火绒安全
HUORONG SECURITY

2024

火绒安全
终端安全洞察报告

北京火绒网络科技有限公司

概　述

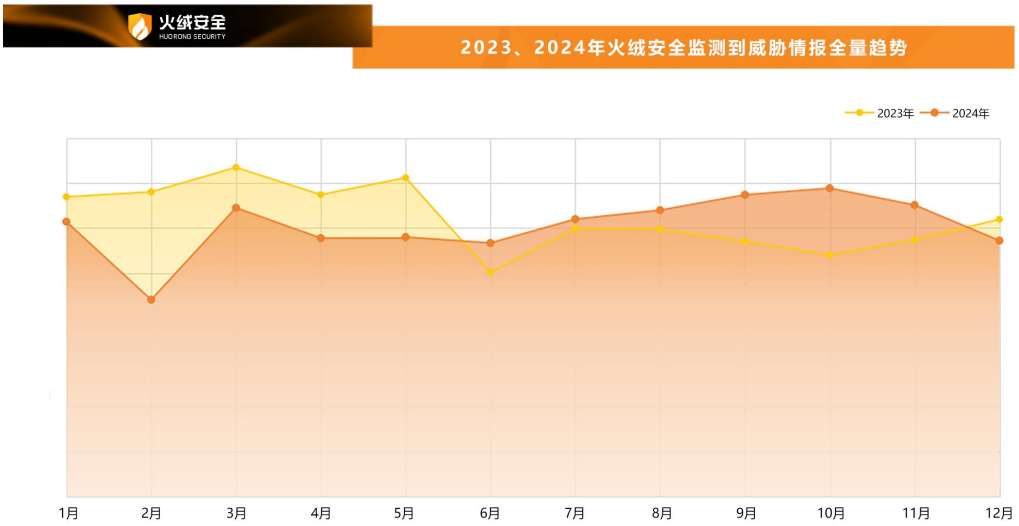
《火绒安全 2024 年终端安全洞察报告》以“火绒威胁情报系统”为统计基础，汇总梳理 2024 全年终端攻击威胁态势。希望为个人用户和企业客户提供更真实、更直观、更全面的终端威胁感知，帮助大家提高风险预防意识，有效采取防御措施应对潜在终端安全威胁。

- 火绒安全产品共拦截终端攻击 36.33 亿次，上半年拦截数量波动较大，下半年攻击逐渐增多，10 月达到峰值后略有回落但仍维持在较高水平。
- 黑客主动向全网投放的病毒中，木马病毒占 50.89%、下载者木马病毒占 18.11%、感染型病毒占 7.91%、后门病毒占 7.16%。其中，木马病毒与下载者木马病毒均已攻击数百万终端。
- 银狐病毒家族与 LummaStealer 家族成为年度活跃表现尤为突出的家族。
- 2024 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，银狐病毒和勒索病毒成为仅次于主页劫持病毒的威胁，个人用户切莫掉以轻心。
- 近两年数据显示，勒索攻击、木马病毒与银狐病毒成为企业安全主要威胁来源。其中，银狐病毒异军突起，成为威胁企业安全的病毒 TOP3。

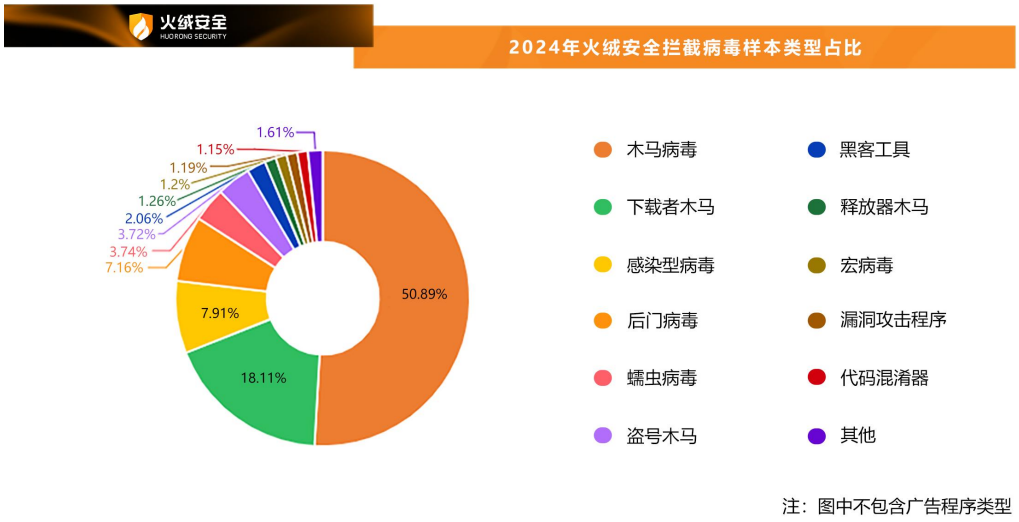
目　录

终端攻击趋势

根据“火绒威胁情报系统”监测和评估，2024 年火绒安全产品共拦截终端攻击 36.33 亿次，略低于 2023 年（37.35 亿次）。上半年的终端攻击趋势波动较大，但攻击量整体较低于 2023 年上半年；下半年攻击逐渐增多，在 10 月达到峰值后略有回落，但仍维持在较高水平。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、河南、湖北、北京、上海。



