IBM 安全解决方案
2011 年 5 月

IBM X-Force威胁洞察季度报告

IBM

目录

关于此报告

IBM X-Force® 季度报告重点列出安全专业人员如今面临的一些最主要的威胁和挑战。 此报告由 IBM 托管安全服务和 IBM X-Force 研发团队编写。 每个议题都关注特定挑战，并回顾近期最大的在线威胁。

IBM 托管安全服务专用于通过外包安全操作或辅助您现有的安全团队帮助组织提高其信息安全性。 IBM 按需保护平台帮助提供托管安全服务和组织保护其信息资产免遭互联网攻击所需的专业技术、知识和基础设施。

X-Force 团队为互联网安全的预先方法奠定了基础。 X-Force 团队是全球最富盛名的商业安全研究团体之一。 此安全专家团队研究并评估漏洞和安全问题、为 IBM 安全产品开发评估和应对技术，并向公众提供有关新兴互联网威胁的培训。

欢迎您提供反馈。 有关此报告的问题或评论，应提交到 XFTAS@us.ibm.com。

演变： 从不良程序到武器

Creeper、Wabbit、Animal、Elk Cloner、Brain、Vienna、Lehigh、Stoned 和 Jerusalem， 我们如今通常简单称之为恶意软件，这些是其早期例子的名称，出现于 1971 至 1987 年间。

这只是开始。 这些例子可感染多种平台并提供多种有效负载，某些仅仅是示例消息对屏幕的响应。 虽然《震荡波骑士》中的 John Brunner 等科幻作家概念性地描写了病毒和蠕虫，但直到 1984 年 Fred Cohen[1] 才对此类程序进行了真正的数学定义。 “计算机病毒”史离我们并不算遥远。

Creeper[2] 可以说是第一个病毒，或者更精确地说是蠕虫，并且仅感染 DEC PDP-10 计算机。 在将其作为实证进行编写时，1971 年它通过简单的负载扩散至阿帕网，并伴随着一条文本消息“我是爬虫，有本事你就过来抓我吧”！ 通过网络自行复制和扩展的特性是恶意软件的重要概念，今天仍然存在。 针对 Creeper，出现了 Reaper，Reaper 本身也是病毒，也会扩散到同一网络，但它旨在删除 Creeper 实例。 可以认为 Reaper 是第一款反病毒软件的例子。 它的任务是检测并清除恶意软件。 但是，在未经许可在系统上执行或在网络上扩散的代码根本不受欢迎。 最近，用于创建僵尸网络的现代型恶意软件使用同一项技术尝试清除其他僵尸网络恶意软件的实例，以便控制受影响的系统。

此处有一个更值得注意的例子是 Brain[3]，这是一个源于巴基斯坦并在 1986 年发布的引导扇区感染程序，是感染运行 MS-DOS 的个人计算机的首个恶意软件实例之一。 它感染 FAT 格式且可移动的介质的引导扇区（读取软盘），实际上它是作为一种控制软件剽窃的手段而编写。 它本身并不是恶意的，但是又无法阻止它感染除了预定目标之外的受害者。 作者还将其联系信息置于代码中，这导致他们不得不掐断电话线，因为接到了大量 Brain 的愤怒受害者的来电。

在 1987 年 12 月圣诞节，Tree Exec[4] 出现在 IBM 大型机中，导致 EARN、BITNET 和 IBM 的 VNET 受到严重破坏。 一个用户收到邀请其执行 “CHRISTMAS”的电子邮件，并在其终端画了棵圣诞树。它确实这样做了，并且还通过 NAMES 和 NETLOG 文件将其发送给位于其中的其他用户。 虽然此复制技术在现在看来非常常见，但当时并不常见。 恶意软件的作者称其代码的目的仅仅是为了向朋友发送祝福，但没想到会造成禁止访问其系统这种结果。

到 1988 年，我们迎来了史上最出名的恶意软件项之一，而我们也开始注意到事情越来越复杂。在这个时期的 Robert Morris 蠕虫[5] 是绝无仅有的，因为它利用了发送邮件、指纹和脆弱密码中的漏洞。 它还可感染多个架构。 其传输工具是刚刚成熟的互联网。 该恶意软件发布后，开始堵塞系统，不久就造成拒绝服务条件，这直接或间接地影响了连接到互联网的大部分系统。

1 Fred Cohen 及合作人
http://all.net/resume/bio.html

2 计算机病毒 25 周年纪念？
http://news.cnet.com/8301-13506_3-9745010-17.html

3 搜索源于巴基斯坦的第一个计算机病毒
http://campaigns.f-secure.com/brain/index.html

4 安全摘要存档
http://securitydigest.org/rutgers/mirror/pyrite.rutgers.edu/christmas.exec

