卡巴斯基威胁情报

kaspersky 引领未来

挑战

跟踪、分析、解析和缓解不断演变的 IT 安全威胁是一项庞大的工程。企业的所有部门都面临着最新相关数据的短缺，但他们需要这些数据帮助其管理与 IT 安全威胁相关联的风险。

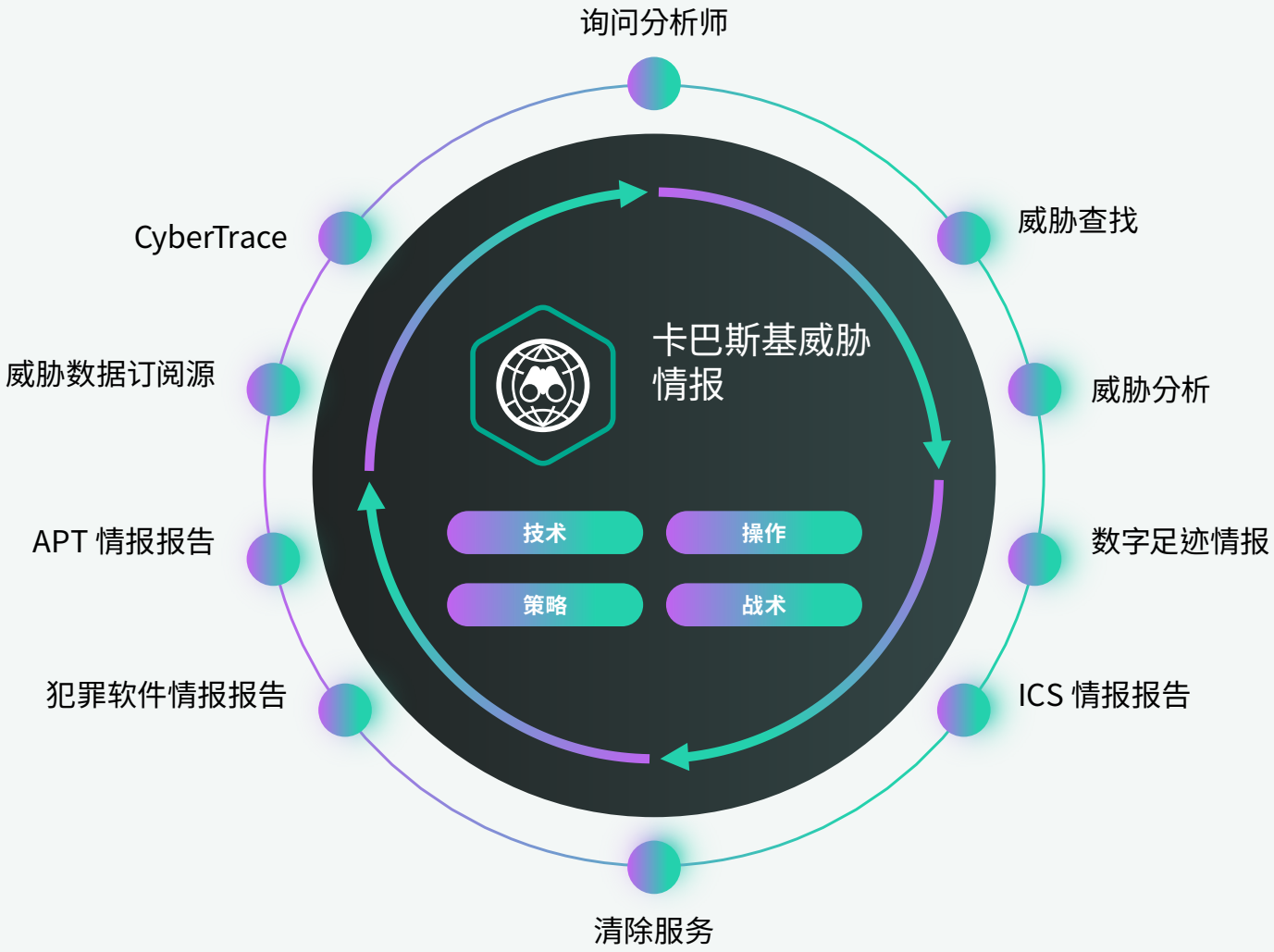
卡巴斯基威胁情报

卡巴斯基的威胁情报让您可以访问限制网络威胁所需的情报，这些情报由我们全球一流的研究人员和分析师团队提供。

卡巴斯基在网络安全各个方面的知识、经验和深度情报，使其成为世界上最重要的执法和政府机构，包括国际刑警组织和领先的应急响应团队的信任伙伴。卡巴斯基威胁情报让您即时获得技术、战术、操作和策略性威胁情报。

