SearchSecurity.com.cn

技术手册

下一代网络攻击应对技术

- ☆ 企业应如何防范内存抓取恶意软件
- ☆ 饱受争议的SMB v2安全问题：禁用还是打补丁？
- ☆ 应对微型botnet的最佳实践
- ☆ SSL加密网络连接是怎样被截获的
- ☆ 网络战是企业的真正威胁吗？

TechTarget
TT中国

下一代网络攻击应对技术

目录

企业应如何防范内存抓取恶意软件

一种新型恶意软件正逐渐风行起来，它能从系统的随机访问存储器（RAM）中捕获数据。在 Verizon 公司最近的数据泄露报告中曝光的 RAM 抓取技术，代表了一种相对新颖的针对信用卡数据攻击方法。

然而内存抓取并不是一种全新的技术。曾在 2008 年黑客大会中使用的冷启动攻击就是 RAM 抓取技术的另一种形式。对于那些不记得这些的人，研究员们演示了如何通过突然切断计算机的电源使得计算机的内存保留一份最近的内存镜像近乎完美的拷贝，从而绕过磁盘加密。只需简单地冷却并拆下内存芯片并将其放入另一台计算机，然后查看内存芯片，攻击者瞬间就可以获得原有计算机的磁盘加密密钥。

通过注入已运行的进程来隐藏自身或者直接在机器上运行，当今的内存抓取软件能够躲过大多数的安全防护并访问敏感的信用卡数据。

如果计算机重启并且立刻载入用来倾倒内存内容的特定操作系统，即使不拿走内存，这种攻击方法也可能奏效。

这种冷启动的漏洞清楚地指出了存储在内存中的数据是唾手可得的。同样的方法可以用来访问存储在内存中的信用卡数据，但是报告中提到的内存抓取技术并不需要物理访问。

通过注入已运行的进程来隐藏自身或者直接在机器上运行，当今的内存抓取软件能够躲过大多数的安全防护并访问敏感的信用卡数据。一旦进驻系统，内存抓取软件能读取密码、加密密钥、信用卡、社会保障编号或者是容易转换成现金的其它类型数据。接着内存抓取软件要么保存这些敏感数据到本地系统或者通过各种方法直接发送给犯罪分子。即使偷取的信用卡数据是加密的，但如果攻击者能够使用类似之前描述的方法抓取到用于加密的私钥，那么他仍然可能得逞。

企业中的内存抓取软件

因此内存抓取软件能够以许多不同的方式危害企业的信息安全就不足为奇了。通过直接读取内存甚至是在离线的情况下读取交换文件（硬盘上的虚拟内存）这种恶意软件都可以收集到数据。无论内存抓取软件如何获得数据，为了执行成功，这种攻击必须要么利用弱配置或者让有足够权限的可执行文件来读取内存。从整个内存中读取数据是缓慢、低效的并且容易被侦测到，但它仍然是一种潜在有效的攻击。

编写内存抓取的恶意软件比起通常看到的恶意软件要求更高的熟练水平，因为编写者需要根据特定的软件或者环境来定制。

可被攻击的软件是内存抓取软件的另一个可能的目标。更具体地说，此类的恶意软件攻击内存管理方面的软件和敏感数据。比起读取整个内存这种方法会更有效，因为只需要监控程序写入数据到内存的位置而不是读

取数十亿字节的内存。此外这种内存抓取方式更难被侦测到，但是对于攻击者来说也有不利之处。

这些类型的攻击给企业带来的威胁很现实，但只是针对那些价值高的目标而言。编写内存抓取的恶意软件比起通常看到的恶意软件要求更高的熟练水平，因为编写者需要根据特定的软件或者环境来定制。

对于企业的信息安全主管来说为了防范内存抓取攻击，保障对于组织具有重要价值的对象（通常是那些存储敏感数据或者是很容易就可以被访问到的设备），最好采取有效的预防和侦测措施。很明显首先需要辨识出这些对象，然后评估以判断现有的防护措施是否充足或是需要新的技术或过程。

通过恰当的流程来追查潜在的内存抓取攻击（或就此而言包括任何攻击）同样重要。如果网络监控系统发现高价值的对象例如，某个固定销售点的终端开始与企业内网或因特网中的新系统开始通信，那么这时的告警不仅应该引起安全职员的注意，同样需要迅速地进行调查。快速地调查潜在的非法通信有助于在早期就发现严重的事故并且限制或预防破坏或数据丢失。

