火绒安全
HUORONG SECURITY

2022
（上半年）

火绒安全终端防护数据报告

HUORONG SECURITY
ENDPOINT PROTECTION DATA REPORT

北京火绒网络科技有限公司

前 言

PREFACE

2022 年上半年，全球安全局势复杂动荡，疫情反复影响着各国的经济发展，而网络攻击犯罪却没有停歇，漏洞利用、勒索攻击、数据泄露等事件频发，给社会造成了巨大的经济损失，政企安全和个人信息保护面临新的威胁挑战。

新常态背景下，国务院发布《“十四五”数字经济发展规划》，要求“增强网络安全防护能力、提升数据安全保障水平、切实有效防范各类风险”；《2022 年政府工作报告》指示“强化网络安全、数据安全和个人信息保护”，为我国数字经济安全体系的发展和完善指明了方向。

火绒安全作为终端安全领域的排头兵，积极响应国家各项法律法规，致力于为千万用户提供专业的产品和专注的服务，不断升级自主知识产权的反病毒引擎技术，不断打磨各项产品功能。在过去的 11 年里，“干净、轻巧、强大”的火绒安全产品收获了用户的广泛好评。

本报告回顾了 2022 上半年火绒安全产品及服务的各项数据，其中涵盖了恶意攻击防护、病毒拦截、漏洞攻击拦截等维度，对于威胁较大的勒索、挖矿病毒也做了特别的梳理。报告中所使用的所有安全数据均来自于“火绒威胁情报系统”和“火绒在线支持响应中心”，不涉及企业终端数据及个人用户数据隐私。

在“情报驱动、技术创新”的理念下，火绒安全由衷希望能务实有效地服务到更多政企单位和个人用户，从我们擅长的一点一滴做起，让用户的安全生产生活成为触手可及的现实。

关键数据概览

KEY DATA

恶意攻击拦截

19.52 亿次

1-6 月，火绒安全产品拦截恶意攻击总计 19.52 亿次，病毒事件拦截、高危风险动作防护和网络攻击事件拦截效果显著。

病毒事件拦截

8.91 亿次

1-6 月，火绒安全产品拦截各类病毒事件总计 8.91 亿次。文件监控、下载保护、U 盘保护、行为分析、邮件监控和 Web 扫描六大模块继续发挥重要作用。

弹窗广告拦截

14.55 亿次

1-6 月，火绒安全产品拦截（不含用户手动拦截）弹窗广告 14.55 亿次。

漏洞攻击拦截

1.57 亿次

1-6 月，火绒安全产品拦截漏洞攻击 1.57 亿次，涵盖 Web 漏洞拦截、系统漏洞拦截和软件漏洞拦截。其中拦截 Log4j2 漏洞攻击 32.19 万次。

勒索病毒拦截

42.84 万次

1-6 月，火绒安全产品拦截勒索病毒 42.84 万次。病毒新变种多发，企业用户需特别注意防范。

挖矿病毒拦截

219.84 万次

1-6 月，火绒安全产品拦截挖矿病毒 219.84 万次，数量呈下降趋势。

钓鱼邮件拦截

33.91 万次

1-6 月，火绒安全产品拦截钓鱼邮件 33.91 万次。利用钓鱼邮件攻击的 Agent Tesla 和 Emotet 病毒影响依然不容小觑。

用户安全响应

5752 次

1-6 月，火绒安全累计为用户提供 5752 次安全响应服务。其中企业用户响应 2325 次，个人用户响应 3427 次。

目 录

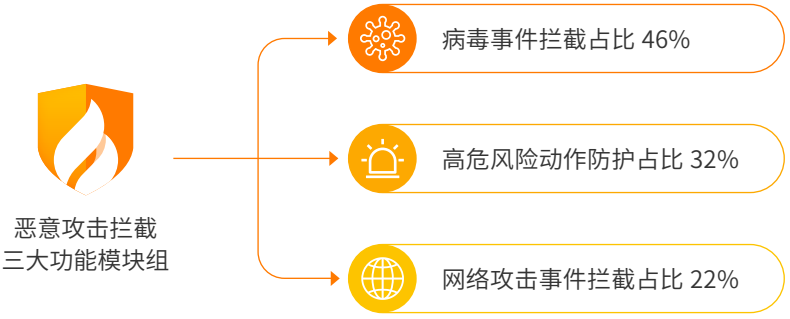
CONTENTS

一、上半年拦截恶意攻击总计 19.52 亿次，整体防护效果显著

19.52 亿次

恶意攻击拦截

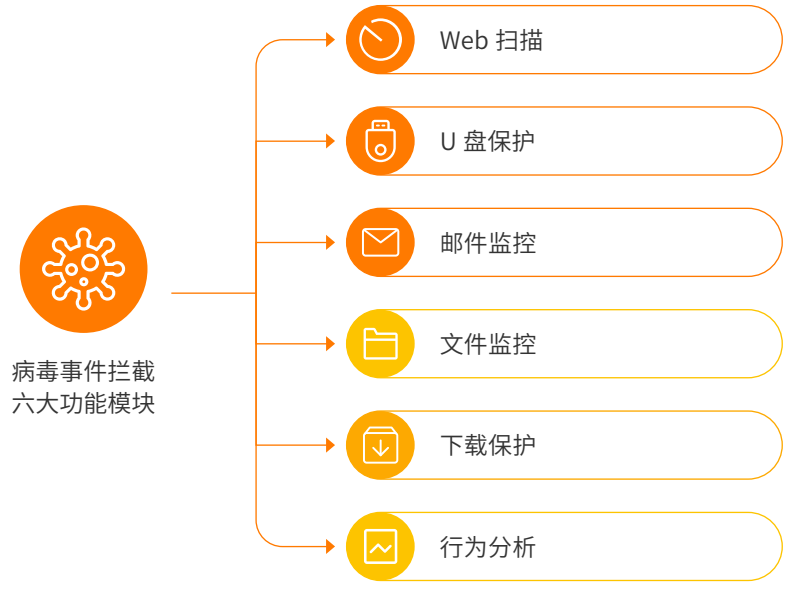
1-6月，火绒安全产品总计拦截恶意攻击 19.52 亿次。其中病毒事件拦截 8.91 亿次；高危风险动作防护 6.32 亿次；网络攻击事件拦截 4.29 亿次。



8.91 亿次

病毒事件拦截

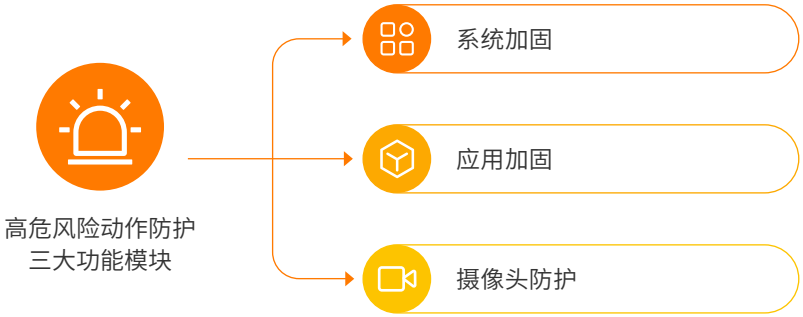
病毒事件拦截六大功能模块总计拦截病毒 8.91亿次。其中 Web扫描功能拦截病毒 1.13 亿次；U 盘保护功能拦截病毒 6202.75 万次。



6.32 亿次

高危风险动作防护

高危风险动作防护三大功能模块总计拦截风险 6.32 亿次，系统加固、应用加固和摄像头防护功能继续发挥强大的保护作用。表面的静默无声，背后是全面周到的主动防御功能，有效保护用户的系统、应用和个人隐私安全。



