

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 >>>



公 司：北京火绒网络科技有限公司  
地 址：北京市朝阳区红军营南路 15 号瑞普大厦 D 座 4 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。

火绒安全不对本文件的内容、使用，或本文件中的说明的产品承担任何责任或保证，特别对有关商业技能和适用任何特殊目的的隐含性保证不负任何责任。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，恕不另行通知。

# 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
<b>第三章 主机防护加固项</b> .....	9
3.1 部署安全软件.....	9
3.2 开启勒索诱捕.....	10
3.3 开启远程登录防护.....	11
3.4 开启终端动态口令安全认证.....	12
3.5 高危端口控制.....	14
3.6 账号密码管理.....	16
<b>第四章 员工安全意识、使用习惯</b> .....	18
4.1 移动存储设备的使用.....	18
4.2 邮件收发.....	18
4.3 漏洞修复.....	18

4.4 事件日志 .....	20
<b>第五章 总结 .....</b>	<b>22</b>
<b>第六章 案例 .....</b>	<b>23</b>
6.1 恶意邮件 .....	23
6.2 RDP 远程桌面账户被爆破 .....	24

# 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，会修改火绒的默认监控级别，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。

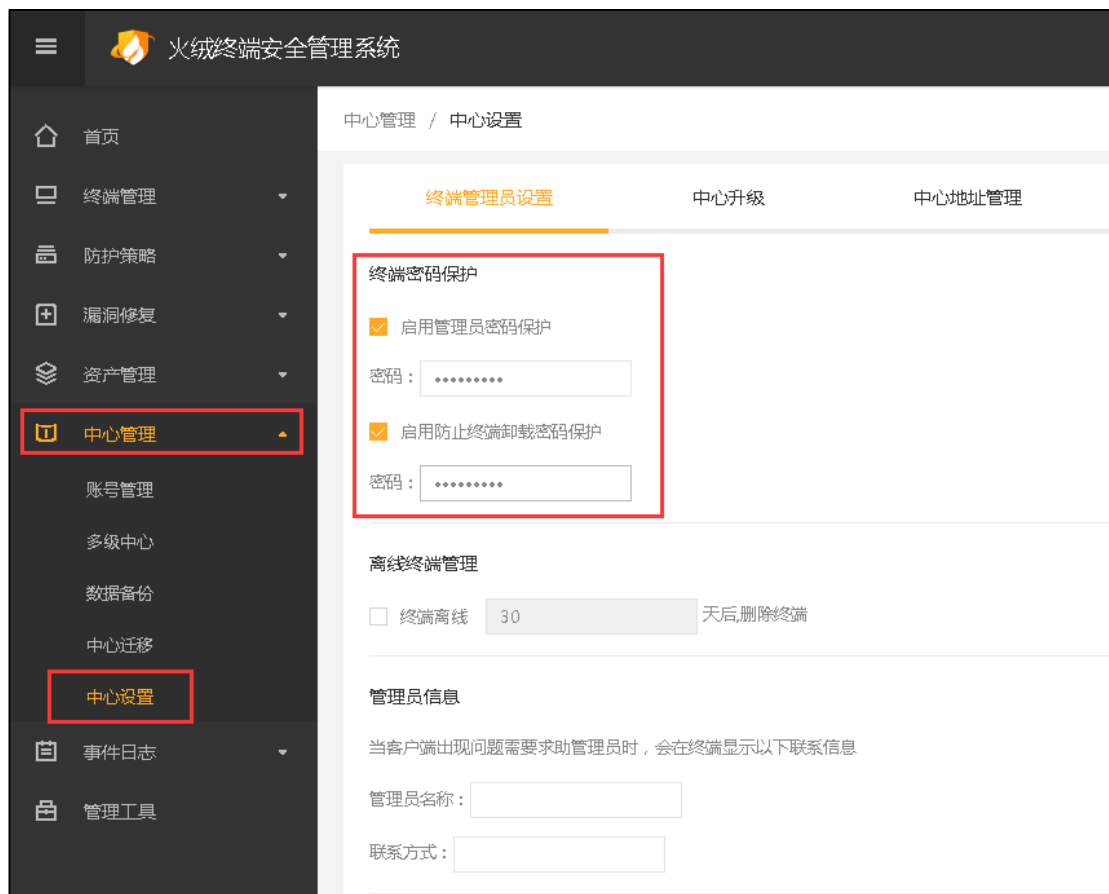


(2) 设置文件实时监控->发现病毒时选项为“自动处理”，防止员工在终端误操作导致病毒被运行。



## 2.3 火绒终端安全防护

(1) 设置火绒终端“管理员密码”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。





## 第三章 主机防护加固项

### 3.1 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”功能创建周期性的扫描。

(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“自动处理病毒”。无需人工再次点击确认。

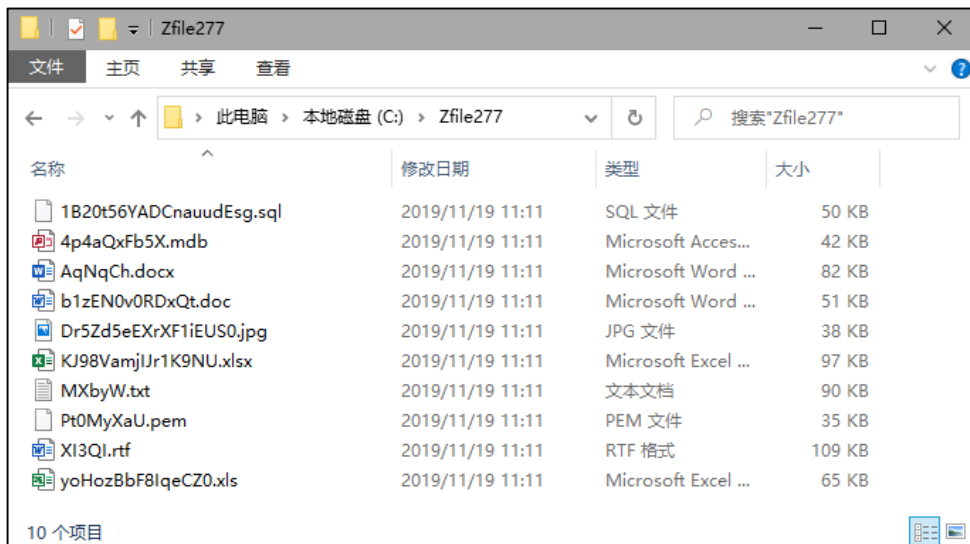


## 3.2 开启勒索诱捕

开启火绒勒索诱捕功能，增强终端对勒索病毒的防护。



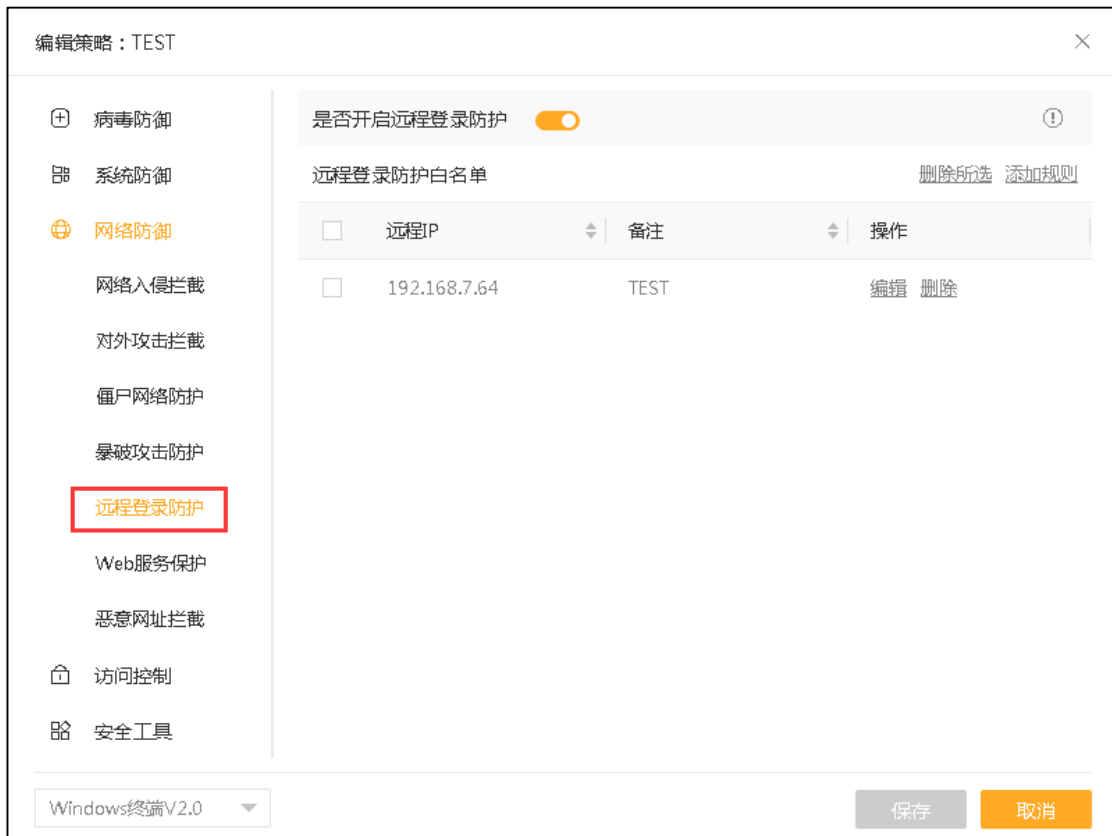
开启此功能后，终端 C 盘内会生成两个随机名文件夹，该文件夹内保存随机名诱捕文件，建议部署完成后，在中心启用此功能。



