统信UOS应急响应手册（2024年）

国家工业信息安全发展研究中心

统信软件技术有限公司

工业和信息化部网络安全威胁和漏洞信息共享

平台信创政务产品安全漏洞专业库

统信软件技术有限公司 UnionTech Software Technology Co., Ltd.

工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）

信创政务产品安全漏洞专业库（CITIVD）

cic 工信安全

目录 CONTENTS

编制单位

PREPARED BY

国家工业信息安全发展研究中心

统信软件技术有限公司

工业和信息化部网络安全威胁和漏洞信息共享平台信创政务产品安全漏洞专业库

技术支持单位

TECHNICAL SUPPORT UNIT

深信服科技股份有限公司

北京神州绿盟科技有限公司

北京天融信网络安全技术有限公司

北京长亭科技有限公司

飞腾信息技术有限公司

杭州迪普科技股份有限公司

杭州美创科技股份有限公司

奇安信网神信息技术（北京）股份有限公司

上海兆芯集成电路股份有限公司

天翼安全科技有限公司(中国电信股份有限公司网络安全产品运营中心)

郑州埃文科技有限公司

中电科网络安全科技股份有限公司

中电信数智科技有限公司

中孚安全技术有限公司

前言

PREFACE

工业和信息化部网络安全威胁和漏洞信息共享平台信创政务产品安全漏洞专业库（简称“信创漏洞库”）是在工业和信息化部网络安全管理局指导下，由国家工业信息安全发展研究中心建设和运营的。面向信创产品提供者、网络产品安全漏洞收集平台和其他发现漏洞的组织或个人，收集并上报信创产品安全漏洞。信创政务产品安全漏洞专业库通过开展信息收集、风险研判、处置通报等相关工作，提供漏洞缓解措施及修复方案等，进一步提升我国信创产品安全防护能力，助力构建良好信创安全生态环境。

统信软件技术有限公司（简称“统信软件”），由中国主流操作系统厂商于 2019 年联合成立，其前身为 2004 年组建的深度操作系统团队，至今研发历史已有二十年，是中国操作系统领创企业。统信软件总部设立于北京，在上海、广州、深圳、武汉、南京、成都、西安等地设立分支机构，以“打造操作系统创新生态，给世界更好的选择”为愿景，致力于研发安全稳定、智能易用的中国操作系统产品，以操作系统为核心，引领中国软硬件生态建设，让世界见证中国科技力量！

本手册是由信创漏洞库和统信软件联合发布，针对统信 UOS 在使用中开展应急响应处置的安全基线检查操作及安全事件响应的处置措施。

本手册适用于统信 uos 通用使用环境下应急处置场景，变更配置基线、应急处置等操作可能会出现与原配置冲突的情况，在执行操作前请充分做好安全测试及备份工作。

01

PART.01

统信UOS服务器版
应急响应手册

BASELINE CHECK

基线检查

安全加固

判断依据

检查方法

以 root 或安全管理员账号登录系统，打开服务器安全中心，查看当前安全基线等级是否为高

判定结果

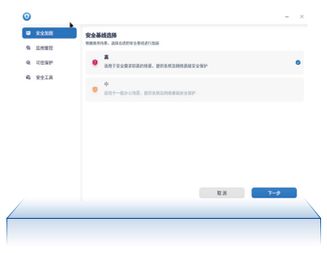
若当前基线等级为高，则通过

检查点

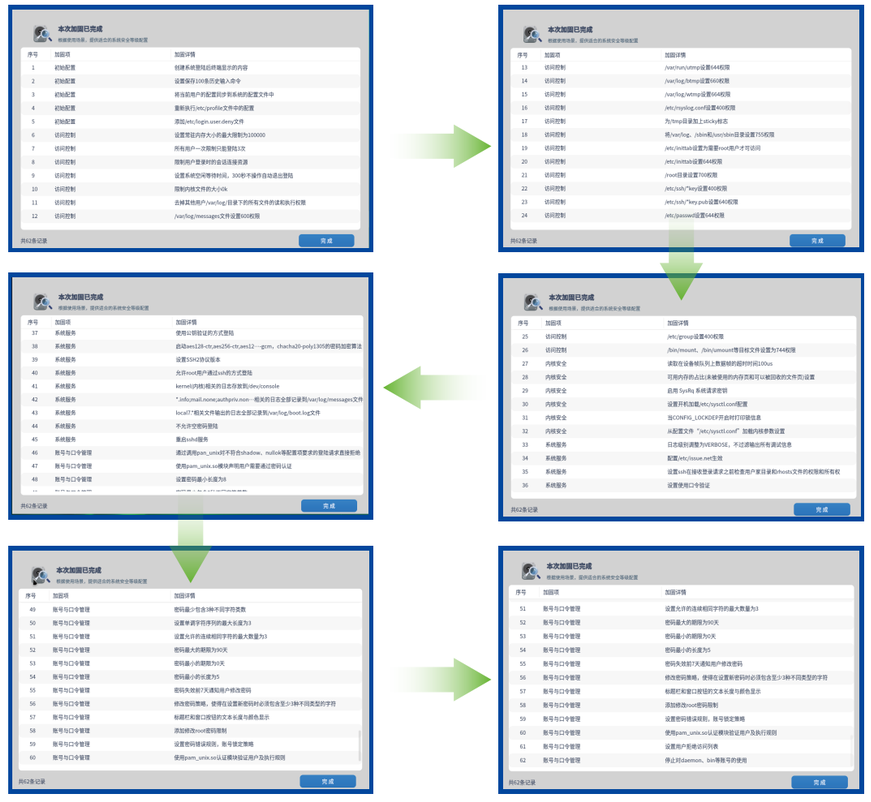
服务器安全中心 - 当前基线等级

加固方法

打开服务器安全中心，点击开始加固，选择高等级，点击下一步开始加固



加固项如下所示：



应用管控

判断依据

检查方法

打开服务器安全中心 - 应用管控，查看应用管控状态

判定结果

应用管控状态为开启，则通过

检查点

服务器安全中心 - 应用管控

加固方法

打开服务器安全中心 - 应用管控，开启应用管控，需要重启才能开启

选择应用加入网络防护，对于设置了网络防护的应用，无法连接网络

添加应用进程防杀死，对于设置了进程防杀死的应用，启动后无法被其他进程杀死

添加应用防卸载，对于设置了防卸载的应用，无法通过rpm、yum、dnf等命令卸载，也无法删除应用相关的文件

可信保护

判断依据

检查方法

打开服务器安全中心 - 可信保护，查看可执行文件保护、文件防篡改、内核模块防卸载、内核模块黑名单功能是否使用

判定结果

若可信保护中，可执行文件保护、文件防篡改、内核模块防卸载、内核模块黑名单功能已配置并使用，则通过

检查点

服务器安全中心 - 可信保护

加固方法

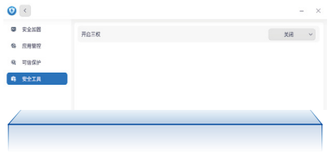
打开服务器安全中心 - 可信保护，配置并启用可执行文件保护、文件防篡改、内核模块防卸载、内核模块黑名单功能

三权分立

判断依据

检查方法

打开服务器安全中心 - 安全工具 - 三权分立，查看三权分立功能是否启用



判定结果

服务器安全中心 - 安全工具 - 三权分立中，若三权分立功能已开启，则通过

检查点

服务器安全中心 - 安全工具 - 三权分立

加固方法

打开服务器安全中心 - 安全工具 - 三权分立，开启三权分立功能，配置系统管理员、审计管理员、安全管理员密码

系统版本

判断依据

检查方法

执行 yum update 命令（若 yum 适用），查看是否存在更新

判定结果

若不存在新版本，则通过

检查点

yum update（若 yum 适用）

加固方法

执行 yum update 下载安装更新（若 yum 适用）

EMERGENCY RESPONSE METHODS FOR SECURITY INCIDENTS

常见安全事件应急处置方式

挖矿事件

情况介绍

挖矿事件指的是攻击者利用技术手段对受害者进行网络攻击，在受害者的网络设备中植入挖矿木马，非法占用其计算资源来进行加密货币的挖掘活动。挖矿事件不仅消耗大量的计算机处理资源，严重危害受害者的计算机安全和性能，还可能导致业务中断等严重后果。以下是挖矿事件的显著特征：