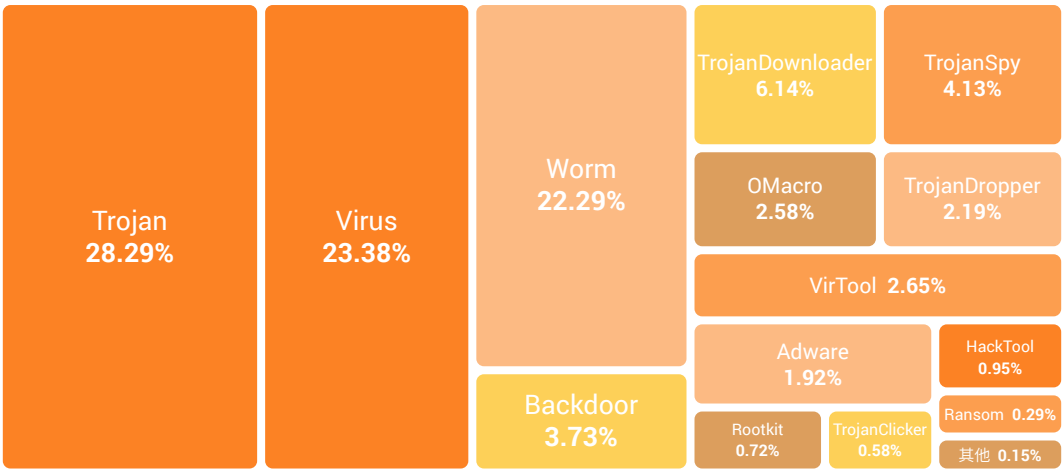
4.29 亿次

网络攻击事件拦截

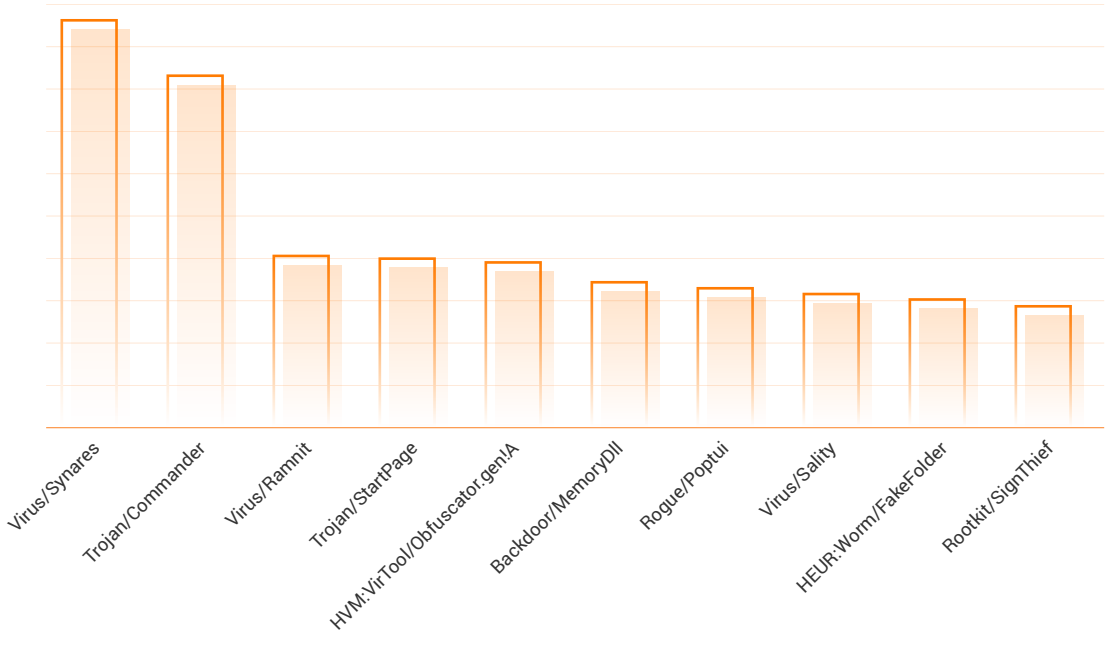
网络攻击事件拦截七大功能模块总计拦截攻击 4.29 亿次。其中横向渗透防护功能总计拦截攻击 5292.57 万次，该功能可有效阻断病毒在局域网内扩散，防止黑客在内网环境里获得更多的终端控制权。

二、木马病毒新增样本量居首，蠕虫和黑客工具有所减少

1-6 月，火绒安全产品截获各类病毒新增样本中，木马病毒（Torjan）数量居首，感染型病毒（Virus）排名第 2。与去年相比，蠕虫病毒（Worm）虽然依然排名第 3，但数量有所减少；而黑客工具（HackTool）数量排名由去年的第 2 位下降至 11 位。很多蠕虫病毒都会在用户本地释放黑客工具进行横向传播，因此黑客工具的减少与上半年此类蠕虫病毒的整体减少有一定关系。



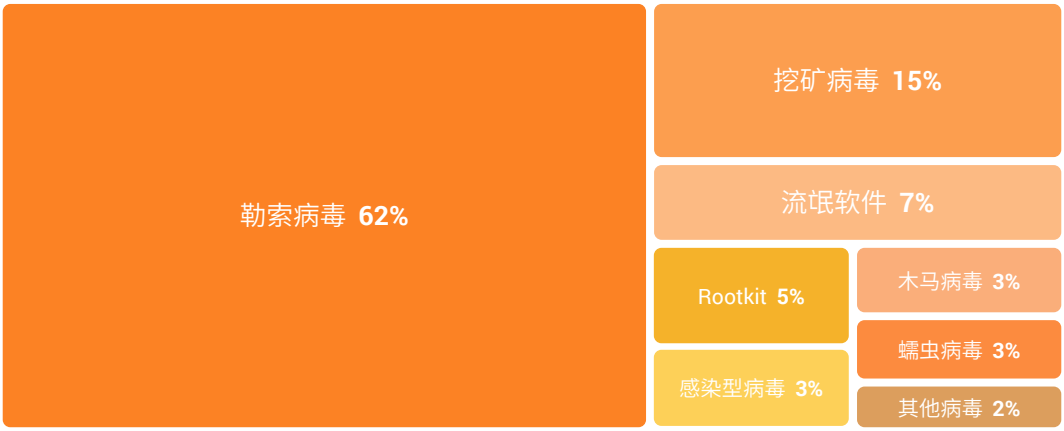
2022 上半年截获病毒样本占比



2022 上半年攻击终端病毒家族数量 TOP10

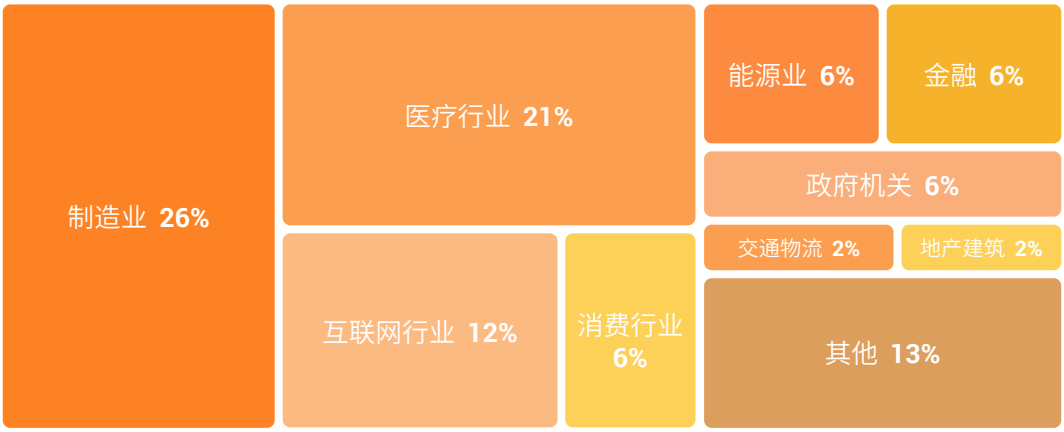
三、累计为用户提供 5752 次安全响应服务，勒索事件处理居首

根据“火绒在线支持响应中心”数据显示，1-6 月，火绒安全团队共为企业用户提供 2325 次在线支持响应服务。其中勒索病毒事件占到病毒类事件总数的 62%；挖矿病毒位列第 2，占 15%；流氓软件位列第 3，占 7% 。