5 Morris 蠕虫
http://en.wikipedia.org/wiki/Morris_worm

Robert Morris 蠕虫的影响很大，促使卡耐基梅隆大学创建 CERT 协调中心。 据蠕虫的创建者 Robert Morris 称，蠕虫的编写不带有恶意目的，不过是将其作为工具计量互联网的规模。 它所造成的破坏在预料之外。 但是，Morris 的行为已认定为违反了 1986 年修订的美国计算机反欺诈和滥用法案[7]（自 1986 年修订）并判处 3 年缓刑、400 小时的社区工作和 10,000 美元的罚款。

在 1989 年年初，我们可以在自然环境下看到多态加密，这是病毒发展史上非常著名的时期。 它由 Fred Cohen 预测，由 Mark Washburn[8] 和 1260 病毒实现，但最为人所知的则是出现在具有传奇色彩的 legendary Dark Avenger[9] 编写的 Mutation Engine 中。 简言之，多态就是代码定期修改自身以避免检测的能力。 Dark Avenger 从未得到完全确定，只有（在线）采访 Dark Avenger 的 Sara Gordon[10] 撰写并在 1993 年出版的书中对作者的想法留下了匆匆一笔。 Dark Avenger 创建的病毒感染力和杀伤力都很强。

自 1991 年以来，称为 Michelangelo[11] 的病毒值得一提。但是，要提到的不光是病毒，还有通过病毒进行的大肆宣传。 关于 Michelangelo 有着疯狂极端的预测，即 Michelangelo 会造成毁灭性破坏。 该病毒会如何广泛地扩散难以确定。 看似它会全球性地扩散，一些报告中引用的 1992 年 3 月 6 日感染的计算机最大预计数量达 500 万，但这与目标不符。 众多专家和学者就计算机的感染数量、病毒如何扩散以及用户可以通过什么方式避免病毒在触发日期临时造成破坏提出了多点看法。 病毒本身是 DOS 启动磁区感染程序，并且在触发日期之前一直处于休眠状态。

在 1999 年我们才真正开始注意我们今天如何了解病毒的演变，其中，Happy99[13] 和 Melissa[14] 作为休眠状态示例。Happy99 可视为我们如今所广泛了解的通过电子邮件传播的第一个病毒。 在另一方面，Melissa 是 Word 文档中实现的蠕虫。 一旦启动，蠕虫的任务之一就是通过将其自身发送给受害者地址簿中的前 50 名用户来进行复制。 这不仅会快速扩散病毒，而且产生的电子邮件流量会堵塞电子邮件服务器。 当时，Melissa 是史上扩散最快的病毒。

6 Meet CERT
http://www.cert.org/meet_cert/

7 美国法典： 标题 18，1030。与计算机相关的欺诈和关联活动
http://www.law.cornell.edu/uscode/18/1030.html

8 1260（计算机病毒）
http://en.wikipedia.org/wiki/1260_(computer_virus)

9 Dark Avenger
http://en.wikipedia.org/wiki/Dark_Avenger

10 Dark Avenger 的深度思索
http://www.research.ibm.com/antivirus/SciPapers/Gordon/Avenger.html

11 Michelangelo（计算机病毒）
http://en.wikipedia.org/wiki/Michelangelo_%28virus%29

12 Michelangelo Fiasco： a 历史大事年表
http://vmyths.com/column/1/1992/6/1/

13 电子邮件蠕虫.Win32.Happy
http://www.securelist.com/en/descriptions/old22314

14 病毒：W32/Melissa
http://www.f-secure.com/v-descs/melissa.shtml

在 1988 年，当 Morris 蠕虫肆虐时，互联网中将近 100,000 个系统连接到其中。 到 1998 年 12 月，在 Melissa 之前的 4 个月，互联网已有 148 百万个用户。 其本身就很明显 Melissa 的影响比 Morris 蠕虫的影响广泛。 Melissa 的创作者被逮捕并判处[15]在美国联邦监狱中监禁 20 个月，徒刑期满后开始三年的监督释放并判处 5,000 美元的罚金。

另外值得谨记的是，此时大多数互联网用户都在运行 Microsoft® Windows® 操作系统，此操作系统之后成为病毒创作者的众矢之的。 到 2000 年 3 月，互联网用户的数量已上升到 3.04 亿，而在 2000 年 5 月，全世界都会说“IloveYou”[16]。

自 2000 年 5 月 4 日前后，主题行中为“IloveYou”的电子邮件开始发到电子邮件收件箱。 包含名为“LOVE-LETTER-FOR- YOU.TXT.vbs”（或类似内容）和 .vbs 扩展名的附件的电子邮件隐藏在 Windows 系统中，除非默认文件查看选项已由用户更改。 这使得受害者认为许多打开的附件是无害的文本文件。 一旦受害者打开 .vbs 文件，则代码会导致电子邮件从受害者发送给受害者 Windows 地址簿中的每个地址。 它还会更改受害者的系统。

