

H.4、360企业安全云[适合钓鱼]

2023年10月1日 14:22

By:弱鸡

笔者微信: vivo50KFCKFC

项目地址: <https://github.com/RuoJi6/Deskbypass>

博客: <https://vlog.taoyuan.cool/>

工具链接:

链接: https://pan.baidu.com/s/1XdVkJAJU_Q9rD0PMiSDZFKQ?pwd=zdpm

提取码: zdpm

--来自百度网盘超级会员v4的分享

360企业安全云作为新一代数字安全与管理SaaS服务, 基于360安全大脑安全能力, 依托全面SaaS架构, 实现硬件、软件、数据、资产、上网、防勒索等全方位数字安全与管理服务。从管人员、管资产、管数据三大价值层面助力企业数字化管理提效, 对人员身份及行为管理、软、硬资产兼管、数据全链路守护等实现了一体化综合统效, 全面赋能企业数字化转型。

地址: <https://saas.360.cn/>

步骤一：选择部署方式

1. 选择部署方式, 创建部署连接



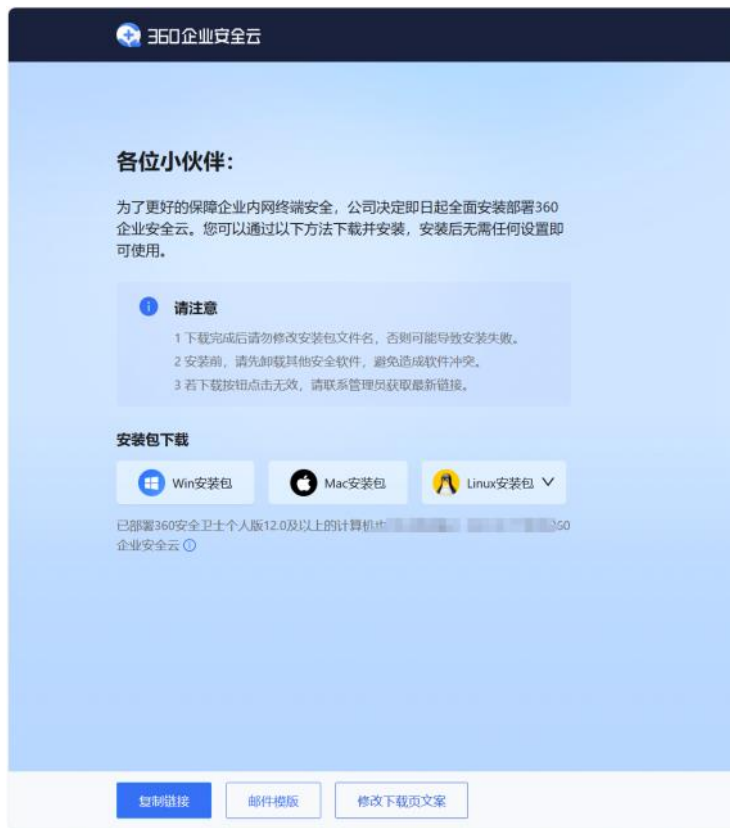
这里提供三种安装方式:

- 手动下载安装: 该方式需管理员自己下载好客户端安装包, 并在需要安装客户端的主机上运行。
- 员工自主下载: 该方式需要客户端用户自行下载客户端, 并安装, 需管理员提供下载链接, 通过沟通软件或者邮件发送给所需用户。
- 域控分发: 管理员通过AD域环境将安装包分发到终端并执行。在指引中提供了分发方案。

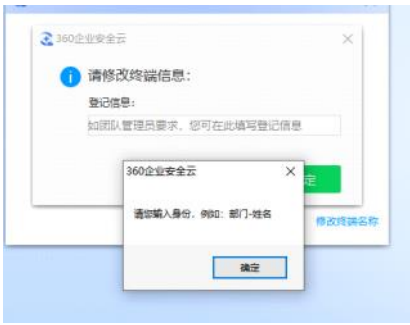
在攻防场景中, 如果去钓鱼的话, 建议使用方式一和方式二 (而且该平台还贴心提供了邮件信息模版), 如果在内网已经有了一定的权限, 可使用方式一和方式三进行远控。



