火绒安全
HUORONG SECURITY

2025 火绒安全
终端安全洞察报告

北京火绒网络科技有限公司

目　录

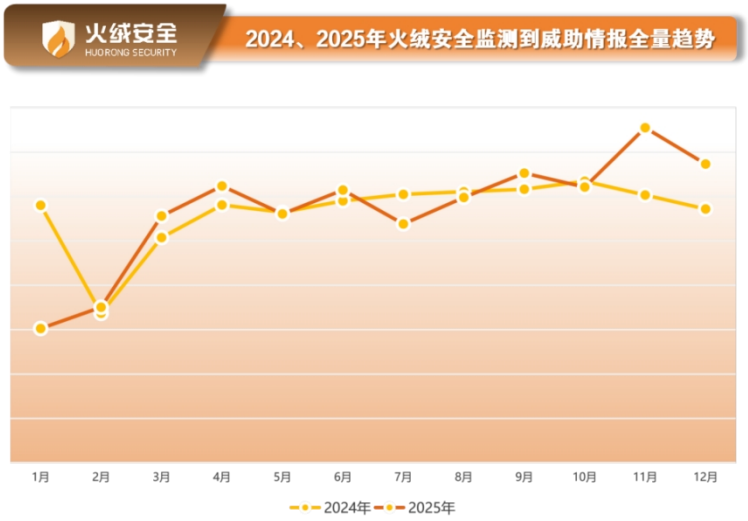
一 前 言

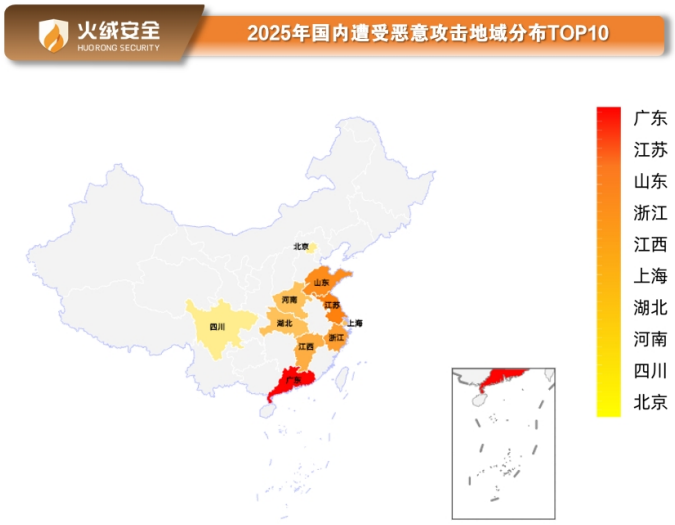
《火绒安全 2025 年终端安全洞察报告》以“火绒威胁情报系统”为统计基础，汇总梳理 2025 全年终端攻击威胁态势。希望为个人用户和企业用户提供更真实、更直观、更全面的终端威胁感知，帮助广大用户提高风险预防意识，有效采取防御措施应对潜在的终端安全威胁。

- 火绒安全产品共拦截终端攻击 34.23 亿次，终端攻击趋势波动较大，下半年攻击趋势逐步升高；
- 黑客主动向全网投放的病毒中，木马病毒占 35.38%、感染型病毒占 20.64%、蠕虫病毒占 12.71%。其中，木马病毒与感染型病毒占比最大；
- 银狐病毒家族成为年度活跃表现尤为突出的家族；
- 2025 年，火绒产品共提示软件安装超 10 亿次。除常见软件外，浏览器、办公软件与杀毒软件排名靠前；
- 火绒安全技术人员协助处理的个人终端问题中，银狐病毒占比高达 41.87%，是当前最主要的威胁；勒索病毒也以 22.94%的占比紧随其后，个人用户需重点防范这两类病毒风险；
- 近两年数据显示，银狐病毒、勒索病毒仍是企业安全的核心威胁，且银狐病毒的占比在 2025 年进一步攀升，成为企业终端最突出的风险来源；木马病毒的威胁占比也处于较高水平，企业需重点强化对这几类病毒的防护力度。

