安全威胁每周警讯

2011/11/27～2011/12/03

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	TROJ_DOWNAD.INF	木马	★★★	↑	DOWNAD 蠕虫关联木马
2	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。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
3	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
4	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
5	Cryp_Xed-12	木马	★★★	→	木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染
6	HTML_IFRAME.AZ	网页病毒	★★	↑	网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站
7	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
8	CRCK_KEYGEN	破解程序	★★	↓	破解程序
9	PAK_Generic.001	加壳文件	★★	↑	经过加壳技术加密的文件
10	Expl_ShellCodeSM	脚本病毒	★★	↑	疑似恶意 java 脚本

系统漏洞信息

MS11-086：Active Directory 中的漏洞可能允许特权提升 (2630837)

Windows XP

Windows Server 2003

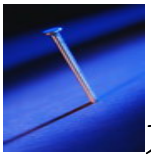
Windows Vista

Windows Server 2008

Windows 7

Windows Server 2008 R2

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS11-086



系统安全技巧

1、监听

大多数通过网络发送的数据都是“文本”形式，也就是在加密成密码文本之前的普通的可读文本。这意味着，任何人使用网络“嗅探器（例如 Network Monitor 3.x 或者第三方程序 Wireshark 等）”都可以轻松地读取这些文本信息。

一些保存自己用户名和密码列表的服务器应用程序允许这些登录信息以文本格式在网络传输。网络攻击者只要简单地使用嗅探程序，接入到集线器或者交换器的可用端口就可以获取这些信息。事实上，大部分通过网络发送的数据都是文本格式的，这使得攻击者很容易可以获得这些信息。而这些信息可能包含敏感数据，例如信用卡号码、社保号码、个人电子邮件内容和企业机密信息等。很明显，解决这个问题的解决方案就是使用 IPsec 或者 SSL 等技术，对在网络传送的数据进行加密。

2、欺诈

源 IP 地址和目的 IP 地址是为 TCP/IP 网络的计算机之间建立会话的前提条件。IP“欺诈”行为是指假冒网络中合法主机计算机的身份，来获取对内部网络中计算机的访问权限。欺诈的另一种说法是“模拟”，实际上，入侵者是使用合法 IP 地址来“模拟”合法主机计算机。

为了防止 IP 欺诈攻击，你可以使用 IPsec 用于计算机间的通信，使用访问控制列表（ACLs）来阻止下游端口的私有 IP 地址，过滤入站和出站流量，并将路由器和交换机配置为阻止源自外部局域网而声称自己源自内部网络的流量。你还可以启用路由器上的加密功能，这样可以允许你信任的外部计算机与内部计算机进行通信。

3、TCP/IP 序列号攻击

另一种常见欺诈攻击是“TCP/IP 序列号攻击”。传输控制协议（TCP）主要负责 TCP/IP 网络的通信的可靠性，这包括确认信息发送到目的主机。为了追踪通过网络发送的字节，每个段都被分配了一个“序列号”。高级攻击者可以建立两台计算机之间的序列模式，因为序列模式并不是随机的。

4、密码盗用

攻击者只要成功盗用网络密码就能访问不能访问的资源，他们可以通过很多方法来获取密码。

社会工程学攻击：攻击者使用一个假的身份联系对目标信息拥有访问权限的用户，然后他要求用户提供密码。

嗅探：很多网络应用程序允许用户名和密码以未加密文本形式在网络传输，这样的话，攻击者就可以使用网络嗅探应用程序来拦截这个信息。

破解：“破解者”使用很多不同的技术来“猜测”密码，尝试所有可能的数字字母组合，直到猜出正确的密码。破解技术包括字典攻击和暴力攻击等。

如果管理员密码被盗用，攻击者将能够访问所有受访问控制保护的网络资源，入侵者现在可以访问整个用户账户数据库了。有了这些信息，现在他可以访问所有文件和文件夹，更改路由信息，在用户不知情的情况下，修改用户需要的信息。

抵御密码盗用攻击需要一个多方面的战略，教导用户关于社会工程学的知识，制定密码保护制度，规定密码复杂度和长度要求，要求用户定期修改密码。部署多因素身份验证，这样攻击者不能仅凭一个密码就获得访问权限。

5、拒绝服务攻击

有许多不同类型的拒绝服务攻击，这些技术的共同点就是扰乱正常计算机或者目标机器运行的操作系统的能力。这些攻击可以将大量无用的数据包塞满网络，损坏或者耗尽内存资源，或者利用网络应用程序的漏洞。分布式拒绝服务攻击源自多台机器（例如，由几十、几百甚至成千上万台分布在不同地理位置的“僵尸”电脑组成的僵尸网络）。

传统拒绝服务攻击的例子包括：

TCP SYN 攻击

SMURF 攻击

Teardrop 攻击

Ping of Death 攻击

6、TCP SYN 攻击

当 TCP/IP 网络的计算机建立会话时，他们会通过“三次握手”过程，这三步握手包括：

源主机客户端发送一个 SYN（同步/开始）数据包，这台主机在数据包中包括一个序列号，服务器将在下一步骤中使用该序列号。

服务器会向源主机返回一个 SYN 数据包，数据包的序列号为请求计算机发来的序列号+1

客户端接收到服务端的数据包后，将通过序列号加 1 来确认服务器的序列号

每次主机请求与服务器建立会话时，将通过这个三次握手过程。攻击者可以通过从伪造源 IP 地址发起多个会话请求来利用这个过程。服务器会将每个打开请求保留在队列中等待第三步的进行，进入队列的条目每隔 60 秒会被清空。

