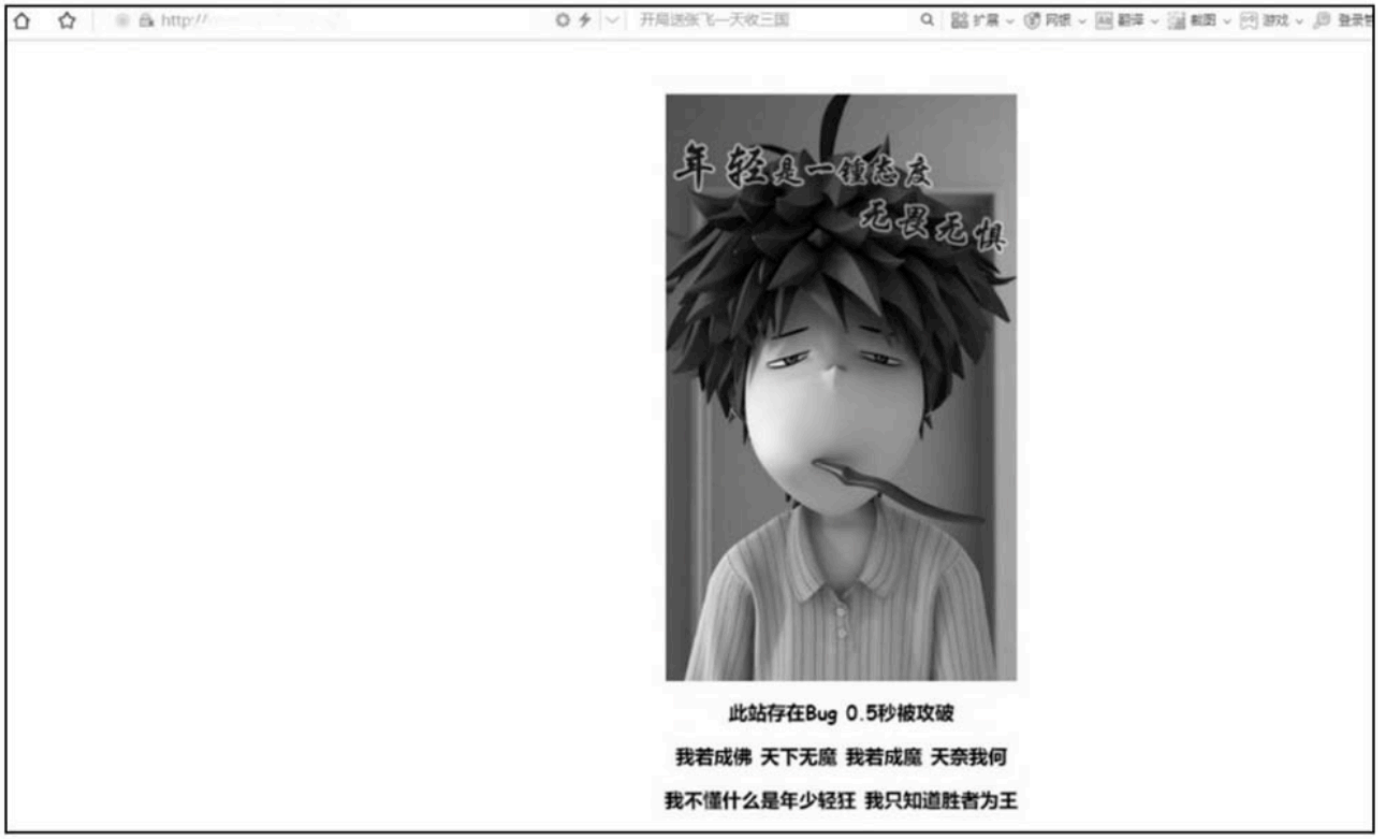
第7章　网页篡改网络安全应急响应

7.1　网页篡改概述

网页篡改，即攻击者故意篡改网络上传送的报文，通常以入侵系统并篡改数据、劫持网络连接或插入数据等形式进行。网页篡改事件想要做到预先检查和实时防范有一定难度。网页篡改攻击工具趋向简单化与智能化。由于网络环境复杂，因此导致责任难以追查。虽然目前已经有防火墙、入侵检测等安全防范手段，但各类Web应用系统的复杂性和多样性导致其系统漏洞层出不穷、防不胜防，攻击者入侵和篡改页面的事件时有发生。因此，网页防篡改技术成为信息安全领域研究的焦点之一。