同样为了防止内存抓取攻击，软件不应该以管理员权限或者是通常具有系统访问的高权限运行。对于攻击者来说访问内存中敏感数据最容易的途径就是利用以管理员权限已经运行的软件。其次存放敏感数据的位置应该以详细的系统清单的形式

保持最新。信息基础设施随着时间增长和发生变化，所以确保恰当合适的安全措施是重要的。

内存抓取并不是全新的技术，但是最近的发展代表了之前攻击的演变并且会在今后持续地进行。企业必须通过实施上述的一些最佳实践来不断地提高自身的防护以保证尽可能有效地保护敏感数据。

（作者：Nick Lewis　译者：杨帆）

饱受争议的 SMB v2 安全问题：禁用还是打补丁？

2009 年 9 月初微软向用户通告了一个远程代码执行漏洞，它存在于第二版服务器消息块（SMB v2）协议中。SMB 是 Windows 环境下的一种文件共享和打印协议，用于网络设备间消息的传递。

安全研究员们开发出的攻击代码能够利用这个缺陷造成拒绝服务攻击（DoS）或者是未认证的远程代码执行。漏洞代码也已经被公布于众。

早期微软发布了一个补丁禁用 v2 版本的 SMB。V2 版本的 SMB 是该协议的更新版本，只支持 Windows Server 2008、Windows Vista 和 Windows 7。并且只有当客户端和服务器都支持时才能够使用。Windows Vista SP2 及其早期版本和 Windows 2008 SP2 及其早期版本都存在该漏洞。Windows 7 RC 版也存在该漏洞，但是 Windows 7 官方正式版在发布前已打上补丁。Windows XP、Windows 2003 和 Windows 2008 R2 不存在该漏洞。

2009 年 10 月份微软在其周二的例行补丁更新中发布了一个安全补丁。建议企业在正常补丁周期中应用该补丁，并且如果不能现在部署该补丁也应该在微软的下次补丁发布前这样做。在本文中让我们探究下为什么企业应该考虑加快 SMB 补丁的部署或采纳某种变通方案。

日常环境中远程代码执行或者拒绝服务攻击是严重的威胁。第二版的服务器消息块的安全漏洞可能被融合到僵尸程序、蠕虫或者其它恶意软件代码中，以攻击某组织、访问数据并进一步渗透到其网络中。许多僵尸程序、蠕虫或其它类型的恶意代码以模块化的方式开发以方便融入新的攻击方法和漏洞。

例如，臭名昭著的 Conficker 蠕虫（又名 Conficker/Downadup）使用几个不同的 Windows 漏洞来传播和感染系统。类似地这个 SMB 漏洞也能够包含到蠕虫程序中并且快速地传播。虽然该漏洞代码还未被包含到其它恶意软件中，它可能被融入蠕虫或者僵尸程序并且用于目标性的攻击中。开源渗透软件 Metasploit 的测试框架也把它包含其中。

然而在客户端计算机上利用这个漏洞的可能性非常小，除非没有遵循几个最佳实践。也就是说禁用了默认的主机防火墙和在边界上没有防护 Windows 网络包括 SMB 功能。这种攻击依赖使用 SMBv2 的 Windows 网络将恶意代码传播到漏洞主机中。在 Windows Server 2008 上该漏洞被利用的可能性更高，因为不太可能用防火墙隔离来自客户端系统的文件或打印机服务器网络连接请求。

无法立即部署该补丁的企业应该使用变通方案之一，即禁用 SMBv2 以确保系统有足够的保护直到部署补丁，我们在一分钟内就能完成这些。但是企业在部署一

个变通方案前必须回答的问题是如果这样做比起部署补丁是否费力较少。应用补丁和变通方案间的部署机制可能会有所不同。

可以使用标准的补丁工具部署补丁，但是执行变通方案可能需要额外的测试和部署尝试。使用变通方案有两种方式禁用 SMBv2：微软发布了一个 FixIt 修补软件包会禁用第二版的服务器消息块。也能通过需要重启服务的注册表键值修改完成。两者都需要在部署补丁后再次启用 SMBv2 以便让该功能再次可用。

