卡巴斯基研究沙盒

卡巴斯基威胁归因引擎

Kaspersky Similarity

卡巴斯基威胁分析

kaspersky 引领未来

卡巴斯基威胁分析

Kaspersky Threat Analysis

面对潜在的网络威胁，你所做的决定以及如何做出这些决定至关重要。仅仅使用传统的反病毒工具不可能防止今天的针对性攻击。反病毒引擎只能阻止已知的威胁及其变异，而复杂的威胁发起者会利用他们掌握的所有手段来规避自动检测。SOC 每天处理的安全警报数量呈指数级增长。面对每天生成的恶意软件样本数量，有效的警报优先级排序、分类和验证几乎变得不可行。

将威胁情报、动态分析、威胁归因和相似性技术相结合，为检测以前从未见过的恶意对象提供了强大的工具。为了帮助安全研究人员随时了解现有和新出现的威胁，卡巴斯基提供了一个单一的弹性框架，以自动对可疑文件进行常规分析。

除了传统的威胁分析技术，如沙盒，卡巴斯基威胁分析使用最先进的归因和相关相似性技术为您提供支持，这是一种提供高效威胁分析的混合方法，以便您可以做出充分知情的决策和确保基础架构安全。

卡巴斯基威胁分析通过统一的 Web 和 RESTful 接口提供，允许用户设置特定参数以高效分析可疑对象。多个威胁分析工具集于一体，帮助您和您的团队从各个角度对情况进行分析，配备全面详细的报告，从而可让您迅速作出有效响应。

运作方式

沙盒技术

是强大的动态分析工具，可让人调查文件样本来源、收集基于行为分析的 IOC、并识别传统反病毒工具未检测到的恶意对象。

可提供云和本地版本。

沙盒

卡巴斯基研究沙盒直接从我们的实验室沙盒综合体发展而来，后者是一项二十多年来不断发展完善的技术。它融合了我们在持续的威胁研究中获得的关于恶意软件行为的所有知识，使我们能够每天检测 42 万多个新的恶意对象。它提供了一种混合方法，将行为分析和强大的反规避技术与人类模拟技术相结合。