### 3.3 开启远程登录防护

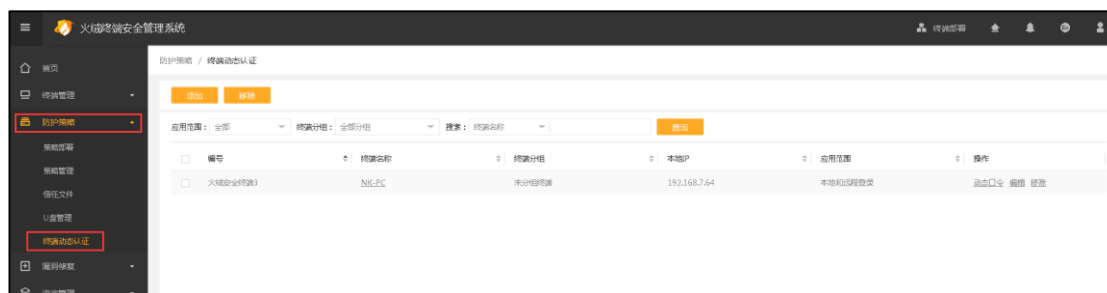
RDP(远程桌面)是勒索病毒的主要传播方式之一。黑客在获取到 Windows 账户的密码后，通过“远程桌面”登录到企业内,如被登录计算机被勒索价值较小(员工使用),会继续进行内网渗透寻找高价值服务器，成功后使用“远程桌面”登录服务器，运行勒索病毒对文件进行加密。