包含蠕虫的原始电子邮件从蠕虫编写所在的国家菲律宾发送。 到 5 月 5 日，据报告[17]估计有 4500 万计算机感染“IloveYou”或 10 个左右的变种，这些变种在前 24 小时内也出现了。 另据报告称[18]，此蠕虫导致 Pentagon、CIA 和英国议会关闭其电子邮件系统。 预计由 IloveYou 及变种导致的财务损失高达 55 亿美元。 隐藏扩展名、社会工程和采用脚本引擎的概念在今天仍不过时。

之后，我们看到涌现出的感染性极强的恶意软件，如 Code Red、Nimda 和 Slammer 都极为常见。 现在我们一般看不到具有像 IloveYou、Code Red 或 Slammer 这样直接和可见影响的恶意软件。 我们现在看到的是每天检测到的大量新的或现有恶意软件的变种，可能每天达到 50,000 个。

有些重要事情要谨记在心。 首先，在 2003-2004 年之前绝大多数恶意软件都是由个人编写。 某些恶意软件并非存有恶意。 在大多数情况下，就编写者而言并没有直接的财务动机。 实际上，恶意软件编写者为众人所不齿的原因不仅仅在于他们创建的代码会导致损害，而且还因为这些代码被广泛视为不良程序。 但是，至少对于 Dark Avenger 和 Mutation Engine 等某些情况而言这样说可能不是很公平。 另外，我们今天通常使用的普遍存在的互联网在 2011 年年初用户就达到了 20 亿。与早期相比，这是巨大的竞技场。 恶意软件得到了真正的巩固，并将继续存活至可预见的未来。 中途局势发生了变化，正在演变扩张的网络犯罪开始利用恶意软件。

15 Melissa 计算机病毒的创作者被判处在联邦监狱监禁 20 个月 http://www.justice.gov/criminal/cybercrime/melissaSent.htm

16 VBS.ILoveYou.A - CA 技术 http://gsa.ca.com/virusinfo/virus.aspx?ID=9024

17 专家预计病毒造成数十亿的损失 http://news.cnet.com/2100-1001-240112.html

18 十年的技术恐慌 http://www.cio.in/article/tech-scares-decade

19 互联网用户数量达 20 亿 http://news.ninemsn.com.au/technology/8202354/number-of-internet-users-reaches-2-bln

恶意软件已成为当今网络犯罪的主体。 它主要用作盗窃信息和创建僵尸网络的介质。 以某种方式传递的恶意软件感染个人计算机，并将其变为僵尸网络客户端或僵尸。 Think Storm 僵尸网络。 该蠕虫被 F-Secure 称为 Storm，因为它的首个迭代在有关风暴 Kyrill 的消息中扩散。 此蠕虫还使用许多其他主题来鼓励受害者查看消息、网页和下载内容，或打开恶意软件。 Storm 僵尸网络是众多来去匆匆的恶意软件之一，但是在那时它炙手可热，因为它有着数百万僵尸客户端。 在某种形式上的社会工程在当今仍不过时，它通常用作引诱受害者打开恶意文件或网页的手段。

已存在勒索软件，它不算全新，但却不时出现。 通常的勒索软件情况会对受害者的文件加密。 要对文件解密，受害者需要支付给攻击者一笔钱。

另一个经典恶意软件是 Zeus。 Zeus 用于从受害者处盗取财务信息并获得用户凭证。 Zeus 还将受感染的个人计算机融合到具有数百万计僵尸客户端的僵尸网络。 Zeus 是可以在地下论坛中购买的商务软件包。 它不光有开发周期，甚至还有基于硬件的授权系统，以预防软件的剽窃和未经授权的使用。

如今，恶意软件常用于定向攻击，当恶意软件利用自然环境中发现的前所未知的漏洞时，它们往往是这些漏洞的来源。 或许最臭名昭著的定向攻击之一是针对大量大型企业的，也就是广为人知的“极光行动”[20]。 该行动始于 2009 年年中，止于 2009 年年末，由 Google 于 2010 年 1 月 12 日公开披露。

Google 的披露概述了受攻击的对象为知识产权，但不止于此，其主要目标是访问某些持不同政见者的 Gmail 帐户。 另一个以类似方式发动攻击的众人皆知的恶意软件示例为“幽灵网”[21]。 这种情况下的恶意软件出现在外交部、大使馆和达赖喇嘛的办事处。 从回显的简陋文本消息一直到终端，恶意软件确实有了极大的提升。那么留下了什么呢？ 嗯，一场网络大战吧。