7.1.1　网页篡改事件分类

网页篡改一般有明显式和隐藏式两种。明显式网页篡改指攻击者为炫耀自己的技术技巧，或表明自己的观点实施的网页篡改；隐藏式网页篡改一般是在网页中植入色情、诈骗等非法信息链接，再通过灰色、黑色产业链牟取非法经济利益。攻击者为了篡改网页，一般需提前找到并利用网站漏洞，在网页中植入后门，并最终获取网站的控制权。网页篡改方法包括文件操作类方法和内容修改类方法。文件操作类方法指攻击者用自己的Web网页文件在没有授权的情况下替换Web服务器上的网页，或在Web服务器上创建未授权的网页；内容修改类方法就是对Web服务器上的网页内容进行增、删、改等非授权操作。如图7.1.1所示，攻击者直接将网站主页修改，显示为炫耀式的图片。



7.1.2　网页篡改原因

1）攻击者获取经济利益

经济利益一直是攻击者攻击的主要动机之一，搜索引擎一般占据了互联网入口的大部分流量，我们在日常使用搜索引擎时，通常会优先选择排名靠前的搜索结果，因此有些黑色产业（网络赌博、色情等）经营者会通过与攻击者合作，购买攻陷站点来批量篡改页面，实现非法站点推广，从而获得巨大的经济利益，如图7.1.2所示。

另外，随着虚拟货币的不断发展，让很多不法分子看到了商机。攻击者会向被篡改站点网页嵌入浏览器挖矿脚本或在网站中加入一段JavaScript代码，用户通过浏览器访问这些站点时，脚本会在后台执行，并占用大量资源，出现计算机运行变慢、卡顿，CPU 利用率飙升的情况，进而使用户计算机沦为挖矿的"肉鸡"，且用户很难察觉。

2）攻击者展现能力，损坏他人形象

例如，攻击者会通过修改相关机构的门户网站主页，来展示自己的攻击能力，并损坏网站拥有者的形象。或者通过网页篡改，以权威部门的名义发布恶意或不良信息，以达到抹黑权威部门的意图。

3）通过网页篡改，实现后续其他攻击

（1）网页挂马。攻击者通过网页篡改，在Web网页中嵌入恶意脚本，从而可以实施网页挂马。

（2）水坑攻击。攻击者通过网页篡改，在Web服务器上植入攻击代码，从而实施水坑攻击。

（3）网络钓鱼。攻击者通过网页篡改，在Web网页中嵌入网络钓鱼代码，从而实施网络钓鱼。

7.1.3 网页篡改攻击手法

利用网站漏洞实现对网站主机的控制并篡改网站页面是网页篡改的主要攻击手法。

7.1.4 网页篡改检测技术

1）外挂轮询技术

用一个网页读取和检测程序，以轮询方式读出要监控的网页，与真实网页比较，来判断网页内容的完整性，对被篡改的网页进行报警和恢复。

2）核心内嵌技术

将篡改检测模块内嵌在Web服务器软件中，它在每个网页流出时都进行完整性检查，对于篡改网页进行实时访问阻断，并及时报警和恢复。

3）事件触发技术

使用操作系统的文件系统或驱动程序接口，在网页文件被修改时进行合法性检查，对于非法操作进行报警和恢复。

7.1.5 网页篡改防御方法

1）将服务器安全补丁升级到最新版

操作系统、应用程序、数据库等都需要使用最新的安全补丁，打补丁主要是为了防止攻击者利用缓冲溢出和设计缺陷等进行攻击。

2）封闭未使用但已经开放的网络服务端口及未使用的服务

对于Windows Server 2003操作系统，推荐使用TCP/IP筛选器，可以配合Windows Server 2003系统防火墙，当然也可以通过操作比较复杂的IP安全策略来实现；对于Linux系统，可以使用自带的IPTable防火墙。一般用户服务器在上架前，会做好服务器端口封闭，以及关闭不使用的服务，但不排除部分运维人员为了方便而开启服务器的端口。