卡巴斯基威胁情报产品组合包括

威胁数据源、网络威胁追踪服务（一个威胁情报平台）、威胁查找、威胁分析（云沙盒和云威胁归因引擎）、一系列威胁情报报告选项，以及按需提供威胁情报专业知识的服务。



卡巴斯基威胁数据源

网络攻击每天都在发生。随着攻击者尝试削弱您的防御等级，网络威胁变得愈加频繁、复杂、混乱。攻击者使用复杂的入侵杀伤链、攻击活动和自定义的战术、技术和流程 (TTP) 来破坏您的业务或损害您的客户。很明显，要提供保护，需要以威胁情报为基础，使用新的方法。

通过将最新威胁情报源（包含有关可疑和危险 IP、URL 和文件哈希值的信息）集成到 SIEM、SOAR 和威胁情报平台等现有安全系统中，安全团队可以实现初始警报分类自动化，同时为他们的分类专家提供足够的上下文，以立即确定需要调查的警报，或需要上报给事件响应团队进行进一步调查和响应的警报。

上下文数据

每个数据源中的每条记录都包含丰富且可行的上下文（威胁名称、时间戳、地理位置、受感染 Web 资源的解析 IP 地址、哈希值、流行度等）。上下文数据有助于揭示“整体情况”，从而进一步验证和支持对于数据的广泛使用。根据上下文，可以更容易地使用数据来回答与“人物、事件、地点、时间”有关的问题，以确定攻击者，并帮助您做出快速决策和采取行动。

亮点

收集和处理

数据源来自融合、异构且高度可靠的来源，比如卡巴斯基安全网络和我们自己的 Web 爬虫、僵尸网络监控服务（全天候监控僵尸网络及其目标和活动）、垃圾邮件陷阱、研究团队和合作伙伴。

然后，实时对所有聚合的数据进行仔细检查，并使用多种预处理技术进行提炼，比如统计标准、沙盒、启发式引擎、相似性工具、行为分析、分析师验证和允许列表验证。

根据全球范围内的调查结果实时自动生成数据源（卡巴斯基安全网络可以监测很大比例的互联网流量，覆盖了超过 213 个国家/地区的数千万最终用户），从而提供出色的检测率和准确性

轻松实施。补充文档、样本、专门的技术客户经理和卡巴斯基的技术支持，所有这些资源都有助于实现直接集成

通过 HTTPS、TAXII 或专用交付机制的简单轻量级传播格式（JSON、CSV、OpenIoC、STIX），轻松将信息源集成到安全解决方案中

夹杂误报的数据源没有价值，因此在发布数据源前将应用非常广泛的测试和过滤，以确保交付 100% 经过审查的数据。

数百名专家（包括来自全球各地的安全分析师、来自 GReAT 的世界知名安全专家和研发团队）为生成这些数据源做出了贡献。安全官收到由高质量数据生成的关键信息和警报，无需浪费时间去处理过多的指标和警告

由一个高度容错的基础架构生成和监控所有数据源，从而确保了持续的可用性

优点

通过不断更新的入侵指标 (IOC) 和可行的上下文来加强您的网络防御解决方案（包括 SIEM、防火墙、IPS/IDS、安全代理、DNS 解决方案、反 APT），以提供对于网络攻击的见解，并对攻击者的意图、能力和目标提供更深入的了解。全面支持优秀的 SIEM（包括 HP ArcSight、IBM QRadar、Splunk 等）和 TI 平台

通过为初始分类过程实现自动化，改善并加快您的事件响应和取证功能，同时为您的安全分析师提供足够的上下文，以立即确定需要调查的警报，或需要上报给事件响应团队进行进一步调查和响应的警报

防止敏感资产和知识产权从受感染的机器渗出到组织外。快速检测受感染的资产，以保护您的品牌声誉，保持您的竞争优势并保护商机

作为 MSSP，以高级服务的形式向客户提供优秀的威胁情报，从而发展您的业务。作为 CERT，加强和扩展您的网络威胁检测和识别功能

卡巴斯基网络威胁追踪服务

通过将最新的可机读威胁情报整合到现有的安全控制机制（如 SIEM 系统）中，安全运营中心可以自动化初始分类流程，同时为其安全分析师提供足够的情景信息，以立即识别出哪些警报需要调查或上报给事件响应团队，以开展进一步的调查和响应。然而，威胁数据订阅源和可用威胁情报来源的数量持续增长，使得组织机构难以确定哪些信息与他们相关。威胁情报提供不同的格式，并包括大量的入侵指标（IoC），导致 SIEM 或网络安全控制机制难以消化处理。

