占 2%，其他国家/地区占 17%。

于 Conficker 所引起的感染恶意软件的网站和其他此类恶意内容方面的大幅增长。不过，并非所有这一切都是由 Conficker 造成的。加拿大在托管恶意 Web 服务器方面一直排在前十位，这主要归功于这些网站提供的多种恶意软件和间谍软件。

我们发现很重要的一点是，同一国家/地区存在多种攻击媒介（恶意网站、托管间谍软件/广告软件的网站、网络钓鱼和垃圾邮件）。在托管恶意网站方面排在前七位的国家/地区，同时也在托管网络钓鱼、垃圾邮件、恶意软件/广告软件方面排进前十位。

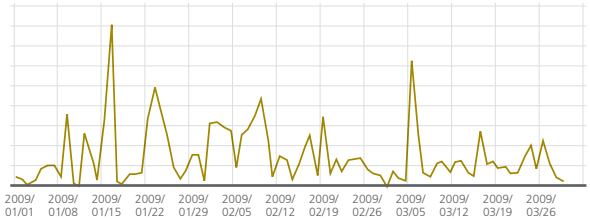
恶意网站在目标选择、合法性、隐蔽性或欺诈性方面千差万别。在访问与知名合法企业没有任何联系的色情或赌博网站时，您仍然会冒较大的风险。不过，没有任何网站是绝对安全的，无论用户访问何种类型的内容都会给恶意软件散布者提供可乘之机。



获得 TrustedSource “恶意网站” 信誉的前 20 种合法类别

在本季度，由于恶意软件散布者将内容服务器作为传播恶意和非法内容的工具，而使内容服务器访问量急剧增加。在信誉良好的知名提供商创办的网站以及不太有名且信誉较差网站上，我们都发现了这种趋势。由于博客和搜索引擎优化技术的广泛使用，这种威胁可谓是如虎添翼。与以前相比，现在为每台计算机配备所有 Web 安全功能显得尤为重要。

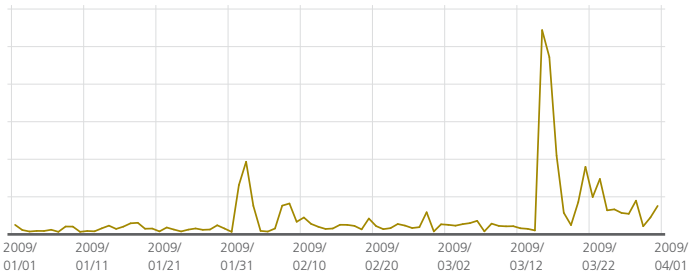
我们已经介绍了威胁的**出处**，现在让我们讨论一下令人关注的威胁**类型**。本季度除了 Conficker 以外，Web 上的新恶意软件和漏洞攻击也一直频繁发生。



新增的提供恶意软件和 PUP 的网站

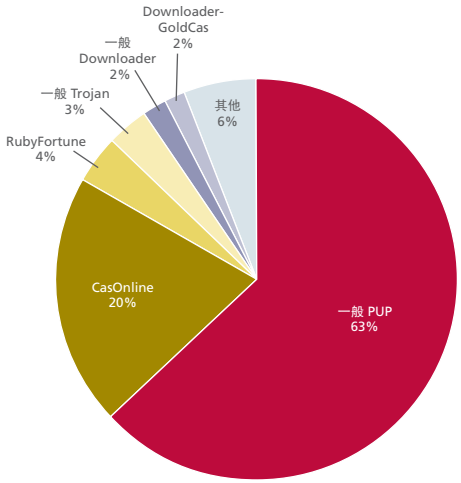
在上面的图表中，说明了 McAfee TrustedSource 网络本季度检测到的提供恶意软件和潜在有害程序 (PUP) 的网站数量。(此图表说明了实际托管恶意软件的网站，并反映了访问这些网站的用户数量。其中不包括因漏洞攻击而导致用户访问恶意网站的合法网站。另外，此图表删除了我们的主动搜索结果，从而为我们提供了一个在常规浏览时 (在学校、工作或家里) 遭遇到的各种独特、新威胁的真实情况。

相比之下，下面的图表说明了我们的主动型方法的最新发现，即各种网站提供了哪些独特的新恶意软件下载。从新漏洞攻击或是当发现提供恶意下载内容或 PUP 的“金矿”网站时，我们发现了一些值得关注的现象。



