

企业版

# 部署火绒后安全加固建议

火绒终端安全管理系统 V2.0 >>>

2024/12



公 司：北京火绒网络科技有限公司  
地 址：北京市朝阳区北苑路北京文化创意大厦 B 座 9 层  
网 址：<https://www.huorong.cn>  
电 话：400-998-3555

## 版权声明

本文件所有内容版权受中国著作权法等有关知识产权法保护，为北京火绒网络科技有限公司（以下简称“火绒安全”）所有。

未经火绒安全允许，不得转载本文件内容，否则将视为侵权。转载或者引用本文内容请注明来源及原作者。

对于不遵守此声明或者其他违法使用本文件内容者，火绒安全依法保留追究其法律责任的权利。

另外，火绒安全保留修改本文件中描述产品的权利。如有修改，不另行通知。

# 目录 | CONTENTS

<b>第一章 概述</b> .....	5
<b>第二章 火绒中心设置</b> .....	6
2.1 火绒终端分组.....	6
2.2 配置终端策略.....	6
2.3 火绒终端安全防护.....	8
2.4 账号设置.....	8
<b>第三章 主机防护加固项</b> .....	10
3.1 信任区和隔离区保护.....	10
3.2 部署安全软件.....	11
3.3 开启勒索诱捕.....	12
3.4 开启远程登录防护.....	13
3.5 开启终端动态口令安全认证.....	13
3.6 高危端口控制.....	15
3.7 账号密码管理.....	17
<b>第四章 员工安全意识与使用习惯</b> .....	18
4.1 移动存储设备的使用.....	18

4.2 即时通讯钓鱼 .....	18
4.3 钓鱼网页 .....	19
4.4 邮件收发 .....	19
4.5 漏洞修复 .....	20
4.6 事件日志 .....	21
4.7 火绒终端拦截日志.....	22
<b>第五章 总结 .....</b>	<b>23</b>
<b>第六章 案例 .....</b>	<b>24</b>
6.1 恶意邮件 .....	24
6.2 RDP 爆破.....	25
6.3 MICROSOFT SQL SERVER 数据库被入侵.....	28
6.4 感染型病毒 .....	29

# 第一章 概述

在安装火绒企业版中心，部署火绒终端后，建议您根据企业网络环境、运行业务、计算机性能、工作习惯对 Windows 系统与火绒进行配置，以提高企业内安全性，该文档以“火绒中心设置”、“主机防护加固项”和“员工安全意识与使用习惯”三方面提出加固建议。

## 第二章 火绒中心设置

可以根据需求，在火绒中心内进行以下设置。

### 2.1 火绒终端分组

对已经部署火绒终端的计算机，根据部门、业务、区域、使用时段等进行分组，应用不同的安全策略，以便后期进行维护。

例如根据业务，对外网可访问的服务器进行单独分组，单独制定针对该服务器的策略，例如修改文件实时监控级别，禁止外网访问该组内服务器的 3389 端口等，以提高安全性。

### 2.2 配置终端策略

(1) 如果业务和机器性能允许，将策略内的文件实时监控->扫描时机修改为以下任意一项：

“在文件发生变化时进行扫描,将占用少量系统资源(中级、推荐)”

“在文件发生所有类型操作时进行扫描，将占用较多系统资源(高级)”

设置此选项后，会修改火绒的监控级别为“在文件发生变化时进行扫描，将占用少量系统资源”，提高文件实时监控敏感度，尽早发现病毒并处理。但是会增加一些系统资源占用，建议根据计算机性能酌情进行设置。



(2) 设置文件实时监控->发现病毒时选项为“自动处理”，防止员工在终端误操作导致病毒被运行。



## 2.3 火绒终端安全防护

(1) 设置火绒终端“管理员密码保护”和“防止终端卸载密码”，防止员工修改火绒终端设置，退出或卸载火绒终端。



## 2.4 账号设置

(1) 配置账号的联系方式等信息明确账号使用者，配置登录地址限制，防止密码泄露后非授权登录。



账号设置

\* 账号: admin 5/32

\* 密码: ..... 重置密码

下次登录:  强制修改密码

联系方式: 请输入手机号

备注: 请输入备注 0/512

\* 登录地址限制:  不限制  IP地址 ⓘ

多个IP通过换行进行区分, 支持单个IP和IP段 0/2000

(2) 配置账号的自动登出设置和动态认证设置防止账户非授权访问。定期修改密码设置防止密码泄露。

管理员账号设置

自动登出设置

账号自动登出时间: 30 分钟

动态认证设置 [查看动态口令操作指南](#)

开启动态认证

账号登录启用动态认证

高危操作启用动态认证 ⓘ

高危操作认证有效时间: 0 分钟 ⓘ

定期修改密码设置

开启密码更新检查

更新周期: 90 天 ⓘ

保存 取消

# 第三章 主机防护加固项

## 3.1 信任区和隔离区保护

开启禁止信任区操作功能，防止用户将病毒文件（目录）添加信任区。

开启禁止隔离区操作功能，防止用户恢复隔离区内病毒文件。



### 3.2 部署安全软件

全网部署火绒企业版终端，通过火绒终端安全管理系统监控全网环境。定期下发查杀任务，可使用火绒中心内的“计划任务”工具创建周期性的扫描。

(1) 在发现病毒后，将中毒终端移动至临时分组，并设置相应防护策略，例如修改“文件实时监控”级别，下发全盘扫描等。处理结束后可在中心日志内查看相应终端的查杀结果，判断病毒处理情况。

(2) 如在分组内计算机长时间运行在无人值守的情况下，无法在病毒查杀后点击处理，就需要将该分组策略进行修改，将病毒查杀->发现病毒时的动作，修改为“自动处理”。无需人工再次点击确认。