2024 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。



注：图中不包含广告程序类型

常见病毒防护建议

❖ 感染型病毒

感染型病毒擅长“寄生”，会寄居在正常程序或文件中，进行不断自我复制并快速感染其他文件，导致正常使用的软件被安全软件频繁报毒。感染型病毒具有强感染性和顽固性，若未能在第一时间处理便会迅速感染传播，若未能彻底清除便会卷土重来。火绒安全产品对感染型病毒的报毒提示以“Virus”开头，如发生频繁报毒现象，需清空【信任区】并将【防护中心】-【病毒防护】中的【文件实时监控】级别调整为高级后，对全网终端使用【全盘查杀】功能进行查杀，查杀完成后重启电脑。（**注：**火绒安全产品在处理感染型病毒时仅清除恶意代码，不会破坏原文件，用户可放心查杀。）

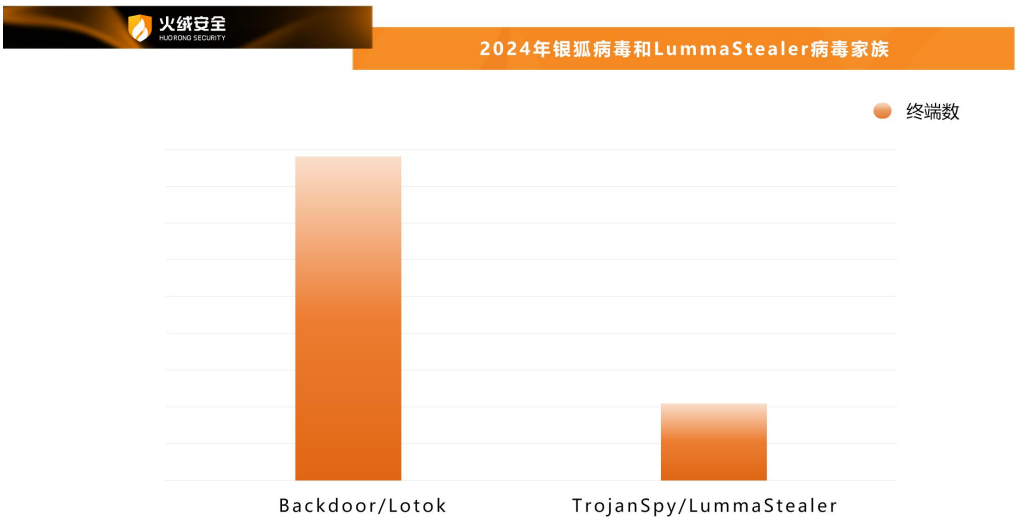
❖ 木马病毒

木马病毒擅长“伪装”，通常会伪装成正常程序，能够长期存在于被感染者终端，进行信息盗取、系统资源占用、远程控制等。火绒安全产品对木马病毒的报毒提示以“Trojan”开头，建议大家定期使用【全盘查杀】功能进行查杀，全盘查杀后，再使用【安全工具】中的【专杀工具】进行二次查杀。两次查杀完成后重启电脑再次【快速扫描】确认是否有残留报毒。

银狐、LummaStealer 病毒大幅活跃

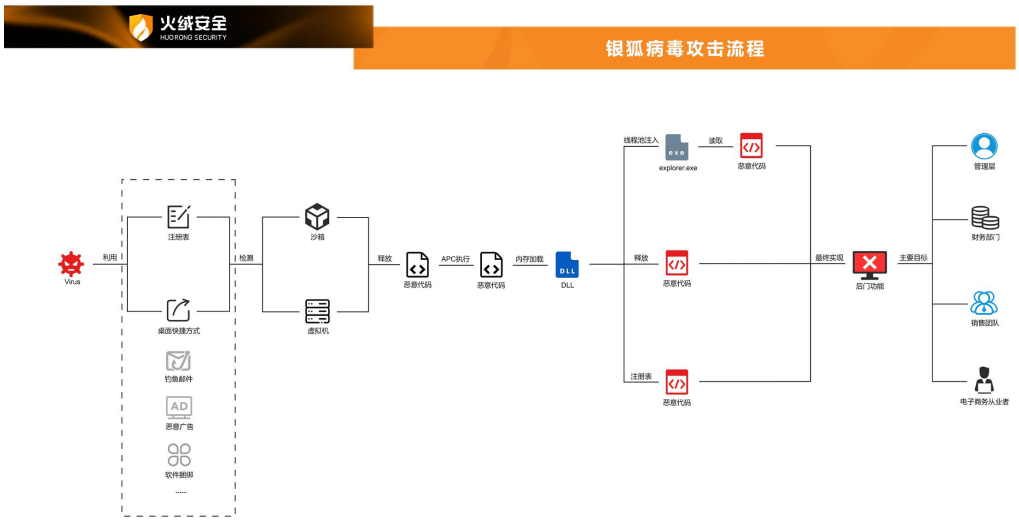
在 2024 年的网络安全威胁中，银狐（SilverFox）、LummaStealer 等恶意木马家族的活跃表现尤为突出。其中，银狐病毒的攻击呈上升趋势，对企业和关键机构造成了巨大的影响；LummaStealer 病毒从籍籍无名到现在的排名靠前，成为窃取敏感信息的主要威胁之一。