- 电脑变得非常卡，频繁无响应、风扇异响、反复重启
- CPU 的使用率会变得非常高，甚至会超过 100%
- 网络流量变大
- 耗电量急剧上升

应急处置

处置前准备

备份数据：在进行任何处置前，确保对重要数据进行冗余备份，防止数据丢失

隔离受感染服务器：从网络中隔离受影响的服务器，防止影响扩散到其他系统

收集证据：记录当前系统状态，包括进程列表、网络连接、系统日志等，为后续分析和追踪溯源提供依据

准备工具：确保拥有必要的安全工具，如杀毒软件、系统监控工具、网络分析工具等

处置过程

确认病毒类型

- **确定病毒 ioc 信息**

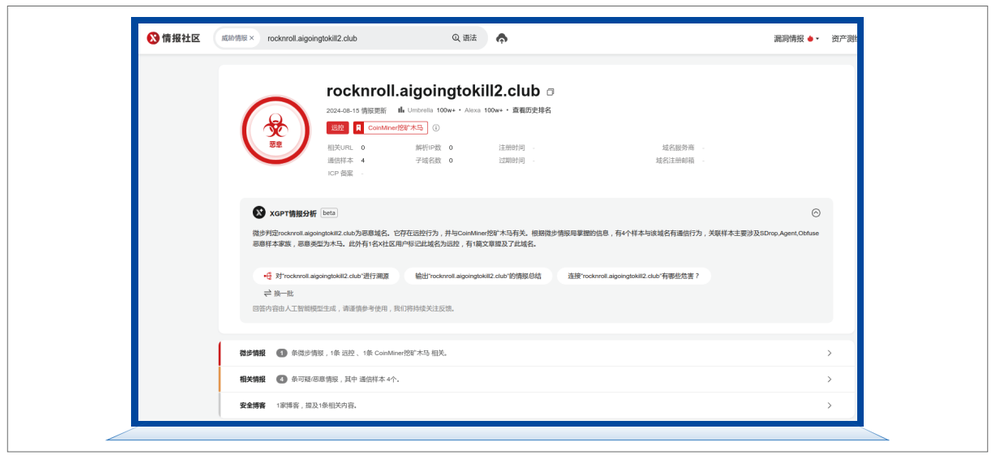
对系统日志、网络流量、安全设备警报等进行全面监测和分析，获取病毒 ioc 信息

- **确认恶意木马类型**

根据 ioc 确定木马类型：

Virustotal　深信服威胁情报中心　微步在线

安恒威胁情报中心　360 威胁情报中心　绿盟威胁情报中心



获取异常进程 pid

- **CPU 占用**

top -c -o %CPU

- -c 参数显示进程的命令行参数
- -o 参数可按照进程 CPU 使用百分比进行排序
- -p 参数可指定进程的 pid

- **内存占用**

top -c -o %MEM

- -c 参数显示进程的命令行参数
- -o 参数可按照进程内存使用百分比进行排序
- -p 参数指定进程的 pid

- **网络占用**

nethogs

- yum install nethogs 安装 nethogs
- nethogs 查看网络占用

确认恶意文件样本

- **根据 pid 获取进程信息**

lsof -p pid

- 查看进程正在读写的文件

pwdx pid

- 获取该 pid 的进程启动时候的目录

systemctl status pid

- 获取进程的 status 信息

cat /proc/pid/maps

- 查看进程加载的链接库

ls -al /proc/pid/exe

- 查看进程文件的路径

pstree -agplU

- 全面展示进程与线程间的关系

- **确定恶意程序运行时间**

查看程序运行时间：ps -w -eo pid,lstart,etime,cmd | grep <pid>

处理异常进程

- **进程查杀**

若存在守护进程，先杀掉守护进程

- ps -w ajfx
- kill -9 pid

查看异常进程是否存在子进程

- ps -w ajfx
- systemctl status

无子进程，杀掉进程

- kill -9 pid

有子进程，杀掉进程组

- kill -9 -pid

- **线程查杀**

如果木马病毒作为线程，被附到现有正常业务的进程中，查杀该线程风险比较大，极可能会导致业务进程崩掉，杀死线程的方法和杀死进程一样

pstree -agplU 全面展示进程与线程间的关系

kill -9 pid 杀掉线程

- **计划任务清理**

需要检查的文件：

/etc/crontab

/etc/cron.d/*

/var/spool/cron/xxxx

/etc/anacrontab

使用 vim 打开文件，检查是否存在恶意的计划任务，并删除

删除恶意文件

查看文件占用

- lsof eval.sh
- 如果存在进程占用，那么占用进程也可能是恶意进程，需要按照之前的步骤进行查看

a 和 i 属性导致文件不可删除

- a 属性文件只能增加内容，不能修改之前的文件，不能删除文件
- i 属性内容不能改变，文件不能删除
- 可以使用 chattr -a 和 chattr -i

奇怪文件名导致文件不可删除

- 从 windows 向 linux 传输的文件或者攻击者恶意制造的文件，很多会有文件名乱码，无法直接通过乱码的文件名进行删除，可以 使用 inode 来确定文件名，之后删除
- 查看 inode：ls -li eval.sh
- 删除文件：find ./* -inum 12327526 -exec rm -i {} \; (会有一步确认是否删除)

目录挂载导致无法删除

- 查看目录挂载情况：lsblk -a
- 取消挂载：umount /dev/xx

处置情况确认

通过以下方式确认挖矿病毒是否清理完成：

检查 CPU 和内存使用情况：
使用 top、htop 或 nmon 等工具监控系统资源使用情况，确认没有异常的资源占用

检查进程列表：
再次使用 ps、ps aux 或 top 命令检查所有运行中的进程，确保没有可疑的挖矿进程

检查网络连接：
使用 netstat、ss 或 lsof 等命令检查网络连接和监听端口，确保没有可疑的网络活动

检查计划任务和定时任务：
使用 crontab -l 检查当前用户的所有计划任务，确认没有可疑的定时执行任务

检查系统启动项：
检查 /etc/rc.local、/etc/init.d/、systemctl 等与系统启动相关的配置，确保没有添加可疑的自启动程序

全盘搜索挖矿程序：
使用 find 命令搜索整个文件系统，查找可能遗漏的挖矿程序文件或脚本

使用杀毒软件扫描：
使用杀毒软件或反恶意软件工具进行全系统扫描，确保没有遗漏的病毒或恶意软件

检查账户安全：
确认没有新增的可疑用户账户，检查现有账户的密码强度，并确保没有弱口令

检查系统漏洞：
使用漏洞扫描工具检查系统是否存在已知漏洞，并及时打补丁更新

检查系统配置：
确认系统配置没有被篡改，如 .bashrc、.bash_profile、.profile 等配置文件

监控系统行为：
在一段时间内持续监控系统行为，看是否有复发的迹象

远控后门

情况介绍

远控后门，也称为远程控制木马或后门程序，是一种恶意软件，一般由攻击者攻击成功之后植入受害者网络设备，从而使攻击者可持续未经授权情况下远程控制受害者的计算机或网络设备。这类程序具有强大的功能，能够在受害者完全不知情的情况下执行各种操作，包括但不限于窃取数据、配置代理服务器、攻击其他计算机、控制摄像头等。以下是远控后门的一些关键特点和分析：

隐蔽性

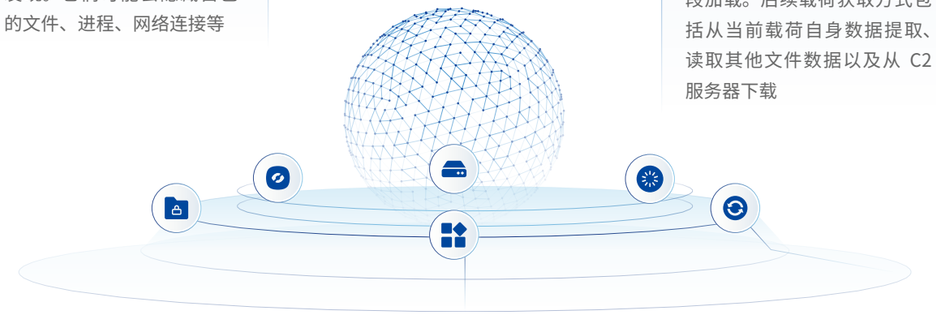
远控后门被设计为尽可能隐蔽，避免被用户或安全软件发现。它们可能会隐藏自己的文件、进程、网络连接等

持久化机制

远控后门会在系统中建立持久化机制，确保在系统重启后依然能够执行。这可能通过修改服务、启动文件夹或计划任务来实现

多阶段加载

恶意代码从植入目标系统到最终远控运行，通常会经历多阶段加载。后续载荷获取方式包括从当前载荷自身数据提取、读取其他文件数据以及从 C2 服务器下载



代码混淆和加密

为了避免检测分析，远控后门的载荷基本都会经过加密处理，使用的加密算法包括各类 XOR 加密和对称加密（比如 RC4、AES）。有些还会使用图片隐写技术隐藏后续载荷

反侦察功能

一些高级的远控后门具备反调试和反沙箱功能，能够检测并规避分析和安全措施

更新和变种

远控后门会不断更新和变化，以逃避检测和查杀，包括使用新的免杀技术、传播途径和控制指令

应急处置

处置前准备

应急处置前，准备工作如下：

备份数据

在进行任何处置前，确保对重要数据进行备份，防止数据丢失

隔离受感染服务器

从网络中隔离受影响的服务器，防止影响扩散到其他系统

收集证据

记录当前系统状态，包括进程列表、网络连接、系统日志等，为后续分析和追踪溯源提供依据

准备工具

确保拥有必要的安全工具，如杀毒软件、系统监控工具、网络分析工具等

处置过程

获取后门信息

根据 EDR、态势感知平台的安全产品告警的信息，获取后门文件的路径或外连 ip

获取远控后门进程

根据后门文件查找进程 pid：

- lsof | grep test.sh
- lsof /test.sh　需要指定后门路径

根据目的 ip 及端口查找进程 pid：

- netstat -pantu | grep “ip”
- netstat -pantu | grep “port”
- lsof -i: “port”

确定远控后门运行时间

- 查看运行时间：ps -w -eo pid,lstart,etime,cmd | grep <pid>

处理异常进程

- **进程查杀**

若存在守护进程，先杀掉守护进程

- ps -w ajfx
- kill -9 pid

查看异常进程是否存在子进程

- ps -w ajfx
- systemctl status

无子进程，杀掉进程

- kill -9 pid

有子进程，杀掉进程组

- kill -9 -pid

- **线程查杀**

如果木马病毒作为线程，被附到现有正常业务的进程中，查杀该线程风险比较大，极可能会导致业务进程崩掉，杀死线程的方法和杀死进程一样

pstree -agplU 全面展示进程与线程间的关系

kill -9 pid 杀掉线程

- **计划任务清理**

需要检查的文件：

/etc/crontab

/etc/cron.d/*

/var/spool/cron/xxxx

/etc/anacrontab

使用 vim 打开文件，检查是否存在恶意的计划任务，并删除

删除恶意文件

查看文件占用

- lsof eval.sh
- 如果存在进程占用，那么占用进程也可能是恶意进程，需要按照之前的步骤进行查看

奇怪文件名导致文件不可删除

- 从 windows 向 linux 传输的文件或者攻击者恶意制造的文件，很多会有文件名乱码，无法直接通过乱码的文件名进行删除，可以 使用 inode 来确定文件名，之后删除
- 查看 inode：ls -li eval.sh
- 删 除 文 件：find ./* -inum 12327526 -exec rm -i {} \; (会有一步确认是否删除)

a 和 i 属性导致文件不可删除

- a 属性 文件只能增加内容，不能修改之前的文件，不能删除文件
- i 属性 内容不能改变，文件不能删除
- 可以使用 chattr -a 和 chattr -i

目录挂载导致无法删除

- 查看目录挂载情况：lsblk -a
- 取消挂载：umount /dev/xx

处置情况确认

通过以下方式确认远控后门是否清理完成：

勒索病毒

情况介绍

勒索病毒，是一种极具传播性和破坏性的恶意软件，泛指一切通过锁定被感染者计算机系统或文件并施以敲诈勒索的新型计算机病毒。采用复杂的加密算法对用户的文件进行加密，使受害者无法访问或使用这些数据。加密完成后，病毒通常会显示一条勒索信息，要求受害者支付一定金额的赎金以获取解密密钥或恢复数据的方法。这些赎金通常以加密货币的形式支付，以隐藏交易的真实身份和避免追踪。其特征如下：

- 系统文件被加密无法读取、计算机无法正常使用
- 会在桌面等明显位置生成勒索提示文件

应急处置

处置前准备

应急处置前，准备工作如下：

备份数据
在进行任何处置前，确保对重要数据进行备份，防止数据丢失

隔离受感染服务器
从网络中隔离受影响的服务器，防止影响扩散到其他系统

收集证据
记录当前系统状态，包括进程列表、网络连接、系统日志等，为后续分析和追踪溯源提供依据

准备工具
确保拥有必要的安全工具，如杀毒软件、系统监控工具、网络分析工具等

处置过程

确定勒索病毒类型

判断勒索病毒类型方式如下：

勒索页面主动说明的，直接粘贴到 baidu、google 里面搜索

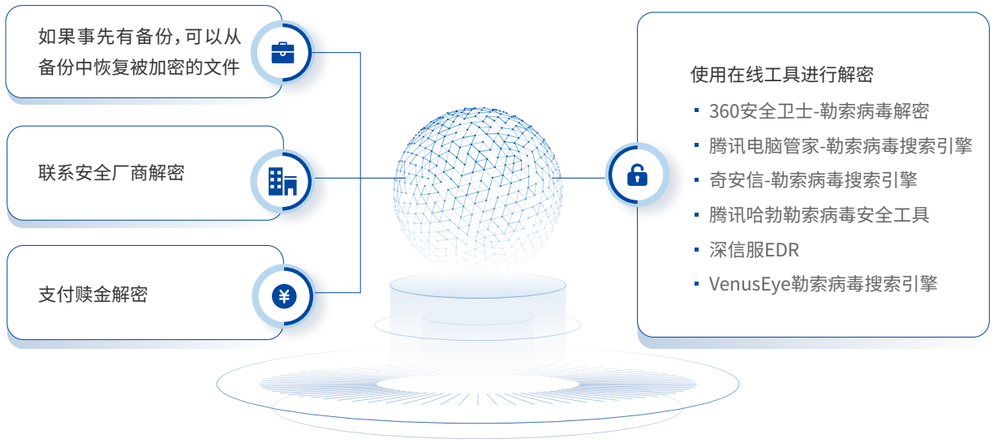
勒索加密文件的后缀名

在线网站识别

- 360 安全卫士 - 勒索病毒解密
- 腾讯电脑管家 - 勒索病毒搜索引擎
- 奇安信 - 勒索病毒搜索引擎
- 腾讯哈勃勒索病毒安全工具
- 深信服 EDR
- VenusEye 勒索病毒搜索引擎