响应企业用户 - 病毒类事件占比

按行业统计，安全问题突出的领域分别是制造、医疗和互联网，分别占到总数的 26%、21% 和 12%。



响应企业用户 - 按行业统计

放眼全球，1-6 月间，制造、医疗和互联网企业被攻击的事件频发。有的用户信息大量泄露，有的造成了严重的经济损失，影响极其恶劣。本报告选编部分事件，简要梳理如下，提醒广大企业用户引以为鉴，加强防范意识，提前做好安全部署。

制造业

2 月，瑞典相机巨头安讯士被网络攻击致服务网络关闭；
3 月，英伟达、三星遭 Lapsus$ 勒索组织泄露数据源代码；
4 月，美国工业巨头 Parker Hannifin 遭勒索团伙泄露数 G 文件；
松下证实加拿大业务遭到有针对性的网络攻击；
德国风力涡轮机制造商 Nordex 被网络攻击致网络瘫痪；
5 月，美国农业机械制造商 AGCO 遭受勒索病毒攻击；
宜家加拿大分公司数据泄露致 95000 客户受影响；
6 月，汽车软管制造商 Nichirin 遭勒索病毒攻击致断网。

医疗

4 月，美国医疗机构 SuperCare 宣布数据泄露影响超过 30 万患者；
法国医院集团遭黑客窃取数据后被迫断网；
美国牙科协会（ADA）遭受网络攻击后运营中断；
5 月，哥斯达黎加公共卫生机构被 Hive 勒索病毒袭击；
美国医疗技术提供商 Omnicell 披露遭勒索病毒攻击；
美国医疗机构 CHRISTUS Health 遭勒索攻击致数据泄露；
6 月，美国医疗机构 Shields 数据泄露影响 200 万患者；
美国眼科护理机构 Eye Care Leaders 数百万患者信息泄露。

互联网

1 月，新加坡加密货币交易平台 Crypto.com 遭黑客入侵；
2 月，OpenSea 用户在网络钓鱼攻击中损失近 200 万美元；
3 月，拉丁美洲电商巨头 Mercado Libre 被黑；
知名游戏厂商育碧遭黑，游戏服务被迫中断；
链游 Axie Infinity 用户 6 亿美元加密货币被黑客盗取；
4 月，Beanstalk 遭黑客盗取近 1.82 亿美元加密币；
5 月，索尼 PS VR 被黑客利用漏洞攻破。

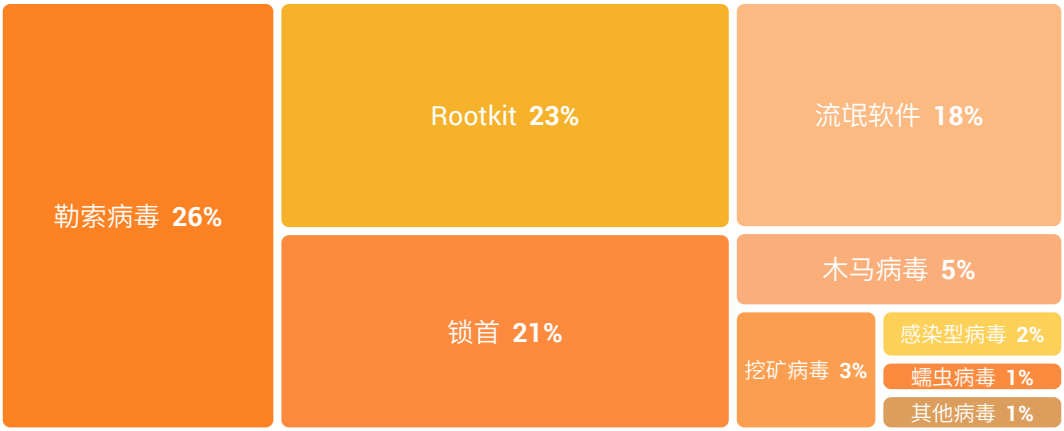
从对各行业的病毒类事件响应结果来看，勒索病毒均有较高占比；挖矿病毒、感染型病毒、Rootkit 程序和流氓软件问题突出。

病毒类事件占比 - 制造业

病毒类事件占比 - 医疗企业

病毒类事件占比 - 互联网企业

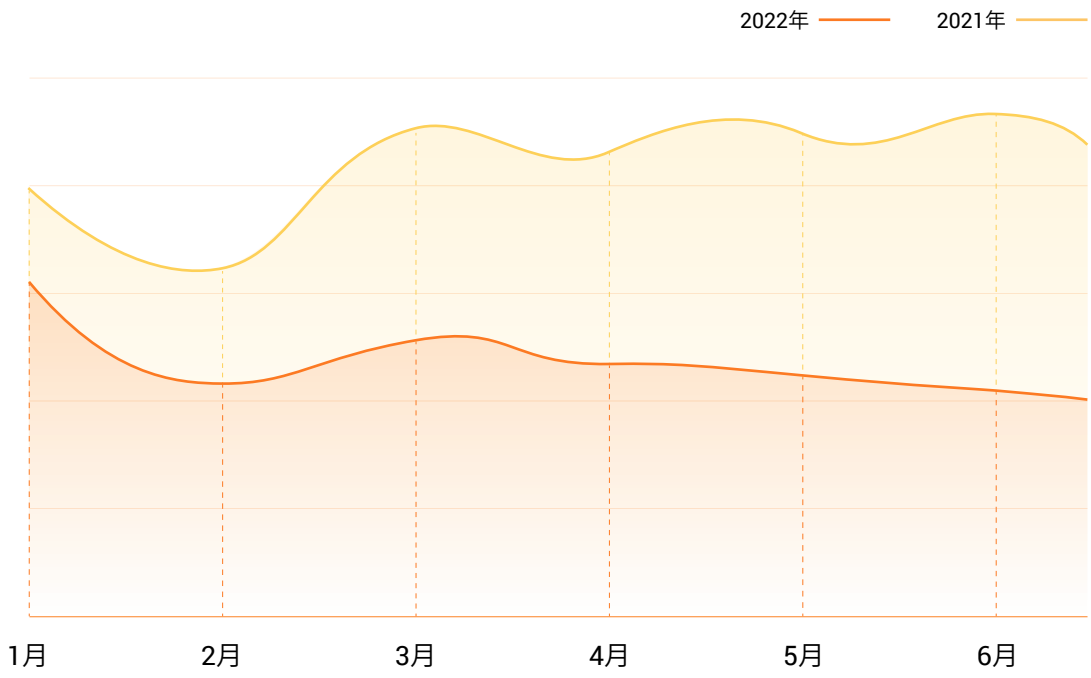
个人用户响应方面，1-6 月，火绒安全团队共为个人用户提供 3427 次在线支持响应服务。其中勒索病毒事件问题排名第 1，占到病毒类事件总数的 26%，Rootkit 程序位列第 2，占 23%；锁首占 21%；流氓软件占 18%。