技术部署在本地，可以防止数据泄露到组织外部。本地卡巴斯基研究沙盒还允许创建自定义执行环境进行分析，以量身定制用于实际环境，这提高了威胁检测的准确性和调查速度。

为什么要使用？

反病毒工具未检测到的可疑文件只能在其行为过程中显示恶意特征。卡巴斯基研究沙盒可让人模拟行为并突出显示危险操作。

产品亮点

Windows、Linux 和 Android 环境中的自动化对象分析

自定义映像允许跨 Windows 操作系统和应用程序（仅限应用于实际环境的应用程序）进行威胁分析

基于文件执行过程中获得的指标和数据得出威胁分数，显示所分析对象的危险级别

先进的反规避技术和人类模拟技术

手动上传样本，并提供增强的 REST API 以集成自动化工作流程

支持对 200 多种文件类型进行分析，并提供详细的分析报告

可以添加用于扫描网络流量的自定义 Suricata 规则，并与 Suricata 规则一起使用

1000+ 次独特搜索通过 MITRE ATT&CK 提取 TTP

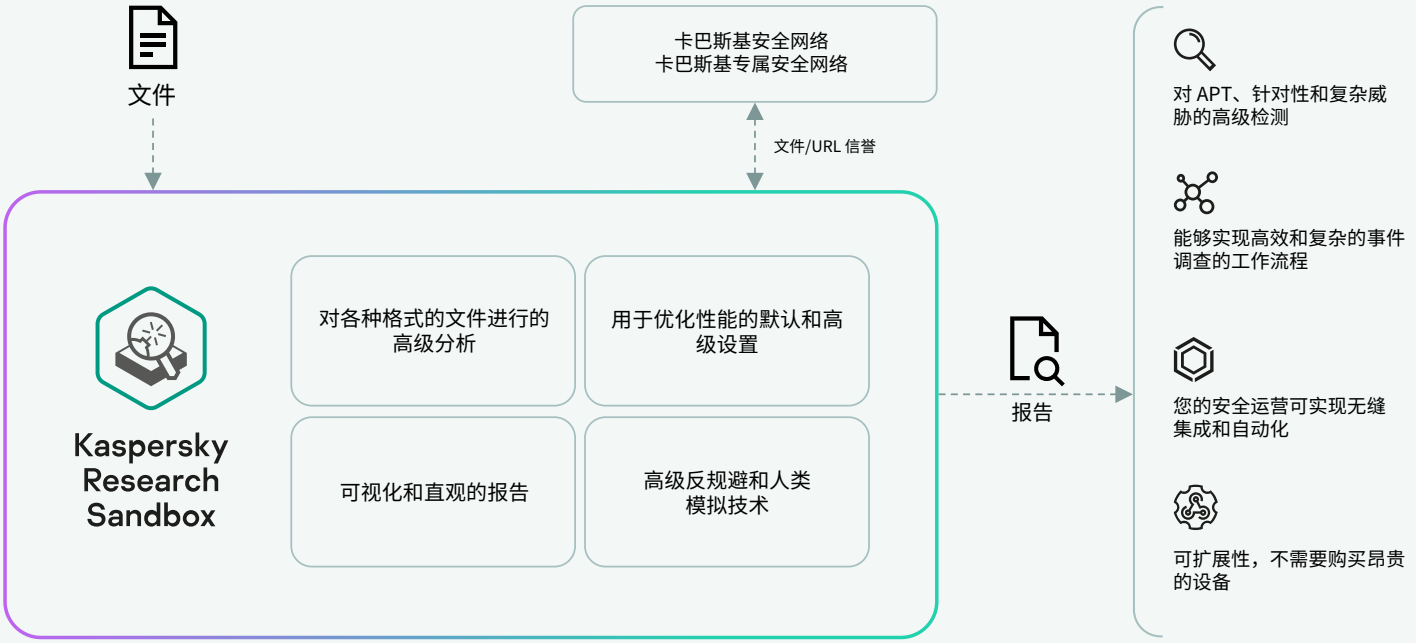
交互模式支持（预计 2024 年第一季度）

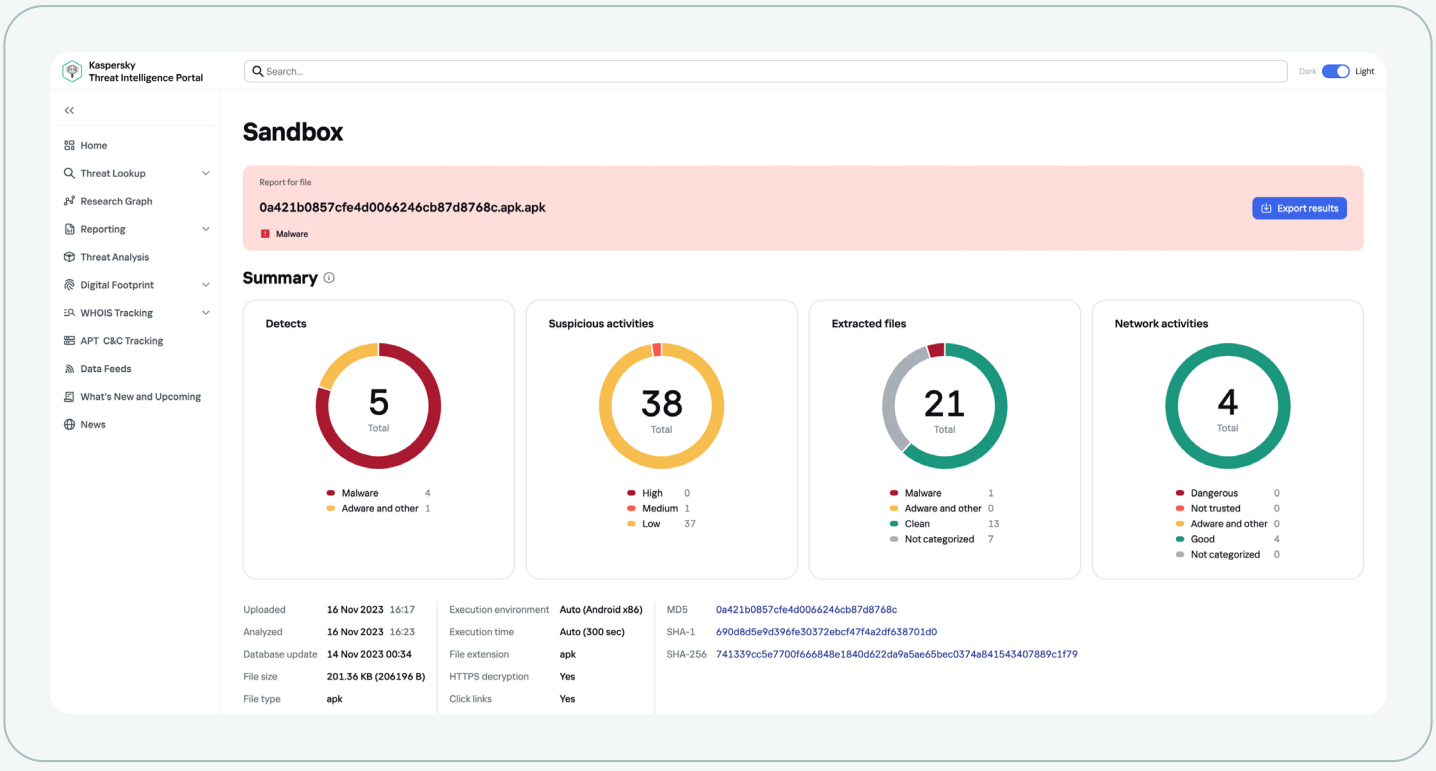
该产品支持裸机部署。硬件配置取决于所需性能，并且可以扩展。它需要至少一个独立的 ISP 连接（建议两个或更多的容错），每个通道 100 Mbps。

卡巴斯基研究沙盒基于专利保护的专有技术（专利号：US10339301）通过创建触发恶意软件执行的确切条件，研究人员只需一次尝试即可分析可疑文件/URL。