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。

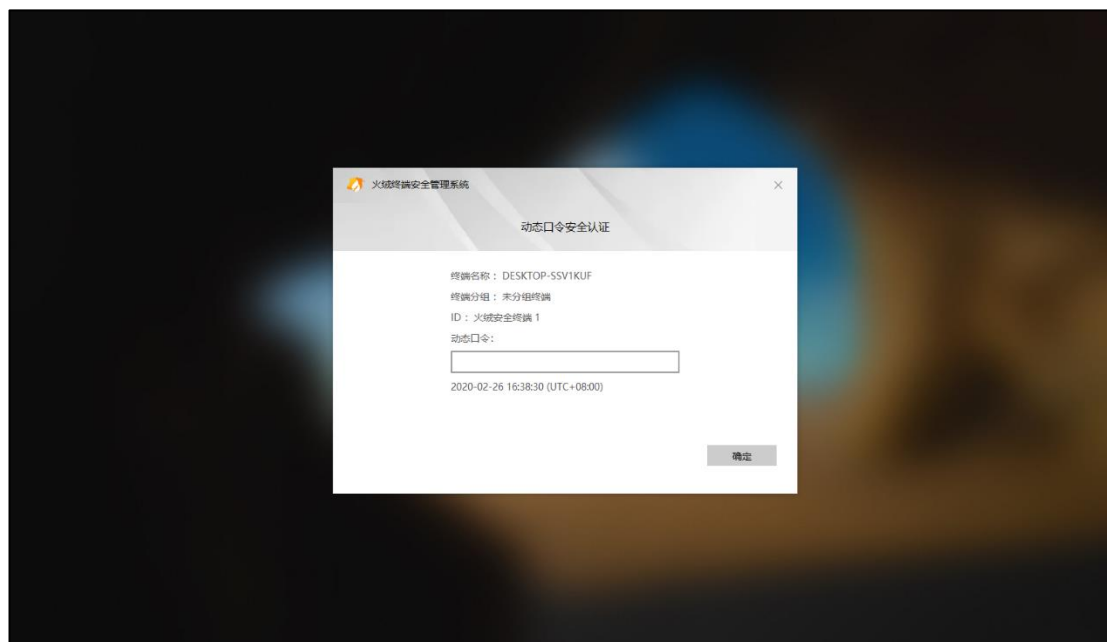


### 3.4 开启终端动态口令安全认证

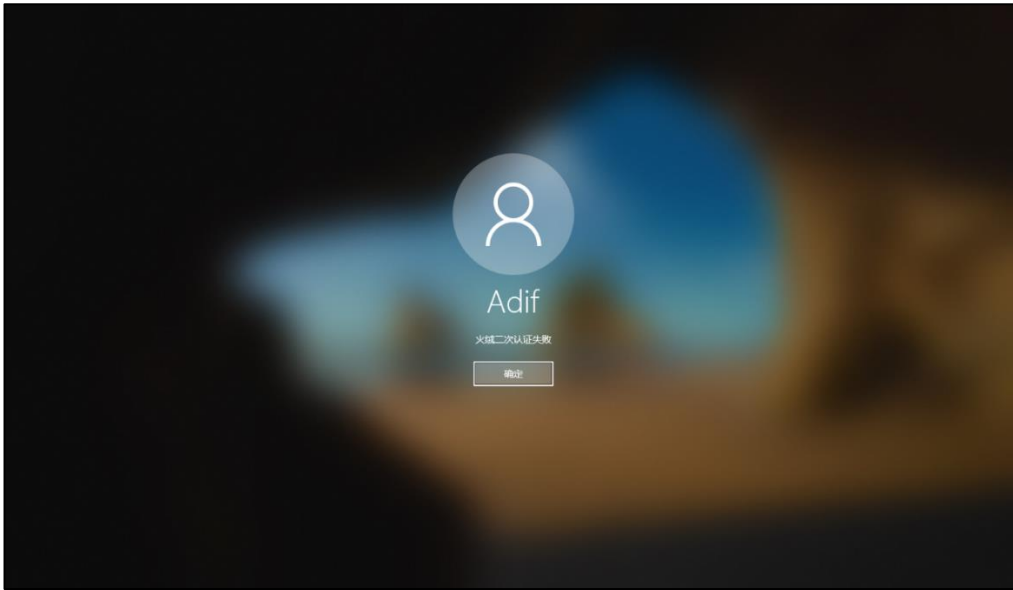
除“远程登录防护”功能外，您也可以选择火绒“终端动态口令安全认证”功能，对您的重要服务器的远程\本地登录进行保护。



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。

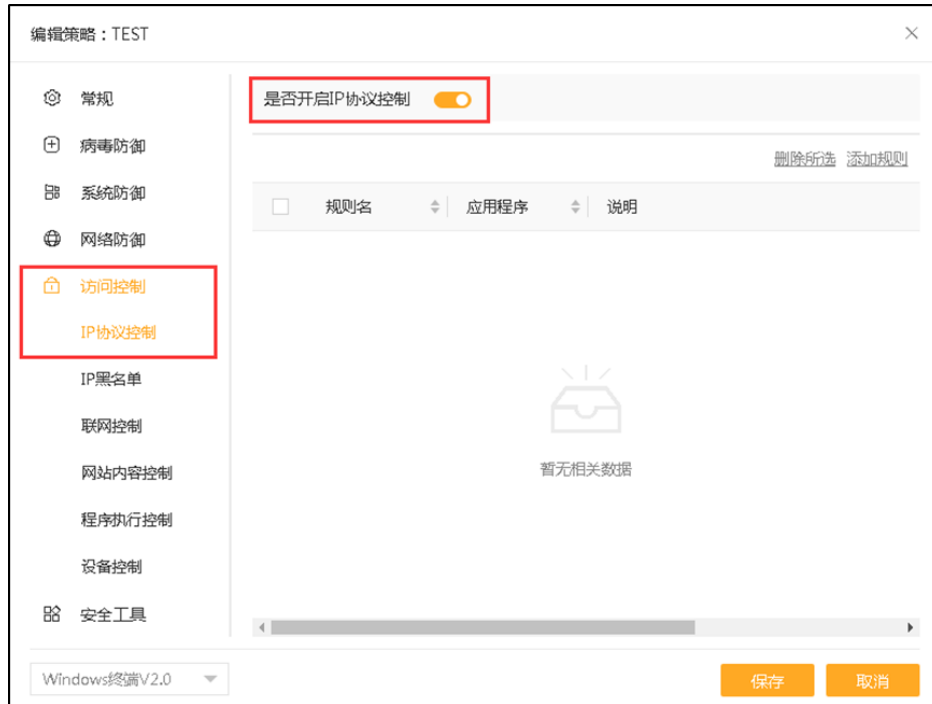


### 3.5 高危端口控制

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：

规则名称：

应用程序：

操作：

方向：

协议：

本地IP： !

