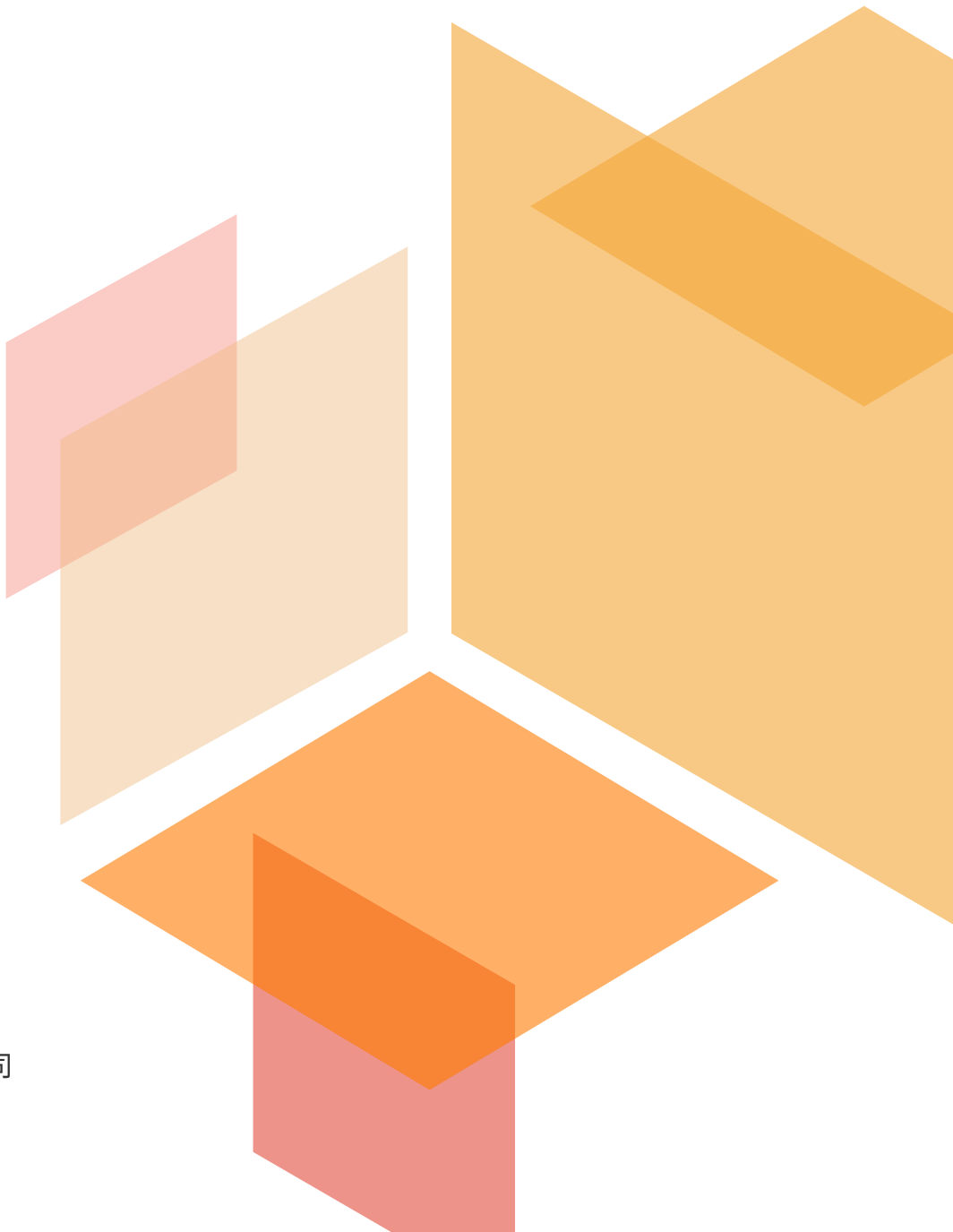
火绒安全
HUORONG SECURITY

2022 火绒安全 终端安全洞察报告

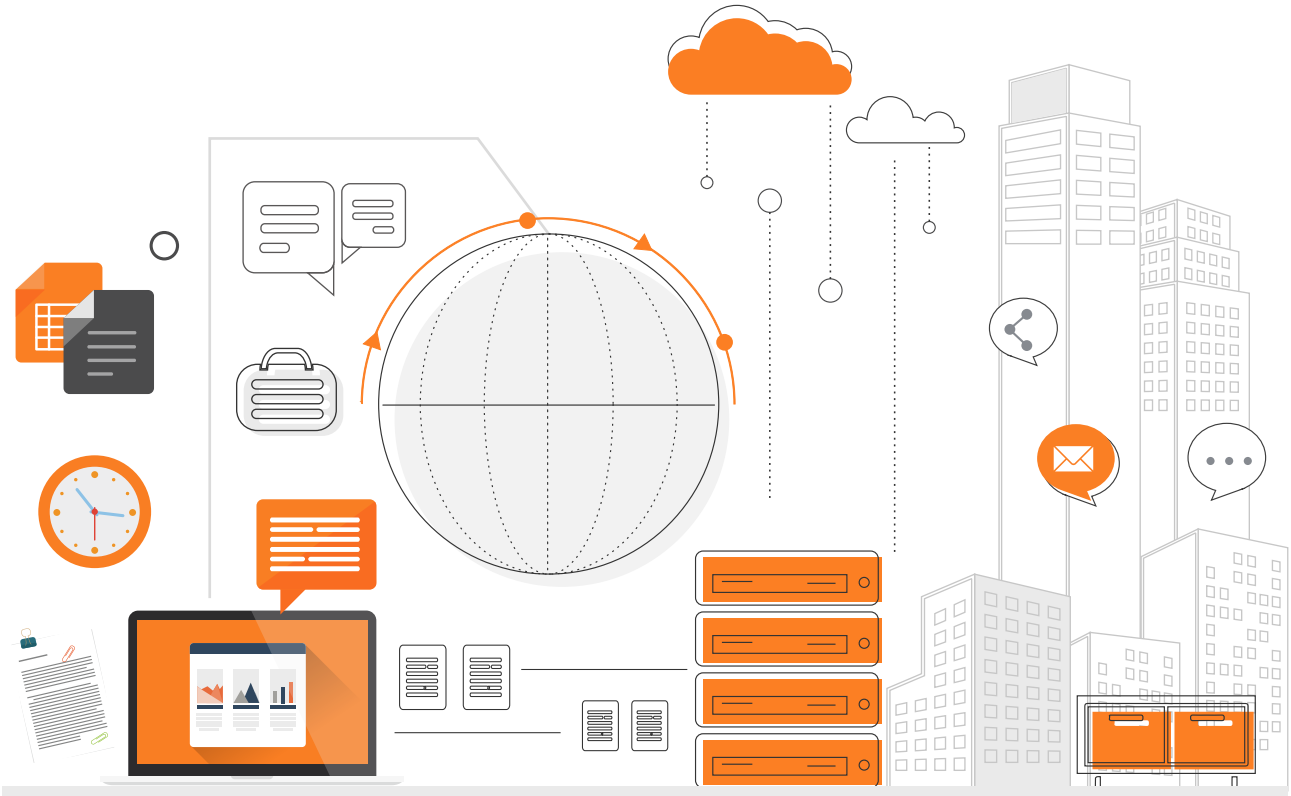


北京火绒网络科技有限公司

前言

《火绒安全 2022 年终端安全洞察报告》由火绒安全实验室、火绒在线支持响应中心联合撰写。统计数据展现了2022 年新政策新形势下的病毒攻击趋势、个人终端乱象变化、企业终端威胁现状。

