kaspersky 引领未来

Kaspersky Threat Attribution Engine

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。威胁情报的真正价值绝不仅仅限于信息安全行业大肆宣传的新兴资源，威胁归因或许是威胁情报领域最主要的关注点和争论点。

产品亮点：

- 支持即时访问有关数百个 APT 攻击发起者和样本的精选数据存储库
- 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，并提供开放式 API 以集成自动化工作流
- 可以在采用“气隙”式物理隔离机制的安全环境中部署，以保护您的系统和数据并满足任何合规性要求
- 维护所有提交内容的绝对隐私和机密性，避免暴露敏感信息

这其中有着明确的理由。由于调查和反向工程流程十分复杂，因此从检测到响应高度复杂威胁之间的平均时间往往过于漫长。在很多时候，如此漫长的时间间隔足以让攻击者伺机达成目标。正确和及时的归因不仅有助于将事件响应时间从几小时缩短到几分钟，而且还可以减少误报数量。

辨别针对性攻击、对攻击者进行概况分析并为不同威胁发起者创建归因因素是一项长期而全面的工作；可能需要耗费数年时间。多年来，创建切实可行的归因还需要积累大量的数据，还需要具备相关调查经验和精湛技能的研究人员团队。通常，研究人员会跟踪不同群体的活动，并通过零散的方式在数据库中填充信息。这种数据库会成为可作为工具分享的宝贵资源。

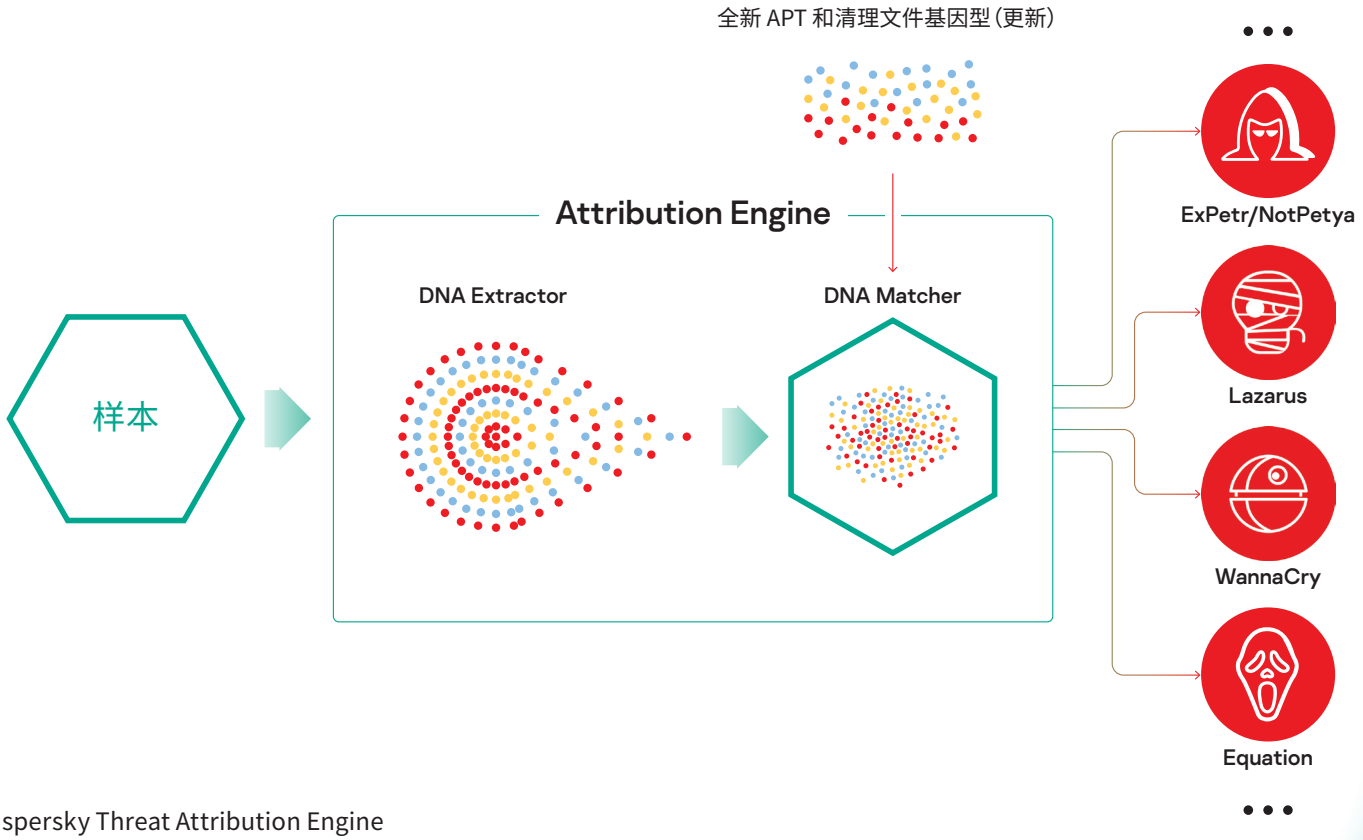
Kaspersky Threat Attribution Engine 整合了 Kaspersky 专家在过去 22 年间收集的 APT 恶意软件样本和未受感染文件的数据库。我们对超过 600 个攻击发起者和攻击活动进行跟踪，每年发布超过 120 份 APT 情报报告。我们目前开展的研究支持包含 6 万多个文件的大型 APT 集合，能保证契合现实。它能利用自动工具改善错误标记检测，并尽可能提高归因的准确性。

