

## IDC供应商聚焦

# 超越基于病毒特征的防毒方式：新的病毒威胁传染媒介需要前慑的防毒保护

2007年7月

根据世界防病毒“2006.2010预测更新”和“2005 Brian E. Burke供应商分析”改写，IDC #204715

### ESET 主办

木马、病毒、蠕虫和其它类型恶意代码仍然是当今企业和公司所面对的最严重的威胁。随着入侵企业和公司网络的威胁数量和危害程度不断地上升，企业和公司越来越需要更具有前摄性的病毒侦测技术。有远见的公司开始意识到，他们无法依靠仅基于病毒特征的反病毒 (AV) 技术。实时行为分析反病毒技术，使用启发式算法，它正是基于病毒特征反病毒的完美补充。这次供应商聚焦调查了迅速演变的威胁环境和只基于病毒特征的反病毒在侦测未知威胁的不充分性。本文着眼于能保护企业和公司免受病毒的入侵的先进反病毒技术，并且谈论ESET在安全产品市场的这段非常重要阶段中所充当的角色。

### 新的威胁传染媒介

不论是病毒、蠕虫或间谍软件，恶意代码(也称恶意软件)的数量和狡猾性都在不断增加，让企业和公司疲于自我保护。威胁环境从一个恶作剧式的爱好演变成了以赚钱为目的的犯罪冒险，这吸引了一批老练的黑客和犯罪组织。

如今的老练黑客并不会关心怎样去破坏系统或是攻击WEB服务器。他们意识到，他们可以窃取机密的个人信息和公司的重要数据，并卖给非法推销者或那些从事犯罪和欺诈的组织，从中牟利。这种被赢利驱使的动机导致大量攻击的狡猾性、频率和严重性都在不断增加。

数字威胁的环境迅速地改变，不仅表现在恶意软件作者的动机，还包括他们攻击目标的漏洞。曾经几时，携带病毒的邮件是那些寻求破坏或扰乱商业运转的黑客们最有吸引力的武器。但是，存在一个恶意软件攻击更大的威胁传染媒介—网页。

当许多组织对传统携带病毒的邮件攻击进行适度的防护时，网页渠道成为黑客们提供了一个可以选择的目标。在多数情况下，出于金钱利益，黑客们发掘了网页浏览器和其它应用程序中的多个漏洞，来进行各种的类型的恶意攻击。

基于网页的威胁可以自动地繁殖，这种自动繁殖是通过“drive-by”下载(一个被传染的网页，可以侵入网站访客们的计算机，甚至访客没有点击网页上的任何东西)或通过从互联网邮箱下载电子邮件和其它相似的技术。不断增长的互联网威胁能够有效地应用这些技术，它们使间谍软件、病毒、蠕虫、键盘钩子和其它恶意软件蜂拥出现。

基于网页的攻击，通常使用老练而狡猾的技术。它是一种目的性很强的攻击，用于窃取金钱、身份或机密信息。例如键盘钩子，如果在个人计算机运行该程序，它能捕获并传送用户的每个击键信息，从而允许窃贼获得密码和其它与身份相关的信息。Rootkits和恶意软件一起被安装，用于隐藏恶意代码，防止被用户、管理员和安全软件发现。

基于网页的攻击的复杂性也在不断增加。例如，一种基于网页威胁的技术，是使用加密技术来隐藏恶意代码，传统的URL过滤和防病毒解决方案无法对它进行解码。基于网页攻击的应用是

最近蜂拥出现的间谍软件的驱动之一，发布间谍软件网站的数量剧增足以证明其危害程度。

根据IDC需求调查，病毒和其它恶意软件仍然是所有的大小企业的首要威胁(参见图1);间谍软件是第二威胁。利用没有打补丁或无特征码漏洞的零天攻击，使得引人注目的并在全世界范围内针对企业的目的性攻击成为可能，该攻击虽然流行却很隐蔽。至今，由于和病毒、蠕虫和木马进行斗争而造成的资源损耗，是非常难以容忍的，这些资源损耗包括人力和资金。

**图1**

企业网络安全的主要威胁：2005年\2006年统计结果

木马、病毒、蠕虫和其它恶意代码（不考虑来源）  
间谍软件  
垃圾邮件  
雇员的过失（无意的）  
应用软件漏洞  
雇员或商业竞争者的数据盗取  
黑客  
无线局域网  
内部人员的恶意破坏  
部署新技术（无线局域网，远程访问）  
商业合作伙伴的过失（无意的）  
移动设备（PDA，智能手机）  
偶然的入侵者  
网络恐怖主义  
无力满足政府的调整命令  
竞争者的间谍

(被调查者中的百分比)

2006 (n = 430)

2005 (n = 435)

注：

- 值代表那些回答4或5的被调查者，可选范围为1至5，其中“5”代表重大的威胁。
  - 允许多种回答。
  - “竞争者”、“网络恐怖分子”、“雇员”或“伙伴”的定义中不包括“偶然的入侵者”。
- 来源: 2005年、2006年IDC 企业安全调查。