系统恢复

通过以下步骤恢复系统：



系统升级

升级操作系统安装安全补丁

系统备份

异地备份被感染过的系统

处置情况确认

通过以下方式确认勒索病毒是否清理完成：

文件排查

- 确保系统中的文件不存在被加密的迹象，比如文件扩展名未修改为勒索病毒特定的扩展名

远控后门排查

- 确保系统中是否存在远控后门

漏洞排查

- 确保系统是否存在已知漏洞

检查网络连接

- 使用 netstat、ss 或 lsof 等命令检查网络连接和监听端口，确保没有可疑的网络活动

检查计划任务和定时任务

- 使用 crontab -l 检查当前用户的所有计划任务，确认没有可疑的定时执行任务

检查系统启动项

- 检查 /etc/rc.local、/etc/init.d/、systemctl 等与系统启动相关的配置，确保没有添加可疑的自启动程序

全盘搜索远控后门

- 使用 find 命令搜索整个文件系统，查找可能遗漏的远控后门文件

使用杀毒软件扫描

- 使用杀毒软件或反恶意软件工具进行全系统扫描，确保没有遗漏的远控后门文件

检查账户安全

- 确认没有新增的可疑用户账户，检查现有账户的密码强度，并确保没有弱口令

检查系统配置

- 确认系统配置没有被篡改，如 .bashrc、.bash_profile、.profile 等配置文件

监控系统行为

- 在一段时间内持续监控系统行为，看是否有复发的迹象

暴力破解

情况介绍

暴力破解（Brute Force Attack）是一种常见的攻击行为，攻击者通过尝试各种组合和密码来解密目标系统或数据的加密保护。这种攻击方法不涉及深入的技术细节或社会工程学的高级手段，多依赖于大量的计算资源和时间来进行穷举式的尝试。暴力破解攻击主要针对以下服务：

ssh　mysql　ftp　redis

应急处置

处置前准备

应急处置前，准备工作如下：

备份数据

- 在进行任何处置前，确保对重要数据进行备份，防止数据丢失

隔离服务器

- 从网络中隔离受影响的服务器，防止影响扩散到其他系统

收集证据

- 记录当前系统状态，包括进程列表、网络连接、系统日志等，为后续分析和追踪溯源提供依据

准备工具

- 确保拥有必要的安全工具，如杀毒软件、系统监控工具、网络分析工具等

处置过程

SSH 暴力破解

检查网络连接信息：netstat -pantu

```
lixin@lixin-PC:~/Desktop$ netstat -pantu
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:50010         0.0.0.0:*               LISTEN      7838/wineserver
tcp        0      0 10.20.33.202:5821       0.0.0.0:*               LISTEN      7838/wineserver
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:16308         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:16090         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:16067         0.0.0.0:*               LISTEN      -
tcp       32      0 10.20.33.202:49280      157.148.45.186:443      CLOSE_WAIT  7838/wineserver
tcp        0      0 127.0.0.1:40910         127.0.0.1:41531         ESTABLISHED 7838/wineserver
```

- Proto 协议类型
- Recv-Q：表示收到的数据已经在本地接收缓冲，但是还有多少没有被进程取走，如果接收队列 Recv-Q 一直处于阻塞状态，可能是遭受了拒绝服务 denial-of-service 攻击
- Send-Q：对方没有收到的数据或者说没有 Ack 的，还是本地缓冲区。如果发送队列 Send-Q 不能很快的清零，可能是有应用向外发送数据包过快，或者是对方接收数据包不够快
- Local Address：本机地址，一般有以下几种模式
  - *:80 监听 IPv4 或 IPv6 的任意 IP 的 80 端口
  - :::80 监听 IPv6 和 IPv4 的任意 IP 的 80 端口
  - 0.0.0.0:80 监听任意 IPv4 地址的 80 端口
  - 127.0.0.1:80 监听本地的 80 端口，只能本地访问
  - ::1:80 监听本次 IPv6 的回环地址，只能本地访问
  - 192.168.1.1:80 监听 IP 地址 192.168.1.1 的 80 端口
- Foreign Address：外部地址
- 规则和 Local Address 规则一样
- State 网络状态
  - LISTEN 侦听状态，等待对端连接
  - SYN_SENT 客户端发送建立连接的 SYN 请求后状态为 SYN_SENT
  - SYN_RECV 服务端发送 SYN+ACK 后网络状态为 SYN_RECV
  - ESTABLISHED 已经建立起连接
  - FIN_WAIT1 主动端四次挥手主动发起的第一个包，也就是 FIN 包之后网络状态为 FIN_WAIT1
  - CLOSE_WAIT 被动端收到四次挥手的 FIN 包，发送 ACK 后处于 CLOSE_WAIT
  - FIN_WAIT2 主动关闭端接到 ACK 后进入 FIN_WAIT2，等待对端发下一个 FIN
  - LAST_ACK 被动关闭端发送第二个 FIN 后进入 LAST_ACK 状态，等待最后一个 ACK 的到来
  - TIME_WAIT 主动端发送最后一个 ACK，之后进入 TIME_WAIT 状态，等待一段时间确保对端接收到了 ACK
  - CLOSING 在 TCP 四次挥手期间，主动关闭端发送了 FIN 包后，没有收到对应的 ACK 包，却收到对方的 FIN 包，此时，进入 CLOSING 状态
  - CLOSED 被动关闭端在接受到 ACK 包后，就进入了 closed 的状态。连接结束
  - UNKNOWN 未知的 Socket 状态
- PID/Program name 进程 ID 和进程名

SSH 遭到暴力破解时，22 端口将会存在大量的 ESTABLISHED 状态的连接

查看正在连接的 ssh sessions：who -a

查看 SSH 日志信息

- 查看登录成功的日志：cat /var/log/auth.log | grep "Accept"
- 查看登录失败的日志：cat /var/log/auth.log | grep "Failed password for" | more
- 统计登录失败的用户名以及次数：grep "Failed password" /var/log/auth.log|perl -e 'while($_=<>){ /for (.*?)from/; print "$1\n";}'|sort|uniq -c|sort -nr
- 统计暴力破解的登录者（IP）：cat /var/log/auth.log | grep "Failed password for" | cut -d " " -f 9 | sort -nr | uniq|grep -v "invalid"| while read line;do echo [$line];cat /var/log/auth.log | grep "Failed password for" | grep $line | grep -Po '(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|[1-9])(\.(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|\d)){3} '|sort|uniq -c |sort -nr; done
- 统计不存用户的登录：cat /var/log/auth.log | grep "Failed password for" | grep "invalid"| cut -d " " -f 11 | sort -nr | uniq| while read line;do echo [$line];cat /var/log/auth.log | grep "Failed password for" | grep $line | grep -Po '(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|[1-9])(\.(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|\d)){3} '|sort|uniq -c |sort -nr;done

Mysql 暴力破解

查看登录错误用户名的登录 IP 以及次数：cat /var/log/mysql/error.log | grep "Access denied for user" | grep "using password: YES" | awk -F "'" '{print $2}' | sort| uniq | while read line;do echo $line;cat /var/log/mysql/error.log | grep "Access denied for user" | grep "using password" | awk -F "'" '{print $4}' | sort | uniq -c | sort -nr; done

FTP 暴力破解

检查网络连接信息：netstat -pantu

- 若存在暴力破解，则 21 端口有大量的 ESTABLISHED 状态和 TIME_WAIT 状态的网络连接

查看登录失败的用户的登录 IP：cat /var/log/vsftpd.log | grep FAIL | cut -d "[" -f 3 | cut -d "]" -f 1 | sort | uniq | while read line;do echo $line;cat /var/log/vsftpd.log | grep $line | cut -d ":" -f 7 | cut -d '"' -f 1 | sort | uniq -c | sort -nr; done

Redis 未授权访问 & 暴力破解

redis 未授权访问：

连接 redis：redis-cli -hip

redis 暴力破解：

检查网络连接信息：netstat -pantu

- 若存在暴力破解，则 6379 端口有大量的 ESTABLISHED 状态的网络连接

处置情况确认

通过以下方式确认暴力破解处置完成：

隧道

情况介绍

隐蔽隧道是指通过改变或伪装数据包的结构和内容，使恶意流量在传输过程中不被传统的网络安全设备轻易检测出来。它通常利用标准通信协议，如 HTTP、DNS、ICMP、TCP、UDP 等，通过修改协议字段或载荷部分，将恶意数据伪装成正常通信流量进行传输。从而实现绕过安全设备和监管，实现网络穿透、恶意攻击或数据窃取等目的。

应急处置

处置前准备

应急处置前，准备工作如下：

备份数据

在进行任何处置前，确保对重要数据进行备份，防止数据丢失

隔离受感染服务器

从网络中隔离受影响的服务器，防止影响扩散到其他系统

收集证据

记录当前系统状态，包括进程列表、网络连接、系统日志等，为后续分析和追踪溯源提供依据

准备工具

确保拥有必要的安全工具，如杀毒软件、系统监控工具、网络分析工具等

处置过程

获取隧道信息

隧道事件的事件来源一般有以下几种：

- 流量设备发现存在网络隧道
- 主机安全程序发现存在网络隧道或相关文件、进程
- 排查过程中发现存在跳板机痕迹等，进而发现隧道
- 运维相关人员发现异常端口等

SSH 隧道

检查监听端口

- netstat -tulnp | grep LISTEN
- 使用 netstat 命令查看系统上所有监听的端口。SSH 隧道可能会在本地端口上创建监听点

检查 SSH 进程

- ps aux | grep ssh
- 使用 ps 命令查看所有 SSH 相关进程，特别是那些使用端口转发的进程

检查已建立的隧道

- ss -o state established -t '(dport = :ssh or sport = :ssh)'
- 对于已经建立的 SSH 隧道，可以使用 ss 命令查看所有 SSH 连接，包括隧道

检查 SSH 日志

- cat /var/log/auth.log
- 查看 SSH 服务的日志文件，搜索与端口转发相关的日志条目

DNS 隧道

网络连接检查

- 使用 netstat -anp 命令查看系统中所有的网络连接
- 查找与 DNS 相关的连接，特别是那些连接到外部 DNS 服务器的不寻常连接

监控网络流量

- 使用网络流量分析工具，如 Wireshark，设置过滤器来重点关注 DNS 流量，可以使用 dns 作为过滤器关键字，分析捕获到的 DNS 数据包，查看是否有异常的 DNS 请求和响应
- 正常情况下，DNS 请求的频率相对较低且较为随机。如果发现某个主机频繁地发出 DNS 请求，可能存在异常
- 观察 DNS 请求的域名模式，DNS 隧道可能会使用一些不寻常的、长且复杂的域名，或者域名中包含编码信息

