SSH?????????DDoS?????????

SSH暴力破解入侵（蠕虫DDoS木马）完整处置流程

一、事件定性

告警核心信息：

1. 攻击源：`140.174.49.38` 境外IP暴力破解SSH成功，已拿到服务器权限；
2. 恶意产物：蠕虫DDoS木马`kswpad`、`kal64`，篡改sshd、systemd服务、伪造getty登录进程；
3. 危害：被控服务器会对外发起DDoS攻击、挖矿、中继爆破其他主机，留存后门持续入侵。

二、紧急止损（第一步，阻断攻击链路）

1. 隔离服务器

- 若为云服务器：控制台**断开公网IP/加入安全组全拦截**；
- 物理服务器：临时断开外网网线，仅保留内网运维通道；
- 火绒/服务器防火墙：立即拉黑攻击IP `140.174.49.38`，同时启用仅放行国内IP规则，阻断境外SSH扫描。

2. 阻断SSH入侵入口

1. 临时关闭SSH服务
```bash
systemctl stop sshd
systemctl disable sshd
```
2. 禁止密码登录（修复漏洞根源）
```bash
sed -i 's/#PasswordAuthentication yes/PasswordAuthentication no/' /etc/ssh/sshd_config
sed -i 's/PermitRootLogin yes/PermitRootLogin no/' /etc/ssh/sshd_config
```
3. 修改SSH默认22端口（规避批量扫描）
```bash
sed -i 's/#Port 22/Port 22222/' /etc/ssh/sshd_config
systemctl restart sshd
```

3. 查杀恶意进程

```bash
# 杀死木马进程
pkill -f kswpad
pkill -f kal64
pkill -f bsd-port/getty
```

```
# 验证进程是否残留
ps aux | grep -E "kswpad|kal64|bsd-port"
```

三、彻底清除木马文件（对应告警恶意实体）

1. 删除木马本体

```bash
# 恶意配置文件
rm -rf /etc/kswpad
# 临时木马程序
rm -rf /tmp/kal64
# 伪造登录后门程序
rm -rf /usr/bin/bsd-port/getty
# 篡改的sshd后门（替换为官方原版）
rm /usr/bin/sshd
# 恢复官方openssh
yum reinstall openssh-server -y  # CentOS/RHEL
apt reinstall openssh-server -y   # Ubuntu/Debian
```

2. 清理恶意systemd自启服务

告警中`/lib/systemd/system/`下恶意单元，批量清理：

```bash
# 查找木马相关自启文件
find /lib/systemd/system -name "*ksw*" -o -name "*kal*"
# 删除匹配到的恶意service文件，执行daemon-reload刷新
systemctl daemon-reload
```

3. 清理定时任务（蠕虫会写入crontab持久化）

```bash
# 查看所有用户定时任务，删除恶意脚本
crontab -l -u root
rm -rf /var/spool/cron/root
# 系统级定时任务
ls /etc/cron.*
```

四、账号安全排查（暴力破解成功，账号已泄露）

1. **禁用root远程登录**，所有业务账号重置高强度密码（大小写+数字+符号，16位以上）；
2. 检查是否新增恶意后门账号：

```bash
cat /etc/passwd | grep "/bin/bash"
```

异常账号直接删除`userdel -r 用户名`；
3. 清空所有SSH密钥文件，重新部署可信密钥：
```bash
rm -rf /root/.ssh/authorized_keys
```

五、日志溯源，确认入侵范围
```bash
# 查看SSH登录记录，确认入侵时间、操作
journalctl -u sshd --no-pager
# 查看系统登录日志
last
# 查看恶意程序操作日志
cat /var/log/messages | grep -E "kswpad|kal64"
```
重点确认：黑客是否横向扫描内网、是否窃取业务数据、是否上传其他木马。

六、长期加固方案（杜绝二次入侵）
1. SSH基础加固
- 关闭密码登录，仅使用密钥认证；
- 更换非标准SSH端口；
- 限制SSH登录来源IP（仅办公内网/运维出口IP放行）。

2. 防火墙/主机防护（你之前配置的火绒规则落地）
1. 服务器防火墙：仅放行国内IP入站22端口；
2. 火绒IP协议控制：放行国内网段，拦截全部境外IP入站；
3. 安装fail2ban自动封禁爆破IP：多次SSH失败自动拉黑IP。

3. 系统基线加固
1. 定期更新系统补丁`yum update / apt update`；
2. 禁止root直接登录SSH；
3. /tmp目录挂载限制执行权限，防止木马落地；
4. 监控`/tmp`、`/etc`、`systemd`目录文件变更告警。

4. 告警联动优化
安全平台配置规则：SSH暴力破解成功立即触发阻断脚本，自动拉黑攻击IP；同时监控`kswpad/kal64/bsd-port/getty`恶意文件名，发现即隔离主机。

七、风险兜底判断
如果满足以下任意一条，建议**重装系统**（木马深度植入无法彻底清理）：
1. 黑客篡改了系统内核、lib库、sshd二进制文件；
2. 发现rootkit内核级后门；
3. 溯源日志发现黑客已获取数据库、业务核心数据；
4. 多次查杀后木马自动复活，存在多层持久化后门。

Revision #1
Created 22 June 2026 08:57:52 by Admin
Updated 22 June 2026 08:58:19 by Admin