为了避免暴露，恶意文件可能会先调查是否处在虚拟机中，或者在沙盒运行过程中保持非活动状态。在这种情况下，这项专利技术可以加速虚拟机内的时间流逝，从而迫使恶意代码更早执行。

卡巴斯基研究沙盒高级别操作方案





详细的分析报告

一旦分析完成后，研究沙盒会提供关于分析样本的行为和功能的详细报告，让您定义适当的响应程序：

总结	关于文件执行/URL 浏览结果的常规信息。
检测名称	在文件执行期间注册的检测列表（AV 和行为检测）。
触发的网络规则	在分析来自执行对象的流量时触发的网络 Suricata 规则的列表。
执行地图	以图形方式表示的对象活动序列及其相互之间的关系。
可疑活动	可疑活动 — 注册的可疑活动列表。
屏幕截图	在文件执行/URL 浏览期间截取的一组屏幕截图。
加载的 PE 映像	在文件执行/URL 浏览期间检测到的加载的 PE 映像的列表。
文件操作	在文件执行/URL 浏览期间注册的文件操作列表。
注册表操作	在文件执行/URL 浏览期间检测到对操作系统注册表上执行的操作列表。
进程操作	文件与在文件执行期间注册的各种进程之间的交互列表。
同步操作	在文件执行/URL 浏览期间注册的已创建同步对象（互斥、事件、信号量）的操作列表。
已下载文件	在文件执行/URL 浏览期间从网络流量中提取的文件列表。
丢弃的文件	被执行文件保存（创建或修改）的文件列表。
HTTPS/HTTP/DNS/IP/TCP/UDP 等	在文件执行/URL 浏览期间注册的网络会话/请求详情。
网络流量转储 (PCAP)	网络活动可以用 PCAP 格式导出。
MITRE ATT&CK 矩阵	在模拟过程中记录的所有识别的进程活动都以 MITRE ATT&CK 矩阵的形式表示。

