北京师范大学-香港浸会大学联合国际学院

网络安全事件专项应急预案

目录

一、总则

为提高学校网络与信息系统处理突发事件的能力，形成科学、有效、反应迅速的应急工作机制，减轻或消除突发事件的危害和影响，确保学校信息系统安全运行，最大限度地减少网络与信息安全突发公共事件的危害，特制定本预案。

本预案适用于学校信息系统安全突发事件的应急响应。当发生信息安全事件时，针对不同类型的事件，启动专项应急处置措施。

二、重要事件专项应急处置措施

2.1 信息篡改（含信息窃取）类攻击事件专项应急处置措施

2.1.1 事件描述

是指未经授权将信息系统中的信息窃取，或者更换为攻击者所提供的信息而导致的信息安全事件，网页被篡改是最常见的一类信息篡改安全事件。

2.1.2 事件识别与检测

- **事件识别**

信息篡改（含信息窃取）类攻击事件，一般可从攻击特性、影响程度、原始告警信息三方面识别，详见下表：

攻击特性	影响	原始告警信息举例
利用恶意文件上传、SQL 注入的非正常查询；系统漏洞或后门程序；	造成信息篡改（含信息窃取）	应用的检测：WEB 服务器日志发现大量异常的请求； 重要文件被改动，例如：WEB 页面； 出现名字异常的文件和目录，例如：以点开头的文件或目录等； IDS 的告警：出现 SQL 注入攻击告警 系统层面的现象：系统配置发生异常变动，包括：进程和服务异常变动；系统开放了异常的端口；系统异常重起、关闭；系统日志被修改，日志策略发生变动；系统出现新的管理员账

		户。 一些重要文件的属性、时间戳、权限线被修改，包括：可执行程序、系统内核、动态连接库、配置文件，以及其它的重要数据。 异常的账号使用，例如：空闲账户和系统账户的使用；平常账户执行异常命令。

安全设备检测

- 态势感知：控制台-->处置中心-->安全事件视角-->详情模式-->在筛选界面“事件类型”勾选“信息破坏事件”;
- 深信服云眼：业务检测-->篡改监测

- **事件检测**

必须对业务系统、IDS、防火墙、应用系统进行定期维护和日志审计，及时发现黑客通过网页遍历、SQL 注入、漏洞扫描、暴力破解、溢出攻击等方式攻击网站的行为，重点关注以下告警：

- 分析 web 应用日志,确认有无恶意文件上传、SQL 注入的非正常查询;
- 分析系统日志，确认主机上有无异常权限用户非法登陆，并记录其 IP 地址、登陆时间等信息;

针对 windows 系统：

- 可以通过“事件管理器”查看。建议日志的文件大小不小于 100M。
- 安全日志文件：%systemroot%\system32\config\SecEvent.EVT
- 检查端口与网络连接： Netstat.exe 是一种命令行实用工具，可以显示 TCP 和 UDP 的所有打开的端口;
- 检查系统帐户：可以在“计算机管理”—“客户管理”中查看系统帐号;
- 可以使用命令查看：net user ； net localgroup administrators;

- 查找恶意进程：方法：任务管理器（系统工具） Psinfo.exe（第三方工具）；
- 监视已安装的服务和驱动程序。

针对 unix 系统：

- 使用 w 命令查看 utmp 日志，获得当前系统正在登录帐户的信息及来源
- 使用 last 命令查看 wtmp 日志，获得系统前 N 次登录记录
- 分析系统目录以及搜索全盘近期被修改的和新创建的文件，查找是否存在可疑文件和后门程序；
- Su 命令日志，记录了每一次执行 su 命令的动作：时间日期，成功与否，终端设备，客户 ID.有些 UNIX 具有单独的 su 日志，有些则保存在 syslog 中；
- Cron 日志记录了定时作业的内容，通常在/var/log/cron 或默认日志目录中一个称为 cron 的文件里；
- 分析系统服务、进程、端口等，确认有无可疑项；
- Netstat －an 列出所有打开的端口及连接状态；
- Lsof －i 只显示网络套接字的进程；
- Ps －ef 会列出系统正在运行的所有进程。

结合上述日志审计，确定攻击者的方式、以及入侵后所获得的最大管理权限和是否对被攻击服务器留有后门程序和嗅探程序等。

2.1.3 事件处置

- 安全设备处置流程

- 防火墙：策略-->应用控制策略-->新增-->新增应用控制策略-->源 IP（受害 IP）至目的 IP（any），动作禁止；
- 深信服云图：云图公众号首页-->我的-->一键断网工具-->选择需要断网的 IP 地址-->点击确定；

- 紧急处理措施

  a) 进行系统临时性恢复，迅速恢复系统被篡改的内容；

  b) 需要根据具体应用细化恢复方式，包括数据库恢复或页面文件恢复；

  c) 严格监控对系统的业务访问以及服务器系统登陆情况，确保对再次攻击的行为能进行检测。

- 针对 windows 系统

  - 可以通过“事件管理器”查看。建议日志的文件大小不小于 100M。
  - 安全日志文件：%systemroot%\system32\config\SecEvent.EVT

针对 unix 系统：

- 使用 w 命令查看 utmp 日志，获得当前系统正在登录帐户信息及来源
- 使用 last 命令查看 wtmp 日志，获得系统前 N 次登录记录
- 必要情况下可考虑将发生安全事件的设备脱网，做好安全审计及系统恢复准备；