卡巴斯基网络威胁追踪服务是一款威胁情报平台，可实现威胁数据订阅源与 SIEM 解决方案的无缝集成，帮助分析师更有效地在现有安全运营工作流程中利用威胁情报。它可以与任何威胁情报源（来自卡巴斯基、其他供应商、OSINT 或您自己的客户情报源）进行集成（以 JSON、STIX、XML 和 CSV 格式），并支持与众多 SIEM 解决方案和日志源进行开箱即用的集成。

卡巴斯基网络威胁追踪服务提供了一套可有效实施威胁情报的工具：

- 指标数据库包含全文搜索功能，并且支持使用高级搜索查询进行搜索，从而实现跨所有指标字段（包括上下文字段）的复杂搜索
- 包含有关各指标详情的页面，可提供更深入的分析。每个页面都呈现了所有威胁情报提供者就某个指标提供的所有信息（删除重复数据），这让分析师可以在评论中讨论威胁，并添加关于该指标的内部威胁情报
- 研究图表可让您视觉化探索存储在 CyberTrace 中的数据和检测并发现威胁共性
- 指标导出功能允许将指标集导出到安全控制机制，如策略列表（阻止列表），以及在卡巴斯基网络威胁追踪服务实例之间或与其他威胁情报 (TI) 平台共享威胁数据
- 给入侵指标做标签可简化其管理。您可以创建任何标签并指定其权重（重要性），使用它手动给入侵指标做标签。您也可以基于这些标签及其权重来排序和筛选入侵指标
- 历史关联功能（回溯扫描）使您可以使用最新的数据订阅源来分析先前检查过的事件中的可观察信息，以发现先前未发现的威胁
- 过滤器将检测事件发送到 SIEM 解决方案，从而减少它们自身以及分析人员的负担
- 多租户支持 MSSP 和大型企业用例
- 数据订阅源使用情况统计信息会衡量集成数据订阅源和数据订阅源交叉矩阵的有效性，有助于选择最有价值的威胁情报提供者
- HTTP RestAPI 允许您查找和管理威胁情报

该工具采用一种内化流程对传入数据进行解析和匹配，从而大大降低 SIEM 的工作负载。卡巴斯基网络威胁追踪服务会解析传入的日志和事件，迅速将所获得的数据与数据订阅源进行匹配，并在威胁检测中生成自己的警报。解决方案集成的高层架构如下图所示：

借助卡巴斯基网络威胁追踪服务和卡巴斯基威胁数据源，安全分析人员能够：

- 有效地提炼大量安全警报并为其划分优先级
- 改善并加快分类和初步响应过程
- 立即识别对企业至关重要的警报，并就哪些警报应上报给 IR 团队做出更明智的决定
- 建立由情报驱动的主动防御机制