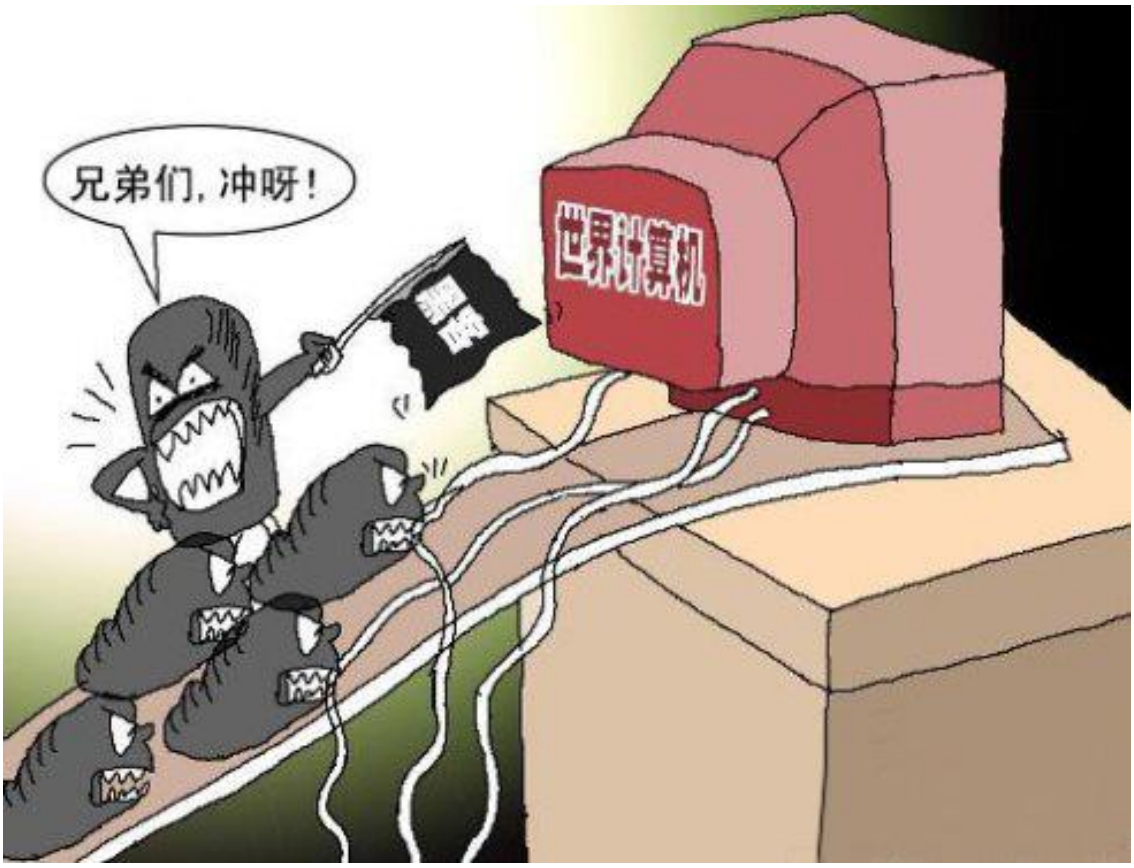
可以使用标准的补丁工具部署补丁，但是执行变通方案可能需要额外的测试和部署尝试。

禁用系统服务是推荐的一种变通方案，但是这会对系统有极大的影响，因为这种服务器服务是一些管理系统操作的核心，它会提供 Windows 文件和打印服务。另一个变通方案是再次启用 Widows 防火墙到默认状态。这两种方案在部署前都需要足够的测试，重新开启 Windows 防火墙后需要鉴定相应的软件或服务。

对于今后类似的 Windows 网络或者 SMB 漏洞，企业应该遵循一样的建议，并且将补丁部署和变通方案所作的努力进行对比，并对攻击代码的可行性做尝试，以选择最适合他们环境的策略。权衡新漏洞带来的风险以及攻克该漏洞的努力程度，

以达到防御新漏洞的目的。部署边界防火墙和利用客户端的防火墙将会帮助减少网络上的计算机被 SMBv2 漏洞利用的风险。

（作者：Nick Lewis　译者：0dyssey）



应对微型 botnet 的最佳实践

最近出现一些有关于大型 botnet 的事件，比如那些用来破坏 Twitter 和 Facebook 网站的 botnet，已经是众所周知的新闻了。虽然那些大型的安全事件很容易引起人们的注意，但那些规模较小的、更加隐蔽的 botnet 攻击才是对于企业来说更大的威胁，这一点已被人们所证实。