这些恶意软件大多采用模块化设计，因此攻击者能够根据目标需求动态调整恶意行为进行信息窃密。它们不仅具备高度的隐蔽性和破坏性，还会通过不断更新技术手段，试图绕过传统的安全防护措施，严重威胁终端安全。



▶ 银狐（SilverFox）病毒家族

银狐是一种新型的恶意木马家族，主要传播途径为钓鱼邮件、恶意广告和软件捆绑。银狐病毒家族将目标锁定在企业与机构中的关键岗位人员，如管理层、财务部门、销售团队以及电子商务从业者，通过精心设计的定向钓鱼攻击来获取敏感信息。



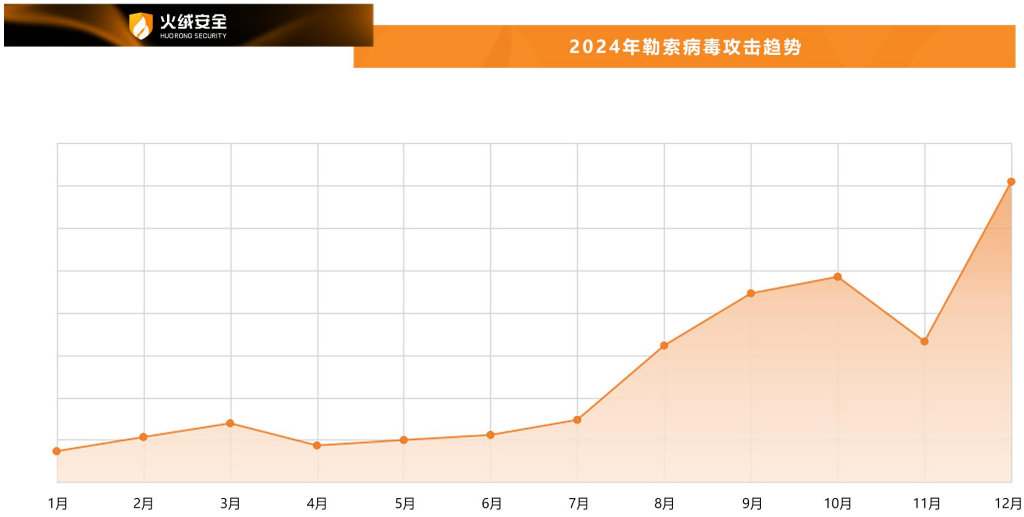
自 2021 年以来，银狐木马活动显著增多，并持续至今(2024 年 12 月)，始终维持着高活跃态势，持续构成跨年度高危网络威胁。根据火绒威胁情报系统的梳理，2024 年银狐病毒及其重要变种的时间线如下：

▶ LummaStealer 窃密家族

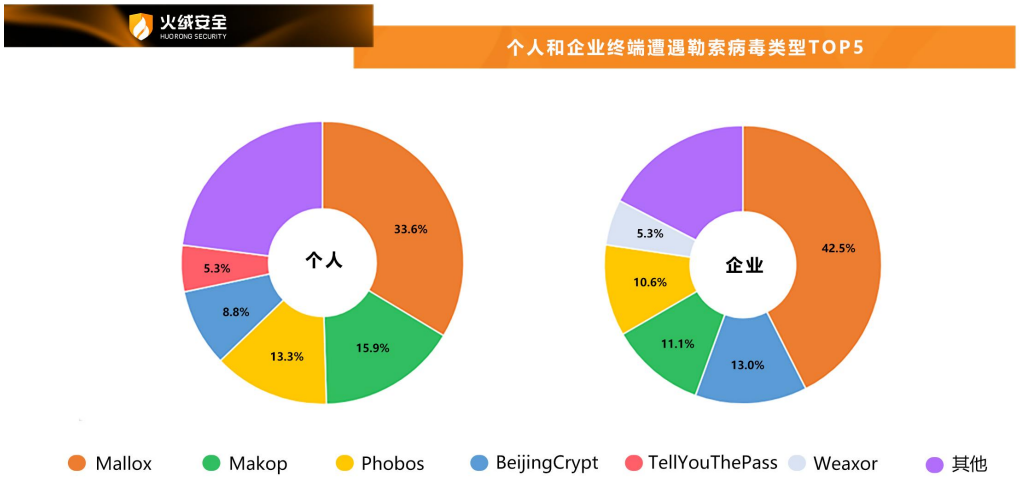
LummaStealer 是一种信息窃取类恶意木马家族，能够攻击多种操作系统，如 Windows 系统、macOS 系统和 Linux 系统。近年来，LummaStealer 窃密家族的活跃度显著上升。LummaStealer 木马拥有强大的数据窃取能力，专注于窃取浏览器保存的密码、加密货币钱包信息、Cookies 以及其他敏感数据；而采用恶意软件即服务（MaaS）模式传播，使得攻击者可以购买其服务并定制攻击目标，大大降低了攻击门槛，进一步加剧了网络安全隐患。