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

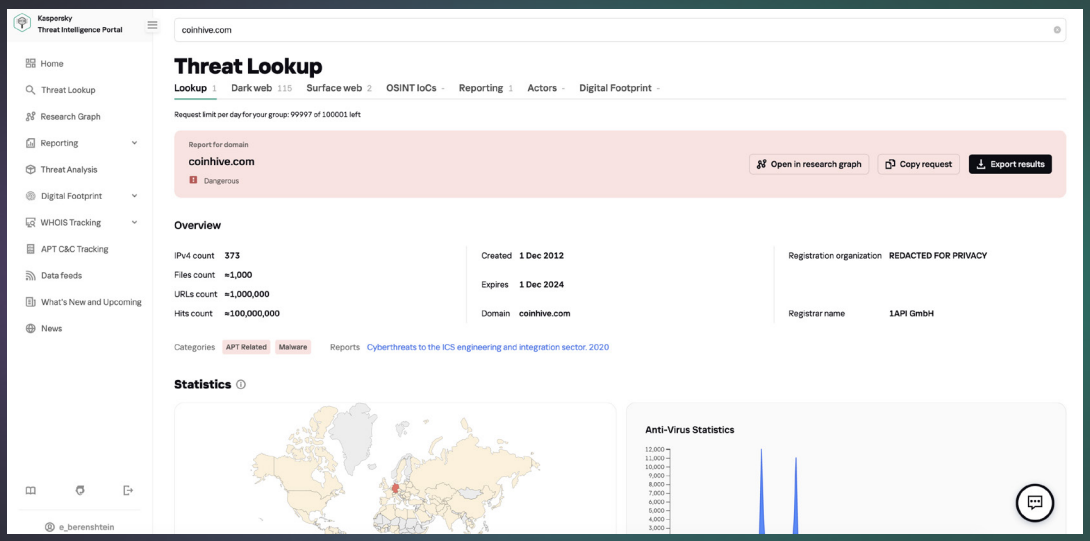
优点

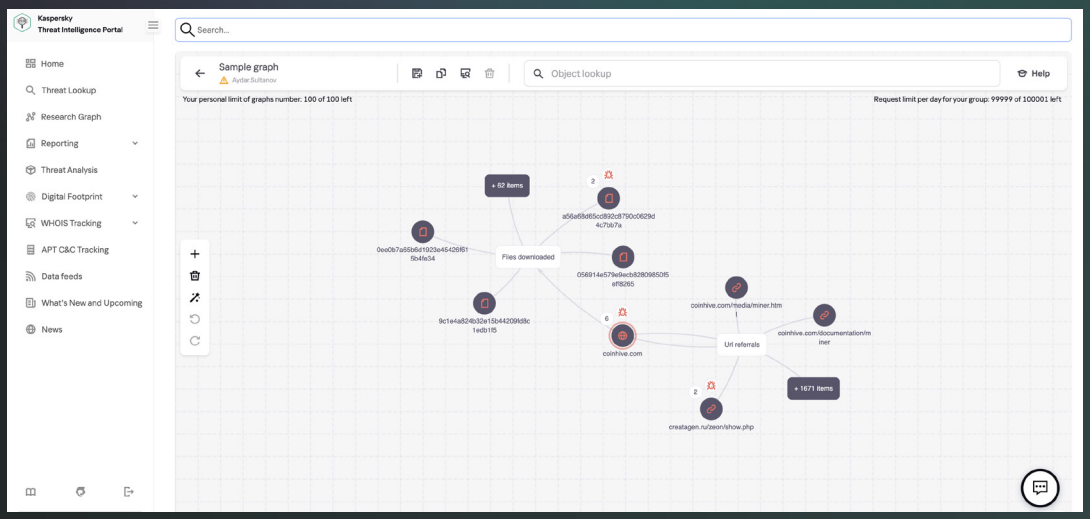
借助充分验证的威胁上下文对威胁指标进行深入搜索，使您可以划分攻击应对措施的优先级，并专注于抵御对您的业务构成巨大风险的威胁

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

卡巴斯基云沙盒

仅仅依靠传统 AV 工具不可能防范当今的定向攻击。反病毒引擎只能阻止已知的威胁及其变异，而复杂的攻击者会利用他们掌握的所有手段来规避自动检测。信息安全事件造成的损失继续大幅增长，这凸显了即时威胁检测功能日益重要，它可以确保在任何重大损害发生之前作出快速响应并抵御威胁。

根据文件的行为做出智能决策，同时分析进程内存、网络活动等，这是了解最新的、复杂的针对性定制威胁的最佳方法。统计数据可能缺乏与最近修改的恶意软件有关的信息，而沙盒技术是强大的工具，可以调查文件样本的来源，收集基于行为分析的入侵指标，并检测以前没有见过的恶意对象。

全面报告

- 已加载和运行的 DLL
- 与域名和 IP 地址的外部连接
- 创建、修改和删除的文件
- 详细的威胁情报，为每个发现的入侵指标 (IOC) 提供了可行的上下文
- 进程内存转储和网络流量转储 (PCAP)
- HTTP 和 DNS 请求及响应
- 创建的相互扩展 (mutexes)
- RESTful API
- 修改和创建的注册表项
- 被执行文件创建的进程
- 屏幕截图
- **更多内容**