本地端口： !

远程IP： !

远程端口： !

优先级： !

日志： 记录日志

(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。

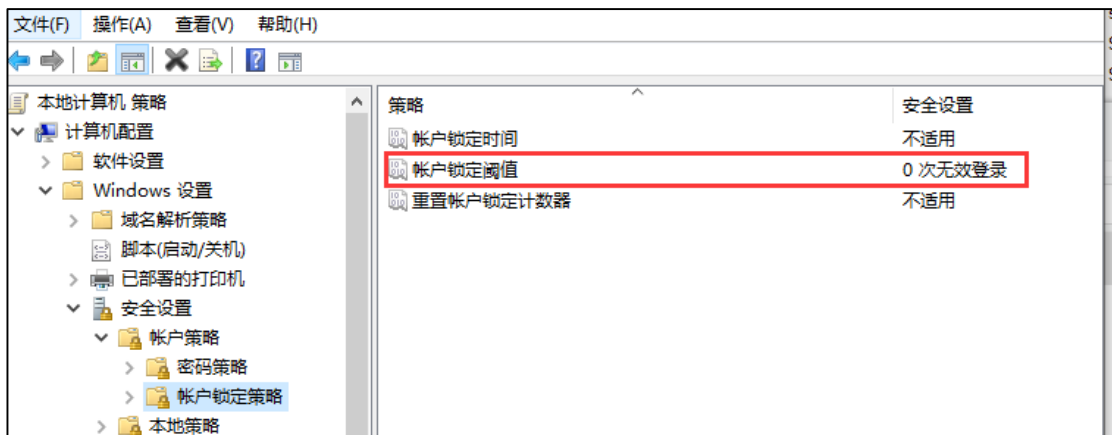
## 3.6 账号密码管理



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。

企业内对员工账户和服务器远程登录密码需要有强度和策略要求：

- (1) 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 远程桌面暴破，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 远程桌面账户被暴破](#)》

## 第四章 员工安全意识、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 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