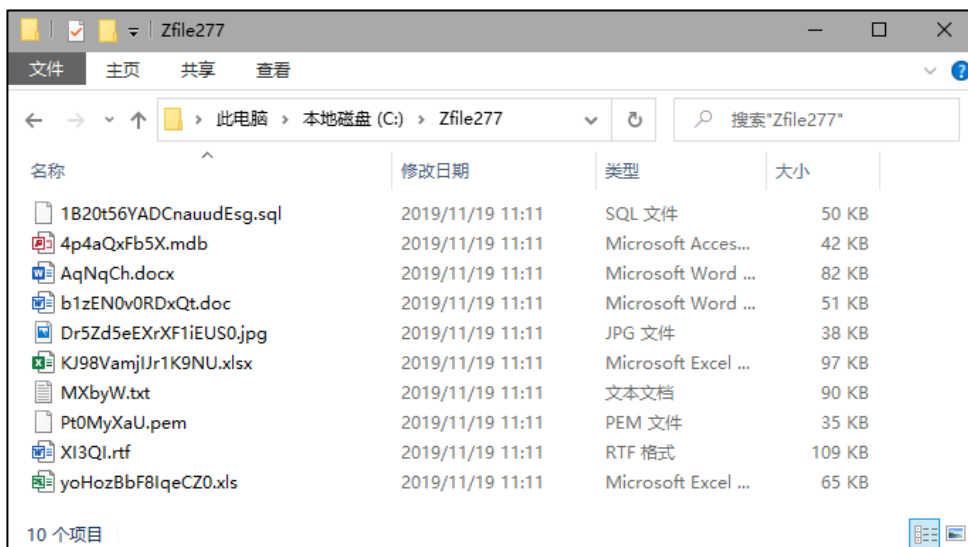


### 3.3 开启勒索诱捕

开启火绒勒索诱捕功能，增强终端对勒索病毒的防护。



开启此功能后，终端 C 盘内会生成两个随机名文件夹，该文件夹内保存随机名诱捕文件，建议部署完成后，在中心启用此功能。



### 3.4 开启远程登录防护

RDP(远程桌面)是勒索病毒的主要传播方式之一。黑客在获取到 Windows 账户的密码后,通过“远程桌面”登录到企业内,如被登录计算机被勒索价值较小(员工使用),会继续进行内网渗透寻找高价值服务器,成功后使用“远程桌面”登录服务器,运行勒索病毒对文件进行加密。

针对此类问题,火绒提供了“远程登录防护”功能。开启此功能后,所有部署了火绒终端的计算机拒绝“远程桌面”登录,只允许添加到“远程登录 IP 白名单”内的计算机,通过“远程桌面”登录。

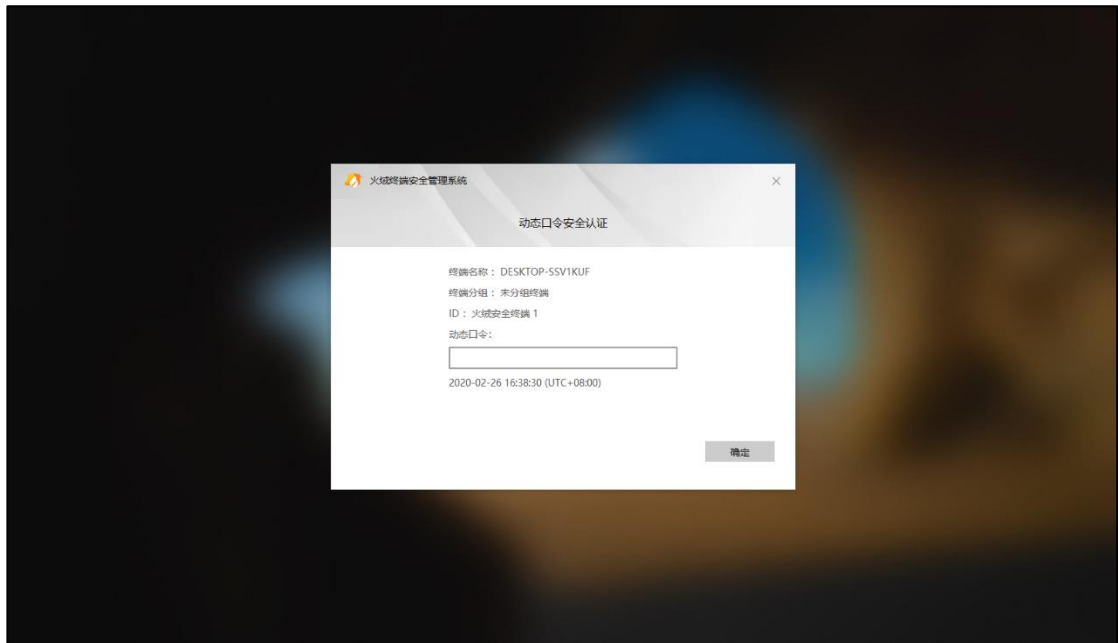


### 3.5 开启终端动态口令安全认证

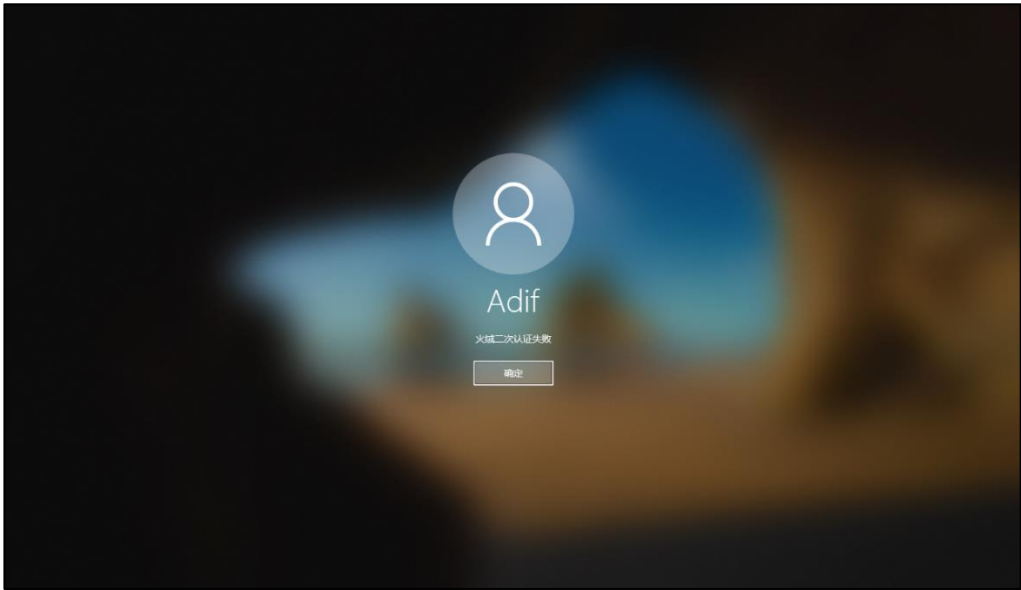
除“远程登录防护”功能外,您也可以选择火绒“终端动态口令安全认证”功能,对您的重要服务器的远程\本地登录进行保护。