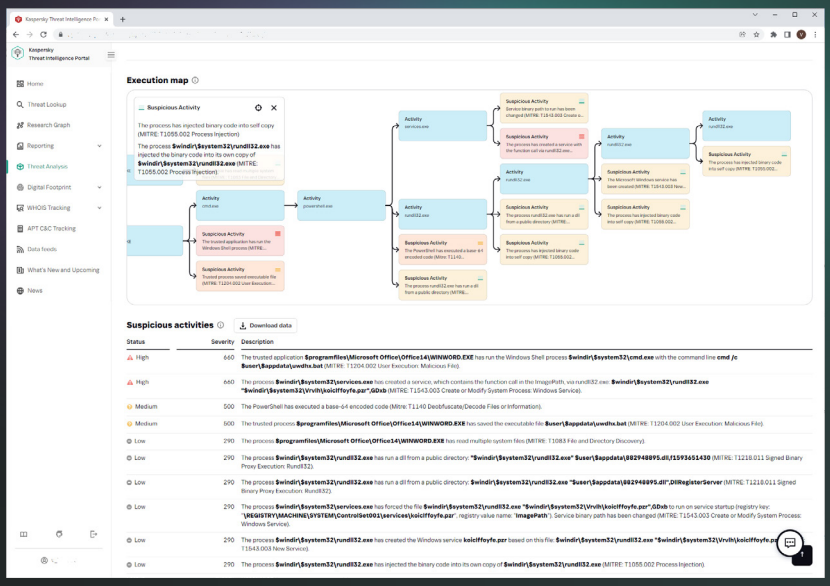
主动威胁检测和抵御

恶意软件使用各种方法来伪装自身的执行，以免遭到检测。如果系统不符合要求的参数，恶意程序几乎肯定会自我毁灭，不留任何痕迹。要使恶意代码执行，沙盒环境必须能够准确模仿正常的最终用户行为。

卡巴斯基云沙盒提供了一种混合方法，把从 PB 级统计数据中收集的威胁情报（得益于卡巴斯基安全网络和其他专有系统）、行为分析和强大的反规避功能，与自动点击器、文件滚动和虚拟进程等人类模拟技术结合起来。

该产品是在我们的内部沙盒实验室中开发的，迄今已历经十余年的发展完善。该技术融合了我们在 20 多年的持续威胁研究中获得的关于恶意软件行为的所有知识。这使我们能够每天检测超过 360000 个新的恶意对象，为我们的客户提供卓越的安全解决方案。

作为我们的威胁情报门户的一部分，云沙盒是您的威胁情报工作流程中的重要组成部分。威胁查找可检索与 URL、域、IP 地址、文件哈希值、威胁名称、统计/行为数据、WHOIS/DNS 数据等信息有关的最新详细威胁情报，云沙盒则将这些知识与分析样本生成的 IOC 关联起来。



现在您可以运行高效且复杂的事件调查，从而立即了解威胁的性质，并在深入研究时进行关联，继而揭示相互关联的威胁指标。

检查可能非常耗费资源，特别是在涉及多阶段攻击时。卡巴斯基云研究沙盒促进了您的事件响应和取证活动，为您提供了用于自动处理文件的可扩展性，而无需购买昂贵的设备或担心系统资源。

卡巴斯基 APT 情报报告

卡巴斯基 APT 情报报告客户具备持续查看我们的调查和发现的专享权限，包括每个 APT 被发现时的完整技术数据（各种格式），以及许多永远不会公开的威胁的完整技术数据。报告包含一个执行摘要，提供了面向核心高管的、易于理解的信息（描述了相关的 APT），以及 APT 的详细技术说明，包括相关的 IOC 和 YARA 规则，以便为安全研究人员、恶意软件分析师、安全工程师、网络安全分析师和 APT 研究人员提供可行的数据，从而快速、准确地应对威胁。

我们的专家在发现网络犯罪团伙的战术有变时，也会立即向您发出提醒。您还可以访问卡巴斯基完整的 APT 报告数据库，这是您的安全防御措施中的另一个强大的研究和分析组件。

优点

MITRE ATT&CK
报告中描述的所有 TTP 都被映射到 MITRE ATT&CK，通过制定相应的安全监控用例并划分优先级，进行差距分析，以及针对相关 TTP 测试当前的防御措施，提高检测和响应能力

