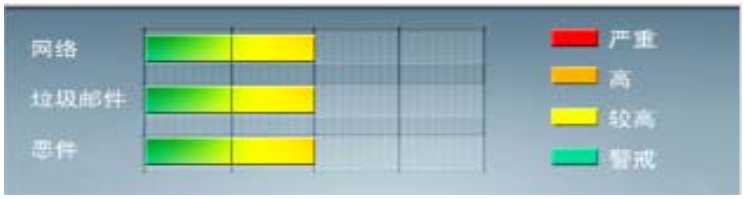
安全威胁每周警讯

2010/12/18～2010/12/25

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	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
3	TROJ_IFRAME.CP	木马病毒	★★★	→	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
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	★★★	→	疑似病毒
6	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
7	CRCK_KEYGEN	破解程序	★★	↓	非法破解程序
8	PAK_Generic.001	加壳程序	★★	→	对加壳文件的通用检测。病毒通常会使用加壳手法来达到不被杀毒软件检测的目的
9	Gray_Gen	灰色软件	★★★	→	灰色软件的通用检测名。在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件
10	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

系统漏洞信息

MS10-092:任务计划程序中的漏洞可能允许特权提升 (2305420)

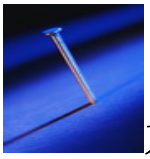
受影响的软件:

Windows Vista

Windows Server 2008

Windows 7

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-092.mspx



系统安全技巧

摘要: 当黑客入侵一台主机后，会想方设法保护自己的“劳动成果”，因此会在肉鸡上留下种种后门来长时间得控制肉鸡，其中使用最多的就是账户隐藏技术。在肉鸡上建立一个隐藏的账户，以备需要的时候使用。本文就对隐藏账户这种黑客常用的技术进行揭密。

当黑客入侵一台主机后，会想方设法保护自己的“劳动成果”，因此会在肉鸡上留下种种后门来长时间 得控制肉鸡，其中使用最多的就是账户隐藏技术。在肉鸡上建立一个隐藏的账户，以备需要的时候使用。账户隐藏技术可谓是最隐蔽的后门，一般用户很难发现系统 中隐藏账户的存在，因此危害性很大，本文就对隐藏账户这种黑客常用的技术进行揭密。

在隐藏系统账户之前，我们有必要先来了解一下如何才能查看系统中已经存在的账户。在系统中可以进 入“命令提示符”，控制面板的“计算机管理”，“注册表”中对存在的账户进行查看，而管理员一般只在“命令提示符”和“计算机管理”中检查是否有异常，因 此如何让系统账户在这两者中隐藏将是本文的重点。

一、“命令提示符”中的阴谋

其实，制作系统隐藏账户并不是十分高深的技术，利用我们平时经常用到的“命令提示符”就可以制作一个简单的隐藏账户。

点击“开始”→“运行”，输入“CMD”运行“命令提示符”，输入“net user piao$Content$nbsp;123456 /add”，回车，成功后会显示“命令成功完成”。接着输入“net localgroup administrators piao$Content$nbsp;/add”回车，这样我们就利用“命令提示符”成功得建立了一个用户名为“piao$”，密码为“123456”的 简单“隐藏账户”,并且把该隐藏账户提升为了管理员权限。

我们来看看隐藏账户的建立是否成功。在“命令提示符”中输入查看系统账户的命令 “net user”，回车后会显示当前系统中存在的账户。从返回的结果中我们可以看到刚才我们建立的“piao$”这个账户并不存在。接着让我们进入控制面板的 “管理工具”，打开其中的“计算机”，查看其中的“本地用户和组”，在“用户”一项中，我们建立的隐藏账户“piao$”

暴露无疑。

可以总结得出的结论是：这种方法只能将账户在“命令提示符”中进行隐藏，而对于“计算机管理”则无能为力。因此这种隐藏账户的方法并不是很实用，只对那些粗心的管理员有效，是一种入门级的系统账户隐藏技术。

二、在“注册表”中玩转账户隐藏

从上文中我们可以看到用命令提示符隐藏账户的方法缺点很明显，很容易暴露自己。那么有没有可以在“命令提示符”和“计算机管理”中同时隐藏账户的技术呢?答案是肯定的，而这一切只需要我们在“注册表”中进行一番小小的设置，就可以让系统账户在两者中完全蒸发。

1、峰回路转，给管理员注册表操作权限

在注册表中对系统账户的键值进行操作，需要到 “HKEY_LOCAL_MACHINESAMSAM”处进行修改，但是当我们来到该处时，会发现无法展开该处所在的键值。这是因为系统默认对系统管理员 给予“写入”和“读取控制”权限，没有给予修改权限，因此我们没有办法对“SAM”项下的键值进行查看和修改。不过我们可以借助系统中另一个“注册表编辑 器”给管理员赋予修改权限。

点击“开始”→“运行”，输入“regedt32.exe”后回车，随后会弹出另一个“注册表编 辑器”，和我们平时使用的“注册表编辑器”不同的是它可以修改系统账户操作注册表时的权限(为便于理解，以下简称 regedt32.exe)。在 regedt32.exe 中来到“HKEY_LOCAL_MACHINESAMSAM”处，点击“安全”菜单→“权限”， 在弹出的“SAM 的权限”编辑窗口中选中“administrators”账户，在下方的权限设置处勾选“完全控制”，完成后点击“确定”即可。然后我们 切换回“注册表编辑器”，可以发现“HKEY_LOCAL_MACHINESAMSAM”下面的键值都可以展开了。