响应个人用户 - 病毒类事件占比

四、拦截弹窗广告 14.55 亿次，同比呈下降趋势

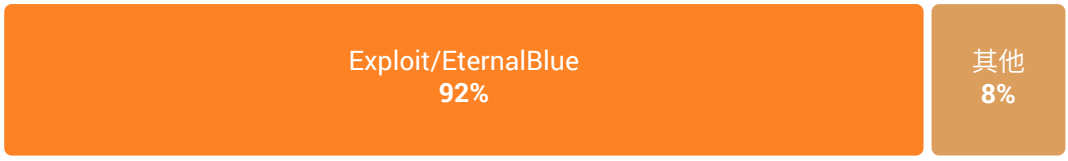
根据“火绒威胁情报系统”数据显示，2022 年 1-6 月，火绒安全产品共拦截（不含用户手动拦截）14.55 亿次弹窗广告，少于去年同期水平，呈下降趋势，“618”购物节期间也并无出现爆发状态。这与国家层面出台的法律法规和重拳治理不无关系。3 月，国家互联网信息办公室发布《互联网弹窗信息推送服务管理规定（征求意见稿）》，进一步规范了互联网弹窗信息推送服务管理，保障了公民、法人和其他组织的合法权益。



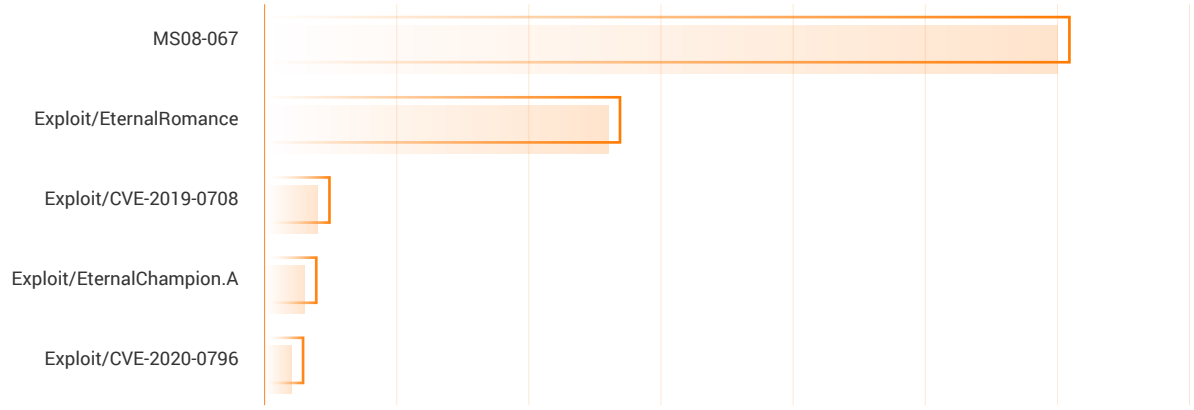
2022 上半年弹窗拦截同比趋势图

五、拦截漏洞攻击 1.57 亿次，旧漏洞影响不容忽视

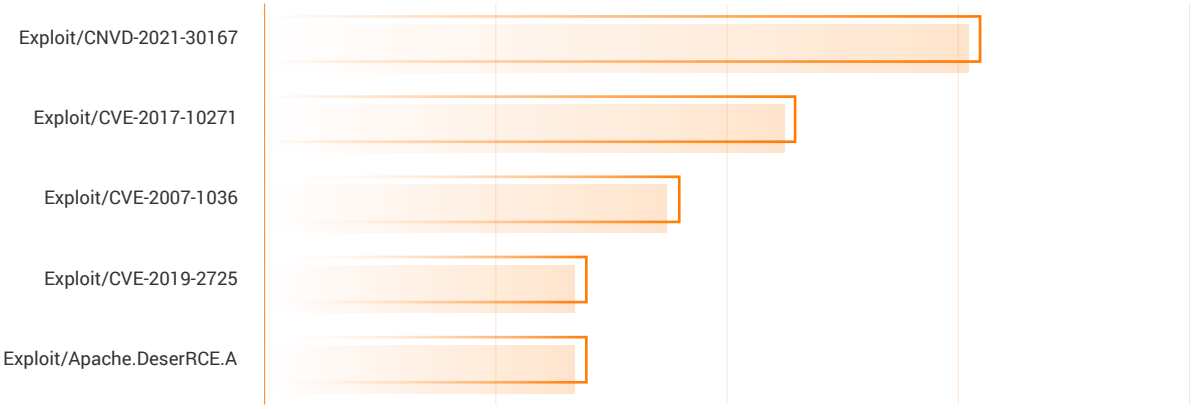
据“火绒威胁情报系统”监测，2022 年 1-6 月，火绒安全产品共拦截 1.57 亿次漏洞攻击。从数量排名上看，系统漏洞前三名为 EternalBlue “永恒之蓝”、MS08-067 和 EternalRomance “永恒浪漫”；Web 漏洞前三名为 CNVD-2021-30167、CVE-2017-10271 和 CVE-2007-1036；软件漏洞上，数量较多的是 CVE-2013-3810 和 CNVD-2022-03672。不少政企用户系统老旧和打补丁不及时是导致大量漏洞攻击的主要原因，旧漏洞威胁依然值得警惕。