勒索病毒攻击逐渐增多

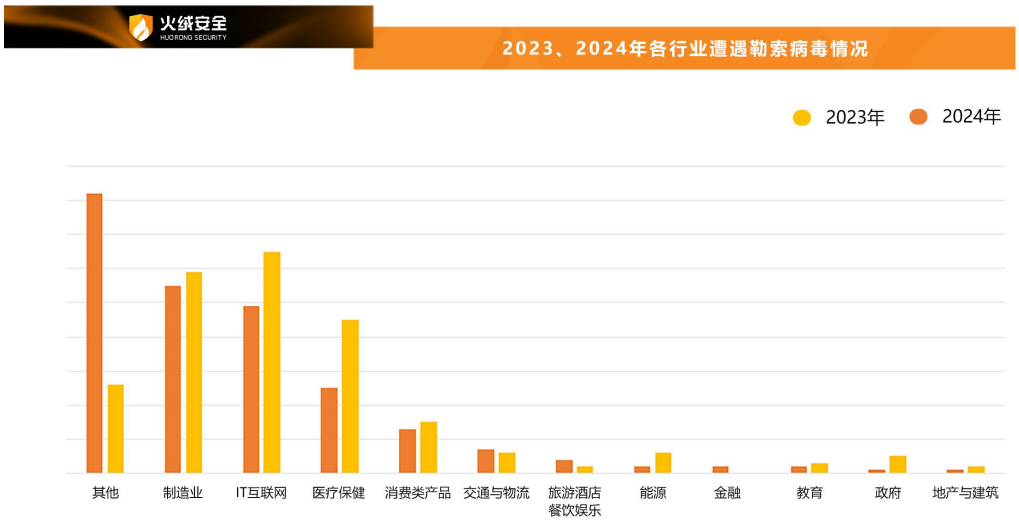
根据“火绒威胁情报系统”监测和评估，2024 年火绒安全拦截勒索病毒攻击 152.8 万次，全年终端攻击趋势在 4 月和 11 月短暂下降。其中，上半年的终端攻击趋势波动略有起伏，下半年攻击急剧增多，11 月短暂回落后，在年底（12 月）达到峰值。



从勒索病毒类型来看，2024 年较为活跃的勒索病毒家族是 Mallox、Makop、Phobos 和 BejingCrypt 四大家族。其中，个人终端遭遇的勒索病毒主要来自于 Mallox、Makop 和 Phobos 这三个家族；企业终端遭遇的勒索病毒主要源于 Mallox、BejingCrypt、Makop 和 Phobos 这四个家族。



相较于 2023 年，2024 年勒索病毒的整体攻击趋势虽有所缓和，但这并不意味着可以放松对勒索攻击的警惕，国内勒索软件攻击态势依旧严峻。近两年数据显示，勒索攻击目标主要集中在制造业、IT 互联网行业和医疗保健行业。这三大行业与大众生产、生活密切相关，拥有大规模的个人数据和商业信息，一旦某个环节出现安全风险，便很容易引发蝴蝶效应，造成严重影响。



勒索攻击防护建议

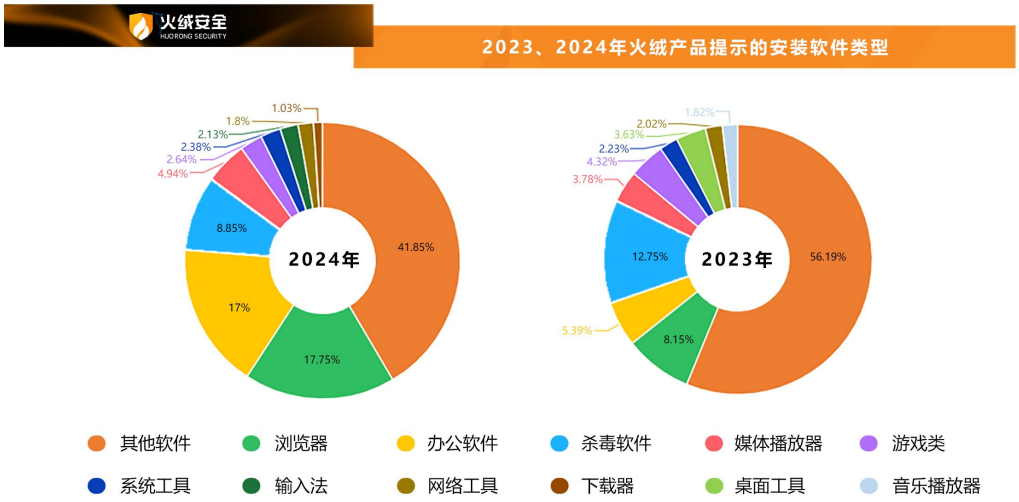
- 使用能够检测和阻止已知勒索软件变体的反恶意软件或安全软件。
- 实时监测和检测网络活动，及时发现和应对异常行为，以遏制勒索软件攻击的扩散。
- 定期进行安全审计和评估，以识别网络和系统漏洞，并确保所有安全控制措施到位并正常运行。
- 对员工定期开展网络安全培训，加强员工的网络安全意识，包括识别和应对勒索软件等网络威胁。
- 定期对重要文件和数据进行非本地备份，并设置访问限制，以降低勒索软件造成的影响。