该链接是企业专属的下载链接。即按照我创建的链接下载客户端，安装后会加入到我的企业管理后台，被我远控。（hw钓鱼那个事就是这个方式）
或者12.0及以上版本卫士主界面右上角三条横杠菜单 > 加入团队 > 输入pin码
邮件模板【这个下载之后，需要手动安装才行】



而且按照之后，需要输入这个



步骤三：进行远控

安装完成后，在远程运维-远程控制，可进行远控，如下图

终端分组(支持拖拽排序)

+ 新增分组

所有分组

未分组

1 可查看全网终端的详细信息，对终端信息进行分组、移动、删除、推送信息等操作

全部状态

计算机名/IP/计算机备注名/登记信息

搜索

编辑数据列

导出

导入备注

+ 移动到

补充登记信息

开启防护

关机

重启

终端黑名单

共选中 0 台终端 全选当前分组

<input type="checkbox"/>	终端	终端策略	终端备注	登记信息	用户名	显示名	开关机	今日在线时长	操作
<input type="checkbox"/>	DESKTOP-48IQ...	未分组		admin	123456	-	开 9分钟前 关 9个月前	00小时01分	

远程使用说明

本周远程次数

本周远程总时长/分

当前分组:

设备信息

Windows PC

DESKTOP-48IQAVS

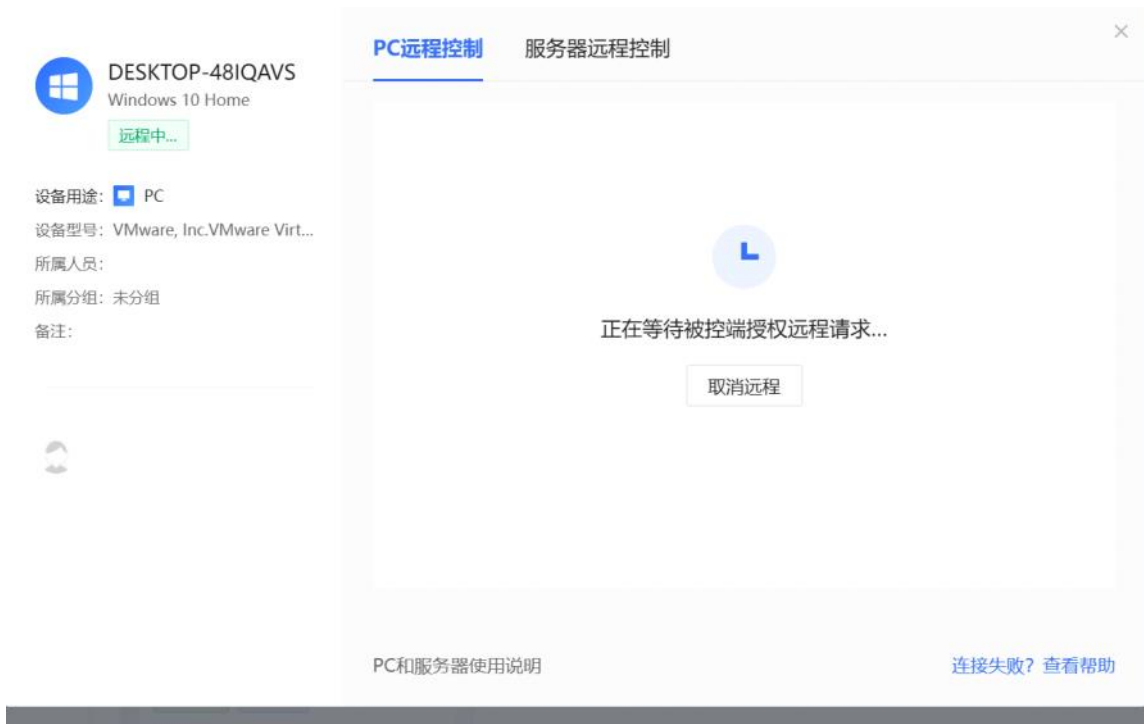
VMware, Inc.VMware Virtual Platform

未分组

在线 可远程

远程控制

而且需要对方同意



这几个需要80一年[在实战的适合，可以买一个]



