安全威胁每周警讯

2011/07/10～2011/07/16

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	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	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	Expl_ShellCodeSM	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
7	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
8	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
9	CRCK_KEYGEN	网页病毒	★★	→	非法破解程
10	TROJ_SPNR.03CG11	木马	★★	↑	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。 通常携带有效载荷木马或其他恶意行为，可从轻度恼人的范围到无可挽回的破坏。他们也可以修改系统设置为自动启动。

系统漏洞信息

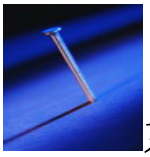
MS11-048：**SMB 服务器中的漏洞可能允许拒绝服务**

Windows Vista

Windows Server 2008

Windows 7

描述： http://www.microsoft.com/china/technet/security/bulletin/MS11-048.mspx



系统安全技巧

随着大众的数字生活领域变得越来越复杂，恶意安全黑客和恶意软件带来的威胁也处于增长的情况;为了避免导致出现安全事故的情况，强密码的使用就变得越来有必要性了;而对于大部分普通人来说，它的内容非常难于记忆，所以，将其写在即时贴或者保存在文本文件里的情况也变得越来越普遍。因此，使用密码管理器已经成为解决这一问题的唯一方法。优秀的密码管理器可以将记忆数百个强密码的问题转换成为使用简单的独立密码就可以保存所有强密码的情况，并且系统的安全性还不会受到影响。

在之前的文章中，作者介绍了如何使用 pwsafe 作为快捷键来驱动 x 工具，从而大大地提高了采用 X Window 模式的类 Unix 桌面系统上通用密码管理器的性能。即便没有将 pwsafe 转换为快捷键驱动工具这样的解决方案，它本身也是一个非常不错的密码管理工具，和密码卫士以及我的密码安全一样优秀。

这三种密码管理器都采用了同行评议、深度测试和针对密码存储的强加密模式，并且由于它们都属于开放源代码的工具，所以，全部的设计内容都属于可核查的。实际上，我的密码安全采用的是基于伯克利软件分发许可模式下的自由拷贝授权条款。由于在设计时就选择兼容被称作密码安全的密码管理器，因而都采用了相同的密码数据库格式，这让它们三者之间可以互相兼容。

密码安全是由布鲁斯 •施奈尔与 Counterpane 实验室为微软 Windows 用户开发的密码管理器，它已经发布，采用的是艺术授权模式。使用者可以登录官方网站选择内容为“点击这里获取最新版本”的链接，选择直接下载该工具。根据网站的说明：

密码安全容许使用者对以前的密码进行管理，并且可以方便快速地生成、保存、管理、搜索和应用复杂的新

密码;此外，还可以针对密码部署控制策略。一旦完成存储，只要点击几下就选择使用用户名和密码。

对于大多数用户来说，由于不存在选择非默认配置选项的必要性，所以软件的整个安装过程非常简单。在安装时，用户最有可能修改的项目就是“安装类型”;某些情况下，有些用户可能希望选择“绿色”选项，这样就可以利用单独的优盘来保存密码数据库以方便携带，并且不会在 Windows 注册表中写入信息。不过，对于大多数用户来说，选择“常规”选项就可以了。

在启动密码安全后，它提供了一个叫做打开密码数据库的文本字段标签，可以用于访问已保存的密码。因此，在第一次启动的时间，使用者就需要选择创建一个密码数据库。为了以后的顺利工作，请点击新建数据库按钮。

接下来，使用者就会看到要求输入新密码数据库名称的对话框。在输入了自己想好的名称或者选择接受默认名称，并点击保存按钮后，组合设置对话框就将会出现。尽管“安全组合”这一名称看上去很有深度，但实际上这里要求的全部操作仅仅就是设置一个主密码，用于对于访问即将保存在密码安全加密数据库中的密码这一操作进行验证。在这里，需要重复输入两次主密码，一次是在安全组合部分，一次是在验证部分，然后点击确认按钮将其设定为密码数据库的主密码。如果设定的密码过于简单，软件就会弹出一个警告窗口，询问用户是否确定继续使用该密码，还是重新选择更强大的密码。

在设定完数据库密码后，就可以打开密码安全的主界面了，顶端排列了一系列按钮，下面的空白区域表明密码数据库中目前还没有保存数据。只要密码安全的窗口处于活动状态，使用者将鼠标放在没有变灰的按钮上就会出现一条提示，对该操作的基本功能进行说明。它看起来就象一张表格，位于右下角包含加号的绿色圆形按钮就是用来添加新条目的;点击添加，就可以打开数据输入窗口，将新密码加入到数据库中。