报告以真实、全面、及时的数千万“火绒安全软件”终端为情报基石，以专业、严谨、可靠的“火绒威胁情报系统”为信息中枢，汇聚了火绒安全反病毒专家的行业洞察和威胁响应团队的实践经验，真实地反映了当前国内终端安全最新状况及变化趋势。



关键数据

39.9 亿

2022 年，火绒安全拦截终端攻击 39.9 亿次，小幅增长于 2021 年。

50 %

火绒安全产品共拦截（不含手动拦截）23.03 亿次弹窗广告，弹窗总量较 2021 年明显下降近 50%。

1476 %

从 2018 年至今，Win64 位病毒样本数量提高了 1476%，且依然在加速增长。这与 64 位操作系统市场占有率的扩大，以及 Win32 病毒与安全软件的对抗愈发复杂有关。

60 %

内核级病毒（Rootkit）远超流氓软件、勒索病毒、木马病毒，成为个人终端最常见病毒。其中，60% 的内核级病毒被应用于锁定用户浏览器首页。

3.03 亿

据“火绒威胁情报系统”监测，2022 年火绒安全产品共拦截 3.03 亿次漏洞攻击。

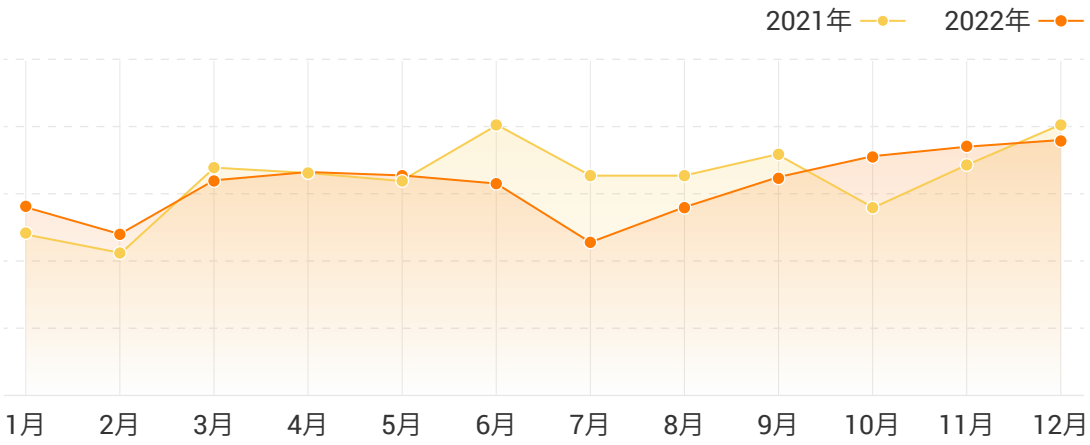
200 万+

火绒安全拦截 200 余万次勒索病毒攻击。勒索事件的增长，与勒索软件即服务（RaaS）体系的成熟运作有关。

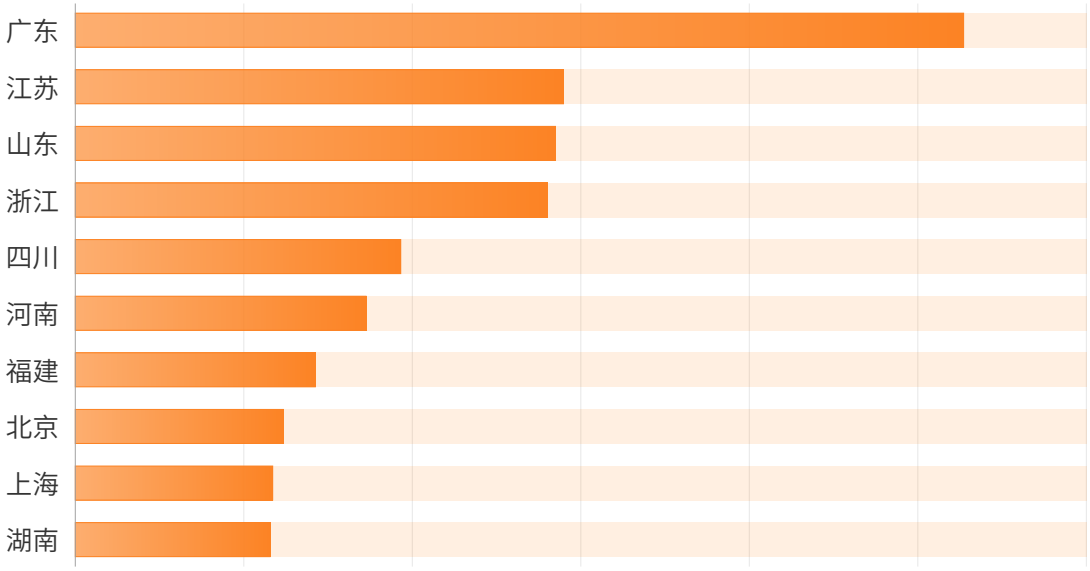
目录 CONTENTS

终端攻击趋势

根据“火绒威胁情报系统”的监测和评估，2022 年火绒安全拦截终端攻击 39.9 亿次，小幅增长于 2021 年（39.2 亿次）[1]，全年终端攻击趋势仅在 2 月和 7 月短暂下降。从全国省份分布看，广东、江苏、山东、浙江、四川、河南、福建、北京、上海、湖南成为恶意攻击的主要地区。



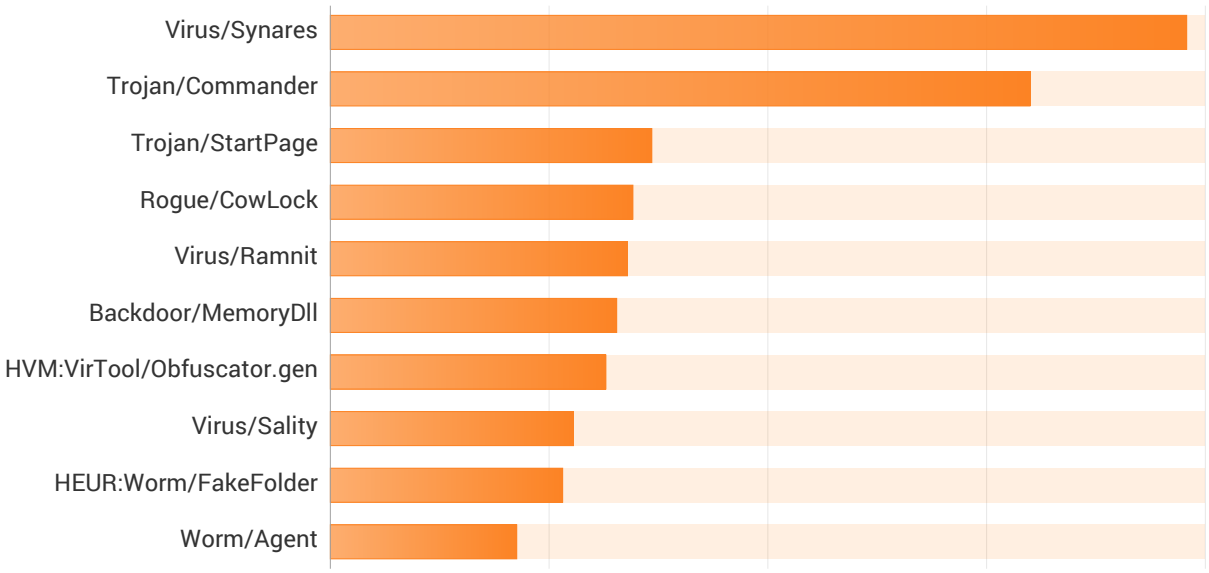
2021、2022 年火绒安全威胁情报趋势



2022 年国内遭受恶意攻击的省份 TOP10

[1] 注：为体现更全面的威胁趋势，2022 年扩增“终端攻击”数据统计维度，2021 年数据与《火绒安全 2021 终端安全情报年鉴》存在差异。

经统计，攻击终端的恶意程序主要来自感染型病毒（Virus）、木马病毒（Trojan）、流氓软件（Rogue）、后门病毒（Backdoor）、代码混淆器（VirTool）、蠕虫病毒（Worm）等。



