FREEBUF
黑客与极客

《网站攻击生存手册》

2014年度网络安全专题白皮书

2014年1月1日

FreeBuf黑客与极客背景介绍

热爱互联网安全的人都是热爱生活的人，爱安全的人应该感谢这个时代，应该感谢发达的资讯和媒介让我们可以学习到如此丰富多彩的安全技术；但是同时热爱安全的人往往也会痛恨这个时代，祖国复杂的大环境，每天耳边眼前某某大黑客又进去喝茶了，某某大型电商又被拖库了，无时不刻的轰击着我们的耳朵，同时也对我们敲响警钟，禁锢着我们的行为。我们想为祖国的网络安全做贡献，但是却又被各种各种条条框框乱七八糟的法律法规约束着。是的，爱生活，爱自由，我们对技术的选择却很累很不自由。

FreeBuf希望为国内网络安全领域带来一抹正能量，传递真正的黑客与极客精神。

联系我们：
新浪微博
http://www.weibo.com/freebuf
腾讯微博
http://t.qq.com/freebuf
EMAIL
root#freebuf.com

目录

一、前言

你将在网络空间中遇到什么样的噩梦？

- 收到一封“赎金通知”，要求你在限定时间内汇给对方上百万美元，否则销毁你电脑中所有资料。
- 眼睁睁看着你的公司网站在洪水猛兽般的拒绝服务攻击（DDoS）下瘫痪。
- 打开了一封不详邮件，信中写到“你的网站将是我们下次攻击的目标”。
- 发现自己网站的应用框架布满了千疮百孔的漏洞，连打补丁都需要好几个月。

当这些噩梦成为现实，你该怎么办？

这份《网站攻击生存手册》描述了当前网络空间包含的各种威胁，包括黑客和网络罪犯使用的攻击手法和工具。本手册详细说明了如何利用安全技术来保护网站免受攻击以及相关的操作程序。本手册还帮助你区分防护工作中的重点以及你可能忽视的一些安全技巧。

在阅读完《网站攻击生存手册》之后，相信大家能够充满自信地面对任何潜在的网络攻击，利用成熟的战略化解危机。

二、网站应用安全状态

网站应用威胁概要

网站应用是最受黑客青睐的攻击目标。事实上，75%的网站攻击都是针对网站应用。大多数网站每天都要遭受数十次攻击，有一些网站平均每分钟遭受攻击的次数超过26次。

虽然网站攻击并不是新兴事物—自互联网创立就已经存在—但却随着黑客主义的兴起，已经成为一种经久不衰的黑客手段。

“黑客主义”的兴起

“黑客主义”从2010开始进入到人们的视线之中，那时出现了匿名组织（Anonymous）、“鲁兹安全”（LulzSec）以及“反安全”（Anti-Sec）等知名黑客组织。从最初攻击金融机构开始，匿名组织及类似黑客群体将目标迅速转移到了政府和商业组织。在两年内，全球58%的数据盗窃案件都是源自黑客攻击。