软件捆绑安装现象频发

软件捆绑安装问题现已成为多年来普遍存在的一种现象，稍不留神就会下载到的无用软件让用户不胜其烦。这些捆绑软件往往会进行频繁弹窗、恶意篡改网页、占用系统内存等操作，造成系统卡顿、内存不足等问题，甚至会携带恶意代码或病毒，严重威胁终端安全，使用户面临个人隐私和财产信息等泄露风险。

针对这一现象，火绒安全产品能够对曾经被捆绑安装的软件进行识别。此外，2024 年火绒个人版产品迭代升级后，还新增了对潜在不受欢迎软件进行监控的功能。一旦检测识别到可能存在威胁的软件，火绒产品就会及时提醒用户，帮助用户有效规避在不知情状况下被安装不必要软件的潜在风险。

2024 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。相较于 2023 年，对浏览器与办公软件的提示比例大幅增加。

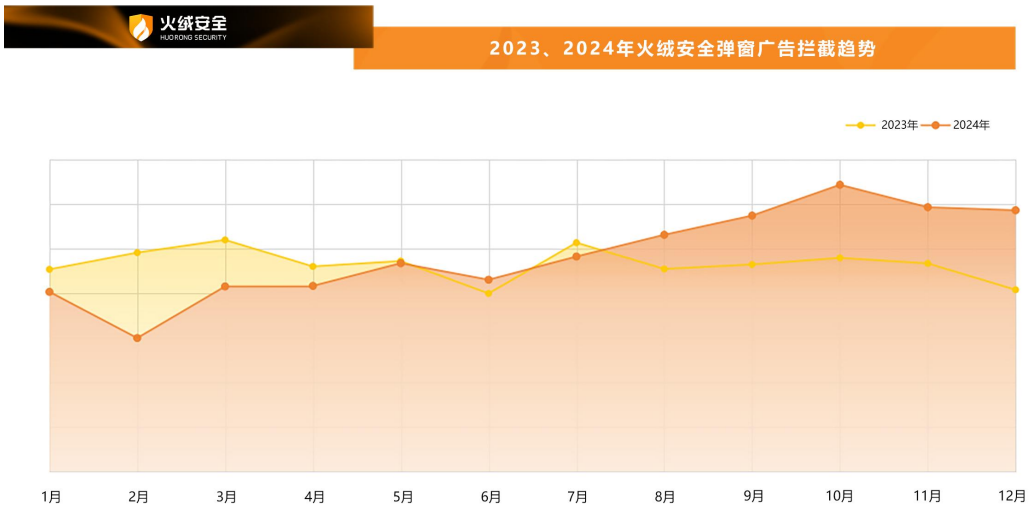


弹窗广告再度反弹

自计算机和互联网普及以来，弹窗广告成为公众在网络生活中难以避免的“顽疾”。作为一种新兴的广告推广形式，弹窗广告为商家开辟新的营销渠道的同时，也为用户提供了多元化的产品与服务信息。

然而，随着时间的推移，弹窗广告逐渐变得无孔不入。无论是工作所用的办公软件，还是休闲娱乐所浏览的各类网站、应用，弹窗广告总会不合时宜地突然弹出。广告内容也变得良莠不齐，除了正常的推广信息之外，大多充斥着大量低俗、虚假甚至恶意推广的信息，不仅严重干扰公众正常上网，甚至还对终端安全和数据安全造成严重威胁。

“火绒威胁情报系统”数据显示，2024 年火绒安全产品共拦截（不含用户手动拦截）11.66 亿次弹窗广告，相较于 2023 年小幅增长。全年拦截量呈波动上升趋势：1-5 月相对稳定，6 月起波动加剧，7-10 月大幅攀升至峰值，年末逐渐回落，整体走势起伏显著。