在启用此功能后，每当终端用户登录计算机时都将弹出动态口令安全认证窗口（见下图），若用户设置了计算机密码，该弹窗将在用户输入正确的账户密码后弹出。用户需再次输入正确的动态口令才可登入计算机。



动态口令输入错误时，将自动清空动态口令与账户密码并提示：火绒二次认证失败。用户需再次输入密码并再次验证动态口令。

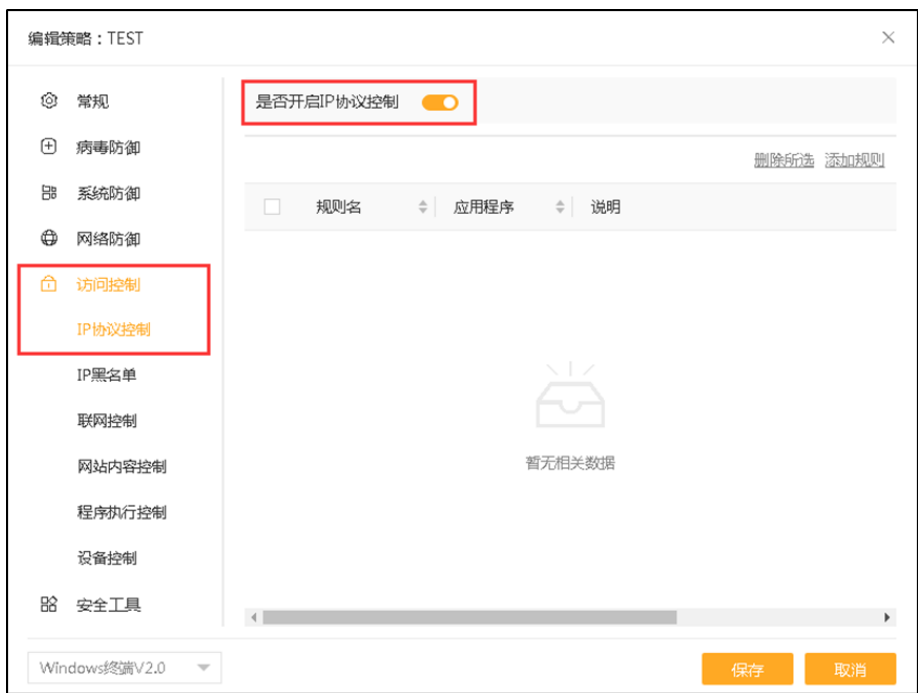


### 3.6 高危端口控制

在业务允许的情况下,使用火绒的“IP 协议控制”功能,对常见的高危端口进行限制(139,445,3389 等),防止因此类端口打开导致的安全问题。

可在火绒中心内,使用“IP 协议控制”根据分组进行限制,以下为操作方法:

- (1) 在火绒中心的防护策略中,开启此功能,并添加规则。



(2) 如想阻止其他计算机访问您的 139, 445 端口, 防御通过共享进行传播的病毒, 可以按照下图的方式进行设置。

IP协议控制

规则模板: 默认模板

规则名称: 139,445

应用程序: \*

操作: 阻止

方向: 入站

协议: TCP

本地IP: 任意IP

本地端口: 139,445

远程IP: 任意IP

远程端口: 任意端口

优先级: 1

日志:  记录日志

确定 取消

(3) 禁用端口会影响某些功能的使用, 例如禁用 139、445 会影响访问该计算机上的共享, 可使用其他服务对此功能进行替代, 例如使用 FTP 代替文件共享, 使用火绒“远程桌面连接”代替 Windows 的远程桌面功能, 或使用火绒“远程登录防护”只允许白名单内设备登录等。

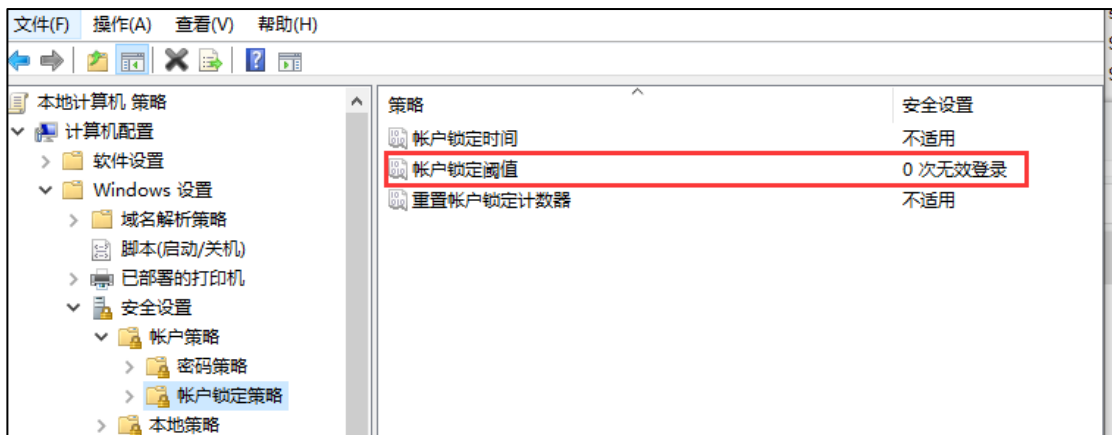


### 3.7 账号密码管理

目前包含密码爆破模块的勒索病毒、窃密木马、蠕虫病毒、挖矿病毒逐渐增多。使用符合安全性要求的密码，可大幅度降低此类攻击成功的可能，提高网络内安全性，以下为加固建议。