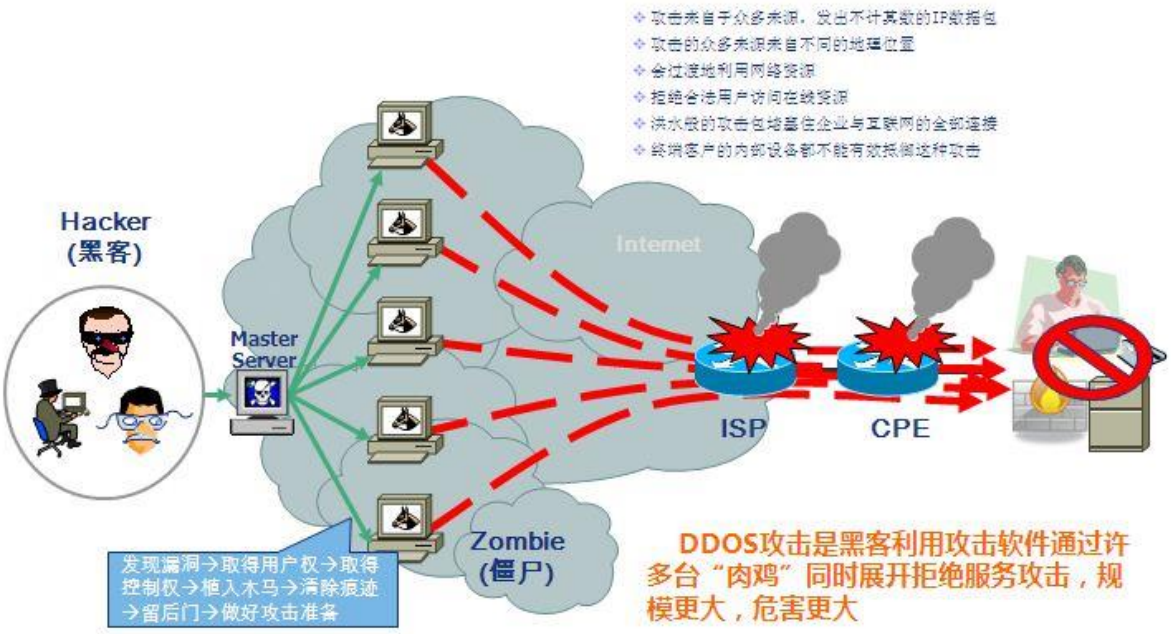
2012年出现的新的黑客组织，比如叙利亚电子军、AnonGhost以及伊朗网军等，这些黑客组织针对美国银行和西方国家发起了一系列黑客攻击。这些攻击大多包含传统的网站攻击手段。比如SQL注入和跨站脚本攻击，以及我们熟悉的DDoS攻击。黑客攻击不仅对目标公司造成了巨大的损失，还造成了隐私数据的大量泄漏和网站长期停运。

DDoS攻击走上商业路线

排除黑客攻击的因素，许多组织都在持续不断地遭受竞争对手或网络勒索者发起的DDoS攻击。这些商业化的DDoS攻击破坏力很大—超出传统带宽数百倍，达到了300Gbps或更高，而且这些DDoS攻击越来越高级，传统的安全控制措施对此已经失效。由于目前流行的DDoS攻击利用网站应用和数据库漏洞开展攻击，而不是单纯发送TCP或UDP数据包，因此危害性更大。

反击

黑客每天都在利用大量攻击迫使网站下线，并从中窃取机密数据或修改网站内容。幸运的是，我们可以做一些准备来应对这些危机。根据网站应用安全顾问以及一线防护技术人员的反馈，这份生存手册列出了应对网站攻击的系列措施。



三、抵御网站攻击的分步战略

第一步：理解攻击者意图

在应对网络攻击之前，第一步首先要理解攻击者的意图。对方是什么身份？是像匿名组织一样的知名黑客团体还是叙利亚电子军？是一个无聊的“脚本小子”还是商业罪犯？通过研究他们的攻击手段和工具我们可以了解基本情况。

“知己知彼，百战不殆”
—《孙子兵法》

注意观察社交媒体

如果黑客威胁攻击你的网站，那么你可以到一些知名社交媒体上看看，他们有可能在讨论你网站的漏洞和缺陷，在推特、Facebook、YouTube上好好找找，或许能发现他们的攻击手段和时间安排。

黑客组织有可能会公布他们的DDoS攻击工具，招募互联网自愿者对你的网站进行攻击。分析类似的信息，通过创建网站应用安全签名来封堵这些攻击工具。

在一段时间的攻击后，黑客有可能发布一些“增强包”来强化攻击工具，以此达到利用网站漏洞和URL的目的。注意这些“增强包”的发布，你可以通过添加策略来应对。

网络罪犯比黑客更可怕，因为他们不会公布策略或战术。遇到这种情况，你要坚持关注黑客论坛，或者与同行进行交流，讨论攻击来源、技术和工具。你要经常阅读黑客情况报告以及与你所在产业相关的安全研究报告。

