网络技术:四个原因让僵尸网络难以对抗计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/585/2021_2022__E7_BD_91_E7_BB_9C_E6_8A_80_E6_c98_585087.htm 2009年下半年全国计算机三级考试时间是2009年9月19日至23日。2009年下半年全国计算机等级考试报名时间会在考前两个月开始报名！更多优质资料尽在百考试题论坛 百考试题在线题库。 僵尸网络无休止的肆虐几乎已经是司空见惯，人们只是在思考那些坏家伙是如何在不被用户察觉的情况下，轻而易举的就入侵了用户的计算机。 长期以来僵尸网络是利用计算机中的各种配置，部分是对控制机制进行伪装。随着表面看似用户友好却并不安全的应用软件继续在计算机系统中使用，特别是社交网络程序存在某些非技术漏洞，可供黑客利用的安全漏洞的数量呈增长趋势。而且根据监控僵尸网络活动的僵尸网络猎人的报告，这些黑客在建立灵活体系架构方面也变得愈发狡猾。 以下是与僵尸网络作斗争更加艰难的四个原因，以及我们应该采取的措施： 1.避开监控操作 最近大部分僵尸网络的活动都与Conficker蠕虫病毒有关。研究学者称大型僵尸网络大部分都避开了媒体的监控，这是这些坏家伙得逞的原因。 位于美国旧金山海湾地区的安全厂商FireEye Inc公司的高级安全研究专家Alex Lanstein表示，这是因为这些病毒的始作俑者就是想要制造新闻，让人知道他们的计算机被感染了。举例来说，Cimbot是一种用来建立僵尸网络的木马病毒，目前它占到世界上兜售垃圾邮件的15%。 亚特兰大的安全厂商Purewire Inc公司的首席研究专家保罗.罗伊发现了僵尸网络逃脱网络监控进行操作的几个其他案例。在他参与的Project ZeroPack项

目中，他发现自动混淆技术能允许这些坏家伙以服务器端多形态的表象去活动。对于有规律的木马变种，传统的防病毒厂商要跟上正确的AV签名就愈加的困难。Waledac僵尸网络就是利用这种方法取得的成功。 同时罗伊还表示，黑客们从集中型的命令与控制僵尸网络结构迁移到以更加对等为基础的体系架构。这是很不幸的，因为对于集中型更强的结构，至少安全研究专家还有一个大的目标可以瞄准。而P2P的方式意味着目标变的更加细化而很难被逐一消灭。 罗伊还强调说：""Conficker.C, Storm和Waledec病毒都已经从集中型体系架构转向了P2P类型的体系架构"。 2.木马病毒可以自我防护 Cryptography Research的总裁兼首席科学家Paul Kocher表示，安全专家在试图追踪和关闭僵尸网络的过程中所遭遇的问题是用来构建僵尸网络的新型蠕虫正在使用强大的密码系统来保护他们的命令和控制中心。 Kocher表示"你可能习惯去追踪僵尸网络如何获取命令，将假冒的命令传播出来，这么做变得越来越困难了"。 更加新型的僵尸网络也更擅长扼杀计算机的安全控制。 "我们还发现在构建僵尸网络的蠕虫病毒中采用了更加狡猾的方式来逃避侦测"Kocher表示"从复制到复制这些蠕虫病毒有了更加多样化的改变。这就让反病毒专家在设计签名来阻断这些病毒的过程变得更加困难"。 3.常用应用软件超出了IT的控制范围 研究专家们还发现对僵尸网络抵御能力最弱的是人们用在公司计算机上的应用软件，这些应用软件经常超出了IT的控制范围。他们使用这些应用软件到处传递各种敏感数据，包括医疗记录，财务数据等等。 安全厂商Palo Alto Networks最近发布的2009年度春季应用软件使用和风险报告分析了超过60个大型企业的企业级应用软件的使用

和流量，这些企业的类型涵盖金融服务，制造业，卫生保健，政府机构，零售和教育部门。从2008年8月到12月的评估描述了将近90万用户的行为。研究成果包括： 在494种应用软件中有超过一半(57%)的应用软件会绕过安全体系架构--会使用端到端，端口80或端口443。这些应用程序的某些代表包括微软的SharePoint, Microsoft Groove和一系列软件升级服务(Microsoft Update, Apple Update, Adobe Update)，以及Pandora和Yoics这样的最终用户应用软件。 不被企业IT认可(CGIProxy, PHProxy, Hopster)的代理服务器和远程桌面系统访问通道应用软件(LogMeIn!, RDP, PCAnywhere)也在调研中被发现，比例分别为81%和95%。调研中还发现了诸如SH, TOR, GPass, Gbridge, and SwIPe这样的加密通道应用软件。 P2P结构所占的比例为92%，BitTorrent和Gnutella是所发现的最常用的21种变种中的一份子。以浏览器为基础的文件共享中，YouSendit就占到了76%。MediaFire是22种变种中最常见的。 据报告称，总的来说企业在防火墙，入侵检测系统，代理和URL过滤产品上的支出每年超过了60亿美元。这些产品都号称能执行应用程序控制。分析显示100%的企业都设置了防火墙，87%的企业还配置了1种或多种防火墙辅助工具(代理，入侵检测系统，URL过滤)--但是仍然不能对通过网络的应用软件流量执行有效控制。 因此木马病毒的制造者能相对容易的利用应用软件，包括建立僵尸网络。 4.社交网络扩大了攻击面 Facebook, Twitter和Myspace这样的社交网络的使用率日渐增高，他们很容易被黑客利用，企业IT部门也很难对其进行监控。 举例来说，今年2月在华盛顿特区举行的ShmooCon安全大会上，研究专家Nathan Hamiel和Shawn

Moyer表示，在社交网络上用户可以轻而易举的上传和交换图片，文本，音乐和其他内容，黑客就是利用这些网站的自然属性来轻松发动攻击。 在针对这些程序的攻击中，黑客利用社交网络欺骗用户点击开放式链接，然后将木马植入用户的计算机，用户的计算机就这样成为这些黑客僵尸网络中的肉鸡。 对用户的培训仍然是关键的防御手段 亚特兰大的安全厂商Damballa, Inc.研究副总裁Gunter Ollmann表示，近年来企业IT部门在侦测制破坏性后果的不知名木马病毒方面取得了不错的效果。近两年，IT部门配置了大范围的侦测和防御技术，每个防御层都能更好的抵御某种攻击。 但Ollmann也强调说"风险越常见，保护措施效果就会越好，但是这些坏家伙也非常清楚这些防御措施的工作原理，因此他们使用的手段也更加狡猾，比如目标型社交工程攻击。使用入侵检测系统和AV代理在发现已知木马上占到很高比例"。 Ollmann和其他专家都提供了同样的建议：由于攻击者在利用社交工程伎俩上如此的成功，他们以虚假的大标题来诱骗用户带你及恶意链接--对此最好的防御方式之一就是对这些用户进行培训。专家称，调研显示有防范意识的用户每次上线时，被诱骗下载制造僵尸代码的可能性就会比较小。 特别推荐： 2009年9月全国计算机等级考试时间及科目预告 2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com