网络大战历史中的某些片段是脱离恶意软件这一环境的。 针对民族国家发动的大规模分布式拒绝服务 (DDoS) 攻击中使用的“僵尸网络”便是一例。 武器是僵尸网络，而隐藏在每个邪恶僵尸网络背后的是一些恶意软件。 爱沙尼亚[22]、立陶宛[23]和格鲁吉亚[24]广泛报道的攻击都表明了持续 DDoS 攻击所能造成的严重影响。 没有僵尸网络启动攻击，这些攻击将难以进行。

恶意软件从起初并不引人注目，现已演变成网络犯罪、间谍活动和战争中的主要武器。 恶意软件不再是单一病毒编写人员的据点，专业人员也可以为构想中的特定目标开发恶意软件。 但这给我们带来了当前的核心恶意软件 – 超级工厂病毒[25]。

20 中国的新方法 http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

21 未被覆盖的主要电子间谍网络 http://news.bbc.co.uk/2/hi/7970471.stm

22 黑客攻克了欧洲网络最发达的国家 http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

23 立陶宛经受住了网络攻击，预备迎接又一轮攻击 http://voices.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html

24 针对格鲁吉亚的网络攻击： 明确的法律教训 www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

25 W32.Stuxnet Dossier http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

超级工厂病毒不仅移动了恶意软件的门柱，还改变了比赛场地和游戏规则。 事实上，超级工厂病毒涵盖了恶意软件的各个方面。 包括蠕虫、特洛伊木马和 rootkit。 它入侵不超过 4 个之前未知的漏洞，感染多个平台，包括攻击 PLC（可编程逻辑控制器）设备。 它攻击 SCADA（监测监控及数据采集）系统，旨在蓄意破坏操作的同时不被检测到。

虽然对于超级工厂病毒的幕后主使存在很多推测，且没有确切答案，但是我们可以从恶意软件本身和其工作原理观察到某些情形。 它是一个团队经过很长一段时间开发出来的，而不是凭个人力量所能及。 开发团队对于目标系统拥有大量认知，这一点可从超级工厂病毒代码定义的目标得到佐证。 在其目标锁定的企业传播时，似乎不会超出其目标范围。 偶尔会在目标之外发现为数不多的感染。 其目标似乎是蓄意破坏制造系统或处理系统的某些功能，同时隐藏并提供系统正在正常运行的反馈。 总之，超级工厂病毒背后有非常殷实的资源和资金。 似乎向此类项目投入资源以进行犯罪操作不存在任何合适的利益动机。

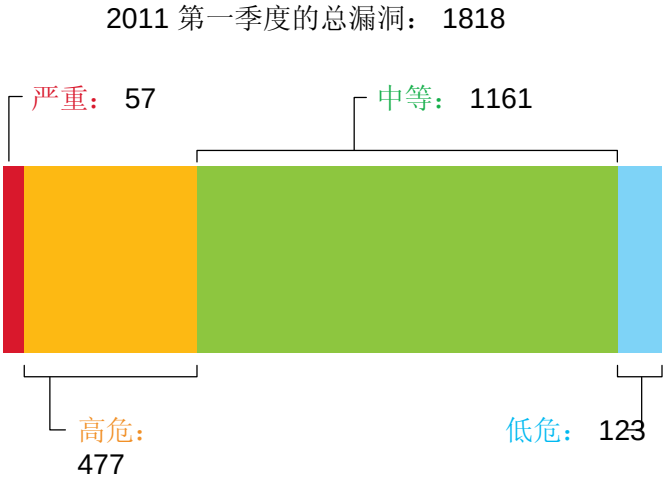
1971 年至 2011 年，恶意软件被有效地武器化，这一过程科幻小说作家曾描述过，早期病毒编写人员只是幻想过。 然而，许多基本特性保留了下来。 那么它给今天的我们留下了什么？

反病毒策略在当今比任何时候都更为重要。 无论是国家的还是企业的，声誉良好的最新反病毒解决方案都应该采用。 IDS/IPS 系统可以协助预防攻击和检测恶意网络流量，如 zombie 僵尸网络客户端与其命令和控制主机之间的通信。 始终建议敏感入口和出口筛选。 与声誉良好的托管安全服务提供商交谈也是非常有好处的，因为他们不仅能提供对关键保护系统的管理，还是训练有素的分析师，能在处理以往未知的威胁时提供格外有益的援助。 因此，无论是您的 PDP-10 隐藏在某处但仍在运行并以某种方式与互联网连接，还是您负责整个现代企业，您都面临着同样的基本威胁。 武装自己。