2022 年攻击终端 TOP10 病毒家族

攻击终端的主要恶意程序

流氓软件换“新装”

2022年央视3·15晚会曝光下载站捆绑安装、强制弹出、诱导下载乱象后，流氓软件赖以生存的环境得到集中整治。流氓软件为了继续推广，转而换上了一套“新装”，即伪造正常软件的官网，并利用该软件“关键词”投放搜索引擎广告，诱导用户点击下载。

例如一款流氓软件（下图）伪造了“钉钉”官网，该链接在搜索引擎中排在第一位，用户搜索“钉钉”时一旦点击进入，触击页面任意区域都会下载安装此款流氓软件。

伪造的官网

搜索结果

此外，一些流氓软件的推广过程中，存在较为明显的对抗安全软件痕迹，如对多款安全软件进行检测规避，甚至利用系统程序隐匿推广行为（注入 explorer 进程）。

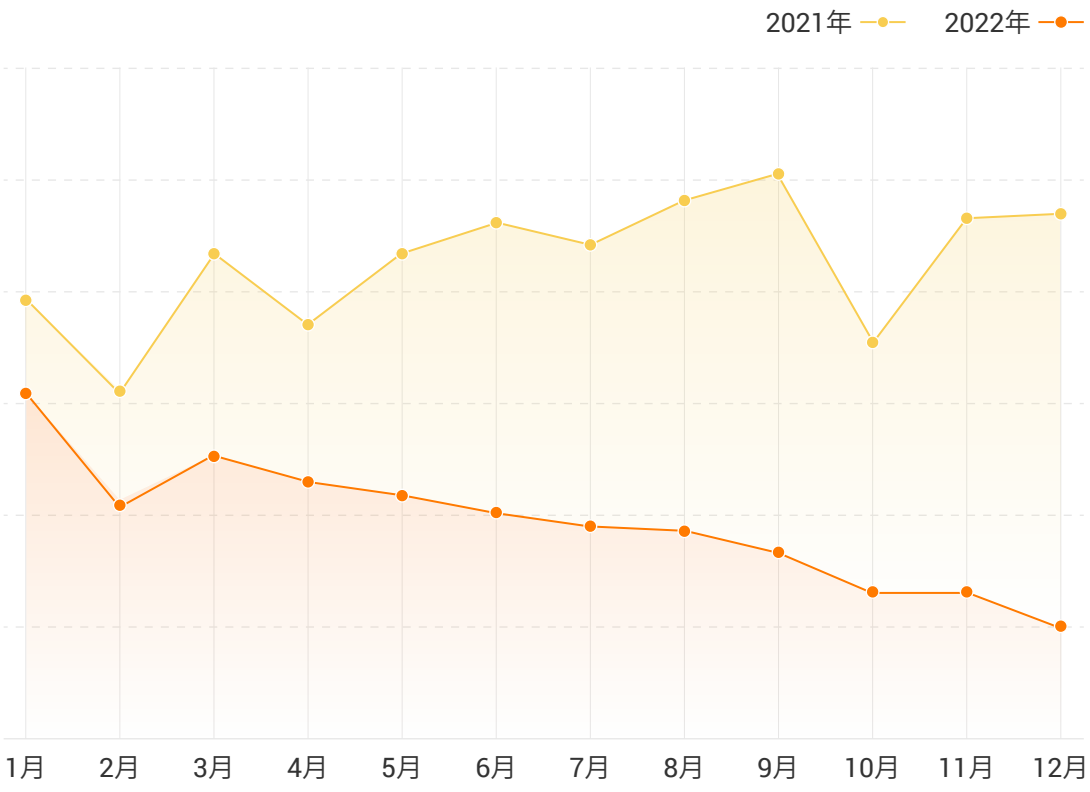
弹窗乱象大幅减少

根据“火绒威胁情报系统”数据显示，2022 年火绒安全产品共拦截（不含用户手动拦截）23.03 亿次弹窗广告，大幅度少于去年（45 亿次），且全年明显呈下降趋势。“618”、“双 11”等购物节期间也未出现爆发状态。

数据表明，国家互联网信息办公室发布的《互联网弹窗信息推送服务管理规定》从意见征集到正式实施，效果显著地遏制了互联网弹窗乱象，在规范广告推送、防止流量劫持、个人信息保护等方面有力保障了用户权益。

弹窗广告拦截

23.03 亿次



2021、2022 年火绒安全弹窗广告拦截趋势

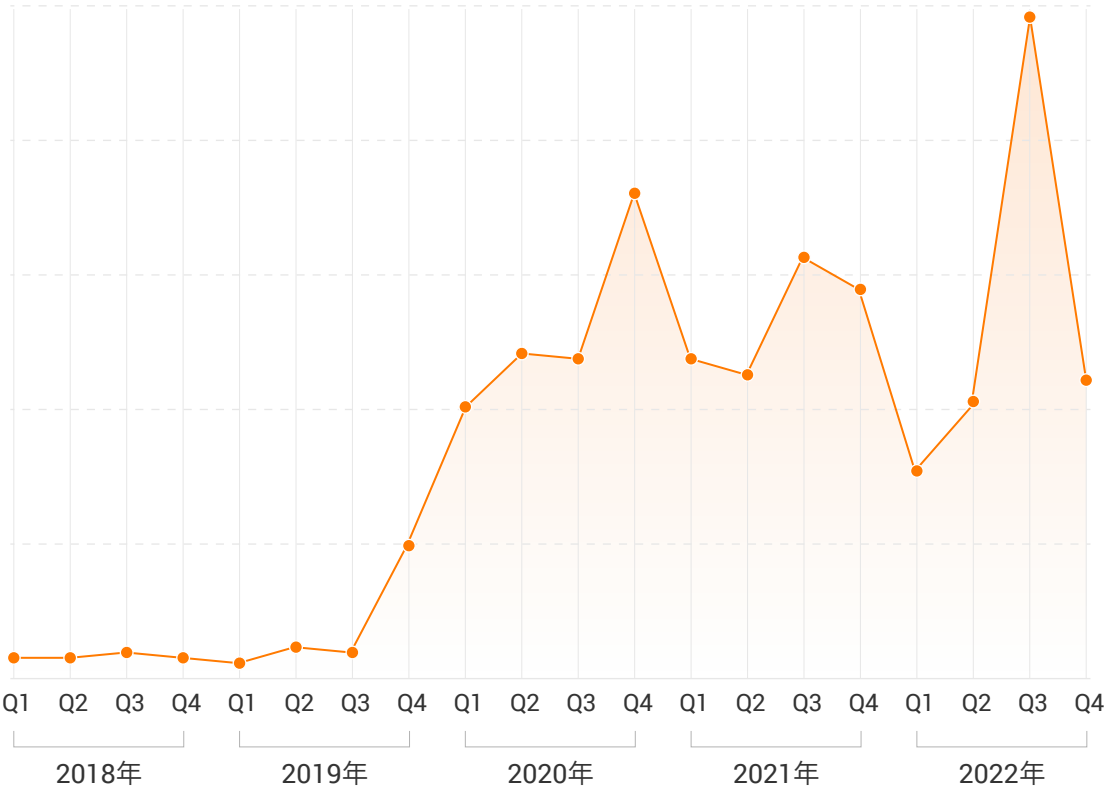
Win64位病毒翻倍涌现

近几年 Win64 位病毒样本数量增长明显，从 2018 年至今，Win64 位病毒样本数量增长了 1476%，且速度明显加快。主流病毒家族如 Emotet、IcedID、Dridex 均出现大量 64 位新变种。