企业内对员工账户密码和服务器远程登录密码需要有强度和策略要求：

- (1) 建议设置为字母数字混合并带特殊字符，长度不低于 8 位的强口令，重要的服务器请勿使用默认的 Administrator 账户，或者直接禁用，如果有多台服务器的企业用户建议设置不同的强口令进行管理。
- (2) 使用火绒“远程登录防护”功能。
- (3) 在组策略中新建账户锁定策略，账户密码输入多次，自动锁定账户，避免被黑客使用工具暴力破解(建议设置为 5-6 次)。



- (4) 如条件允许，定期更换密码，防止密码意外泄露导致安全问题。

此案例为用户外网服务器遭受 RDP 爆破，黑客在成功获取 Administrator(默认管理员账户)密码后，登录该服务器运行勒索病毒加密文件。案例：《[RDP 爆破](#)》

## 第四章 员工安全意识与使用习惯

### 4.1 移动存储设备的使用

U 盘接入电脑后遵循先查杀，后使用的原则，避免感染通过 U 盘传播的蠕虫病毒。

局域网内经常遇见隐藏文件的蠕虫病毒，中了病毒的 U 盘再插入装火绒的电脑，火绒会提示病毒，需要立即单独对 U 盘进行扫描，确认没有病毒之后才能继续使用。

此案例即为因 U 盘使用不当，导致病毒在企业内部传播。案例：[《U 盘使用不当导致 10 余种病毒肆虐》](#)

### 4.2 即时通讯钓鱼

即时通讯钓鱼是常见的病毒传播方式，更强的对抗性和欺骗性，终端员工需要提高警惕，避免点击不明链接和打开陌生文件。

(1) 不要随意打开即时通讯（微信、企业微信、腾讯 QQ、钉钉等）中发送的文件和链接。这一切目的为了欺骗用户打开病毒文件（病毒文件结尾.msi/.rar/.exe/.chm/.bat/.vbs）。

(2) 一些即时通讯工具可以进行锁定，在离开电脑时可以对即时通讯工具进行锁定。防止攻击者远程控制发送钓鱼消息。

病毒相关的报告：

[请注意，微信群聊再现“银狐”病毒新变种](#)

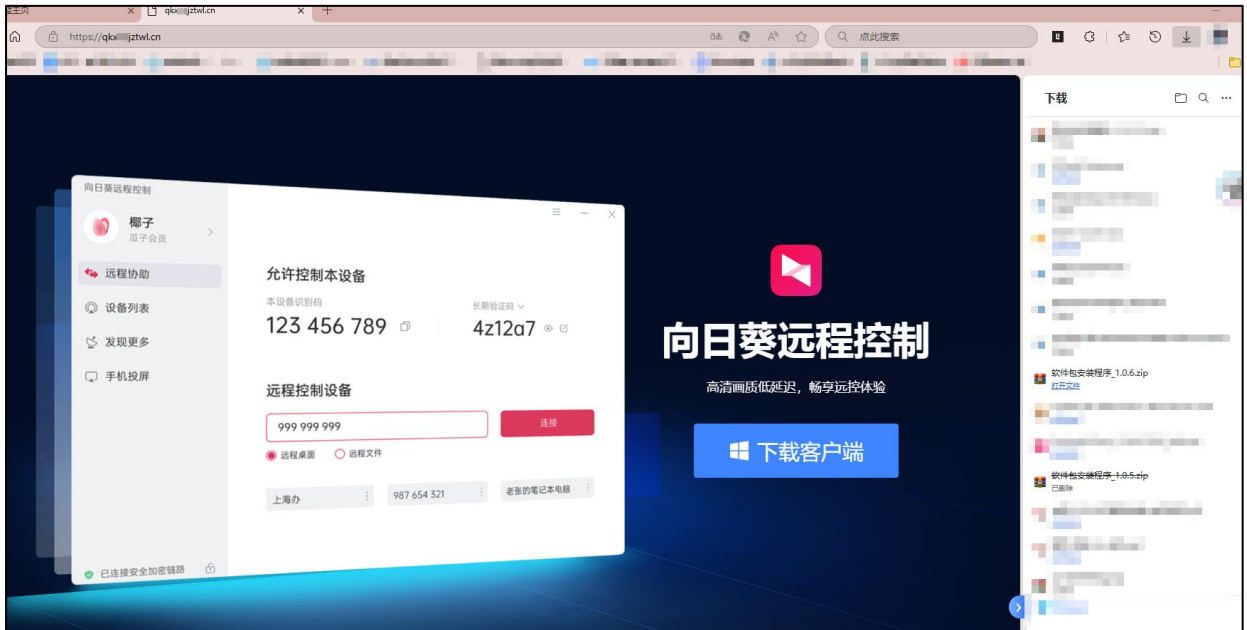
[银狐新变种于幕后潜行，暗启后门远控窃密](#)

[勿轻易解压陌生压缩包，后门病毒或在其中](#)

[反沙箱与杀软对抗双重利用，银狐新变种快速迭代](#)

## 4.3 钓鱼网页

许多人都有通过搜索引擎下载应用程序的习惯，虽然这种方式简单又迅速，但这也可能被不法分子所利用，通过设置钓鱼网站来欺骗用户。这些钓鱼网站可能会通过各种方式吸引用户点击，从而进行病毒的传播，危害个人或企业的信息安全。



我们还可以通过以下几点来防御此类攻击：

- (1) 使用搜索引擎注意识别官方网站。
- (2) 使用火绒应用商店下载软件。

相关病毒的报告：[钓鱼网页散播银狐木马，远控后门威胁终端安全](#)