第二步：制定安全应急计划

如果你的组织成为了黑客攻击的目标，那你应该组建一支应急小组来处理安全问题。这支应急小组应该随时待命，根据攻击的严重性，制定7x24小时的应急措施，保证在发生此类事件时有人能够及时做出应对。

调整是不可避免的

你的应急反应小组需要在受到攻击时快速转变安全策略。你需要恰当放宽内部批准程序，保证你能够迅速适应千变万化的攻击形式。

红色应急小组

创建一支“红色应急小组”—一支由安全人员组成的小组，负责寻找黑客可能会利用的漏洞。“红色小组”的职责是评估所有可能发生的威胁，包括针对网站应用、网络结构和终端用户等发起的社会工程学甚至是硬件攻击。

联系人备忘录

准备一本备忘录，记载以下机构的名字、电话号码和电子邮件地址。

- 负责信息安全、网络建设、应用程序研发、数据库管理、法律和执行管理机构。
- 域名和互联网服务供应商
- 提供DDoS保护服务的供应商
- 相关安全专家和顾问—例如记录你网站应用防火墙（WAF）的架设人员、安全和事件管理员以及入侵保护系统供应商的联系信息。在你遭到网络攻击时你有可能需要他们的帮助。

安全贴士：

✓必须保证你的应急计划信息、网络拓扑图和IP地址方案的安全性。

✓不要将网络结构和联系人通过邮件发送给整个安全部门，不要将这些信息存储在公共共享文件夹中

记录网络和服务器信息

搜集网络和服务器信息，包括：

- 服务器IP地址、数据库、DNS服务器、网络防火墙、网站应用防火墙、数据库防火墙以及路由器和转发信息。
- 基于IP的灾难恢复（Disaster recovery）数据。

同样，你还要准备所有数据中心的网络拓扑图。如果已经获得了这些拓扑图，经常回顾它们，保持他们处于最新状态。

通知经营管理团队和雇员

当你知道即将遭受网络攻击时，及时通知你的经营管理团队，告诉它们威胁的严重性并做好定期更新汇报。另外，你还要通知公司雇员。在遭受DDoS攻击时，告诉所有相关用户你们网站的应用或网络有可能暂停服务。

如果你的公司正在遭受黑客攻击，通知所有用户升级不安全的密码并告诉它们发生网络钓鱼的风险。让你的信息技术人员准备好应对社会工程学攻击，让他们核实任何密码修改请求。

必要时候黑客有可能发起硬件攻击。因此需要保护好雇员的笔记本、网线和网络设备等。

建立“作战室”

指定一个“作战室”，在遭受网络攻击时在“作战室”中展开所有决策和交流。工作人员可以集中在“作战室”中审查安全更新并制定战略防御机制。比如选会议室就是一个不错的选择。

为你的“作战室”指定一名“将军”，在遇到网络攻击时，这名“将军”将拥有战役的指挥权。适当给他放宽一些权限，保证他在做出决策时不必考虑很多规章制度上的繁文缛节。

第三步：定位和评估网站应用和服务器

即使你在网络拓扑图中记录了已知的服务器，你还是需要通过扫描网络来找出恶意服务器和网站应用。应用研发人员或质量监督测试人员可能添加了新的网站应用和数据库，其它人员可能安装了未经批准的应用。如果你不扫描整个网络并定位所有服务器和应用，你就不能进行完整的风险评估。

进行再三分类

一旦你定位了所有应用和数据库，你需要找出哪些包含敏感数据（私人身份信息、个人医保信息、信用卡号或知识产权）。找出那些是你商业（网站）正常运转需要的基础应用。即便你的公司网站不包含敏感信息，也有可能会遇到一些黑客的攻击。

一旦你找出了哪些服务器和应用是处于高风险状态的，你就可以有重点地进行评估。

注意云服务

数字资产并不仅限于你物理网络上的那些，挂在云上的客户信息管理系统、内网应用、邮件应用和内部网站都是你需要注意的。这些应用可能会包含机密信息，因此保护这些应用的安全非常重要。