由于 Win32 病毒样本与安全软件对抗的复杂度逐渐增高，以及近年来 64 位操作系统市场占有率的扩大增长，致使病毒作者开始尝试转向开发基于 Win64 的恶意代码及病毒混淆器来对抗安全厂商的查杀。

Win64 位病毒样本数量增长

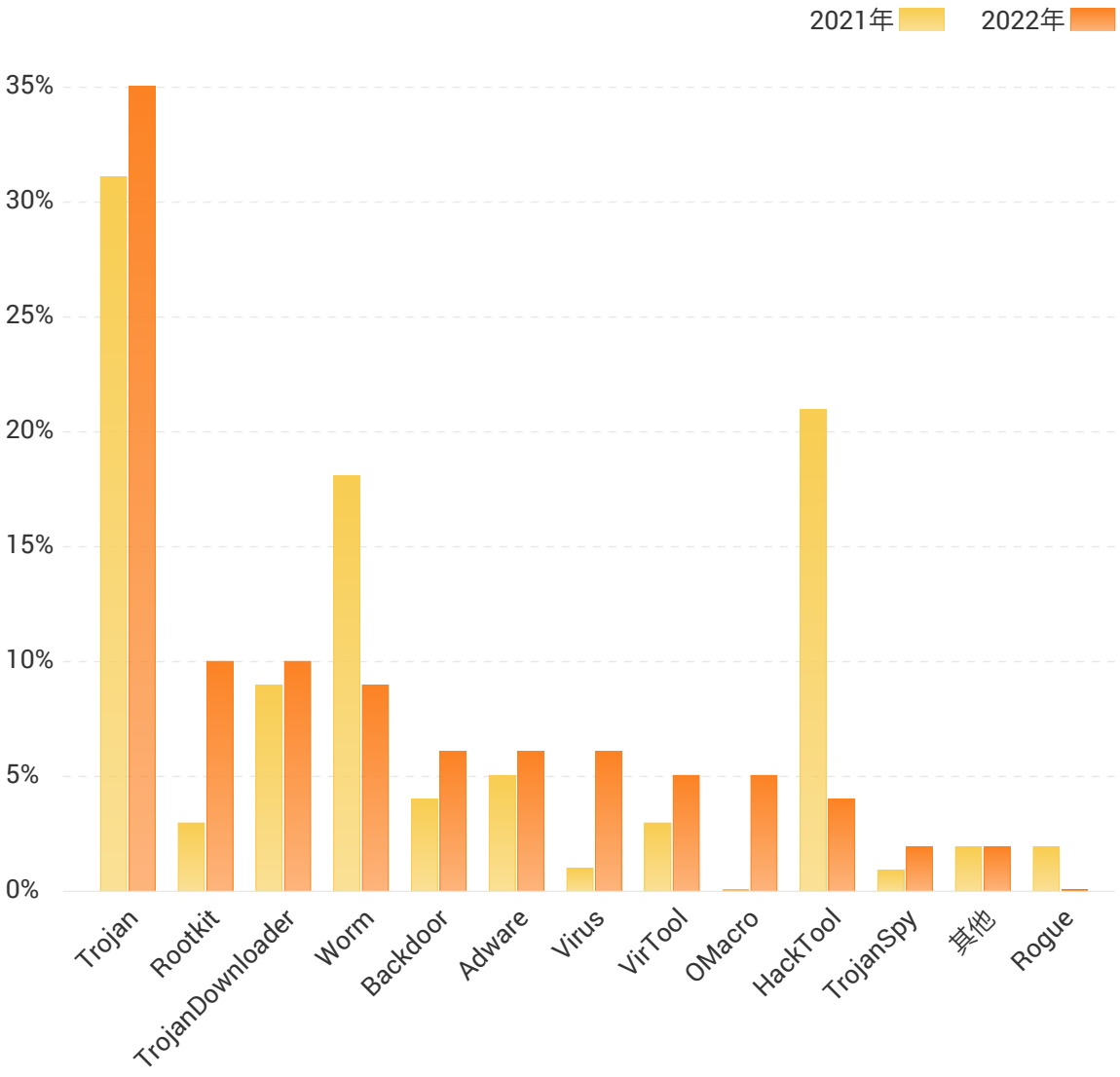
1476%



2018 至 2022 年 64 位病毒样本增长趋势

内核级病毒正当道

在黑客投向全网的主要病毒中，内核级病毒（Rootkit）数量增长明显，宏病毒卷土重来。2022 年 Rootkit 一跃成为第二大黑客攻击手段，该病毒进入内核模块后能获取到操作系统高级权限，通过隐藏其他病毒进程、注册表、文件相关操作等方式与安全软件进行对抗。另外，借助宏进行传播的病毒（如：Emotet、IcedID 等）在 2022 年增多，导致整体宏病毒数量上涨。



2021、2022 年火绒安全截获病毒样本类型占比

其中，内核级病毒成为个人终端最常见病毒，且主要被应用于流量劫持。流量劫持具体表现为：记录用户访问的流量、劫持浏览器首页（锁首）、劫持用户访问内容（如：劫持推广计费号、篡改网页内容等）。中了此类病毒的终端还可能被下发其他的恶意模块如：代理模块、后门模块等恶意模块。

2022 年个人终端常见病毒占比

个人终端遭遇锁首来源占比

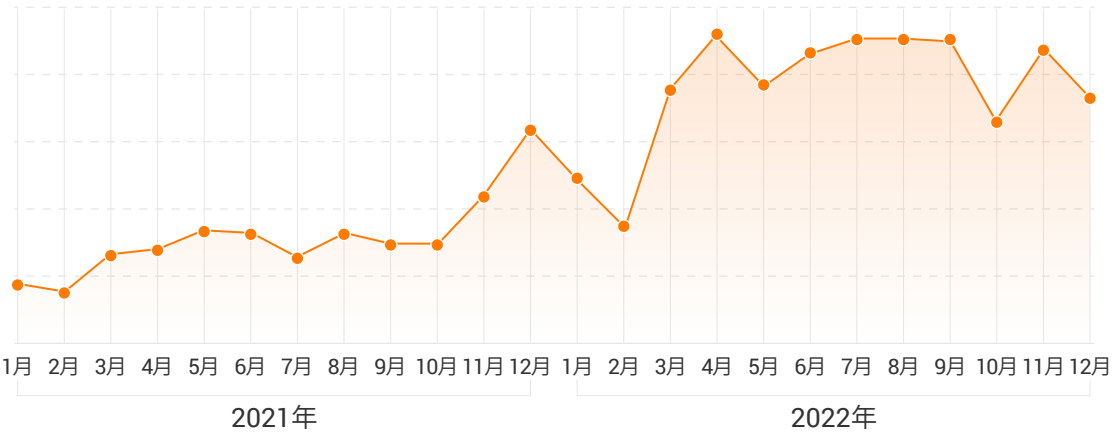
值得关注的是，主要造成锁首问题的内核级病毒，大多数（超 50%）由传奇私服登录器携带传播。例如，7 月份火绒安全截获的 Rootkit 病毒新变种利用传奇私服进行传播。当用户访问传奇相关网页时，会被劫持到病毒作者预设的劫持网页，且该 Rootkit 病毒会通过文件自保对抗安全软件查杀，并将系统版本和计算机名等终端信息上传到病毒服务器。