## 4.4 邮件收发

钓鱼邮件是银行木马、APT 攻击、勒索病毒常用的传播方式，企业常遭到此类攻击，除了邮箱运营者提供的安全防护外，我们还可以通过以下几点来防御此类攻击：

- (1) 尽量避免直接点击邮件中的链接。
- (2) 在火绒中心开启火绒的邮件监控功能。

(3) 对火绒报毒的邮件附件，请勿加入信任区继续使用，应立即杀毒，并及时与火绒联系协助您进行排查。

该案例为企业内员工收到恶意邮件后，因不当操作导致文件被加密。案例：《[恶意邮件](#)》

## 4.5 漏洞修复

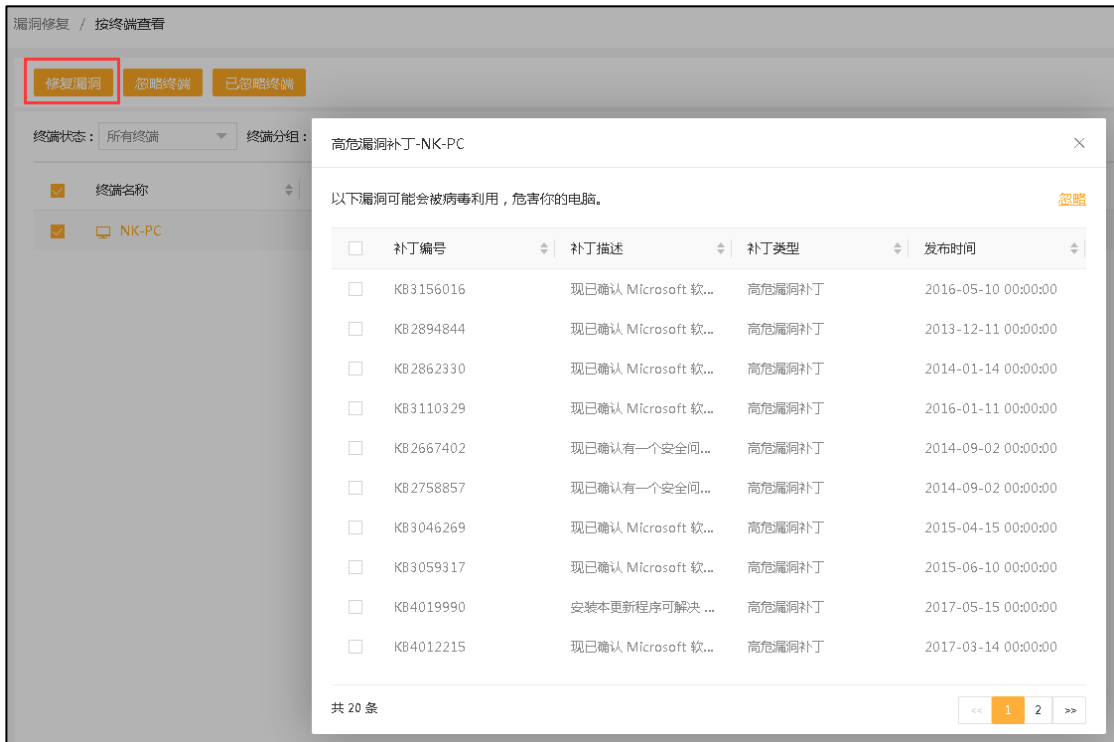
微软会定期推送已知系统漏洞的安全补丁，建议使用火绒的漏洞修复，安装最近的漏洞补丁，防止受到因 Windows 漏洞未及时修补导致的安全问题。

(1) 在中心可以设置开机自动扫描漏洞，及时安装最近的安全补丁。



(2) 火绒中心的漏洞修复页面，可以根据终端选择修复漏洞的类型（修复所有漏洞或修复高危漏洞）

下发漏洞修复。



## 4.6 事件日志

在日常使用中，定时查看电脑运行情况，Windows 日志，安全软件日志，账号情况。

(1) 定期审查关键服务器日志，如日志内出现异常，如果此类日志出现异常增多，例如安全日志内出现大量的“审核失败”日志时，需要判断出现此异常的原因：










某公用账户(例如共享目录)近期修改过密码导致。

其他电脑尝试访问共享目录时凭据失效。

远程登录密码暴力破解攻击导致。

视具体情况，工程师需要进行详细排查。

(2) 对重要的电脑，定时查看账户情况，启动 cmd 输入 net user 查看是否有可疑的新建账户，如果有可疑账号并且非管理员创建，应该立即清除该账户。

入侵子	日期和时间	来源
 审核失败	2019/9/4 16:07:06	Microsoft Windows security auditing.
 审核失败	2019/9/4 16:07:06	Microsoft Windows security auditing.
 审核失败	2019/9/4 16:07:06	Microsoft Windows security auditing.
 审核失败	2019/9/4 16:07:06	Microsoft Windows security auditing.
 审核失败	2019/9/4 16:07:06	Microsoft Windows security auditing.
 审核失败	2019/9/4 16:07:06	Microsoft Windows security auditing.
 审核失败	2019/9/3 18:56:02	Microsoft Windows security auditing.
 审核失败	2019/9/3 18:56:02	Microsoft Windows security auditing.
 审核失败	2019/9/3 18:56:02	Microsoft Windows security auditing.

(3) 定期审查火绒日志，查看是否有新的病毒事件、网络攻击等情况，此类日志可提交给火绒工程师进行分析，帮助您判断网络内是否存在安全隐患。

## 4.7 火绒终端拦截日志

在日常使用中，周期查看火绒管理中心的终端各类日志，火绒拦截一些日志代表着有攻击者在入侵、病毒在运行和传播。虽然被拦截了，但是攻击源可能不会消失。攻击会不断免杀、改变攻击方式和等待防御薄弱时趁虚而入。出现查杀和拦截日志要第一时间做出反应。终端重点关注日志分别如下：

病毒日志、文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、Web 扫描、系统加固、应用加固、网络入侵拦截、横向渗透防护、对外攻击拦截、僵尸网络防护、爆破攻击防护、远程登录防护、Web 服务保护、恶意网址拦截、程序执行控制。