扫描网络和应用的漏洞

保护你应用的最重要的一个手段就是漏洞测试。通过扫描服务器和网络设备，你能够找出潜在的漏洞和没打补丁的软件。特别需要注意的是，网络扫描器只是一个基础，网站应用扫描器才能找出黑客经常利用的应用漏洞。

使用各种不同的扫描器来测试你的应用。不同的扫描器可能发现不同的漏洞。

不要把评估工作仅限于你公司的网站。扫描所有的应用，包括你合作伙伴的门户网站、用户信息管理应用、外联网以及其它有可能被攻击的目标。所有这些应用都有可能被黑客拿下，从而对你的公司造成潜在危害。

在准备应对针对应用的DDoS攻击时，首先分析应用中连接数据库的URL地址，比如登录、注册、密码更改或搜索页面。在应用表格中输入通配符，检测是否会出现逻辑漏洞，比如常见的万能密码1or1=1之类。

搜集黑客使用的工具，比如Havij SQL注入工具和其它免费的扫描器。

在扫描完应用之后，为所有漏洞打上补丁并再次进行扫描。如果时间有限不能补上所有漏洞，那么首先处理处于高风险级别的应用漏洞。

评估数据库

由于敏感数据一般都存储在数据库中，因此你需要通过扫描数据库来寻找漏洞和配置缺陷。根据评估结果，决定是否要为操作系统和数据库打上安全补丁或者修改配置。

为了加强数据库的安全，你需要删除默认的数据库用户账号并禁用任何不必要的服务。为了保证承载的服务器不受攻击，禁用不必要的Telnet、FTP和远程登录服务（rlogin）。

第四步：加强应用、网络和终端的安全控制

当你为所有应用和服务器打上补丁之后，你就可以加速你的防护工程。为了阻止网络攻击，你应该采用更加严格的网络应用、结构和安全策略。

在执行严格的策略时与应用研发人员保持密切联系。研发人员能够帮助你准确分析配置文件。他们还能通过审查安全警告，确保你的新策略不会封锁合法请求。

保护网络设备和服务器

1. 执行严格的网络防火墙和入侵检测系统策略。将入站流量限制在HTTP和HTTPS等必要的网站应用服务上。通过配置入侵防御系统策略，阻止严重的安全违规现象。
2. 在服务器上安装杀毒软件和反恶意软件，保证它们的数据库处于最新状态。
3. 配置数据库防火墙，控制对数据库未经授权的访问。

关闭网站应用

由于网站应用是网站攻击的最终目标，我们必须将精力集中在调整和测试网站应用上面。以下措施描述了如何最好地保证网站应用防火墙能够阻止所有在线威胁:

- 审查并调整网站应用配置文件—也称为“白名单”安全模式。确保配置文件的准确性：
  - 检查已经从网站上移除但仍包含在配置文件中的URL地址和目录。
  - 审查合法的字符和参数值的长度，并寻找错误的规则。
  - 将应用配置文件与漏洞扫描结果相比较，确保所有评估报告中的URL能够在应用配置文件中找到，同时所有应用配置文件中的URL都得到了扫描器的评估。
  - 严格配置文件策略，阻止白名单安全违规，比如出现带有非法字符的参数值（括号和问号）。禁止表单中出现过于长的值，防治出现缓冲区溢出和SQL注入攻击。
- 通过配置网站应用防火墙来执行HTTP协议。审查并调整协议相关安全策略，比如双编码、过于长的URL以及异常的Apache URI信息。通过强制执行HTTP协议，至少在遭到攻击时，能够破坏对方入侵手段，防止出现缓冲区溢出和拒绝服务的现象。

- 确保制定标准的网站应用防火墙策略，比如启用SQL注入和跨站脚本。所有风险性的应用，比如目录遍历、远程文件包含、本地文件包含以及跨站请求伪造攻击都应该被禁用。
- 封锁攻击其它网站的恶意来源。充分利用安全界的情报来阻止恶意用户和攻击。
- 网站应用防火墙能够通过表头信息检测扫描黑客工具（Nikto、Paros和Nessus）的请求。它们还能阻止扫描工具在短时间内检测安全违规操作。为了阻止黑客获取你网站的漏洞，你需要通过配置网站防火墙来阻止扫描器和网站侦查。