Kaspersky
Threat Analysis

Kaspersky
Threat Attribution
Engine

威胁归因

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。撇开所有的炒作不谈，威胁情报具有真正的价值，而威胁归因是其中一个关键因素。

可提供云和本地版本。

归因

卡巴斯基威胁归因引擎是一个独特的威胁分析工具，提供对知名恶意软件及其可能作者的起源的洞察。它将可疑文件快速连接到已知的 APT 威胁、参与者和活动，其中使用了独特的算法和包含 APT 恶意软件样本的特殊数据库，以及卡巴斯基专家在过去 25 年及更长时间里收集的业界最大的干净文件集。

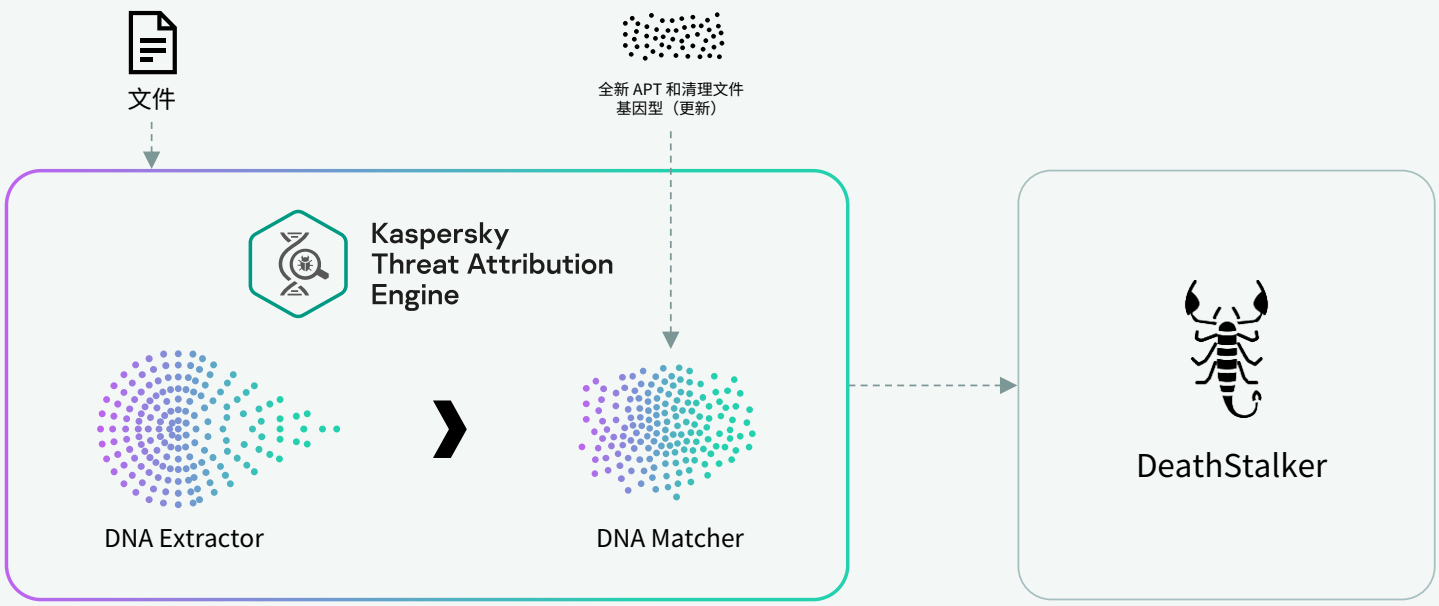
我们跟踪 1100 多个威胁发起者和活动，一年发布 200 多份威胁情报报告。我们正在进行的研究支持 APT 集合，其中包含超过 80,000 个文件，这些文件与自动化工具的使用一起，产生了非常准确的归因水平。