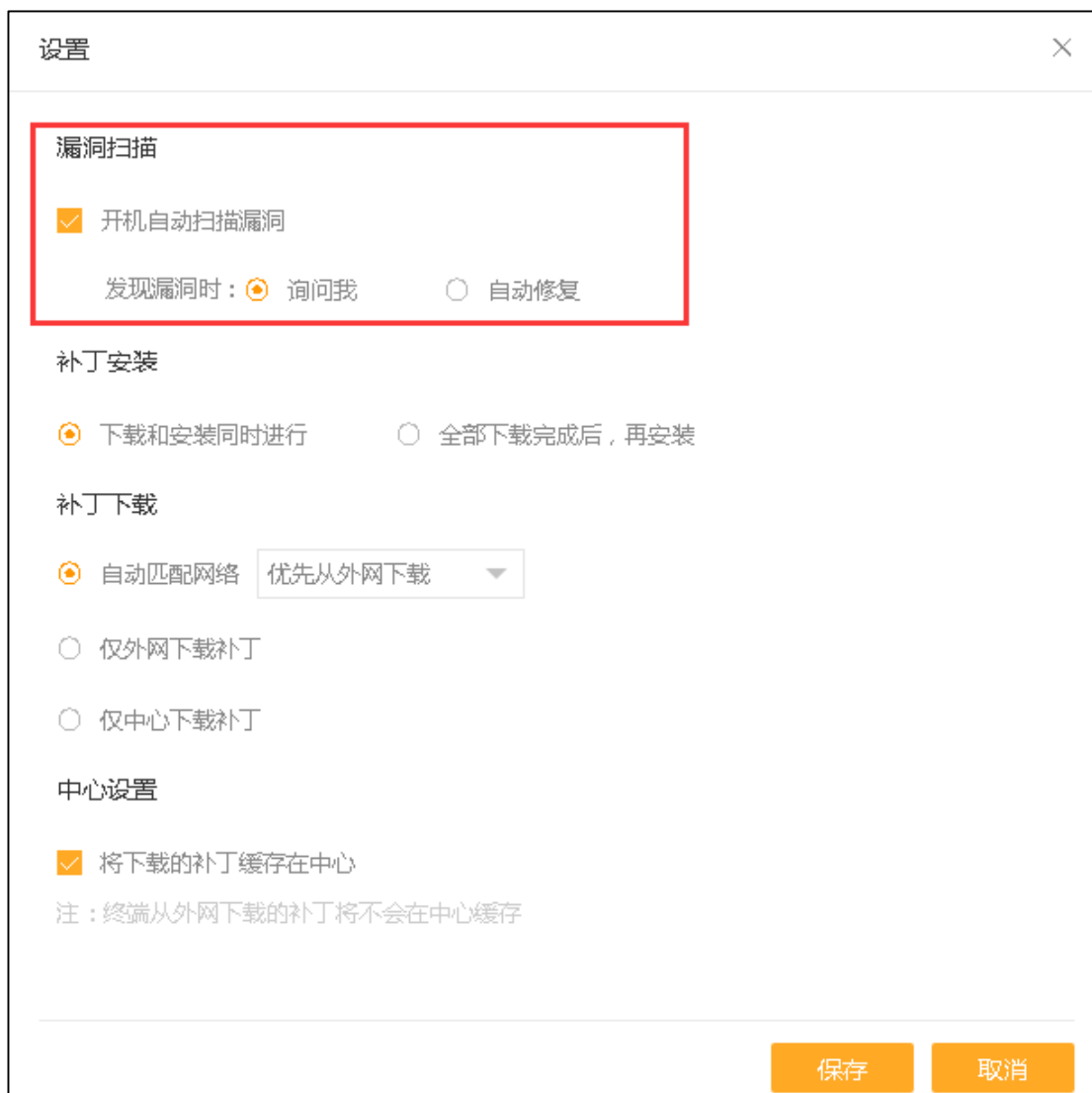
排查。

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](#)》

### 4.3 漏洞修复

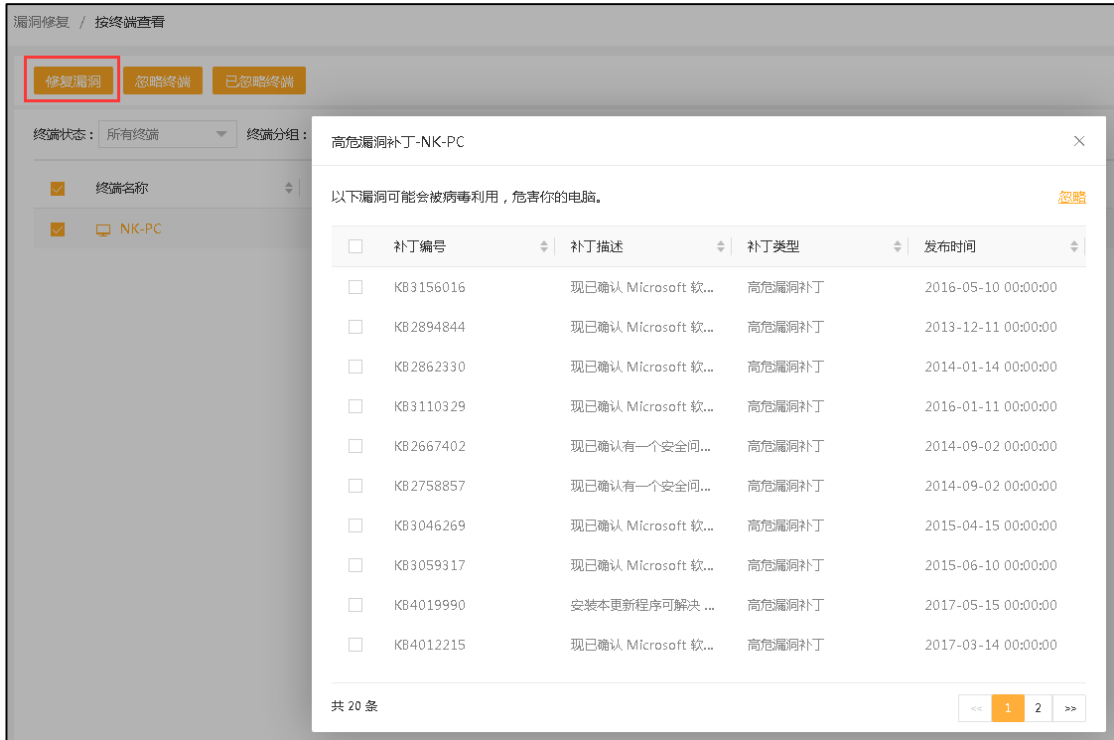
微软会定期推送已知系统漏洞的安全补丁，建议使用火绒的漏洞修复，安装最近的漏洞补丁，防止受到因 Windows 漏洞未及时修补导致的安全问题。