## 第五章 总结

安全产品本质是降低安全事故的概率。企业安全是一个整体,安全产品是整个企业安全防护中的一环,企业和企业员工安全意识也同样重要,需要多方面进行防护。

# 第六章 案例

## 6.1 恶意邮件

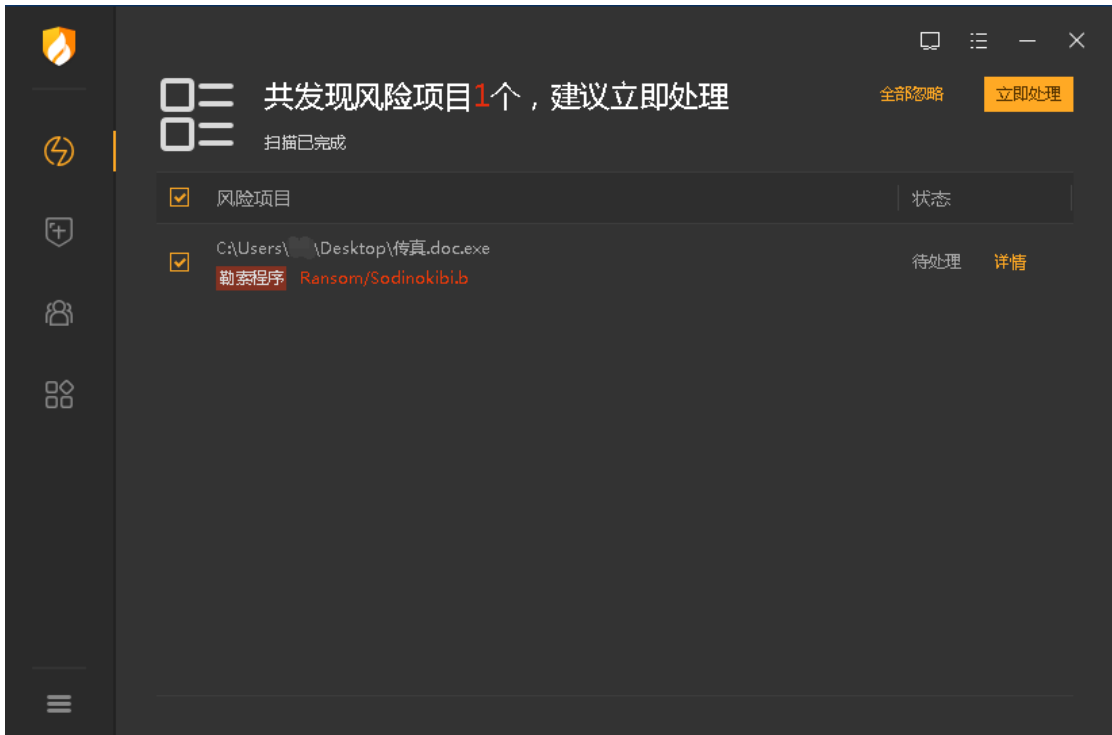
用户反馈收到了名称为《你收到了传真中华人民共和国最高人民法院》的邮件，发件人为免费传真服务网站 FaxZero，并包含附件。用户在电脑内未安装火绒的情况下，下载并运行了附件，导致文件被加密。后联系火绒并提供邮件样本。



火绒工程师查看该附件内样本，确认该附件内病毒为 Sodinokibi 勒索病毒，钓鱼邮件为此勒索病毒常用的传播方式，该样本火绒可以查杀，被加密文件暂时无解密方法。