2022 上半年拦截系统漏洞攻击中“永恒之蓝”占比



2022 上半年拦截系统漏洞攻击 TOP5（不计算“永恒之蓝”）

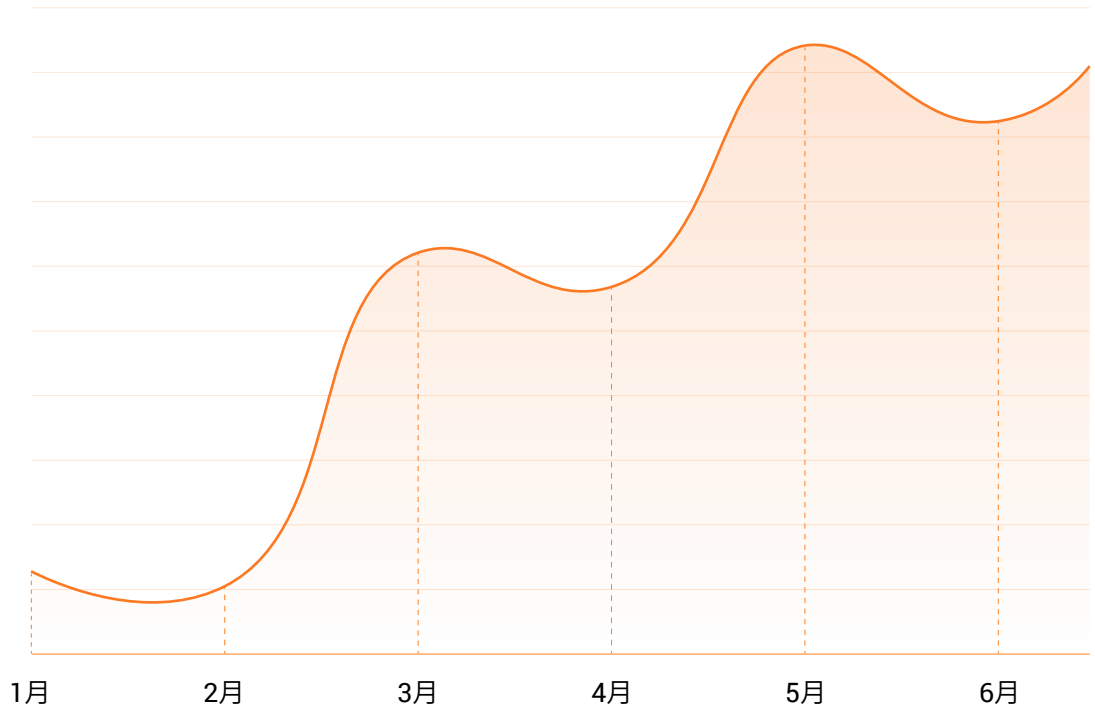


2022 上半年拦截 Web 漏洞攻击 TOP5

1. 上半年拦截 Log4j2 漏洞攻击 32.19 万次，其威胁影响将持续存在

2021 年 12 月，Apache Log4j2 反序列化远程代码执行漏洞（CVE-2021-44228）细节被公开。Log4j2 日志项目作为 Apache 开源项目之一，它因灵活易用的特性得到了广大 Java 开发者的喜爱。据不完全统计，Java 最重要的 Maven 存储库中依赖 Log4j2 的组件包总计超 3.5 万，影响范围极广。鉴于该漏洞的普遍性和易利用性，未来一段时间内相关隐患可能持续存在。

2022 年 1-6 月，火绒安全产品共拦截 Log4j2 漏洞（CVE-2021-44228）攻击 32.19 万次。在监测中发现，漏洞的影响迅速扩大，拦截数量平均每两个月翻倍。火绒安全已发布“Log4j2 漏洞缓解工具”以方便用户进行风险自查和处置。检测到漏洞后，会自动通过“热补丁”+“静态加固”的方式，对此模块进行临时加固，帮助用户更好地防护该漏洞。



2022 上半年 Log4j2 漏洞攻击活跃趋势图

2. 其他高危漏洞回顾（部分）

向日葵远控软件远程代码执行漏洞（CNVD-2022-10270/03672）

上半年受疫情影响，部分城市远程办公场景增多，远控工具被漏洞利用的风险增加。2 月，向日葵远程控制软件被发现存在远程代码执行漏洞（CNVD-2022-10270/03672）。成因主要是低版本下存在未授权访问漏洞，影响 Windows 系统使用的个人版和简约版，攻击者可利用该漏洞获取服务器控制权。火绒安全产品可拦截此漏洞攻击。

Spring Framework 远程代码执行漏洞（CVE-2022-22965）

4 月，Spring 官方披露了一个远程命令执行漏洞（CVE-2022-22965），其框架存在处理流程缺陷，攻击者可远程实现对目标主机的后门文件写入和配置修改，继而通过后门文件访问获得目标主机权限。任何引用 Spring Framework 的框架均受此漏洞影响，包括但不限于 Spring Boot 等。火绒安全已发布“CVE-2022-22965（Spring Boot）漏洞版本检测工具”，排查有关系统中是否使用了漏洞组件。

Windows 网络文件系统远程代码执行漏洞（CVE-2022-26937）

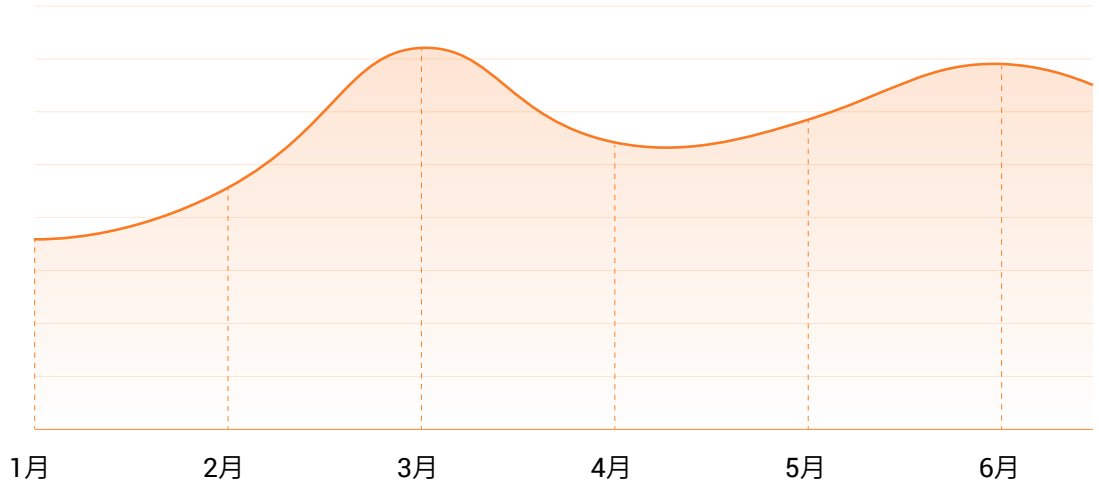
5 月，Windows Network File System 被发现存在远程代码执行漏洞。由于系统对 Windows Network File System 中用户的输入内容验证不充分，导致远程攻击者可利用该漏洞，在未获得权限的情况下，将恶意代码传递给应用程序并在目标系统上执行任意代码。火绒安全产品可拦截此漏洞攻击。

Fastjson 反序列化漏洞

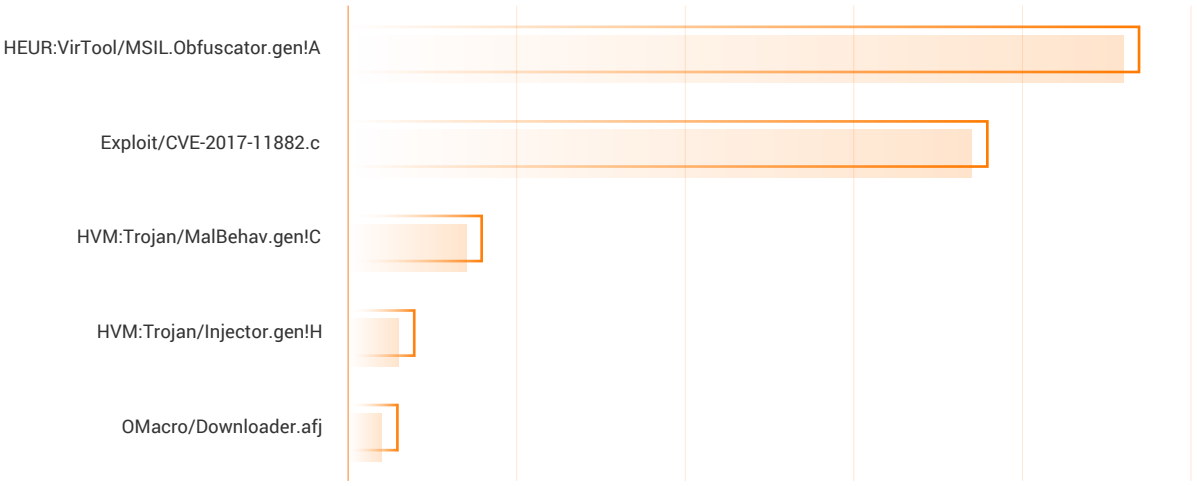
Fastjson 官方已于 5 月在版本 1.2.83 中将其修复。Fastjson 是一个开源的 Java 对象和 JSON 格式字符串快速转换的工具库，其使用非常广泛。该漏洞在特定条件下可绕过默认 AutoType 关闭限制，攻击远程服务器。火绒安全已发布 Fastjson 漏洞本地检测工具，帮助用户排查本地是否有存在漏洞的 Java 库。