检查系统进程

- 查看正在运行的进程，查找可能与 DNS 隧道相关的程序
- 使用 ps aux 命令列出所有进程，一些已知的用于建立 DNS 隧道的工具可能会在进程列表中出现，如 dns2tcp、dnscat2、iodine 等

入侵检测系统（IDS）：使用 IDS 监视网络流量，查找表明恶意活动的模式和行为，以检测 DNS 隧道

分析 DNS 隧道工具流量特征：DNS 隧道工具的流量特征与其正常流量不同，例如，使用特定记录类型（如 TXT 或 NULL）的比例异常高，或者域名中数字字符占比异常，可以作为检测 DNS 隧道的指标

ICMP 隧道

检查网络连接

- 使用 netstat -anp 命令查看系统中所有的网络连接，包括 TCP、UDP 和 ICMP
- 查找与 ICMP 相关的连接，看是否有不寻常的连接到外部服务器的情况

监测网络流量

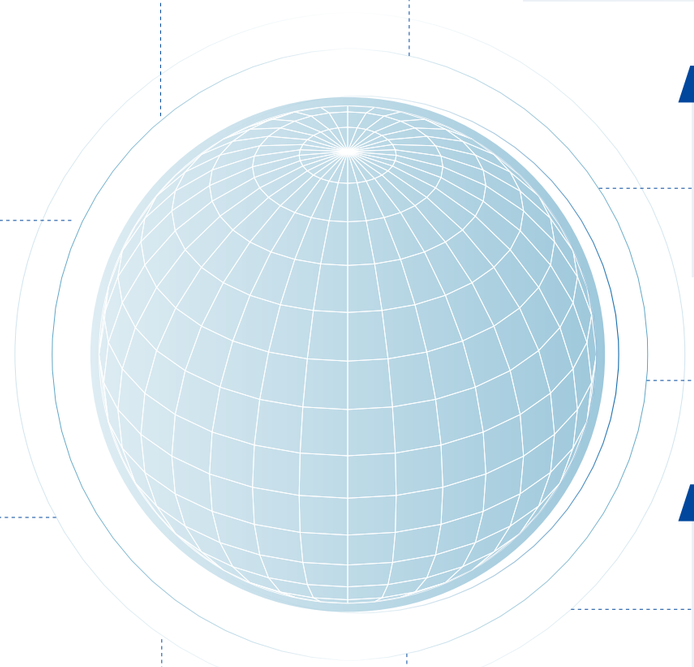
- 使用网络流量监测工具，如 Wireshark、Tcpdump 等，捕获网络数据包
- 对于 Wireshark，可以选择合适的网络接口进行捕获，然后在过滤器中输入 icmp 来筛选出 ICMP 数据包
- 使用 Tcpdump 可以运行命令如 tcpdump -i eth0 icmp（假设 eth0 是要监测的网络接口）
- 正常的 ICMP 数据包通常是用于网络诊断和错误报告，如 ping 请求和响应，而 ICMP 隧道可能会表现出异常的数据包大小、频繁的 ICMP 请求和响应、不寻常的 ICMP 类型和代码等

检查系统进程

- 查看系统中正在运行的进程，是否有可疑的进程可能在使用 ICMP 隧道
- 使用 ps -aux 命令列出所有进程，然后仔细检查进程名、命令行参数和运行用户等信息
- 对于一些已知的可能用于建立隧道的工具，如 icmptunnel、ptunnel 等，可以通过 grep 进行搜索，例如 ps -aux | grep icmptunnel

检查系统日志

- 查看系统日志文件，如 /var/log/syslog、/var/log/messages 等，看是否有与 ICMP 相关的异常日志记录



HTTP/HTTPS 隧道

检查系统连接

- 使用 netstat -anp 命令查看系统中所有的网络连接，查找与 HTTP/HTTPS 端口相关的连接，特别是那些连接到陌生 IP 地址或不常见的域名的连接

监测网络流量

- 使用网络流量分析工具，如 Wireshark，设置过滤器来重点关注 HTTP/HTTPS 流量，可以使用 http 或 tcp.port==80（对于 HTTP）以及 tcp.port==443（对于 HTTPS）作为过滤器关键字，查看是否有异常的 HTTP/HTTPS 请求和响应
- 正常的 HTTP/HTTPS 流量通常是用户发起的网页浏览、API 调用等。如果发现大量持续的、规律性的流量，且流量的大小、频率或目的地不寻常，可能存在隧道的迹象

检查系统进程

- 使用 ps -aux 命令列出所有正在运行的进程，查找可能与 HTTP/HTTPS 隧道相关的进程，如代理软件、网络工具等

分析系统日志

- 查看 Web 服务器日志（如果系统中有运行的 Web 服务器）
- 例如，Apache 的访问日志通常位于 /var/log/apache2/access.log，Nginx 的访问日志通常在 /var/log/nginx/access.log
- 检查是否有异常的请求记录，如大量来自同一 IP 地址的请求、不寻常的请求方法或 URL 路径等
- 检查系统安全日志，如 /var/log/syslog 或 /var/log/messages，看是否有与 HTTP/HTTPS 相关的异常事件记录

文件查杀

- 使用 webshell 查杀工具进行查询，如 D 盾、webshellkiller、河马查杀等

Socks 隧道

检查网络连接

- 使用 netstat -anp 命令查看系统中所有的网络连接状态
- 查找与 SOCKS 相关的连接，通常 SOCKS 服务器使用端口 1080，但也可能使用其他自定义端口
- 可以结合 lsof -i :<port> 命令来查看特定端口上的进程信息，以确定是否有与 SOCKS 相关的进程在使用该端口

检查系统进程

- 使用 ps aux 命令列出所有正在运行的进程
- 查找可能与 SOCKS 隧道相关的进程，如 SOCKS 代理软件、网络工具等

分析系统日志

- 查看系统日志文件，如 /var/log/syslog、/var/log/messages 等
- 查找与网络连接或可疑进程相关的日志记录

处置情况确认

通过以下方式确认挖矿病毒是否清理完成：

检查网络连接

使用 netstat、ss 或 lsof 等命令检查网络连接和监听端口，确保没有可疑的网络活动

检查计划任务和定时任务

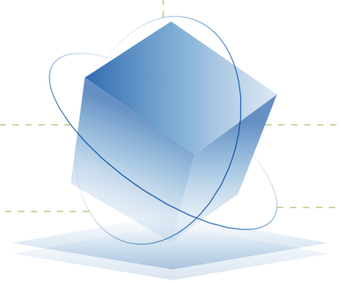
使用 crontab -l 检查当前用户的所有计划任务，确认没有可疑的定时执行任务

检查系统启动项

检　查 /etc/rc.local、/etc/init.d/、systemctl 等与系统启动相关的配置，确保没有添加可疑的自启动程序

监控系统行为

在一段时间内持续监控系统行为，看是否有复发的迹象



全盘搜索远控后门

使用 find 命令搜索整个文件系统，查找可能遗漏的远控后门文件

检查系统配置

确认系统配置没有被篡改，如 .bashrc、.bash_profile、.profile 等配置文件

使用杀毒软件扫描

使用杀毒软件或反恶意软件工具进行全系统扫描，确保没有遗漏的远控后门文件

检查系统漏洞

使用漏洞扫描工具检查系统是否存在已知漏洞，并及时打补丁更新

检查账户安全

确认没有新增的可疑用户账户，检查现有账户的密码强度，并确保没有弱口令

02

PART.02

统信UOS桌面专业版应急响应手册

PREFACE

基线检查

账号与口令策略

密码策略

应有密码复杂度要求，如：

- 口令长度至少 8 个字符
- 口令必须包含如下至少三种字符的组合：
  - 一至少一个小写字母
  - 一至少一个大写字母
  - 一至少一个数字
  - 一至少一个特殊字符：`~!@#$%^&*()-_=+\|[{}];:'",<.>/? 和空格
- 口令不能和帐号一样
- 设置密码失效时间

判定依据

检查方法

打开安全中心 - 安全工具，查看密码强度是否设置为高，改密周期是否设置

判定结果

若安全中心 - 安全工具 - 登录安全中密码强度设置为高、改密周期 90 天内则通过

检查点

安全中心 - 安全工具 - 登录安全

加固方法

将安全中心 - 安全工具 - 登录安全中密码强度设置为高、改密周期设置为 90 天

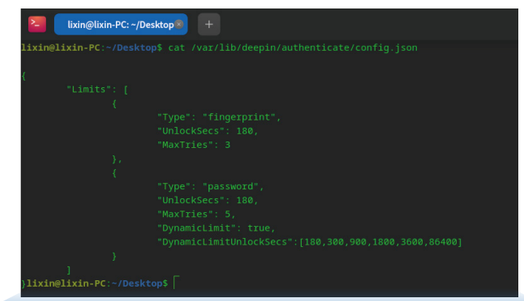
账号锁定策略

多少次登录失败后，应有账号锁定策略

判定依据

检查方法

执行命令：
cat /var/lib/deepin/authenticate/config.json



参数说明：

01 **type：**
认证方式，fingerprint 为指纹认证，password 为密码认证

02 **UnlockSecs：**
超出认证失败次数后，解除锁定需要等待的时间（秒数），如果 <0 则永久锁定

03 **MaxTries：**
认证失败几次后拒绝 , 如果 == 0 则不限制

04 **DynamicLimi：**
是否动态锁定

05 **DynamicLimitUnlockSecs：**
动态锁定时间 , 可随次数变化 , 次数起始为 MaxTries , 第一个元素 x 含义为 , 失败 MaxTries 之后 , 锁定 x 秒

判定结果

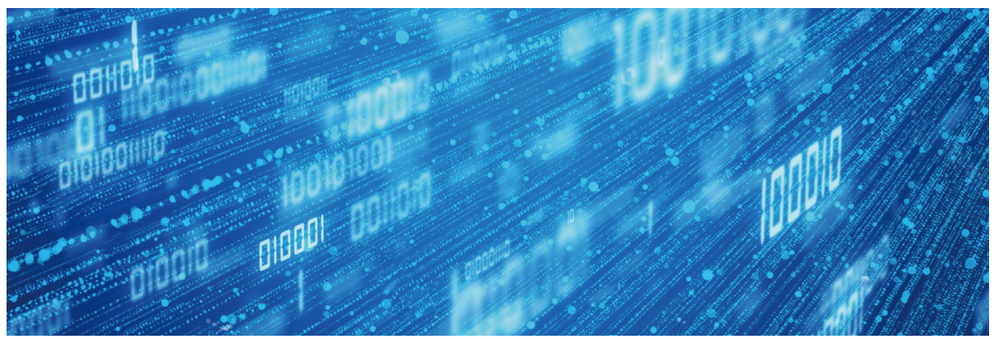
若 MaxTries 大于 0，UnlockSecs 大于 180，则通过

检查点

/var/lib/deepin/authenticate/config.json

加固方法

执行命令：sudo vim /var/lib/deepin/authenticate/config.json
将 MaxTries 设置大于 0，UnlockSecs 设置大于 180



