山石云·影

分秒级检测
并阻断未知威胁

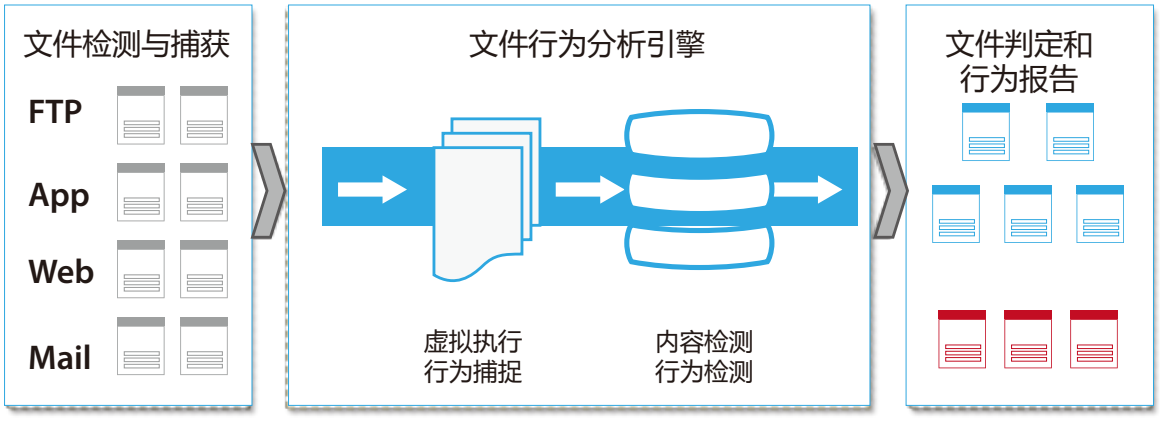
销售与服务热线:400-828-6655

安全的变化和挑战

当前恶意软件防护正面临巨大的挑战，一方面随着恶意软件变种技术和免杀技术的发展，恶意软件变种正变得多样化和容易化，黑客用几秒钟到几分钟的时间就可以制作出恶意软件的新变种，而基于特征库匹配方法的网络防病毒方案很难检测出变种的恶意软件，变种和免杀技术的发展需要有未知威胁检测方案。另一方面，威胁越晚被检测到，对企业的影响就越大，同时恶意软件的传播速度也越来越快，近期爆发的勒索软件 WannaCry 一天左右就传播到 100 多个国家，造成几十万台电脑中招，所以，针对最新的恶意软件或者恶意文件的变种防护必须要快。

利用沙箱的行为技术检测未知威胁

沙箱技术是 Gartner 认可的一项高级威胁检测技术，可实时的检测未知威胁，并被主流安全厂商广泛使用。同传统的基于特征匹配的检测方式不同 ,沙箱技术通过分析文件运行时的行为来发现隐藏在其中的未知威胁。沙箱会模拟文件执行的操作环境，同时动态监控和分析文件的执行。如果这些未知文件在虚拟环境中启动了攻击行为，沙箱可以捕获这些攻击行为，进而判定该文件为恶意软件。



上图显示了沙箱系统的工作流程：首先从网络流量中提取出文件，然后对文件的运行行为进行分析，根据行为分析，判断文件是否为恶意软件，并输出详细的行为分析报告。

免杀技术可以改变恶意软件的静态特性，但是不会改变该恶意软件的动态行为特征。所以沙箱技术可以有效对抗最新的免杀技术，发现未知恶意软件的威胁和攻击，从而对多层次立体防御系统的构建起到关键的作用。

山石云•影：分秒级检测未知威胁

山石云•影是通过云端技术构建的高性能沙箱集群，可以实现对未知威胁和恶意软件的检测。防火墙连接到山石云•影后，可以将特征匹配无法识别的文件传送到山石云•影进行动态行为分析。山石云•影可以模拟文件的真实运行环境，并通过触发文件的各种行为来发现隐藏其中的未知威胁，从而使得安全管理员可以及时调整安全策略，阻止进一步的数据泄露。

山石云•影采用了三个层次的威胁分析模块，以确保恶意软件检测的效率和精度。

- **静态分析模块**

文件的静态特征分析，如文件类型识别、文件格式识别、已知的恶意软件特征码等。另外，通过多种前置过滤技术，如 URL 白名单、文件签名验证、云端海量样本库等，对未知文件进行过滤，减轻沙箱的处理压力。