2011 年第一季度的多产问题和影响问题

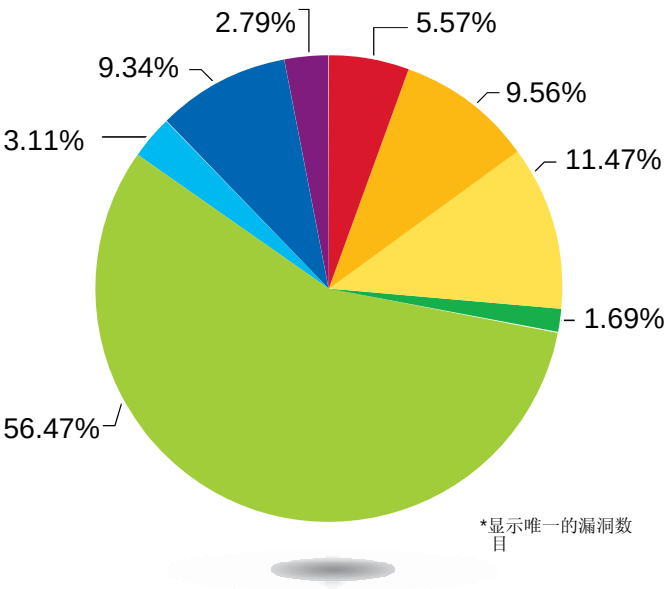
重要披露

2011 年第一季度，X-Force 团队研究并评估了 1818 个与安全相关的威胁。 X-Force 数据库内相当大百分比的漏洞成为了恶意代码编写人员的焦点，其产品包括恶意软件和定向漏洞入侵。



来源： IBM X-Force

下图对 X-Force 团队分析师研究的漏洞进行了归类，依据的是他们
认为入侵漏洞可能导致的安全后果的最大类别。 类别包括：绕过安全检查、数据操控、拒绝服务、文件操控、获取访问、获取特权、获得信息以及其他。 *



来源： IBM X-Force

绕过安全检查	绕过安全检查限制，如防火墙或代理及 IDS 系统或病毒扫描程序。
数据操控	操控由与服务或应用程序关联的主机使用或存储的数据。
拒绝服务	服务或系统崩溃或中断，以致网络崩溃。
文件操控	创建、删除、读取、修改或覆盖文件。
获取访问	获得本地和远程访问。 这也包括黑客用以 执行代码或命令的漏洞，因为这通常允许黑客获得对系统的访问。
获取特权	特权只能在本地系统上获得。
获得信息	获得信息，如文件和路径名称、源代码、密码或服务器配置详细信息。
其他	其他类型未涵盖的任何事务。

一月份第一周，公开披露了一个漏洞，并且发布了影响某些版本的 Windows 图形渲染引擎的利用代码。 期望入侵此漏洞的攻击需要用户打开带有内嵌缩略图的恶意文档文件或带恶意图像的其他 Microsoft Office 文档，这些文档中可能含有获取特权的代码。

- IBM 提供的保护警告： Microsoft Windows 图形渲染引擎缓冲区溢出[26]
  - IBM 保护签名： CompoundFile_Windows_Thumbnail_Overflow、CompoundFile_Shellcode_Detected
- CVE-2010-3970
- Microsoft 安全公告 MS11-006： Windows 外壳程序图形处理中的漏洞可能允许执行远程代码 (2483185)[27]

一月还有两个 0day 漏洞，IBM X-Force 为其发布了保护警告。 首先，影响 Microsoft Windows 传真封面编辑器。 如果受害者被引诱至打开恶意传真封面文档，则远程攻击者可执行任意代码。 第二个问题是 Microsoft IIS7 中的缓冲区溢出漏洞，这也会导致执行远程代码。

- IBM 提供的保护警告： Microsoft Windows 传真封面编辑器可能允许拒绝服务[28]
  - IBM 保护签名： FAX_Coversheet_Shellcode_Detected
- CVE-2010-4701

- IBM 提供的保护警告： Microsoft IIS FTP 转义序列 (IAC) 溢出[29]
  - IBM 保护签名： FTP_IIS_IAC_Overflow
- CVE-2010-3972
- Microsoft 安全公告 MS11-004： 互联网信息服务 (IIS) FTP 服务中的漏洞可能允许执行远程代码 (2489256)[30]

26 IBM 提供的保护警告： Microsoft Windows 图形渲染引擎缓冲区溢出
http://www.iss.net/threats/406.html

27 Microsoft 安全公告 MS11-006： Windows 外壳程序图形处理中的漏洞可能允许执行远程代码 (2483185)
http://www.microsoft.com/technet/security/Bulletin/MS11-006.mspx

28 IBM 提供的保护警告： Microsoft Windows 传真封面编辑器可能允许拒绝服务
http://www.iss.net/threats/408.html

29 IBM 提供的保护警告： Microsoft IIS FTP 转义序列 (IAC) 溢出
http://www.iss.net/threats/407.html

30 Microsoft 安全公告 MS11-004： 互联网信息服务 (IIS) FTP 服务中的漏洞可能允许执行远程代码 (2489256)
http://www.microsoft.com/technet/security/bulletin/ms11-004.mspx