- 抑制处理措施

  a) 安置好取证工作环境，进行攻击分析，包括：取证采样（包括前一时段的防火墙日志、入侵检测日志、路由器日志等）、流量特征分析、报文特征分析及其他分析，确定攻击方式、类型等；

  b) 给易受攻击的系统打上补丁，保持补丁的有效；

  c) 对系统进行安全加固；

  d) 修改所有系统密码和应用密码；

  e) 更新防病毒软件

f） 根除措施：

g） 进一步深入监控和分析业务系统、IDS、防火墙、应用程序日志，采取更准确而针对性的处置措施，然后继续观察处置措施的效果，同时进一步寻找更有效和根本的解决措施，直至确认危险解除；

- 恢复措施

a） 消除攻击源后，验证相关服务的运行情况；

b） 进行业务测试，确定系统完全恢复；

c） 系统上网运行；

2.2 计算机病毒（木马）类攻击事件专项应急处置措施

2.2.1 事件描述

计算机病毒指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

特洛伊木马（简称木马）是一种隐藏在计算机系统中不为所知的恶意程序，通常用于潜伏在计算机系统中来与外界连接，并接受外界的指令。被植入木马的计算机会被外界所控制，也可能会被利用作为攻击其它系统的攻击源。

攻击者利用计算机病毒（木马）实施攻击行为，从而影响信息系统正常运行为目的的信息安全事件，定义为计算机病毒（木马）类攻击事件。

2.2.2 事件识别与检测

病毒木马类攻击事件，一般可从攻击特性、影响程度、原始告警信息三方面识别，详见下表：

攻击特性	影响	原始告警信息举例
特洛伊木马（简称	被植入木马的	防病毒系统的告警：防病毒软件产生病毒

木马）是一种隐藏在计算机系统中不为所知的恶意程序，通常用于潜伏在计算机系统中来与外界连接，并接受外界的指令；	计算机会被外界所控制，也可能会被利用作为攻击其它系统的攻击源；	报警，标识出发现病毒的主机名、IP 地址、病毒类型、感染时间等信息，可作为感染病毒的明确标识； IDS 的告警：出现病毒程序相关的攻击告警信息； 操作系统的检测：无法在计算机上安装反病毒程序，或安装的反病毒程序无法运行；Windows 下用任务管理器查看现有进程，Linux 下 Ps －ef 列出系统正在运行的所有进程，发现不明进程正在运行；以 netstat －naple 查看进程和端口的绑定情况，发现异常的端口或者进程正在进行网络连接。

- 安全设备检测
  - 态势感知：控制台-->处置中心-->安全事件视角-->详情模式-->在筛选界面“事件类型”勾选“特洛伊木马时间”和“计算机病毒事件”；
  - 深信服 EDR：EDR 控制台-->威胁检测-->终端病毒查杀-->全盘查杀-->选择终端-->扫描模式选择“均衡”-->点击确定；
- 事件检测

通过计算机病毒（木马），能对系统数据进行破坏，受攻击系统将会出现系统不能正常运行、死机、CPU 占用率过高、内存占用率过高等种种现象。

对于此类攻击方式，可通过以下方法检测：

- 将杀毒软件更新到最新版本，病毒库更新到最新版本，对全盘进行病毒扫描；
- 使用资源管理器（Solaris 使用 ps －aux 命令）检查当前内存、CPU 等资源占用情况；
- 检测系统进程和快照对比，找出非法进程；
- 检测网络连接和快照对比，找出可疑的的网络连接。

2.2.3 事件处置

- 安全设备处置流程
  - 深信服 EDR：EDR 控制台-->响应中心-->威胁响应-->威胁事件视角-->输入主机地址-->勾选对应的“病毒木马”事件-->点击“一键处置”；
  - 防火墙：策略-->应用控制策略-->新增-->新增应用控制策略-->源 IP（受害 IP）至目的 IP（any），动作禁止；
- 紧急处理措施

a) 断开被感染的服务器网络；

b) 启用备用服务器；

c) 通过在防火墙或网络设备设置访问控制策略，限制外部的访问。

d) 抑制处理措施

e) 安置好取证工作环境，进行攻击分析，包括：取证采样（包括前一时段的防火墙日志、入侵检测日志、路由器日志等）、流量特征分析、报文特征分析及其他分析，确定攻击方式、类型等；

f) 在问题主机上，确定病毒（木马）代码特征：进程、端口等，通

常以 netstat －naple 查看进程和端口的绑定情况，分析出异常的端口或者进程；

g) Windows 下用任务管理器查看现有进程，Linux 下 Ps －ef 会列出系统正在运行的所有进程，一般先停止恶意进程，同时将其相关文件删除。

- 根除措施

a) 更新防病毒软件病毒库；

b) 更新系统补丁及漏洞修补程序；

c) 使用反病毒软件进行查杀，清除病毒（木马）；

d) 确认病毒类型后，下载专杀工具进行病毒清理；

e) 更新防火墙安全策略，将病毒网络数据包进行过滤。

- 恢复措施

a) 消除攻击源后，验证相关服务的运行情况；

b) 进行业务测试，确定系统完全恢复；

c) 木马被完全清除后，系统上网运行。

2.3 僵尸网络类攻击事件专项应急处置措施

2.3.1 事件描述

僵尸网络是指采用一种或多种传播手段，将大量主机感染 bot 程序（僵尸程序），从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。攻击者通过各种途径传播僵尸程序感染互联网上的大量主机，而被感染的主机将通过一个控制信道接收攻击者的指令，组成一个僵尸网络。