该产品采用独特的方法来比较样本的相似性，同时确保零误报率。它可以将新攻击与已知 APT 恶意软件、先前的针对性攻击和黑客组织快速关联起来，从而有助于在不太严重的事件中发现高风险威胁，并及时采取保护措施，防止攻击者在系统中站稳脚跟。

运作方式

Kaspersky Threat Attribution Engine 以自动化的方式分析恶意软件的“基因”，探寻与先前研究的 APT 样本和相关联的攻击发起者相似的代码。它会将“基因型”（即经过分解的文件的小二进制碎片）与 APT 恶意软件样本数据库进行比较，并提供有关恶意软件来源、威胁发起者和与已知 APT 样本的文件相似性的报告。此外，该产品还允许安全团队向其数据库添加不公开的攻击发起者和对象，并对该产品进行训练，以检测与您的私人集合中的文件相似的样本。借助 Threat Attribution Engine，原本需要数年之久的归因过程如今仅需几秒钟即可完成。

该产品可以在采用“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。该 Engine 可通过一个 API 接口与其他工具和框架相连接，从而在现有基础架构和自动化流程内实现归因。



Kaspersky Threat Attribution Engine

有关相关 APT 攻击者的详细信息，可在 Kaspersky APT Intelligence 报告[1] 中找到。如果您是 Kaspersky APT Intelligence Reporting 的订阅用户，我们为您提供调查和发现的独家最新访问权限，包括在每份 APT 报告中以各种形式提供其揭示的全部技术数据，包括从未公开公布的那些威胁。

Kaspersky Threat Attribution Engine 通过支持国家网络安全机构和商业安全运营中心 (SOC) 建立有效的事件管理流程，进一步扩展和增强了 Kaspersky 产品组合。

Kaspersky Attribution Engine 显著加强了安全运维，有助于：

- 快速将文件归因于已知的 APT 攻击发起者，以揭示网络事件背后的动机、方法和工具；
- 快速评估您是攻击目标还是连带受害者，以建立适当的遏制和响应程序；
- 根据 Kaspersky APT Intelligence Reporting 告中提供的有关 APT 攻击系列、可作为行动依据的威胁情报，确保有效、及时地缓解威胁。

1 订阅 Kaspersky APT Intelligence Reporting 服务需要单独购买

网络威胁新闻：www.securelist.com
IT 安全新闻：business.kaspersky.com
中小企业 IT 安全：kaspersky.com/business
企业 IT 安全：kaspersky.com/enterprise

www.kaspersky.com.cn

屡获殊荣独立自主透明可信我们致力于打造一个通过科技改善生活的更加安全的世界。我们保护世界安全的目的，是让地球上的每个人都能享受它带来的无限机会。确保网络安全，创造更安全的明天。

如需了解更多信息，请访问 kaspersky.com/transparency

Proven.
Transparent.
Independent.