一月还针对影响 Windows 备份管理器的问题公布了 IBM 保护警告，该问题已在 Microsoft 一月份的安全发布中得到处理。 攻击者说服用户打开远程 SMB 或 WebDAV 共享上的此类文件，然后提供能够利用当前用户的特权执行的任意代码。

- IBM 提供的保护警告： Microsoft Windows 备份管理器可能允许执行远程代码[31]
  - IBM 保护签名： HTTP_Windows_Backup_Mgr_DLL_Hijacking, SMB_Windows_Backup_Mgr_DLL_Hijacking
- CVE-2010-3145
- Microsoft 安全公告 MS11-001： Windows 备份管理器中的漏洞可能允许执行远程代码 (2478935)[32]

二月份公布了第一季度数目最多的保护警告和公告 – 总共 7 个。 其中一个保护警告是针对 Microsoft 二月份安全发布中处理的漏洞生成的。 Microsoft Internet Explorer 未初始化的内存损坏漏洞可能导致执行远程代码。

二月份的同一天还发布了另外一个保护警告，该警告也重点突显了一个 Microsoft 问题，但是这一影响 Microsoft Windows 的漏洞直到三月份才得到 Microsoft 的处理。 这一问题涉及公开利用代码，并且三月份 Google 表示他们观察到攻击者利用这一问题对其用户实施高度定向的攻击[33]。

- IBM 提供的保护警告： Microsoft Internet Explorer 远程代码执行[34]
  - IBM 保护签名： Script_IE_Document_Corruption
- CVE-2011-0036
- Microsoft 安全公告 MS11-003： 针对 Internet Explorer 的累计安全更新 (2482017)[35]

- IBM 提供的保护警告： Microsoft Windows MHTML 可能允许信息披露[36]
  - IBM 保护签名： MHTML_CRLF_Injection, MHTML_Handler_Detected
- CVE-2011-0096
- Microsoft 安全公告 MS11-026： MHTML 中的漏洞可能允许信息披露 (2503658)[37]

31 IBM 提供的保护警告： Microsoft Windows 备份管理器可能允许执行远程代码
http://www.iss.net/threats/405.html

32 Microsoft 安全公告 MS11-001： Windows 备份管理器中的漏洞可能允许执行远程代码 (2478935)http://www.microsoft.com/technet/security/bulletin/MS11-001.mspx

33 遭到活跃入侵的 MHTML 漏洞
http://googleonlinesecurity.blogspot.com/2011/03/mhtml-vulnerability-under-active.html

34 IBM 提供的保护警告： Microsoft Internet Explorer 远程代码执行
http://www.iss.net/threats/409.html

35 Microsoft 安全公告 MS11-003： 针对 Internet Explorer 的累计安全更新 (2482017)
http://www.microsoft.com/technet/security/bulletin/MS11-003.mspx

36 IBM 提供的保护警告： Microsoft Windows MHTML 可能允许信息披露
http://www.iss.net/threats/410.html

37 Microsoft 安全公告 MS11-026： MHTML 中的漏洞可能允许信息披露 (2503658)
http://www.microsoft.com/technet/security/bulletin/MS11-026.mspx

IBM X-Force 还针对他们发现的影响 Adobe Shockwave 的漏洞公布了两个保护公告。 使用受影响版本的 Adobe Shockwave Player 的受损计算机，可能导致机密信息泄漏、工作效率损失和进一步的网络损坏。 可以通过引诱用户访问网页来实现远程代码执行，该网页将加载精心制作的入侵此漏洞的 Director 文件。

- IBM 提供的保护顾问： Adobe Shockwave（无效数组索引）远程代码执行[38]
  – IBM 保护签名： RIFF_Director_Movie_ Detected
- CVE-2010-4306
- Adobe 安全公告 APSB11-01： Shockwave Player 可用的安全更新[39]

- IBM 提供的保护顾问： Adobe Shockwave（常量表）远程代码执行[40]
  – IBM 保护签名： RIFF_Director_Movie_ Detected
- CVE-2010-4307
- Adobe 安全公告 APSB11-01： Shockwave Player 可用的安全更新[41]

该月晚些时候，IBM X-Force 公布了三个保护警告，以处理多种不同威胁。 第一个保护警告指示了 zwShell 的覆盖范围，zwShell 是与下面的“2011 年第一季度的其他季度重要事项”部分讨论的“夜龙”攻击有关的木马植入程序。 此木马植入程序旨在创建要安装在目标计算机上的可自定义后门远程管理工具。 然后，该后门程序可用于打开目标系统的远程桌面或外壳程序。

- IBM 提供的保护警告： zwShell 命令和控件[42]
  – IBM 保护签名： Trojan_zwShell_CnC
- McAfee Foundstone Professional Services 和 McAfee Labs： 全球能源网络攻击： “夜龙”[43]