名称	修改日期	类型	大小
 传真.doc.exe	2019/8/27 2:53	应用程序	344 KB

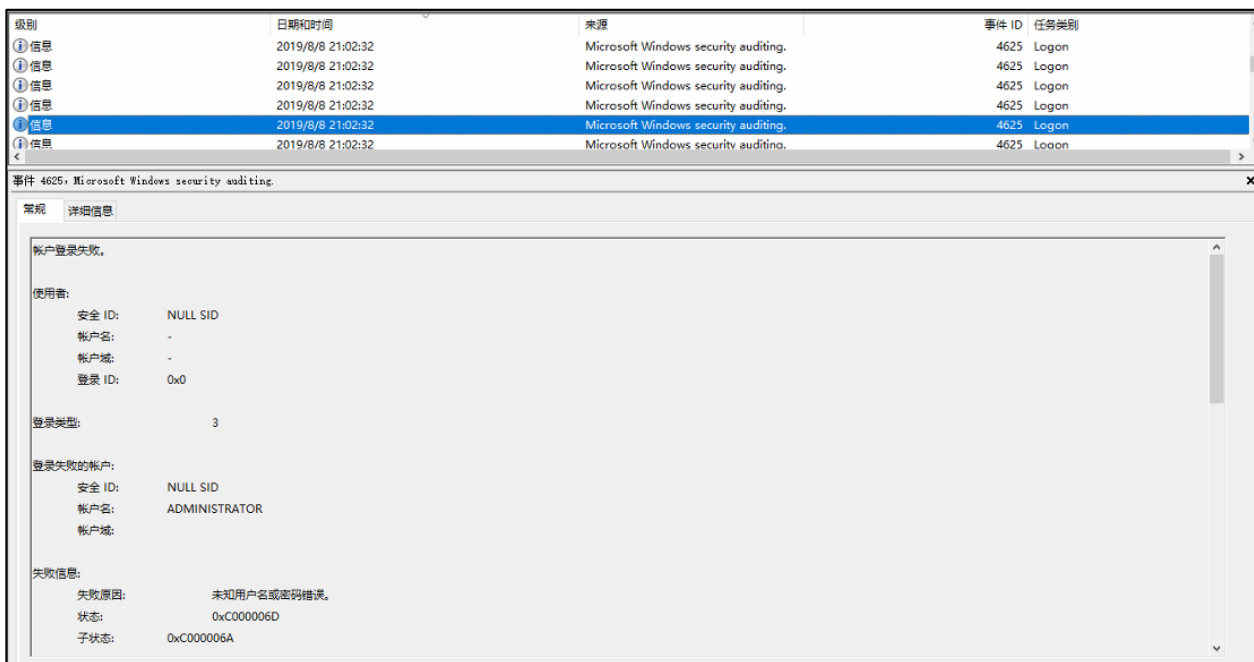




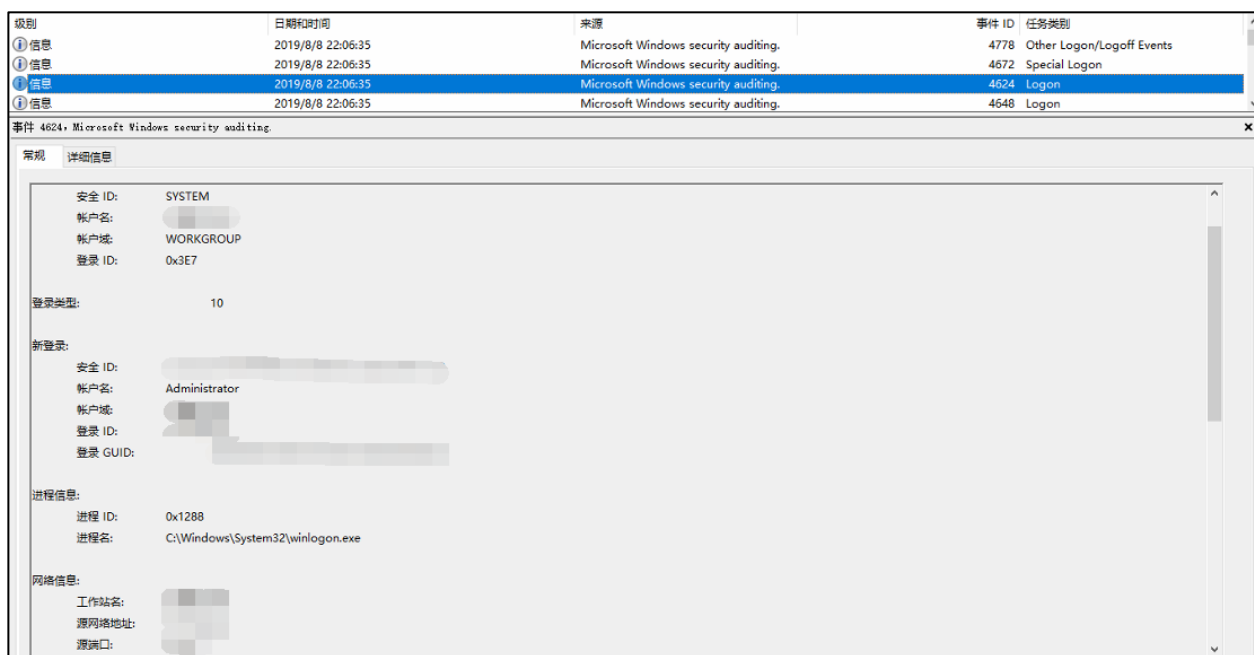
如用户及时部署火绒, 在接收邮件时不轻易下载、运行附件, 获取到可疑邮件时提交给安全公司进行分析, 便可避免此类事件发生。

## 6.2 RDP 爆破

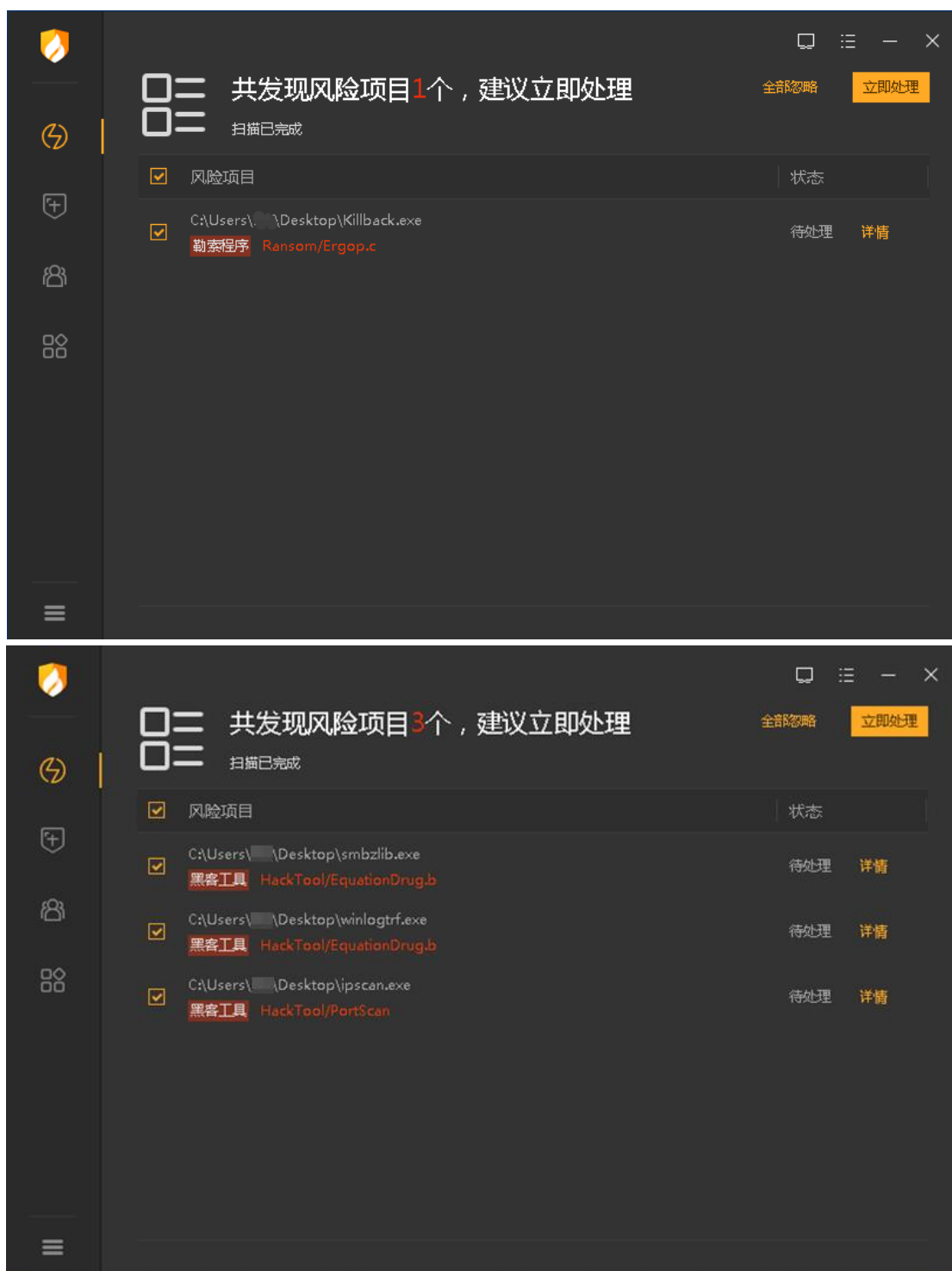
某医疗行业用户发现企业内有大量服务器文件被加密, 联系火绒对现场进行排查, 排查时发现服务器内有未安装安全软件、或安装安全软件被退出的情况, 根据 Windows 日志发现以上服务器内均出现大量访问失败(ID4625)的日志, 应为内网扫描密码爆破导致。



