卡巴斯基云沙盒

kaspersky 引领未来

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**

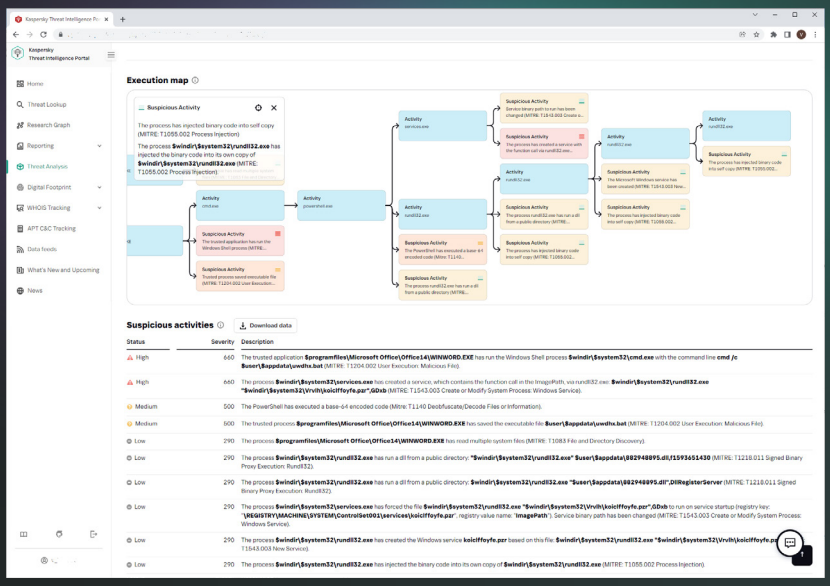
主动威胁检测和抵御

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。

www.kaspersky.com.cn