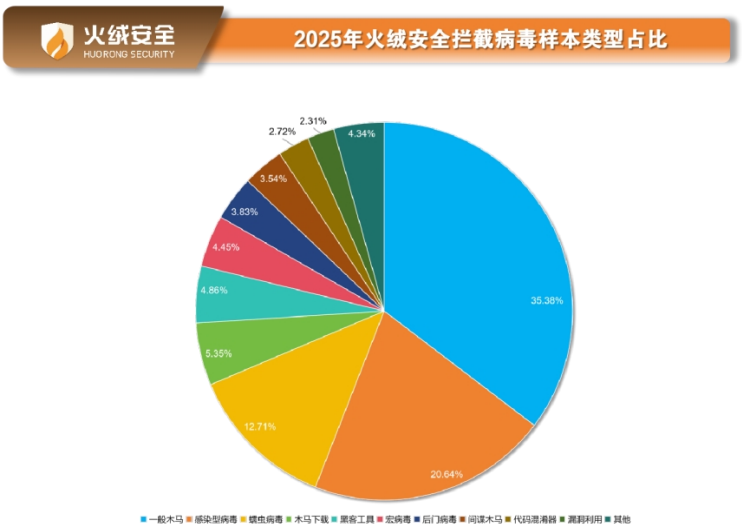
二 终端攻击整体态势

根据“火绒威胁情报系统”监测和评估，2025 年火绒安全产品共拦截终端攻击 34.23 亿次，略低于 2024 年（36.33 亿次），终端攻击趋势波动较大，下半年攻击趋势逐步升高。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、江西、上海、湖北、河南、四川、北京。





2025 年，木马病毒、感染型病毒、后门病毒、蠕虫病毒等恶意程序仍在持续对用户发起攻击，继续主导攻击场景，对用户终端安全构成严重威胁。



三 重点恶意病毒家族动态

攻击态势

2025 年网络威胁呈现智能化、协同化、产业化三大趋势，在此背景下，信息窃取与勒索病毒已形成相互支撑的黑产生态，其中银狐木马以其高频迭代与多元危害成为国内重大威胁。

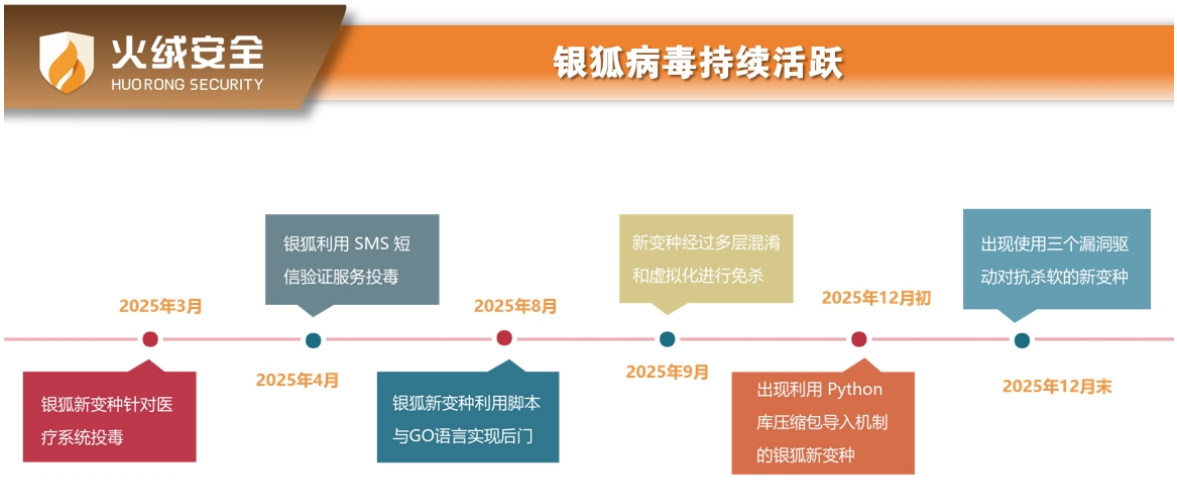
信息窃取

据火绒安全威胁情报系统监测，2025 年仍活跃的窃密病毒家族包括银狐（SilverFox）、Lumma Stealer、Rhadamanthys Stealer、StealC、SnakeStealer、RedLineStealer、Vidar Stealer、AgentaTesla 等；此外，“Steam 假入库”等上传 Steam JWT Token 的行为也可被视为窃密的恶意活动。

