样本智能分析平台

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2019-10-11 11:02:14

网络安全现状

近年来，以 APT（Advanced Persistent Threat，高级持续性威胁）攻击为代表的高级网络威胁愈演愈烈，传统网络攻击、高级针对性攻击、敲诈勒索病毒等传统和新型攻击手段结合，企业遭受的恶意攻击和潜在威胁层出不穷。

典型攻击案例包括：

- 2017年5月，一款名为 Wannacry 的勒索软件袭击全球网络，影响近百个国家和地区以及上千家企业和公共组织，此次袭击事件被认为是迄今为止最大的勒索交费事件。
- 2017年6月，乌克兰等欧洲国家遭受 Petya 勒索程序的大规模攻击。机场、银行、船舶公司、石油公司、私人公司和政府系统都遭到了攻击。
- 2017年10月前后，某 APT 团伙活动频繁，目前确认国内外部分公司、政府机构的对外网站已经受到攻击，我国广东省为重灾区。

什么是样本智能分析平台

腾讯哈勃 - 样本智能分析平台（下文中也称哈勃）是恶意样本智能分析鉴定平台，依靠深度沙箱中自研的动态分析模块、静态分析模块以及稳定高效的任务调度框架，实现自动化、智能化、可定制化的样本分析；通过建设大规模分析集群，沉淀了包括深度学习在内的多个高覆盖率的恶意样本检测模型，能够分析得知样本的基本信息、触发的行为、安全等级等信息，从而精准高效地对现网中的恶意样本进行打击。

部署模式

哈勃是一款提供纯 SAAS 服务的产品。客户无需安装任何硬件或软件，仅需按照 API 文档的格式要求，提交样本进行分析，在降低安全运维成本的同时，也减降低了恶意样本对客户真实网络环境产生危害的风险。

用户收益

哈勃作为恶意样本智能分析鉴定平台，能为您带来如下收益：

- 检测网站存储的恶意文件，降低恶意文件借助网站进行二次传播的风险。

- 识别已知和未知的漏洞攻击，捕获 APT 攻击。
- 识别钓鱼邮件、小型破解网站、小型论坛中携带的勒索病毒、漏洞利用文档和其它类型的恶意样本。
- 阻止企业内网 OA 网站、FTP 服务、邮件或内部通讯工具等文件通过分享方式造成的恶意样本横向传播。

适用领域

哈勃适用于多种场景，包括但不限于：

- 提供行为日志，辅助安全人员进行判断。
- 接入现有安全产品，自动对样本进行智能分析和判定。

产品功能

最近更新时间：2019-05-07 17:46:21

样本提交分析

哈勃具有强大且全面的样本分析能力，支持分析以下格式的文件：

- Windows 可执行文件格式：.exe、.dll、.sys、.msi 等。
- Linux 可执行文件格式：.elf 等。
- 文档类文件格式：.doc、.docx、.docm、.dotm、.xls、.xlsx、.xlsm、.xlsb、.xltm、.xltx、.xlam、.ppt、.pptx、.potx、.ppsx、.pptm、.potm、.ppsm、.rtf、.pdf、.swf 等。
- 压缩文件格式：.rar、.zip、.7z 等。
- Android 应用格式：.apk 等。

行为分析报告

哈勃扫描后为您提供细致的扫描报告，报告文件为 PDF 格式，报告内容包括样本恶意属性判定、动态行为、联网威胁情报等，帮助您快速识别恶意威胁样本，保障业务安全。

产品优势

最近更新时间：2018-12-14 17:37:45

哈勃是恶意样本智能分析鉴定平台，其产品优势如下：

多平台支持

哈勃支持企业中最常用到的 Windows 和 Linux 操作系统，对于不同平台上传播的样本都能进行虚拟化运行、行为捕获和恶意鉴定。同时针对企业办公移动化的趋势，哈勃也支持对 Android 平台上的样本进行分析，进一步阻止来自智能手机等移动终端的攻击。

种类全面

目前哈勃支持常见的可执行文件（包括 32 位和 64 位）、脚本、文档、压缩包、ELF 文件、APK 文件等多种文件格式的分析，同时具备脚本内容提取、文档宏提取、多重压缩包解压、密码猜解、格式推断等多种高级能力，可以支持对现网绝大部分文件种类进行全面的处理。

行为丰富

哈勃采用自研的动态行为监控模块，具备高可疑行为监控、网络发包监控、隐私窃取监控等能力，全方位监控样本运行后的动态行为，行为覆盖的全面性在国内外多个沙箱的对比中表现优异。支持 json、pdf 等多种格式，将丰富的样本行为向用户进行展示和自动化接入处理。

挖掘高危

哈勃对常规恶意样本具有极高的识别率，同时有针对性地诱发和监控漏洞攻击、勒索病毒等高危风险行为特征，包括利用漏洞、加密文件、修改登录密码等典型行为，从而更准确地识别已知和未知的高级攻击。

样本防逃逸

哈勃采用远程沙箱的 SaaS 化服务，其自身具有高度真实模拟，样本不会在客户网络中真实执行，并且样本具有反沙箱对抗的能力，能够防止样本从沙箱中逃逸，因此可以在不对真实环境产生危害的前提下，诱导和捕获更多的样本行为。