认证授权

本地登录认证

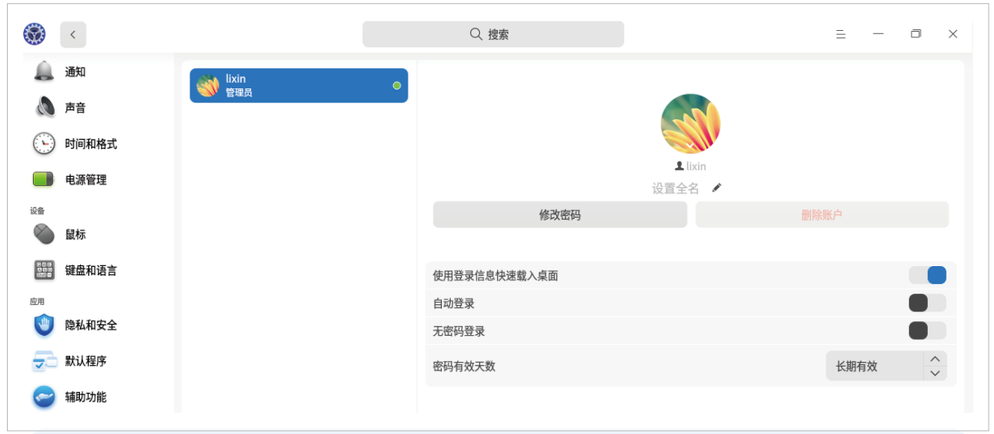
关闭直接登录

关闭免密登录

判定依据

检查方法

打开设置 - 账号，查看是否进行了配置



判定结果

若关闭了直接登录、关闭了免密登录，则通过

检查点

设置 - 账号

加固方法

打开设置 - 账号，关闭直接登录、关闭免密登录

清理账号

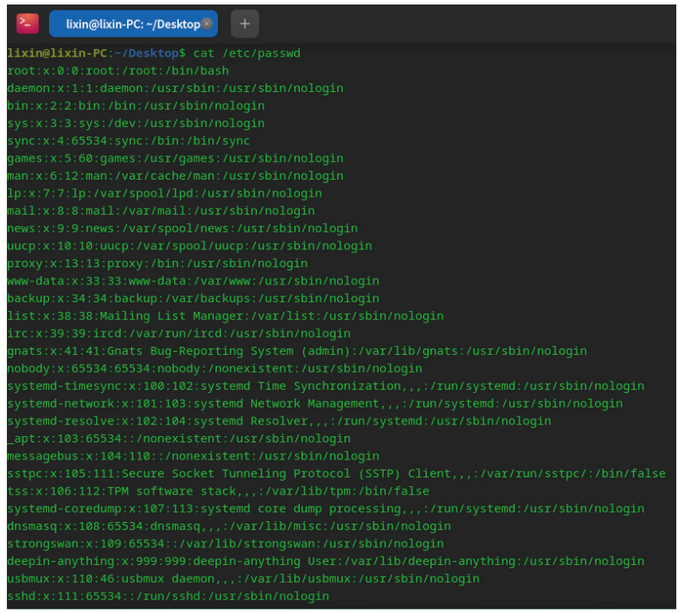
锁定系统中多余的自建账号

禁止存在除 root 之外 UID 为 0 的用户

判定依据

检查方法

执行命令：cat /etc/passwd



判定结果

若不存在无用账号，或无用账号不不允许登录、不存在除 root 账号外，uid 为 0 的用户则通过

检查点

/etc/passwd

加固方法

执行命令：passwd -l < 用户名 > # 锁定账号

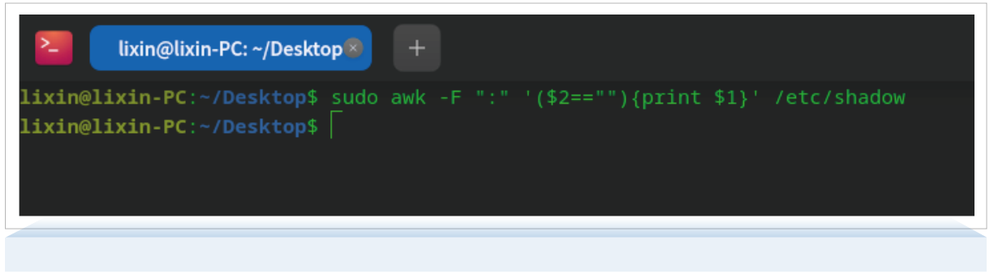
检查空口令账号

检查系统中的空口令账号

判定依据

检查方法

执行命令：sudo awk -F: '($2 == "") { print $1 }' /etc/shadow



判定结果

若无输出，则通过

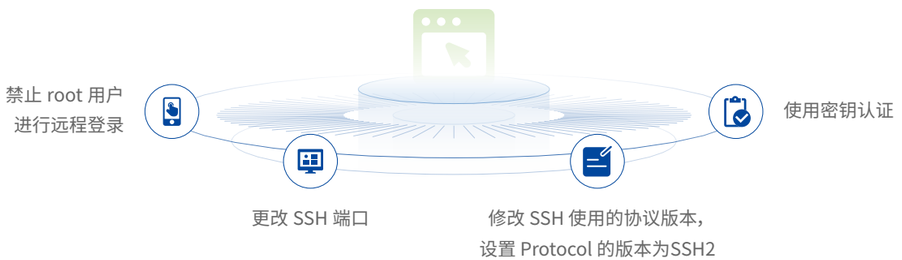
检查点

/etc/shadow

加固方法

执行命令：passwd -l < 用户名 > # 锁定账号

SSH 登录



判定依据

检查方法

执行命令：cat /etc/ssh/sshd_config

查看是否存在以下配置：

- PermitRootLogin no # 禁止 root 用户进行远程登录
- Port 2222 # 更改 SSH 端口
- Protocol 2 # 修改 SSH 使用的协议版本
- PubkeyAuthentication yes # 使用密钥认证
- AuthorizedKeysFile .ssh/authorized_keys # 制定存放密钥的文件路径
- PasswordAuthentication no # 关闭密钥认证方式

判定结果

若存在以上配置，则通过

检查点

/etc/ssh/sshd_config

加固方法

执行命令：cat /etc/ssh/sshd_config

按照以下配置：

- PermitRootLogin no # 禁止 root 用户进行远程登录
- Port 2222 # 更改 SSH 端口
- Protocol 2 # 修改 SSH 使用的协议版本
- PubkeyAuthentication yes # 使用密钥认证
- AuthorizedKeysFile .ssh/authorized_keys
- PasswordAuthentication no

重启 SSH 服务：sudo systemctl restart sshd

SSH 密钥配置方法：

- 执行命令，在家目录的 .ssh 目录下生成 id_rsa、id_rsa.pub 两个文件：ssh-keygen -t rsa
- 拷贝客户端 id_rsa.pub 的内容到服务器某个用户家目录下 .ssh 目录下的 authorized_keys 的文件中

文件权限

文件权限设置

设置 umask

判定依据

检查方法

执行命令，查看 umask 值：umask

判定结果

若结果为 0022，则通过

检查点

/etc/profile~/.profile

加固方法

执行命令打开配置文件，删除 umask 配置

- vim /etc/profile
- vim ~/.profile

执行命令，刷新配置文件

- sourc /etc/profile
- sourc ~/.profile

日志审计

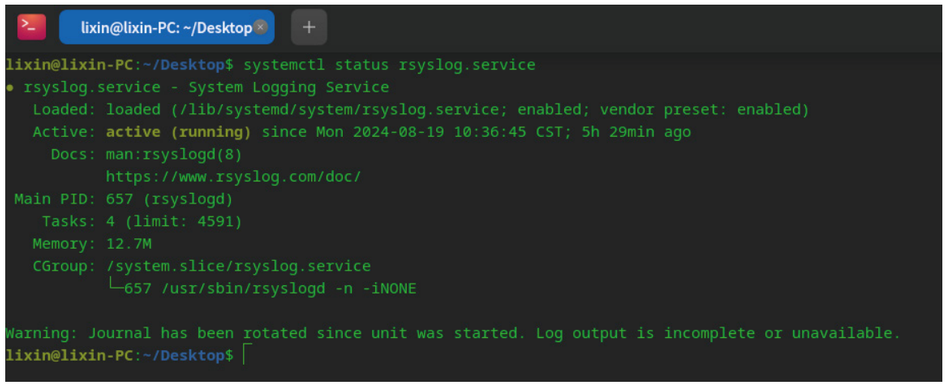
开启日志审计

开启 rsyslog 服务 | 设置日志权限 | 记录登录事件

判定依据

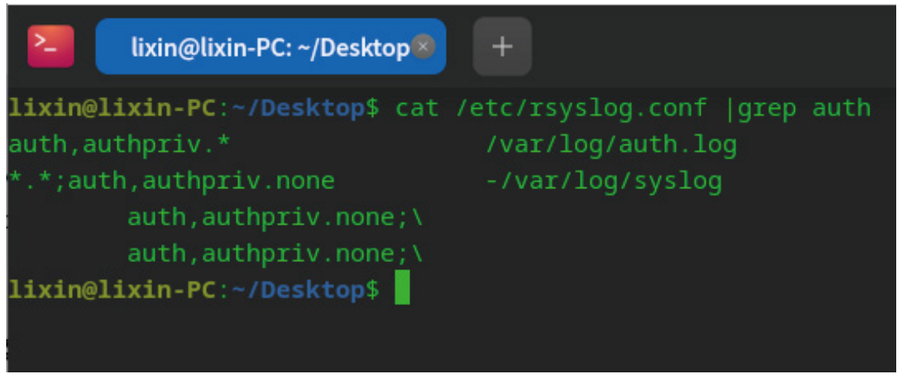
检查方法

执行命令，查看 rsyslog 是否启动：systemctl status rsyslog



执行命令，查看日志文件权限是否正确：ls -la /var/log/xxx.log

执行命令，查看是否开启了登录日志功能：cat /etc/rsyslog.conf |grep auth



判定结果

满足以下条件，则通过：

- rsyslog 服务已启动，服务状态为 running
- 日志文件拥有者为 root，拥有组为 root，或 adm
- authpriv.* 已配置文件路径，如 /var/log/auth.log

检查点

rsyslog 服务状态 | /var/log/*.log | /etc/rsyslog.conf

加固方法

01 执行命令，启动 rsyslog 服务：sudo systemctl start rsyslog

02 执行命令，设置 log 文件权限：sudo chmod 640 /var/log/xxx.log &chown root:root /var/log/xxx.log