近年来窃密病毒已由单一窃取演进为多阶段、多模块化攻击，常结合无文件落地、云控下发、天堂之门等技术，并采用多语言实现，整体专业化与多样化趋势明显。同时，多数家族以 MaaS（恶意软件即服务）模式售卖，降低攻击门槛并加剧安全风险，其中以 Lumma Stealer、Rhadamanthys Stealer 等家族较具代表性。

银狐（SilverFox）病毒家族：2025 年，“银狐”持续活跃，以 ValleyRAT/Winos 等远控木马为核心，常通过钓鱼邮件、伪装安装包与搜索引擎投毒入侵并长期潜伏，侧重窃密与横向渗透。其在多起行动中滥用易受攻击的驱动以绕过 EDR 并实现持久化，变种迭代迅速，免杀对抗策略随版本持续调整。预计攻势将延续至 2026 年，企业需强化供应链与安装包审计、驱动完整性检测与端点/网络异常监控。

根据火绒威胁情报系统的梳理，2025 年银狐病毒在不同时间点的新变种与手段变化时间线如下：



2025 年银狐的投放策略进一步“下沉”：攻击目标不再局限于政府/企业财务人员等高价值人群，逐渐转向借助虚假安装包进行传播的“广撒网”模式，受影响范围扩展至学校师生、医疗机构等更广泛的行业领域。值得关注的是，银狐在伪装对象上新增了安全软件，这表明攻击者正在利用“安全焦虑”心理进行投毒——针对缺乏有效防护、且有安装安全软件意愿的用户群体，提高恶意载荷的投放成功率。

Lumma Stealer 窃密病毒家族：2025 年，Lumma Stealer 窃密病毒家族仍持续活跃，呈“打击后快速复苏+技术迭代升级”态势，购买者所投毒的领域主要为作弊或破解工具、供应链、Github 开源项目、软件安装包等，从而获取浏览器缓存的身份验证信息、Cookies 以及数字货币钱包等高价值敏感数据。

Rhadamanthys Stealer 窃密病毒家族：2022 年发布于黑客论坛，且 2025 年仍活跃于 Google 广告推送机制或 Github 项目中，该窃密病毒使用无文件落地、自定义 PE 头、天堂之门等手段进行免杀，从而窃取信息。此外，根据公开执法信息，2025 年 11 月相关基础设施被欧洲机构联合打击，后续活跃度仍需持续观察。

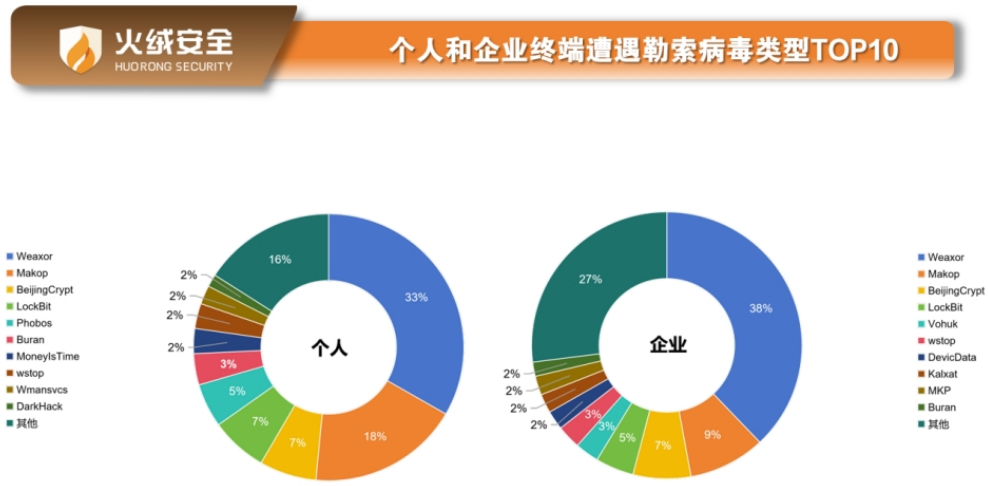
StealC 窃密病毒家族：2023 年出现于黑客论坛，在 2025 年 StealC V2 版本整体呈现典型的多阶段与云控驱动（C2/配置下发）特征，并额外添加 RC4 算法加密进行免杀。其云控配置中携带下一阶段的窃密模块地址，最终窃密时可根据云控策略动态调整窃取范围。在窃取能力上，除常规的 Cookies 与浏览器数据外，StealC 还会结合浏览器插件实现网页交互的能力，例如在加密货币交易平台执行转账脚本，从而将货币窃取至盗窃者账号中。

