
# 卡巴斯基威胁查找

kaspersky 引领未来

# 卡巴斯基威胁查找

网络犯罪不分边界，技术功能也在快速改进：我们看到攻击变得越来越复杂，因为网络犯罪分子在利用暗网资源来威胁他们的目标。随着攻击者进行各种新的尝试来削弱您的防御等级，网络威胁变得愈加频繁、复杂、混乱。攻击者在实施攻击的过程中，使用复杂的杀伤链以及自定义的战术、技术和程序 (TTP)，意图扰乱企业运转，窃取资产或破坏您的客户端。

卡巴斯基威胁查找涵盖卡巴斯基所具有的与网络威胁及其相互关系有关的全部知识，这些知识融合成一项强大的 Web 服务。目标是为您的安全团队提供尽可能多的数据，在网络攻击影响到您的组织之前加以防范。该平台可检索有关 URL、域、IP 地址、文件哈希值、威胁名称、统计/行为数据、WHOIS/DNS 数据、文件属性、地理位置数据、下载链、时间戳等信息的最新详细威胁情报。因此可以在全球范围内监测新型威胁，帮助您保护组织并提高事件响应能力。

## 亮点

值得信赖的情报：卡巴斯基威胁查找的一个关键特性就是威胁情报数据高度可靠，并且提供了丰富且可行的上下文。卡巴斯基在反恶意软件测试中取得了出色的成绩[1]，通过提供优秀的检测率和近乎零的误报率，证明了我们的安全情报所具备的卓越质量

搜寻威胁：主动预防、检测和应对攻击，以尽量减少攻击的影响和频率。尽早跟踪并积极消除攻击。您越早发现威胁，蒙受的损失就越小，修复的速度就越快，网络运行就能越早恢复正常

事件调查：研究图表可让您直观地探索存储在威胁查找中的数据和检测，从而促进事件调查。它为 URL、域、IP、文件和其他上下文之间的关系提供了图形可视化效果，使您可以更好地了解事件的完整范围，并确定事件的根本原因

强大的搜索：在一个强大的界面上搜索所有处于活动状态的威胁情报产品和外部来源（包括 OSINT IoC、暗网和表网）的信息

易于使用的 Web 界面或 RESTful API：通过 Web 界面（使用 Web 浏览器），以手动模式使用服务，或根据您的喜好通过简单的 RESTful API 进行访问

广泛的导出格式：将 IOC（入侵指标）或可行的上下文导出为广泛使用且更有条理的机器可读共享格式，比如 STIX、OpenIOC、JSON、Yara、Snort、甚至 CSV，以充分利用威胁情报，实现操作流程自动化，或与安全控制系统（比如 SIEM）集成

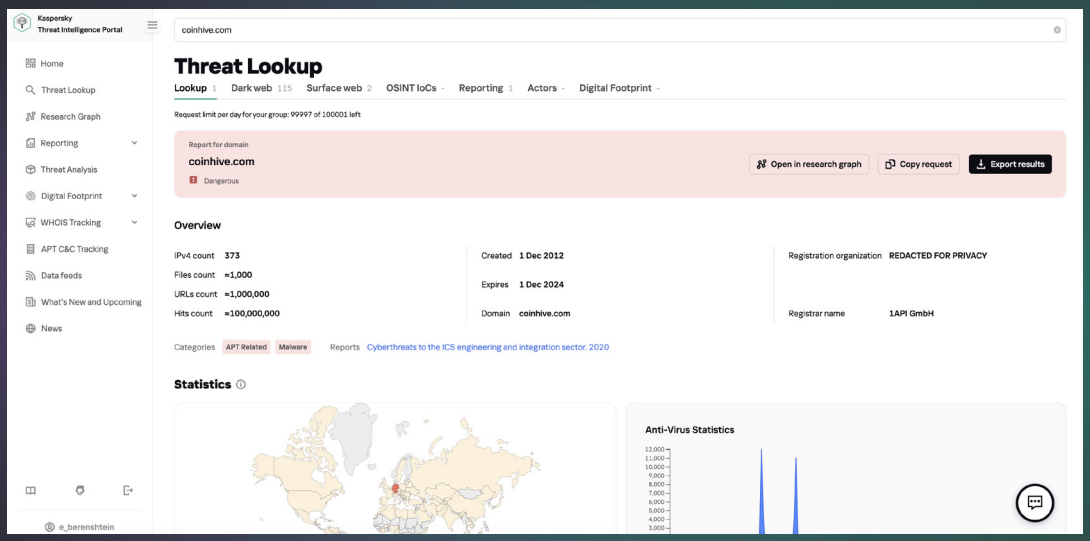
## 优点

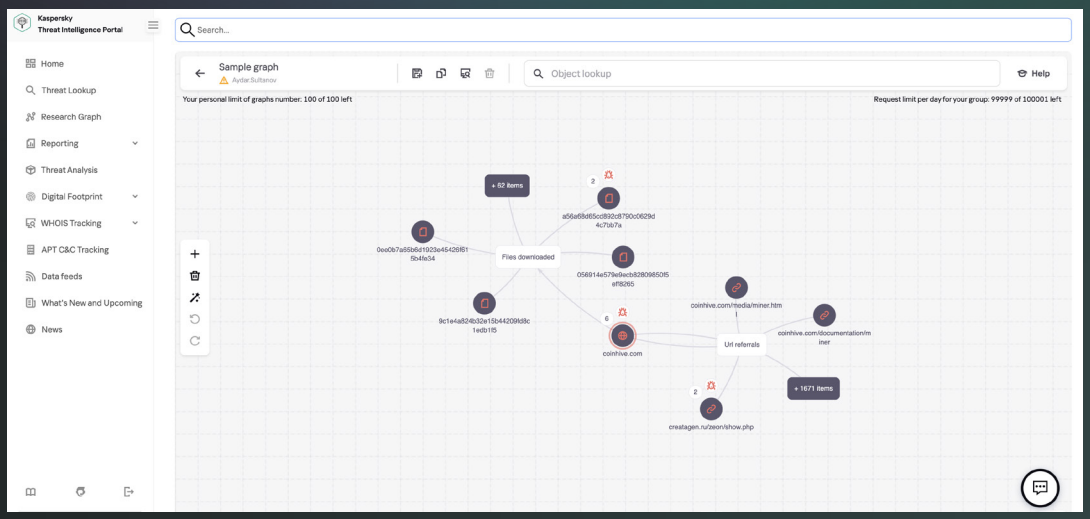
借助充分验证的威胁上下文对威胁指标进行深入搜索，使您可以划分攻击应对措施的优先级，并专注于抵御对您的业务构成巨大风险的威胁

更高效、有效地诊断和分析主机和网络上的安全事件，并为来自内部系统的信号划分优先级，以应对未知威胁

改进您的事件响应和威胁搜寻功能，在关键系统和数据遭到入侵之前破坏杀伤链

[1] kaspersky.com/top3




# 您即可实现

从基于 Web 的界面或使用 RESTful API 查找威胁指标

检查高级设置细节（包括证书、常用名称、文件路径或相关 URL），以发现新的可疑对象

检查发现的对象是普遍存在，还是独一无二

了解为什么一个对象应被视为恶意对象


www.kaspersky.com.cn