在成功获取到 Windows 账户密码后，使用“远程桌面连接”登录(登录类型:10)，经用户确认该登录并非员工登录，Administrator 账户密码强度低。



根据用户现场与获取到的样本，确认文件被 Globelmposter 勒索病毒加密，该勒索病毒与黑客使用的工具，火绒均可查杀。



RDP 爆破为勒索病毒主要传播方式之一，如服务器打开了 3389 端口并连接外网，系统内账户密码强度较低遭到爆破，在爆破成功获取到密码后，通过 RDP 远程桌面连接，手动投放病毒。如服务器没有进行过相关的安全加固，便有极大的可能被攻击成功。

## 6.3 Microsoft SQL Server 数据库被入侵

某企业用户反馈发现 SQL 相关的病毒，联系火绒对现场进行排查，排查时发现数据库有大量登录失败日志，而且账户被爆破成功。爆破成功后利用数据库高级功能对系统释放木马程序。虽然木马被查杀，但是数据库内数据还是有被删除和加密的风险。

日期	源	消息	日志类型	日志源
2024/12/4 15:57:24	Logon	Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: .46]	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:57:24	Logon	错误: 18456, 严重性: 14, 状态: 8。	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:54:55	Logon	Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: .71]	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:54:55	Logon	错误: 18456, 严重性: 14, 状态: 8。	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:53:48	Logon	Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: .46]	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:53:48	Logon	错误: 18456, 严重性: 14, 状态: 8。	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:50:34	Logon	Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: .46]	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:50:34	Logon	错误: 18456, 严重性: 14, 状态: 8。	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:50:28	Logon	Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: .73]	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:50:28	Logon	错误: 18456, 严重性: 14, 状态: 8。	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:49:33	Logon	Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: .45]	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:49:33	Logon	错误: 18456, 严重性: 14, 状态: 8。	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:48:55	Logon	Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: .72]	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:48:55	Logon	错误: 18456, 严重性: 14, 状态: 8。	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:46:56	Logon	Login failed for user 'yg'. 原因: 找不到与提供的名称匹配的登录名。 [客户端: .46]	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:46:56	Logon	错误: 18456, 严重性: 14, 状态: 5。	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:43:36	Logon	Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: .46]	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:43:36	Logon	错误: 18456, 严重性: 14, 状态: 8。	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:41:56	Logon	Login failed for user 'hydee'. 原因: 找不到与提供的名称匹配的登录名。 [客户端: . . .]	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:41:56	Logon	错误: 18456, 严重性: 14, 状态: 5。	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:41:03	Logon	Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: .74]	SQL Server	当前 - 2024/12/2 9:50:00
2024/12/4 15:41:03	Logon	错误: 18456, 严重性: 14, 状态: 8。	SQL Server	当前 - 2024/12/2 9:50:00

全部
全部
全部
概要

2024-12-05 10:26:13	病毒防御	病毒查杀	快速扫描, 发现0个风险项目
2024-12-04 17:13:15	网络防御	横向渗透防护	受到 .242 的远程WMI调用, 已阻止
2024-12-04 17:13:15	网络防御	横向渗透防护	受到 .242 的远程WMI调用, 已阻止
2024-12-04 16:00:15	网络防御	恶意网址拦截	svchost.exe 尝试 [load.wpd0126.info/], 已阻
2024-12-04 16:00:14	病毒防御	文件实时监控	发现病毒Backdoor/Meterpreter.ak, 已处理
2024-12-04 14:54:35	病毒防御	病毒查杀	全盘扫描, 发现0个风险项目

病毒名称: Backdoor/Meterpreter.ak

病毒ID: A00D08EFDA1AA78C

病毒路径: C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\TmpFC11.tmp

操作类型: 修改

操作结果: 已处理, 删除文件

进程ID: 6920

操作进程: D:\MSSQL10\_50.MSSQLSERVER\MSSQL\Binn\sqlservr.exe

操作进程命令行: "D:\MSSQL10\_50.MSSQLSERVER\MSSQL\Binn\sqlservr.exe" -sMSSQLSERVER

父进程: C:\Windows\System32\services.exe

如果出现手动退出终端杀毒或关闭功能时可能被成功运行病毒，也有可能后续释放病毒可能会持续免疫对抗杀毒软件。很多用户现场成功运行病毒后电脑内数据被勒索病毒加密。

SQL Server 爆破是网络入侵以及勒索病毒的重要传播方式之一，如果服务器打开了数据库端口，高权限数据库账户密码强度低，容易被爆破成功，进而导致被入侵或植入勒索病毒。

需要对服务器进行安全加固，并关注终端安全日志，定时修改数据库所有账号密码，增强密码策略，不要对外网直接映射 1433 等高危端口，防止暴力破解。定期更换密码。

## 6.4 感染型病毒

某企业用户反馈局域网部分机器中了感染型病毒，并且查杀不干净，反复感染反复报毒。经过分析用户信任了病毒样本，导致病毒无法得到查杀，进而对局域网内其他机器不断感染。局域网段内都要部署安全软件，处理具有感染行为病毒时，需要统一集中查杀处理。出现病毒不要随意信任病毒文件，并且及时对中毒终端处理，否则会对内网其他终端进行传播病毒。

