安全威胁每周警讯

2012/03/18～2012/03/24

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

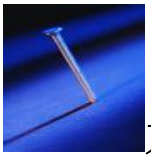
排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	WORM_DOWNAD.AD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
2	TROJ_DOWNAD.INF	木马	★★★	↓	DOWNAD 蠕虫关联木马
3	WORM_DOWNAD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
4	TROJ_IFRAME.CP	木马	★★★	→	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
5	Cryp_Xed-12	疑似病毒	★★★★	→	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	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	Adware_Adplus	灰色软件	★★	↑	广告软件
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	JS_OBFUSCATED.FI	脚本病毒	★★	↓	当用户访问包含此脚本的网站时，会自动运行此此脚本，并被重定向到其他包含恶意代码的站点。

系统漏洞信息

MS12-010 ： Internet Explorer 的累积性安全更新 (2647516)

Internet Explorer 6
Internet Explorer 7
Internet Explorer 8
Internet Explorer 9

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-010



系统安全技巧

试想一下，一台被感染了网络病毒的普通计算机连接到网络后，对应系统中的网络病毒很有可能会通过网络传染给局域网中的其他计算机。这样相互传播、感染，整个网络势必就会受到网络病毒的严重攻击，此时网络的安全性自然也就受到破坏了。

为了保证网络安全，必须对网络的接入进行适当控制，确保那些可以信任的普通计算机才能接入本地网络并访问互联网。

那么，究竟哪些普通计算机是可以信任的呢？在这里，我们可以强制普通计算机自动从 DHCP 服务器那里获得 IP 地址，在申请 IP 地址的过程中，要求 DHCP 服务器对普通计算机的合法性进行认证。如果计算机能够顺利通过认证，那么 DHCP 服务器才能将上网参数地址，包括 IP 地址、网关、DNS 服务器等，分配给这台计算机，这样一来可以信任的普通计算机系统就能正常接入到网络了。

如果计算机没有通过 DHCP 服务器的验证，那么对应系统就无法从 DHCP 服务器那里获得有效的上网参数，此时这些不值得信任的普通计算机也就不能连接到本地网络。这样一来，本地网络的安全性就能得到保证了。

在进行客户端系统的合法性认证时，可以先在 DHCP 服务器中创建合法性规则，同时为该规则配置相应的上网参数，包括 IP 地址、网关、DNS 服务器等，之后为客户端系统设计合法性标记。这样，以后普通计算机向 DHCP 服务器申请上网参数时，DHCP 服务器中的合法性规则就会对客户端系统的合法性标记进行检查验证：如果发现客户端系统没有合法性标记或标记不能通过合法性规则验证时，就不会为它分配有效的上网参数;如果客户端系统通过合法性规则验证，对应规则下面的上网参数就能自动分配给目标客户端系统了，

这个时候普通计算机就能正常地接入到本地网络中。

创建合法性规则

为了对客户端系统的上网安全性进行控制，可以在 DHCP 服务器中创建合法性规则，来对普通计算机的合法性进行认证。

可以在 DHCP 服务器中创建一个新的 DHCP 用户类别，并要求对客户端系统的用户类别进行验证，验证通过之后才能对客户端系统的上网请求做出响应。

在创建新的 DHCP 用户类别时，首先打开 DHCP 服务器主机系统的“开始”菜单，从中依次选择“程序”→“管理工具”→“DHCP”命令，进入 DHCP 服务器控制台界面，选中该界面左侧列表中的目标主机图标，同时右击该主机图标，并选择右键菜单中的“定义用户类别”命令或“定义提供商类别”命令，弹出新建用户类别向导窗口，如图 1 所示。在该向导窗口的“显示名称”位置处，输入一个 DHCP 用户类别名称，例如，将该用户类别名称输入为“hefa”。

为了方便日后管理，还可以对该用户类别的作用进行一些描述，例如，在“描述”位置处输入“控制网络接入安全”之类的描述性信息。当然，如果 DHCP 用户类别名称比较少，可以不设置描述信息。

