# 卡巴斯基询问分析师

kaspersky 引领未来

# 卡巴斯基询问分析师

网络犯罪分子不断开发攻击企业的复杂方式。如今的网络威胁变化无常、增长迅速，突出表现在网络犯罪技术日益灵活多变。组织面临着各种原因引起的复杂事件：非恶意软件攻击、无文件攻击、离地攻击、零日漏洞利用以及所有这些组合成的复杂威胁，还有类似 APT 和定向攻击。

## 持续的威胁研究

使卡巴斯基可以发现、渗透和监控对手和网络犯罪分子经常光顾的封闭社区和地下论坛。我们的分析师利用此访问权限主动监测和调查最具破坏性的、臭名昭著的威胁，以及针对特定组织量身定制的威胁

在网络攻击可以瘫痪业务的时代，网络安全专业人员史无前例的重要，但是找到和留住他们不容易。即使您有一支稳固的网络安全团队，也不能总是期望您的专家们单打独斗抗击复杂威胁，**他们需要能够召唤第三方专家协助。**外部专家能够阐明复杂攻击或 APT 的可能路径，并且以最果断的方式提供可行的建议以消除它们。

## 询问分析师可交付的成果

（基于请求的统一订阅）

**卡巴斯基询问分析师**服务延伸了我们的威胁情报产品组合，使您可以对正在面临的，或者感兴趣的具体威胁请求指引和洞彻了解。该服务可让卡巴斯基强大的威胁情报和研究能力为您的具体需求提供定制服务，从而使您可以建立弹性防护，抵御针对您的组织的威胁。

### APT 和犯罪软件

已发布的报告和现行研究的其它信息（除了 APT 或者犯罪软件情报报告服务之外）[1]

### 恶意软件分析

- 恶意软件样本分析
- 有关进一步修复操作的建议

### 威胁、漏洞和相关入侵指标的描述

- 具体恶意软件种类的一般性描述
- 威胁的其它上下文（相关哈希，网址，CnC 等）
- 具体漏洞信息（紧急程度，卡巴斯基产品中的相应保护机制）

### 暗网情报[2]

- 关于特定工件、IP 地址、域名、文件名称、电子邮件、链接或者镜像的暗网研究
- 信息研究和分析

### ICS 相关请求

- 有关已发布的报告的补充信息
- ICS 漏洞信息
- 区域/行业的 ICS 威胁统计信息和趋势
- 有关法规或标准的 ICS 恶意软件分析信息

[1] 仅向具有主动 APT 和/或“犯罪软件情报报告”的客户提供

[2] 已包括在“卡巴斯基数字足迹情报”订阅中

## TT服务优势

### 增强您的专业知识

根据需求随时联系业界专家，无需苦苦搜索、雇佣难以寻觅的全职专业人员。

### 加速调查

基于定制的详细上下文信息，有效地审视事件，并确定事件的优先级。

### 快速响应

使用我们的指导方案快速响应威胁和漏洞，以阻止通过已知向量进行的攻击

## 运作方式

“卡巴斯基询问分析师”可以单独购买，也可以和我们的任何威胁情报服务一起购买。

您可以通过卡巴斯基公司账户、我们的企业客户支持门户提交请求。我们将通过电子邮件进行回复，但是必要的话经您同意，我们可以组织会议电话和/或者屏幕共享会话。一旦您的请求得到接受，我们将通知您预计的处理时间框架。

## 服务使用案例：

- 阐明之前发布的威胁情报报告中的任何细节
- 就已提供的入侵指标获取额外情报
- 获得漏洞详情，以及如何保护系统，防止漏洞被利用的建议
- 关于您感兴趣的具体暗网活动获取额外详情
- 获取恶意软件综述报告，包括恶意软件行为、潜在影响和卡巴斯基观察到的相关活动的详情
- 使用简短报告提供的详细上下文信息和相关入侵指标分类，有效优先处理警报/事件
- 请求协助识别检测到的异常活动是否与 APT 或者犯罪软件有关
- 提交恶意软件文件进行全面分析，以理解所提供样本的行为和功能

## 扩充您的知识和资源

“卡巴斯基询问分析师”可让您在个案的基础上获得卡巴斯基研究员核心群组的服务。该服务可提供专家之间的全面沟通，用我们的独特知识和资源增强您的现有能力。


www.kaspersky.com.cn