火绒安全
HUORONG SECURITY

2023 火绒安全 终端安全洞察报告

北京火绒网络科技有限公司

前言

《火绒安全 2023 年终端安全洞察报告》以“火绒威胁情报系统”为统计基础，汇总梳理 2023 全年终端攻击威胁态势。希望为个人用户和企业客户提供更真实、更直观、更全面的终端威胁感知，帮助大家提高风险预防意识，有效采取防御措施应对潜在终端安全威胁。

- 火绒安全产品共拦截终端攻击 37.35 亿次，下半年攻击逐渐减少并进入平缓期。
- 黑客主动向全网投放的病毒中，感染型病毒占 32%、木马病毒占 22%、蠕虫病毒占 19%。其中，感染型病毒已感染数百万终端。
- 银狐病毒家族成为年度最活跃家族，最早可以溯源到 2022 年底，2023 年开始活跃，呈现众多变种和传播形式。
- 火绒产品共提示软件安装 8.61 亿次，除了常见软件，杀毒软件、浏览器、办公软件、游戏类软件排名靠前。
- 火绒安全技术人员协助处理的个人终端问题中，勒索病毒已经仅次于内核级病毒，成为二号威胁，个人用户切莫掉以轻心。
- 近三年数据显示，勒索攻击已经超过挖矿病毒，成为企业安全主要威胁来源，且数量远超其他病毒威胁。

目录

终端攻击趋势

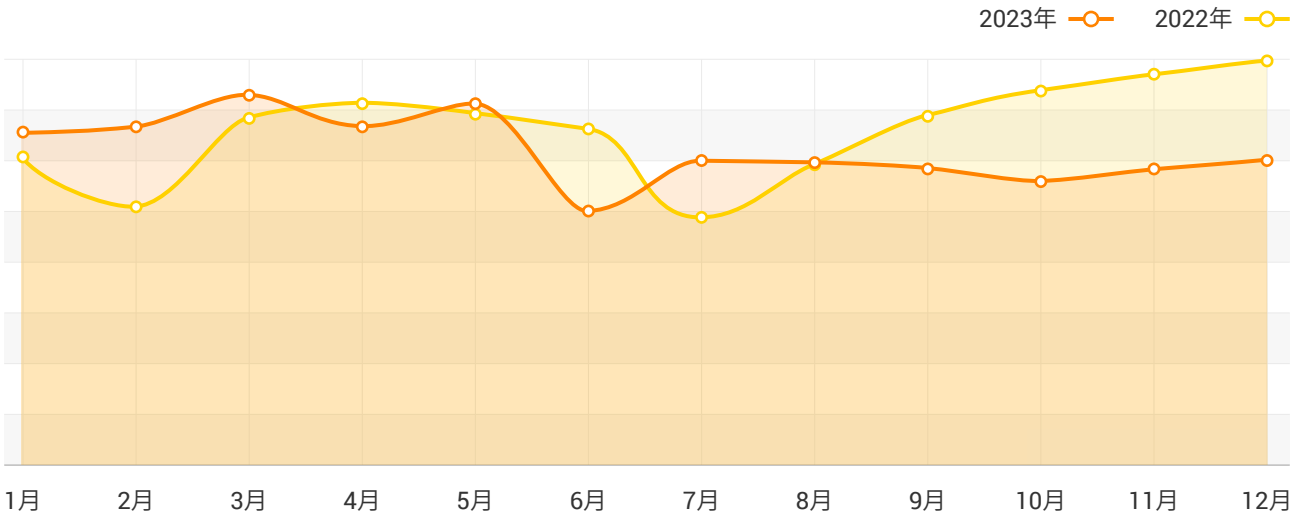
“火绒威胁情报系统”监测情况显示，2023 年火绒安全产品共拦截终端攻击 37.35 亿次，下半年攻击逐渐减少并进入平缓期。从全国范围来看，广东、江苏、山东成为易受恶意攻击地区，其次为浙江、四川、福建、河南、北京、湖北、湖南。

拦截终端攻击

37.35亿次

火绒安全 HUORONG SECURITY

2022、2023 年火绒安全监测到威胁情报全量趋势



火绒安全 HUORONG SECURITY

2023 年国内遭受恶意攻击地域分布 TOP10

感染型病毒
32%

木马病毒
22%

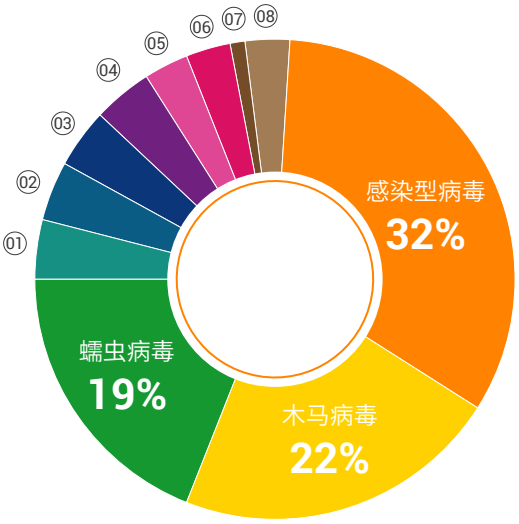
蠕虫病毒
19%

2023 年黑客主动向全网投放的病毒中，感染型病毒占 32%、木马病毒占 22%、蠕虫病毒占 19%，三者仍然是终端安全的主要病毒威胁来源。其中，感染型病毒主要来自 Synares、Virut、Sality、Ramnit 四个家族，已感染数百万终端。

由于感染型病毒具备隐蔽性、潜伏性等特征，往往难以分辨，用户可通过两种方式判别：一是看到以“Virus”开头的火绒报毒提示，直接查杀即可（火绒查杀不会损坏程序、文档）。二是需要警惕看似正常的软件被报毒，其中很可能存在感染型病毒。

