



**IntelliSIGHT™**

Security beyond the edge

# 近期恶意代码分析和统计

2008年11月24日

## 近期恶意代码分析

### 综述

2008 年 11 月对于埃赛特伙伴公司的恶意代码分析小组来说真的是非常繁忙的一个月。这是由于微软的定期补丁导致了（范围不小的）漏洞利用活动，漏洞开发工具和恶意代码的快速蔓延。埃赛特伙伴公司实验室原创性研究关于 Adobe Reader 的漏洞利用，Koobface 攻击的更新（08-2702）和主机提供者 McColo 及 UATelecom 的活动也都意义非凡。

### 关于微软公布 netapi32.dll RPC 组件堆栈缓冲器溢出漏洞补丁的恶意代码所造成的影响

10 月 23 日周四，微软公布了其周期性补丁，本次是针对所有微软主要产品中的组件 netapi32.dll RPC 堆栈缓冲器溢出漏洞的补丁。许多值得关注的恶意代码很快地就与相关的漏洞利用联系起来，名为 Gimmiv (08-3544)、KernelBot (08-3641) 和 WeCorl (08-3645)。MS08-067 漏洞的快速扫描工具也开始大量涌现，尤其是在中国（请阅读今天的“关注中国部分”的中国 MS08-067 活动相关文章）。

这些工具绝大多数都是来自早期 Milw0rm 漏洞利用中简单的执行 shell 命令，而不会造成某种严重后果，类似某种 Blaster 蠕虫的工具。自从这种大量的 RPC 蠕虫攻击事件出现以来，基于主机或者网络的防火墙即开始急剧增多，而且已经相当程度上解决了这类问题的。但是，这类基于服务的漏洞一旦发生，仍然会存在通过其它的某种方式损害到内部主机的重大风险，比如浏览器漏洞利用，攻击者利用此类漏洞可以毫无阻碍或轻松跳过外部防火墙在企业内部散播传染源。因此，此类问题必须严肃对待。

### 来自从事不法活动主机提供商 McColo 的更新

埃赛特伙伴公司过去曾经报导过关于从事不法活动主机的提供商 McColo，它的运营方式类似以前的 Russian Business Network (RBN)，就像一把罪犯的保护伞。McColo 大概有一年多曾经是恶意代码攻击和垃圾邮件的聚集地。在 2008 年 11 月 11 日的晚上，McColo 被关闭了，但是它于 15 日通过 Teliasonera 的链接重新回到了线上。与以往不同的是，McColo 主机提供商已经受到了安全组织的注意和监控。这一系列的事件在过去的几周里触发了一系列有趣的变化，其中包括大量黑客活动被迫暂时停止。一些有影响力的成员开始忙于向其它一些活跃着的主机供应商迁移，就像当初 RBN 倒闭的时候一样。就在本篇报告在撰写的过程中，McColo 已经与另外一家逆流而上的供应商取得了联系，并宣布现在想让它去死还为时过早。

### 新一轮正在进行的网络钓鱼活动

埃赛特伙伴公司最近发现了数起安装木马的网络钓鱼活动。坏蛋们有计划的使用伪装为疾病预防控制中心为主题的电子邮件信息来哄骗目标用户浏览恶意网站，并将其转发给其他同事：“这是一个政府程序而你的任务就是验证你收到的附件内容直至完成（如果你没有收到请在<URL>这里查找并将它转发给其他员工。）”，还有的电子邮件使用美国财政部主题警告所谓的网络钓鱼活动。这些恶意 URL 将使你转跳到一个服务器上（123.134.66.8）并尝试利用基于 Flash 的 CVE-2007-

0071 漏洞。一旦成功，该代码就会打开一个包含诈骗信息的文档并试图安装一个黑客控制软件。如果不能成功，该网站仅作为一个访问过的域名出现。

### 埃赛特伙伴公司实验室原创性研究：Adobe Reader 8.1.2 堆栈缓冲器溢出漏洞

2008 年 11 月 7 日周五，SANS 报导了一篇编号为 CVE-2008-2992 的漏洞利用信息，一个名为“Adobe Reader 8.1.2 堆栈缓冲器溢出漏洞”（埃赛特伙伴公司实验室原创性研究）的问题于 2008 年 11 月 4 日被发布了出来（IntelliSIGHT 报告# 08-2397）。漏洞利用代码在随后的一天被公布，漏洞利用事件在其被披露后第三天开始陆续发生。

埃赛特伙伴公司拥有一些过去积累下来的珍贵历史档案，而且能够快速准确地捕捉、清除混乱的 JavaScript 程序中的 bug，逆向推理漏洞利用文件和多种负载的测试。黑客攻击往往会投放下大量的木马程序，按其感染程度还会出现吸引来大批二次攻击的可能性。IntelliSIGHT 活动报告 #08-3710 中收录了关于此问题的完整报告的链接。负载工具主要由民间漏洞开发产品和搜索引擎中自动跳出的恶意广告软件组成。这些恶意广告软件的代码能够暗中的侦测到用户的搜索内容并发送目标广告，经常是将用户的需求重定向到有意安排好的搜索结果上。在众多安全事件中都有发现此类代码的存在，我们的恶意代码分析小组已经对其进行了数月的跟踪研究。其中有这样一则安全事件提到了一种变异的 DNS 修改器，它会尝试着以 telnet 和 HTTP 协议为跳板入侵本地路由器；它还会在机器上安装一个很多反病毒引擎和扫描器都无法侦测到的组件。

