安全威胁每周警讯

2011/06/11～2011/06/18

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_OBFUSCA.AA	木马	★★★	↑	该病毒通过用户访问带有该病毒的站点感染所得，会窃取用户电脑上的个人信息以及收集帐号等功能
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_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
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	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
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	Expl_ShellCodeSM	木马	★★★	↑	疑似病毒
8	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
9	HEUR_OLEXP.A	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
10	TROJ_DLOADER.UVD	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

MS11-034: Windows 内核模式驱动程序中的漏洞可能允许特权提升 (2506223)

受影响的软件:

Microsoft XP

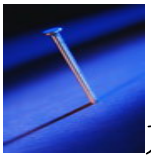
M crosoft Server 2003 Service

Microsoft Vista

Microsoft Server 2008

Windows 7

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS11-034.mspx



系统安全技巧

面对从一开始就围绕 SOC 的纷纷扰扰，作为 SOC 从业者的我也始终在寻找 SOC 的定位、运用场景、价值、效果和发展方向。站在当下，回首过去，看到的是一条 SOC 发展的曲折道路，是一条 SOC 中国化的路。眼望未来，又有很多的可能在向我们招手，选择哪种可能性，都必定不会顺畅。

在所有关于 SOC(这里指安全管理平台)的是是非非中，一个很常见的问题就是：SOC 到底是什么，能够给我解决什么问题?带来什么实际的效果?也许是业界同仁们经历了太多的失败，面对这个问题，大都显得很沮丧。

首先，我想说，正如我在探寻安全管理平台(SOC)项目的关键成功因素中提及的那样，这个问题是一个世界性的难题，是由于系统自身的技术特点，以及使用者(用户)的条件决定的。

一方面，安全管理平台的技术特点决定了这是一个复杂的系统，仅就收集异构 IT 资源的信息而言，其工作量就无法固化下来，且不论所有管理类软件的需求与功能模糊化的通病。另一方面，客户的客户条件也是一个问题，包括客户的期望、认知程度，以及客户单位的体制、流程和组织架构。

所有这一切，决定了安管平台不会像 FW、IDS 那样发展起来。

接下来，我想说，这个问题并不是不可解决的，这需要业界与客户的共同努力，需要这个市场的不断成熟。

就目前阶段而言，我认为，从系统和产品的角度来看，安管平台到底是什么?安管平台就是一个工具!一个帮助用户进行安全管理的工具!这个话至少表明：1)安管平台是手段和方式，不是安全管理的目标;2)这个工具是帮助用户而不是取代用户的，他是一个提升安全管理生产力的工具。

这就好比说安管平台是一把扫帚，而你拥有一把扫帚并不意味着你的房间就干净了，还需要你自己去打扫!扫帚可以更先进一些，成为吸尘器，但依然需要你自己去插电，去使用，否则房间不会自己干净的。

同理，安管平台就好比是一个相机，但并不意味着你有了相机就有好的照片了，还取决与你的拍摄技巧。即便他是一个傻瓜相机，那也需要你去拍!更加的，现在很多人并不喜欢傻瓜的，还偏偏要去买高级单反的，要自己去苦练和积累拍摄技巧。

所以说，有了安管平台不代表安全管理工作就做到位了，还需要使用、需要运维。使用安管平台是需要技巧的。你可以自己去学习，也可以雇人帮你用，那就叫购买服务。如果你自己要用好，可能还要建立相应的配套，包括组织、流程的配套，等等。这些也是属于服务的范畴。

如果你赞同我上述观点，我觉得接下来的问题就好办了。

从这个意义上说，我建议客户在安管平台立项的时候，可以有两种思路：一种是购买工具的思路。也就是说自己已经做了必要的各项准备工作，需要一个这样的工具来改进当前的安全管理工作。这个时候，问题的焦点就在于产品选型对比，就好比你去选择买什么样的扫帚，或者选购哪款相机。

另一种思路是把这件事当成一个建设项目来做。即不仅局限于购买工具，还包括购买工具配套的服务。很多管理类产品都有这个运作方式，例如 ERP，OA，CRM 等等，不是买了工具就 OK 的。这时候，你要认识到服务的价值，咨询师的价值、实施工程师的价值。甚至，你还可能对工具进行定制，包装，二次开发等。

总而言之，一般情况下，用户在听到安管平台后，总是会自然而然的想到他的效果，美化他的效果，而忽略了达成效果的途径，结果就是“希望越大、失望越大”。所以，我们一开始就要告诉客户，这玩意儿就是一个工具，用好了，才有可能达成效果。

所以说，对于用户而言，不仅要买对，还要用对。这要求可不低。尤其是当前很多用户还处于大量部署基础的单点安全防御设施的阶段的时候，更加不容易认识到这点。

正如我一直强调的，作为一个 SOC 售前顾问，咨询师，在给客户交流的时候，应该澄清这个问题，要帮助客户建立正确的对安管平台的认知。

来源：ZDNET 安全频道