火绒安全 HUORONG SECURITY

2023 年火绒安全拦截病毒样本类型占比

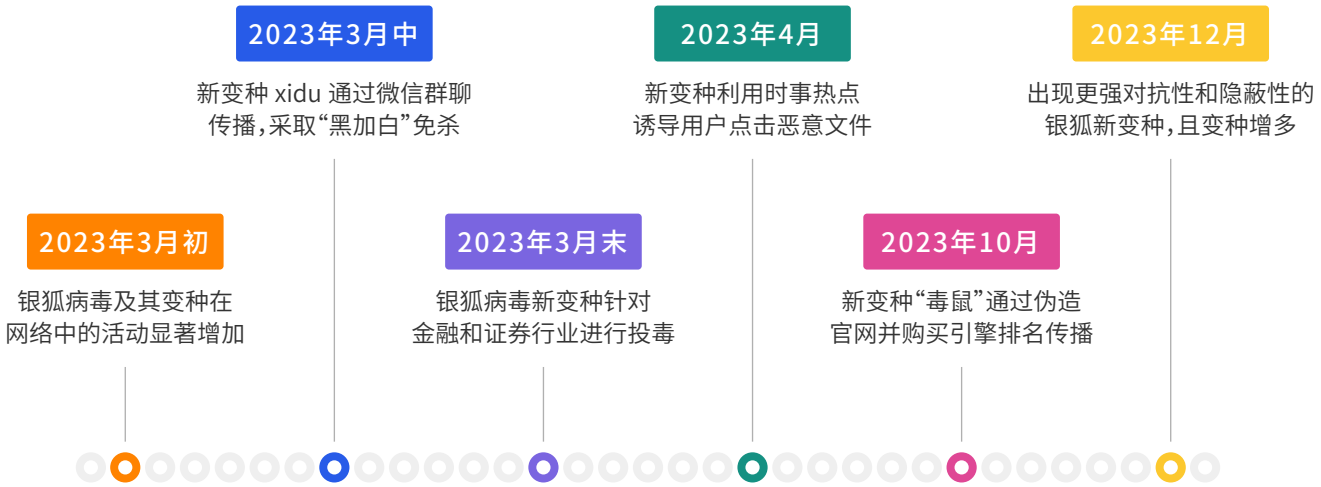


⑴ 宏病毒 5%	⑵ 内核级病毒 4%	⑶ 后门病毒 4%	⑷ 代码混淆器 4%
⑸ 下载者木马 3%	⑹ 流氓程序 3%	⑺ 间谍木马 1%	⑻ 其他 3%

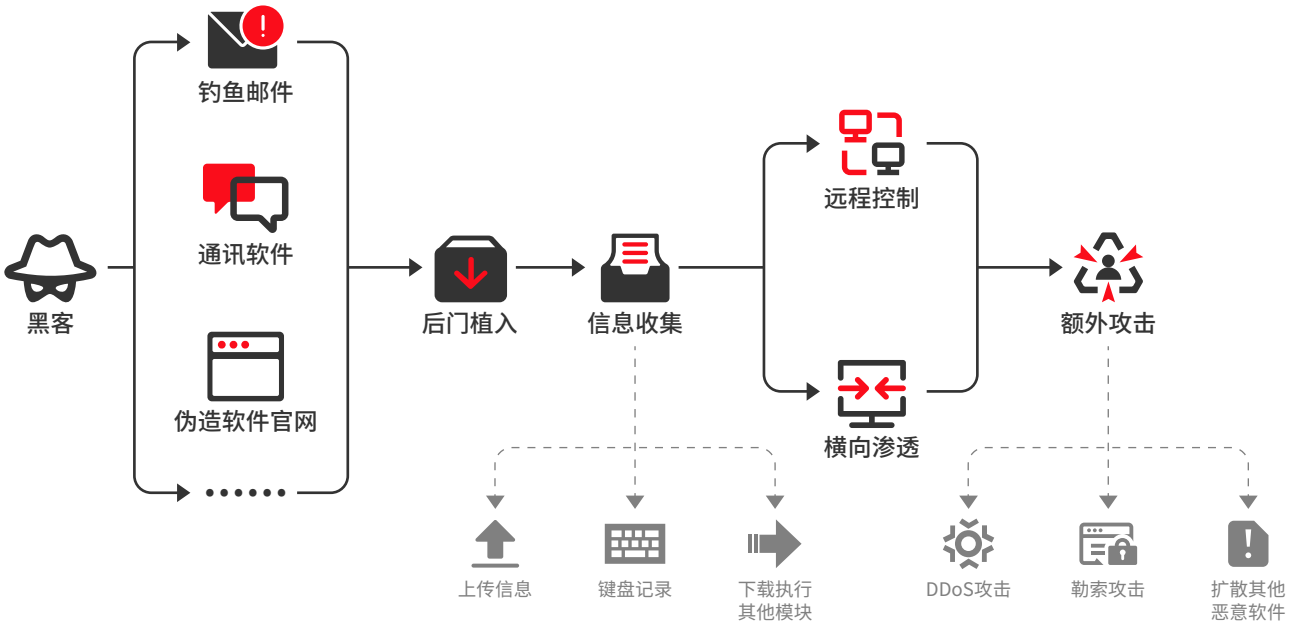
注：图中不包含广告程序类型

银狐病毒活跃

银狐病毒家族最早可以溯源到 2022 年底，2023 年开始活跃，呈现众多变种和传播形式。最常见的是，该病毒以国内企业的管理、财务、销售人员为主要目标，伪装成带有关键词的文件，诱骗用户点击运行。黑客则可以远程控制受害者的终端，监控电脑使用情况，并伺机盗取用户敏感数据及财产信息。根据火绒威胁情报系统的梳理，2023 年银狐病毒及其重要变种的时间线为：



黑客通常利用钓鱼邮件、通讯软件、伪造软件官网等手段，将后门病毒植入目标系统，收集敏感信息并执行其他恶意模块，以对受害者电脑进行远程控制和横向渗透，随后发起 DDoS 攻击和勒索攻击等恶意行为，给用户造成财产损失。银狐病毒的攻击流程，如下图所示：



弹窗进入平缓期

互联网弹窗广告作为公众诟病较集中的互联网问题，国家相关部门于近两年陆续发布管理规定，2022 年 9 月施行的《互联网弹窗信息推送服务管理规定》、2023 年 5 月施行的《互联网广告管理办法》，分别强化了对互联网弹窗的约束力度，同时加大了对广告参与主体违法行为的惩戒力度。