恶意软件和 PUP 下载，
预定观测日

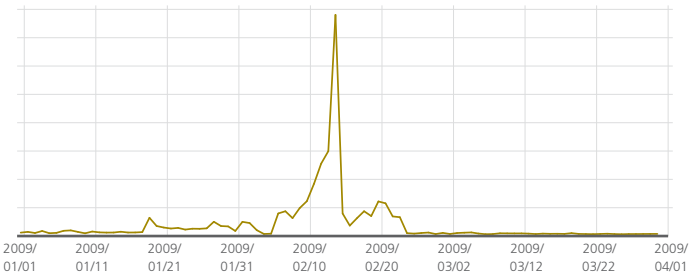
我们的主动型观测方法使用常规爬网和网站验证以及独特的挖掘方法来查找详细的恶意信息，结果发现在一月末和二月初，与赌场有关的新恶意软件下载数量激增，在上季度末常规 PUP 的数量也大大增加。在该季度，此类活动位列恶意软件下载类型的前四位。(请参见下面的图表。) 另一种值得关注的恶意软件是持续存在的 Vundo Trojan 木马程序，该活动在过去三个月里变得更加猖獗。



恶意软件和 PUP 下载流行程度比较（按类型）

我们面对的一种无形 Web 威胁是**漏洞攻击**，对于分析人员和用户来说，这一术语具有很多含意 (通常是不相同的)。当我们爬网并监视 Web 时，Avert Labs 跟踪暗藏浏览器漏洞的新网页，我们经常会发现新的浏览器安全漏洞。如果浏览器 (及其插件) 不是最新的，这些“沙盘”可能很容易变成恶意软件作者的推演战场。在恶意软件攻克了山头后，用户的计算机可能会收到一些编程代码，这些代码会使用户感染广告软件、键击记录程序和其他恶意活动。

如果浏览器（及其插件）不是最新的，这些“沙盘”可能很容易变成恶意软件作者的推演战场。

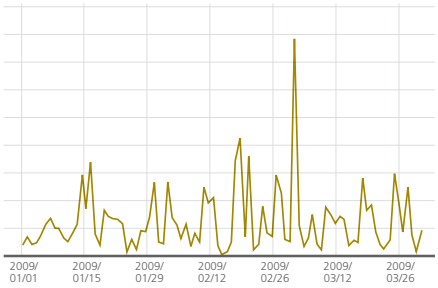


已发现的承载浏览器漏洞攻击的网站

匿名工具活动

恶意软件编写者正在肆无忌惮地使用重定向的 URL 发动攻击（无论是通过匿名工具还是使用内容服务器的 Web 2.0 接口）。这可能是为了避免标准检测（通过充当嵌入式 URL 而不是源 URL），或者是利用这些看起来提供了恶意软件的网站固有的声誉。

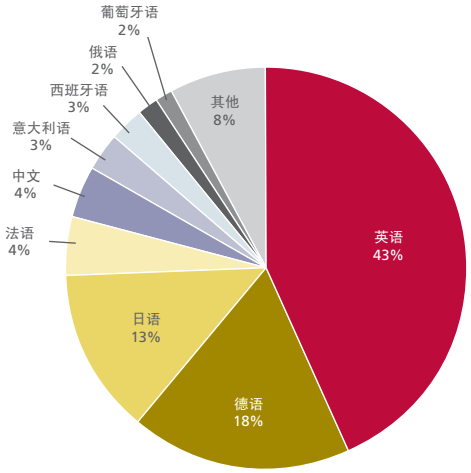
匿名工具是一种在联机时隐藏用户身份的工具。大多数匿名工具并不是恶意的，因此，我们前面讨论的安全危险中没有包括这些工具。不过，使用此类工具可能会向“中间人”攻击敞开大门，恶意匿名工具或被劫持的匿名工具会在用户和服务器之间传送的邮件（无论是哪种方向）中注入代码。这不仅会使用户处于危险的境地，而且还会危及本来受到很好保护的主机和网络。从总体上讲，本季度的匿名工具活动较上一季度有所增加。本季度与去年同期相比也略有增加。