随着企业的安全防护机制日渐增强，攻击者会去寻找系统的弱点，然后开始使用规模较小的、不太引人注意的 botnet，从而避开企业的安全防卫体系。在这篇

技巧文章中，我们将分析为什么这些所谓的微型 botnet 能够成功地进行攻击、怎样识别它们，以及怎样阻止它们的破坏行为。

为什么微型 botnet 的攻击效果更好

大型的 botnet 经常被用来发起拒绝服务（DoS）攻击。为了能够让一个电子商务网站崩溃，或者阻止一个企业访问 Web，这些攻击需要一些资源——即 botnet 军队。就像在战争中派遣成千上万的士兵去打败敌人一样，攻击者会将很多计算机的资源集中起来去攻击一个服务器或网络。当攻击者想对一个企业发起 DoS 攻击时，他会给很多分散的 botnet 军队发送命令，让他们集中起来攻击受害者。因为这在目标环境中创建了多条连接，所以会引起几乎所有主机和周边保护系统的注意（以及资源），致使受害者完全没有任何办法，甚至整个系统都会崩溃。

与大型 botnet 利用大量资源去冲击网络发起拒绝服务攻击所不同的是，微型 botnet 被检测到的可能性很小。因为它们只需使用较少的计算机，发送较少的数据包，所以它们在避开防火墙的 botnet 监测以及入侵检测系统方面更有优势。为了进一步避开监测，控制 botnet 的人还可以通过对自己的微型 botnet 进行设置使得杀毒软件不能工作（虽然软件看起来还在正常工作）、长期潜伏在机器上、或者不定期的呼叫攻击者以获取新命令。没有能够监测的识别标志、没有不正常行为

的模式，这使得哪怕是最先进的、基于行为的入侵防护系统都很难注意到微型 botnet。

为什么微型 botnet 能够成功

为了进入企业、绕过防火墙和 IPSes，攻击者们经常以用户为目标。

使用社会工程学对目标用户进行攻击是渗透到一个企业最简单的方法之一。它能够相对容易地找到企业和员工的信息，然后把这些信息融入到一个构思巧妙的钓鱼 email 里，并以恶意软件为邮件的附件。探测和踩点分析（footprinting）网络的弱点也是微型 botnet 攻击者常用的方法，但这比发送简单的 email 需要更长的时间。一旦一台机器被攻破，攻击者要么可以给受害者的发送恶意软件命令，让它们继续攻破其他的主机，进一步的扩展 botnet，从而在受害者的网络中提取到目标数据；要么干脆把 botnet 卖给别人，转而去寻找下一个受害者。

更糟的是，一旦他们攻破了一个网络，微型 botnet 还可以潜伏一段时间，等待进一步的命令或者特定的“触发”事件。大型 botnet 需要更好的命令和控制，这样做可能导致响应不正常或者被发现，与此不同的是，小型 botnet 更加精确，最适合发起定向的攻击，特别对特定数据进行偷窃时。

微型 botnet 能够比传统 botnet 更有效地搜寻出数据。微型 botnet 经常将多种方法混合来使用，从而获得敏感数据。

微型 botnet 能够比传统 botnet 更有效地搜寻出数据。微型 botnet 经常将多种方法混合来使用，从而获得敏感数据。它们更加谨慎，在探测网络时一次只发送几个包，能利用受操纵的帐户搜寻商业秘密，并且能通过删除关键的软件文件使得杀毒软件失效。一个微型 botnet 在跟正常的网络流量一起穿过网络时，会试图发起这些攻击，而且还会尝试其他的混合攻击。

帮助找到并组止微型 botnet 的最佳办法

很明显，人的因素是一个重要的环节，而且很明显 botnet 可以避开传统的防护系统并渗透到企业环境中去。为了保护自己不受到微型 botnet 的攻击，企业必须开始分配更多的资源来检测它们，而不是只把重心放在防御上。就像前面描述的一样，botnet 经常能够轻易的潜入企业环境，而传统的防御系统却总是不起作用。不是说防御就没有必要了，而是说监测已经进入企业的 botnet 是最应该做的，哪怕是一次鼠标的点击也不应该忽视。如果你认为防火墙、IDS 或者恶意软件防御软件足以应付外界的攻击，那么这种心态会导致你误认为自己的工作环境是安全的。企业必须做得更多，才能了解自己的网络中到底发生了什么。