漏洞攻击特征

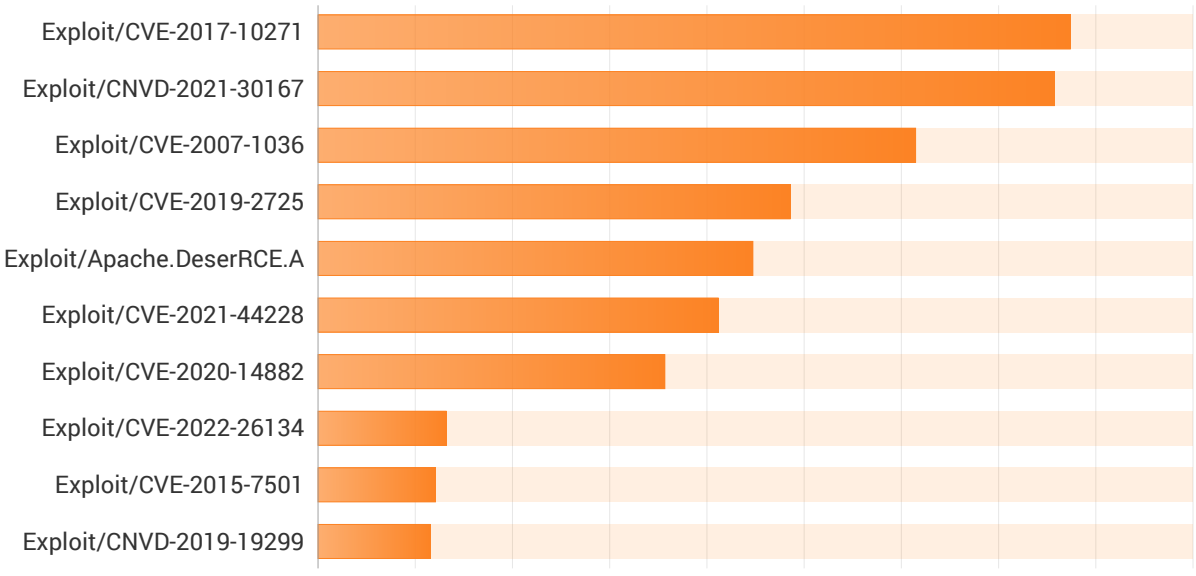
2022 年，火绒安全产品共拦截 3.03 亿次漏洞攻击。Web 漏洞攻击中最易被利用的漏洞依次为 CVE-2017-10271、CNVD-2021-30167、CVE-2007-1036。微软系统漏洞中，特权提升漏洞、远程执行代码漏洞占比较高。

Web漏洞攻击

根据“火绒威胁情报系统”监测，2022 年针对用户 Web 漏洞攻击整体呈现大幅上升趋势。2021 年末 Log4j2 安全漏洞（CVE-2021-44228）大爆发，2022 年利用其攻击的事件随之显现，进一步印证了其影响范围广和危害程度大的特点，未来会继续被黑客利用。



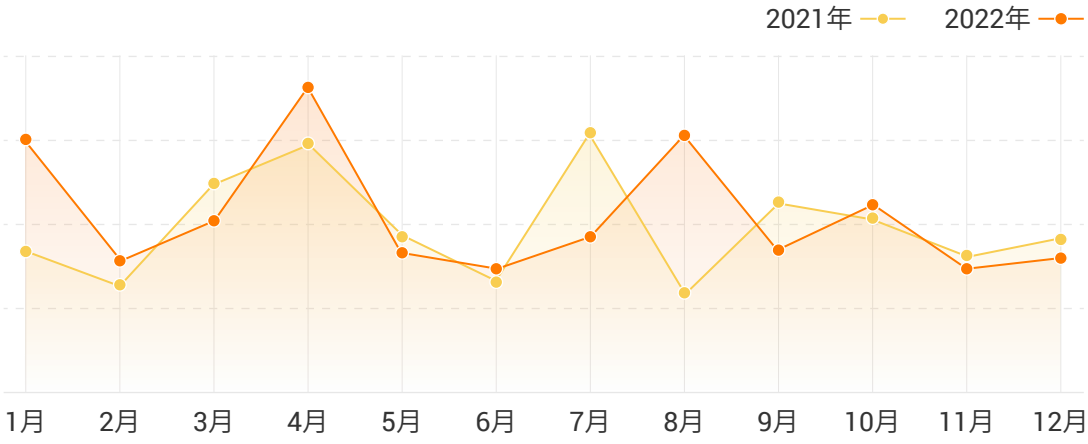
2021、2022 年 Web 漏洞攻击趋势



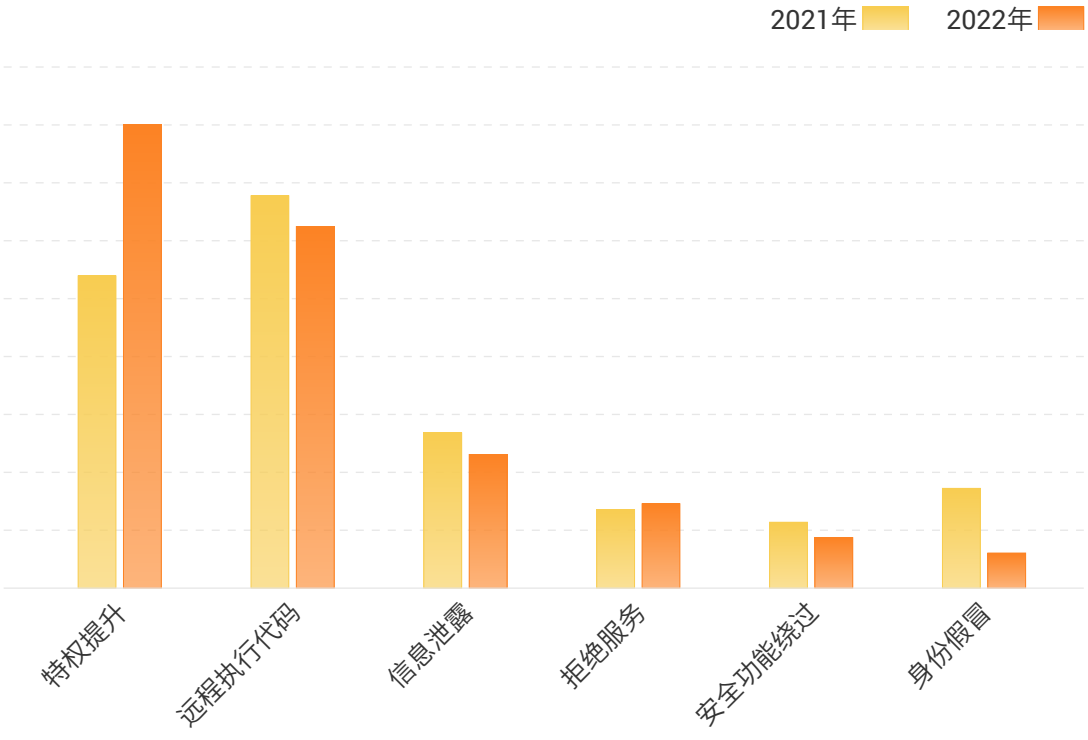
2022 年被利用的 Web 漏洞 TOP10

微软系统漏洞

2022 年，微软对外披露 1263 个漏洞，其中高危漏洞 88 个，严重漏洞 864 个。特权提升漏洞、远程执行代码漏洞依然是最多的微软漏洞类型。特权提升漏洞达 400 个，比去年增加了 33.5%，攻击者通过特权提升漏洞能够获取系统管理员权限，从而执行任意代码。远程执行代码漏洞，由于可以直接执行恶意代码，比特权提升漏洞危害更高，对用户影响较为严重。



