卡巴斯基威胁数据源

kaspersky 引领未来

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。

- IP 信誉源
- 哈希源 (WIN/*nix/ MacOS / AndroidOS / iOS)
- URL 源（恶意、网络钓鱼和 C&C）
- 勒索软件 URL源
- APT IOC 源
- 漏洞源
- 被动 DNS (pDNS) 源
- 物联网 URL 源
- 允许列表源
- ICS 哈希源
- 等等

Kaspersky Threat Data Feeds

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

www.kaspersky.com.cn