在推论调查中, 35% 被调查者报告了针对他们企业的成功的攻击, 24% 报告了10 次或更少成功的攻击(参见图2) 。另外, 来自超大企业的被调查者中, 27% 阐明, 针对他们企业的成功的攻击有10 次或更少。

**图 2**

不同规模公司的成功攻击数

小型 中型 大型 超大型

(被调查者中的百分比)

无

1.10

11.50

51.100  
101.1,000  
More than 1,000  
大于 1,000  
未知  
n = 430

注：小型公司员工数量 1—99人，中型公司员工数量 100—999人，大型公司员工数量 1,000—9,999人，超大型公司员工数量 多于1,0000人。  
来源: IDC ， 2007 年

从图2可以清楚看到，在过去12个月中至少对企业做出一次成功的攻击的流行威胁。很明显，即使有1,000个尝试被阻止，也不能弥补企业被攻击一次所造成的商业损失。

对网页威胁剧增的关注，使人们对解决方案的要求在不断提高，如网页过滤、网页入侵预防、网页防病毒和网页防间谍软件。但是，网页威胁不断增长的狡猾性强调了用实时、前摄性安全防护来完善传统的安全解决方案，传统的安全解决方案基于为每个已知威胁开发一个特征码。当今，许多恶意软件攻击使用加密技术、多态性(每个病毒样本看似不同)快速繁殖技术，恶意软件捆绑技术和其它方法来逃避传统的解决方案，在特征码准备好之前传染数量庞大的个人计算机。

所以，有效地保护计算机免受涌现的基于网页的威胁，企业需要能够补全现有反应式安全解决方案的防病毒技术。现有的反应式安全解决方案在防护已知威胁中有着重要的地位。基于特征码的技术仍然很重要，因为已经有特征码的一些威胁仍然在肆虐或是在保持休眠状态，等待预定或偶然事件的触发重新发动攻击。

## 基于特征的防恶意软件与启发式(Heuristic-Based)防恶意软件的对比

正如前文所述，更具有前摄性的病毒侦测技术的需求日益增加的原因，归结于基于网页的威胁逃脱了传统的、基于特征的病毒保护。这个问题主要因为病毒是“未知的”或企业没有更新病毒特征码。

不同于依靠用户传播被传染文件的传统病毒，这些新的“捆绑”威胁可以自动传播。在家庭和企业中，被病毒感染的计算机总在扫描网页和局域网中其它脆弱的计算机，将病毒传染它们。这意味它们的传播完全不需要用户的介入与操作。当今的恶意软件之所以能够迅速的蔓延，就是因为它能经常在防病毒厂商能发布相应的特征码之前，它们能够避开桌面电脑和服务器的传统防毒软件进行传播。

被捆绑的威胁通常可以通过点解决方案安全系统 (point-solution security system)，因此IDC相信，这种情形将会强烈地推动“分层安全 (layered security)”方式，该方式能更好的与捆绑型威胁交战。前摄、基于行为分析并使用启发式方法，越来越成为分层安全架构的重要需求。

同样，网站依靠各种各样的嵌入程序如Java和ActiveX控件，来打造他们独特的外观和感觉。当站点被用户浏览时，这些程序能够自动地运行并感染浏览该网页的用户。许多公司阻止Java程序通过他们的防火墙，但不幸的是，这种做法可能限制重要的合法Java程序。

实时行为分析技术使用先进的启发式识别，当被下载的代码进入网络时，对其分析。所有代码的特征被实时审查，确定是否会构成安全威胁。任何入侵公司安全策略的代码都会在网关被拦截，同时，在屏幕上向终端用户发出警告。安全策略威胁包括：企图删除文件、打开网络连接和修改注册表。

实时行为分析使公司允许信任的网页应用程序或服务进入公司网络，并扫描所有其它网页内容是否包含恶意行为。这种方法允许信任内容自由进入网络，而所有其它“未知”内容在能够运行之前对其进行检查。

## 关于ESET

ESET，一个17岁的公司，其美国总部设在圣迭戈、加利福尼亚，为全球企业和消费者提供安全防护软件。公司的旗舰产品是NOD32防病毒软件系统，该产品可提供实时安全保护，免受已知和未知的病毒、间谍软件、rootkits和其它恶意软件侵害。

NOD32提供快速的、先进的安全保护，却占用很少的系统资源和最小的系统影响。比其他防病毒产品赢得了更多Virus Bulletin 100奖项。NOD32被认为不仅仅是防病毒产品，它的设计是保护用户免受病毒、间谍软件、广告软件、木马、蠕虫、rootkits和网络钓鱼的攻击，是一个统一的防威胁系统。