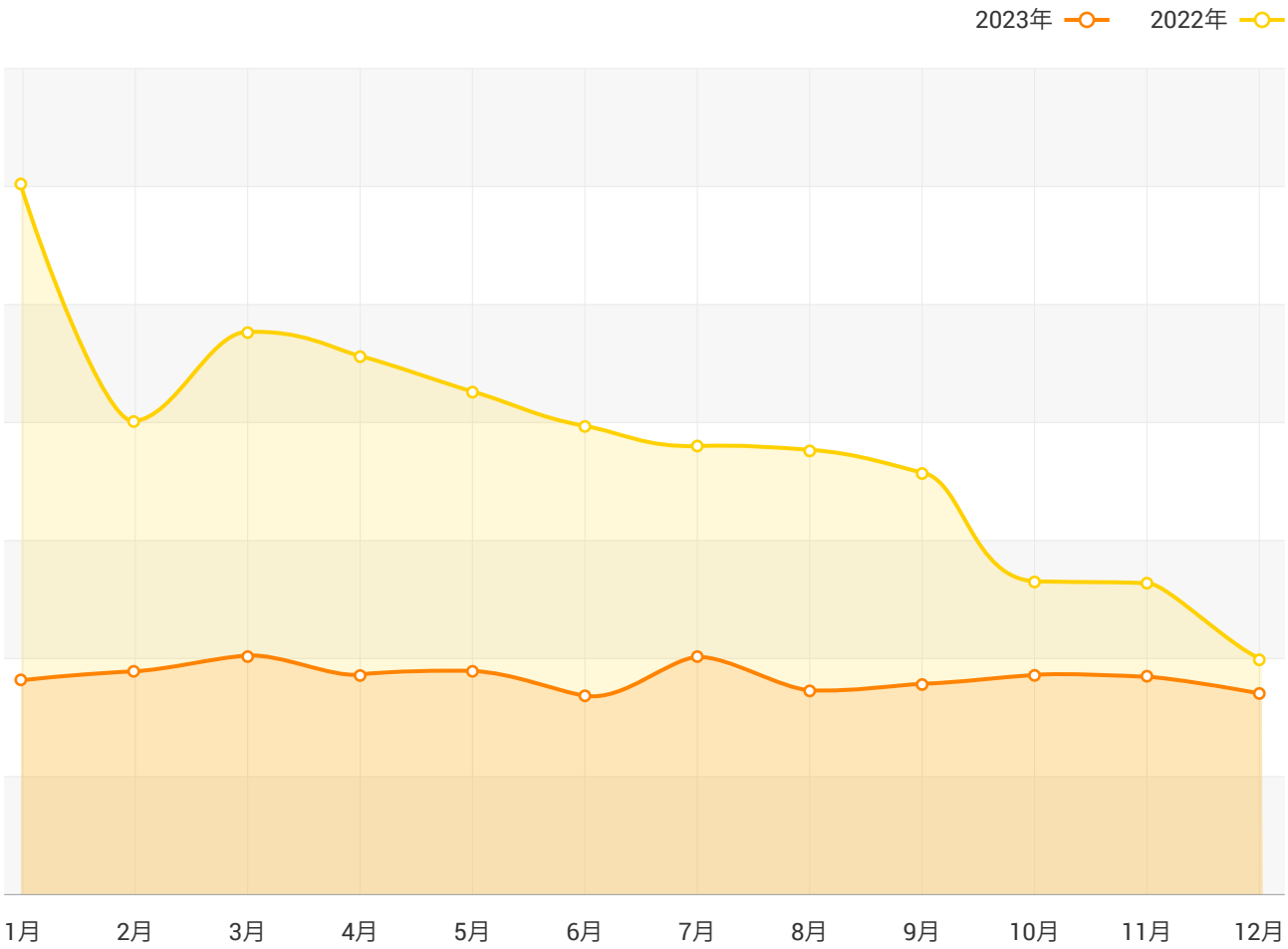
“火绒威胁情报系统”数据显示，2023 年火绒安全产品共拦截（不含用户手动拦截）11.15 亿次弹窗广告，明显比去年减少一半，且各月总量持平，特殊促销时间节点并未出现明显波动情况。

拦截弹窗广告
（不含用户手动拦截）

11.15亿次

火绒安全 HUORONG SECURITY

2022、2023 年火绒安全弹窗广告拦截趋势



软件安装拦截

软件捆绑安装也是互联网用户经常遇到的问题之一，其花样百出、防不胜防，用户稍有不注意则下载到若干无用软件，随之而来的就是各种广告弹窗、网页篡改、系统卡顿、内存不足等一系列问题，甚至存在个人隐私、财产信息泄露风险。

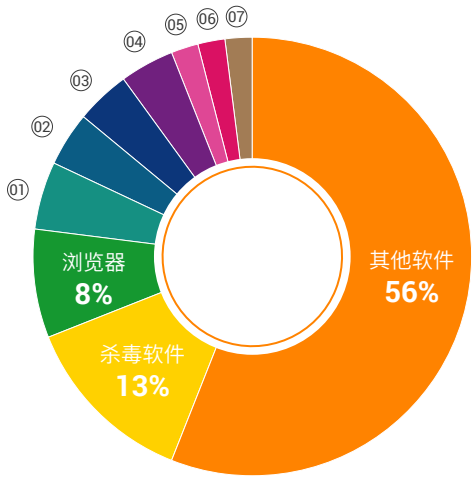
为了有效减少用户在不知情的情况下被安装不需要的软件的风险，火绒产品会对曾经被捆绑安装的软件进行识别，并及时提示用户。2023 年，火绒产品共提示软件安装 8.61 亿次，除了常见软件，杀毒软件、浏览器、办公软件、游戏类软件排名靠前，而在 2022 年，阅读翻译类工具则被拦截较多。