(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。



## 4.4 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，数据库，第三方业务服务程序（OA、IIS）账号情况等。

(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) 启用数据库的日志功能，并定期审查和分析日志记录，以及检查异常查询、访问错误和安全事件。定期备份数据库，并将备份文件存储在安全的位置。测试和验证备份的可恢复性。

(5) 确保第三方业务服务程序及其相关组件和插件都是最新版本，并安装最新的安全更新和补丁。对第三方业务服务程序适当进行安全配置，包括限制访问权限、日志记录和监控等。定期审查第三方业务服务程序的访问日志，关注异常活动、非法访问和攻击尝试。

## 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

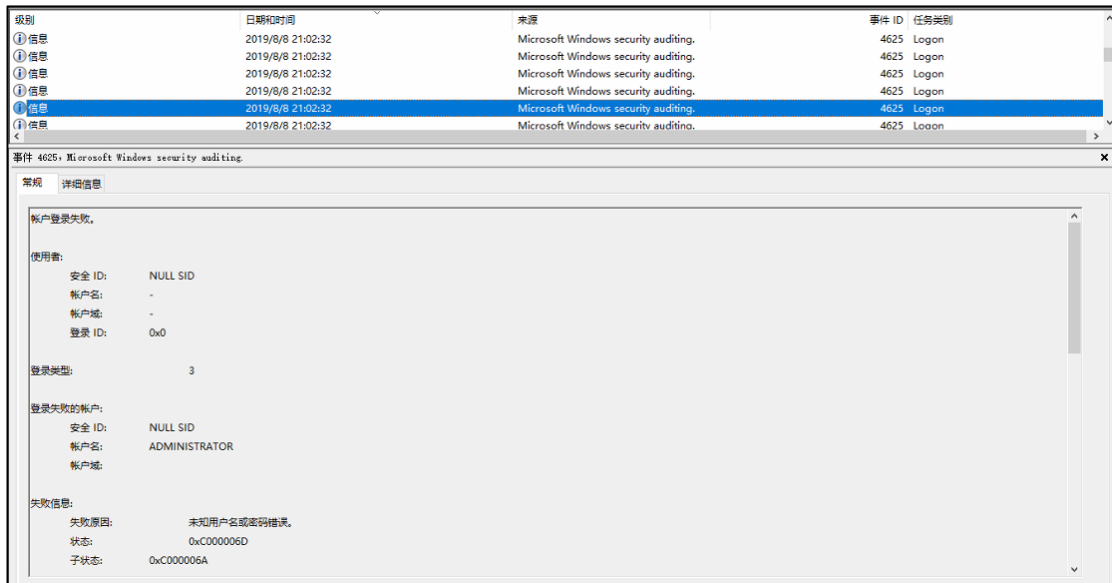