攻击者利用僵尸网络实施分布式拒绝服务（DDos）攻击、消耗网络资源、发

送垃圾数据等攻击行为，从而影响信息系统正常运行为目的的信息安全事件，定义为僵尸网络类攻击事件。

2.3.2 事件识别与检测

僵尸网络类攻击事件，一般可从攻击特性、影响程度、原始告警信息三方面识别，详见下表：

攻击特性	影响	原始告警信息举例
将大量主机感染 bot 程序（僵尸程序），从而在控制者和被感染主机之间所形成的一个可一对多控制的网络；	攻击者利用僵尸网络实施分布式拒绝服务（DDos）攻击、消耗网络资源、发送垃圾数据等攻击行为。	防病毒系统的告警：防病毒软件产生病毒报警，标识出发现病毒的主机名、IP 地址、病毒类型、感染时间等信息，可作为感染病毒的明确标识； IDS 的告警：出现僵尸程序相关的攻击告警信息； 防火墙日志：源地址发送的数据包，数量非常多，或者数据包的大小非常大； 操作系统的检测：受攻击服务器某端口建立 TCP 连接，已完成三次握手，但是客户端不结束连接，消耗服务器连接资源，造成正常用户很难访问此服务器。

- 安全设备检测

- 态势感知：控制台-->处置中心-->安全事件视角-->详情模式-->在筛选界面“事件类型”勾选“僵尸网络事件”

- 防火墙：监控-->安全日志-->僵尸网络

- 事件检测

1. 针对主机的僵尸网络攻击检测方法：

攻击者可以利用主机系统漏洞、电子邮件或者其他方式入侵主机，下载运行僵尸网络程序，使主机变为一台僵尸网络中的受控制的僵尸主机。

- 如果系统服务无法正常运行，查看杀毒软件报警日志，查看主机中存在可疑文件；

- 在主机系统中查看系统进程，并使用 netstat 命令，通过网络端口号确定非法进程网络连接；

- 在命令行（cmd.exe）里输入“netstat-an”命令，如果出现本地 IP 向多个目标 IP 的相同端口（如 135，445）发起连接的现象，则很可能是僵尸网络程序的扫描行为。发现扫描后，可以用端口与进程对应工具，如 fport.exe，找到扫描进程，从而发现可疑的僵尸网络程序；

- 根据 TCP 数据报文的内容发现可疑僵尸网络，可疑的数据报文包含 udp、syn、ddos、http://、download、.exe、update、scan、exploit、login、logon、advscan、lsass、dcom、beagle、dameware 等。

2. 针对网络协议的僵尸网络攻击检测方法：

攻击者利用僵尸网络可以针对网络协议某些特性发动拒绝服务攻击，协议类攻击是以发起大量连接或数据包为基础，造成被攻击方连接队列耗尽或 cpu、内存资源的耗尽。此类攻击为最常见。比如：syn flood。

- 对于 SYN-FLOOD 攻击，可通过利用 netstat －an 命令（适用于 Windows/Unix 系统），能发现当前活动连接的状态中存在大量的

SYN_RECEIVED 状态包，这表明系统正受到 SYN-FLOOD 拒绝服务攻击；

- 通过使用 SNIFFER，如果发现大量非正常网络连接，或协议的非正常分布，如 icmp 或 UDP 协议数据超过总流量的 20%；表明系统正在受到僵尸网络攻击。

3. 针对应用类服务的僵尸网络攻击检测方法：

应用类，主要是指针对 web 服务发起的攻击，表现在分布式的大量 http 请求，以耗尽 web 服务的最大连接数或者消耗数据库资源为目的。比如：对某一大页面的访问或者对某一页面的数据库搜索。

- 通过登陆 http 页面，确定是否可以正常提供 http 服务。如果页面显示缓慢或者无法显示，表明系统正在受到僵尸网络攻击；
- 在防火墙设备上查看 NAT 访问信息及流量，确定访问源地址及服务端口，如果访问源地址存在一定的规律性，表明系统正在受到僵尸网络攻击；
- 通过网络流量分析软件，确定数据包类型特征，比如利用的是 UDP、TCP 还是 ICMP 协议。

2.3.3 事件处置

- 安全设备处置流程
  - 防火墙：策略-->应用控制策略-->新增-->新增应用控制策略-->源 IP（受害 IP）至目的 IP（any），动作禁止；
- 紧急处理措施

a） 确定僵尸网络程序源头，即定位到哪个机房的哪台机器；

b） 必要情况下切换备机，断网隔离；

c） 通过在防火墙或网络设备设置访问控制策略，限制外部的访问。

- 抑制处理措施

d） 在问题主机上，确定僵尸网络程序特征：进程、端口等，通常以 netstat －naple 查看进程和端口的绑定情况，分析出异常的端口或者进程；

e） 僵尸网络程序，一般先停止僵尸网络程序，同时将其相关文件删除；

f） 用 msconfig 查看现行进程；

g） Windows 下用任务管理器查看现有进程；

h） Linux 下 Ps －ef 会列出系统正在运行的所有进程；

i） 僵尸网络程序程序。

- 根除措施

a） 进一步采取更准确而针对性的处置措施，然后继续观察处置措施的效果，同时进一步寻找更有效和根本的解决措施，直至确认危险解除；

b） 消除攻击源后，验证相关服务的运行情况；

c） 进行业务测试，确定系统完全恢复。

2.4 恶意代码类攻击专项应急处置措施

2.4.1 事件描述

恶意代码是一种程序，它通过把代码在不被察觉的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据、运行具有入侵性或破坏性的程序、破坏被感