每日新增匿名工具

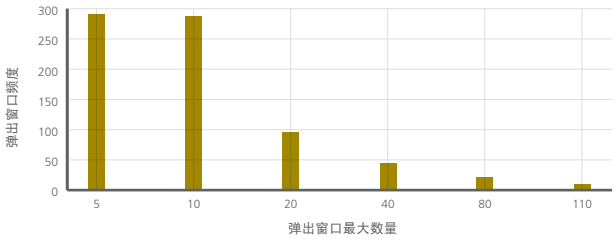
一般 Web 趋势

Web 是一个全球性社区。只需看一下专业或社交网站上的链接，便可见一斑。网页数量在持续稳定地增加以支持更多的语言。在美国的顶级网站中出现的相同博客攻击也会通过中国博客、巴西博客和很多其他国家/地区的博客进行传播。而如今的攻击使用的是一个范围广泛的网络。此外，恶意软件散布者利用了品牌知名度的优势（如重要体育赛事和使用嵌入到联赛对阵表和球员图片中的恶意软件），只要他们利用全球性品牌就可以攻击使用各种语言的用户。



网站内容所使用的语言分布

令人讨厌的弹出窗口仍然会不时出现。有趣的是，尽管有弹出窗口拦截程序和其他支持此功能的工具，但大多数网站仍然乐此不疲地使用它们。某个网站上的弹出窗口数量竟然高达 116 个。



网站弹出窗口数分布（仅统计 5 个以上）

对于 Web 上的企业，您需要采用与对付上门推销的销售员相同的安全防范措施。

我们仍然可以看到与 Web 2.0 及企业有关的合法 URL 在传播恶意软件，并且呈迅速蔓延的势头。在十年前或是更早以前，那时您只要别碰某些内容，就安全无忧。但是现如今，无论我们浏览到哪里，威胁都如影随形。所有可利用的网站都会被利用（通过暗藏在其中的各种各样的安全漏洞），而管理员需要天天扫描查找服务器上的安全漏洞。值得注意的是，这些来自网站和服务器的扫描呈流行趋势，它们与非法软件、恶意网站或匿名工具有关。如果一个高访问量的网站是易受攻击的，那么我们勿需置疑该网站会不会被漏洞攻击，这只是时间问题。

我们发现 Web 上的诈骗呈明显上升趋势。网络骗子们通过垃圾电子邮件和 Web 给世界各地的人们不断造成侵扰并从中获益，我们预计这种诈骗还会不断蔓延。通常很难甄别某个组织是否合法。对于 Web 上的企业，您需要采用与对付上门推销的销售员相同的安全防范措施。用户必须清楚，一旦他们给骗子提供了信用卡信息以进行网上捐款或购买虚假的服务，该数据就会落到骗子手里了。

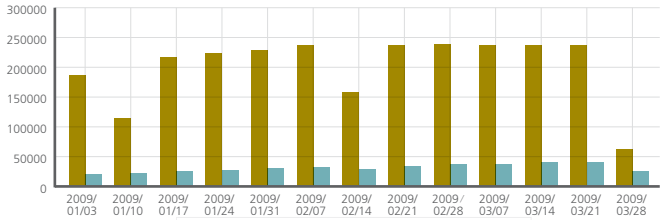
不过，我们的分析还表明经济出现了复苏的迹象。本季度的房地产网站访问量明显增加，在为用户提供的十大内容类别中占有一席之地（而将体育内容挤出前十位）。

恶意软件：Conficker 言过其实，AutoRun 不可小觑

前几个月，到处充斥着与 Conficker 有关的消息。您可能会认为这是唯一值得担心的威胁。然而，当我们看到具体的分析数字后，却发现情况并非如此。Conficker 不是最大的威胁。

确实，从各个方面分析 Conficker 都是一种非常可怕的恶意软件。它感染了许多主机。并且一直为别有用心的人积极开发和维护着，也经常为人提起。但尽管受到广泛关注，其实际的感染情况却并没有人们所想像的那样严重。

而与此同时，在本季度我们还发现了一种令人担忧的恶意软件。这是一种基于 AutoRun 的恶意软件，它主要使用 USB 驱动器或闪存驱动器自我复制。在本季度由此类恶意软件所造成的感染数量要远远多于 Conficker。下面让我们逐一比较这两种恶意软件：