接下来，还要在 ID 位置处设置合法计算机的匹配类 ID，例如，当我们在 ASCII 字符位置处输入“hefa”信息时，对应 ID 位置处的二进制数值就是合法计算机的匹配类 ID。日后 DHCP 服务器会通过这个匹配类 ID 来验证普通计算机的合法性。在确认上面的设置正确无误后，单击“确定”按钮，保存好上述设置操作。

配置合法上网参数

如果 DHCP 服务器发现普通计算机系统的匹配类 ID 符合要求时，就认为该客户端系统是合法的。此时就应该为目标客户端系统分配合法、有效的上网参数，确保该计算机可以顺利地接入到本地网络中。

为此，在我们创建好“hefa”用户类别名称时，还应该为该用户类别配置合法的上网参数，确保那些通过用户类别验证的普通计算机可以从 DHCP 服务器那里申请到有效的上网参数。

下面就是具体的配置步骤：

首先，切换进入 DHCP 服务器的控制界面，展开该界面左侧子窗格中的目标主机选项，右击“作用域选项”，选择右键菜单中的“配置选项”命令，继续选择弹出界面中的“高级”选项卡，打开高级选项设置页面，如

图 2 所示。

在这里可以为合法计算机分配 IP 地址、默认网关、DNS 服务器等上网参数，同时可以设置 IP 地址的租约期限等参数。例如，要为“hefa”用户类别配置上网参数时，可以先单击“用户类别”位置处的下拉按钮，并从下拉列表中将先前创建好的“hefa”用户类别选中，之后从可用选项列表中选中“003 路由器”，并在对应选项下面的设置区域输入合适的默认网关地址，然后单击“添加”按钮，即可完成默认网关的分配操作。

之后选中“006DNS 服务器”选项，在对应该选项下面的设置区域，输入本地网络上网访问时用到的 ISP 提供的 DNS 服务器地址，再单击“添加”按钮，完成 DNS 服务器的分配操作。同样地，还可以选中“051 租约”选项，来设置动态 IP 地址的有效租约期限。

如果想为普通计算机修改动态 IP 地址，必须展开目标作用域下面的“地址池”选项，并在对应选项的设置页面中修改上网 IP 地址，修改完毕后单击“确定”按钮保存好设置操作。

设置合法性标记

为了保证那些值得信任的普通计算机系统可以顺利地通过 DHCP 服务器的合法性验证，应该事先为那些安全的客户端系统设置合法性标记，确保该系统的 DHCP 类 ID 名称符合合法性验证要求。

在为普通计算机设置合法性标记时，可以依次选择“开始”→“运行”命令，打开客户端系统的运行文本框，在其中执行“CMD”字符串命令，进入对应系统的 MS-DOS 工作窗口。

接下来，在 MS-DOS 工作窗口的命令行提示符下，执行“ipconfig/setclassidLocalConnectionhefa”字符串命令，这样就可以成功地将客户端系统本地连接的 DHCP 类 ID 名称设置为“hefa”标记了。

控制网络接入安全

为了让普通计算机接受 DHCP 服务器的合法性控制，必须强制要求客户端系统在上网访问时，主动连接 DHCP 服务器。这样一来，DHCP 服务器就能自动对上网计算机的合法性进行验证了。

要做到这一点，其实很简单，我们可以设置普通客户端系统的上网参数，让其自动获得 IP 地址。

在设置自动获得 IP 操作时，先打开客户端系统的“开始”菜单，从中逐一选择“设置”→“网络连接”选项，用鼠标右键单击网络连接列表界面中的本地连接图标，再执行右键菜单中的“属性”命令，弹出本地连

接属性设置对话框。

选择该对话框中的“常规”选项卡，选择该选项设置页面中的 TCP/IP 协议选项，同时单击“属性”按钮，打开对应的选项设置对话框，选中这里的“自动获得 IP 地址”、“自动获得 DNS 服务器地址”等选项，再单击“确定”按钮，执行设置保存操作。

以后，当包含有“hefa”标记的普通计算机尝试连接 DHCP 服务器时，DHCP 服务器的合法性规则就会认为该计算机是可以信任的，就会将对应规则下面的上网参数分配给该计算机了。

有了上网参数，该计算机系统就能正常接入到本地局域网中了;而那些不安全的普通计算机则因为无法得到上网参数而不能进行网络连接，网络安全因此得到一定的保障。

来源： 51CTO