染电脑数据的安全性和完整性的目的。

攻击者利用恶意代码实施攻击行为，从而影响信息系统正常运行为目的的信息安全事件，定义为恶意代码类攻击事件。

2.4.2 事件识别与检测

恶意代码类攻击事件，一般可从攻击特性、影响程度、原始告警信息三方面识别，详见下表：

攻击特性	影响	原始告警信息举例
通过把代码在不被察觉的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据、运行具有入侵性或破坏性的程序；	破坏被感染电脑数据的机密性和完整性，导致信息系统不能正常运行或瘫痪。	防病毒系统的告警：防病毒软件产生恶意代码报警，标识出发现恶意代码的主机名、IP地址、恶意代码类型、感染时间等信息，可作为感染恶意代码的明确标识； IDS 的告警：出现恶意代码相关的攻击告警信息； 操作系统的检测：无法在计算机上安装反病毒程序，或安装的反病毒程序无法运行；屏幕上出现奇怪的对话框或消息框，扬声器中意外放出奇怪的声音或乐曲；系统意外地自动重新启动；系统出现新的程序不是由您安装的，或者与任何最近安装的程序都不关联。

- 安全设备检测流程

  - 态势感知：控制台-->处置中心-->安全事件视角-->详情模式-->在筛选界面“事件类型”勾选“网页内嵌恶意代码事件”。

- 事件检测

通过恶意代码，能对系统数据进行破坏，受攻击系统将会出现系统不能正常运行、死机、CPU 占用率过高、内存占用率过高、浏览器设置被更改等种种现象。对于此类攻击方式，可通过以下方法检测：

- 将防病毒软件更新到最新版本，病毒库更新到最新版本，对全盘进行病毒扫描；
- 使用资源管理器（Solaris 使用 ps －aux 命令）检查当前内存、CPU 等资源占用情况；
- Windows 下用任务管理器查看现有进程，Linux 下 Ps －ef 列出系统正在运行的所有进程，发现不明进程正在运行；
- 以 netstat －naple 查看进程和端口的绑定情况，发现异常的端口或者进程正在进行网络连接；

浏览器被劫持，现象包括但不限于：默认主页被修改、主页设置被屏蔽锁定，且设置选项无效不可更改、默认的 IE 搜索引擎被修改、IE 标题栏被添加非法信息、鼠标右键菜单被添加非法网站链接、鼠标右键弹出菜单功能被禁用失常、IE 收藏夹被强行添加非法网站的地址链接、在 IE 工具栏非法添加按钮、锁定地址栏的下拉菜单及其添加文字信息、IE 菜单“查看”下的“源文件”项被禁用等。对于此类攻击方式，可通过以下方法检测：

- 检测系统进程和快照对比，找出非法进程；
- 检测网络连接和快照对比，找出可疑的网络连接；
- 查看浏览器设置，检查是否设置被修改；
- 连接网络过程中，检查是否会被重定向到并不想访问的网站，或者下载不明文件。

2.4.3 事件处置

- 安全设备处置流程

  防火墙：策略-->应用控制策略-->新增-->新增应用控制策略-->源 IP（受害 IP）至目的 IP（any），动作禁止；

- 紧急处理措施

  a) 断开被感染的服务器网络；

  b) 启用备用服务器；

  c) 通过在防火墙或网络设备设置访问控制策略，限制外部的访问。

- 抑制处理措施

  a) 安置好取证工作环境，进行攻击分析，包括：取证采样（包括前一时段的防火墙日志、入侵检测日志、路由器日志等）、流量特征分析、报文特征分析及其他分析，确定攻击方式、类型等；

  b) 在问题主机上，确定恶意代码的代码特征：进程、端口等，通常以 netstat －naple 查看进程和端口的绑定情况，分析出异常的端口或者进程；

  c) Windows 下用任务管理器查看现有进程，Linux 下 Ps －ef 会列出系统正在运行的所有进程，一般先停止恶意进程，同时将其相关文件删除；

  d) 对于 Windows 系统，当运行 IE 时，点击“工具→Internet 选项→安全→ Internet 区域的安全级别”,把安全级别由“中”改为“高”。

  e) 对于 Windows 系统，IE 窗口中点击“工具”→“Internet 选项”，在弹出的对话框中选择“安全”标签，再点击“自定义级别”按钮，就会弹出“安全设置”对话框，把其中所有 ActiveX 插件和控件以

及与 Java 相关全部选项选择“禁用”。

- 根除措施

a） 更新防病毒软件病毒库；使用反病毒软件进行查杀，清除恶意代码；

b） 确认恶意代码类型后，下载专杀工具进行恶意代码清理；

c） 更新防火墙安全策略，将恶意代码网络数据包进行过滤；

d） 更新系统补丁及漏洞修补程序。

- 恢复措施

a） 消除攻击源后，验证相关服务的运行情况；

b） 进行业务测试，确定系统完全恢复；

c） 确定恶意代码完全清除后系统上网运行。

2.5 间谍软件类攻击事件专项应急处置措施

2.5.1 事件描述

间谍软件通常被泛泛的定义为从计算机上搜集信息，并在未得到该计算机用户许可时便将信息传递到第三方的软件，包括监视击键，搜集机密信息（密码、信用卡号、PIN 码等），获取电子邮件地址，跟踪浏览习惯等。它能够在不知情的情况下，在其电脑上安装后门，收集用户信息，获取用户的软硬件配置等，并发送出去用于商业目的。间谍软件还不可避免的影响网络性能，减慢系统速度，进而影响整个商业进程。