产品提供独特的类似样品比较方法，同时确保接近零的误报率。任何新的攻击都可以快速与已知的 APT 恶意软件、以前的针对性攻击和黑客组织联系起来，从而帮助您区分高风险威胁和不太严重的事件，这样您就可以及时采取保护措施，防止攻击者在您的系统中立足。卡巴斯基威胁归因引擎可以在采用“气隙”式物理隔离机制的安全环境中部署，从而限制任何第三方访问已处理的信息和提交的对象。

为什么要使用？

将文件归因于某个威胁发起者，与对该威胁发起者的了解一道，可以让人知道该样本特定于该对手在整个网络杀戮链条中的位置。反过来，它提供了在哪里查找其他 ICO/IoA 的知识，不会通过仅阻止一个特定文件而错过整个攻击。

卡巴斯基威胁归因引擎高级别操作方案



产品亮点

提供对精选数据存储库的即时访问（通过反病毒引擎），存储库涉及数千个 APT 参与者、样本和更广泛的威胁

对卡巴斯基专家调查的知名活动（400+）提供独特见解

允许高效执行自动或手动的威胁优先级划分和警报分类

允许添加不公开的攻击发起者和样本，以训练该产品检测与私人集合中的文件类似的样本

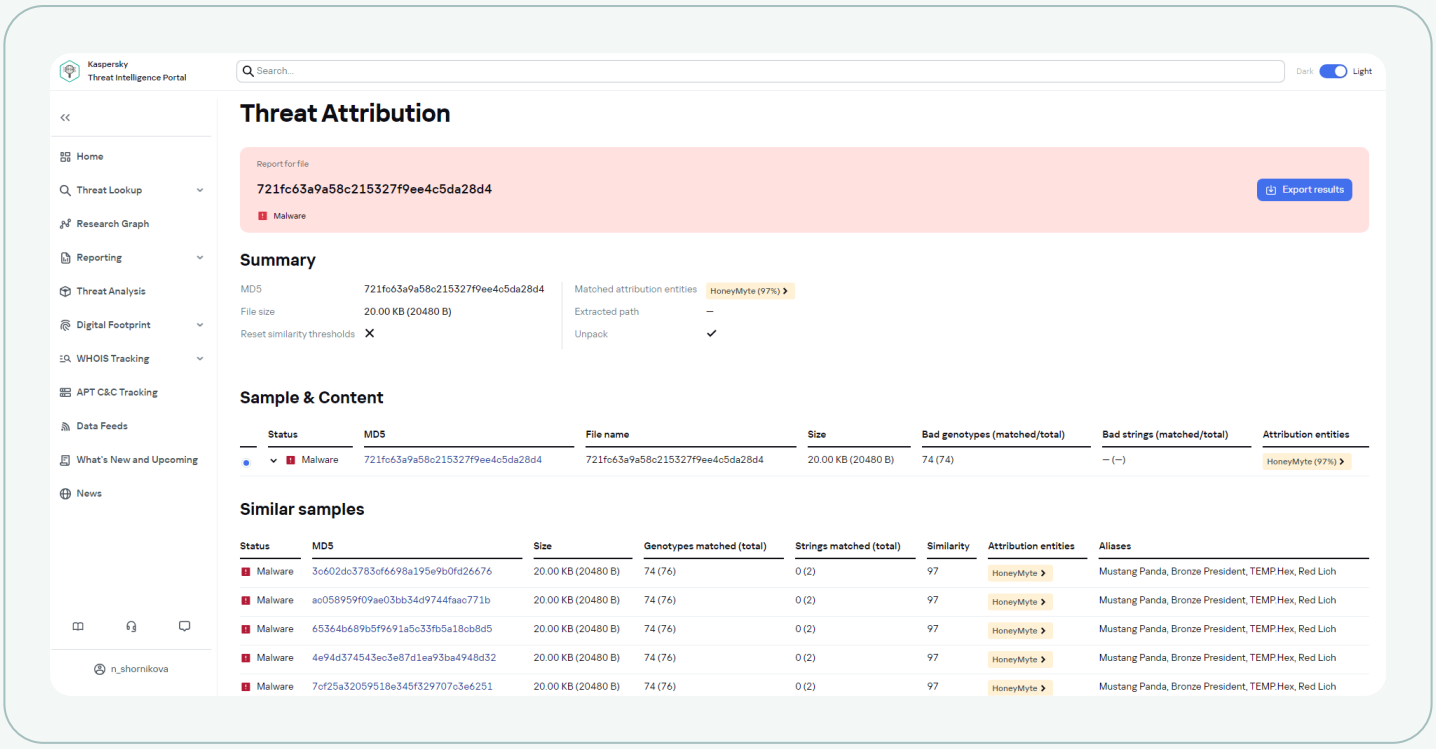
手动上传样本，并提供增强的 REST API 以集成自动化工作流程

支持在 Amazon Web Services (AWS) 等云基础架构上部署，从而实现快速的产品设置并节省成本，因为无需预先投资硬件

