



了解如何抵御威胁 — 揭示组织面临的真实威胁形势

威胁形势 揭示威胁形势

kaspersky 引领未来



Kaspersky Threat Intelligence Portal

卡巴斯基威胁情报门户帮助您了解组织面临的威胁形势

在全球范围内，威胁形势不断变化，新的攻击手段层出不穷，而已知的攻击手段也变得越来越复杂。如今，对于信息安全团队来说，能够有效地优先处理需要迅速应对的威胁变得日益重要。但是，如何精准聚焦与您的企业、行业和地区最相关的威胁呢？



卡巴斯基威胁情报门户

用户可以获得独特的机会，在“威胁形势”部分评估自身面临的威胁形势，该部分专门提供针对特定行业和地区的攻击者信息，并将检测技术与全球威胁情报相结合。它还提供了与潜在对手及其战术、技术和程序 (TTP) 相关的最新且完整的威胁信息。

“威胁形势”部分提供与以下方面相关的威胁信息：



地域



行业



威胁类型



威胁发起者



技术、战术和程序 (TTP)



所使用的恶意软件



相关入侵指标 (IoC)

25 年来，卡巴斯基一直利用各种专家系统实时收集威胁情报数据，并以此打击网络犯罪：卡巴斯基安全网络接收来自全球数百万用户的匿名数据，每天自动处理数百万个文件、网络爬虫、僵尸程序集、垃圾邮件陷阱、诱捕系统、传感器、被动 DNS、公开和暗网来源以及合作伙伴。在过去的 25 年里，我们借助这些数据在独立测试和外部评审中获得了最高分。卡巴斯基威胁研究团队会对所获取的数据进行仔细分析，并通过沙盒、启发式引擎和相似性工具等现代自动化系统进行处理，从而将其转化为经过核实的最新信息。

[了解更多](#)

运作方式

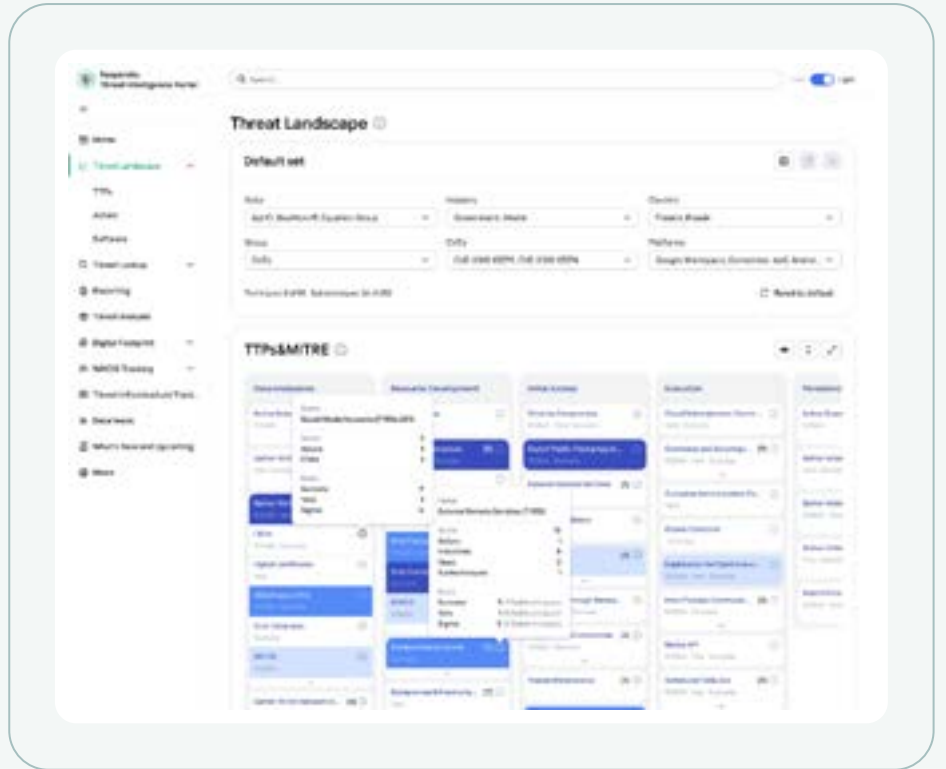


我们每天会处理数十万个恶意文件样本，提取它们的地理位置和行业数据，然后，卡巴斯基内部系统会提取相关的 TTP，并将文件归因于已知的网络犯罪团伙和恶意软件。“威胁形势”部分还基于我们的专家研究团队从世界各地获得的真实事件数据流。