有关非公开 APT 的信息
由于各种原因，并非所有高调的威胁都会公之于众。但我们会与我们的客户分享这些信息

特权访问
收到有关正在调查的最新威胁的技术描述（在向公众发布之前）

回顾性分析
在订阅期间，为您提供所有此前发布的非公开报告的访问权限

获取技术数据
包括一个扩展的 IOC 列表（以标准格式提供，包括 openIOC 或 STIX），并可访问我们的 YARA 规则

攻击者概况
包括疑似来源国家/地区和主要活动、使用的恶意软件系列、目标行业和地域以及使用的所有 TTP 的描述，并映射到 MITRE ATT&CK

持续不间断的 APT 活动监控
在调查期间获得可行的情报（与 APT 分布、IOC、命令和控制基础架构等有关的信息）。

RESTful API
安全工作流程的无缝集成和自动化

卡巴斯基数字足迹情报

随着您的业务增长，您的 IT 环境的复杂性和分布也在增长，这带来了一项挑战：在没有直接控制或所有权的情况下，保护您广泛分布的数字业务。动态和相互连接的环境让公司受益无穷。但与此同时，不断增加的互连也扩大了攻击面。随着攻击者变得更加熟练，您不仅要对您的组织的在线业务具备准确的了解，还要跟踪它发生的变化，并对与曝光的数字资产有关的最新信息作出反应，这至关重要。

企业在安全运营中使用了广泛的安全工具，但仍有数字威胁隐现：需要拥有适当的功能来检测和抵御内部人员活动，以及位于暗网论坛上的网络犯罪分子的计划和攻击方案，等等。为了帮助安全分析师探索攻击者对其公司资源的看法，及时发现他们可用的潜在攻击媒介，并相应调整防御措施，卡巴斯基创建了卡巴斯基数字足迹情报。

对您的组织发动攻击的最佳方式是什么？用于攻击您的最具成本效益的方式是什么？将您的企业视为目标的攻击者可以获得哪些信息？您的基础架构是否已在您不知情的情况下遭到入侵？

卡巴斯基数字足迹情报可以回答这些问题及其它问题，我们的专家将针对您的攻击状态综合出来，识别容易被利用的薄弱点，并揭示过去、现在以及已经计划好的攻击的证据。

该产品提供：

- 使用非侵入式方法进行网络边界清单检查，以确定客户的网络资源和曝光的服务，这些资源和服务是攻击的潜在入口点（比如无意中留在边界上的管理接口或配置错误的服务、设备接口，等等）。
- 对现有漏洞进行定制分析，根据 CVSS 基本得分、公共漏洞的可用性、渗透测试经验和网络资源（托管/基础架构）的位置进行进一步评分和综合风险评估。
- 识别、监控和分析任何处于活动状态的定向攻击或正在计划的攻击，以及针对您的公司、行业和运营地区的 APT 活动。
- 识别将目标锁定为您的客户、合作伙伴和订阅用户的威胁，他们受感染的系统可被用于攻击您的系统。
- 谨慎监控文本存储网站、公共论坛、博客、即时消息渠道、受限制的地下在线论坛和社区，以发现遭到入侵的帐户、信息泄漏或正在计划和讨论的、针对您的组织的攻击。

亮点

卡巴斯基数字足迹情报使用 OSINT 技术，结合对表网、深网和暗网的自动和手动分析，再加上卡巴斯基内部知识库，提供了可行的见解和建议。

可在卡巴斯基威胁情报门户上获得该产品。您可以购买四份季度报告（包含年度实时威胁警报），或者购买一份报告（激活六个月的警报）。

搜索表网和暗网，以获得与威胁您的资产的全球安全事件有关的准实时信息，以及在受限制的地下社区和论坛上搜索曝光的敏感数据。年度许可证包括每天 50 次跨外部来源和卡巴斯基知识库的搜索。

卡巴斯基数字足迹情报与卡巴斯基清除服务形成了一个单一解决方案。年度许可证包括每年 10 次清除恶意和网络钓鱼域的请求。

卡巴斯基 ICS 威胁情报报告

卡巴斯基 ICS 威胁情报报告对针对工业组织的恶意活动提供了深入的情报和更出色的认知，同时提供了在热门工业控制系统和基础技术中发现的漏洞的相关信息。报告通过一个基于 Web 的门户交付，这意味着，您可以立即开始使用该服务。

您的订阅中包含的报告

1. **APT 报告。**关于针对工业组织的全新 APT 和大规模攻击活动的报告，以及关于活跃威胁的最新动态。
2. **威胁形势。**关于工业控制系统威胁形势的重大变化、新发现的影响 ICS 安全水平的关键因素以及 ICS 面临的威胁的报告，包括地区、国家和行业特定的信息。
3. **发现的漏洞。**关于卡巴斯基在工业控制系统、工业物联网和各行业基础架构中使用的热门产品中发现的漏洞的报告。
4. **漏洞分析和抵御。**我们的顾问服务提供了卡巴斯基专家给予的可行建议，以帮助识别和抵御您的基础架构中的漏洞。