攻击者利用间谍软件实施攻击行为，从而影响信息系统正常运行为目的的信息安全事件，定义为间谍软件类攻击事件。

2.5.2 事件识别与检测

间谍软件类攻击事件，一般可从攻击特性、影响程度、原始告警信息三方面

识别，详见下表：

攻击特性	影响	原始告警信息举例
攻击者利用间谍软件实施攻击行为，从而窃取信息系统上存储的重要数据。	未得到该计算机用户许可时便将信息传递到第三方的软件，包括监视击键，搜集机密信息（密码、信用卡号、PIN 码等），获取电子邮件地址，跟踪浏览习惯等。	防病毒系统的告警：防病毒软件产生病毒报警，标识出发现病毒的主机名、IP 地址、病毒类型、感染时间等信息，可作为感染病毒的明确标识； IDS 的告警：出现病毒相关的攻击告警信息； 操作系统的检测：计算机上发现来源不明的软件或进程；木马查杀软件发现恶意程序或木马等；来源不明的软件无法卸载、主机弹出广告等种种现象。无法在计算机上安装反病毒程序，或安装的反病毒程序无法运行；系统出现新的程序不是由您安装的，或者与任何最近安装的程序都不关联；

- 安全设备检测流程
  - 态势感知：控制台-->处置中心-->安全事件视角-->详情模式-->在筛选界面“事件类型”勾选“间谍软件”
- 事件检测

通过间谍软件，能对系统数据进行破坏，受攻击系统将会出现系统不能正常运行、死机、CPU 占用率过高、内存占用率过高、软件无法卸载、弹出广告等种

种现象，可通过以下手段进行检测：

- 将防病毒软件更新到最新版本，病毒库更新到最新版本，对全盘进行病毒扫描；
- 使用资源管理器（Solaris 使用 ps －aux 命令）检查当前内存、CPU 等资源占用情况；
- 检测系统进程和快照对比，找出非法进程；
- 检测网络连接和快照对比，找出可疑的网络连接；
- 查看系统安装程序列表，是否有未经允许安装的不明程序；
- 软件卸载的过程中，检查是否有无法卸载的不明程序；
- 检查系统是经常否弹出广告；
- 检查在进行搜索的过程中，是否通过某种手段改变搜索结果，有目的地把搜索结果指向一个错误的地方。

2.5.3 事件处置

- 安全设备处置流程
  - 防火墙：策略-->应用控制策略-->新增-->新增应用控制策略-->源 IP（受害 IP）至目的 IP（any），动作禁止；
- 紧急处理措施

a) 断开被感染的服务器网络；

b) 启用备用服务器；

c) 通过在防火墙或网络设备设置访问控制策略，限制外部的访问。

d) 抑制处理措施

e) 安置好取证工作环境，进行攻击分析，包括：取证采样（包括前一时段的防火墙日志、入侵检测日志、路由器日志等）、流量特征分析、报文特征分析及其他分析，确定攻击方式、类型等；

f) 在问题主机上，确定间谍软件的代码特征：进程、端口等，通常以 netstat －naple 查看进程和端口的绑定情况，分析出异常的端口或者进程；

g) Windows 下用任务管理器查看现有进程，Linux 下 Ps －ef 会列出系统正在运行的所有进程；

h) 先停止间谍软件进程，然后将其相关文件删除；对于 Windows 系统，进入安全模式，确认间谍软件的位置，进行手动删除。

- 根除措施

a) 更新防病毒软件病毒库；

b) 更新系统补丁及漏洞修补程序；

c) 使用反病毒软件进行查杀，清除间谍软件；

d) 确认间谍软件类型后，下载专杀工具进行间谍软件清理；

e) 更新防火墙安全策略，将间谍软件网络数据包进行过滤。

- 恢复措施

a) 消除攻击源后，验证相关服务的运行情况；

b) 进行业务测试，确定系统完全恢复；

c) 确定间谍软件完全清除后系统上网运行。

2.6 数据库注入类攻击安全事件专项应急处置措施

2.6.1 事件描述

SQL 注入攻击，就是攻击者把 SQL 命令插入到 Web 表单的输入域或页面请求的查询字符串，欺骗服务器执行恶意的 SQL 命令。在某些表单中，输入的内容直接用来构造（或者影响）动态 SQL 命令，或作为存储过程的输入参数，比如典型的攻击类型是在 newsid 变量后加后 sql 语句：exec xp_cmdshell ‘net user’，这样就执行了一个加用户的命令了。

2.6.2 事件识别与检测

SQL 注入攻击特征虽然千变万化，但攻击造成某种现象相对一致，常见的特征匹配技术不可能完全识别所有变种攻击，仅能识别其中很小一部分，如下图所示：

从上图的例子中不难看出，只要随便把 1 改成其他任意数字，就是一次 SQL 注入的变种攻击。在这种情况下，可见采用这种方法来防御 SQL 注入攻击存在一定的局限性。