六、邮件监控功能拦截钓鱼邮件攻击 33.91 万次

据“火绒威胁情报系统”监测，1-6 月，火绒安全产品的邮件监控功能共拦截钓鱼邮件攻击33.91 万次，数量呈逐月平缓上升趋势，3 月达到小高峰。间谍木马、后门等病毒常借助钓鱼邮件进行渗透攻击，严重威胁政企类用户的网络安全。



2022 上半年钓鱼邮件攻击活跃趋势图



2022 上半年利用钓鱼邮件传播病毒 TOP5

Agent Tesla

2014 年以来，Agent Tesla 病毒持续活跃，逐渐成为全球互联网中主要病毒威胁之一。根据“火绒威胁情报系统”监测，Agent Tesla 病毒影响终端数量整体呈快速上升态势。其主要通过钓鱼邮件进行传播，钓鱼邮件内容多会伪装成装运建议、财务报表或预付款通知单等，邮件附件中包含病毒本体。Agent Tesla 病毒样本通常使用混淆器，通过数据加密、代码加密、控制流混淆等多种混淆方式藏匿自身病毒特征，对抗安全软件查杀。火绒安全产品可有效针对 Agent Tesla 病毒进行查杀。

Emotet

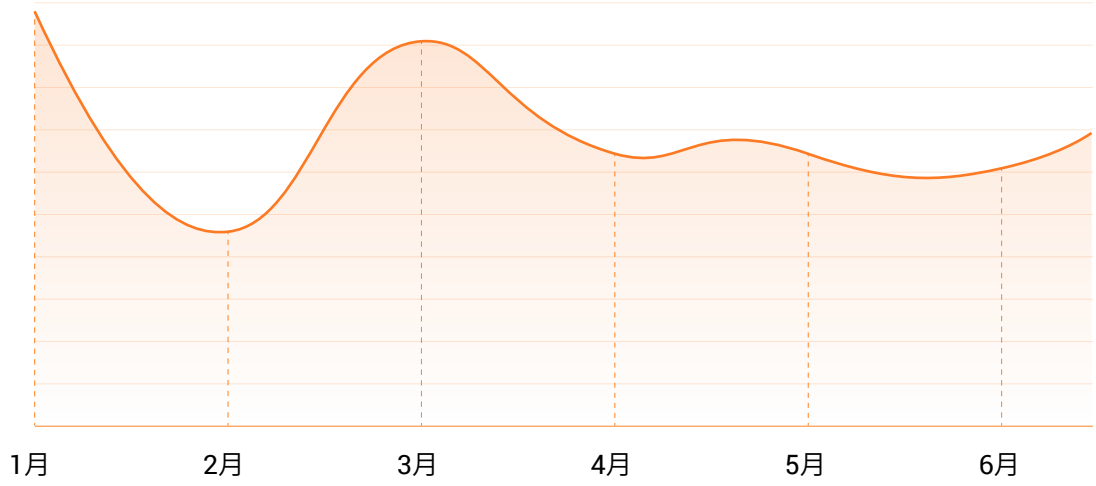
2021 年 1 月， Emotet 基础设施被多国执法机构联合关闭之后，其一度销声匿迹，同年 11 月 Emotet 重新浮出水面。2022 年初 Emotet 木马病毒数量开始持续增加，还新增了 64 位 Emotet 模块，该模块占比也逐渐上升。Emotet 木马病毒主要通过钓鱼邮件进行传播，钓鱼邮件中会将恶意文档（通常为 doc、docx、xls、xlsx 等）伪装成发票、转账等信息，诱导用户打开恶意文档后，病毒就会启动，在后台窃取用户各种隐私信息。火绒安全产品可对 Emotet 木马病毒进行查杀。

七、拦截勒索病毒 42.84 万次，新型病毒危害越来越大

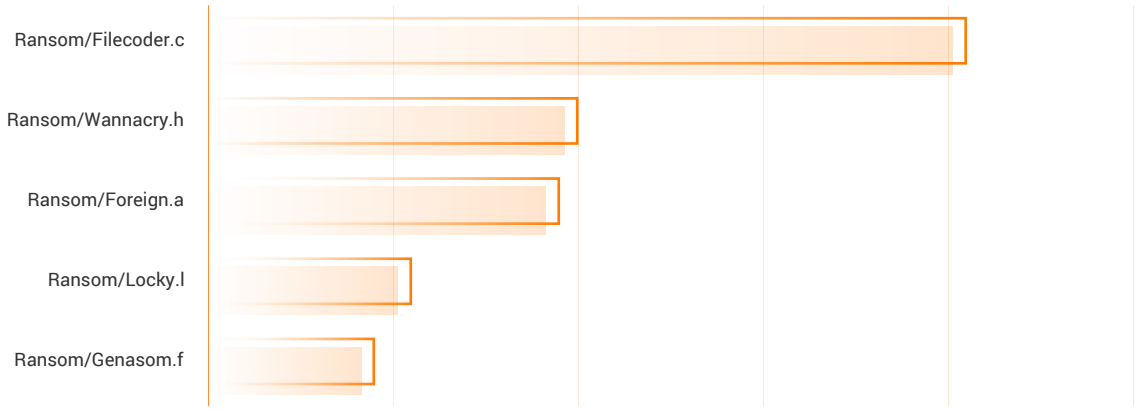
勒索病毒发展演化至今，已形成了一条供销分明的完整产业链。基于虚拟货币的匿名性和隐私性，勒索病毒使用虚拟货币作为交易方式或将成为主流。近年来，勒索病毒的功能、入侵手段开始多样化，且攻击范围也不再局限于政企单位的高价值数据，针对个人隐私的勒索也越来越多，且成功率更高。有理由相信，勒索病毒的攻击面只会越来越广，在万物互联的时代，IoT设备、元宇宙等新兴领域很可能会成为新的主流攻击面。