二月份，影响 Microsoft Windows 的 0day 内存损坏漏洞同样面临着理念验证代码锁定此问题的情况。 稍后，Microsoft 将此问题作为其三月份的安全公布对其进行了处理。

- IBM 提供的保护警告： Microsoft Windows 服务器浏览器选择请求缓冲区溢出[44]
  – IBM 保护签名： SMB_Mailslot_Election_Overflow
- CVE-2011-0654
- Microsoft 安全公告 MS11-015： Windows Media 中的漏洞可能允许执行远程代码 (2510030)[45]

38 IBM 提供的保护顾问： Adobe Shockwave（无效数组索引）远程代码执行
http://www.iss.net/threats/412.html

39 Adobe 安全公告 APSB11-01： Shockwave Player 可用的安全更新
http://www.adobe.com/support/security/bulletins/apsb11-01.html

40 IBM 提供的保护顾问： Adobe Shockwave（常量表）远程代码执行
http://www.iss.net/threats/411.html41 Adobe 安全公告 APSB11-01： Shockwave Player 可用的安全更新 http://www.adobe.com/support/security/bulletins/apsb11-01.html

42 IBM 提供的保护警告： zwShell 命令和控件
http://www.iss.net/threats/413.html

43 McAfee Foundstone Professional Services 和 McAfee Labs： 全球能源网络攻击： “夜龙”
http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

44 IBM 提供的保护警告： Microsoft Windows 服务器浏览器选择请求缓冲区溢出
http://www.iss.net/threats/415.html

45 Microsoft 安全公告 MS11-015： Windows Media 中的漏洞可能允许执行远程代码 (2510030)
http://www.microsoft.com/technet/security/bulletin/MS11-015.mspx

第三个保护警报处理影响 Oracle 的 JRE 和 JDK 6 Update 23 及其早期版本、5 Update 27 及其早期版本以及 JRE 1.4.2_29 和早期版本的 Windows、Solaris 和 Linux 的拒绝服务漏洞。 未经验证的用户使用带有漏洞版本的 JRE 的 Apache Tomcat 会耗尽系统的资源。 漏洞入侵简单并且有很多关于怎样执行此类攻击的报道。

- IBM 提供的保护警报： Sun Java Double.parseDouble() 拒绝服务[46]
  - IBM 保护签名： HTTP_Tomcat_AcceptLanguage_DoS
- CVE-2010-4476
- Oracle Java SE 及 Java 业务关键补丁更新顾问 – 2011 年 2 月[47]

发布保护警报是为了重点突显微软三月份安全发布上处理的漏洞之一。

- IBM 提供的保护警报： Microsoft Windows Media 可能允许远程代码[48]
  - IBM 保护签名： ASF_DVR_MS_Code_Exec
- CVE-2011-0042
- Microsoft 安全公告 MS11-015： Windows Media 中的漏洞可能允许执行远程代码 (2510030)[49]

三月中旬，报道了一个影响 Adobe Flash 的漏洞，该漏洞在自然情况下通过嵌入 Microsoft Excel (.xls) 文件中的 Flash (.swf) 文件以电子邮件附件形式侵定向目标。 受影响的平台包括 Windows 最新版的 Adobe Flash 10、Macintosh、Linux 和 Solaris 操作系统、Android OS 及 Adobe Reader 9.x 和 10x 版本附带的 Authplay 组件。 入侵此漏洞可能导致利用当前用户的特权执行远程代码。

- IBM 提供的保护警报： Adobe Flash Player authplay.dll 代码执行[50]
  - IBM 保护签名： CompoundFile_Nested_SWF
- CVE-2011-0609
- 安全公告 APSA11-01： Adobe 安全顾问 Flash Player、Adobe Reader 和 Acrobat[51]

46 IBM 提供的保护警报： Sun Java Double.parseDouble() 拒绝服务
http://www.iss.net/threats/414.html

47 Oracle Java SE 及 Java 业务关键补丁更新公告 – 2011 年 2 月
http://www.oracle.com/technetwork/topics/security/javacpufeb2011-304611.html

48 Microsoft Windows Media 可能允许执行远程代码
http://www.iss.net/threats/416.html

49 Microsoft 安全公告 MS11-015： Windows Media 中的漏洞可能允许执行远程代码 (2510030)
http://www.microsoft.com/technet/security/bulletin/MS11-015.mspx

50 IBM 提供的保护警告： Adobe Flash Player authplay.dll 代码执行
http://www.iss.net/threats/417.html

51 安全公告 APSA11-01： 针对 Adobe Flash Player、Adobe Reader 和 Acrobat 的安全公告
http://www.adobe.com/support/security/advisories/apsa11-01.html

