

## 战胜将来的僵尸网络（Botnet）

本文摘自 WatchGuard® LiveSecurity® 团队成员 Scott Pinzon 和 Corey Nachreiner 经过深入研究后撰写的白皮书《了解并阻止新型僵尸网络（Understanding and Blocking the New Botnets）》，二人均为信息系统安全认证专业人员（CISSP）。如希望深入了解僵尸网络的特点以及当前僵尸网络如何变异和运行，可登录 [www.watchguard.com/whitepapers.asp](http://www.watchguard.com/whitepapers.asp) 免费下载此白皮书。

僵尸网络是一种最为严重的混合威胁。其代码中携带了能想得到的几乎每一种形式的恶意软件，包括间谍软件、下载器、rootkit、垃圾邮件引擎等。为了针对不同的情况对症下药，防御者必须部署多个层次的安全措施。好消息是各种历经时间验证的应对技巧仍然对僵尸网络非常有效。以下是我们所建议的各种应对措施，可显著降低网络中感染僵尸程序（bot）的可能性。

### 1. 迅速打补丁

僵尸程序能利用多种漏洞来感染受害者。不过规模最大且得逞的僵尸程序，都是利用了已由厂商在 6 - 8 个月前打了补丁的漏洞。在某些极端案例中，我们甚至见到僵尸程序企图利用 4 年前就已打了补丁的漏洞。我们无法说明为什么在僵尸程序通讯及后端系统以日新月异的速度不断革新的同时，僵尸程序仍然能使用已知的旧漏洞。根据我们的猜测，这最有可能是因为僵尸操控者（botmaster）寻找可利用的漏洞的方式是等到厂商给某一漏洞打补丁后，再用逆向工程的方法研究该补丁，进而找出其缺陷所在。

我们预计，从更新一些的缺陷中寻找漏洞将是僵尸操控者接下来要着手改进的领域之一。不过就目前而言，这对普通的网络管理员是个好消息。如果在您网络上所运行软件的厂商发布修复程序的同时立即打补丁，那您就可比僵尸操控者动作更快并抵御他们的入侵。

### 2. 阻止 JavaScript

当僵尸程序利用基于 web 的漏洞攻击受害者计算机时，一定会执行 JavaScript 脚本。将浏览器设置为在执行 JavaScript 脚本前进行提示，可使大量的僵尸程序感染途径失效。我们强烈建议用户将 Firefox 作为自己的首选浏览器，同时使用 [NoScript 插件](#) 来提示试图执行的脚本。

### 3. 监控某些端口

本建议分为 2 个部分。

1) 尽管最新的僵尸程序能在每名管理员都必须打开的端口上通讯，但是大多数的僵尸程序仍然使用 IRC（端口 6667）和其它高奇数端口（如 31337 和 54321）来进行通讯。所有 1024 以上的端口都应设置为禁止流入和流出，除非您所在组织要使用定制的应用或有打开某一指定端口的特殊需要。在此情况下，可小心地打开所需端口并对其实施相应的政策，如“仅在工作时间打开”或“除来自以下受信 IP 地址列表的流量外，拒绝所有流量”。这一简单措施可防止各种普通且技术更新较慢的僵尸程序与其命令和控制中心（Command and Control Center, C&C）联系并获取指令和更新，本质上相当于已立即杀死了此类僵尸程序。

2) 僵尸网络流量在如 80 或 7 号端口等所需端口上传输时，通常会因在本该没有流量时出现流量而暴露自身。通常，僵尸操控者会在凌晨 1:00 至 5:00 这段时间段内更新其所操控的僵尸计算机（zombie），因为他们估计这时没人会查看计算机。所以应养成在早晨检查服务器日志的习惯。如果发现在本应没人浏览 web 时有 web 浏览活动，就应对此进行调查。

使用 WatchGuard Firebox® 设备的管理员会非常高兴地发现，Firebox 的代理（proxy）可阻止企图在标准端口上传输的非标准流量。例如，垃圾邮件型僵尸网络 Mega-D 将在 HTTP 80 端口上传输非标准的 homebrew 流量。Firebox 的 HTTP 代理在默认情况下能立即发现并阻止此流量。