NOD32使用以下的模块来提供对多传染媒介的威胁防护：

### 文件实时监控 (AMON)

常驻内存的扫描器，它会自动的扫描计算机将要访问的文件。

### NOD32

手动扫描器（按用户要求进行扫描），可以选择要扫描的文件和磁盘分区。也可以排程一个空闲时间自动扫描。

### 网络监控器 (IMON)

常驻于内存，在Winsock的等级来防止恶意代码进入电脑，它会扫描网页(HTTP)、以及POP3电子邮件协议。

### 电子邮件监控器 (EMON)

一个辅助的模块，通过MAPI接口与电子邮件客户端软件协同工作，比如 Microsoft Outlook Microsoft Exchange。

### MS Office文件监控器 (DMON)

通过监视微软提供的API，在打开微软Office文件时首先检测文件是否被感染(包括在IE上打开办公文件)。

NOD32的核心就是ESET公司的前辈ThreatSense技术，约93%的零天防护都可以在其释放之前就被NOD 32主动式的ThreatSense技术拦截。其最优化的引擎可以进行高级侦测和快速扫描，同时拥有最小的性能影响。

NOD32主要使用汇编语言编写，因为其在所有防病毒软件中拥有最快的速度表现，NOD32 获得了许多奖项。根据Virus Bulletin，NOD32能够比其竞争产品快34倍。

NOD32节约内存和硬盘上的资源，让它们为更重要的应用服务，本软件只有11M，平均占用23M的内存(根据检测状态会有变化)。Threatsense 每次更新（包括启发式逻辑和病毒特征码）通常都只有20KB到50KB左右。

NOD32 还是灵活的并且可以配置，还拥有集中化管理和报表功能。对于大型企业，我们提供了强大的远程分布式的网络管理，管理员可以集中部署、安装、监测和管理成千上万的NOD32工作站和服务器。其宽广的产品线可以提供对Windows、Linux、Novell和MS DOS等不同平台机器的保护。

## 机遇与挑战

凭着NOD32及其实时行为分析能力，ESET 做了一项大胆举措，接受前摄安全防护的复杂挑战。绝大多数机构组织IDC同意，需要更具有前摄性的安全解决方案才能与新威胁可能传播的速度进行抗衡。这些公司无法承受特征码发布前的等待。

IDC相信ESET面临的巨大挑战是：病毒防护是广泛部署的安全技术，横跨所有规模的机构组织，只有很少的“绿地”可以让ESET进入。在桌面电脑领域，部署NOD32需要替换现有的防病毒解决方案—让许多机构组织头疼的任务。

ESET 必须继续教育那些组织机构，如今对企业的保护，远比传统基于特征码的防病毒解决方案可以处理的年代更为复杂。随着威胁环境不断的增长以及互联网中急速的“零日（zero-day）”传染发生，企业要不停的努力才能应对无穷无尽的网络攻击。

IDC认为，行为分析工具是一个优秀方式，能够使企业论及前摄安全策略的某些方面。但是，我们强烈推荐，行为分析只是作为一种整体安全分析的一部分被实施。前摄方法必须被认为是传统反应式安全方案的补充。

## 结论

IDC 相信，病毒防护市场将继续它从产品到套装的演变，最后将转变成更加全面的安全解决方案。我们进一步相信，病毒防护越来越作为端点安全、通讯安全、网页安全和网络安全解决方案的被销售。例如，很显然，防病毒和防间谍软件已经聚合成一种单一的端点解决方案。

IDC 需求调查结果清楚地显示，**组织机构想要少量客户端代理**。另外，为了统一的管理、策略和报告，组织机构希望能够使用单一控制台来管理端点安全。IDC 认为，实时行为分析技术（如先进的启发法）与传统基于特征码的防病毒技术的综合，将更准确的侦测已知和未知的威胁。

IDC 预测全世界防病毒市场将会从2005 年的43亿增长到2010 年的73亿，代表11%的复合年增长率。在某种程度上，ESET 将会应对本文所描述的挑战，它加强防病毒领域，通过增强行为保护以及增加防火墙和反垃圾邮件(antispam)保护来创造一个统一的威胁防护安全套装。从而，公司有一个保持成功的重大机会。

### 关于本出版物

本出版物由IDC Go-to-Market Services发行。文中提及的观点、分析和研究结果摘自IDC 执行和独立出版的更加详细的研究和分析，除非署名具体供应商赞助者。IDC Go-to-Market Services 使得IDC 内容以多种版式被众多公司发行。许可发布IDC 内容并不代表获许可人的观点和认可。

### 版权与制约

任何将IDC 信息或参考用作做广告、新闻发布或促销产品，需要预先从IDC获得书面同意。为了请求被允许，请与GMS信息线联系：508-988-7610 或gms@idc.com。

翻译或者地方化此文件需要从IDC获得一个另外的执照。

更多关于IDC的信息，请查看[www.idc.com/gms](http://www.idc.com/gms)。更多关于IDC GMS的信息，请查看[www.idc.com/gms](http://www.idc.com/gms)。全球性总部: 5 Speen 街道 Framingham, MA 01701 美国P.508.872.8200 F.508.935.4015 [www.idc.com](http://www.idc.com)