03 执行命令，开启登录日志记录功能，设置 authpriv.* 文件路径：sudo vim /etc/rsyslog.conf

网络通信

开启防火墙

开启防火墙 | 配置防火墙规则

判定依据

检查方法

打开安全中心 - 防火墙，查看防火墙状态

判定结果

防火墙状态为开启，则通过

检查点

安全中心 - 防火墙

加固方法

打开安全中心 - 防火墙，开启防火墙

设置防火墙规则

系统版本

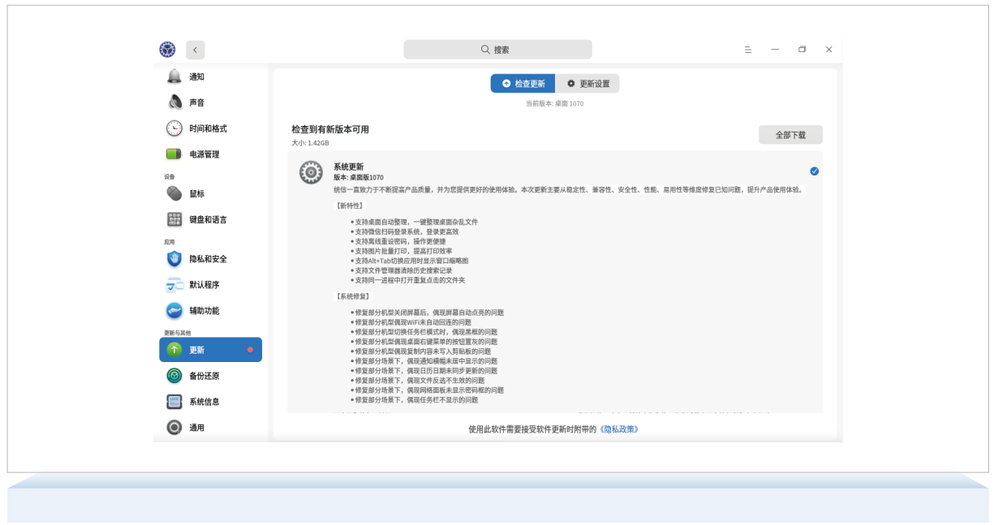
更新系统

更新系统至最新版本

判定依据

检查方法

打开安全中心 - 设置 - 更新，查看是否有新版本可用



判定结果

若不存在新版本，则通过

检查点

安全中心 - 设置 - 更新

加固方法

打开安全中心 - 设置 - 更新，点击全部下载

PREFACE

常见安全事件应急处置方式

挖矿事件

情况介绍

挖矿事件指的是攻击者利用技术手段对受害者进行网络攻击，在受害者的网络设备中植入挖矿木马，非法占用其计算资源来进行加密货币的挖掘活动。挖矿事件不仅消耗大量的计算机处理资源，严重危害受害者的计算机安全和性能，还可能导致业务中断等严重后果。以下是挖矿事件的显著特征：

- 电脑变得非常卡，频繁无响应、风扇异响、反复重启
- CPU 的使用率会变得非常高，甚至会超过 100%
- 网络流量变大
- 耗电量急剧上升

应急处置

处置前准备

备份数据
在进行任何处置前，确保对重要数据进行冗余备份，防止数据丢失

隔离受感染服务器
从网络中隔离受影响的服务器，防止影响扩散到其他系统

收集证据
记录当前系统状态，包括进程列表、网络连接、系统日志等，为后续分析和追踪溯源提供依据

准备工具
确保拥有必要的安全工具，如杀毒软件、系统监控工具、网络分析工具等

处置过程

确认病毒类型

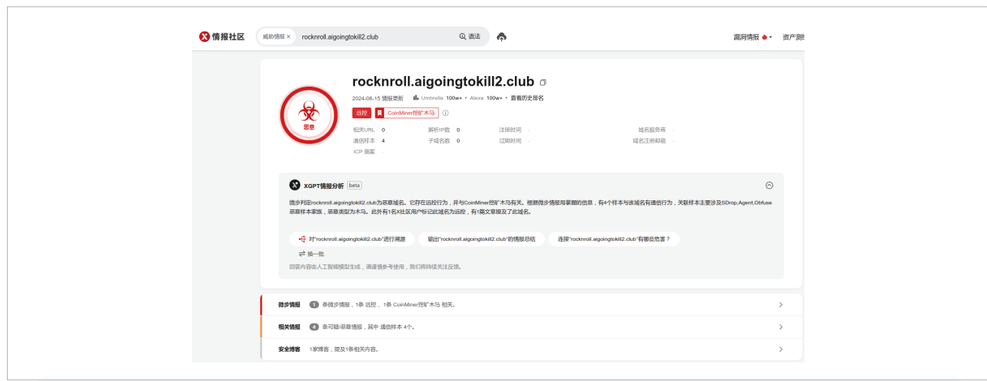
- **确定病毒 ioc 信息**

对系统日志、网络流量、安全设备警报等进行全面监测和分析，获取病毒 ioc 信息

- **确认恶意木马类型**

根据 ioc 确定木马类型：

- Virustotal
- 深信服威胁情报中心
- 微步在线
- 安恒威胁情报中心
- 360 威胁情报中心
- 绿盟威胁情报中心



获取异常进程 pid

▪ **CPU 占用**

top -c -o %CPU

- -c 参数显示进程的命令行参数
- -o 参数可按照进程 CPU 使用百分比进行排序
- -p 参数可指定进程的 pid

▪ **内存占用**

top -c -o %MEM

- -c 参数显示进程的命令行参数
- -o 参数可按照进程内存使用百分比进行排序
- -p 参数指定进程的 pid

▪ **网络占用**

nethogs

- apt-get install nethogs 安装 nethogs
- nethogs 查看网络占用

确认恶意文件样本

▪ **根据 pid 获取进信息**

lsof -p pid

查看进程正在读写的文件

pwdx pid

获取该 pid 的进程启动的时候的目录

systemctl status pid

获取进程的 status 信息

cat /proc/pid/maps

查看进程加载的链接库

ls -al /proc/pid/exe

查看进程文件的路径

pstree -agplU

全面展示进程与线程间的关系

▪ **确定恶意程序运行时间**

ps -w -eo pid,lstart,etime,cmd | grep <pid> 查看程序运行时间

处理异常进程

▪ **进程查杀**

若存在守护进程，先杀掉守护进程

- ps -w ajfx
- kill -9 pid

查看异常进程是否存在子进程

- ps -w ajfx
- systemctl status

无子进程，杀掉进程

- kill -9 pid

有子进程，杀掉进程组

- kill -9 -pid

▪ **线程查杀**

如果木马病毒作为线程，被附到现有正常业务的进程中，查杀该线程风险比较大，极可能会导致业务进程崩掉，杀死线程的方法和杀死进程一样

pstree -agplU 全面展示进程与线程间的关系

kill -9 pid 杀掉线程

▪ **计划任务清理**

需要检查的文件：

/etc/crontab

/etc/cron.d/*

/var/spool/cron/xxxx

使用 vim 打开文件，检查是否存在恶意的计划任务，并删除

删除恶意文件

查看文件占用

- lsof eval.sh
- 如果存在进程占用，那么占用进程也可能是恶意进程，需要按照之前的步骤进行查看

a 和 i 属性导致文件不可删除

- a 属性文件只能增加内容，不能修改之前的文件，不能删除文件
- i 属性内容不能改变，文件不能删除
- 可以使用 chattr -a 和 chattr -i

奇怪文件名导致文件不可删除

- 从 windows 向 linux 传输的文件或者攻击者恶意制造的文件，很多会有文件名乱码，无法直接通过乱码的文件名进行删除，可以 使用 inode 来确定文件名，之后删除
- 查看 inode：ls -li eval.sh
- 删除文件：find ./* -inum 12327526 -exec rm -i {} \; (会有一步确认是否删除)

目录挂载导致无法删除

- 查看目录挂载情况：lsblk -a
- 取消挂载：umount /dev/xx

处置情况确认

通过以下方式确认挖矿病毒是否清理完成：

检查 CPU 和内存使用情况

使用 top、htop 或 nmon 等工具监控系统资源使用情况，确认没有异常的资源占用

检查进程列表

再次使用 ps、ps aux 或 top 命令检查所有运行中的进程，确保没有可疑的挖矿进程

检查网络连接

使用 netstat、ss 或 lsof 等命令检查网络连接和监听端口，确保没有可疑的网络活动

检查计划任务和定时任务

使用 crontab -l 检查当前用户的所有计划任务，确认没有可疑的定时执行任务

检查系统启动项

检查 /etc/rc.local、/etc/init.d/、systemctl 等与系统启动相关的配置，确保没有添加可疑的自启动程序

全盘搜索挖矿程序

使用 find 命令搜索整个文件系统，查找可能遗漏的挖矿程序文件或脚本

使用杀毒软件扫描

使用杀毒软件或反恶意软件工具进行全系统扫描，确保没有遗漏的病毒或恶意软件

检查账户安全

确认没有新增的可疑用户账户，检查现有账户的密码强度，并确保没有弱口令

检查系统漏洞

使用漏洞扫描工具检查系统是否存在已知漏洞，并及时打补丁更新

检查系统配置

确认系统配置没有被篡改，如 .bashrc、.bash_profile、.profile 等配置文件

监控系统行为

在一段时间内持续监控系统行为，看是否有复发的迹象

远控后门

情况介绍

远控后门，也称为远程控制木马或后门程序，是一种恶意软件，一般由攻击者攻击成功之后植入受害者网络设备，从而使攻击者可持续未经授权情况下远程控制受害者的计算机或网络设备。这类程序具有强大的功能，能够在受害者完全不知情的情况下执行各种操作，包括但不限于窃取数据、配置代理服务器、攻击其他计算机、控制摄像头等。以下是远控后门的一些关键特点和分析：

远控后门被设计为尽可能隐蔽，避免被用户或安全软件发现。它们可能会隐藏自己的文件、进程、网络连接等

隐蔽性

持久化机制

远控后门会在系统中建立持久化机制，确保在系统重启后依然能够执行。这可能通过修改服务、启动文件夹或计划任务来实现

多阶段加载

恶意代码从植入目标系统到最终远控运行，通常会经历多阶段加载。后续载荷获取方式包括从当前载荷自身数据提取、读取其他文件数据以及从 C2 服务器下载

反侦察功能

一些高级的远控后门具备反调试和反沙箱功能，能够检测并规避分析和安全措施

更新和变种

远控后门会不断更新和变化，以逃避检测和查杀，包括使用新的免杀技术、传播途径和控制指令

代码混淆和加密

为了避免检测分析，远控后门的载荷基本都会经过加密处理，使用的加密算法包括各类 XOR 加密和对称加密（比如 RC4、AES）。有些还会使用图片隐写技术隐藏后续载荷

应急处置

处置前准备

应急处置前，准备工作如下：

备份数据

在进行任何处置前，确保对重要数据进行备份，防止数据丢失

隔离受感染服务器

从网络中隔离受影响的服务器，防止影响扩散到其他系统

收集证据

记录当前系统状态，包括进程列表、网络连接、系统日志等，为后续分析和追踪溯源提供依据

准备工具

确保拥有必要的安全工具，如杀毒软件、系统监控工具、网络分析工具等

处置过程

获取后门信息

根据 EDR、态势感知平台的安全产品告警的信息，获取后门文件的路径或外连 ip

获取远控后门进程

根据后门文件查找进程 pid：

- lsof | grep test.sh
- lsof /test.sh　需要指定后门路径

根据目的 ip 及端口查找进程 pid：

- netstat -pantu | grep “ip”
- netstat -pantu | grep “port”
- lsof -i:“port”