如果你的公司在云上存储了顾客应用、伙伴方信息或外联网应用，你需要确保这些应用处于网站应用防火墙的保护之下。保护应用的方法还有很多，比如“安全即服务”和基于虚拟设备的网站应用防火墙。

阻止应用层的DDoS攻击

应用层的DDoS攻击占所有DDoS攻击的25%，经常被用于消耗应用资源或利用应用漏洞。通过配置以下策略来阻止应用层DDoS攻击:

- 封锁那些在短时间内发送大量请求的用户、IP地址和会话。
- 封锁那些在短时间内下载大量数据的用户。另外为了防止黑客耗尽服务器资源，封锁那些在短时间内发送“.pdf”“.mp3”“.mpg”“.mp4” 等文件请求的用户。
- 封锁那些发送大量请求导致拖慢服务器速度的用户。这些用户有可能在使用应用中的商业逻辑漏洞。另外，封锁那些发送大量请求导致网站出现400, 405, 或503错误的用户。
- 限制高风险URL的访问请求，比如登录和搜索页面。这些页面是攻击重点。为了防止针对登陆页面的DDoS攻击，你需要采取以下策略：

  A. 登陆失败次数上限

  B. 同一用户多重合法登陆
- 许多应用层的DDoS攻击都来源于僵尸网络。另外，许多黑客都会利用匿名服务隐藏身份。
- 通过封锁恶意IP、匿名代理和架顶式（Tor）网络来阻止这些高风险源头。

保证你可以通过带外网络（out-of-band network）来管理所有安全产品。不然的话，在DDoS攻击的峰值时段那些产品可能会不受控制。

对于黑客攻击，受到攻击的公司可以通过关注社交媒体网站来了解黑客使用的工具。为了制定精确的危机缓解策略，你可以下载这些DDoS攻击工具并进行测试。寻找黑客用以创建自定义攻击签名的异常标头或有效内容字符串。在网站应用防火墙中定义新的策略封锁这些工具。

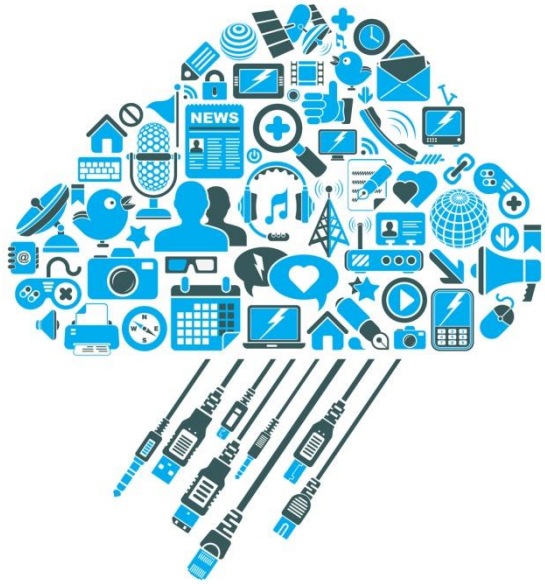
利用基于云的DDoS缓解服务来阻止DDoS威胁

为了应对网络层的DDoS攻击，你的网络需要有每分钟处理上百GB流量的能力。目前许多公司都依赖基于云的DDoS缓解服务来避免支付昂贵的硬件和带宽费用。

基于云的DDoS缓解服务能够根据你的需要进行“私人定制”，确保恶意流量不会访问你的网络。

在选择DDoS缓解服务时，你需要注意以下几点：

- 能不能同时阻止网络层和应用层的攻击？
- 能不能准确检测僵尸攻击？是否提供浏览器检测和验证码检测功能，确保只封锁恶意行为？
- 支不支持任播（anycast）NDS路由技术，确保自身的DDoS过滤数据中心不被误判为攻击源。
- 提不提供全天候检测和安全专家服务？