了解和理解网络的活动可以更早的识别出攻击，从而能够更好的对攻击作出回击。然而，这超出了资产管理的范围，而且还需要对主机上运行的全部程序、主机

放置在什么地方、它们使用什么端口等等信息有所了解。它包括对环境的映射、保持客户端软件升级到最新配置的详细资料等。

在微型 botnet 开始显现的时候，不管这一动作多么的微小，都需要你注意网络流量中异常的增长、意外开放的端口，以及帐户权限突然提升等情况。如果你正在使用一个模式扫描器（pattern scanner），那么请提高灵敏级别，花点额外的时间确定那是不是一个错误的确认。对日志进行分析是一个好的网络安全习惯，这样你可以了解网络中到底发生了什么事情。如果想对大部分的日志进行自动化分析，你可以看看由 LogLogic Inc.、ArcSight Inc 公司或者 Tenable Network Security Inc 公司提供的产品。

最后，一定要重视培训和教育用户。用户必须懂得怎样识别和报告不正常的网络活动，以避免成为社会工程攻击的受害者。为了引起用户的注意，培训过程必须安排得有趣，还应该检查用户是否真正懂得了课程所学内容。为了找到以及阻止微型 botnet 的攻击，企业必须把更好的培训和上面提到的安全措施结合起来，列入到企业的安全策略中去。

（作者：Marcos Christodonte II 译者：Sean ）

SSL 加密网络连接是怎样被截获的

企业常常有正当的理由截获加密的网络连接。不幸的是，黑客可以用相同的方法接入安全连接，这通常是因为终端的脆弱性。

在本文中，我们将研究企业和黑客如何拦截用传输层安全（TLS）协议或者其前身——加密套接字协议层（SSL）——加密的网络连接。

数字证书——通常与 TLS / SSL 配合使用——只是带有数字签名用于描述身份的一小块数据——比如一个组织的名称和网址。签名是一个基于证书内容和签名者的密钥的复杂的数学运算。如果证书中的值在传输中改变，数字签名将不匹配，于是浏览器将显示错误信息。

数字证书——通常与 TLS / SSL 配合使用——只是带有数字签名用于描述身份的一小块数据——比如一个组织的名称和网址。

你怎么知道一个数字证书真的是你所以为的人所拥有？这一切都基于信任链（chain of trust）。例如,当你去 Alice 的网站，她向你提供她的证书。Alice 的证书已得到她的朋友 Bob 的确认和签署。反过来，Bob 的证书已得到确认并由他的朋友 Charlie 签署。Charlie 也是你的好朋友，你很自然地信任他。在这种情况下，Charlie 是作为我们的公钥基础设施（PKI）的根（root）认证中心（CA）。当你看到 Alice 的核查证书链上 Charlie 的签名，你就会相信这的确是 Alice。

在现实生活中， Web 浏览器拥有预安装的——比如网络基础设施公司 VeriSign——受信根证书颁发机构的证书。你的 Web 浏览器会自动信任被预安装的根证书颁发机构的数字证书。但是，黑客可以利用这种信任。

数字证书有多值得信赖？

没有什么东西是完美的——即使是受信的根证书颁发机构。 2001 年， VeriSign 错误地“给一个谎称是微软雇员的人发出代码签名数字证书”（ MS01-017 ）。根据微软安全公告，“拥有使用属于微软的密钥来签署可执行内容的能力，无疑非常有利于那些想要说服用户同意代码执行的恶意用户。该证书可用于签署程序、ActiveX 控件、微软 Office 宏和其他可执行的内容。

数字签名也可以是伪造的。去年，在柏林的 Chaos 通信大会上，一组研究人员揭示了可以用 MD5 加密算法来创造一种“无赖”证书的缺陷，而该证书拥有有效根证书颁发机构的签名。此证书从未被受信根证书颁发机构认证过，但由于它拥有一个有效的签名，它将被所有常见的浏览器信任。

SSL 拦截工具

更常见的情况是，攻击者可以使用凭空造出来的证书和中间人攻击技术，绕过 TLS/SSL 连接。

企业经常拦截的 TLS / SSL 连接。为什么？想象一下，你是一个在工作时检查基于网络的个人邮箱的公司雇员。你的公司会有强烈的动机窥视你的数据流，以确保你没有泄露私密数据或者错误的下载病毒。企业经常要检查所有进出其网络的数据流，以防止恶意软件感染并保护他们的私密数据。