确定远控后门运行时间

- 查看运行时间：ps -w -eo pid,lstart,etime,cmd | grep <pid>

处理异常进程

▪ **进程查杀**

若存在守护进程，先杀掉守护进程

- ps -w ajfx
- kill -9 pid

查看异常进程是否存在子进程

- ps -w ajfx
- systemctl status

无子进程，杀掉进程

- kill -9 pid

有子进程，杀掉进程组

- kill -9 -pid

▪ **线程查杀**

如果木马病毒作为线程，被附到现有正常业务的进程中，查杀该线程风险比较大，极可能会导致业务进程崩掉，杀死线程的方法和杀死进程一样

- pstree -agplU 全面展示进程与线程间的关系
- kill -9 pid 杀掉线程

▪ **计划任务清理**

需要检查的文件：

- /etc/crontab
- /etc/cron.d/*
- /var/spool/cron/xxxx

使用 vim 打开文件，检查是否存在恶意的计划任务，并删除

删除恶意文件

查看文件占用

- lsof eval.sh
- 如果存在进程占用，那么占用进程也可能是恶意进程，需要按照之前的步骤进行查看

a 和 i 属性导致文件不可删除

- a 属性文件只能增加内容，不能修改之前的文件，不能删除文件
- i 属性内容不能改变，文件不能删除
- 可以使用 chattr -a 和 chattr -i

奇怪文件名导致文件不可删除

- 从 windows 向 linux 传输的文件或者攻击者恶意制造的文件，很多会有文件名乱码，无法直接通过乱码的文件名进行删除，可以使用 inode 来确定文件名，之后删除
- 查看 inode：ls -li eval.sh
- 删除文件：find ./* -inum 12327526 -exec rm -i {} \; (会有一步确认是否删除)

目录挂载导致无法删除

- 查看目录挂载情况：lsblk -a
- 取消挂载：umount /dev/xx

处置情况确认

通过以下方式确认远控后门是否清理完成：

检查网络连接

使用 netstat、ss 或 lsof 等命令检查网络连接和监听端口，确保没有可疑的网络活动

检查计划任务和定时任务

使用 crontab -l 检查当前用户的所有计划任务，确认没有可疑的定时执行任务

检查系统启动项

检查 /etc/rc.local、/etc/init.d/、systemctl 等与系统启动相关的配置，确保没有添加可疑的自启动程序

全盘搜索远控后门

使用 find 命令搜索整个文件系统，查找可能遗漏的远控后门文件

使用杀毒软件扫描

使用杀毒软件或反恶意软件工具进行全系统扫描，确保没有遗漏的远控后门文件

检查账户安全

确认没有新增的可疑用户账户，检查现有账户的密码强度，并确保没有弱口令

检查系统漏洞

使用漏洞扫描工具检查系统是否存在已知漏洞，并及时打补丁更新

检查系统配置

确认系统配置没有被篡改，如 .bashrc、.bash_profile、.profile 等配置文件

监控系统行为

在一段时间内持续监控系统行为，看是否有复发的迹象

勒索病毒

情况介绍

勒索病毒，是一种极具传播性和破坏性的恶意软件，泛指一切通过锁定被感染者计算机系统或文件并施以敲诈勒索的新型计算机病毒。采用复杂的加密算法对用户的文件进行加密，使受害者无法访问或使用这些数据。加密完成后，病毒通常会显示一条勒索信息，要求受害者支付一定金额的赎金以获取解密密钥或恢复数据的方法。这些赎金通常以加密货币的形式支付，以隐藏交易的真实身份和避免追踪。其特征如下：

- 系统文件被加密无法读取、计算机无法正常使用
- 会在桌面等明显位置生成勒索提示文件

应急处置

处置前准备

应急处置前，准备工作如下：

处置过程

确定勒索病毒类型

判断勒索病毒类型方式如下：

- 勒索页面主动说明的，直接粘贴到 baidu、google 里面搜索
- 勒索加密文件的后缀名
- 在线网站识别
  - 360 安全卫士 - 勒索病毒解密
  - 腾讯电脑管家 - 勒索病毒搜索引擎
  - 奇安信 - 勒索病毒搜索引擎
  - 腾讯哈勃勒索病毒安全工具
  - 深信服 EDR
  - VenusEye 勒索病毒搜索引擎

系统恢复

通过以下步骤恢复系统：

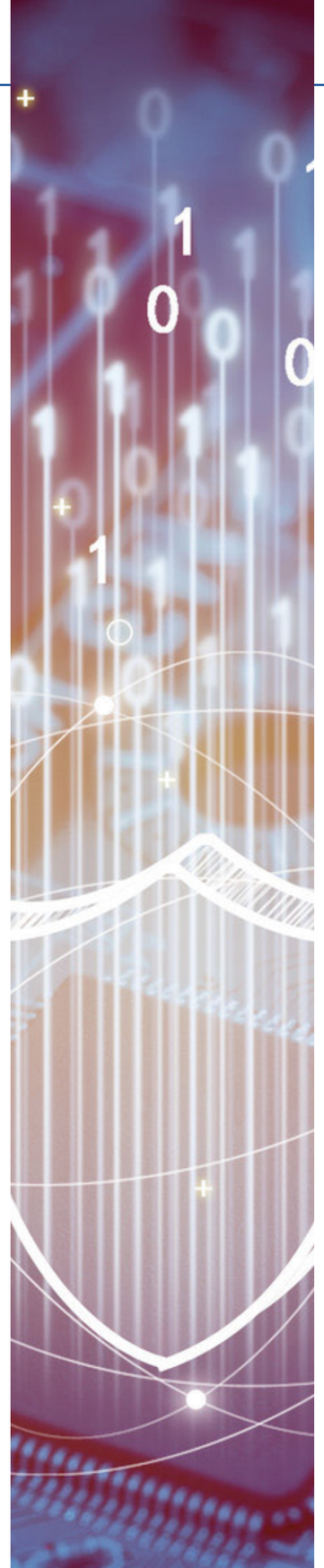
- 如果事先有备份，可以从备份中恢复被加密的文件
- 使用在线工具进行解密
  - 360 安全卫士 - 勒索病毒解密
  - 腾讯电脑管家 - 勒索病毒搜索引擎
  - 奇安信 - 勒索病毒搜索引擎
  - 腾讯哈勃勒索病毒安全工具
  - 深信服 EDR
  - VenusEye 勒索病毒搜索引擎
- 联系安全厂商解密
- 支付赎金解密

系统升级

升级操作系统安装安全补丁

系统备份

异地备份被感染过的系统



处置情况确认

通过以下方式确认勒索病毒是否清理完成：

文件排查

确保系统中的文件不存在被加密的迹象，比如文件扩展名未修改为勒索病毒特定的扩展名

远控后门排查

确保系统中是否存在远控后门

漏洞排查

确保系统是否存在已知漏洞

检查网络连接

使用 netstat、ss 或 lsof 等命令检查网络连接和监听端口，确保没有可疑的网络活动

检查计划任务和定时任务

使用 crontab -l 检查当前用户的所有计划任务，确认没有可疑的定时执行任务

检查系统启动项

检查 /etc/rc.local、/etc/init.d/、systemctl 等与系统启动相关的配置，确保没有添加可疑的自启动程序

全盘搜索远控后门

使用 find 命令搜索整个文件系统，查找可能遗漏的远控后门文件

使用杀毒软件扫描

使用杀毒软件或反恶意软件工具进行全系统扫描，确保没有遗漏的远控后门文件

检查账户安全

确认没有新增的可疑用户账户，检查现有账户的密码强度，并确保没有弱口令

检查系统配置

确认系统配置没有被篡改，如 .bashrc、.bash_profile、.profile 等配置文件

监控系统行为

在一段时间内持续监控系统行为，看是否有复发的迹象

暴力破解

情况介绍

暴力破解（Brute Force Attack）是一种常见的攻击行为，攻击者通过尝试各种组合和密码来解密目标系统或数据的加密保护。这种攻击方法不涉及深入的技术细节或社会工程学的高级手段，多依赖于大量的计算资源和时间来进行穷举式的尝试。暴力破解攻击主要针对以下服务：

ssh | mysql | ftp | redis

应急处置

处置前准备

应急处置前，准备工作如下：

备份数据

在进行任何处置前，确保对重要数据进行备份，防止数据丢失

隔离服务器

从网络中隔离受影响的服务器，防止影响扩散到其他系统

收集证据

记录当前系统状态，包括进程列表、网络连接、系统日志等，为后续分析和追踪溯源提供依据

准备工具

确保拥有必要的安全工具，如杀毒软件、系统监控工具、网络分析工具等

处置过程

SSH 暴力破解

检查网络连接信息：netstat -pantu

```
lixin@lixin-PC:~/Desktop$ netstat -pantu
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:50010         0.0.0.0:*               LISTEN      7838/wineserver
tcp        0      0 10.20.33.202:5821       0.0.0.0:*               LISTEN      7838/wineserver
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:16308         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:16090         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:16067         0.0.0.0:*               LISTEN      -
tcp       32      0 10.20.33.202:49280      157.148.45.186:443      CLOSE_WAIT  7838/wineserver
tcp        0      0 127.0.0.1:40910         127.0.0.1:41531         ESTABLISHED 7838/wineserver
```


Proto 协议类型

Recv-Q：表示收到的数据已经在本地接收缓冲，但是还有多少没有被进程取走，如果接收队列 Recv-Q 一直处于阻塞状态，可能是遭受了拒绝服务 denial-of-service 攻击。

Send-Q：对方没有收到的数据或者说没有 Ack 的，还是本地缓冲区。如果发送队列 Send-Q 不能很快的清零，可能是有应用向外发送数据包过快，或者是对方接收数据包不够快

Local Address：本机地址，一般有以下几种模式

- *:80 监听 IPv4 或 IPv6 的任意 IP 的 80 端口
- :::80 监听 IPv6 和 IPv4 的任意 IP 的 80 端口
- 0.0.0.0:80 监听任意 IPv4 地址的 80 端口
- 127.0.0.1:80 监听本地的 80 端口，只能本地访问
- ::1:80 监听本次 IPv6 的回环地址，只能本地访问
- 192.168.1.1:80 监听 IP 地址 192.168.1.1 的 80 端口

Foreign Address：外部地址规则和 Local Address 规则一样

State 网络状态

- LISTEN 侦听状态，等待对端连接
- SYN_SENT 客户端发送建立连接的 SYN 请求后状态为 SYN_SENT
- SYN_RECV 服务端发送 SYN+ACK 后网络状态为 SYN_RECV
- ESTABLISHED 已经建立起连接
- FIN_WAIT1 主动端四次挥手主动发起的第一个包，也就是 FIN 包之后网络状态为 FIN_WAIT1
- CLOSE_WAIT 被动端收到四次挥手的 FIN 包，发送 ACK 后处于 CLOSE_WAIT
- FIN_WAIT2 主动关闭端接到 ACK 后进入 FIN_WAIT2，等待对端发下一个 FIN
- LAST_ACK 被动关闭端发送第二个 FIN 后进入 LAST_ACK 状态，等待最后一个 ACK 的到来
- TIME_WAIT 主动端发送最后一个 ACK，之后进入 TIME_WAIT 状态，等待一段时间确保对端接收到了 ACK
- CLOSING 在 TCP 四次挥手期间，主动关闭端发送了 FIN 包后，没有收到对应的 ACK 包，却收到对方的 FIN 包，此时，进入 CLOSING 状态
- CLOSED 被动关闭端在接受到 ACK 包后，就进入了 closed 的状态。连接结束
- UNKNOWN 未知的 Socket 状态

PID/Program name 进程 ID 和进程名

SSH 遭到暴力破解时，22 端口将会存在大量的 ESTABLISHED 状态的连接

查看正在连接的 ssh sessions：who -a

查看 SSH 日志信息

查看登录成功的日志：cat /var/log/auth.log | grep "Accept"

查看登录失败的日志：cat /var/log/auth.log | grep "Failed password for" | more

统计登录失败的用户名以及次数：grep "Failed password" /var/log/auth.log|perl -e 'while($_=<>){ /for(.*?)from/; print "$1\n";}'|sort|uniq -c|sort -nr