第五步：反击－监控行为并调整策略

一旦你的网站遭到攻击，你的安全应急小组应该利用所有现有资源来监控并处理攻击事件。对于密集的攻击，你还需要指派人员全天候值班，周末也应如此。

- 如果攻击来自于特定地区，创建策略封锁来自那个地区的请求，前提是不影响你的客户群。
- 分析僵尸攻击的行为，确定哪些URL是其攻击目标。创建相应规则阻止僵尸网络访问这些URL。
- 分析攻击模式、调整封锁策略。比如，黑客攻击了你的搜索页面，创建一个策略，封锁那些在一分钟内搜索超过10次的用户。或者创建一个“如果在10分钟内搜索超过25次则封锁4小时”的策略。让黑客们知难而退。

持续关注那些记录你网站被黑的社交网站、黑客论坛和聊天室等。黑客经常在聊天室中使用“#TangoDown”（击杀）一词来表示已经拿下网站。

除了审查应用安全警告和调整策略以外，监控来自其他网络和安全设备的警告。

- 审查数据库防火墙的日志，寻找异常行为。
- 利用网络性能监控工具分析安全警告，检测通信行为或硬件性能。
- 分析路由器、交换机、网站服务器和安全信息和事件管理器（SIEM）的日志。

第六步：请求专业支持－选择性的安全顾问服务

如果你即将受到网络攻击，但公司又缺乏有效应对的经验和技术，那你就需要考虑外请专家。安全专家可以通过分析硬件和软件的漏洞来制定应对措施。他们还能加强网站防护并调整安全产品的策略到最佳状态。

安全顾问可以作为你公司安全小组的外援，帮助你监控网站攻击流量并调整相应规则。根据他们自身的实战经验，他们可以帮助你应对任何形式的攻击。

总结过程需要解决以下问题：

✓你的网络因为攻击被迫停运了吗？

✓攻击有没有影响网站性能或带来网络延迟？

✓敏感信息有没有被窃取？

✓现在拥有的安全技术和程序管用吗？

✓未来改进的余地在哪？

第七步：从攻击中吸取教训

根据大量采访，当安全应急小组解决网络攻击之后，第一反应就是“庆祝一番”。在遭受长期网络攻击和压力之后，你的安全工程师需要时间恢复。然而，一旦问题解决，你需要立刻组织人员总结经验教训。

其中一步就是评估攻击带来的影响。分析网站应用防火墙的安全报告，调查攻击趋势。检查WAF、SIEM和网络监控工具的日志。

一旦你完成了总结，你就可以更好地应对外来的网络攻击。

四、总结和建议

网站攻击危害有大有小。攻击零售商获取信用卡号的小黑客和攻击50强银行网站的大黑客使用的方法肯定不一样。攻击工具也在不断改变—黑客会研发新的工具来规避签名检测。因此，你需要灵活应变。

通过采访许多位于网络战一线的安全专家，我们撰写了这一份《网站攻击生存手册》。它为任何面临黑客攻击的组织提供了一份策略指导。

不管黑客攻击的意图是什么，黑客总是攻击那些他们认为存在漏洞的网站。一旦黑客对一个网站用尽了伎俩，他们就会寻找下一个目标。如果你能让你的网站看起来很难被攻破（比如添加实时攻击封锁、反自动攻击、使用数千兆位弹性带宽以及会话保护），那么黑客们肯定知难而退。

如果你能遵守《网站攻击生存手册》中列出的优秀策略，你就可以保护你的网站不受黑客攻击和竞争对手发起的网络攻击。

作者：李伯特（Robert.Li）
审阅：pnig0s、Johnson Yuan、thanks

本报告属于FreeBuf研究报告系列。FreeBuf报告针对当前网络空间面临的安全挑战展开研究并提出应对策略。所有报告均经过同行的严格审阅，以此保证研究的质量和客观性。