检测到 AutoRun 和 Conficker 的计算机

AutoRun

Conficker

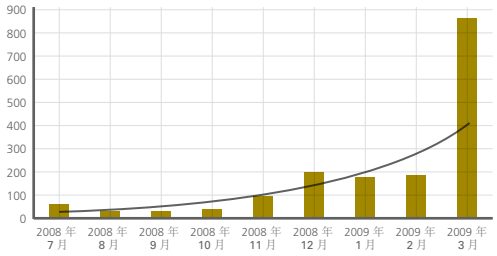
在过去的 30 天里，报告的所有感染中有不到 10% 是源于 AutoRun 蠕虫。Conficker 最初约占 1%，后来增加到 12%，但这仍低于 AutoRun 蠕虫近期检测到的峰值 15%。

预测更新

在今年年初，McAfee Avert Labs 发布了《2009 年威胁预测》[2]。其中许多有根据的推测在本季度都得到了印证。

警惕您的好友

在过去的十年里，从朋友那里收到病毒这种常见的威胁媒介已经受到了有效的控制。但 Web 2.0 又使这种老套的攻击方式重新焕发了生机。在本季度，Koobface 变种突然感染了数以千计的用户，而这些受害者正是由于接收了 Facebook 上的好友所发送的病毒。受害者并不知道与发送病毒的邮件关联的链接将定向到散布这种蠕虫的网站。此后不久，他们的计算机就会感染这种病毒，并向其朋友圈发送感染病毒的邮件。社交网站依然是攻击者发动社会工程攻击所常用的媒介。

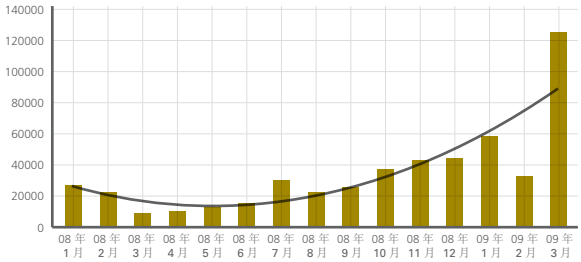


已发现的独特的 Koobface 软件

2. McAfee Avert Labs 威胁中心。http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report.pdf

欺诈性网络

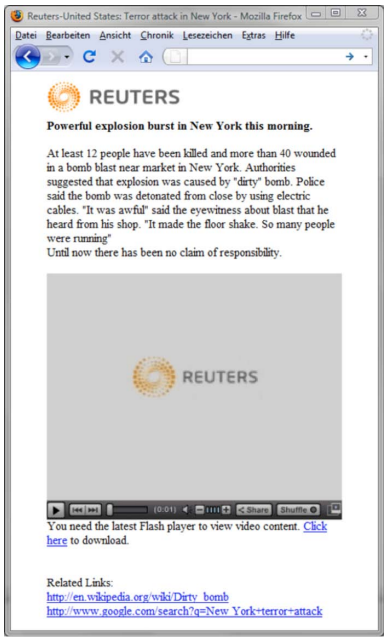
在二月份，Facebook 遭到漏洞攻击，攻击者利用 Facebook 平台创建了欺诈性的应用程序。很多用户中了圈套，安装了这些应用程序。该事件引起媒体的关注，也促使 McAfee Avert Labs 着手调查针对 Google 高频搜索词而产生的大批量搜索引擎优化链。攻击者不仅从各热门网站窃取受版权保护的资料，而且还滥用其他热门网站（如 Democrats.org）帮助其提升 Google 排名。在优化搜索结果背后，攻击者的最终目的是安装恶意防病毒软件。恶意 Facebook 应用程序就属于这种情况，它可导致列出恶意搜索结果并安装恶意安全软件。这些事件充分说明用户亟需确保安全地上网冲浪。



已发现的独特的恶意防病毒程序

利用母语发动的威胁

攻击者知道攻击越贴近用户的生活，用户越可能乖乖就范：单击链接、输入用户名和密码以及安装应用程序。与地球另一侧发生的事情相比，发生在身边的事情更容易引起我们的注意。在二月和三月，隐藏在 Waledac 病毒后的网络骗子正是利用了这一观点。毫无戒备的受害人被引诱访问根据其位置定制的网站，这种方式使伪装显得更加逼真。当用户浏览“本地新闻”时，网络就会尝试通过“随看随下”漏洞代码悄悄安装病毒。