提示：上文中提到的方法只适用于 Windows NT/2000 系统。在 Windows XP 系统中，对于权限的操作可以直接在注册表中进行，方法为选中需要设置权限的项，点击右键，选择“权限”即可。

2、偷梁换柱，将隐藏账户替换为管理员

成功得到注册表操作权限后，我们就可以正式开始隐藏账户的制作了。来到注册表编辑器的“HKEY_LOCAL_MACHINESAMSAMDomainsAccountUsersNames”处，当前系统中所有存在的账户都会在这里显示， 当然包括我们的隐藏账户。点击我们的隐藏账户“piao$”，在右边显示的键值中的“类型”一项显示为 0x3e9，向上来到 “HKEY_LOCAL_MACHINESAMSAMDomainsAccountUsers”处，可以找到“000003E9”这一项，这两者是相互对 应的，隐藏账户“piao$”的所有信息都在“000003E9”这一项中。同样的，我们可以找到“administrator”账户所对应的项为 “000001F4”。 将“piao$”的键值导出为“piao$.reg”，同时将“000003E9”和“000001F4”项的 F 键值分别导出为 user.reg，admin.reg。用“记事本”打开 admin.reg，将其中“F”值后面的内容复制下来，替换 user.reg 中的“F”值内 容，完成后保存。接下来进入“命令提示符”，输入“net user piao$Content$nbsp;/del”将我们建立的隐藏账户删除。最后，将 piao$.reg 和 user.reg 导入注册表，至此，隐藏账户制 作完成。

3、过河拆桥，切断删除隐藏账户的途径

虽然我们的隐藏账户已经在“命令提示符”和“计算机管理”中隐藏了，但是有经验的系统管理员仍可能通过注册表编辑器删除我们的隐藏账户，那么如何才能让我们的隐藏账户坚如磐石呢?

打开“regedt32.exe”，来到“HKEY_LOCAL_MACHINESAMSAM” 处，设置“SAM”项的权限，将 “administrators”所

拥有的权限全部取消即可。当真正的管理员想对“HKEY_LOCAL_MACHINESAMSAM”下面的项进行操作 的时候将会发生错误，而且无法通过“regedt32.exe”再次赋予权限。这样没有经验的管理员即使发现了系统中的隐藏账户，也是无可奈何的。

三.专用工具，使账户隐藏一步到位

虽然按照上面的方法可以很好得隐藏账户，但是操作显得比较麻烦，并不适合新手，而且对注册表进行操作危险性太高，很容易造成系统崩溃。因此我们可以借助专门的账户隐藏工具来进行隐藏工作，使隐藏账户不再困难，只需要一个命令就可以搞定。

我们需要利用的这款工具名叫“HideAdmin”，下载下来后解压到 c 盘。然后运行“命令提示 符”，输入“HideAdmin piao$Content$nbsp;123456”即可，如果显示“Create a hiden Administrator piao$Content$nbsp;Successed!”，则表示我们已经成功建立一个账户名为 piao$，密码为 123456 的隐藏账户。利用这款 工具建立的账户隐藏效果和上文中修改注册表的效果是一样的。

四、把“隐藏账户”请出系统

隐藏账户的危害可谓十分巨大。因此我们有必要在了解了账户隐藏技术后，再对相应的防范技术作一个了解，把隐藏账户彻底请出系统

1、添加“$”符号型隐藏账户

对于这类隐藏账户的检测比较简单。一般黑客在利用这种方法建立完隐藏账户后，会把隐藏账户提升为 管理员权限。那么我们只需要在“命令提示符”中输入“net localgroup administrators”就可以让所有的隐藏账户现形。如果嫌麻烦，可以直接打开“计算机管理”进行查看，添加“$”符号的账户是无法在这里隐藏 的。

2、修改注册表型隐藏账户

由于使用这种方法隐藏的账户是不会在“命令提示符”和“计算机管理”中看到的，因此可以到注册表 中删除隐藏账户。来到 “HKEY_LOCAL_MACHINESAMSAMDomainsAccountUsersNames”，把这里存在的账户和“计算机管理”中存在的账 户进行比较，多出来的账户就是隐藏账户了。想要删除它也很简单，直接删除以隐藏账户命名的项即可。

3、无法看到名称的隐藏账户

如果黑客制作了一个修改注册表型隐藏账户，在此基础上删除了管理员对注册表的操作权限。那么管理 员是无法通过注册表删除隐藏账户的，甚至无法知道黑客建立的隐藏账户名称。不过世事没有绝对，我们可以借助“组策略”的帮助，让黑客无法通过隐藏账户登 陆。点击“开始”→“运行”，输入“gpedit.msc”运行“组策略”，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”，双击右边的“审核策略更改”，在弹出的设置窗口中勾选“成功”，然后点“确定”。对“审核登陆事件” 和“审核过程追踪”进行相同的设置。

4、开启登陆事件审核功能

进行登陆审核后，可以对任何账户的登陆操作进行记录，包括隐藏账户，这样我们就可以通过“计算机 管理”中的“事件查看器”准确得知隐藏账户的名称，甚至黑客登陆的时间。即使黑客将所有的登陆日志删除，系统还会记录是哪个

账户删除了系统日志，这样黑客 的隐藏账户就暴露无疑了。

5、通过事件查看器找到隐藏帐户

得知隐藏账户的名称后就好办了，但是我们仍然不能删除这个隐藏账户，因为我们没有权限。但是我们可以在“命令提示符”中输入“net user 隐藏账户名称 654321”更改这个隐藏账户的密码。这样这个隐藏账户就会失效，黑客无法再用这个隐藏账户登陆。

来源： ZDNET