服务时长：

1年

3年 67折

全额购买可得1600积分/年

终端数量：

-

1

+

服务总价 ¥80/终端/年 *1台 = ¥80

☐ 数据云盘

用于文件分发、内部软件库、远程录屏、日志审计等功能的数据存储，可实现定制策略的终端数据自动备份，杜绝本地存储损坏或勒索攻击导致的数据丢失。

参数配置：

最低方案

最佳方案

自定义订阅

尊享账号

仅高级账号可使用高级账号容量

-

3

+

个

1年

▼

¥20/账号/年

尊享账号存储容量

大量存储1折优惠通道：

仅尊享备份账号可使用高级账号容量

-

100

+

GB

1年

▼

¥3/GB/年 原价16元/GB/年

订阅类型：

新购买服务

购买后：0个尊享备份账号 0GB 到期

服务总价 ¥0

优惠券 暂无可用优惠券

0张可用 选择优惠券

已选 1 项

本单可得积分 1600 积分奖品

明细 订单总价 ¥80 确认订单

而且这个三个都需要授权(因为我付了80大元子)



同意之后

DESKTOP-481QAVS
Windows 10 家庭版 64位

远程中...

设备用途：

PC

设备型号：VMware Virtual Platform ...

所属人员：

所属分组：未分组

备注：

PC远程控制

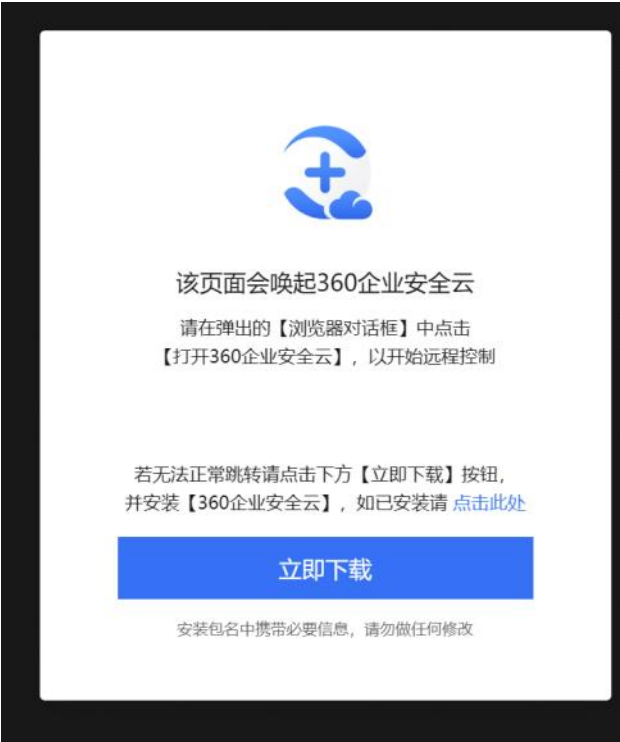
服务器远程控制

已连接成功，可随时开始远程

取消远程

开始远程

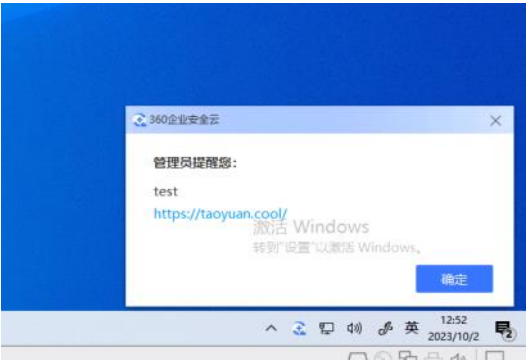
而且本机需要安装360企业云



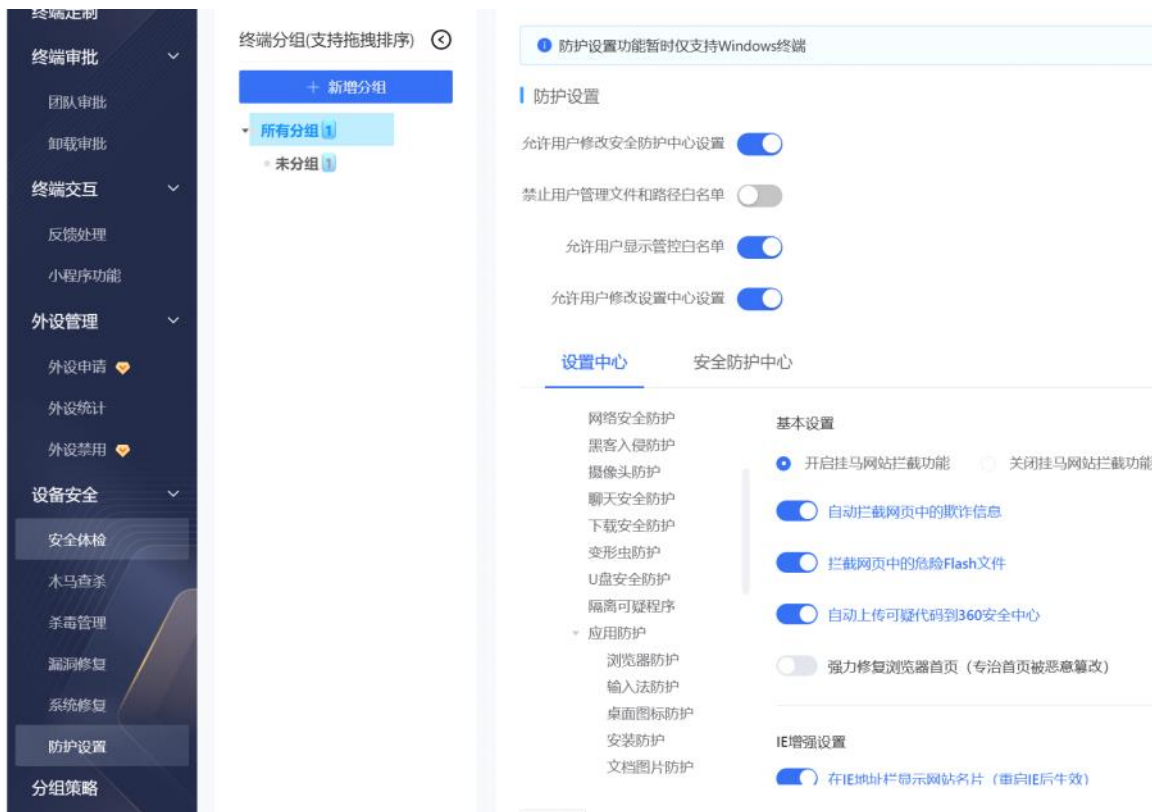
但是可以进行消息推送



就会出现



其实我这边建议[可以在自己电脑安装一共，相比卡巴，这个杀毒没有广告和捆绑，而且80一年，功能多，实时更新漏洞防护]



而且，可以上cs，被杀也没事，因为



19:0520:1021:1522:2023:2500:3001:3502:4003:4504:5005:5507:0008:0509:1010:1511:2012:25