#### 4. 加强用户培训

有些僵尸程序将在因特网上实施大规模扫描，寻找有漏洞的机器并将其感染。这种做法实际上越来越少见。如今更常见的是，僵尸程序采用“社会工程学”方法进入网络，即诱使受害者点击某一链接或打开某一文件。这些僵尸程序和某些传说中的吸血鬼一样，都受到同样的限制：除非您邀请它们进入，否则它们无法跨入门内。

这种“引诱”式的做法逐渐限制了其自身进行深入攻击。攻击者过去还曾经将恶意可执行代码当作电子邮件的附件对外发送。这种做法也逐渐减少了。目前大多数此类活动都是基于 web 的。恶意电子邮件在两年前会包含附件，如今则包含指向恶意网站的链接。某些原本无害的网站在被 Mpack 或其它隐秘的恶意软件感染后，会感染那些因不慎点击链接而来到此网站的访问者。

这便可以据此向用户简明扼要地解释，为什么绝不能邀请“吸血鬼”进入。告诉他们不要打开主动提供和不期而至的附件；告诉他们为什么不应点击电子邮件中的链接以及为什么必须慎重考虑是否点击任何不常见的链接。如果您需要帮助，请登录 <http://video.google.com/videoplay?docid=-4094518401580008932> 查看我们专为非技术人员准备的视频，其中演示了推动式（drive-by）下载的工作原理。那些始终采用我们以上所列出的各种控制措施的网络，在持续数年的运行中都未感染僵尸程序。

#### 5. 保持警惕

这一建议似乎不值一提，和说“尽量不要被感染”差不多。不过我们总是能碰到这样一些 IT 管理员，他们花费了大量的时间四处灭火并维持着人手不足的服务台，以至于他们从来都没查看过系统日志。他们从不监控带宽的使用情况。他们也无法说出网络中谁正在连接什么东西。他们甚至将设备连接到了自己都不知道具体情况的网络之中。

如果您符合以上描述，我们就只能说您这是自寻烦恼。在您阅读本文时，或许您的网络中就已经有了僵尸程序。如果您是一名很少检查日志的管理员，现在就必须开始查看日志了。在了解到自己的网络怎样才是“正常”情况后，每天只需 30 分钟即可完成一次抽样检查。

如果您符合以上描述，也有可能不是因为您懒惰——而是因为您受限于人力及资源不足。向老板解释此威胁，看看他是否支持您每天早晨抽出半个小时来检查网络状态。这段时间不应被会面请求、电话会议等各种常见事宜打断。与网络泄密的代价相比，这种保险措施的花销要低很多。

---

我们相信，最近僵尸程序的空前突破只是即将到来的技术创新的前兆。因为在我们对因特网安全的多年研究中，似乎每个月都会新发现研究人员无法完全解释的漏洞。

结果是僵尸网络变成了一种混合威胁，但是它们还不是最终的混合威胁。目前僵尸操控者可通过添加组件的方式随意补充传统的僵尸网络架构，增强其自动化、管理及躲避能力。综合采用这些技术后，其将非常难于处理且毁坏力惊人。任何观察者都能准确地预测到这种趋势不仅将继续，还将会滋长。

那坏人赢了吗？显然没有，毕竟我们仍然在使用网上银行，也仍然在进行网上购物。不过鉴于僵尸程序活动日益猖獗，我们必须采取措施抑制僵尸程序活动并揭露其操控者所采用的技术。有一种简单的方法能削弱僵尸操控者的力量，那就是设法使僵尸程序代码难以感染受害者。WatchGuard 安全设备采用了多层次的安全措施，可智能化地适用于多种协议，此外还采用了功能强大的代理技术来过滤流入和流出的流量，可确保网络的安全。

如需了解更多有关 WatchGuard 安全解决方案及其对僵尸网络和其它网络威胁的保护措施等相关信息，请访问 [www.watchguard.com](http://www.watchguard.com) 或与经销商联系。