1. 上半年勒索病毒防护总览

据“火绒威胁情报系统”监测，1-6 月，火绒安全产品共拦截勒索病毒 42.84 万次，1 月到达顶峰，3 月达到次高峰。

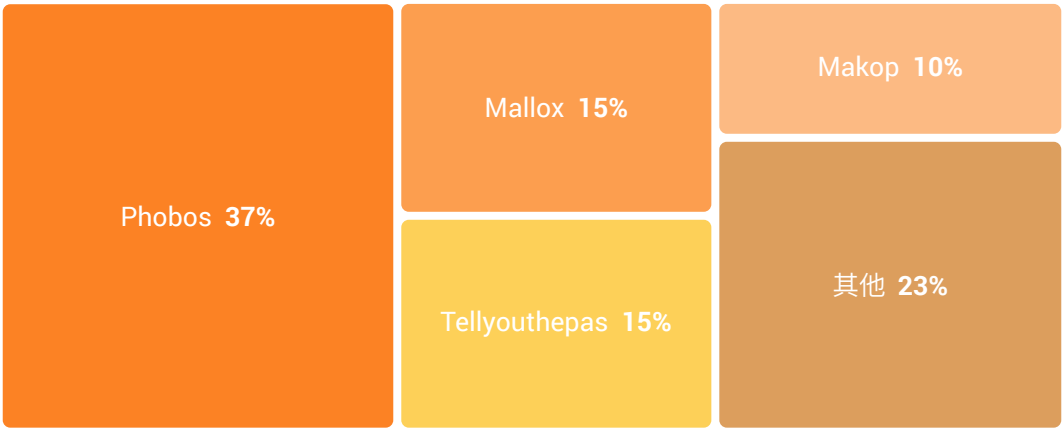


2022 上半年勒索病毒活跃趋势图



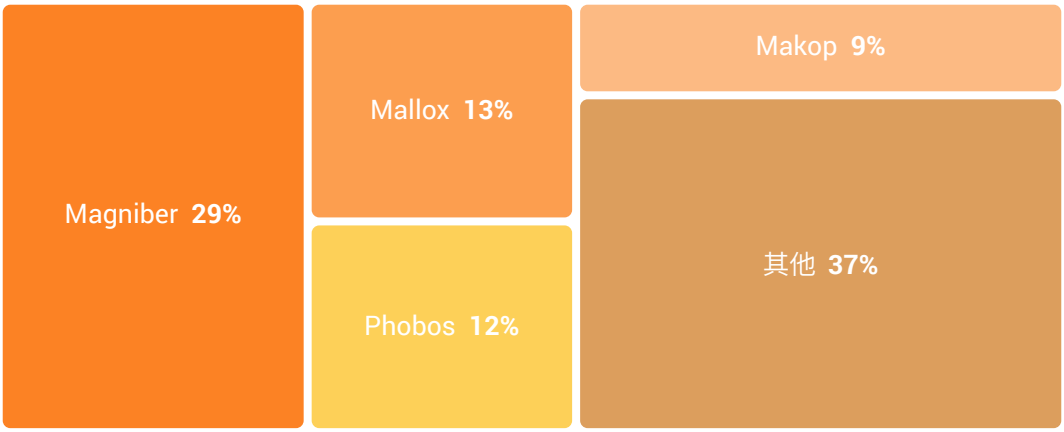
2022 上半年截获勒索病毒 TOP5

根据“火绒在线支持响应中心”数据显示，1-6 月，火绒安全团队响应企业用户的勒索病毒事件中，数量第 1 的是依然是 Phobos 病毒，但占比有所下降，从去年的 48% 下降到今年上半年的 37%；2-4 位分别是 Mallox、Tellyouthepas 和 Makop，相较去年占比均有所上升，值得广大企业用户警惕。



响应企业用户 - 勒索病毒家族占比

响应个人用户的勒索病毒事件中，数量第 1 的是 Magniber 病毒，占比 29%；2-4 位分别是 Mallox、Phobos 和 Makop，三病毒合计占比达 36%。



响应个人用户 - 勒索病毒家族占比

2. 活跃勒索病毒回顾（部分）

Phobos

Phobos 勒索病毒于 2019 年被发现，并不断更新病毒变种。该病毒感染目标系统后，通过 RDP 暴力破解、人工投放和钓鱼邮件等方式扩散，感染数量持续增长，令企业用户防不胜防。它以勒索软件即服务（RaaS）工具包的形式在黑市出售，让没有黑客技术的人也可以借助于工具包创建勒索病毒变种。Phobos 病毒样本数量居高不下，是现阶段最流行的勒索病毒家族之一。

Mallox

Mallox（又被称作 Target Company）早期主要通过 SQL GlobeImposter 渠道进行传播。Mallox 注入的方式有两种：钓鱼邮件和木马，邮件附件用作勒索病毒载体。其可以伪装成合法程序、重要更新或大量扩展程序提供下载。Mallox 主要针对企业的 Web 应用发起攻击，病毒运行后迅速加密数据库文件，导致文件不可用，影响业务运行，同时还会尝试在内网中横向移动，获取更多设备的权限并进一步扩散，危害性极大。

Magniber

Magniber 勒索病毒在 2017 年首次被发现，在韩国和亚太地区造成了较大影响。该病毒积极使用 IE 漏洞进行勒索病毒的传播，每个被加密目录下会被释放一个勒索提示文件，文件加密完成后会被弹出以提示用户。最新的传播手法是伪装成 Windows 更新的 MSI 文件诱使用户下载。一旦感染 Magniber，磁盘上几乎所有格式的文件都会被加密，有极大外泄风险。此勒索病毒会在各种类型网站上大范围投放，企业、学校和个人用户需要特别小心。

Lockbit 3.0

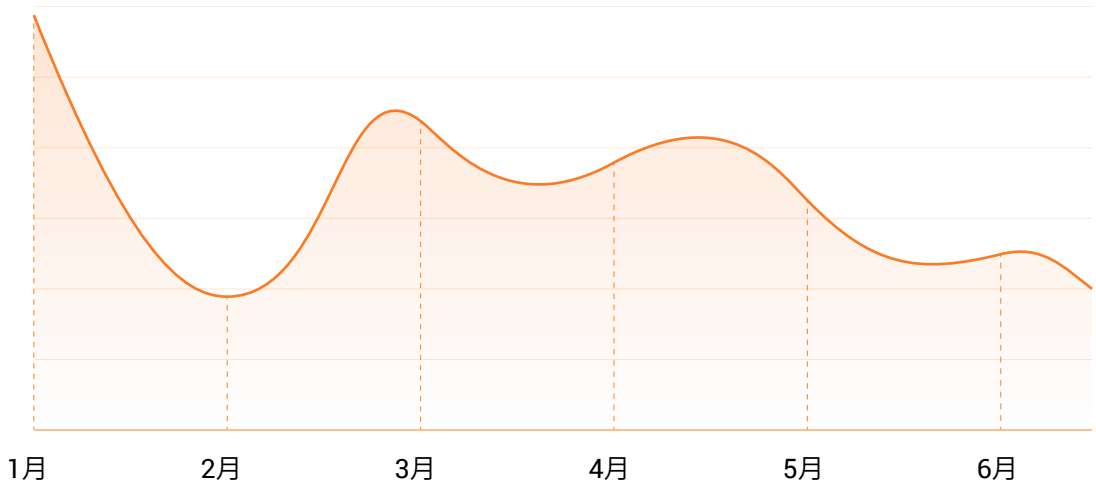
Lockbit 3.0（也被称为 Lockbit Black）是 Lockbit 勒索病毒的新变种。病毒加密文件时会修改文件名，并将文件名和扩展名替换为随机动态和静态字符串。该病毒还会使用代码保护机制和字符串混淆来对抗检测和分析。在流行的勒索病毒团伙中，Lockbit 拥有最快的加密速度。由于其采用 RaaS 的商业模式进行扩散传播，造成的影响越来越大。政企用户要特别注意防范，预防比后期处理要更为关键。

八、拦截挖矿病毒 219.84 万次，攻击活跃度有所下降

1 月 10 日，国家发改委发文宣布，淘汰虚拟货币“挖矿”活动。碳中和背景叠加虚拟货币交易金融风险，“挖矿”行为正面临金融和环保部门的双重监管。继 5 月 25 日内蒙古严令叫停虚拟货币 “挖矿” 后，国家能源局四川能监办一纸摸底通知书更是拉开四川地区“挖矿”整顿的大幕。有分析称，“挖矿”行业在国内消失或许只是时间问题。

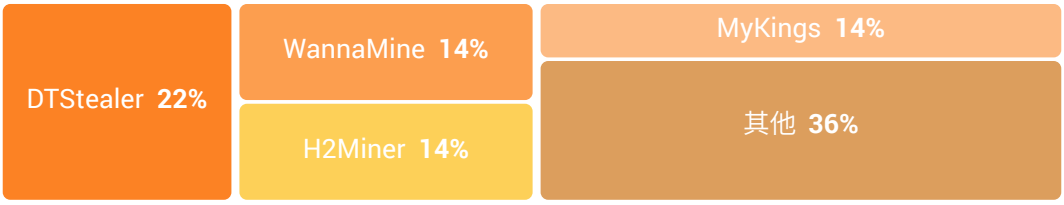
1. 上半年挖矿病毒防护总览

据“火绒威胁情报系统”监测，1-6 月，火绒安全产品共拦截挖矿病毒 219.84 万次，其数量在 1 月到达顶峰，3-6 月整体呈下降趋势。



2022 上半年挖矿病毒活跃趋势图

根据“火绒在线支持响应中心”统计，1-6 月，火绒安全团队响应的挖矿病毒事件中，DTStealer 排名第 1，占比 22%，相较去年的 43% 有所下降；排名 2-4 的挖矿病毒为 WannaMine、H2Miner 和 MyKings，共占据 42% 的份额。