病毒查杀日志病毒防护日志隔离区木马查杀

获取终端数据恢复恢复并信任

<input type="checkbox"/>	病毒名	MD5	文件名	隔离时间
<input type="checkbox"/>	木马:HEUR/QVM202.0.5EA8.Malware.Ge n	6724adca934a8a79f42b17da809735d5	C:\Users\123456\Desktop\1.exe	2023-10-02 12:54:11
<input type="checkbox"/>	木马:Trojan.Win64.Cobalt.A	6cfa45491ec09782bc39851de982bfd1	C:\Users\123456\Desktop\123\artifact.ex e	2023-10-02 12:56:05
<input type="checkbox"/>	木马:HEUR/QVM202.0.5EA8.Malware.Ge n	0f8cf25769bec869dd2f9fb2d1bd3d9	C:\Users\123456\Desktop\123\4.exe	2023-10-02 12:56:10
<input type="checkbox"/>	无效启动项:无效的注册表启动项	4d5b420132e2a2f880c632d870073003	C:\Program Files\Java\jre-9.0.1\bin\ssv.dl l	2023-10-02 12:57:34

共 4 条10条/页

离线

19:0520:1021:1522:2023:2500:3001:3502:4003:4504:5005:5507:0008:0509:1010:1511:2012:25

病毒查杀日志病毒防护日志隔离区木马查杀

获取终端数据恢复恢复并信任

<input checked="" type="checkbox"/>	病毒名	MD5	文件名	隔离时间
<input checked="" type="checkbox"/>	木马:HEUR/QVM202.0.5EA8.Malware.Ge n	6724adca934a8a79f42b17da809735d5	C:\Users\123456\Desktop\1.exe	2023-10-02 12:54:11
<input checked="" type="checkbox"/>	木马:Trojan.Win64.Cobalt.A	6cfa45491ec09782bc39851de982bfd1	C:\Users\123456\Desktop\123\artifact.ex e	2023-10-02 12:56:05
<input checked="" type="checkbox"/>	木马:HEUR/QVM202.0.5EA8.Malware.Ge n	0f8cf25769bec869dd2f9fb2d1bd3d9	C:\Users\123456\Desktop\123\4.exe	2023-10-02 12:56:10
<input checked="" type="checkbox"/>	无效启动项:无效的注册表启动项	4d5b420132e2a2f880c632d870073003	C:\Program Files\Java\jre-9.0.1\bin\ssv.dl l	2023-10-02 12:57:34

共 4 条10

但是恢复并信任不了(不知道为什么,但是可以使用下面这个),但是可以恢复配合下面使用

软件管理
软件运行
软件运行策略
软件禁用
软件运行统计
正版软件授权
软件管家设置
文件分发
文件白名单
软件优化
弹窗过滤
启动项优化

全部设备(1)

所有分组 (1/1)
未分组 (1/1)

将企业安全云误拦的文件加白,加白成功后可正常使用。请确保添加的无可信的MD5/文件/目录。

提交官方加白,省心省力

文件被误拦?提交此文件,由360专家处理
如文件在360安全产品环境中被误拦,可提交此文件样本,查看处理进度及结果。
处理完成后,360查杀引擎在扫描时会将其跳过。(本服务由360专家提供)

提交记录去提交

自定义加白,即时生效
当前所在分组 所有分组 所有分组

MD5加白 什么是MD5? 如何查询?
团队各终端的同一文件安装路径不同时,推荐使用MD5加白

目录加白
对添加文件夹目录下的所有文件加白

文件加白
对添加绝对路径的单个文件进行加白

MD5白名单(0) 目录白名单(0) 文件白名单(0)

添加

MD5

操作

暂无数据



而且上传一个木马，点击分发



[但是这个需要你的企业认证才行]

分发对象

时间 ☒ 立即 ☐ 指定时间

存放位置

桌面

☐ 替换同名文件

执行方式 ☒ 接收后运行 ☐ 只接收

☐ 分发失败

20

 分钟后再次执行分发

☐ 终端资源占用率不高于70%时执行

☐ 终端重启时安装

运行参数 (配置软件运行参数，可以使软件有各种不同的展现形式，如使软件静默运行)

ccc.exe

运行参数

添加

文件名称	运行参数	操作
暂无数据		

终端提示 ☒ 运行时需要终端确认 ☐ 提示后自动运行 ☐ 不提示直接运行

亲爱的用户，管理员正在进行分发任务，请配合管理员完成相关文件阅读或者软件下载安装操作

有效时间 ☒ 一周 ☐ 指定时间

分发

取消