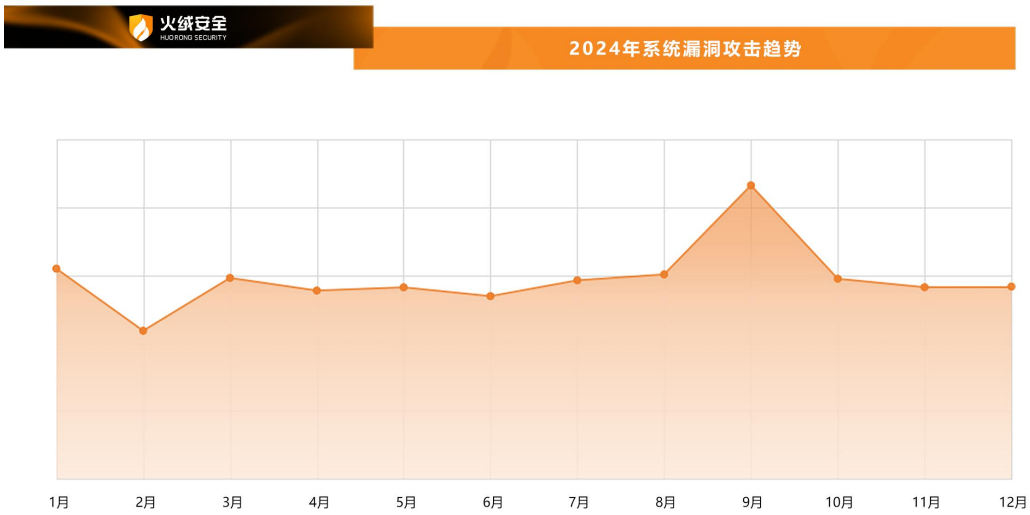


漏洞攻击

2024 年火绒安全产品共拦截 1.9 亿次漏洞攻击，其中拦截 1.77 亿次微软系统漏洞攻击，拦截 1317 万次 Web 漏洞攻击。

▶ 系统漏洞持续威胁，潜在威胁不容忽视

根据“火绒威胁情报系统”监测数据显示，2024 年针对系统漏洞的攻击呈现波动趋势，攻击量在不同时间段内有所起伏。尽管部分漏洞在补丁发布后得到缓解，但系统漏洞的潜在危害依然巨大，尤其是未及时修复的漏洞可能成为攻击者长期利用的目标。系统漏洞不仅为攻击者提供了直接入侵的通道，还可能被用于横向渗透，进一步扩大攻击范围。



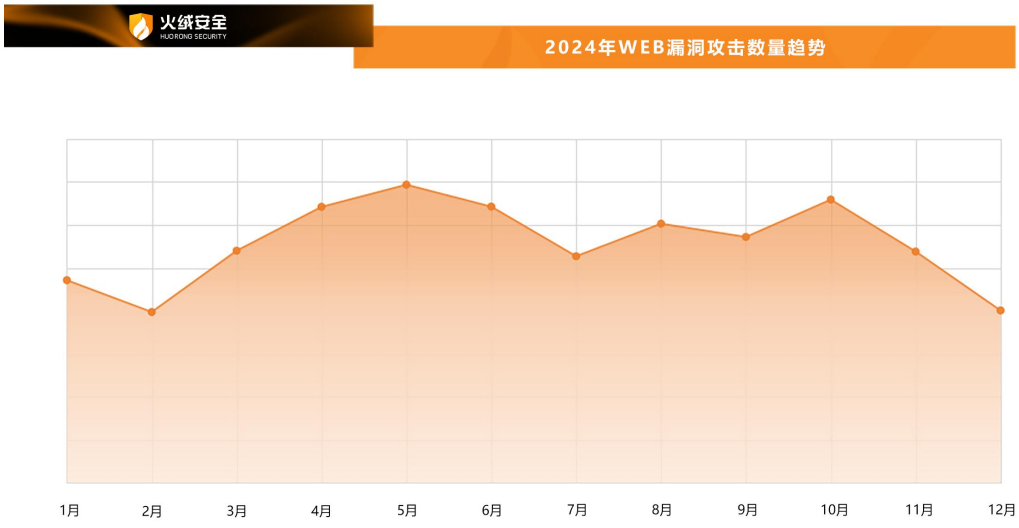
2024 年微软对外披露了 3618 个漏洞，包含高危漏洞 76 个，严重漏洞 983 个。其中，远程执行代码漏洞数量与 2023 年相同仍居于首位，而安全功能绕过漏洞和信息泄露漏洞较 2023 年明显增长。这些漏洞会给用户带来严重的安全风险，一旦被成功利用，将会严重威胁用户的数据安全和隐私。

- **远程执行代码漏洞**一旦被成功利用后，攻击者能够对目标计算机进行远程控制、系统破坏和窃取机密等任意操作。

- **安全绕过功能漏洞**一旦被成功利用后，攻击者能够绕过系统中的安全机制，实现对目标计算机的非法访问或操作。
- **信息泄露漏洞**一旦被成功利用后，攻击者能够从目标计算机获取用户敏感信息。

▶ Web 漏洞攻击呈波动趋势，企业安全压力不减

根据“火绒威胁情报系统”监测数据显示，2024 年针对 Web 服务漏洞的攻击呈现波动趋势，攻击量时有上升，时有下降。尽管如此，Web 服务漏洞与黑客渗透攻击之间的高度关联性依然显著，使其成为攻击者入侵企业网络的重要突破口之一。攻击量的起伏变化反映了攻击者在策略和技术上的不断调整，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。



▶ 2024 年度漏洞 TOP3

2024 年度漏洞 TOP3 均为远程执行代码漏洞，分别是 CVE-2024-38063、CVE-2024-38077、CVE-2024-43639。

- CVE-2024-38063

此漏洞为影响 Windows 系统 IPv6 协议栈的高危漏洞，攻击者可通过发送特制的 IPv6 数据包触发整数下溢，导致远程代码执行（RCE）或系统崩溃（蓝屏），火绒曾对此漏洞进行单独发稿警示。