企业常常使用 SSL 代理（如 Blue Coat Systems 公司的 ProxySG），来破解 TLS/SSl 连接和监视雇员的数据流量。SSL 代理可以截取私人电脑和外面世界的数据流。当用户访问一个“安全”的网站，SSL 代理提取真正的 Web 服务器证书，并在代理服务器和网络服务器之间建立一个合法的 TLS/SSL 连接。然后，代理工具凭空制作一个虚假的证书，这个证书类似于网络服务器的证书。它提供这个假数字证书给用户，并在用户的浏览器和网络代理之间建立另一个 TLS/SSL 会话。用户可能会收到弹出的错误信息（点击它，可以让它消失），因为假数字证书不受信任。当然，如果企业花时间为用户网络浏览器引入代理证书为受信根证书，那么用户完全不会看到错误的消息。而最终的结果会是什么呢？在用户的计算机和代理之间有一个“安全的” TLS / SSL 会话，以及另一个在代理和网络服务器之间的“安全的” TLS/SSL 会话。

企业常常使用 SSL 代理（如 Blue Coat Systems 公司的 ProxySG），来破解 TLS/SSl 连接和监视雇员的数据流量。

作为代理，个人信息可以被作为纯文本检查，这样公司就能够自动搜索流量中特定关键字或屏蔽其中的恶意代码。

不幸的是，攻击者可以使用和公司一样的技术拦截 SSL 连接。一个特别自由、公开的工具使这样做很轻松。因为有了企业 TLS/SSL 拦截工具，攻击者可以利用这些工具来自动连接到真正的网络服务器、捕获证书信息，并用同样的信息凭空生成一个新的证书。随后提供新证书给用户，并建立一个 SSL 连接。在这个以后，用户的计算机和黑客之间建立起了一个“安全的”SSL 会话，以及另一个在黑客和网络服务器之间的“安全的”SSL 会话。其他类似的工具完全移除了客户的 SSL 连接，并使用社会工程技术（比如锁图标（lock icons））来欺骗客户，使他以为连接是加密的。

用户可以做什么来防止 SSL 拦截攻击？这里有四个关键策略：

始终使用受信任的计算机访问有价值的信息的网站。如果你的计算机不受信任或曾受到过危害，那么有人可能在你的网络浏览器安装了非法的信任证书。

考虑使用完整检查或回滚的软件，检测并消除那些未经授权的、对受信任的证书颁发机构列表的更改。

不要接受非信任证书。如果可能的话，配置用户的浏览器，从而自动拒绝不受信任的证书。

在点击前先想想。请记住，即使是受信任的证书管理机构也会犯错误。对员工和家庭用户进行培训，让他们学会谨慎地访问网站。

TLS / SSL 就像一个很好的坚固的小玩意（two-by-four）。你能使用它来建立一个安全的基础设施吗？能。单就它自身而言是一个安全的基础设施吗？不是。

围绕 SSL 拦截，整个行业在进步。企业和执法者，以及黑客都一样希望能够获取加密数据流的信息，所以终端对一个更强的保护措施的需求是很复杂的。然而，只要注意细节，企业和家庭用户可以检测并避免 TLS / SSL 拦截和迂回（bypass）攻击。

（作者：Sherri Davidoff 译者：Sean）

网络战是企业的真正威胁吗？

2009 年 7 月初，出现了不少关于“大规模网络攻击”的报道，这些新闻说有来自朝鲜，目标是韩国和美国的一些重要网站。据报道，这些攻击是由分布在全球各地的“数万台”受感染的计算机发起的，它们被用来发动分布式拒绝服务（DDoS）攻击。被感染的系统本来要自毁（大概还想与全世界同归于尽）。

大多数安全爱好者都不解，为什么这么一次规模不大，动机不复杂，造成的破坏也不大的僵尸网络攻击会上华尔街日报的头版呢。一些面向大众的政府网络变得很慢或者有几天无法访问，但是并没有经济损失或者严重的服务中断的报告。

所有的这些炒作都是为了什么？网络战真的是企业信息安全专业人士应该关注的内容吗？

上个月发起这次攻击的僵尸网络还算是不太过分的，但是网络战（或网络事故）的潜在危害是巨大的--不是因为敌人有多么高超，而是因为我们自己的基础设施很薄弱，维护也不到位。在美国，关键的基础设施对 IT 的依赖已经超出了大多数人的认识。摩天大楼的加热，制冷和准入系统都可以通过互联网控制。医院通过 VoIP 电话联系心脏移植。这些只是两个例子，但是还有许多其它例子能说明一起有预谋，有针对性的攻击真的能造成大规模的混乱，甚至造成生命损失。