- 安全设备检测
  - 态势感知：控制台-->处置中心-->安全事件视角-->详情模式-->在筛选界面“事件类型”勾选“SQL 注入”和“系统命令注入”
  - 防火墙：监控-->安全日志-->WEB 应用防护

- 事件检测
- 检查 SQL 注入的手段

1） 使用参数化的过滤性语句

要防御 SQL 注入，用户的输入就绝对不能直接被嵌入到 SQL 语句中。用户的输入必须进行过滤，或者使用参数化的语句。参数化的语句使用参数而不是将用户输入嵌入到语句中。在多数情况中，SQL 语句就得以修正。然后，用户输入就被限于一个参数。下面是一个使用 Java 和 JDBC API 例子：

```
PreparedStatement prep = conn.prepareStatement("SELECT * FROM USERS WHERE PASSWORD=?");

prep.setString(1, pwd);
```

避免使用解释程序，因为这正是黑客们借以执行非法命令的手段。

防范 SQL 注入，还要避免出现一些详细的错误消息，因为黑客们可以利用这些消息。要使用一种标准的输入确认机制来验证所有的输入数据的长度、类型、语句、企业规则等。

2） 使用专业的漏洞扫描工具

一个完善的漏洞扫描程序不同于网络扫描程序，它专门查找网站上的 SQL 注入式漏洞。最新的漏洞扫描程序可以查找最新发现的漏洞。

总体上，有两种方法可以保证应用程序不易受到 SQL 注入的攻击，一是使用代码复查，二是强迫使用参数化语句。强迫使用参数化的语句意味着嵌入用户输入的 SQL 语句在运行时将被拒绝。

- SQL 注入攻击的检测方法有：

1） 安装 ids

在 ids 过滤规则当中定义上’xp_cmdshell’、’net user’。当 ids 发现 web 数据中有 xp_cmdshell 等字样时就会产生报警。那么这就是 sql 注入攻击了。

2） 安装 sniffer

在过滤规则中定义上’xp_cmdshell’、’net user’。当 sniffer 数据中发现 web 数据中有 xp_cmdshell 等字样时那么这就是 sql 注入攻击了。

3） 检测 web 日志

在 web 日志中如果存在 xp_cmdshell 那么就说明有 sql 注入攻击，但值得注意的是如果黑客是 post 请求方式进行注入的话，那么日志中就不会有注入的记录。

2.6.3 事件处置

- 安全设备处置流程
  - 防火墙：策略-->应用控制策略-->新增-->新增应用控制策略-->源 IP（受害 IP）至目的 IP（any），动作禁止；
- 紧急处理措施

a） 启动系统恢复，将网站恢复到没有被注入的状态

b） 确认向网站发起攻击的 IP；

c） 在边界路由器或防火墙上对发起攻击的 IP 进入流量进行过滤

d） 修补 SQL 注入点

- 抑制处理措施

a） 安置好取证工作环境，进行攻击分析，包括：取证采样（包括前一时段的防火墙日志、入侵检测日志、路由器日志等）、流量特征分析、报文特征分析及其他分析，确定攻击方式、类型等；

b) 给易受攻击的系统打上补丁，保持补丁的有效；

c) 修改所有系统密码和应用密码；

d) 更新防病毒软件

e) 对网页进行安全加固，修补 SQL 注入点，可利用表单输入的内容构造 SQL 命令之前，把所有输入内容过滤，具体措施如下：

1) 对于动态构造 SQL 查询的场合，可以使用下面的技术：

■ 替换单引号，即把所有单独出现的单引号改成两个单引号，防止攻击者修改 SQL 命令的含义。再来看前面的例子，“SELECT * from Users WHERE login = ''' or ''1''=''1' AND password = ''' or ''1''=''1'”显然会得到与“SELECT * from Users WHERE login = '' or '1'='1' AND password = '' or '1'='1'”不同的结果。

■ 删除输入内容中的所有连字符，防止攻击者构造出类如“SELECT * from Users WHERE login = 'mas' -- AND password =''”之类的查询，因为这类查询的后半部分已经被注释掉，不再有效，攻击者只要知道一个合法的用户登录名称，根本不需要知道用户的密码就可以顺利获得访问权限。

■ 对于用来执行查询的数据库帐户，限制其权限。用不同的帐户执行查询、插入、更新、删除操作。由于隔离了不同帐户可执行的操作，因而也就防止了原本用于执行 SELECT 命令的地方却被用于执行 INSERT、UPDATE 或 DELETE 命令。

2) 用存储过程来执行所有的查询。

■ SQL 参数的传递方式将防止攻击者利用单引号和连字符实施攻击。此外，它还使得数据库权限可以限制到只允许特定的存储过程执行，所有的输入必须遵从被调用的存储过程的安全上下文，这样就很难再发

生注入式攻击了。

3) 限制表单或查询字符串输入的长度。

■ 如果用户的登录名字最多只有 10 个字符，那么不要认可表单中输入的 10 个以上的字符，这将大大增加攻击者在 SQL 命令中插入有害代码的难度。

4) 检查用户输入的合法性，确信输入的内容只包含合法的数据。

■ 数据检查应当在客户端和服务器端都执行——之所以要执行服务器端验证，是为了弥补客户端验证机制脆弱的安全性。在客户端，攻击者完全有可能获得网页的源代码，修改验证合法性的脚本（或者直接删除脚本），然后将非法内容通过修改后的表单提交给服务器。因此，要保证验证操作确实已经执行，唯一的办法就是在服务器端也执行验证。你可以使用许多内建的验证对象，例如 RegularExpressionValidator，它们能够自动生成验证用的客户端脚本，当然你也可以插入服务器端的方法调用。如果找不到现成的验证对象，你可以通过 CustomValidator 自己创建一个。

