



全球威胁趋势

– 2007 年 8 月

根据 ESET (该公司创建了一个叫做“ThreatSense.Net”©的全球性传染报告系统)统计, Win32/Obfuscated 是八月份的顶级威胁。除了上榜的前十大威胁, 混淆威胁 (obfuscated threat) 占有所有威胁的 7.58%还要多。

代码混淆...

在八月份期间, 已被侦测到的威胁中, 接近 7.58%是混淆威胁。

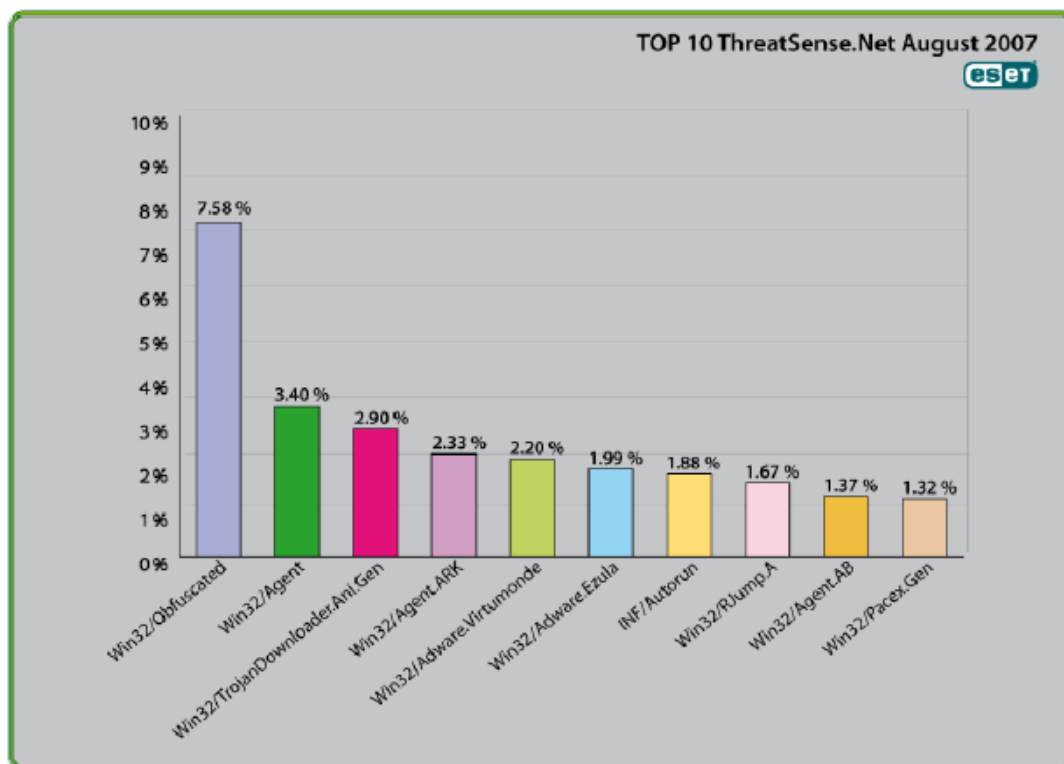
“Win32/Obfuscated” 被用作标识那些使用各种各样的代码混淆方法掩藏恶意功能, 从而逃避 ESET 公司 NOD32 和其它扫描器侦测的恶意软件。这是 ESET 公司对使用混淆技术的各种 Windows 威胁的一个统称。这些威胁包括运行时加壳 (runtime packing)、多态性 (polymorphism) 和垃圾代码注入 (junk code injection), 这些威胁通常属于同一家族, 只是有少量的改变。

特工...

在 8 月份排名第二的是 “Win32/Agent”, 我们发现该威胁在上个月期间已经达到侦测总数的 3.40 %。再一次, “特工” 的头衔被授予那些具有木马功能, 并且在被入侵的机器上作为 “特工” 的恶意软件威胁。这些文件即能连接到一台中央控制服务器接受他们的指令也能够在系统中打开一个可以被黑客用作控制计算机的后门。这些侦测基于 ESET 公司 NOD32 的普通侦测算法, 该算法能在不需要更新的情况下查出千变万化的新威胁。

Animania...