统计暴力破解的登录者（IP）：cat /var/log/auth.log | grep "Failed password for" | cut -d " " -f 9 | sort -nr | uniq|grep -v "invalid"| while read line;do echo [$line];cat /var/log/auth.log | grep "Failed password for" | grep $line | grep -Po '(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|[1-9])(\.(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|\d)){3} '|sort|uniq -c |sort -nr; done

统计不存用户的登录：cat /var/log/auth.log | grep "Failed password for" | grep "invalid"| cut -d " " -f 11 | sort -nr | uniq| while read line;do echo [$line];cat /var/log/auth.log | grep "Failed password for" | grep $line | grep -Po '(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|[1-9])(\.(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|\d)){3} '|sort|uniq -c |sort -nr;done

Mysql 暴力破解

查看登录错误用户名的登录 IP 以及次数：cat /var/log/mysql/error.log | grep "Access denied for user" | grep "using password: YES" | awk -F "'" '{print $2}' | sort| uniq | while read line;do echo $line;cat /var/log/mysql/error.log | grep "Access denied for user" | grep "using password" | awk -F "'" '{print $4}' | sort | uniq -c | sort -nr; done

FTP 暴力破解

检查网络连接信息：netstat -pantu

若存在暴力破解，则 21 端口有大量的 ESTABLISHED 状态和 TIME_WAIT 状态的网络连接

查看登录失败的用户的登录 IP：cat /var/log/vsftpd.log | grep FAIL | cut -d "[" -f 3 | cut -d "]" -f 1 | sort | uniq | while read line;do echo $line;cat /var/log/vsftpd.log | grep $line | cut -d ":" -f 7 | cut -d '"' -f 1 | sort | uniq -c | sort -nr; done

Redis 未授权访问 & 暴力破解

redis 未授权访问：

连接 redis：redis-cli -h ip

redis 暴力破解：

检查网络连接信息：netstat -pantu

若存在暴力破解，则 6379 端口有大量的 ESTABLISHED 状态的网络连接

处置情况确认

通过以下方式确认暴力破解处置完成：

01 **更改口令：**确保口令是否更改，并且为高强度口令

02 **ip 封禁：**确保恶意 ip 已封禁

03 **检查网络连接：**使用 netstat、ss 或 lsof 等命令检查网络连接和监听端口，确保没有可疑的网络活动

04 **检查计划任务和定时任务：**使用 crontab -l 检查当前用户的所有计划任务，确认没有可疑的定时执行任务

05 **检查系统启动项：**检查 /etc/rc.local、/etc/init.d/、systemctl 等与系统启动相关的配置，确保没有添加可疑的自启动程序

06 **全盘搜索远控后门：**使用 find 命令搜索整个文件系统，查找可能遗漏的远控后门文件

07 **使用杀毒软件扫描：**使用杀毒软件或反恶意软件工具进行全系统扫描，确保没有遗漏的远控后门文件

08 **检查账户安全：**确认没有新增的可疑用户账户，检查现有账户的密码强度，并确保没有弱口令

09 **检查系统漏洞：**使用漏洞扫描工具检查系统是否存在已知漏洞，并及时打补丁更新

10 **检查系统配置：**确认系统配置没有被篡改，如 .bashrc、.bash_profile、.profile 等配置文件

11 **监控系统行为：**在一段时间内持续监控系统行为，看是否有复发的迹象

隧道

情况介绍

隐蔽隧道是一种绕过网络安全防护措施，如防火墙和入侵检测系统，进行数据传输的技术。攻击者常利用隐蔽隧道技术隐藏其攻击行为，传输恶意数据

应急处置

处置前准备

应急处置前，准备工作如下：

备份数据

在进行任何处置前，确保对重要数据进行备份，防止数据丢失

隔离受感染服务器

从网络中隔离受影响的服务器，防止影响扩散到其他系统

收集证据

记录当前系统状态，包括进程列表、网络连接、系统日志等，为后续分析和追踪溯源提供依据

准备工具

确保拥有必要的安全工具，如杀毒软件、系统监控工具、网络分析工具等

处置过程

获取隧道信息

隧道事件的事件来源一般有以下几种：

- 流量设备发现存在网络隧道
- 主机安全程序发现存在网络隧道或相关文件、进程
- 排查过程中发现存在跳板机痕迹等，进而发现隧道
- 运维相关人员发现异常端口等

SSH 隧道

检查监听端口

- netstat -tulnp | grep LISTEN
- 使用 netstat 命令查看系统上所有监听的端口。SSH 隧道可能会在本地端口上创建监听点

检查 SSH 进程

- ps aux | grep ssh
- 使用 ps 命令查看所有 SSH 相关进程，特别是那些使用端口转发的进程

检查已建立的隧道

- ss -o state established -t '(dport = :ssh or sport = :ssh)'
- 对于已经建立的 SSH 隧道，可以使用 ss 命令查看所有 SSH 连接，包括隧道

检查 SSH 日志

- cat /var/log/auth.log
- 查看 SSH 服务的日志文件，搜索与端口转发相关的日志条目

DNS 隧道

网络连接检查

- 使用 netstat -anp 命令查看系统中所有的网络连接
- 查找与 DNS 相关的连接，特别是那些连接到外部 DNS 服务器的不寻常连接

监控网络流量

- 使用网络流量分析工具，如 Wireshark，设置过滤器来重点关注 DNS 流量，可以使用 dns 作为过滤器关键字，分析捕获到的 DNS 数据包，查看是否有异常的 DNS 请求和响应
- 正常情况下，DNS 请求的频率相对较低且较为随机。如果发现某个主机频繁地发出 DNS 请求，可能存在异常
- 观察 DNS 请求的域名模式，DNS 隧道可能会使用一些不寻常的、长且复杂的域名，或者域名中包含编码信息

检查系统进程

- 查看正在运行的进程，查找可能与 DNS 隧道相关的程序
- 使用 ps aux 命令列出所有进程，一些已知的用于建立 DNS 隧道的工具可能会在进程列表中出现，如 dns2tcp、dnscat2、iodine 等

入侵检测系统(IDS)

使用 IDS 监视网络流量，查找表明恶意活动的模式和行为，以检测 DNS 隧道

分析 DNS 隧道工具流量特征

DNS 隧道工具的流量特征与其正常流量不同，例如，使用特定记录类型（如 TXT 或 NULL）的比例异常高，或者域名中数字字符占比异常，可以作为检测 DNS 隧道的指标

ICMP 隧道

检查网络连接

- 使用 netstat -anp 命令查看系统中所有的网络连接，包括 TCP、UDP 和 ICMP
- 查找与 ICMP 相关的连接，看是否有不寻常的连接到外部服务器的情况

监测网络流量

- 使用网络流量监测工具，如 Wireshark、Tcpdump 等，捕获网络数据包
- 对于 Wireshark，可以选择合适的网络接口进行捕获，然后在过滤器中输入 icmp 来筛选出 ICMP 数据包
- 使用 Tcpdump 可以运行命令如 tcpdump -i eth0 icmp（假设 eth0 是要监测的网络接口）
- 正常的 ICMP 数据包通常是用于网络诊断和错误报告，如 ping 请求和响应，而 ICMP 隧道可能会表现出异常的数据包大小、频繁的 ICMP 请求和响应、不寻常的 ICMP 类型和代码等

检查系统进程

- 查看系统中正在运行的进程，是否有可疑的进程可能在使用 ICMP 隧道
- 使用 ps -aux 命令列出所有进程，然后仔细检查进程名、命令行参数和运行用户等信息
- 对于一些已知的可能用于建立隧道的工具，如 icmptunnel、ptunnel 等，可以通过 grep 进行搜索，例如 ps -aux | grep icmptunnel

检查系统日志

- 查看系统日志文件，如 /var/log/syslog、/var/log/messages 等，看是否有与 ICMP 相关的异常日志记录

HTTP/HTTPS 隧道

检查系统连接

- 使用 netstat -anp 命令查看系统中所有的网络连接，查找与 HTTP/HTTPS 端口相关的连接，特别是那些连接到陌生 IP 地址或不常见的域名的连接

监测网络流量

- 使用网络流量分析工具，如 Wireshark，设置过滤器来重点关注 HTTP/HTTPS 流量，可以使用 http 或 tcp.port==80（对于 HTTP）以及 tcp.port==443（对于 HTTPS）作为过滤器关键字，查看是否有异常的 HTTP/HTTPS 请求和响应
- 正常的 HTTP/HTTPS 流量通常是用户发起的网页浏览、API 调用等。如果发现大量持续的、规律性的流量，且流量的大小、频率或目的地不寻常，可能存在隧道的迹象

检查系统进程

- 使用 ps -aux 命令列出所有正在运行的进程，查找可能与 HTTP/HTTPS 隧道相关的进程，如代理软件、网络工具等

分析系统日志

- 查看 Web 服务器日志（如果系统中有运行的 Web 服务器）
- 例如，Apache 的访问日志通常位于 /var/log/apache2/access.log，Nginx 的访问日志通常在 /var/log/nginx/access.log
- 检查是否有异常的请求记录，如大量来自同一 IP 地址的请求、不寻常的请求方法或 URL 路径等
- 检查系统安全日志，如 /var/log/syslog 或 /var/log/messages，看是否有与 HTTP/HTTPS 相关的异常事件记录

文件查杀

- 使用 webshell 查杀工具进行查询，如 D 盾、webshellkiller、河马查杀等

Socks 隧道

检查网络连接

- 使用 netstat -anp 命令查看系统中所有的网络连接状态
- 查找与 SOCKS 相关的连接，通常 SOCKS 服务器使用端口 1080，但也可能使用其他自定义端口
- 可以结合 lsof -i :<port> 命令来查看特定端口上的进程信息，以确定是否有与 SOCKS 相关的进程在使用该端口

检查系统进程

- 使用 ps aux 命令列出所有正在运行的进程
- 查找可能与 SOCKS 隧道相关的进程，如 SOCKS 代理软件、网络工具等

分析系统日志

- 查看系统日志文件，如 /var/log/syslog、/var/log/messages 等
- 查找与网络连接或可疑进程相关的日志记录

处置情况确认

通过以下方式确认挖矿病毒是否清理完成：

检查网络连接

使用 netstat、ss 或 lsof 等命令检查网络连接和监听端口，确保没有可疑的网络活动

检查计划任务和定时任务

使用 crontab -l 检查当前用户的所有计划任务，确认没有可疑的定时执行任务

检查系统启动项

检查 /etc/rc.local、/etc/init.d/、systemctl 等与系统启动相关的配置，确保没有添加可疑的自启动程序

全盘搜索远控后门

使用 find 命令搜索整个文件系统，查找可能遗漏的远控后门文件

使用杀毒软件扫描

使用杀毒软件或反恶意软件工具进行全系统扫描，确保没有遗漏的远控后门文件

检查账户安全

确认没有新增的可疑用户账户，检查现有账户的密码强度，并确保没有弱口令

检查系统漏洞

使用漏洞扫描工具检查系统是否存在已知漏洞，并及时打补丁更新

检查系统配置

确认系统配置没有被篡改，如 .bashrc、.bash_profile、.profile 等配置文件

监控系统行为

在一段时间内持续监控系统行为，看是否有复发的迹象