3）使用复杂的管理员密码

无论是系统管理员、数据库管理员，还是FTP及网站管理员使用的密码，都需要及时维护，并将默认密码重置为复杂密码，且避免有明显的规律。

4）网站程序应设计合理并注意安全代码的编写

在设计网站目录时，应尽可能地将只需要读权限的脚本和只需要写权限的脚本分开放置，避免采用第三方不明开发插件，网站程序的名称应按照一定的规律命名，以方便识别；在编写代码时，要注意对输入串进行约束，过滤可能产生攻击的字符串，特殊权限页面要添加身份验证代码。

5）设置合适的网站权限网站权限设置包括为网站目录文件和每个网站创建一个专属的访问用户的权限。网站目录文件权限设置原则是：仅分配只写权限的目录文件，其他均为只读权限。

6）防止ARP欺骗的发生安装ARP防火墙，并手动绑定网关MAC地址等。

7.2 常规处置方法

在进行网页篡改应急响应时，通常需要由应急响应工程师借助安全设备、工具，再配合手动操作才能彻底清除黑链。当发现网页篡改时，可以使用以下处置方法。

7.2.1 隔离被感染的服务器/主机

隔离被感染的服务器/主机的目的：一是防止木马通过网络继续感染其他服务器/主机；二是防止攻击者通过已经感染的服务器/主机继续操控其他设备。有一类黑链会在内存中循环执行程序，产生大量的黑链文件。为了确保木马的控制权限，攻击者还可能会通过跳板机对内网的其他机器进行进一步入侵。所以，若不及时隔离被感染的服务器/主机，则可能导致整个局域网的服务器/主机被感染。

主要的隔离方法如下：

（1）物理隔离的方法主要为断网或断电，关闭服务器/主机的无线网络、蓝牙连接，禁用网卡，并拔掉服务器/主机上的所有外部存储设备等；

（2）对访问网络资源的权限进行严格的认证和控制。常用的操作方法是加策略和修改登录密码。

7.2.2 排查业务系统

业务系统的受影响程度直接关系着事件的风险等级。应急响应工程师应及时评估风险，并采取对应的处置措施，避免造成更大的危害。

在已经隔离被感染服务器/主机后，应对局域网内的其他机器进行排查，检查核心业务系统是否受到影响，生产线是否受到影响，并检查备份系统是否植入后门。在完成以上基本操作后，为了避免造成更大的损失，应第一时间对篡改网页时间、篡改方法、入侵路径种类等问题进行排查。

7.2.3 确定漏洞源头、溯源分析

网页被篡改后，攻击者下一步通常会进行色情、赌博等黑产资源的推广。在确认源头时，可以先在服务器文件中全盘搜索恶意关键字，如赌博、威尼斯、澳门等，然后删除被篡改的网页，再使用正常的备份文件替换。溯源分析一般是通过查看服务器/主机中保留的日志信息和样本信息展开的。

查找木马可以使用Webshell查杀工具进行全盘查杀，然后通过日志判断木马的入侵方式。如果日志被删除了，那么就需要去服务器/主机寻找相关的木马样本或可疑文件，再通过分析这些可疑的文件来判断木马的入侵途径。当然，也可以直接使用专业的日志分析工具或联系专业技术人员进行日志及样本的分析。

7.2.4 恢复数据和业务

（1）使用专业的木马查杀工具进行全盘查杀，清除遗留后门。

（2）如果有数据备份，那么可以通过还原备份数据直接恢复业务；如果没有数据备份，那么可以将网页篡改事件爆发前后被更改过的文件一并进行检查，确认是否有黑链。

7.2.5 后续防护建议

（1）对网站应用进行定期的渗透测试，及时发现安全漏洞并进行修复。

（2）使用网站监测工具进行7×24小时监测，发现篡改事件立即进行应急响应处置。

（3）定期对网站文件进行全盘Webshell扫描，防止出现后门。

7.3 错误处置方法

1）错误操作当确认网页已经被篡改后，只用备份文件恢复，没有下一步排查措施。

2）错误原理网页篡改的原因是网站存在漏洞，从而被攻击者恶意控制，如果只用备份文件恢复网页，却没有找到入侵的源头，那么可能会导致又一次地入侵与篡改。

7.4 常用工具

一般，在网页被篡改后，我们最关心的问题：一是哪些网页被篡改了，二是攻击者是怎么实现攻击的。

1）日志分析

工具要想了解攻击者是如何攻陷主机并执行篡改操作的，就需要从日志分析开始，我们可查看日志中最近登录的可疑IP地址、新增用户、新建服务等。使用观星实验室的信息采集工具，不仅可以采集操作系统的日志内容，还可以采集进程、服务、启动项、系统补丁、任务计划等多维度日志内容，通过综合分析找到可疑的攻击信息。