勒索病毒

根据 2025 年勒索病毒相关统计数据，火绒安全在 2025 年拦截到的勒索病毒攻击总量较 2024 年仅呈小幅上升，整体未出现明显“爆发式增长”，但勒索威胁仍需保持警惕。从全年趋势来看，勒索攻击在上半年相对更为活跃，并于 6 月达到阶段性峰值；进入下半年后，攻击规模整体趋于平稳。

从终端遭遇勒索病毒类型 TOP10 的统计结果来看，2025 年勒索病毒家族排名出现明显变化。与 2024 年相比，原本位列第一的 Mallox 已被 Weaxor 取代，与此同时 Makop、BeijingCrypt

等老牌勒索病毒家族依然活跃，而 LockBit 勒索家族有“死灰复燃”的趋势。值得关注的是，2025 年勒索生态中有更多此前相对少见的家族进入数据量前位，例如 DevicData、MoneyIsTime、DarkHack 等，反映出生态系统碎片化趋势进一步加速。



对 2025 年勒索软件攻击组织的受害行业分布进行分析可见，制造业、IT 与医疗保健领域仍是主要攻击目标，同时，能源和政府部门相较 2024 年呈现出一定程度的攻击倾向上升。

从数据层面来看，2025 年企业遭受勒索攻击的次数较 2024 年有所下降，但勒索攻击的破坏性与潜在业务影响仍然突出，风险不容忽视。

2025 年勒索病毒攻击链条与往年相似，攻击者往往通过入侵的手段获取远程执行能力，再投放勒索载荷实施加密并进行勒索。常见入侵手段包括业务软件漏洞、Web 漏洞利用、

RDP 暴力破解、数据库爆破等方式。

Weaxor 勒索病毒家族：Weaxor 勒索病毒家族与 Mallox 勒索病毒家族存在较高相似度，例如规避俄语区、调整电源计划为高性能模式等，被众多业内人士猜测是从 Mallox 演变而来。从 2025 年勒索家族分布数据来看，Mallox 的出现频次显著下降，而 Weaxor 快速攀升并进入头部位置，呈现出“替代性上升”的趋势。在入侵层面，该勒索病毒家族利用数据库漏洞的方式入侵，并使用漏洞驱动关闭杀软，从而创造执行勒索病毒的环境。

Makop 勒索病毒家族：Makop 勒索病毒家族在 2020 年在黑客论坛发布时宣称推出 RaaS（Ransomware-as-a-Service，勒索软件即服务）模式，2025 年 Makop 仍保持持续活跃，该家族偏爱利用 RDP 暴力破解和数据库爆破等方式进行入侵，且因其在字符串解密等代码实现上表现出高度一致性，被认为与 Phobos 存在较强关联。

BeijingCrypt 勒索病毒家族：BeijingCrypt 勒索病毒从 2020 年开始在网络环境中发现的老牌勒索家族，2025 年依旧活跃在勒索 TOP10 榜单前列，常常通过数据库被入侵后植入远控工具（Anydesk），随后攻击者远程登录受害者主机关闭杀软并执行 BeijingCrypt 勒索病毒，从而实现勒索。