拦截捆绑安装

8.61 亿次

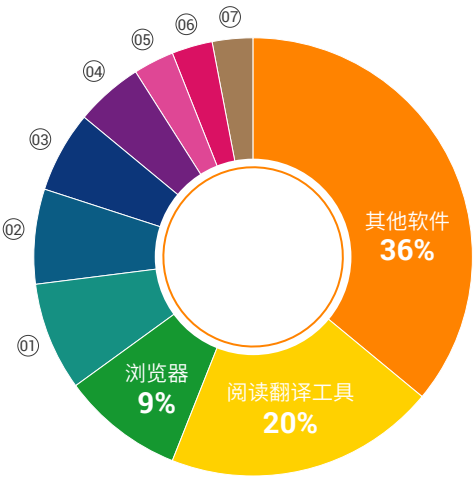
火绒安全 HUORONG SECURITY

近两年火绒产品提示的安装软件类型



2023年

⑴ 办公软件	5%	⑸ 系统工具	2%
⑵ 游戏相关	4%	⑹ 网络工具	2%
⑶ 媒体播放器	4%	⑺ 音乐播放器	2%
⑷ 桌面工具	4%		



2022年

⑴ 杀毒软件	8%	⑸ 办公软件	3%
⑵ 游戏相关	7%	⑹ 系统工具	3%
⑶ 桌面工具	6%	⑺ 压缩软件	3%
⑷ 媒体播放器	5%		

微软系统漏洞

拦截漏洞攻击

2.26亿次

拦截微软系统漏洞攻击

1.67亿次

拦截 Web 漏洞攻击

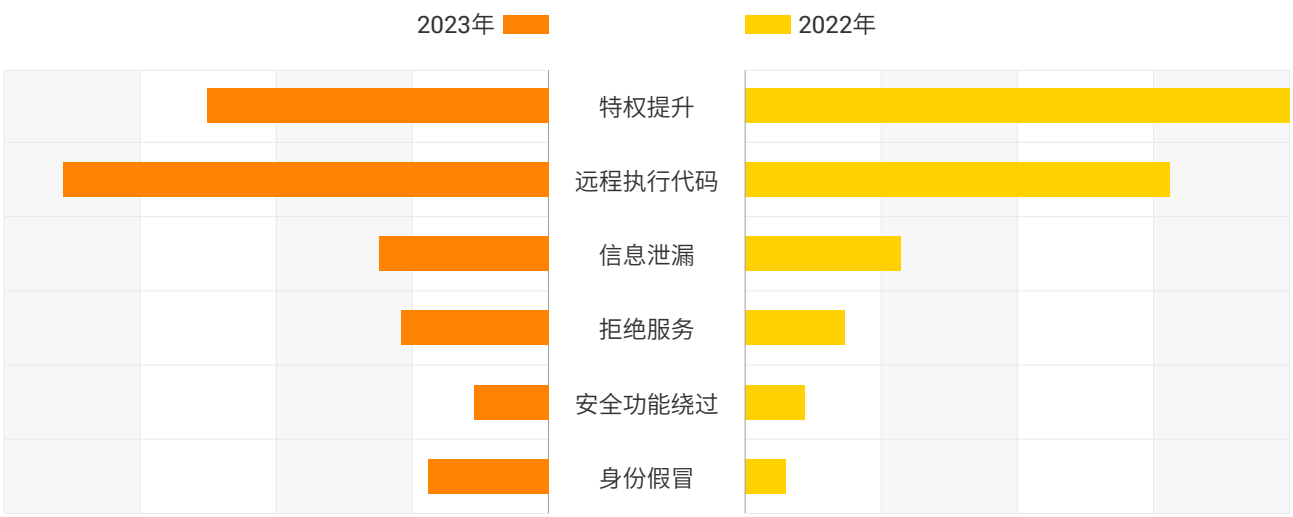
1317万次

2023 年，火绒安全产品共拦截 2.26 亿次漏洞攻击，其中拦截 1.67 亿次微软系统漏洞攻击，拦截 1317 万次 Web 漏洞攻击。

微软去年对外披露了 1374 个漏洞，包含高危漏洞 88 个，严重漏洞 859 个。远程执行代码漏洞一旦被成功利用后，攻击者能够在目标计算机上远程执行任意代码，对用户形成严重的安全风险。

火绒安全 HUORONG SECURITY

近两年微软系统漏洞类型

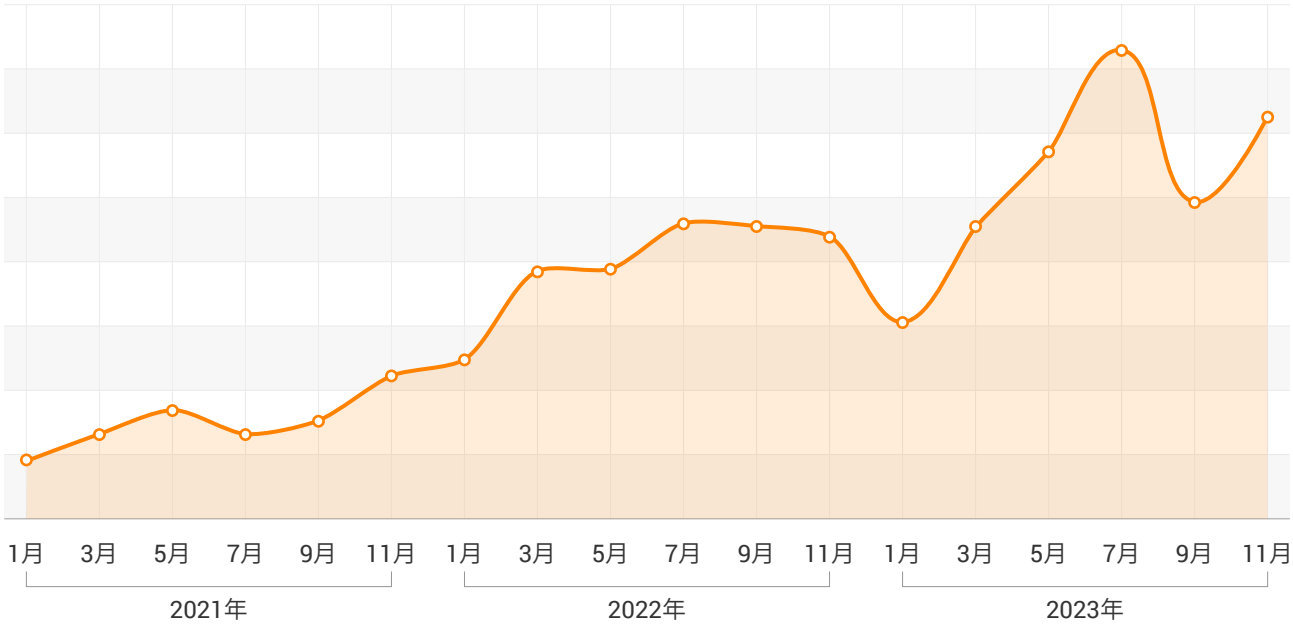


Web漏洞攻击

2023 年特别是上半年 Web 漏洞攻击持续上涨，疫情期间越来越多的企业加速数字化转型的步伐，新系统、新软件、新技术不断被应用，其中漏洞被利用风险随之增长。此外，CVE-2017-10271、CNVD-2021-30167、CVE-2007-1036、CVE-2019-2725 连续多年成为易被利用的 Web 漏洞，针对这些旧漏洞，外界拥有特定开发的漏洞利用代码或工具，黑客更方便拿来攻击未更新修复的目标。