- **沙箱动态分析**

山石云•影实现了对多种操作系统和运行环境的模拟，可以在非常接近实际生产环境的仿真环境里触发文件的各种操作，并使用机器学习模型进行评判。

- **云智能**

应用山石网科全球网络节点上发现的威胁情报信息，如恶意软件特征码、钓鱼网站和恶意域名等，对比可疑文件的静态和动态行为信息，对每一个文件都可以给出风险评分，而不是简单地判定为黑或者白。

山石云•影综合利用上述多种检测方法来判断一款未知文件是否是恶意软件，从而尽可能的避免误判，达到较高的检测精度。

山石云•影：威胁情报共享实现全局威胁防御

山石云•影基于全局威胁情报共享，可将任一单点检测到的未知威胁情报信息共享到所有接入站点，将单点未知威胁检测变全局已知威胁防御。针对那些尝试大规模爆发和传播的恶意软件，一旦在某个云接入点被沙箱检测出来，其他接入点可以在几秒内同步到相关恶意软件的情报信息，其他接入点无需将恶意软件送至云端沙箱环境检测，就能快速基于共享到的威胁情报信息进行威胁阻断。山石云·影的威胁情报共享，可有效阻断恶意软件大规模传播。

山石云•影优势及特点

- **动静结合、全面检测**

云端的海量恶意样本库可到 10 亿 + 级别，可以通过快速匹配发现上传的文件是否存在恶意行为。通过沙箱技术模拟文件的真实运行环境，通过触发文件的各种行为，包括创建进程、修改注册表、回链请求等进行分析，第一时间发现隐藏其中的未知威胁。

- **云端架构、即时启用**

与山石网科现有的安全产品无缝连接，包括山石网科防火墙、山石云•界、入侵检测及防御系统、山石云•景等。无需新增硬件，无需中断业务，即时启用。

- **对加密流量提供保护**

随着 SSL 加密技术的普及，越来越多的应用采用 HTTPS 方式部署，同时恶意软件也借助加密技术来躲避检测。山石云•影可以对 SSL 加密流量进行解密及深度检测，精确还原出加密流量中的各种文件并进行行为分析，使恶意软件无所遁形。

- **反沙箱技术的对抗策略**

山石云•影支持对反虚拟识别技术的识别和检测，通过隐藏沙箱运行的相关信息，包括内核模块、进程名称、注册表中的相关信息等，山石云•影能够最大程度模拟真实的运行环境。对于恶意软件的躲避措施，山石云•影通过模拟人工操作、交互操作、接管 API 等措施，可以最大限度的触发恶意代码的各种动作。

- **详尽的报表和威胁呈现**

在检测到恶意软件和未知威胁后，山石云•影会及时给出安全警报，这些警报会第一时间通过防火墙的管理界面在用户端呈现。同时，山石云影可提供恶意文件的详细行为报告，包括网络行为、进程行为、文件行为、文件关键信息等，并通过 Kill Chain 分析来还原攻击过程，为安全管理员提供威胁处理建议。

- **基于威胁情报共享的全局威胁防御能力**

山石云•影基于全局威胁情报共享，将一个接入点检测到的未知威胁情报信息共享到所有站点，将单点未知威胁变全局已知威胁情报信息，快速阻断变种软件的大规模传播。

山石云•影应用实例

Locky 勒索软件的攻击场景：

1. 黑客通过钓鱼邮件或水坑式攻击的方式，将恶意文件投送到用户端。
2. 用户不小心执行了恶意文件，被安装后门，恶意文件还可能进一步在内网扩散。
3. 恶意软件通过后门与 C&C 服务器通信，进一步下载勒索软件。
4. 勒索软件加密本地文件，弹出弹窗进行勒索。

山石云•影检测：

将邮件中附件进行提取，传送到沙箱进行安全分析。发现存在恶意行为：创建下载进程，回链到外部网站，下载可执行文件。从而判断该邮件为钓鱼邮件，随后防火墙上自动执行预定义安全策略，阻断内网资产和 C&C 服务器之间的通信。