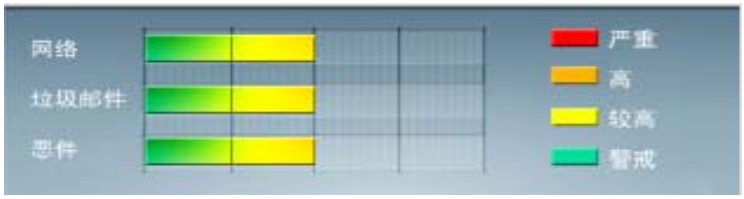
安全威胁每周警讯

2011/02/12～2011/02/19

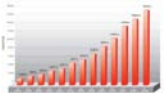
本周威胁指数



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	★★★	→	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	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
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	JS_ISTBAR.CN	脚本病毒	★★	↑	Java 脚本类病毒
8	ACM_AGENT.AVGL	脚本病毒	★★	↑	AutoCad 脚本病毒
9	WORM_AUTORUN.CLX	蠕虫	★★	↑	蠕虫病毒，通过网络共享、IRC、P2P、邮件等方式传播。感染该病毒后会在系统自启动项中加入病毒启动信息
10	TROJ_LAMEWAR.VTG	木马	★★	↑	木马病毒，该病毒不具备传播特性，是由其他恶意程序通过网络下载到终端电脑上的



本周安全趋势分析

趋势科技热门病毒综述-- PE_VIRUX.AA-O

趋势科技已经收到关于此病毒的多个独立包，包括用户反馈、内部报告，分析表明，由于其潜在的传染性和破坏性，此病毒对于用户来说具有高风险。

病毒描述：

此母体文件作为一个蠕虫病毒植入用户电脑，被趋势科技检测为 WORM_LAMIN.A，此文件已经被 PE_VIRUX 变种感染。它将代码注入到进程中，通过创建注册表键值以绕过 Windows 防火墙，同时其感染特定的文件类型，在感染过程中避免感染文件 名中包含某些特定字符串的文件。

该病毒会添加某些特定的字符串到 Windows HOST 文件中。它会连接到特定的 IRC 服务器通过 UDP 和 TCP 的 80 端口。其连接服务器使用的是 8 位随机生成的字符串作为昵称和 1 位随机生成的字符串作为用户名。一旦连接成功，其可以通过特定的渠道接收和执行命令在受影响的系统中。在写此文档时，服务器会返回一个命令到一个特定的下载文件中，特别是 TROJ_DLOAD.JKZQ，这个下载的文件被保存在一个文件夹中，然后执行。因此，被下载文件的恶意操作就会在受感染系统中出现。

该病毒执行 DNS 请求到特定网页，目前已经无法访问。此文件感染者会挂钩某些特定的 API，以便当这些 API 被调用时其代码可以被执行，进而感染文件。其第一次会通过检测脚本文件的扩展名来感染脚本文件。一旦发现目标脚本文件，其会创建一个感染标志。最后它会打开标记文件，然后在文件中检测特定的字符串，如果找到该字符串则略过该文件，否则感染此文件。

此病毒感染者在目标脚本中寻找特定字符串，一旦发现，它会通过插入恶意的 iframe 代码感染脚本文件。趋势科技将此类脚本文件检测为 HTML_IFRME.QAWA。趋势科技也可以检测被感染的.exe 和.scr 为 PE_VIRUX.J, PE_VIRUX.N-3，和 PE_VIRUX.AA。在其执行完病毒例程后会将控制权交给宿主文件的原始代码。

- 对该病毒的防护可以从以下连接下载最新版本的病毒码：7.784.60 或以上版本
  http://support.trendmicro.com.cn/Anti-Virus/Main-Pattern/

- 病毒详细信息请查询：
  http://about-threats.trendmicro.com/Malware.aspx?language=us&name=PE_VIRUX.AA-O