

## 上网行为管理 技术分析系列

### ——黑客入侵攻击方式的四种最新趋势

**相关主题:** 上网行为管理,PatrolFlow,信息安全网关,带宽管理,流量控制,P2P 控制,BT 下载,邮件监控,IM 控制,游戏监管,聊天监控,内容审计,多链路负载均衡,Web 推送,防火墙,防毒墙

#### 正文内容:

黑客入侵攻击方式的四种最新趋势

从 1988 年开始,位于美国卡内基梅隆大学的 CERT CC (计算机应急响应小组协调中心) 就开始调查入侵者的活动。CERT CC 给出一些关于最新入侵者攻击方式的趋势。

#### 趋势一: 攻击过程的自动化与攻击工具的快速更新

攻击工具的自动化程度继续不断增强。自动化攻击涉及到的四个阶段都发生了变化。

1. 扫描潜在的受害者。从 1997 年起开始出现大量的扫描活动。目前,新的扫描工具利用更先进的扫描技术,变得更加有威力,并且提高了速度。

2. 入侵具有漏洞的系统。以前,对具有漏洞的系统的攻击是发生在大范围的扫描之后的。现在,攻击工具已经将对漏洞的入侵设计成为扫描活动的一部分,这样大大加快了入侵的速度。

3. 攻击扩散。2000 年之前,攻击工具需要一个人来发起其余的攻击过程。现在,攻击工具能够自动发起新的攻击过程。例如红色代码和 Nimda 病毒这些工具就在 18 个小时之内传遍了全球。

4. 攻击工具的协同管理。自从 1999 年起,随着分布式攻击工具的产生,攻击者能够对大量分布在 Internet 之上的攻击工具发起攻击。现在,攻击者能够更加有效地发起一个分布式拒绝服务攻击。协同功能利用了大量大众化的协议如 IRC(Internet Relay Chat)、IR(Instant Message) 等的功能。

#### 趋势二: 攻击工具的不断复杂化

攻击工具的编写者采用了比以前更加先进的技术。攻击工具的特征码越来越难以通过分析来发现，并且越来越难以通过基于特征码的检测系统发现，例如防病毒软件和入侵检测系统。当今攻击工具的三个重要特点是反检测功能，动态行为特点以及攻击工具的模块化。

1. 反检测。攻击者采用了能够隐藏攻击工具的技术。这使得安全专家想要通过各种分析方法来判断新的攻击的过程变得更加困难和耗时。

2. 动态行为。以前的攻击工具按照预定的单一步骤发起进攻。现在的自动攻击工具能够按照不同的方法更改它们的特征，如随机选择、预定的决策路径或者通过入侵者直接的控制。

3. 攻击工具的模块化。和以前攻击工具仅仅实现一种攻击相比，新的攻击工具能够通过升级或者对部分模块的替换完成快速更改。而且，攻击工具能够在越来越多的平台上运行。例如，许多攻击工具采用了标准的协议如 IRC 和 HTTP 进行数据和命令的传输，这样，想要从正常的网络流量中分析出攻击特征就更加困难了。

#### 趋势三：漏洞发现得更快

每一年报告给 CERT/CC 的漏洞数量都成倍增长。CERT/CC 公布的漏洞数据 2000 年为 1090 个，2001 年为 2437 个，2002 年已经增加至 4129 个，就是说每天都有十几个新的漏洞被发现。可以想象，对于管理员来说想要跟上补丁的步伐是很困难的。而且，入侵者往往能够在软件厂商修补这些漏洞之前首先发现这些漏洞。随着发现漏洞的工具的自动化趋势，留给用户打补丁的时间越来越短。尤其是缓冲区溢出类型的漏洞，其危害性非常大而又无处不在，是计算机安全的最大的威胁。在 CERT 和其它国际性网络安全机构的调查中，这种类型的漏洞是对服务器造成后果最严重的。

#### 趋势四：渗透防火墙

我们常常依赖防火墙提供一个安全的主要边界保护。但是情况是：

\* 已经存在一些绕过典型防火墙配置的技术，如 IPP (the Internet Printing Protocol) 和 WebDAV (Web-based Distributed Authoring and Versioning)

\* 一些标榜是“防火墙适用”的协议实际上设计为能够绕过典型防火墙的配置。

特定特征的“移动代码”（如 ActiveX 控件，Java 和 JavaScript）使得保护存在漏洞的系统以及发现恶意的软件更加困难。

另外，随着 Internet 网络上计算机的不断增长，所有计算机之间存在很强的依存性。一旦某些计算机遭到了入侵，它就有可能成为入侵者的栖息地和跳板，作为进一步攻击的工具。对于网络基础架构如 DNS 系统、路由器的攻击也越来越成为严重的安全威胁。

#### 采用主动防御措施应对新一代网络攻击

“红色代码”蠕虫病毒在因特网上传播的最初九小时内就感染了超过 250,000 个计算机系统。该感染导致的代价以每天 2 亿美元飞速增长，最终损失高达 26 亿美元。“红色代码”，“红色代码 II”，及“尼姆达”、“求职信”快速传播的威胁显示出现有的网络防御的严重的局限性。市场上大多数的入侵检测系统是简单的，对网络中新出现的、未知的、通常称做“瞬时攻击：Zero-day Attack”的威胁没有足够防御手段。

#### 黑客的“机会之窗”

目前大多数的入侵检测系统是有局限性的，因为它们使用特征码去进行辨别是否存在攻击行为。这些系统采用这种方式对特定的攻击模式进行监视。它们基于贮存在其数据库里的识别信息：类似于防病毒软件检查已知病毒的方式。这意味着这些系统只能检测他们已经编入识别程序的特定的攻击。因为“瞬时攻击”是新出现的，尚未被广泛认识，所以在新的特征码被开发出来，并且进行安装和配置等这些过程之前，它们就能绕过这些安全系统。实际上，仅仅需要对已知的攻击方式进行稍微的修改，这些系统就不会认识这些攻击方式了，从而给入侵者提供了避开基于特征码的防御系统的手段。

从新的攻击的发动到开发新的特征码的这段时间，是一个危险的“机会之窗”，许多的网络会被攻破。这时候许多快速的入侵工具会被设计开发出来，网络很容易受到攻击。下图举例说明了为什么大多数的安全产品在该时期内实际上是无效的。CERT 组织研制的这个图表说明了一个网络攻击的典型的生命周期。该曲线的波峰就在攻击的首次袭击之后，这是大多数安全产品最终开始提供保护的时候。然而“瞬时攻击”是那些最老练的黑客在最早期阶段重点展开的。

同时，现在那些快速进行的攻击利用了广泛使用的计算机软件中的安全漏洞来造成分布更广的破坏。仅仅使用几行代码，他们就能编写一个蠕虫渗透到计算机网络中，通过共享账号克隆自己，然后开始攻击你的同伴和用户的网络。使用这种方式，在厂商开发出特征码并将其分发到用户的这段时间内，“尼姆达蠕虫”仅仅在美国就传播到了超过 100,000 的网络站点。这些分发机制使“瞬间攻击”像 SirCam 和 Love Bug 两种病毒分别席卷了 230 万和 4000 万的计

算机，而不需要多少人为干预。其中有些攻击甚至还通过安装一个后门来为以后的破坏建立基础，该后门允许对手、黑客和其他未获授权的用户访问一个组织重要的数据和网络资源。

更多信息请登录 <http://www.byzoro.com>