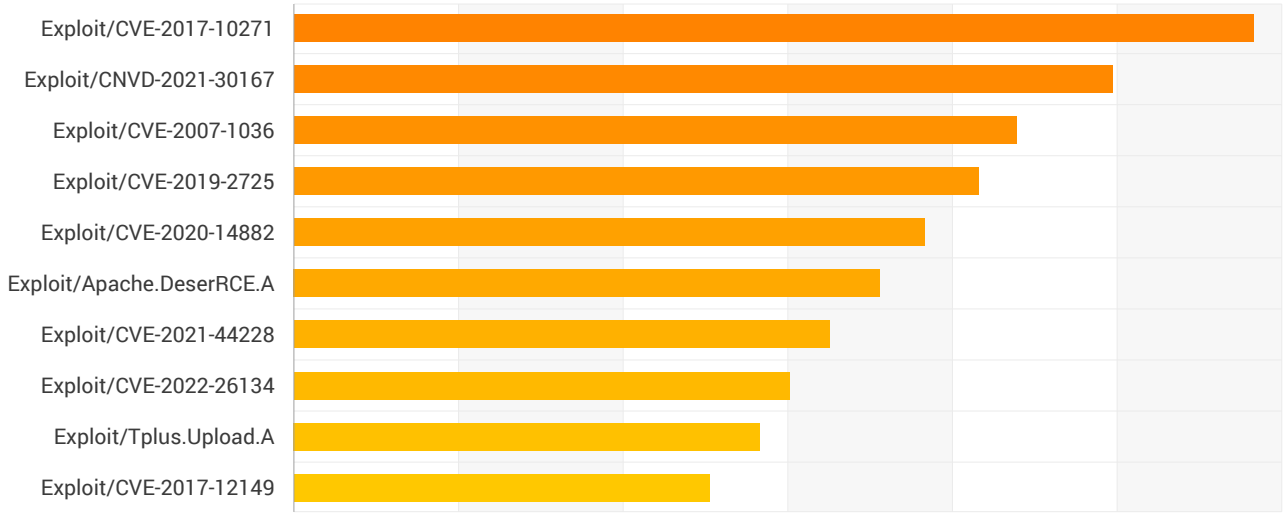
火绒安全 HUORONG SECURITY

近三年 Web 漏洞攻击数量趋势



火绒安全 HUORONG SECURITY

2023 年被利用的 Web 漏洞 TOP10



个人终端应急服务

内核级病毒 **40%**

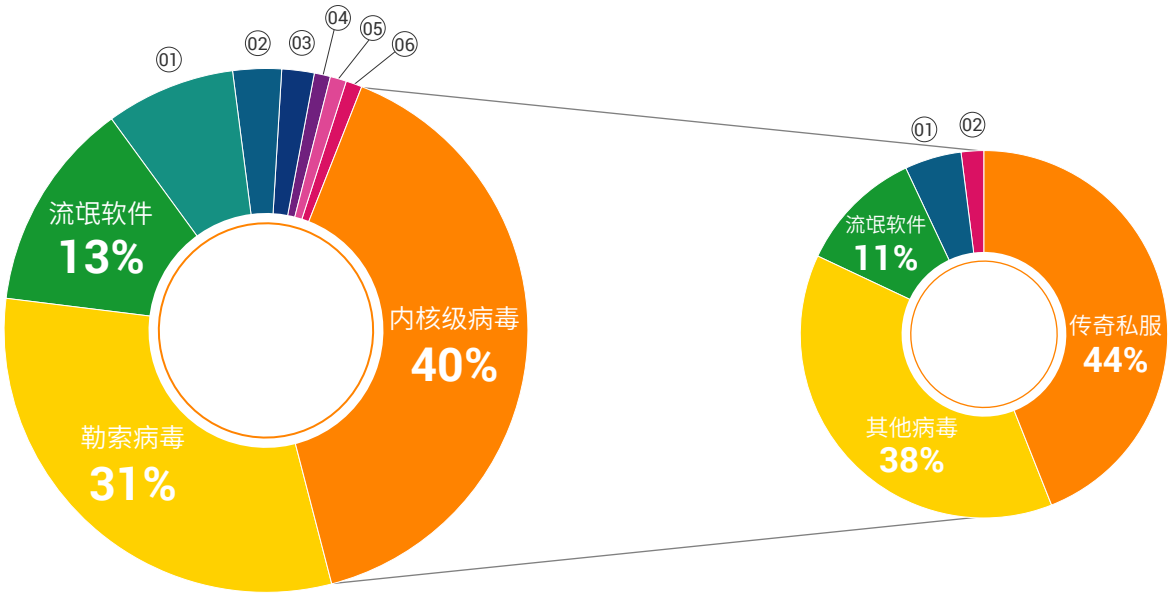
勒索病毒 **31%**

流氓软件 **13%**

根据“火绒在线支持和响应中心”处理的个人终端问题显示，个人终端常见病毒中，内核级病毒占 40%、勒索病毒占 31%、流氓软件占 13%。内核级病毒（Rootkit）一直是困扰用户的头号病毒威胁，其主要被用于劫持用户流量。火绒安全 2023 年发布多篇病毒报告，揭示了 Rootkit 病毒利用传奇私服、天龙八部游戏私服，劫持用户访问的网页到指定网站，并进行信息收集和数据篡改等恶意活动。