2）网站监控工具

使用奇安信全球鹰网站监控工具可以及时发现网站内容被篡改的现象。云监测系统在前期工作中实时监测网站篡改情况，实时输送违规信息。全球鹰云端运营团队实时监测黑链，确保当日通知用户事件详情和技术修复方案，保障用户在第一时间清楚隐患并及时修复，并会在次日下发技术报告。

7.5 技术操作指南

7.5.1 初步预判

网页篡改事件区别于其他安全事件的明显特点是：打开网页后会看到明显异常。

1）业务系统某部分网页出现异常字词

网页被篡改后，在业务系统某部分网页可能出现异常字词，例如，出现赌博、色情、某些违法App推广内容等。2019 年 4月，某网站遭遇网页篡改，首页产生大量带有赌博宣传的黑链，如图7.5.1所示。

2）网站出现异常图片、标语等

网页被篡改后，一般会在网站首页等明显位置出现异常图片、标语等。例如，政治攻击者为了宣泄不满，在网页上添加反动标语来进行宣示；还有一些攻击者为了炫耀技术，留下“Hack by 某某”字眼或相关标语，如图7.5.2所示。

吉林时时彩骗局-吉林时时彩骗局

www.[redacted] › docMecoM

2019年7月24日 - 实力团队拒绝收费. 微信号：xyzd578. QQ号：3003348767. 微信号：xycp1129. 复制微信. 微信号：xycp1129. 添加微信. 加导师微信，免费领取精准 ...

www,mg,4355con - 利群网

www.[redacted] › pocwg89

1月9日至10日，公安部在京召。开全国公安机关公交车安全防范工作现场经验交流会，部署各地公安机关总。结工作经验、分析研判形势，大力宣传推广北京等地新经验 ...

神州彩票信誉度怎么样 - 利群网

w[redacted] ...

2019年7月21日 - 一带一路"最重要的目标就是通过促进民心相通，构。建人类命运共同体，这就需要国际社会在人文科学领域广泛交流、达成共识。。。神州彩票信誉度 ...

玩游戏斗地主赚钱 - 利群网

www.[redacted] › docJRBFNryg235

Your IP address is: [redacted](111031203). The IP Location is not in our service range. We are sorry for the inconvenience. If you have any questions, please ...

7.5.2 系统排查

网页被恶意篡改是需要相应权限才能执行的，而获取权限主要有三种方法：一是通过非法途径购买已经泄露的相应权限的服务器账号；二是使用恶意程序进行暴力破坏，从而修改网页；三是入侵网站服务器，进而获取操作权限。应对网页篡改事件进行的系统排查如下。

1.异常端口、进程排查

初步预判为网页篡改攻击后，为了防止恶意程序定时控制和检测网页内容，需要及时发现并停止可疑进程，具体步骤如下。

（1）检查端口连接情况，判断是否有远程连接、可疑连接。

（2）查看可疑的进程及其子进程。重点关注没有签名验证信息的进程，没有描述信息的进程，进程的属主、路径是否合法，以及CPU或内存资源长期占用过高的进程。

2.可疑文件排查

发现可疑进程后，通过进程查询恶意程序。多数的网页篡改是利用漏洞上传Webshell文件获取权限的，因此也可以使用D盾工具进行扫描。若发现Webshell文件，则可以继续对Webshell进行排查（参考第6章）。

3.可疑账号排查

攻击者为了实现长期对网站的控制，多数会获取账号或建立账号。因此，我们可以对网站服务器账号进行重点查看，一方面是查看服务器是否有弱密码，远程管理端口是否对公网开放，从而防止攻击者获取密码，控制原有系统账号；另一方面是查看服务器是否存在新增、隐藏账号。

4.确认篡改时间

为了方便后续的日志分析，此时需要确认网页篡改的具体时间。可以查看被篡改服务器的日志文件access.log，确认文件篡改大致时间。如图7.5.3所示，可知最后修改时间为2019年10月21日5时51分27秒，因此网页篡改时间在这个时间之前。