防护建议

企业与个人需针对不同病毒类型及家族特点实施差异化防护策略，同时加强安全防护体系建设，以应对日益复杂的勒索软件威胁：

1、警惕聊天过程中对方突然发来的网址和文件，打开前尽量进行身份验证，确认对方身份是否为本人；

2、下载软件时，建议从火绒应用商店或其他官方渠道进行下载；

3、及时更新软件和修复漏洞，以防病毒通过漏洞入侵服务器；

4、建议关闭非必要公网暴露端口，对必须开放的远程管理端口（如 RDP/SSH）设置 IP

白名单、登录失败锁定等限制，防止暴力破解攻击；

5、实时监测和检测网络活动，及时发现和应对异常行为，以防病毒攻击扩散；

6、定期对重要文件和数据进行非本地备份，并设置访问限制，降低勒索或窃密病毒造成的影响；

7、加强员工网络安全意识，定期开展网络安全培训。

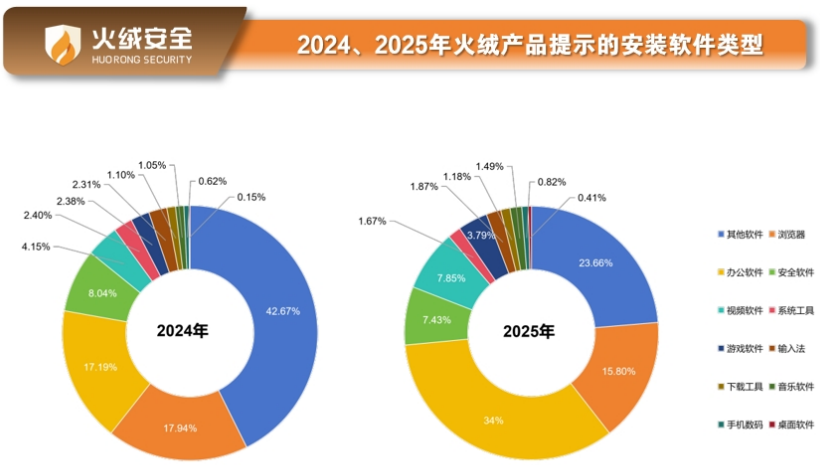
四 软件安装与弹窗广告现状

软件安装提示现状

软件捆绑安装仍是困扰用户的常见问题：这类软件常以弹窗骚扰、篡改网页、占用内存等方式拖慢系统，甚至携带恶意代码，威胁终端安全与用户隐私、财产信息安全。

火绒安全产品可识别曾被捆绑的软件，2024 年个人版升级后新增的“潜在不受欢迎软件监控功能”，能及时提醒风险，帮助用户避免在不知情的情况下安装冗余软件的隐患。

2025 年，火绒产品提示软件安装数据再更新：从类型分布看，办公软件的提示占比大幅提升，同时其他软件、安全软件等类型的占比也有变化。相较于 2024 年，办公软件的提示比例增长显著，反映出这类软件的捆绑安装风险更受关注。



弹窗广告拦截趋势

2025 年火绒安全产品共拦截（不含用户手动拦截）弹窗广告 12.02 亿次，较 2024 年全年有小幅度增长。

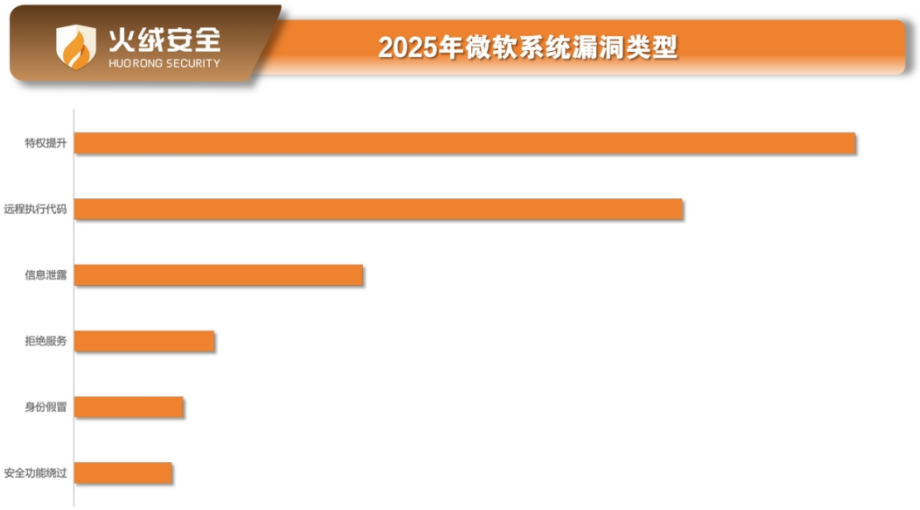
2025 年全年拦截量呈波动起伏趋势：1-2 月小幅回落，3-5 月回升后趋于平稳，6 月大幅攀升至全年峰值，7 月起持续回落至 10 月触底，年末小幅回弹后再度走低，整体趋势波动明显。

