云研究沙盒

kaspersky 引领未来

沙盒技术

沙盒技术是功能强大的工具，可用于调查文件样本的来源，根据行为分析收集 IOC 以及检测以前未发现的恶意对象。

卡巴斯基研究沙盒

根据文件或 URL 行为做出智能决策，同时分析进程内存、网络活动等，这是了解当前复杂的针对性定制威胁的最佳方法。

如今的恶意软件会使用各种各样的方法来避免执行其代码，以防暴露其恶意活动。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。因此，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 38 万多个新的恶意对象。这项强大的技术部署在本地，还可以防止数据泄露到组织外部。

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。卡巴斯基研究沙盒还允许自定义用于分析的系统映像，根据实际环境进行定制，这提高了威胁检测的准确性和调查速度。

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
- 本地部署确保没有数据会泄露到组织外部
- 先进的反规避技术和人类模拟技术
- 手动提交文件/URL 和 RESTful API
- 支持对 100 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，并与开箱即用的 Suricata 规则一起使用
- 该产品支持裸机部署，并且可以根据所需性能轻松扩展

卡巴斯基研究沙盒高级架构

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。它的每个通道需要 100 Mbps 网络连接，并且需要至少一个独立 ISP 连接（建议两个或更多连接，以实现容错）。ISP 应该知道恶意流量并做好应对准备。

卡巴斯基研究沙盒基于获得专利的专有技术（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。

如果恶意软件的目标是沙盒中缺少的特定应用程序，可能不会显示其恶意行为。为解决这个挑战，研究人员必须查看日志、了解缺少的应用程序、将该应用程序添加到虚拟机并再次运行此过程。恶意软件尝试访问应用程序时，该专利系统会拦截这种尝试。它不会等到文件执行结束，而是会暂停进程来创建所需的应用程序以及内容。

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。

卡巴斯基研究沙盒是检测未知威胁的首选工具。它比任何其他解决方案都更成熟，更专注于高级威胁。

www.kaspersky.com.cn