

注意到“informationweek”网站在10月10日报道：“荷兰警方日前宣布捣毁了一个巨型计算机僵尸网络（botnet）。目前，警方已经逮捕了3名涉嫌制造该僵尸网



作者近影

络的荷兰男子。荷兰警方称，被逮捕的3名嫌犯利用Toxbot木马程序感染用户的计算机，然后在染毒计算机上安装广告插件和间谍软件。”CNCERT/CC与荷兰的应急小组联系后确认，其提供的属于中国的29万个IP正是报道中所提到的僵尸网络的成员，此僵尸网络的规模非常之大，受控计算机遍布全球，数目达到120万台左右。

由于此事件涉及中国主机的数目多，并可能产生严重危害，CNCERT/CC立刻启动了处置流程，采取了样本搜集、代码分析、启动863-917平台监测、确认清除办法、影响用户端帮助清除Bot程序等多项应对措施。CNCERT/CC自己的监测结果表

明，该僵尸网络在国内的规模已经大幅度减少，平均每日仅能发现三万个左右活动的客户端IP，僵尸网络中有窃取用户敏感信息的活动发生。但总体上，该僵尸网络已基本不对我国的网络安全造成严重威胁。

CNCERT/CC的监测表明，僵尸网络的确在我国互联网网上有相当的规模，成为了互联网上不可忽视的安全隐患和威胁，这种状况值得我们高度重视。

### 对僵尸网络的处置经验

在对僵尸网络近一年的监测和处置中，CNCERT/CC认为国内目前需要提高对僵尸网络危害的认识，提高对僵尸网络的处置力度。

对CNCERT/CC而言，应继续大力推动和国际国内应急组织间的合作。由于互联网的无国界性，国际应急组织间的合作对事件的完整处理无疑具有重要作用。上面提到的Toxbot事件就是从荷兰应急组织获知的，这再一次说明国际应急组织间的合作是我们发现事件的一个重要来源。国内的有些应急组织，也具备发现僵尸网络的能力，应继续大力推动和国际国内应急组织间就僵尸网络的发现和交换共享的合作。对运营商而言，应在僵尸

网络类事件的处理中扮演更重要角色。一方面，在僵尸网络控制服务器的处理方面，需要现场分析控制服务器和过滤用户对僵尸网络控制服务器的访问，这对发现黑客踪迹以及保护用户不被黑客控制，从而彻底捣毁僵尸网络具有重要作用，但这样的工作必须要得到运营商的积极配合和支持；另一方面，在客户端bot程序的清除方面，运营商可以在其用户中宣传事件危害和清除办法，并且可以及时联系告知其重要用户，从而帮助彻底清除僵尸网络。

最后，应推动各相关部门以及社会各方力量协作处置僵尸网络。对僵尸网络事件的彻底处置，应推动应急小组、运营商、反病毒厂商、其他网络安全机构，以及用户的安全管理部门等社会各方力量进行积极的合作处理，一方面共同帮助用户清除客户端Bot程序，另一方面可以在各个层次过滤对僵尸网络控制服务器的访问。今后，CNCERT/CC仍将继续重点关注大规模僵尸网络事件，并充分利用平台积累的丰富的僵尸网络数据，对僵尸网络的活动规律进行深入研究，为今后对僵尸网络的处置工作提供更符合僵尸网络活动规律的指导。🌐



NETINFO SECURITY

特别报道

## 凤凰科技推出全新安全产品 TrustConnector II

11月29日，全球计算机核心系统软件领导厂商美国凤凰科技（Phoenix Technologies, Nasdaq: PTEC）推出新一代终端安全认证软件TrustConnector II。该产品为每台终端设备设立一个独一无二的身份，用户不可随意进行更改，即使企业外部入侵者取得有效的用户名及密码也无法登陆受保护的网络安全系统。TrustConnector II在现有的安全系统基础上增加了“专机专用”的概念，在企业网络中只有使用已被授权的终端设备才可联网，双重确保网络安全性。