在线响应 - 挖矿病毒家族占比

2. 活跃挖矿病毒回顾（部分）

DTStealer（永恒之蓝下载器）

DTStealer 是一款挖矿病毒（蠕虫病毒），其后更新了“Lemon Duck”、“Bluetea ”“BlackBall” 等多个版本的变种情况。2018 年火绒对其进行披露，其通过“驱动人生”升级通道，并同时利用“永恒之蓝”高危漏洞进行传播。该病毒除了执行挖矿行为，占用终端资源以外，还会窃取终端信息并回传服务器，并利用钓鱼邮件、SMBexec、WMIexec、常见漏洞等方式，在内、外网肆意传播。DTStealer 对内网资源庞大的机构用户（政府、企业、学校、医院等）危害极大，后续会出现更多新型的变种，需要特别注意防御。

WannaMine

WannaMine 是一种蠕虫病毒，也是企业内较为常见的挖矿病毒，于 2017 年底被发现。病毒运行后会扫描企业网络内是否启用了 445 端口的终端，并通过“永恒之蓝 ”漏洞在内网横向传播。WannaMine 病毒对政府、企业、学校、医院等机构危害极大，终端电脑和服务器可能会出现卡顿和蓝屏现象，消耗大量主机 CPU 资源。该病毒已演变到 WannaMine4.0 版本，相较于之前版本，其特征在于组合变形与免杀。

Sysrv-hello

Sysrv-hello 挖矿病毒于 2020 年 12 月首次披露。该病毒通过漏洞攻击方式植入目标主机，在尝试占据系统最大化资源后，释放其自身挖矿模块，并通过进程守护确保挖矿程序的不间断工作，最后通过端口扫描与漏洞利用传播自身，以达到扩散的目的。Sysrv-hello 攻击目标覆盖 Linux 和 Windows 操作系统，具备跨平台型。该病毒对内网资源庞大的机构用户（政府、企业、学校、医院等）危害极大，要特别注意防范。

H2Miner

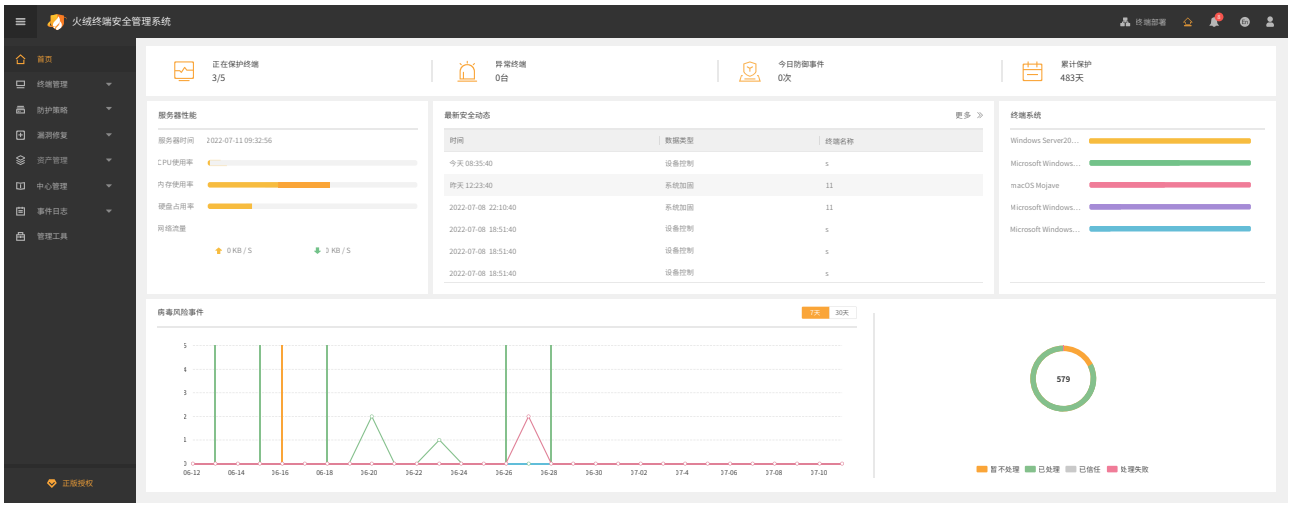
2019 年时，H2Miner 组织主要针对 Linux 服务器使用 Kinsing 僵尸网络发起攻击；2020 年末增加了对 Windows 平台的攻击覆盖。攻击者会向受害主机发送一个构造好的数据包，将数据包中可执行代码部分架设在远程服务器的 XML 文件中，当漏洞利用成功后，受害主机就会访问该 XML 文件并解析执行。H2Miner 利用 Redis 4.x RCE 进行提权，这种方式能够绕过 Redis 安全配置；并且它还具备强大的竞争进程指纹库，帮助它清理大量的竞争对手。因此，H2Miner 病毒得以在短时间内大量传播。

火绒终端安全管理系统 V2.0（企业版）

火绒终端安全管理系统是全面实施 EDR 运营体系的新一代反病毒终端安全产品。系统秉承“情报驱动安全”新理念，集强大的终端防护能力和丰富方便的全网管控功能于一体，性能卓越，轻巧干净，可充分满足企事业单位用户在互联网威胁环境下的电脑终端防护需求。

火绒终端安全管理系统 V2.0 沿袭了 1.0 版本极致专业的产品品质和核心技术，完善了更多针对企业内外网脆弱点的防护功能，拓展了企业对于终端管理的范围和方式，提升了产品的兼容性、易用性，最终实现将威胁可视化、让管理轻便化，充分达到保护企业网络财产与信息安全的目的。

终端安全功能矩阵图



科学清晰的管理系统首页界面

Linux服务器版

支持系统

- CentOS
- 中标麒麟
- Ubuntu
- 中科红旗
- SUSE
- 优麒麟
- 统信UOS
- 深度
- 银河麒麟
- EulerOS
- 龙芯(Loongnix)等发行版

备注

- 目前仅支持64位
- x86_64、aarch64、mips64el、loongarch64架构需要GNU libc2.12及以上版本
- 支持Intel / AMD / 飞腾 / 鲲鹏 / 兆芯 / 海光 / 龙芯等CPU

Linux桌面版

支持系统

- Ubuntu
- 中科红旗
- SUSE
- 优麒麟
- 统信UOS
- 深度
- 银河麒麟
- 龙芯(Loongnix)等发行版

备注

- 目前仅支持64位
- x86_64、aarch64、mips64el架构需要GNU libc 2.17及以上版本/loongarch64架构需要GNU libc2.28及以上版本
- 支持Intel / AMD / 飞腾 / 鲲鹏 / 兆芯 / 海光 / 龙芯等CPU

Windows版

支持系统

- Windows XP (SP3)
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11
- 神州网信 Windows 10

支持CPU

- Intel
- AMD

Windows Server版

支持系统

- Windows Server 2003(SP1)
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

支持CPU

- Intel
- AMD

macOS系统

支持系统

- macOS 10.13及以上版本

支持CPU

- Intel
- M1

多系统终端支持，满足各类需要

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

火绒安全实验室
公众号

火绒安全
公众号