5) 将用户登录名称、密码等数据加密保存。

■ 加密输入的数据，然后再将它与数据库中保存的数据比较，这相当于对用户输入的数据进行了“消毒”处理，输入的数据不再对数据库有任何特殊的意义，从而也就防止了攻击者注入 SQL 命令。System.Web.Security.FormsAuthentication 类有一个 HashPasswordForStoringInConfigFile，非常适合于对输入数据进行消毒处理。

6) 检查提取数据的查询所返回的记录数量

■ 如果程序只要求返回一个记录，但实际返回的记录却超过一行，

那就当作出错处理。

- 根除措施

进一步深入监控和分析业务系统、IDS、防火墙、应用程序日志，采取更准确而针对性的处置措施，然后继续观察处置措施的效果，同时进一步寻找更有效和根本的解决措施，直至确认危险解除。

- 恢复措施

a） 消除攻击源后，验证相关服务的运行情况；

b） 进行业务测试，确定系统完全恢复；

c） 系统上网运行；

2.7 后门攻击事件专项应急处置措施

2.7.1 事件描述

攻击者通过在系统中安插隐藏的程序从而留下进入系统的通道，并通过这种方式攻击。

2.7.2 事件识别与检测

- **事件识别**（包括但不限于）

后门攻击事件，一般可从攻击特性、影响程度方面识别，详见下表：

攻击特性	影响
无明显特殊进程，无端口，无服务，无文件（欺骗、隐藏）	完全控制系统，对系统造成极大破坏
以远程控制为目的，该类后门通过启动进程、端口、服务的方式，来进行控制连接	完全控制系统

攻击特性	影响
该类后门通过启动进程、端口、服务的方式，来进行控制连接。	影响系统性能和稳定性

- 安全设备检测流程
  - 态势感知：控制台-->处置中心-->安全事件视角-->详情模式-->在筛选界面“事件类型”勾选“后门攻击事件”
  - 防火墙：监控-->安全日志-->WEB 应用防护
- **事件检测**
  - 一般的后门入侵，通过杀毒软件、木马软件检测发现后门程序；
  - 对于网站类的后门攻击，到服务器本地上，用文本编辑器打开网页，查找是否存在后门。如果此时发现服务器上的文件被修改过了，则说明服务器可能中了某些后门；服务器上的网页源程序被修改了，如果此时发现服务器上的源文件是正常的，则说明，这种攻击是网络攻击；
  - 登录到服务器本地上：linux 服务器执行 wget http://有问题的网站/index.html 之类的命令 windows 服务器可以用 ie 在本地浏览网来获取网站的首页，检查直接在服务器本地看到的结果是否正常；
  - 把站点配置为 ssl 安全链接站点，然后从别的地方浏览是否正常。

2.7.3 事件处置

- 安全设备处置流程
  - 防火墙：策略-->应用控制策略-->新增-->新增应用控制策略-->源 IP（受害 IP）至目的 IP（any），动作禁止；

- 深信服 EDR：EDR 控制台-->响应中心-->威胁响应-->威胁事件视角-->输入主机地址-->勾选对应的“病毒木马”事件-->点击“一键处置”；

➢ 紧急处理措施

(1) 定位追踪

- 定位到 IP：

a) 使用网络入侵监测系统定位传染源 IP；

b) 使用网络协议分析系统定位传染源 IP；

c) 使用扫描软件发现传染源的 IP；

- 定位到物理位置：

a) 参考企业内的《IP 物理位置表》定位到具体的位置；

b) 追踪 MAC 地址；

c) 定位到接入交换机端口；

(2) 清除后门

a) “切断”：通过物理（如拔网线、关机等）或逻辑（如禁止网卡、交换机关端口等）的方式使传染源完全无法访问网络，“切断”是较为彻底的封堵措施；

b) “隔离”：通过访问控制设备（如防火墙、网络设备等）隔离后门；

c) “监控”：采用入侵检测或其他的网络监控设备追踪传染源的传播行为，对于无法采用“切断”和“隔离”措施的高可用主机，至少应该监控该传染源可能会传染到哪些易感对象，监控不会影响到传染源的可用性；

d) “清除”：通过人工或工具的方式清除传染源上的后门；

- 抑制处理措施
  - 根据后门分析的结果，进行封堵。
- 根除措施

a) 减少系统中的易感对象（主要是因为存在某些漏洞而容易被病毒传染的主机），有利于从根本上遏制后门的进一步扩散。

b) 控制易感对象的主要步骤有：

c) 根据后门分析的结果给出易感对象特征；

d) 采用自动扫描或者人工搜寻的方式寻找易感对象；

e) 根据易感对象的可用性要求进行适当的防护加固；

1) 易感对象特征分析

易感对象一般会具备以下特征：

- 未安装某些补丁，如未安装 RPC 溢出的补丁等；
- 存在某些弱配置，如弱密码；
- 操作系统或应用软件版本过低，如 IE 版本过低；
- 开放某些服务，如共享、WEB 服务等；