五 漏洞攻击

2025 年火绒安全产品共拦截 2.1 亿次漏洞攻击，其中拦截 1.91 亿次微软系统漏洞攻击，拦截 2012 万次 Web 漏洞攻击。

系统漏洞攻击

微软去年对外披露了 3908 个漏洞，包含高危漏洞 187 个，严重漏洞 1230 个。其中特权提升漏洞占据榜首。这些漏洞会给用户带来严重的安全风险，一旦被成功利用，将会严重威胁用户的数据安全和隐私。



特权提升漏洞：攻击者利用系统弱点将自身权限提升到更高等级，从而执行原本不应被授权的操作（例如从普通用户提升到管理员/SYSTEM/root）。其核心是权限边界或授权控制被绕过/破坏，常用于攻击链中的“扩大控制权”阶段。攻击者可以使用该漏洞将本无权限运行的程序变为高权限执行。

远程代码执行漏洞：攻击者能够通过网络与目标交互并触发缺陷，使目标在其自身安全上下文中执行受攻击者控制的任意代码，通常与输入校验不足、代码/命令注入等缺陷相关。漏洞一旦被成功利用后，攻击者可以对目标进行远程控制、病毒下发、机密窃取等操作。

信息泄露漏洞：攻击者可以通过该漏洞，获取到软件、相关服务或系统的敏感信息，例如包括从权限控制不足的接口、页面、日志、错误信息回显等位置中，泄露凭据、令牌、密

钥、个人数据或内部状态信息等，从而破坏机密性并为进一步攻击提供条件。这会让攻击者通过精准踩点扩大攻击面。

Web 漏洞攻击

根据“火绒威胁情报系统”监测数据显示，2025 年针对 Web 服务漏洞的攻击呈现上升趋势，同时也表明企业在 Web 服务安全防护方面仍需保持高度警惕，以应对持续存在的网络威胁。

2025 年度系统漏洞 Top3

漏洞编号：CVE-2025-29824

漏洞名称：Windows Common Log File System 驱动程序特权提升漏洞

公布日期：2025-04-18

漏洞介绍：CVE-2025-29824 是 Windows 内核公共日志文件系统（CLFS）驱动中的一个提权漏洞。漏洞属于内存释放后但仍被继续访问的错误，攻击者可利用该漏洞读取和写入内核内存，从而将自身权限从普通用户最高提升至 SYSTEM 级别。

漏洞编号：CVE-2025-59287

漏洞名称：Windows Server Update Service (WSUS) 远程代码执行漏洞

公布日期：2025-10-14

漏洞介绍：该漏洞存在于 Windows Server Update Services（WSUS）组件中，由对不受信任数据的反序列化错误引起，允许远程未认证攻击者通过发送特制请求在目标 WSUS 服务器上执行任意代码。（WSUS 属于 WindowsServer 系统组件，用于向客户端分发更新）

漏洞编号：CVE-2025-62221

漏洞名称：Windows Cloud Files Mini Filter 驱动程序特权提升漏洞

公布日期：2025-12-09

漏洞介绍：此漏洞发生在 Windows 系统 Cloud Files Mini Filter Driver（云文件迷你过滤驱动）中的本地权限提升漏洞。漏洞属于内存释放后但仍被继续访问的错误，攻击者需已能够在系统上执行低权限代码（本地访问），即可利用该漏洞最高提权至 SYSTEM 权限。