火绒安全 HUORONG SECURITY

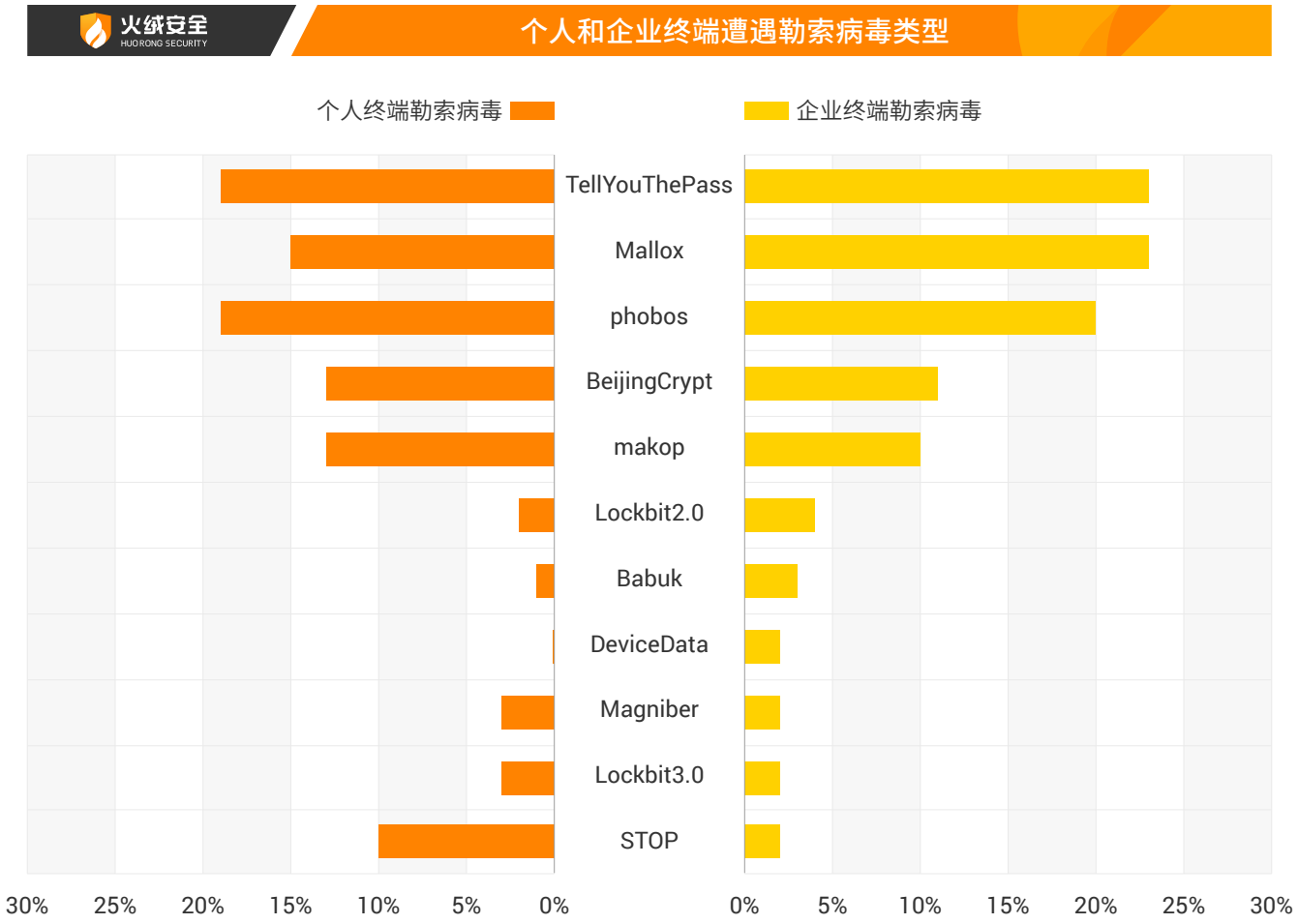
2023 年个人终端常见病毒占比



⑴ 木马病毒	8%	⑷ 挖矿病毒	1%		
⑵ 后门病毒	3%	⑸ 蠕虫病毒	1%		
⑶ 感染型病毒	2%	⑹ 恶意脚本	1%		

⑴ 软件设置	5%	⑵ 插件	2%

勒索病毒已经成为个人终端安全二号威胁，个人用户切莫掉以轻心，一次链接点击、一次文件下载，都有可能进入黑客的圈套。



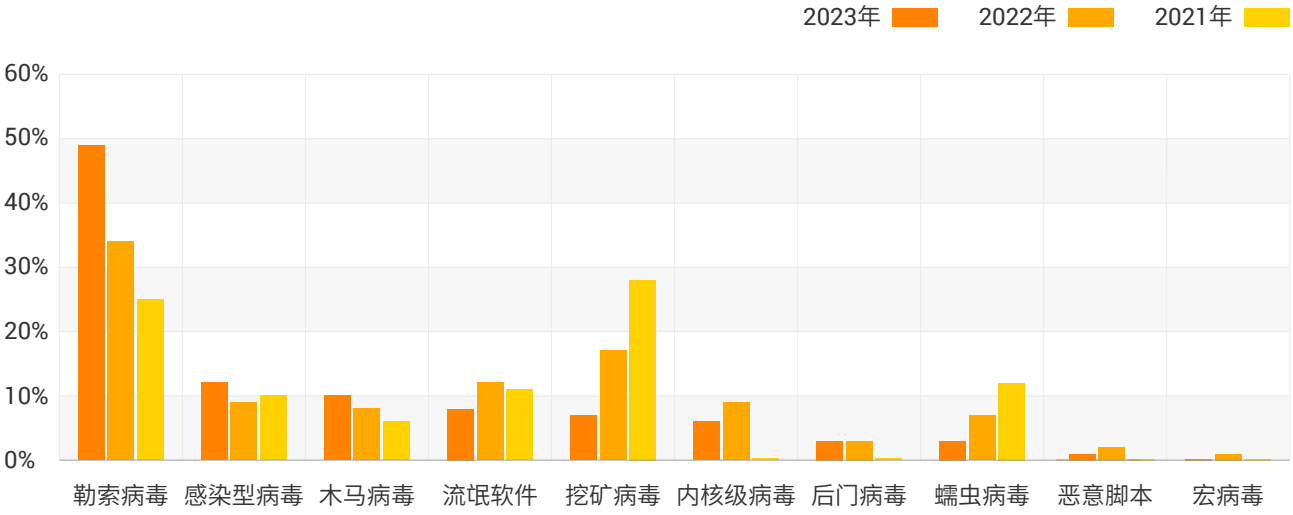
从勒索病毒类型来看，个人终端和企业终端遭遇的勒索病毒主要来自 TellYouThePass、Phobos、Mallox 三大家族：