威胁情报数据使您能够

检测和预防

报告的威胁以保护关键资产，包括软件和硬件组件，同时确保技术流程的安全性和连续性

将

您在工业环境中检测到的任何恶意和可疑活动与卡巴斯基的研究结果相关联，以便将您的检测归因于相关的恶意活动，识别威胁并及时做出事件响应

根据

对漏洞范围和严重性的准确评估，对您的工业环境和资产进行漏洞评估，以就补丁管理制定明智的决策，并实施卡巴斯基建议的其他预防措施

利用

与攻击技术、战术和流程、最近发现的漏洞和其他重要的威胁形势变化有关的信息，以便：

- 识别和评估报告的威胁和其他类似威胁所带来的风险
- 规划和设计工业基础架构的变更，以确保生产的安全性和技术过程的连续性
- 根据真实案例分析来开展安全意识活动，以创建人员培训方案，并计划红蓝对抗演习
- 做出明智的战略决策，投资于网络安全并确保业务的复原力

卡巴斯基询问分析师

网络犯罪分子不断开发攻击企业的复杂方式。如今的网络威胁变化无常、增长迅速，突出表现在网络犯罪技术日益灵活多变。组织面临着各种原因引起的复杂事件：非恶意软件攻击、无文件攻击、离地攻击、零日漏洞利用以及所有这些组合成的复杂威胁，还有类似 APT 和定向攻击。

持续的威胁研究

使卡巴斯基可以发现、渗透和监控对手和网络犯罪分子经常光顾的封闭社区和地下论坛。我们的分析师利用此访问权限主动监测和调查最具破坏性的、臭名昭著的威胁，以及针对特定组织量身定制的威胁

在网络攻击可以瘫痪业务的时代，网络安全专业人员史无前例的重要，但是找到和留住他们不容易。即使您有一支稳固的网络安全团队，也不能总是期望您的专家们单打独斗抗击复杂威胁，**他们需要能够召唤第三方专家协助**。外部专家能够阐明复杂攻击或 APT 的可能路径，并且以最果断的方式提供可行的建议以消除它们。

询问分析师可交付的成果

（基于请求的统一订阅）

卡巴斯基询问分析师服务延伸了我们的威胁情报产品组合，使您可以对正在面临的，或者感兴趣的具体威胁请求指引和洞彻了解。该服务可让卡巴斯基强大的威胁情报和研究能力为您的具体需求提供定制服务，从而使您可以建立弹性防护，抵御针对您的组织的威胁。

APT 和犯罪软件

已发布的报告和现行研究的其它信息（除了 APT 或者犯罪软件情报报告服务之外）[1]

恶意软件分析

- 恶意软件样本分析
- 有关进一步修复操作的建议

威胁、漏洞和相关入侵指标的描述

- 具体恶意软件种类的一般性描述
- 威胁的其它上下文（相关哈希，网址，CnC 等）
- 具体漏洞信息（紧急程度，卡巴斯基产品中的相应保护机制）

暗网情报[2]

- 关于特定工件、IP 地址、域名、文件名称、电子邮件、链接或者镜像的暗网研究
- 信息研究和分析

ICS 相关请求

- 有关已发布的报告的补充信息
- ICS 漏洞信息
- 区域/行业的 ICS 威胁统计信息和趋势
- 有关法规或标准的 ICS 恶意软件分析信息

[1] 仅向具有主动 APT 和/或“犯罪软件情报报告”的客户提供

[2] 已包括在“卡巴斯基数字足迹情报”订阅中

TT服务优势

增强您的专业知识

根据需求随时联系业界专家，无需苦苦搜索、雇佣难以寻觅的全职专业人员。

加速调查

基于定制的详细上下文信息，有效地审视事件，并确定事件的优先级。

快速响应

使用我们的指导方案快速响应威胁和漏洞，以阻止通过已知向量进行的攻击

运作方式

“卡巴斯基询问分析师”可以单独购买，也可以和我们的任何威胁情报服务一起购买。

您可以通过卡巴斯基公司账户、我们的企业客户支持门户提交请求。我们将通过电子邮件进行回复，但是必要的话经您同意，我们可以组织会议电话和/或者屏幕共享会话。一旦您的请求得到接受，我们将通知您预计的处理时间框架。