导出到 YARA 规则，以便进一步自动搜索/扫描类似文件或与第三方解决方案集成

导出为 STIX2.1 格式（TXT 和 JSON 格式也受支持），以便进一步自动分析安全日志或与第三方解决方案/安全控制集成

使用自定义密码解压缩受密码保护的存档的功能



专有搜索方法

为了将恶意软件链接到归因实体，卡巴斯基威胁归因引擎使用了一种独特的专有方法来搜索文件之间的相似基因型和字符串。该方法涉及：

分析样本的遗传学

通过从其代码中提取以下元素：

- 基因型——独特的二进制代码片段
- 字符串——独特的字符字符串

自动搜索所分析文件

以查看它们是否存在与先前分析的 APT 样本的类似的基因型和字符串，或者是否存在已经与归因实体相关联的基因型和字符串。

基于在 APT 样本中发现的相似基因型和字符串，

提供关于所分析样本的起源、相关归因实体以及此样本与已知 APT 样本之间的相似性的报告

Kaspersky
Threat Analysis

Kaspersky
Similarity

文件相似性

要建立有效的防线，并不总是需要通过目测来了解你的敌人。Kaspersky Similarity 可让人识别具有相似功能的文件样本，以抵御未知和规避式威胁。

云版本可通过卡巴斯基威胁情报门户获得。

相似性