六 终端应急服务与安全防护建议

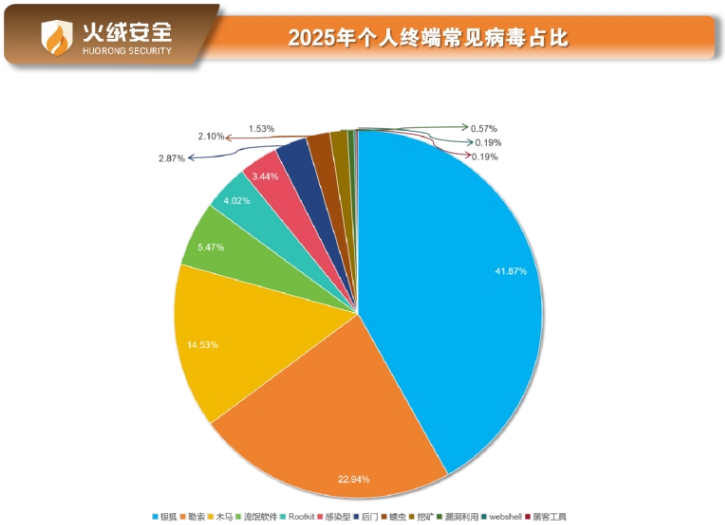
在数字技术飞速发展的当下，网络攻击的技术手段与实施策略正朝着多元化、隐蔽化的方向不断演进，其复杂程度远超以往。终端设备作为连接数字世界与现实生活、办公场景的核心载体，已然成为网络安全风险的核心暴露点，面临的安全挑战日趋严峻。无论是持续迭代的恶意软件、无孔不入的网络渗透，还是靶向精准的定向攻击，都时刻威胁着终端设备的

安全稳定运行，不仅可能导致个人隐私信息泄露、财产权益受损，更会给企业带来核心商业数据流失、业务流程中断等致命影响。

火绒安全深耕终端安全领域多年，以自主研发的反病毒引擎为技术核心，搭建起覆盖“预防——检测——响应——溯源”全流程的多层次主动防御体系，并结合实时更新的火绒威胁情报系统，形成立体化防护矩阵。该体系既能精准识别并拦截各类病毒、木马、勒索软件等恶意攻击，又能针对操作系统底层漏洞、软件安全缺陷等关键脆弱点构建专项防护屏障，通过动态监测终端行为、智能分析威胁态势、快速响应安全事件，实现对终端威胁的精准研判与高效处置，为个人用户与企业客户的终端安全筑起坚不可摧的全方位保障防线。