- CVE-2024-38077

此漏洞为影响 Windows 远程桌面授权服务（RDL）的高危远程代码执行（RCE）漏洞，收录于火绒月度漏洞通告。该漏洞允许攻击者在无需交互的情况下，通过发送处理特制的 RPC 数据包触发。多家网安平台亦对此漏洞进行警示。

- CVE-2024-43639

此漏洞为影响 Windows Kerberos 身份验证协议的高危远程代码执行（RCE）漏洞，收录于火绒月度漏洞通告，多家网安平台对此漏洞进行预警。攻击者可通过发送特制的 Kerberos 请求，无需身份验证即可在目标系统上执行任意代码，完全控制系统。

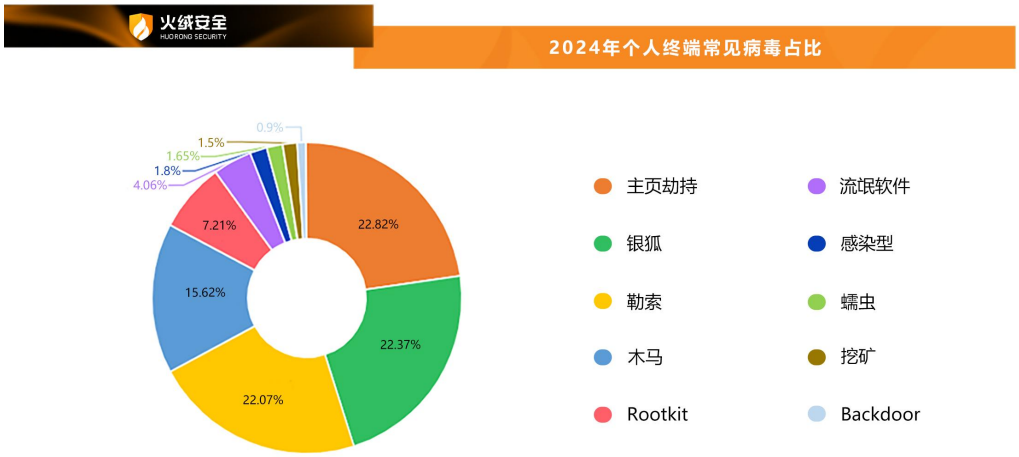
终端应急服务与安全防护建议

在数字化时代，网络攻击手段随着信息技术的蓬勃发展日益复杂化。而终端设备作为公众生活和工作中不可或缺的工具，面临的安全问题愈发严峻。从层出不穷的恶意软件到防不胜防的网络攻击，终端设备随时可能遭受威胁，导致个人隐私和企业数据面临泄漏风险。火绒安全依托自主研发的反病毒引擎，构建起多层次主动防御系统和火绒威胁情报系统，能够有效拦截各类病毒攻击，针对操作系统的脆弱点进行防护，并实现对终端威胁的精准处理与动态防御，为用户的终端安全提供全方位保障。

▶ 个人终端应急服务

个人终端设备中通常会存储着个人隐私数据、财务信息、社交记录等重要内容。一旦终端安全防线被突破，个人隐私泄露、财产受损等问题接踵而至，严重影响个人生活与财产安全。

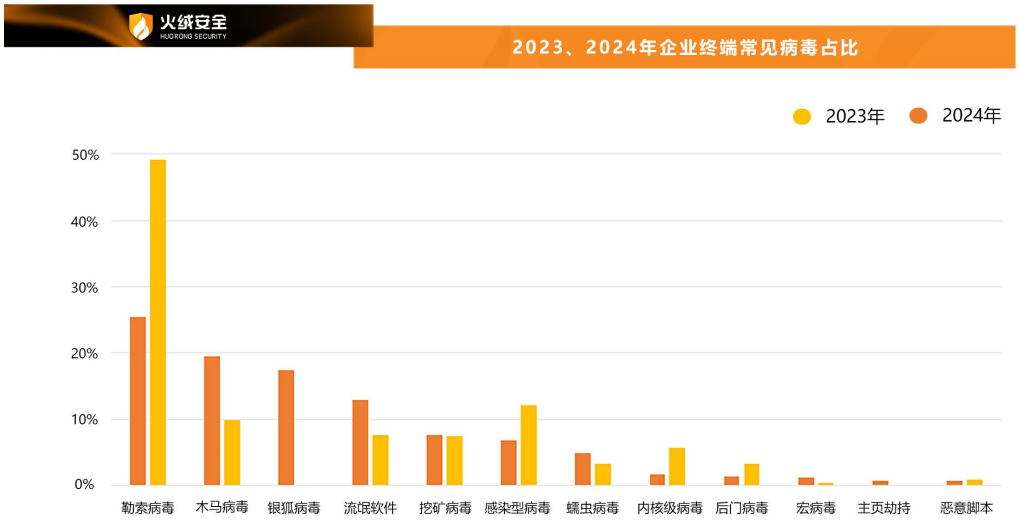
根据“火绒在线支持和响应中心”处理的个人终端问题显示，个人终端常见病毒中，主页劫持病毒占 22.8%、银狐病毒占 22.4%、勒索病毒占 13%。主页劫持病毒成为困扰用户的头号病毒威胁，其主要被用于劫持用户浏览器，且绝大部分主页劫持问题是由传奇私服引发的。火绒安全 2024 年发布的病毒报告，揭示了恶意软件伪装成 Chrome 浏览器在线安装包，劫持用户浏览器主页到指定网站，并通过篡改浏览器配置文件进行网页推广与数据收集等恶意活动。