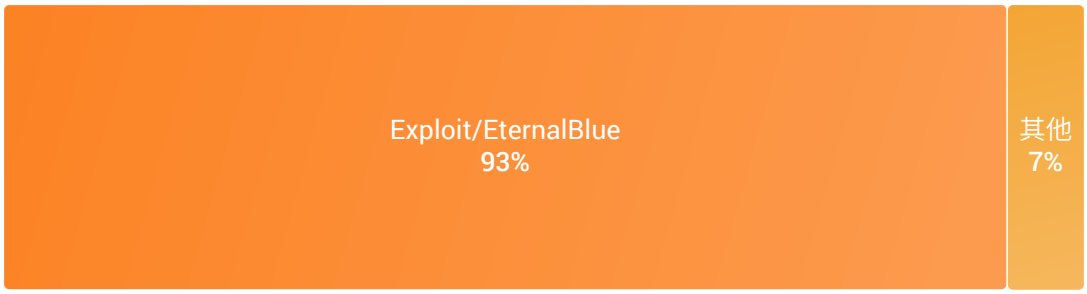
2021、2022 年微软漏洞数量情况



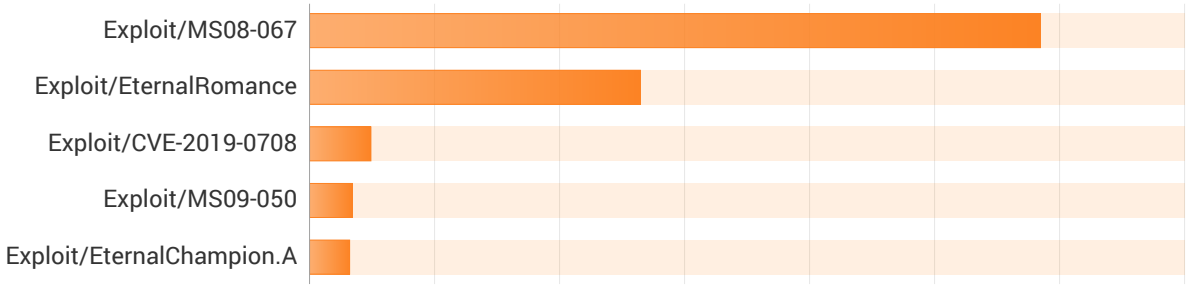
2021、2022 年微软系统漏洞类型

2022 年火绒产品拦截的系统漏洞攻击中，最易被利用的系统漏洞依次是 EternalBlue（永恒之蓝）、MS08-067 和 EternalRomance（永恒浪漫）。“永恒之蓝”仍旧是近几年被利用最多的系统漏洞。

此外，其他旧漏洞威胁依然值得警惕。虽然旧漏洞的发布时间较早，但由于外界存在很多针对其特定开发的漏洞利用代码或工具，旧漏洞利用起来反而更“简单易用”。部分终端长时间存在未修复的旧漏洞，也为黑客提供了可乘之机。



2022 年拦截系统漏洞攻击中“永恒之蓝”占比



2022 年拦截系统漏洞攻击 TOP5（不计算“永恒之蓝”）

年度高危漏洞

Follina（CVE-2022-30190）

CVE-2022-30190 是微软 Windows 支持诊断工具（MSDT）中的一个远程代码执行漏洞。它允许远程攻击者在目标系统上执行任意 shell 命令。

Spring4Shell（CVE-2022-22965）

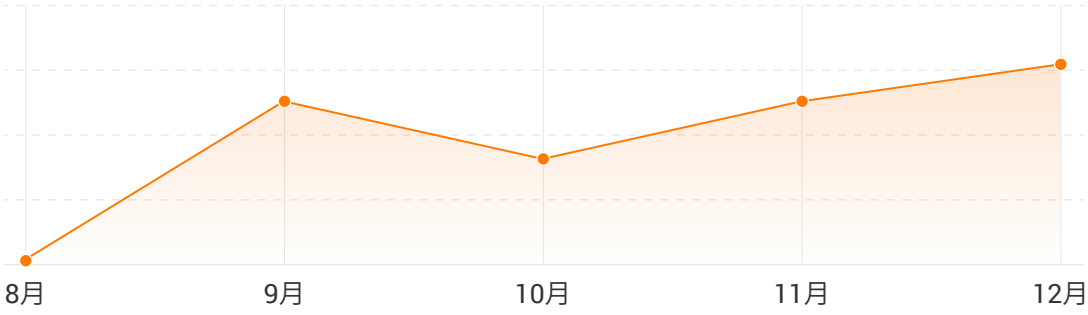
CVE-2022-22965 是 VMware 开源 Java 框架 Spring Framework 中的远程代码执行漏洞。一旦攻击者实现远程代码执行，就可以安装恶意软件，或者利用受影响的服务器作为初始立足点，提升权限进而攻击整个系统。

F5 BIG-IP（CVE-2022-1388）

CVE-2022-1388 于 2022 年 5 月首次被披露，是一个值得关注的严重漏洞。该漏洞影响 F5 BIG-IP 软硬件套件中的 BIG-IP iControl REST 身份验证组件；一旦被利用，允许未经身份验证的攻击者以“root”权限在 BIG-IP 网络设备上执行命令。

畅捷通 T+ 漏洞

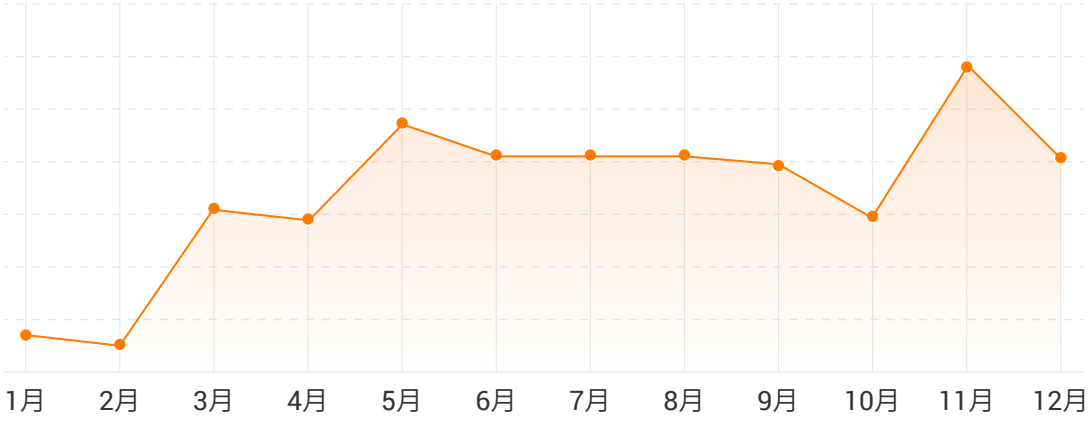
畅捷通 T+ 作为流行的企业管理软件，在 2022 年 8 月出现任意文件上传漏洞（CNVD-2022-60632）。未经身份认证的攻击者可利用漏洞远程上传任意文件，获取服务器控制权限。“火绒威胁情报系统”拦截到 CNVD-2022-60632 漏洞的攻击趋势如下图所示：