网络战只不过是一个更宏大的问题的小部分：我们需要设计出一个稳定的，全球性的 IT 基础设施。

网络战只不过是一个更宏大的问题的小部分：我们需要设计出一个稳定的，全球性的 IT 基础设施。莽撞无知的青少年肆无忌惮地对互联网造成过无数次严重的破坏。例如 1986 年，Morris 蠕虫造成了比这回炒作的 DDoS 攻击还严重的破坏，

它感染了数千台重要的 Unix 服务器。我们最大的问题不在于有人图谋不轨，而在于 Morris 蠕虫都过去了 2 3 年了， 我们的网络基础架构还是和积木塔一样。

即使是纯粹偶然的网络中断，也对关键的基础设施造成了重大损害。早在 2002 年，贝斯以色列女执事医疗中心的网络遭到洪泛攻击，陷入瘫痪，起因仅仅是一个偶然的生成树一路(spanning tree loop)。突然之间，医生和实验室技术人员无法在网络上查看病历和实验室结果，或是填写处方。最终，急诊室只好关门，病人转送到其他医院。

如果有人真的试图通过因特网破坏某些关键系统的话，会发生什么呢？

在去年的 SourceBoston 安全会议上，安全研究人员 Dan Geer 调查了用 2001 年的 Nimda 病毒可以造成些什么破坏 。2001 年，就在 9 月 11 日之后几天，Nimda 通过五种媒介传染到整个网络，第一天就感染了几十万台计算机。还有一种名叫 E911 的老病毒，它会让被感染的系统不断通过调制解调器拨打 911。Geer 评论说，如果病毒作者在代码里加进那个功能的话，美国人“9 月 19 号早上起来发现全国所有的紧急服务全部失效了，它被一次性全部关闭，就像电灯开关一样。那天可正是整个美国还惊魂未定的时候。

如何抵御网络攻击和网络事故

预知网络中的下一个危机很难，但是这里有一些最佳实践能让企业安全团队避免成为受害者。

1.防患于未然。把你们组织的信息流绘制出来。了解哪些系统/服务具需要关键的网络功能。很多情况下，没有网络后公司根本无法运作。我们没有纸笔或是员工培训来人工处理我们的信息。制定网络中断后的短期（即 1 小时）、中期（即 24 小时）和长期（即多天）后备计划。如果有可能的话，对其进行验证。要现实一点，看到会有哪些限制，规划可行的东西。

防患于未然。把你们组织的信息流绘制出来。了解哪些系统/服务具需要关键的网络功能。

鉴于目前的经济不景气，许多企业可能都没有资源投入到灾害规划上。但正如我的母亲所说，只求尽力而为。

2.维护系统。 对所有设备例行打补丁，包括服务器，工作站和网络设备。还一定要包括第三方应用程序。还要定期审计。集中收集日志。即使你没有时间做灾难恢复，那也至少要维护好你的系统。不要成为黑客眼中好。

3.共享信息。 这听起来似乎有悖常理，但我们大家都是唇齿相依的。如果在某个行业里的每个人都发现了相同的探测或是异常活动，那就可以让我们确定攻击

的前导，从而避免重大的灾难。分享关于有效和无效的防御技术的信息也可以帮助我们更有效地作出反应。

4.做一个好邻居。 不要忽略非关键系统。即使角落里的那台 Windows 上“没什么重要的东西“，你也肯定不希望有感染它并利用它来攻击其它主机。

5.要大惊小怪。那些对一起又一起网络攻击的报道造成了不必要的恐慌。害得大家现在觉得，一个并不复杂的僵尸网络就可以造成全球性的恐惧，甚至还可能影响国际关系，这实际又是对那些攻击者的鼓励。我们都有自己的安全问题，网络战肯定是其中之一。但是，如果我们都能保持冷静，攻击者就又少了一个发起网络攻击的理由。

对“网络战”威胁的宣传已经太言过其实，但我们有理由担心：我们的国家基础设施是一个烂摊子。事故造成了和“网络战”或其他恶意袭击一样大的损害。“战争”不是问题所在，管理不善、混乱和恐惧，才是真正的威胁。

（作者：Sherri Davidoff 译者：Sean）