2011 年第一季度其他重要事项

报告的此部分简要涵盖 2011 年第一季度期间安全专业人员面临的一些其他威胁。

“夜龙”

2 月, McAfee 发布一份报告，其中详述了直接针对能源行业的全球公司进行的大规模攻击。 该行动被喻为“夜龙”，它使用 SQL 注入、鱼叉式网络钓鱼和其他定向入侵来获取对“有关石油和天然气领域投标和运营方面的专有行动和项目融资信息”的访问。

此攻击类似于过去几年里新闻中报道的高级持续性威胁 (APT)。 一般来说，这些攻击者所使用策略和技术的复杂程度仅足以完成任务，但他们却非常成功且能隐藏很长时间。

客户可通过利用安全应用程序中的最佳实践来保护自己，也可通过 SQL 注入保护机制、恶意文档保护、未授权通道检测以及持续警觉来保护自己。 我们还建议用户在保护信息资产方面保持警惕，这对持续的业务运营至关重要。

黑客团体 – Anonymous

自 2003 以来，黑客团体 Anonymous 一直以某种形式存在。然而，该团体在第一季度实施的行动，包括对 HBGary Federal 和美国银行文档的公布的攻击，让他们吸引到了更多的目光。

Anonymous 似乎已开始将其自身塑造为一个发布由揭密者提供的或通过其他方式获得的文档（如据报导被 Anonymous 访问过的各种 HBGary 服务器上获取的文档）的场所。 Anonymous 还在 Balboa 保险公司（美国银行在全国范围内并购的一部分）的员工间发送了一系列电子邮件。 Anonymous 的一个成员通过 Twitter 宣称这些邮件具有“欺诈”性质，原因是该银行隐匿了其他收费当中出自“联邦审计员”的止赎权错误。

由于各种 Anonymous 操作中的大量参与者和展现的广泛技能，任何特殊的操作在复杂性和有效性方面可能会有所不同。 攻击可能十分高明， 可以在延长期间实施，耐心地收集信息即便目标已受到危害，以使敏感信息和新机会能得到识别和利用。 或者，也可以由一个小组来组织另一项操作，然后将其发布在 IRC 聊天中，以使志愿者能使用聊天中可用的设置说明来参与。 后一种情形往往会因所提议操作的普适性和其他操作可能已在执行而极其易变。

通常，Anonymous 的大多数工具和方法都已经过多年的完善，这一点人所共知。 使用修改过的 Web 负载测试工具（如 Low Orbit Ion Cannon）是一项相对较新的创新，但仍属于经典的分布式拒绝服务攻击的范畴，其主要差异在于量和易使用性。

Anonymous 很少展现不寻常的技术。 某些攻击展现出了许多精妙和高明之处，这可能表明是经验丰富的攻击者所为。这说明，工具和能力范围很少是新的，并大多受制于正常范围的安全对策。

在 HBGary 攻击中利用了 SQL 注入来获取密码和帐户信息，这使得攻击者可以更深入地访问网络。 SQL 注入在 IDS 供应商的各种方法中都有介绍。 调整此保护并处于有效防范攻击的阻止模式下很关键。

Anonymous 进行的许多成功操作只有在付出成功的社会工程努力之后才会有效。 通常，网络钓鱼和鱼叉式网络钓鱼会带来允许操作继续进行的关键信息。 未能实现社会工程目标似乎限制了该组实施拒绝服务攻击和投机性涂改破坏，但仍会实现其目标。

本文的参与编写者列表包括：

IBM MSS 智能中心

Michelle Alvarez – 团队领导兼网络威胁智能分析师

Lyndon Sutherland

IBM X-Force 数据库团队

参考

2011 年第一季度的多产和影响问题

全球能源网络攻击： “夜龙”
http://www.mcafee.com/us/resources/white-papers/wp-global- energy-cyberattacks-night-dragon.pdf

HBGary Federal 受到 Anonymous 的攻击和侵害
http://nakedsecurity.sophos.com/2011/02/07/hbgary-federal- hacked-and-exposed-by-anonymous/

黑客刚刚发布他们所言是关于美国银行及其抵押实践的势大力沉的电子邮件宝藏
http://www.businessinsider.com/anonymous-hackers-bank-of- america-wikileaks-emails-documents-2011-3

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

在美国印制
2011 年 5 月

与非 IBM 产品相关的此文档中的信息是从这些产品的供应商、他们发布的公告材料或公开可获得的来源获得的。 关于非 IBM 产品的功能的问题应由这些产品的供应商解决。

所有包含在此出版物中的性能数据都是在特定的操作环境和在以上所描述的并作为图形的形势而显示的条件下获得的。 在其他操作环境中所获得的性能可能会有所不同，并且客户应执行他们自己的测试。

WGL03008-USEN-00