2022 年 CNVD-2022-60632 漏洞攻击趋势

Log4j2 漏洞（CVE-2021-44228）

CVE-2021-44228 是 Apache Log4j2 开源日志实用程序中的远程代码执行漏洞，在 2021 年底被揭露。Apache Log4j2 被世界各企业和组织应用于业务系统开发，因此该漏洞影响极大。由于漏洞具有普遍性和易利用性特点，依然是 2022 年黑客最喜欢利用的一项漏洞。

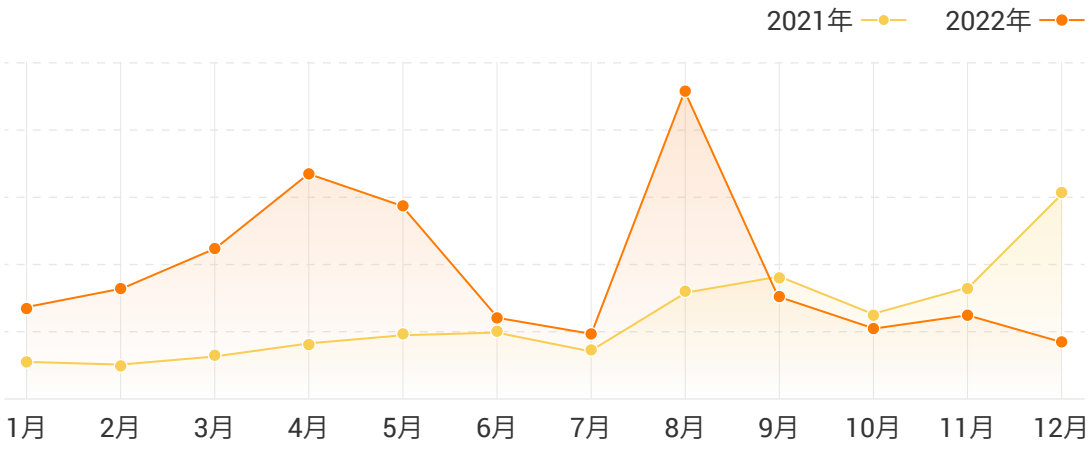


2022 年 Log4j2 漏洞攻击趋势

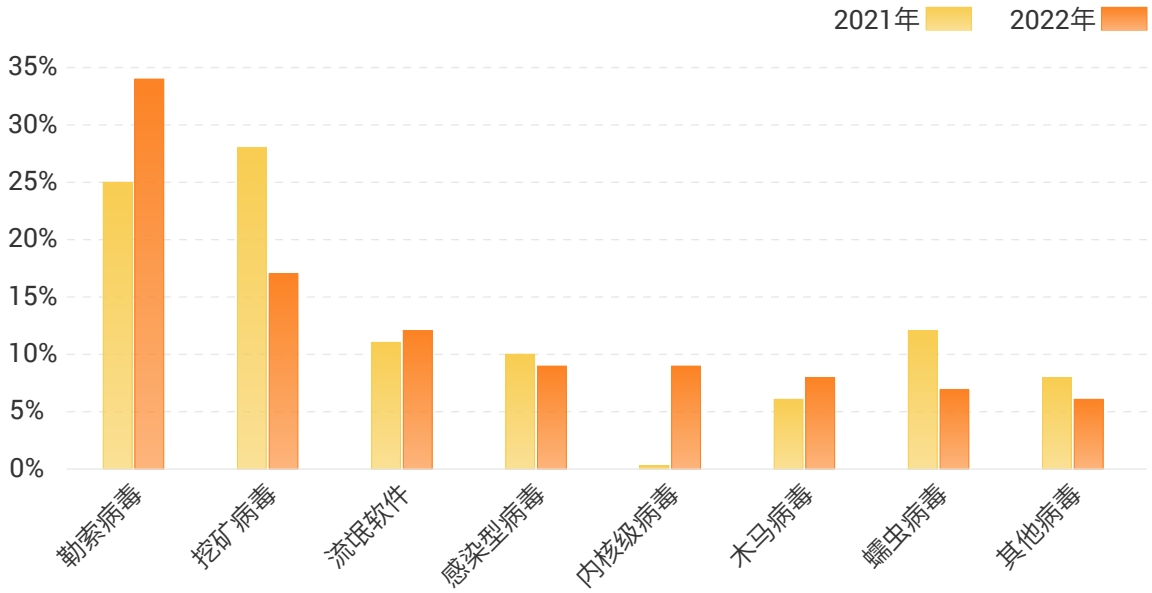
勒索病毒成为首要威胁

勒索病毒攻击情况

随着勒索病毒影响力和破坏力的不断增长，勒索软件即服务（RaaS）的成熟运作，勒索病毒俨然成为当今网络安全最具威胁的病毒存在。2022 年火绒安全拦截 200 余万次勒索病毒攻击。



