
# 安全威胁每周警讯

2012/04/29～2012/05/05

本周威胁指数


***TrendMicro* 中国区网络安全监控中心**


# 前十大病毒警讯

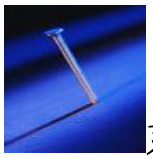
| 排名 | 病毒名称 | 威胁类型 | 风险等级 | 趋势 | 病毒行为描述 |
|---|---|---|---|---|---|
| 1 | WORM_DOWNAD.AD | 蠕虫 | ★★★★ | → | 该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒 |
| 2 | WORM_DOWNAD | 蠕虫 | ★★★★ | → | 该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒 |
| 3 | TROJ_DOWNAD.INF | 木马 | ★★★ | → | DOWNAD 蠕虫关联木马 |
| 4 | Cryp_Xed-12 | 木马 | ★★ | ↑ | 疑似病毒程序 |
| 5 | TROJ_IFRAME.CP | 木马 | ★★★ | ↓ | GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。<br>当这些文件被执行时，会重定向到这些 URL，并下载恶意程序 |
| 6 | CRCK_KEYGEN | 黑客程序 | ★★ | ↑ | 非法破解程序 |
| 7 | PAK_Generic.001 | 加壳文件 | ★★ | ↑ | 经过加壳技术加密的文件 |
| 8 | X97M_LAROUX.BK | 脚本病毒 | ★★ | ↓ | Office 宏病毒，主要感染 Excel 文件，会在 Excel 中创建一个名为 *StartUp* 的自启动宏脚本 |
| 9 | Downloader_Agent | 灰色软件 | ★★ | ↑ | 这灰色软件下载器会自动下载并安装额外的其他的灰色软件，如广告软件和间谍软件。 |
| 10 | WORM_ECODE.E-CN | 蠕虫 | ★★★★ | ↑ | E 语言病毒,产生与当前文件夹同名 exe 文件 |

## 系统漏洞信息

MS12-017 ： DNS 服务器中的漏洞可能允许拒绝服务 (2647170)

Windows Server 2003
Windows Server 2008
Windows Server 2008 R2

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-017



## 系统安全技巧

在不断公布的漏洞通报中，邮件系统的漏洞该算最普遍的一项。黑客常常利用电子邮件系统的漏洞，结合简单的工具就能达到攻击目的。 电子邮件究竟有哪些潜在的风险?黑客在邮件上到底都做了哪些手脚？一同走进黑客的全程攻击，了解电子邮件正在面临的威胁和挑战……

电子邮件的持续升温使之成为那些企图进行破坏的人所日益关注的目标。如今，黑客和病毒撰写者不断开发新的和有创造性的方法，以期战胜安全系统中的改进措施。

**出自邮件系统的漏洞**

典型的互联网通信协议——TCP 和 UDP，其开放性常常引来黑客的攻击。而 IP 地址的脆弱性，也给黑客的伪造提供了可能，从而泄露远程服务器的资源信息。

很多电子邮件网关，如果电子邮件地址不存在，系统则回复发件人，并通知他们这些电子邮件地址无效。黑客利用电子邮件系统的这种内在“礼貌性”来访问有效地址，并添加到其合法地址数据库中。

防火墙只控制基于网络的连接，通常不对通过标准电子邮件端口(25 端口)的通信进行详细审查。

**黑客如何发动攻击**

一旦企业选择了某一邮件服务器，它基本上就会一直使用该品牌，因为主要的服务器平台之间不具互操作性。以下分别概述了黑客圈中一些广为人知的漏洞，并阐释了黑客利用这些安全漏洞的方式。

**一、IMAP 和 POP 漏洞**

密码脆弱是这些协议的常见弱点。各种 IMAP 和 POP 服务还容易受到如缓冲区溢出等类型的攻击。

**二、拒绝服务(DoS)攻击**

1.死亡之 Ping——发送一个无效数据片段，该片段始于包结尾之前，但止于包结尾之后。

2.同步攻击——极快地发送 TCP SYN 包(它会启动连接)，使受攻击的机器耗尽系统资源，进而中断合法连接。

3.循环——发送一个带有完全相同的源/目的地址/端口的伪造 SYN 包，使系统陷入一个试图完成 TCP 连接的无限循环中。

**三、系统配置漏洞**

企业系统配置中的漏洞可以分为以下几类:

1.默认配置——大多数系统在交付给客户时都设置了易于使用的默认配置，被黑客盗用变得轻松。

2.空的/默认根密码——许多机器都配置了空的或默认的根/管理员密码，并且其数量多得惊人。 3.漏洞创建——几乎所有

**四、利用软件问题**

在服务器守护程序、客户端应用程序、操作系统和网络堆栈中，存在很多的软件错误，分为以下几类:

1.缓冲区溢出——程序员会留出一定数目的字符空间来容纳登录用户名，黑客则会通过发送比指定字符串长的字符串，其中包括服务器要执行的代码，使之发生数据溢出，造成系统入侵。

2.意外组合——程序通常是用很多层代码构造而成的，入侵者可能会经常发送一些对于某一层毫无意义，但经过适当构造后对其他层有意义的输入。

3.未处理的输入——大多数程序员都不考虑输入不符合规范的信息时会发生什么。

**五、利用人为因素**

黑客使用高级手段使用户打开电子邮件附件的例子包括双扩展名、密码保护的 Zip 文件、文本欺骗等。

**六、特洛伊木马及自我传播**

结合特洛伊木马和传统病毒的混合攻击正日益猖獗。黑客所使用的特洛伊木马的常见类型有:

1.远程访问——过去，特洛伊木马只会侦听对黑客可用的端口上的连接。而现在特洛伊木马则会通知黑客，使黑客能够访问防火墙后的机器。有些特洛伊木马可以通过 IRC 命令进行通信，这表示从不建立真实的 TCP/IP 连接。

2.数据发送——将信息发送给黑客。方法包括记录按键、搜索密码文件和其他秘密信息。

3.破坏——破坏和删除文件。

4.拒绝服务——使远程黑客能够使用多个僵尸计算机启动分布式拒绝服务(DDoS)攻击。

5.代理——旨在将受害者的计算机变为对黑客可用的代理服务器。使匿名的 TelNet、ICQ、IRC 等系统用户可以使用窃得的信用卡购物，并在黑客追踪返回到受感染的计算机时使黑客能够完全隐匿其名。

**典型的黑客攻击情况**

尽管并非所有的黑客攻击都是相似的，但以下步骤简要说明了一种“典型”的攻击情况。

**步骤 1:外部侦察**

入侵者会进行‘whois’查找，以便找到随域名一起注册的网络信息。入侵者可能会浏览 DNS 表(使用‘nslookup’、‘dig’或其他实用程序来执行域传递)来查找机器名。

**步骤 2:内部侦察**

通过“ping”扫描，以查看哪些机器处于活动状态。黑客可能对目标机器执行 UDP/TCP 扫描，以查看什么服务可用。他们会运行“rcpinfo”、“showmount”或“snmpwalk”之类的实用程序，以查看哪些信息可用。黑客还会向无效用户发送电子邮件，接收错误响应，以使他们能够确定一些有效的信息。此时，入侵者尚未作出任何可以归为入侵之列的行动。

**步骤 3:漏洞攻击**

入侵者可能通过发送大量数据来试图攻击广为人知的缓冲区溢出漏洞，也可能开始检查密码易猜(或为空)的登录帐户。黑客可能已通过若干个漏洞攻击阶段。

**步骤 4:立足点**

在这一阶段，黑客已通过窃入一台机器成功获得进入对方网络的立足点。他们可能安装为其提供访问权的“工具包”，用自己具有后门密码的特洛伊木马替换现有服务，或者创建自己的帐户。通过记录被更改的系统文件，系统完整性检测(SIV)通常可以在此时检测到入侵者。

**步骤 5:牟利**

这是能够真正给企业造成威胁的一步。入侵者现在能够利用其身份窃取机密数据，滥用系统资源(比如从当前站点向其他站点发起攻击)，或者破坏网页。

另一种情况是在开始时有些不同。入侵者不是攻击某一特定站点，而可能只是随机扫描 Internet 地址，并查找特定的漏洞。

**邮件网关对付黑客**

1.在电子邮件系统周围锁定电子邮件系统——电子邮件系统周边控制开始于电子邮件网关的部署。电子邮件网关应根据特定目的与加固的操作系统和防止网关受到威胁的入侵检测功能一起构建。

2.确保外部系统访问的安全性——电子邮件安全网关必须负责处理来自所有外部系统的通信，并确保通过的信息流量是合法的。通过确保外部访问的安全，可以防止入侵者利用 Web 邮件等应用程序访问内部系统。

3.实时监视电子邮件流量——实时监视电子邮件流量对于防止黑客利用电子邮件访问内部系统是至关重要的。检测电子邮件中的攻击和漏洞攻击(如畸形 MIME)需要持续监视所有电子邮件。

在上述安全保障的基础上，电子邮件安全网关应简化管理员的工作、能够轻松集成，并被使用者轻松配置。

来源：51CTO