▶ 企业终端应急服务

终端设备作为业务运营的关键枢纽，存储着大量商业机密、客户资料以及核心业务数据。企业终端安全若出现漏洞，不仅可能导致业务中断，造成直接经济损失，更会损害企业声誉，影响企业发展与市场竞争力。

近两年数据显示，勒索攻击、木马病毒和银狐病毒一举成为企业安全主要威胁来源。其中，勒索攻击对企业造成的威胁呈现明显缓和，木马病毒的威胁大幅增长对企业安全造成威胁。银狐病毒异军突起，成为 2024 年占据企业威胁的 TOP3 病毒。2024 年火绒安全发布的病毒报告中，四度揭示了银狐病毒不断更新迭代，监测并对抗安全防护工具，并通过加载后门模块实现远程控制进行信息窃密的行为，体现了银狐病毒家族的高活跃性、高隐蔽性以及高破坏性。

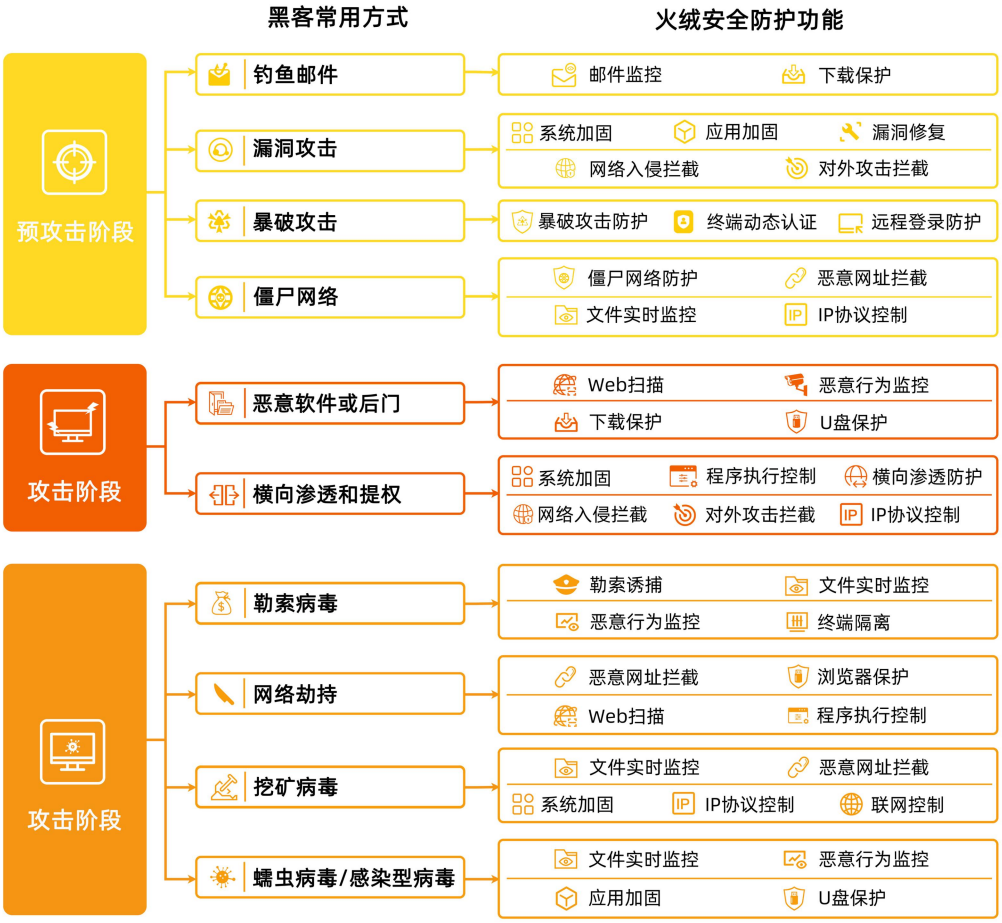


火绒安全团队通过对病毒的各种攻击方式分析发现，黑客会在攻击前期，对目标企业进行探测，以期找到企业系统中的弱点，随后利用各种手段入侵目标系统或局域网，成功入侵系统后，会为其后续的攻击和窃取潜在利益做准备。

▶ 安全防护建议

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、漏洞和技术等破坏网络系统，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，以下为可提高系统和数据的安全性的常见措施。

预防黑客攻击常见基本措施

- **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。
- **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。
- **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。
- **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。
- **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。

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

火绒安全公众号