服务使用案例：

- 阐明之前发布的威胁情报报告中的任何细节
- 就已提供的入侵指标获取额外情报
- 获得漏洞详情，以及如何保护系统，防止漏洞被利用的建议
- 关于您感兴趣的具体暗网活动获取额外详情
- 获取恶意软件综述报告，包括恶意软件行为、潜在影响和卡巴斯基观察到的相关活动的详情
- 使用简短报告提供的详细上下文信息和相关入侵指标分类，有效优先处理警报/事件
- 请求协助识别检测到的异常活动是否与 APT 或者犯罪软件有关
- 提交恶意软件文件进行全面分析，以理解所提供样本的行为和功能

扩充您的知识和资源

“卡巴斯基询问分析师”可让您在个案的基础上获得卡巴斯基研究员核心群组的服务。该服务可提供专家之间的全面沟通，用我们的独特知识和资源增强您的现有能力。

TT服务优势

全球覆盖

恶意或网络钓鱼域在哪里注册并不重要，卡巴斯基将向拥有相关法律权限的地区组织请求清除该域。

端到端管理

我们将管理整个清除过程，尽量减少您的参与。

完整的可见性

从请求登记到成功清除，您将在过程的每个阶段收到通知。

与数字足迹情报集成

对旨在破坏、滥用或冒充您的品牌/组织的网络钓鱼和恶意软件域，该服务与卡巴斯基数字足迹情报集成，提供有关的实时通知。单一解决方案是全面网络安全战略的一个重要组成部分。

卡巴斯基清除服务

挑战

网络犯罪分子创建恶意和网络钓鱼域，用于攻击您的公司和品牌。一旦发现无法迅速抵御这些威胁，就会导致收入损失、品牌损害、客户信任丧失、数据泄露等后果。但是，管理这些域的清除是一个复杂的过程，需要专业知识和时间。

解决方案

卡巴斯基每天阻止超过 15000 个网络钓鱼/诈骗 URL，并防止超过一百万次点击此类 URL 的尝试。我们在分析恶意和网络钓鱼域方面有着多年的经验，这意味着，我们知道如何收集所有必要的证据来证明它们是恶意的。我们将执行清除管理，使您能够迅速采取行动，以尽可能降低您的数字化风险，这样一来，您的团队就可以专注于其他优先任务。

卡巴斯基与国际组织、国家和地区执法机构（比如国际刑警组织、欧洲刑警组织、Microsoft 数字犯罪小组、荷兰警察局的国家高科技犯罪小组 (NHTCU) 和伦敦市警察局）以及世界各地的计算机应急响应团队 (CERT) 合作，为客户的在线服务和声誉提供有效保护。

运作方式

您可以通过卡巴斯基公司账户、我们的企业客户支持门户提交请求。我们将准备所有必要的文档，并将清除请求发送给具有必要法律权限的相关地方/区域当局（CERT、注册商等），以关闭该域。在请求的资源被成功清除的过程中，您会在每一步都收到通知。

轻松保护

卡巴斯基清除服务可在恶意和网络钓鱼域对您的品牌和业务造成任何损害之前，迅速抵御它们带来的威胁。对整个过程的端到端管理为您节省了宝贵的时间和资源。

主要优势

- 监测全球威胁，及时发现网络威胁，确定安全警报的优先级，并对信息安全事件作出有效的响应
- 防止分析师倦怠，让企业员工专注于真正的威胁
- 对不同行业和地区的攻击者所使用的战术、技术和流程的独特见解使我们能够主动防范定向复杂威胁
- 对您的安全状况的全面概览以及关于抵御策略的可行建议，使您能够将您的防御策略集中在被确定为主要网络攻击目标的领域
- 改进和加快的事件响应和威胁搜寻功能有助于减少攻击的“停留时间”，并大大减少可能的损害

结论

抵御当今的网络威胁需要对网络攻击者所使用的策略和工具进行 360 度全方位的观察。要生成这种情报并确定有效的对策，需要不断投入精力和具备高水平的专业知识。借助PB级的丰富的威胁数据、先进的机器学习技术和独特的全球专家库，卡巴斯基致力于为我们的客户提供来自全球的最新威胁情报，帮助他们即使在面对从未见过的网络攻击时，也能从容应对。

FORRESTER®

卡巴斯基在《2021 年 Forrester Wave：外部威胁情报服务》中被评为领导者

www.kaspersky.com.cn