位居第三的是 “Win32/TrojanDownloader.Ani.gen”。这个威胁利用一个最近发现的 Windows 进程动态链接文件漏洞进行攻击。攻击者利用这个安全漏洞向系统安装恶意代码, 然后下载另外的恶意文件到受攻击者的系统。同样, 这是一个普通侦测, 可以侦测任何利用这个漏洞的企图。



第四名...

Win32/Agent.ARK 在八月份排名第四，占侦测总数的 2.33 % 左右。这个恶意软件连接到可能位于新加坡的命令和控制服务器。该恶意软件的目的是：保留对一个被传染的系统的控制以便将来使用；它可以在被传染的计算机上执行命令或下载另外的软件。这样的 botnet 软件能经常自我更新组件以增加新功能，这些功能可以帮助它逃避基于特征码的防病毒软件的侦测。

第五名...

八月份第五名的位置再次被 Win32/Adware.Virtumonde 占居。这是一种潜在的有害程序，它被用作向用户的个人计算机发布广告。在 ESET 公司的 NOD32 中可以选择是否侦测这种程序，但许多用户没有意识到他们的计算机上安装了这些并不希望被安装的广告服务器。

第六名...

排在 Virtumonde 之后的是 Win32/Adware.Ezula，它是一种恶意软件，以安装文件图标出现，但是，当用户双击该文件时不会向用户显示对话框。该恶意软件会在后台默默地被安装，不提供任何信息告诉用户在系统中安装了什么。判断软件是否是

恶意软件的一个重要的标准，就是看给予用户多少许诺或信息。一旦被安装在受害者系统，该软件就会从目前位于菲律宾的网站上下载和执行另外的软件组件。此外，该恶意软件保留搜索关键词的路径，然后发送到一个预设列表中的所有网站。最后，当用户浏览互联网时，该软件通常会根据受害者浏览习惯偶然地显示广告。

第七名...

在第七位，我们发现了 INF/Autorun，再次被检定成一个恶意软件威胁的变种，它使用 autorun.inf 文件装载。当存储媒介 (U 盘、光盘等) 被插入计算机时会自动地运行一些程序，autorun.inf 文件则包含这些程序的相关信息。如果 ESET NOD32 侦测到通过 autorun.inf 文件安装的病毒或修改 autorun.inf 文件的程序，则被认为是 INF/Autorun。U 盘上传播的恶意软件通常是 INF/Autorun。

后三名

在八月份名列前茅的十大威胁中，位于最后三个位置的是两个木马程序 (Win32/Rjump.A—上个月的第 2 名和 Win32/Agent.AB) 和一个邮件群发蠕虫 (Win32/Pacex.gen)。三个威胁占有所有侦测的 1.32% 到 1.67%。

使用ESET的 ThreatSense.Net覆盖全球

如今，迅速蔓延的病毒软件拥有不同的特点和能力，并且每个病毒还会有几个或更多的变种。正因为如此，经常地更新您的反病毒解决方案，前慑侦测就变得尤为重要，就像 NOD32 中的前慑侦测，每天都可以抵御最新的和未知威胁的病毒入侵。

ThreatSense.Net 可以依据分布在世界各地的数百万个客户端计算机报告病毒侦测的统计信息，它被认为是当今最为全面的病毒报告系统。

源于一个原始的想法，在 VIRUS RADAR® <http://www.virusradar.com.hk> 中变为现实，该报告系统发展为如今的 ThreatSense.Net，并在很大程度上的改进了收集到的统计信息。

这些匿名的统计信息，是从 NOD32 用户（可以通过 NOD32 软件向服务器报告的用户）中收集到的，该信息可以比较全面的反映病毒软件在现实世界中的行为和蔓延。即时的数据是通过多于一千万个系统收集的，并且已经跟踪了大于 10,000 个不同的威胁和病毒家族。

**Version 2 Limited****总公司 - 香港科学园**

香港新界沙田香港科学园科技大道西八号西翼三楼二零七室

销售与技术支持 (中国、新加坡):

电话: (852)-2893-8860

销售电子信箱地址: sales@nod32.com.hk

Copyright © 1997 – 2006 ESET. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET. All other names and brands are trademarks of their respective companies.