2021、2022 年火绒安全拦截勒索病毒攻击趋势

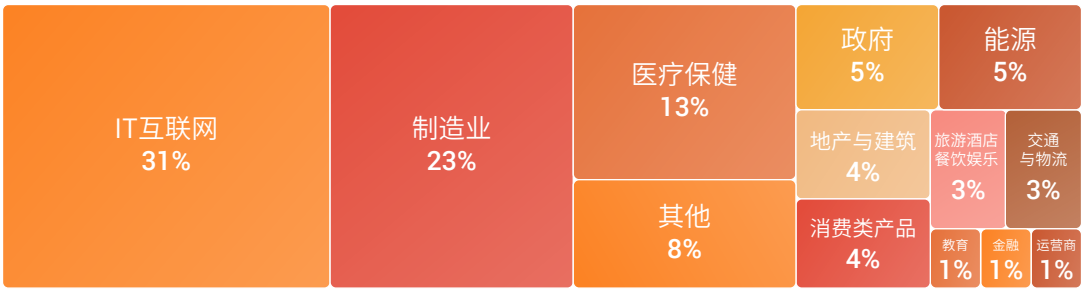


2021、2022 年火绒安全企业终端常见病毒占比

根据“火绒威胁情报系统”和“火绒在线支持响应中心”统计，2022 年火绒安全处理全网的勒索事件呈现以下规律：

- 从行业来看，IT 互联网、制造业、医疗业最易遭受勒索病毒攻击，三者占据 67%；

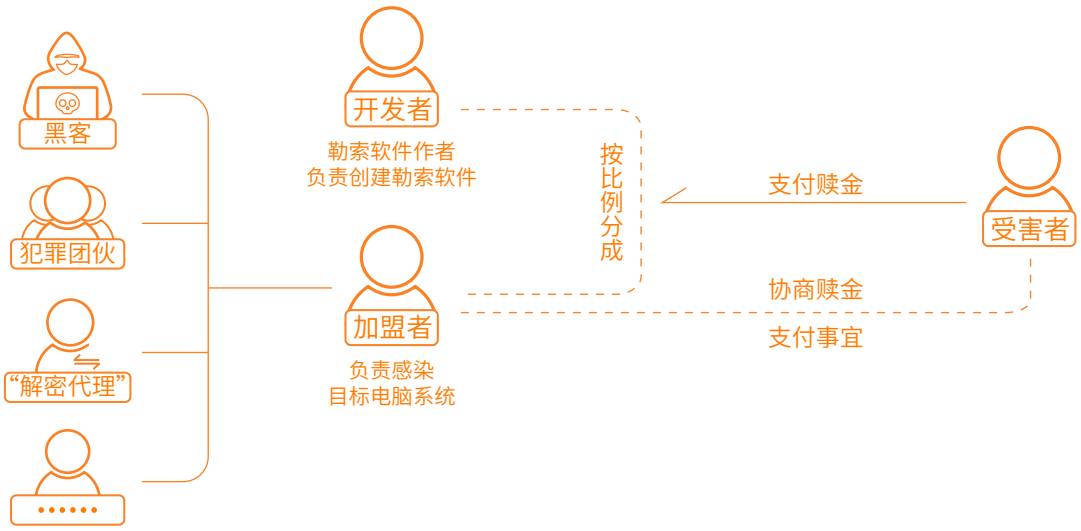
- 从企业规模看，作为我国经济中坚力量的中小企业更易“中招”，围绕网络安全保障的投入较少，IT 人员网安专业知识与操作经验也较薄弱；
- 攻击手段中，黑客主要通过远程桌面入侵用户终端，其次是利用漏洞投放勒索病毒；
- 入侵时间上，非工作时间通常是勒索攻击的高发时段；
- 勒索病毒主要来自 phobos、Mallox、TellYouThePass 三大家族，其他病毒家族依然活跃；
- 勒索事件的增长，与勒索软件即服务（RaaS）体系的成熟运作有关。



各行业遭遇勒索病毒情况

勒索软件即服务（RaaS）

勒索软件即服务（RaaS）是一套靠勒索攻击赚钱的盈利模式。与普通的软件公司无异，从开发到销售再到运营，勒索产业链各个环节的建立与协作已然成熟。在规模效益促进各环节赚取更多收入的背景下，越来越多的勒索攻击来自于 RaaS。



“勒索软件即服务”（RaaS）运营模式

企业遭受勒索攻击后，是否要交纳赎金？火绒安全实验室不建议支付。首先，加密数据不一定 100% 恢复，这其中有技术原因，也可能存在“诚信”问题；其次，企业不应轻易相信“解密代理”，对方很可能也是第三方“加盟者”甚至还有中间商赚差价，都是为了从中骗取更高赎金；再次，企业或许面临双重勒索的风险。

黑客入侵常见方式

火绒安全实验室最新分析显示，高达 85% 的勒索事件是黑客入侵导致的。黑客入侵常用三种方式包括：通过暴力破解方式，如远程桌面入侵（RDP 暴破）、MSSQL 登录暴破；通过漏洞攻击方式，如系统漏洞、软件 0day 漏洞；通过社工方式非法获取用户隐私数据后再进行攻击，如撞库。

◇ 暴力破解

暴力破解入侵路径

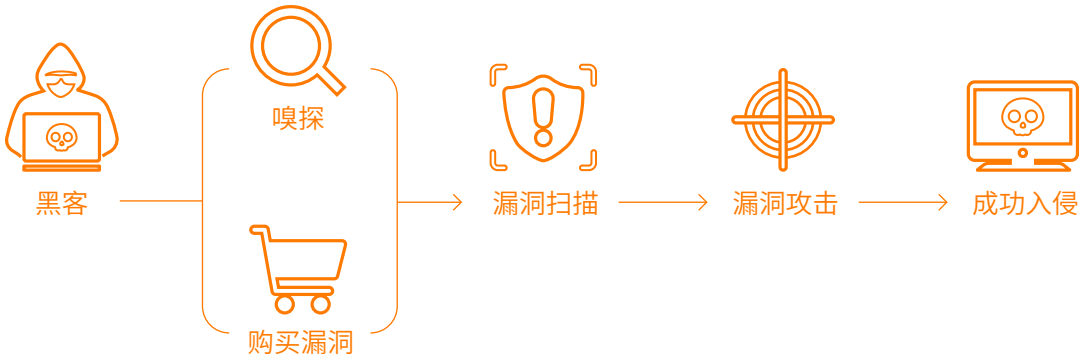
案例：

某国际会展中心遭到勒索攻击，火绒安全团队溯源时发现黑客是通过远程桌面入侵进行的投毒。现场发现当时所用安全终端被直接卸载，且清除了系统中入侵时段的日志记录。

火绒安全建议：

设置强密码，并定期修改密码；关闭不必要端口，如：135，139，445，3389 等；及时异地备份重要数据；采用多重密码防护措施，如火绒企业版中心启用“管理员密码保护”、“终端卸载密码保护”、“终端动态认证”；开启勒索诱捕功能，开启系统防御功能等。

◇ 漏洞攻击



漏洞攻击入侵路径

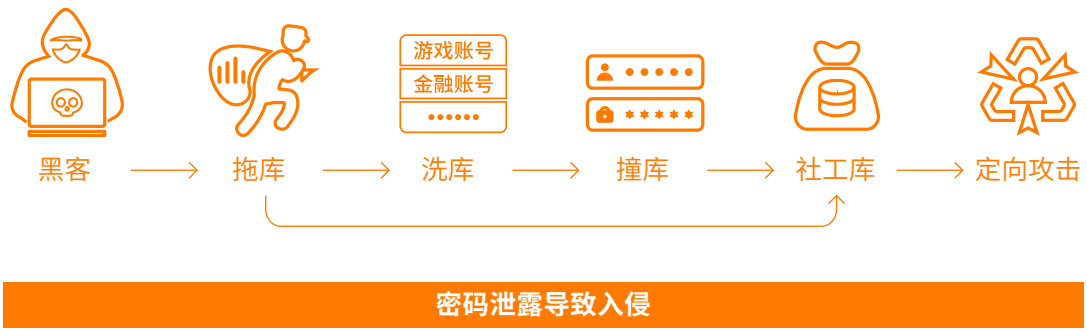
案例：

某公司反馈服务器中勒索病毒，火绒工程师溯源时未发现暴破登录等日志，没有强行破坏系统环境的痕迹，同时发现中毒服务器存在Apache Kafka 业务，且版本存在 Apache Log4j2 反序列化远程代码执行漏洞（CVE-2021-44228）。判断黑客通过该漏洞入侵导致中毒。

火绒安全建议：

定期更新业务软件版本；修复操作系统、软件漏洞，安装最新补丁；采用高强度的密码，避免使用弱口令密码和统一密码，并定期更换密码；对重要文件和数据进行离线备份或者异地备份；开启勒索诱捕功能，增强终端对勒索病毒的防护。

◇ 密码泄露



案例：

某医院反馈有大量横向渗透拦截日志，经火绒安全工程师远程排查后，确定为一台服务器对其他多台服务器进行的攻击。停用该攻击服务器后，远程溯源发现无暴破相关痕迹，但有 Administrator 远程登录成功日志，且该服务器部署在公网，登录密码为中高强度。判断为密码泄露导致。

火绒安全建议：

不自动“保存密码”且杜绝一码多用，避免通过第三方平台登录；定期杀毒、打补丁，不用盗版 / 破解版软件，不随意使用公用 WIFI；可使用密码管理器工具；使用平台提供的多重认证方式，如火绒企业版“终端动态认证”功能；加强用户账户使用策略与账户管理等。

火绒安全产品勒索防护功能矩阵

火绒安全个人产品“火绒安全软件”和企业版产品“火绒终端安全管理系统”通过分析勒索病毒的各种攻击方式，在终端关键节点为用户提供有针对性的防护措施。面对某些风险较高、隐蔽较强的攻击，企业可以使用“火绒终端安全管理系统”优化日常运维，进一步降低被勒索攻击的概率。

火绒安全产品勒索防护功能矩阵

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。

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