如用户及时部署火绒，在接收邮件时不轻易下载、运行附件，获取到可疑邮件时提交给安全公司进行分析，便可避免此类事件发生。

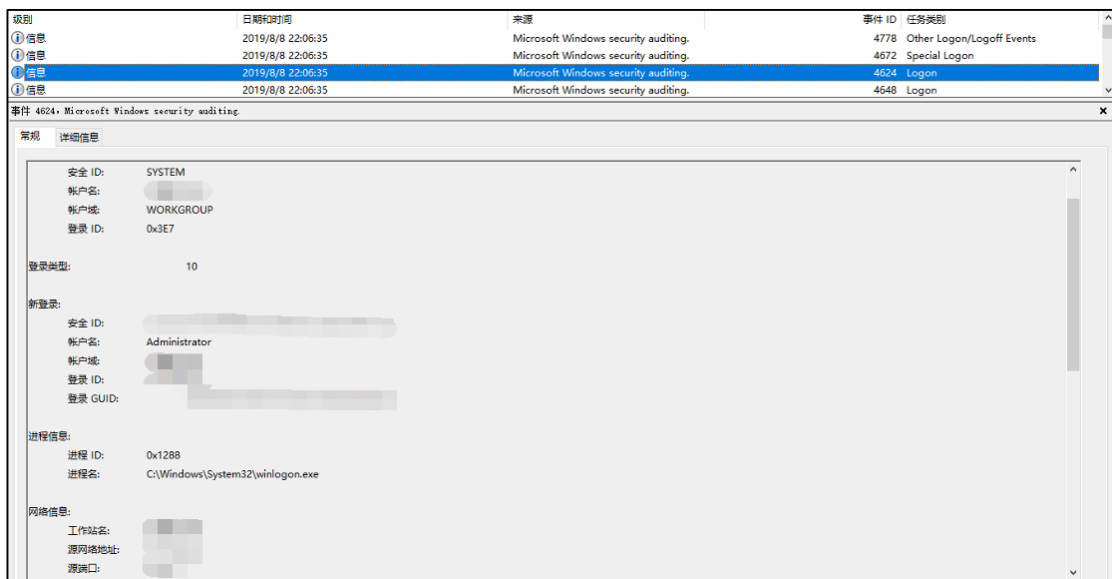
## 6.2 RDP 远程桌面账户被爆破

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。

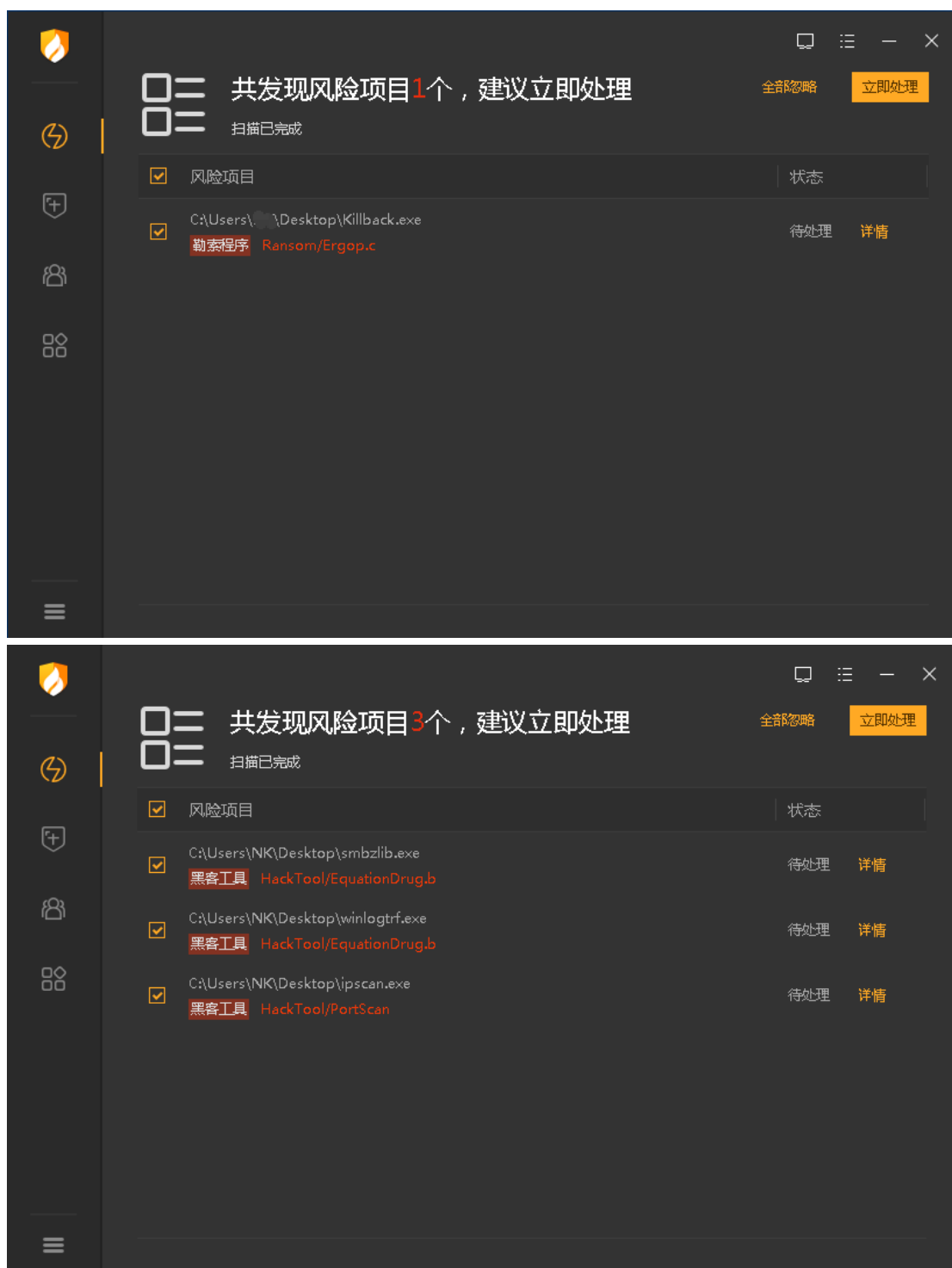




在成功获取到 Windows 账户密码后，使用” 远程桌面连接” 登录(登录类型:10)，经用户确认该登录并非员工登录，Administrator 账户密码强度低。



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 远程桌面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。