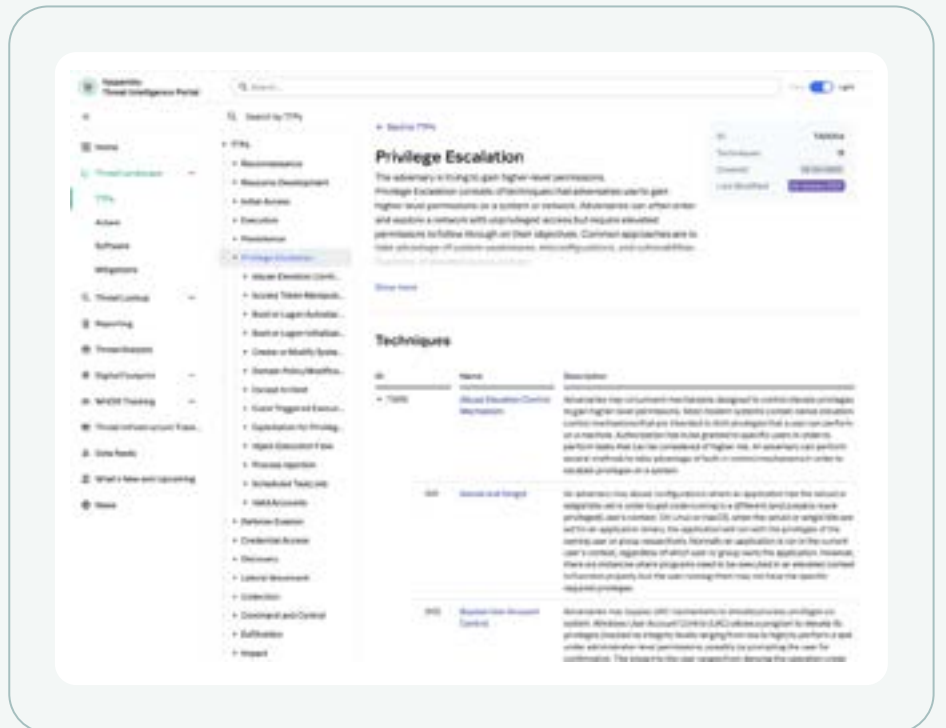
通过使用过滤器，卡巴斯基威胁情报门户的用户能够按照 MITRE ATT&CK 框架创建自己的威胁形势，获得有关潜在对手的最新信息：最有可能用于攻击的技术、战术和程序，有关攻击者、恶意软件及其使用的 TTP 的详细描述，包括攻击详细描述的报告，并最终获得防御措施 — 可用于防止攻击技术得逞的具体建议。

亮点

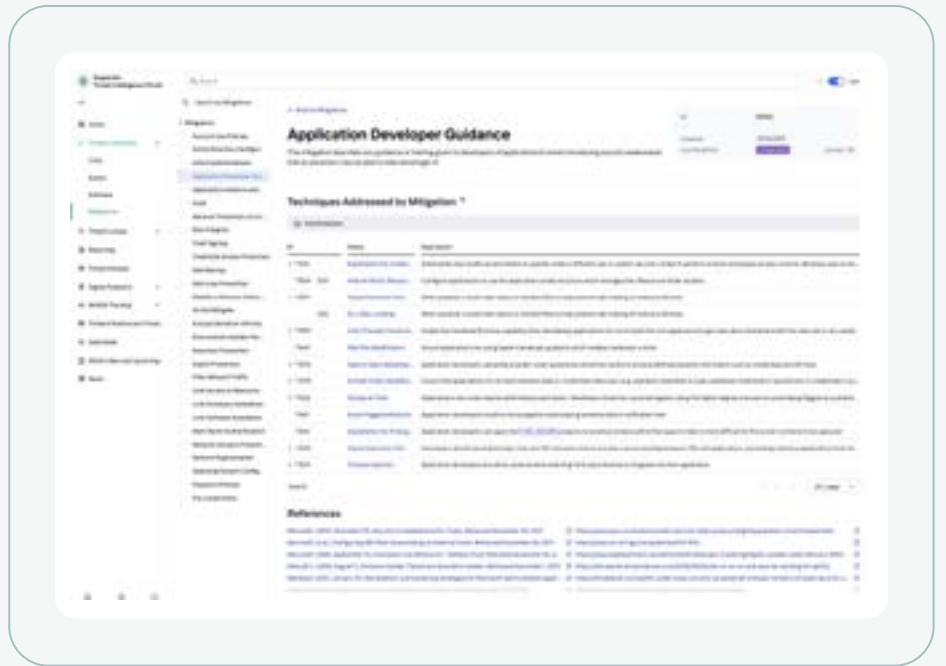
MITRE ATT&CK 热图可实时显示您的组织所面临的**独特的威胁形势**。通过应用过滤器，用户可以访问最新数据，包括过去 24 小时内的最新数据，这些数据由我们的系统和专家通过持续研究获得。该部分能够为国际组织保存不同的图层。



基于卡斯基专家系统提供有关攻击者的**技术、战术和程序**的实时信息。



“防御措施”部分为组织提供了用于避免安全漏洞的**防范和保护措施**的**详细说明**。



访问**业内最全面的攻击者和恶意软件资料库**，以及由卡巴斯基专家汇编的**详细说明**。





如今，随着网络威胁形势的不断演变，通过各种产品和服务可获得大量**威胁情报数据**。通过了解自身的威胁形势，组织能够采取战略性的合理措施，积极防御相关攻击。

使用该服务的优势

主动防御方法

了解最有可能导致组织遭受攻击的媒介，以建立有效的防御策略

攻击面监控

找出安全漏洞以避免被攻击者利用

聚焦相关威胁

能够聚焦最有可能影响您所在企业、行业和地区的威胁

战略性规划

利用威胁形势信息来规划投资和开发防御工具/方法

提高信息安全部门的效率

通过获取有关威胁和全球趋势的信息，提高工作人员的效率并降低人力成本

威胁意识

了解最新威胁及其全球趋势以建立有效防御



知己知彼，百战不殆。不知彼而知己，一胜一负。不知彼知己，每战必殆。

一 孙子

孙子

卡巴斯基威胁情报

卡巴斯基威胁情报提供我们的世界级分析师和研究人员收集的各种信息。这些数据将帮助任何组织**有效应对当今的网络威胁**。

卡巴斯基在网络威胁研究方面拥有深厚的知识和丰富的经验，针对网络安全的各个方面都能提供独到的见解。这使得卡巴斯基成为世界各地的执法机构和政府组织（包括国际刑警组织和全球计算机紧急响应小组）值得信赖的合作伙伴。卡巴斯基威胁情报提供战术、操作和战略方面的最新威胁情报。



Kaspersky Threat Intelligence

了解更多

www.kaspersky.com.cn

© 2024 AO Kaspersky Lab。注册商标和服务标志归其各自所有者所有。

#kaspersky
#bringonthefuture