- TellYouThePass 勒索软件家族在国内出现于 2020 年，通过软件漏洞进行攻击，并且可在短时间内对大量设备进行加密，针对包括政府机构在内的全行业。
- Phobos 勒索软件家族从 2019 年初期开始在全球流行，通过 RDP 暴力破解和钓鱼邮件等方式扩散到企业与个人用户中，并持续更新和演变，成为勒索软件家族中新兴的一个大家族。
- Mallox 勒索软件家族首次出现于 2021 年，专注于 MS-SQL 和暴力攻击，会定期公开被入侵的组织和盗取的数据，利用地下论坛宣传其服务并招募生态组织。

企业终端应急响应

火绒安全 HUORONG SECURITY

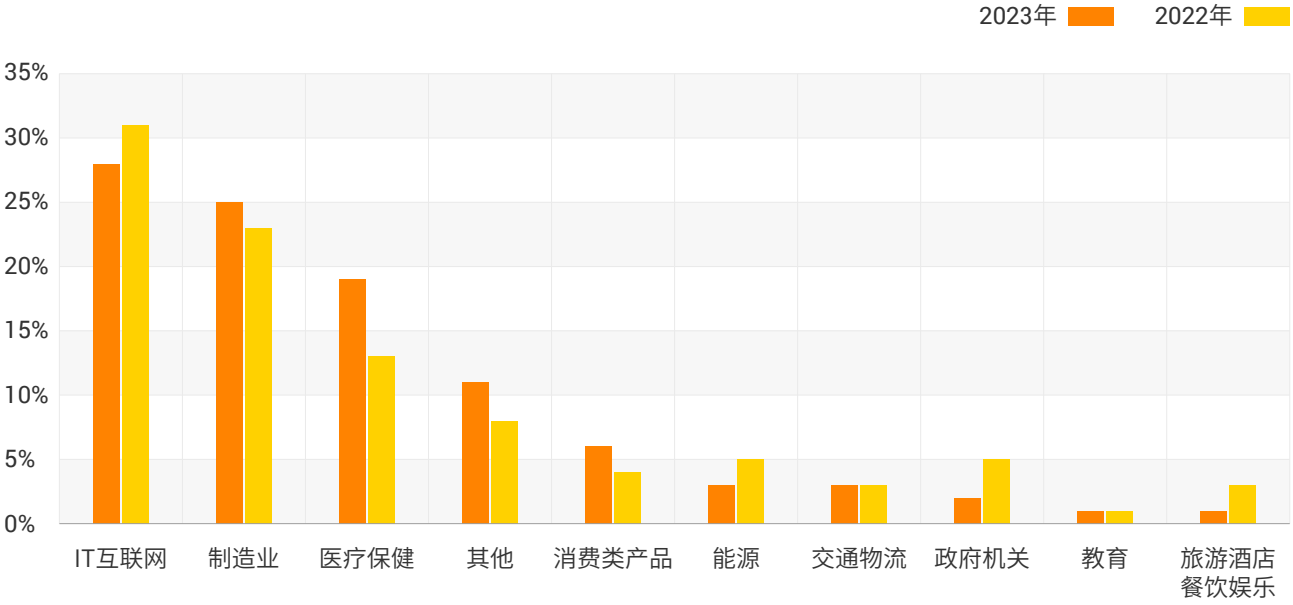
近三年企业终端常见病毒占比



近三年数据显示，勒索攻击已经超过挖矿病毒，成为企业安全主要威胁来源，且数量远超其他病毒威胁。勒索攻击目标集中在 IT 互联网（28%）、制造业（25%）、医疗保健行业（19%）。这三大行业与大众生产、生活紧密相关，拥有大规模的个人数据、商业信息，某个环节出现安全风险，都容易出现牵一发而动全身的情况。

火绒安全 HUORONG SECURITY

2022、2023 年各行业遭遇勒索病毒情况



勒索攻击作为成熟的攻击手段，拥有完整的商业模式（RaaS），RaaS 运营商通常提供易于使用的攻击工具和界面，这些工具涵盖各种功能，如暴力破解、端口扫描、漏洞扫描、加密文件、生成勒索信息、管理支付渠道等。这使得攻击者无需编写复杂的代码或具备深入的技术知识，便可轻松定制和启动攻击，他们可以是专业的黑客团队、犯罪组织，也可以是技术能力较低的个人。

此外，支付方式的匿名性（通常要求使用加密货币进行赎金支付），使得攻击者能够在不被追踪的情况下收取赎金，增加了勒索攻击的成功几率。因此，勒索攻击的易操作性、成功机率、支付匿名性使得越来越多的攻击者，采用这种形式获利。我们则需要加强网络安全意识、采取防御措施和及时更新系统，来应对这些威胁。