7.5.3 日志排查

1.系统日志

1）Winodws系统

（1）系统：查看是否有异常操作，如创建任务计划、关机、重启等。

（2）安全：查看各种类型的登录日志、对象访问日志、进程追踪日志、特权使用、账号管理、策略变更、系统事件等。安全也是调查取证中最常用到的日志。

（3）应用：查看由应用程序或系统程序记录的事件，例如，数据库程序可以在应用程序日志中记录文件错误，程序开发人员可以自行决定监视哪些事件。如果某个应用程序出现崩溃情况，那么可以从应用程序日志中找到相应的记录，有助于解决问题。

2）Linux系统

Linux系统拥有非常灵活和强大的日志功能，可以保存用户几乎所有的操作记录，并可以从中检索出需要的信息，主要查看的日志如下。（1）/var/log/messages：查看是否有异常操作，如sudo、su等命令执行。

（2）/var/log/secure：查看是否有异常登录行为。

（3）last（命令）：查看最近登录行为。

（4）lastb（命令）：查看是否有错误登录行为。

（5）/var/log/audit：查看是否有敏感命令的操作。

（6）/var/spool/mail：查看是否有异常的邮件发送历史。

（7）.bash_history：查看是否有异常的命令执行记录。

2.Web日志

Web日志记录了Web服务器接收处理请求及运行错误等各种原始信息。通过Web日志可以清楚知晓用户的IP地址、何时使用的操作系统、使用什么浏览器访问了网站的哪个页面、是否访问成功等。通过对Web日志进行安全分析，可以还原攻击场景，如图7.5.4所示。

1）Windows系统

（1）查找IIS日志，常见的IIS日志存放在目录“C：\inetpub\logs\LogFiles”下（如果未找到，可通过IIS配置查看日志存放位置）。

（2）查找与文件篡改时间相关的日志，查看是否存在异常文件访问。[插图]图7.5.4　对Web日志进行安全分析

（3）若存在异常文件访问，则确认该文件是正常文件还是后门文件。

2）Linux系统

（1）查找Apache和Tomcat日志，常见存放位置如下。Apache日志位置：/var/log/httpd/access_log。Tomcat日志位置：/var/log/tomcat/access_log。

（2）通过使用【cat】命令，可查找与文件篡改时间相关的日志，查看是否存在异常文件访问。

（3）若存在异常文件访问，则确认该文件是正常文件还是后门文件。

3.数据库日志

1）MySQL数据库日志

（1）使用【show variables like 'log_%'；】命令，可查看是否启用日志。

（2）使用【show variables like 'general_log_file'；】命令，可查看日志位置。

（3）通过之前获得的时间节点，在query_log中查找相关信息。

2）Oracle数据库日志

（1）若数据表中有Update时间字段，则可以作为参考；若没有，则需要排查数据日志来确定内容何时被修改。

（2）使用【select * from v$logfile；】命令，可查询日志路径。

（3）使用【select * from v$sql】命令，可查询之前使用过的SQL

7.5.4 网络流量排查

通过流量监控系统，筛选出问题时间线内所有该主机的访问记录，提取IP地址，在系统日志、Web日志和数据库日志中查找该IP地址的所有操作。

7.5.5 清除加固

（1）对被篡改网页进行下线处理。根据网页被篡改的内容及影响程度，有针对性地进行处置，如果影响程度不大，篡改内容不多，那么可先将相关网页进行下线处理，其他网页正常运行，然后对篡改内容进行删除恢复；如果篡改网页带来的影响较大，被篡改的内容较多，那么建议先对整个网站进行下线处理，同时挂出网站维护的公告。

（2）如果被篡改的内容较少，那么可以手动进行修改恢复；如果被篡改的内容较多，那么建议使用网站定期备份的数据进行恢复。当然，如果网站有较新的备份数据，那么无论篡改内容是多是少，推荐进行网站覆盖恢复操作（覆盖前对被篡改网站文件进行备份，以备后续使用），避免有未发现的篡改数据。（3）如果网站没有定时备份，那么就只能在一些旧的数据的基础上，手动进行修改、完善。因此，对网站进行每日异地备份，是必不可少的。

（4）备份和删除全部发现的后门，完成止损。

（5）通过在access.log中搜索可疑IP地址的操作记录，可判断入侵方法，修复漏洞。