后门的信息中会包含易感对象的相关信息，如：“受影响系统”，“易感染对象”。

2) 易感对象搜寻

搜寻易感对象的主要方法有：

- 查询资产管理库；

- 直接扫描漏洞；
- 扫描开放端口；
- 下发通知等；

3） 易感对象安全优化

易感对象的安全优化的主要内容包括：

- 易感对象补丁的升级（如 Patch 和 Hotfix）；
- 易感对象安全配置的优化（如密码策略、本机安全策略等）；
- 易感对象防护措施的增加（如防病毒、恶意代码类的措施）；

➢ 恢复措施

a） 确认后门清除，验证相关服务的运行情况。

b） 进行业务测试，确定系统完全恢复；

c） 系统上网运行。

2.8 拒绝服务类攻击事件专项应急处置措施

2.8.1 事件描述

利用信息系统缺陷、或通过暴力攻击的手段，以大量消耗信息系统的 CPU、内存、磁盘空间或网络带宽等资源，从而影响信息系统正常运行为目的的信息安全事件。

2.8.2 事件识别与检测

- **事件识别**（包括但不限于）

拒绝服务类攻击事件，一般可从攻击特性、影响程度、原始告警信息三方面识别，详见下表：

攻击特性	影响	原始告警信息举例
利用了被攻击软件的实现上的缺陷完成DoS攻击的。通常这些攻击工具向被攻击系统发送特定类型的一个或多个报文。	造成服务的瘫痪	抗DDOS设备的告警：抗DDOS设备发生DOS攻击告警； IDS的告警：IDS设备发生DOS攻击告警； 网络设备：边界网络设备的CPU、内存使用率过高，出现网络连接缓慢等； 服务器：服务器CPU、内存使用率过高，出现网络连接缓慢等，造成正常用户很难访问此服务器。
发送大量的垃圾数据侵占完目标系统资源，导致目标系统拒绝服务。	对网络性能会有很大影响,可能造成网络瘫痪。	
利用了被攻击软件的早期的缺陷完成DoS攻击的。或者通过发送一定的垃圾数据，侵占完目标系统资源，导致目标系统拒绝服务。	影响系统性能和稳定性	

- 安全设备检测流程
  - 态势感知：控制台-->处置中心-->安全事件视角-->详情模式-->在筛选界面“事件类型”勾选“拒绝服务攻击事件”
  - 防火墙：监控-->安全日志-->Dos攻击
- 事件检测

1. 利用系统漏洞的拒绝服务攻击检测方法

通过利用操作系统漏洞，能对系统进行拒绝服务攻击，受攻击系统将会出现系统不能正常运行，死机，CPU占用率过高，内存占用率过高等种种现象。

对于此类攻击方式，可通过以下方法检测：

- 使用资源管理器（Solaris使用ps －aux命令）检查当前内存、CPU

等资源占用情况；

- 检测系统进程和快照对比，找出非法进程；
- 检测网络连接和快照对比，找出可疑的网络连接；
- 检查网络接口的流量
- IDS 的拒绝服务攻击的告警

2. 利用网络协议的拒绝服务攻击检测方法

攻击者利用网络协议某些特性可能对系统发动拒绝服务攻击，比如说常用的 SYN-FLOOD 就是利用 TCP 协议三次握手的特点发起的攻击。

- 对于 SYN-FLOOD 攻击，可通过利用 netstat －an 命令（适用于 Windows/Unix 系统），能发现当前活动连接的状态中存在大量的 SYN_RECEIVED 状态包，这表明系统正受到 SYN-FLOOD 拒绝服务攻击；
- 通过使用 SNIFFER，如果发现大量非正常网络连接，或协议的非正常分布，如 icmp 或 UDP 协议数据超过总流量的 20%；表明系统正在受到拒绝服务攻击；
- IDS 的拒绝服务攻击的告警
- 检查网络接口的流量

2.8.3 事件处置

- 安全设备处置流程
  - 防火墙：策略-->应用控制策略-->新增-->新增应用控制策略-->源 IP（受害 IP）至目的 IP（any），动作禁止；
- 紧急处理措施

a) 确认发起拒绝服务攻击的 IP；

b) 在防火墙上对进入流量进行过滤，比如：防火墙应该拒绝那些来自内部地址或保留地址发出的数据包，这些包通常都是拒绝服务的伪造包；

c) 在边界路由上进行外出流量过滤，边界路由器应拒绝非来自内部网络的向外的包，这些包通常是被利用来对其它目标进行拒绝服务攻击的；

d) 在边界路由器上对确认的 IP 进行封堵；

- 抑制处理措施

a) 安置好取证工作环境，进行攻击分析，包括：取证采样（包括前一时段的防火墙日志、入侵检测日志、路由器日志等）、流量特征分析、报文特征分析及其他分析，确定攻击方式、类型等；

b) 给易受攻击的系统打上补丁，保持补丁的有效；

c) 调整操作系统或设备的性能设置，增强抵抗拒绝服务的能力；

- 根除措施

  - 进一步采取更准确而针对性的处置措施，然后继续观察处置措施的效果，同时进一步寻找更有效和根本的解决措施，直至确认危险解除；

- 恢复措施

a) 消除攻击源后，验证相关服务的运行情况；

b) 进行业务测试，确定系统完全恢复；

c) 系统上网运行。