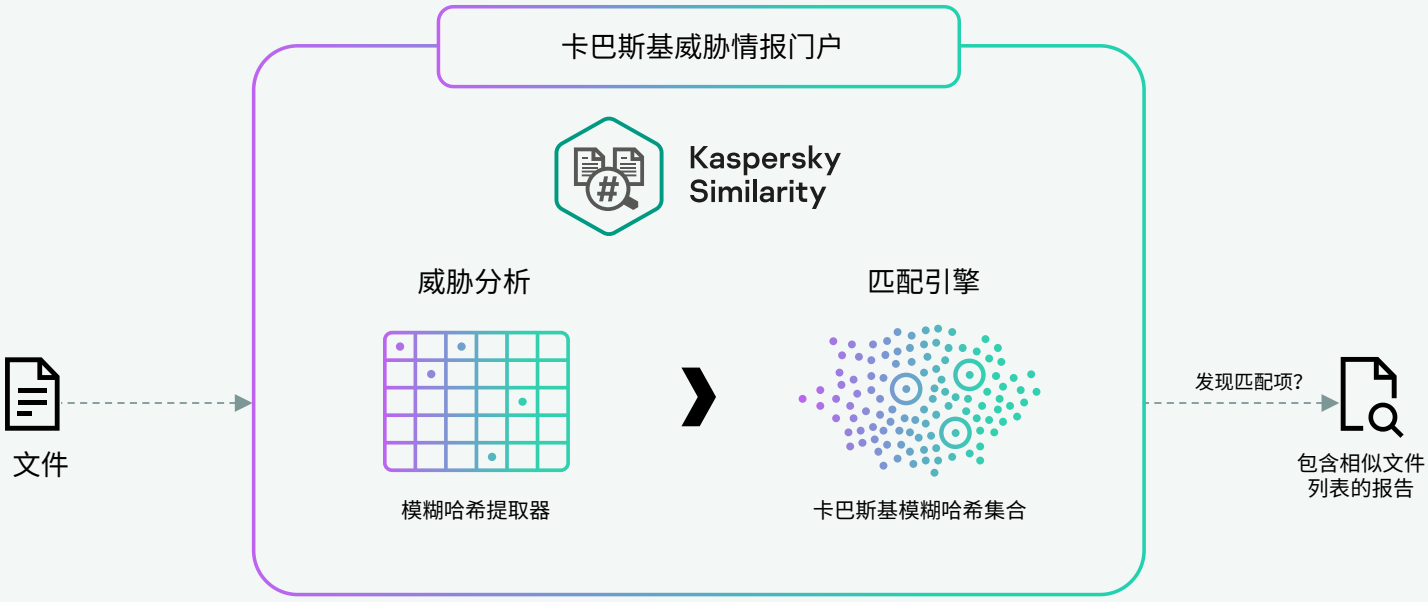
Kaspersky Similarity 是一项通过威胁情报门户提供给卡巴斯基研究沙盒和卡巴斯基威胁归因引擎用户的附加功能，有助于识别外观和行为方式相似的文件。

使用卡巴斯基专家发明的尖端技术，利用超过 50 种独特的相似性哈希类型，对原始文件进行搜索和计算相似文件。这可确保准确和高置信度的相似性结果。

为什么要使用？

查找类似（例如规避）恶意软件，并在您的基础架构中查找它，以确信对手对样本的轻微更改仍然在您的安全雷达上。该技术与归因区别开来：即使没有归因，类似的恶意软件文件也可以找到。

Kaspersky Similarity 高级别工作方案



相似性报告书

每个文件都有特定的格式、使用的打包程序、部分、字符串、导入表等。卡巴斯基专家创建了一组哈希，以根据这些属性确定不同文件之间的相似性。Kaspersky Similarity 可让用户提交可疑文件，提取其模糊哈希，并将其与卡巴斯基威胁数据库中存在的文件的模糊哈希进行比较。如果找到匹配项，它会为卡巴斯基已知的 TOP 类似恶意文件生成哈希列表，并按相似性得分排序。该报告包含每个类似文件的元数据的附加上下文：

- 相似性置信度
- 文件状态（恶意软件，广告软件或其他）
- 威胁名称
- 第一次和最后一次检测的时间戳
- 点击量（检测）
- 文件哈希
- 文件类型
- 文件大小