McAfee Avert Labs 博客

Google 和搜索引擎的滥用

Google。这个名字本身，对于不同的人有着不同的含义。对于求职者，它是查找最新职位列表的途径。对于雇主，它是在线搜索合格人才的方式。对于购物者，它是找到所需物品最低售价的有效工具。而对于恶意软件编写者和网络犯罪分子来说，它逐渐成为不可或缺的工具，用来散布恶意软件和从事网络犯罪活动。考虑到如今搜索引擎与众多互联网活动密切相关，恶意软件编写者设法通过搜索引擎散布其恶意软件也就不足为奇了。有关本主题相关的博客示例，请查看以下 McAfee Avert 博客内容：

- http://www.avertlabs.com/research/blog/index.php/2009/03/15/democratsorg-cans-the-spam/
- http://www.avertlabs.com/research/blog/index.php/2009/03/10/democratsorg-blog-spam-contributes-to-google-search-poisoning/
- http://www.avertlabs.com/research/blog/index.php/2009/02/27/google-bucking-the-trend/
- http://www.avertlabs.com/research/blog/index.php/2009/02/25/google-trends-abused-to-serve-malware/
- http://www.avertlabs.com/research/blog/index.php/2009/01/07/google-code-project-abused-by-spammers/
- http://www.avertlabs.com/research/blog/index.php/2009/01/17/do-not-worry-obama-di-not-refuse-to-be-a-president/

鉴于索引与常用关键字组合产生的强大功能以及网络犯罪分子牟取暴利的野心，我们预计这种滥用情况还会持续下去。

经济和恐慌

全球经济问题依然让很多人寝食难安。而另一些人则受到安全问题和恐惧的困扰。恶意软件编写者和网络犯罪分子可以轻而易举地将这种恐惧转化为不当得利。在《2009 年威胁预测》中我们已经提到了经济趋势这个诱因，而在整个第一季度攻击者已经以各种方式利用了这种趋势。当网络犯罪分子撒下社会工程诱饵时，恐惧将成为一种强大的诱导因素。

- http://www.avertlabs.com/research/blog/index.php/2009/03/16/breaking-news-waledac-terror-attack-in-a-city-near-you/
- http://www.avertlabs.com/research/blog/index.php/2009/02/23/malware-riding-on-the-tides-of-the-economic-crisis/
- http://www.avertlabs.com/research/blog/index.php/2009/02/06/cybercrime-online-threats-and-the-recession/
- http://www.avertlabs.com/research/blog/index.php/2009/01/05/one-hacker-may-conceal-another/
- http://www.avertlabs.com/research/blog/index.php/2009/01/20/fake-antivirus-and-a-real-threat/
- http://www.avertlabs.com/research/blog/index.php/2009/01/29/hoax-or-not-treat-it-the-same/

欺诈、垃圾邮件和网络钓鱼在经济形势良好的时候就大行其道，在经济危机中更将甚嚣尘上。请谨记，那些网络犯罪分子每天与我们读着相同的新闻，而我们需要时刻保持警惕，才能防止他们利用新闻头条和各类事件对我们进行欺诈。

关于 McAfee Avert Labs

McAfee Avert Labs 是 McAfee Inc. 的全球研究团队。Avert Labs 对安全有非常全面且深厚的研究，其下的多个研究团队致力于恶意软件、潜在有害程序、主机入侵、网络入侵、移动恶意软件以及各种本地化漏洞的披露。这种广泛的研究还使得迈克菲的研究人员能继续改进安全技术和更好地保护公众。

关于 McAfee, Inc.

McAfee, Inc. 总部位于美国加利福尼亚州的圣克拉拉，是全球最大的专注于安全技术的公司。迈克菲始终致力于应对全球最严峻的安全挑战。迈克菲提供经实践验证的主动型解决方案和服务，保护全球的系统和网络，使用户能够安全地联网并在 Web 上浏览及购物。迈克菲凭借屡获大奖的研究团队，为家庭用户、企业、公共部门以及服务提供商提供创新产品和强大保护，使他们能够遵守法规、保护数据、防止破坏、发现漏洞以及提高安全。http://www.mcafee.com/cn。

迈克菲（上海）软件有限公司

北京市朝阳门外大街 18 号丰联广场 B 座 1215B	邮编：10020	Tel: (8610) 65383399	Fax: (8610) 65885601
上海市徐汇区虹桥路 3 号港汇 2 座 4005-4006 室	邮编：20030	Tel: (8621) 61458878	Fax: (8621) 61132278
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	Tel: (8620) 38860668	Fax: (8620) 38860638

销售热线：800-819-8879 *www.mcafee.com/cn*

5395rpt_avert_quarterly-threat_0409