如果攻击者能够保持队列填满状态，那么合法连接请求将会被拒绝。因此，服务器会拒绝合法用户的电子邮件、网页、ftp 和其他 IP 相关服务。

7、Ping of Death 攻击

Ping of death 是一种拒绝服务攻击，方法是由攻击者故意发送大于 65536 比特的 ip 数据包给对方。Ping of death 攻击利用了 Internet 控制消息协议（ICMP）和最大传输单元（MTU）的特点，Ping 命令发送 ICMP 回应请求（ICMP Echo-Request）并记录收到 ICMP 回应回复（ICMP Echo-Reply）。MTU 定义了具有不同媒体类型的网络架构的单元最大传输量。

如果数据包大小大于 MTU，数据包将被拆分，并在目的主机重新组合。当数据包被分解时，数据包会涵盖一个“偏移”值，这个偏移值用于在目的主机重组数据。攻击者可以将最后的数据片段替换为合理的偏移值和较大的数据包，这样将会超过 ICMP 回应请求数据部分的数量，如果进行重组，目的计算机将会重新启动或者崩溃。

8、SMURF 攻击

SMURF 攻击试图通过将 ICMP 回显请求和回复塞满网络来禁用网络。攻击者将会欺诈一个源 IP 地址，然后向广播地址发出一个 ICMP 回显请求，这将会导致网络段的所有计算机向假冒请求进行回复。如果攻击者可以将这种攻击保持一段时间，有效的信息将无法通过网络，因为 ICMP 请求信息已经塞满网络。

9、Teardrop 攻击

Teardrop 攻击是使用一种程序（例如 Teardrop.c）来执行的，它将会造成与 Ping of Death 攻击中类似的数据碎片，它利用了重组过程的一个漏洞，可能导致系统崩溃。

10、抵御 DOS 和 DDOS 攻击

抵御 DOS 和 DDOS 攻击应该采取多层次的方法。防火墙可以保护网络抵御简单的“洪水”攻击，而用于流量调整、延迟绑定（TCP 拼接）和深度数据包检测的交换机和路由器可以抵御 SYN flood（利用 TCP 三次握手协议的缺陷，向目标主机发送大量的伪造源地址的 SYN 连接请求，消耗目标主机资源）。入侵防御系统可以阻止某些形式的 DOS/DDOS 攻击，市面上还有专门抵御 DOS 的产品，被称为 DOS 抵御系统或者 DDS。

11、中间人攻击

中间人攻击是这样的情况，两方认为他们只是在与对方进行通信，而实际上，还有一个中间方在监听会话。中间人攻击可以通过模拟发送者或者接受者的身份来偷偷切入会话。在攻击者的介入期间，他可以修改或者删除传输中的消息。

攻击者通过使用网络嗅探器，可以记录和保存信息供以后使用，这可以让入侵者发起后续的重放攻击，在记录了会话信息后，中间人可以重放此信息以便在未来了解网络身份验证机制，这就是所谓的重放攻击。

中间人攻击通常是基于 web 的，中间人对客户端（浏览器）和 web 服务器之间的通信进行拦截。基于 web 的中间人攻击可以通过使用最新版本的浏览器来抵御，最新版本浏览器拥有内置保护机制，并通过使用扩展验证 SSL 证书的网站来通信。双因素身份验证可以用于秘密通信，但是，这并不能完全杜绝中间人攻击，因为中间人通常是等待用户使用智能卡或者令牌来进行身份验证。带外身份验证是最好的保护方法，但是价格昂贵，开销很大。

12、应用程序级攻击

面向应用程序的攻击试图利用某些网络应用程序固有的缺陷。通过利用这些网络应用程序的缺陷，攻击者可以：

破坏或修改重要操作系统文件

更改数据文件内容

造成网络应用程序或者整个操作系统不正常运行，甚至崩溃

扰乱应用程序或操作系统的正常安全性和访问控制

植入程序将信息返回给攻击者，臭名昭著的 Back Orifice 就是一个例子

这些应用程序级攻击为入侵者提供了一片“沃土”。很多网络应用程序还没有完成安全评估和测试以提高对攻击的免疫力。

抵御应用程序级攻击很困难，因为每个应用程序的漏洞都不相同。最基本的抵御应该是采取“纵深防御”的安全措施，并加强对已知漏洞的认识。

13、盗用密钥攻击

密钥是数字，或者“密码”，可以用来验证通信的完整性或者加密通信内容。有很多不同类型的密钥。其中一种类型被称为“共享的密码”，发送计算机使用密钥加密信息，接收计算机使用相同的密钥解密信息。利用这个“共享的密码”，两台计算机可以进行私人通信。

另一种密钥是“私钥”，私钥可以用于确认发送者的身份，也就是所谓的“签名”信息，当接收者收到使用某人的私钥签名的信息时，他可以确认发送者的身份。

如果攻击者获取了这些密钥，他就可以使用“假身份”用别人的私钥进行通信。如果他得到了“共享密钥”，他就可以解密由该密钥加密的信息。

一旦密钥被暴露，就无法保护信息的安全性。然而，发现密钥被暴露往往很难，只有当发现重要信息丢失时，才会意识到密钥丢失。缓解这种损害的方法包括进行多密钥加密。

来源:51CTO