在使用者将密码输入进数据库之前，应该先选择设置密码策略。为了完成这一操作，就需要点击数据输入窗口中的密码策略栏。由于默认的随机密码生成规则比较简单，也不能产生最强大的密码。而使用密码管理器的全部意义就在于节省用户管理难于记忆密码的时间，所以，选择尽可能多的字符类型来创建密码系列看起来就是显而易见的选择，并且对于保障密码的安全性来说，密码安全默认的八字符字母数字密码策略是远远不足够的。因此，为了消除这一缺陷，应该进行如下所示的三项简单处理：

- 选择使用以下策略项：点击打开设置，将密码长度设置参数提高。
- 最少也应该将密码长度设置增加到 20。
- 选择使用符号复选框。

回到常规选项栏，现在就可以利用刚建立好的新策略生成需要的密码了。

在密码分类方面，密码安全采用了简单的分级模式，容许用户按照“群组”进行分类。举例来说，如果用户

设置的是一个电子邮件账户的输入密码，为了将新密码加入到群组中，就应该将电子邮件的名称输入到群组部分。标题部分容许用户标明密码的使用领域，举例来说，如果该项目保存的是 GMail 密码，就可以输入“GMail”。用户名和密码部分将保存在数据库条目中作为验证凭据。网络地址和电子邮件部分将会保存在密码安全的帮助文档中，但在软件工作时不会使用到;备注部分的作用正如其名称所表示的，保存与特定密码有关备注信息的位置。

在创建新密码时间，运用在上面建立的强密码策略来利用生成按钮建立是一个不错的主意。但不幸的是，在当今的一些认证系统中，错误的密码策略会妨碍用户使用最强大的密码;美国运通在最近几年使用的密码策略就是一个反面的典型，它限制了我们使用随机生成的强密码的能力。在出现这种情况时，依然选择使用随机生成的复杂密码，只是利用基本选项栏下方的显示按钮来进行调整，对密码进行手动编辑处理，移除被限制性密码策略所禁止的字符，将密码调整为符合要求的情况，通常都是一个好主意。但更好的主意就是，不再使用强制使用弱密码的应用程序、网站、服务和其它项目。

不幸的是，密码安全不支持在创建数据库里第一项密码条目的时间，将自定义密码策略保存下来。要想更改密码策略，必须首先在数据库中保存一条密码。一旦完成这项操作，密码输入项就会以高亮显示，这时间，选择点击编辑数据按钮，一个类似铅笔状的图形标识就会出现。此时，用户就可以打开密码策略选项，应用按钮就会出现在窗口底部。在对密码策略进行调整后，用户就可以利用应用和确定按钮对其进行保存操作。现在，当选择利用基本选项栏中的生成按钮建立新的随机密码时，就会默认应用新策略。

在密码安全的默认设置中，会将图标添加在微软 Windows 7 系统托盘的“隐藏图标”中;这样的话，任何时间只要双击该图标就可以启动软件。如果用户利用密码安全建立了多个密码数据库，并且同时打开几个的话，在系统托盘处将会出现多个密码安全的图标，每个都对应一个打开的数据库。

如果密码数据库中的密码数量不多的话，查找存储的密码是非常简单的。从系统托盘中找到密码安全，选择启动它。在主窗口中找到需要的具体密码;接下来要做的，就是双击鼠标就可以将密码复制到剪贴板中;当然，也可以先单击接着选择窗口顶部的执行按钮(这两种做法的效果是一样的，都可以将密码复制到剪贴板中)。现在，用户就可以将从数据库中复制到剪贴板里的验证用密码凭证粘帖到需要使用的登录或者其它身份验证窗口中。在粘帖操作完成后，密码安全就会将剪贴板里的数据清除。

与错误的密码策略进行斗争比尽力让其它人选择强密码更重要。实际上，我们都应该从自身做起。密码安全之类的优秀密码管理器就可以帮助人们获得更好的密码策略。

来源：ZDNET 至顶网安全频道

适销性、特定用途适用性以及不受侵害的暗示保证。用户对此邮件列表的准确性和使用承担全部风险，因依赖该资料所致的任何损失，趋势科技均不负责。