个人终端应急服务

个人终端常见病毒 TOP3 中，银狐病毒以 41.87%位居前列，紧随其后的是勒索病毒 22.94%、木马病毒 14.53%。



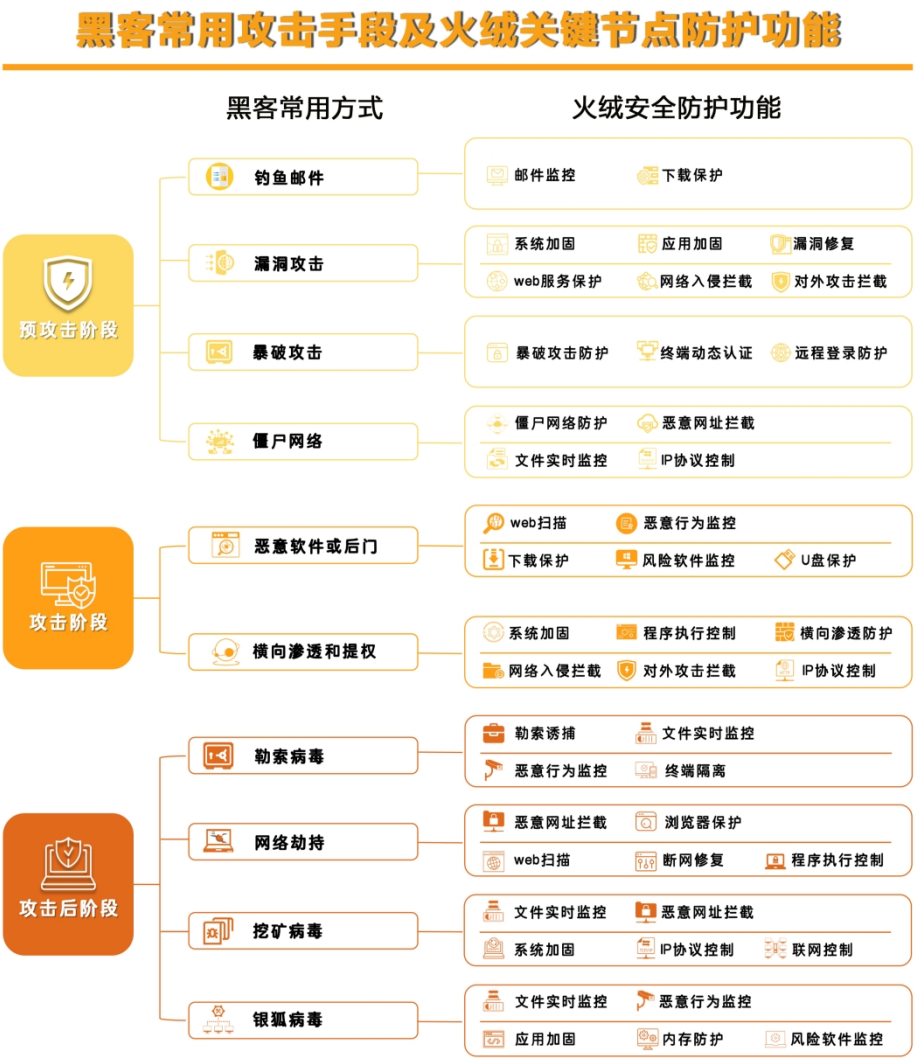
企业终端应急服务

近两年数据显示，企业终端常见病毒 TOP3 中银狐病毒、勒索攻击、木马病毒已成为企业安全的三大主要威胁来源。从病毒任务数占比来看，银狐病毒以 30.14%位居首位，勒索攻击紧随其后为 28.19%，木马病毒则为 12.74%。

这些病毒给企业终端带来了严重的危害。**银狐病毒**通常会通过伪装成正常文件或利用系统漏洞潜入用户终端，它会在后台悄悄收集用户的敏感信息，如账号密码、银行卡号等，然后将这些信息传输给不法分子，导致用户的财产安全受到极大威胁。**勒索病毒**则更为直接和暴力，一旦感染，它会加密用户终端上的重要文件，并要求用户支付高额赎金才能解锁文件。许多用户因重要数据被加密而陷入困境，支付赎金不但可能无法恢复文件，反而还会助长黑客的犯罪行为。**木马病毒**则像隐藏在暗处的间谍，在用户毫不知情的情况下控制终端，它可以窃取用户的隐私数据、监控用户的操作行为，甚至还能为其他恶意软件打开入侵的通道。

安全防护建议

火绒安全产品在持续精进病毒拦截与深度查杀核心能力的同时，始终聚焦攻击源头的全链路防御，构建起覆盖病毒、系统、网络三大核心维度的多重防护体系。通过对恶意程序传播路径的精准阻断、操作系统安全短板的强化加固、网络攻击行为的实时拦截，从根源上压缩黑客攻击空间，最大限度降低各类潜在安全风险，为终端设备构筑起无死角的安全防护网。



黑客往往借助各类恶意病毒、系统漏洞及多元攻击技术，蓄意破坏网络系统的正常运行，非法窃取敏感数据，更有甚者实施网络勒索等违法犯罪行径，对个人权益与企业利益造成严重侵害。因此，筑牢计算机终端安全防线、抵御黑客各类攻击，已成为保障数字安全的关键所在。

以下为可提高系统和数据的安全性的常见措施——

1、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。

2、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。

3、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。

4、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。

5、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。

预防黑客攻击常见基本措施

火绒安全相关加固建议——

1、开启火绒勒索诱捕；

2、开启程序执行控制——远程控制工具、风险工具项；

3、设置定时查杀计划任务，并关注查杀结果，建议一周至少执行一次；

4、设置密码保护，防止终端被恶意退出、卸载；

5、提高终端用户安全意识。

七 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、IT 互联网、能源、汽车、交通等众多行业。

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：北京市朝阳区北苑路北京文化创意大厦 B 座 9 层