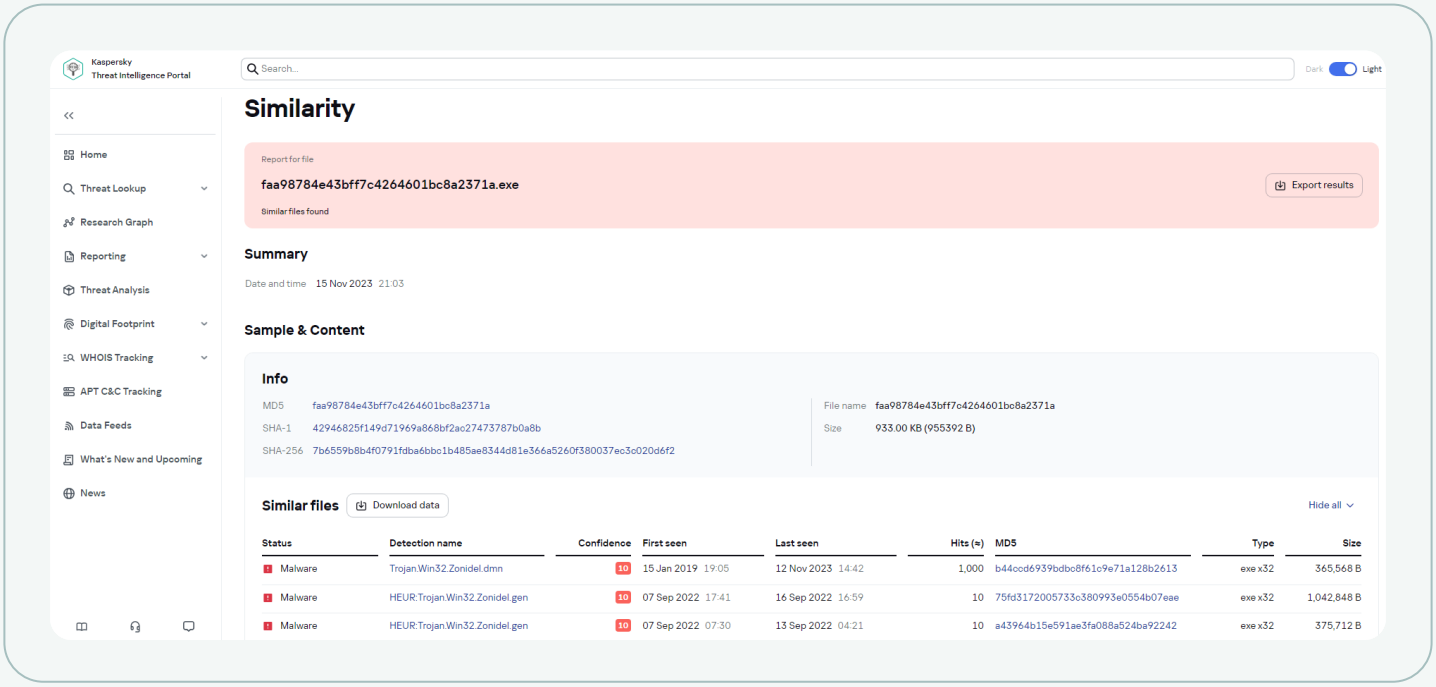
功能重点

利用过去 25 年多来收集的业界最大的恶意文件和干净文件数据库之一，从而实现最大的复盖范围，以获得最高的比较准确性

手动上传样本，并提供增强的 REST API 以集成自动化工作流程

免费提供给卡巴斯基研究沙盒和卡巴斯基威胁归因用户，以增强这两种技术的有效性，并提供有关被分析文件的全面信息

卡巴斯基专家已经广泛使用它来探索新的威胁，以在我们的产品中提供更高的威胁保护，并根据独立测试定期得到最高评级确认：



卡巴斯基威胁分析使用案例

卡巴斯基威胁分析为检测未知威胁提供了成熟的首选工具，可广泛应用于以下场景：

事件响应

揭露规避式威胁

可疑文件的静态/动态分析

揭示新恶意软件与某些威胁发起者的关系，以了解可能的进一步攻击步骤

威胁捕获

对通过报告接收的 IoC 进行基础架构扫描

查找对流行的干净文件进行的潜在恶意修改

识别未知和已知恶意文件之间共享的 IoC

恶意软件分析

未知威胁分析

查找相关恶意软件以帮助对混淆文件进行逆向工程

卡巴斯基威胁分析是一款灵活的研究工具，内含互相连接的组件，可以对可疑对象进行综合、多层次评估以对高级攻击进行识别和分类。它可帮助 SOC 团队、安全研究人员和恶意软件分析师随时了解现有和新出现的恶意软件相关威胁，使他们能够快速确定优先级并解决关键威胁，从而更有效地修正他们。

Kaspersky Threat Analysis

了解更多

www.kaspersky.com.cn

© 2023 AO Kaspersky Lab。注册商标和服务标志归其各自所有者所有。

#kaspersky
#bringonthefuture