## 近期恶意代码统计

### 综述

正如上个月所称，埃赛特伙伴公司近期致力创作一份与其它几家业界顶尖的安全服务提供商共有的恶意 URL 反馈。这种协作效用可以为私有组的成员们提供对民间广泛流传的恶意代码最为广阔的视角和最全面的蓝图。埃赛特伙伴公司已经启动了此项目，以最具洞察力的威胁视角和最及时的响应来满足客户提出的一切需求。

这是从多方数据中整理出来的第二份 IntelliSIGHT 每月威胁报告专题统计，仅仅一个月期间，反馈的数量成天文学数字并不断增长。上个月，埃赛特伙伴公司分析了来自反馈中的超过 185000 条不重复的 URL。本月这个数字为 1107430。这些 URL 指向 61335 个不同的文件，这其中包括可执行的恶意代码，HTML 页面（例如：JavaScript 漏洞、网络钓鱼等）和配置文件等。这种快速增长成功地将计算和详细数据核查统计升级为一种前所未有的挑战。现在，为了能够更高效的应付这种增长中带来的负荷而开始添加额外的基础设备。下列表格即为本月期间所处理过的 URL 中，已侦测到的恶意代码排行以及具有攻击性的域名和 IP 地址排行。

排名	新样品的最强病毒家族
1.	W32/PePatch
2.	W32/Buzus
3.	W32/Banker
4.	W32/Exchanger
5.	W32/BHO.FHG
6.	W32/Zlob
7.	W32/Emogen
8.	W32/TibsPk
9.	W32/OnlineGames

这第一张表包括了在反病毒侦查中频发率最高的病毒家族的名称。首先是 Zlob、Tibs 和 OnlineGames 这几个总是榜上有名的病毒，就不需要更多的介绍了。PePatch 被侦测为一个普通的软件包，但是它能够作用于下载器中，自动给系统的进程打补丁，为了能够绕过安全限制比如软件防火墙之类的，而在磁盘中永久性的执行。Emogen 和 Buzus 都是相当具有代表性的代码包。Exchanger 经常被认为是用于安装导致安全问题的软件和/或 Srizbi。Banker 代码自然就是窃取信息、有效注册的 key 等，通常借助捕捉 POST 函数发送的数据来偷取金融或其它类型在线支付网站的数字证书。BHO.FHG 是一个以浏览器为平台的恶意广告软件，能够在 IE 中自动生成弹出窗口。

特征码匹配排行(AVG):
PSW.Banker4.APJJ
SHeur.CQST
I-Worm/Nuwar.N
Downloader.Zlob.AEWL
Generic11.BLNU
SHeur.CPGD
PSW.OnlineGames.BDQV
PSW.Generic6.ALRA
Generic11.BLMQ
Downloader.Zlob.AFKC
SHeur.CQPP
PSW.Banker4.APMB
PSW.Banker4.VQA
Dropper.Small.VE
Downloader.Agent.ANGS
PSW.Banker4.APAA
PSW.OnlineGames.AZKS
PSW.OnlineGames.BEXI
Downloader.Generic7.BDCG
Dropper.Delf.BNO
Agent.AGYD
Generic11.BLNC
PSW.Generic6.ALST

此表为 AVG 扫描器侦测出的登陆信息窃取器排行（既最常见的个别变种）

提交的主机排行	URL 数量
membres.lycos.fr	1775
usuarios.lycos.es	549
72.232.229.50	316
www.blockyell.com	237
www.shtime.com	213
youhide.com	206
www.messentools.com	206
66.220.17.154	204
64.69.47.202:8080	198
202.131.30.82	169
www.gamecentersolution.com	159
66.220.17.200	154
www.membres.lycos.fr	135
signin-ebay-com-dll.oq.pl	131
www.gatasgyn.com	129
www.alcoy.es	121
www.w8.orgoro.com	121
mix11.mindenkilapja.hu	120

此表显示了主机与其相关联的数量最多的链接。这是证明它们是网络钓鱼或其它类型的骗子网站的最好证据。

独占文件的主机排行	文件数量
64.69.47.202:8080	197
www.gamecentersolution.com	158
66.220.17.200	153
77.245.61.232	94
www.bestprivatetube.net	83
216.95.196.22	77
69.46.16.101	63
www.xprivatetube.com	59
193.33.61.169	52
quickdirectdownload.com	52
up1.viruscatch.co.kr	46
58.65.235.41	44

这是在服务器上发现独占文件的主机排行榜（例如可执行文件或配置文件）。处于榜首的主机是 **64.69.47.202**，上个月的前十名排行中也包括此主机。

还需要注意的是，[www.xprivatetube.com](http://www.xprivatetube.com) 和 [www.bestprivatetube.net](http://www.bestprivatetube.net) 这两个网站同为伪装成视频网站而实际上是用来散播Zlob木马的恶意站点；上个月的统计包含了多个来自同组的入口。IP为 **58.65.235.41** 站点借助没有名气的新主机名加入网络之中但其实是Storm蠕虫的服务器。