勒索攻击防护建议

01

使用能够检测和阻止已知勒索软件变体的反恶意软件或安全软件。

02

实时监测和检测网络活动，及时发现和应对异常行为，以遏制勒索软件攻击的扩散。

03

定期进行安全审计和评估，以识别网络和系统漏洞，并确保所有安全控制措施到位并正常运行。

04

对员工定期开展网络安全培训，加强员工的网络安全意识，包括识别和应对勒索软件等网络威胁。

05

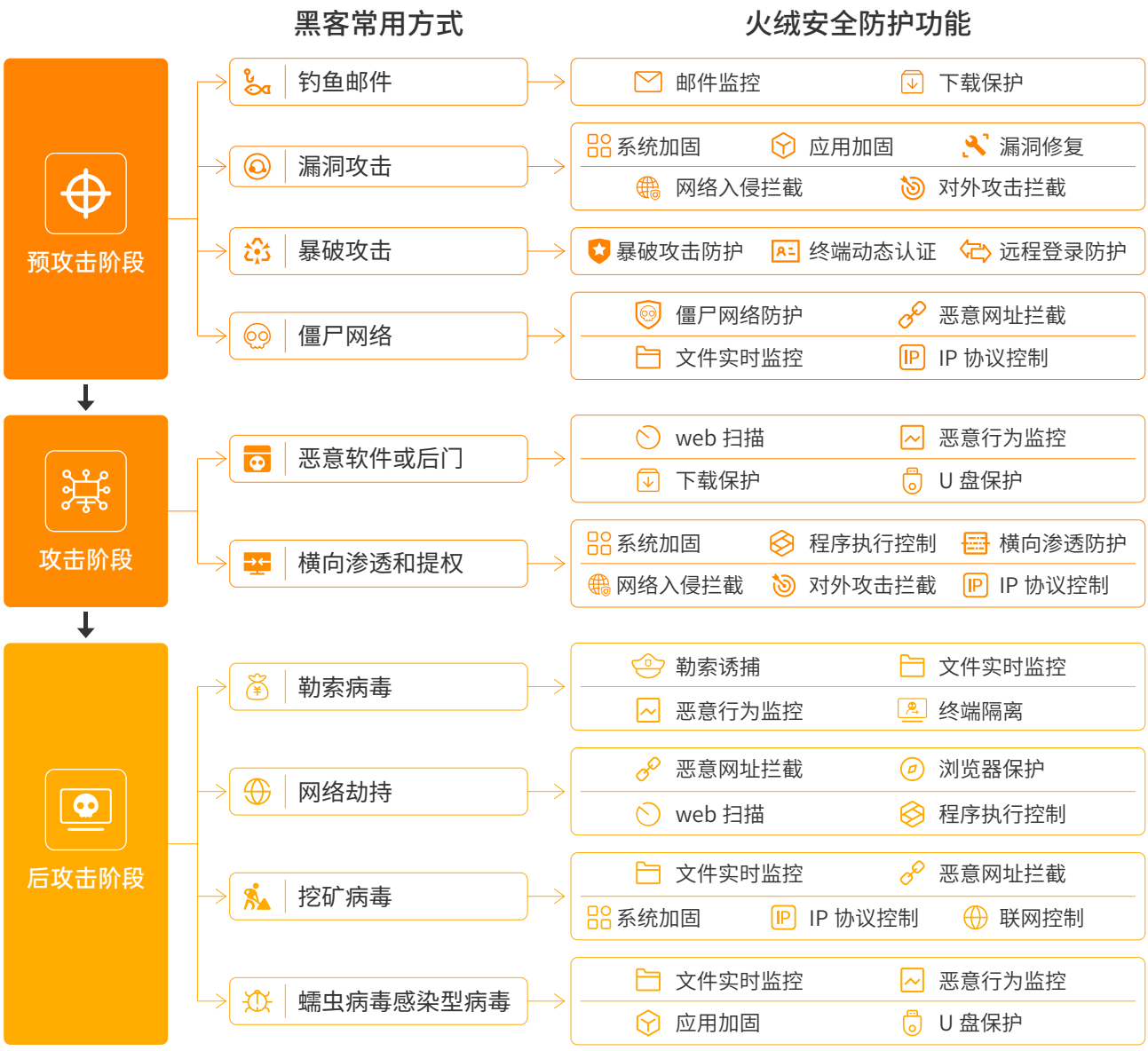
定期对重要文件和数据进行非本地备份，并设置访问限制，以降低勒索软件造成的影响。

黑客攻击阶段

面对日益严峻的网络攻击态势，如果企业不能有效预估和应对网络攻击，就可能导致重大损失。火绒安全团队通过对病毒的各种攻击方式分析发现，黑客会在攻击前期，对目标企业进行探测，以期找到企业系统中的弱点，随后利用各种手段入侵目标系统或局域网，成功入侵系统后，会为其后续的攻击和窃取潜在利益做准备。

火绒安全产品除了不断加强病毒的拦截、查杀以外，始终关注对攻击渠道的防御。从病毒层面、系统层面、网络层面设置多重防护，极大减少黑客攻击和潜在安全风险。

黑客常用攻击手段及火绒关键节点防护功能



综上所述，黑客会利用各种病毒、漏洞、技术，破坏网络系统，窃取敏感信息，甚至进行网络勒索等犯罪行为。因此，保护计算机终端免受黑客攻击至关重要，以下是一些常见的措施，可以提高系统和数据的安全性：

预防黑客攻击常见基本措施

更新和升级软件

保持操作系统、应用程序和安全软件为最新版本，可以修复已知的漏洞和弱点，提高系统的安全性。

01

使用安全软件

安装和定期更新可靠的安全软件，以检测和阻止恶意网络攻击。

02

使用强密码和多因素身份验证

为所有账户设置独特、复杂的密码，并启用多因素身份验证，增加账户的安全性。

03

定期备份数据

定期备份重要数据，防止数据丢失或被勒索软件加密。

04

实施访问控制

设置相应网络访问限制并分配适当权限，以防止未经授权的访问和数据泄露。

05

关于火绒安全

火绒安全成立于 2011 年，是一家专注、纯粹的终端安全公司，致力于在终端领域提供专业的安全产品和优质的用户服务，并持续对外赋能反病毒引擎等相关自主研发技术。

火绒安全个人产品“火绒安全软件”拥有数千万用户，凭借干净、轻巧、强大的特点收获良好的大众口碑与推荐。企业产品“火绒终端安全管理系统”是秉承“情报驱动安全”理念，全面实施 EDR 运营体系的一款反病毒 & 终端安全管理软件。

“火绒终端安全管理系统” 充分满足各企事业单位在当前互联网威胁环境下的电脑终端防护需求。产品支持 Windows、Linux、macOS 等主流操作系统，深度适配统信、鲲鹏、神州网信、中科方德、海光、龙芯等国产操作系统与 CPU。目前，“火绒终端安全管理系统”已部署超百万终端，覆盖政企、制造、医院、能源、汽车、IT 互联网等众多行业。

情报驱动安全

一个纯粹、专注的终端安全技术公司

北京火绒网络科技有限公司

BEIJING HUORONG NETWORK TECHNOLOGY CO., LTD.

电 话：400-998-3555

网 址：https://www.huorong.cn

地 址：北京市朝阳区红军营南路15号院瑞普大厦D座4层

火绒安全公众号