云边端协同的勒索软件防护框架

■ 文 / 仇学博，王小号

勒索软件是一种恶意软件，它会对目标设备上的数据进行加密，并要求支付赎金以解密数据。勒索软件自 1989 年诞生至今，经历了几十年的发展和演变，曾一度消退，但随着互联网的快速发展，又出现了爆炸式的增长，且复苏后的勒索软件变种已经具备了十分强的隐蔽性和攻击性。报告《X-Force 威胁情报指数 2022》指出，勒索软件再次占据 2021 年最主要攻击类型的榜首。DoppelPaymer 组织曾在 2021 年 2 月，成功入侵起亚美国的数据库，向现代汽车集团索要 2000 万美元作为赎金，次事件已影响了起亚美国的自助支付服务、网上平台以及电话支持系统。2021 年 5 月 7 日最大燃油运输管道商科洛尼尔被 DarkSide 勒索病毒攻击，导致 5500 英里输油管系统被迫停运。后续接连出现的如 Cuba 勒索病毒攻击超 49 个美国关键基础设施也向各国敲响了警钟。勒索对象已经从个人转变为大型企事业以及相关基础设施，但是勒索攻击的入侵点还是以企业中的终端设备为主，因此，对于端点设备的入侵防护依然是抵御勒索病毒的关键。



1. 云边端架构

云边端协同架构是一种利用云端和边缘设备的协作和融合，实现对多个终端设备的统一监管和防护的技术方案，相较于传统的单点防护策略，云边端协同架构具备三大优势。第一，通过对多个终端行为的监控，不仅可以观察到单点设备的异常状态；还可以通过分析异常端点与其他终端设备之间的网络通信，检测横向移动等跨主机的异常行为，为安全防护增添一份保障。第二，通过将终端行为分析任务转移至云端，可以解放终端设备，实现对用户无感的终端设备监管，同时可以进一步降低终端设备的硬件配置，减少成本。第三，可以利用云端服务器下发统一策略，终端设备执行决策，实现对海量终端的高效、自动化管控。如图 1 所示，云边端架构主要由以下三部分组成：

1.1 终端

终端设备指易受病毒感染并需要进行安全监管的设备，如台式机、笔记本、手机等。终端需提供日志数据以反映用户操作，为后续异常行为分析方法提供数据基础。借助 Kellect 内核日志采集器可以实时获取端侧设备产生的系统内核日志，Kellect 在 Windows 端的实现是基于 ETW（Event Tracing for Windows）提供的内核事件采集服务，实时获取系统原生事件，并开启多线程并行化地执行日志解析、语义修正等操作，增强了内核日志的语义表征；在 Linux 端的实现基于 eBPF 框架，通过挂载系统中不同类型的追踪点实现对用户行为的监听。为每台终端设备预先部署 Kellect，实现对于端侧用户行为日志的细粒度采集，并在接入边端设备后，将本地产生的系统日志实时传输至边缘侧进行处理。

此外，终端设备需要开放与云端服务通信的端口，以接收来自云端下发的策略管控指令；同时部署指令解析服务与策略实施服务，实现对云端策略的实时响应。

1.2 边端

边缘设备是指连接一定数量的终端设备并具有一定计算能力的设备，主要实现对来自各个终端产生的日志数据的收集、汇总、处理，是边缘计算的执行端，为云端服务器提供压缩处理之后格式统一的日志数据。边端设备可以是提供分布式事件存储和流处理服务的 Kafka 系统，每台边端设备接入一批终端，为不同的终端设备

创建各自的日志传输接口，通过 Kafka 中的 Streams 接口实现对日志数据的过滤、压缩处理，减小冗余数据，同时基于规则存储终端产生的可疑日志事件作为以后溯源处理的基础。

此外，各边缘设备需接入至云端服务器所处网络，以便云服务器可以实时拉取各终端的日志数据进行威胁分析。

1.3 云端

云计算的中心节点，提供强大的计算能力、存储能力等，接收来自边缘侧处理的终端日志数据，通过对日志数据的行为模式分析，达到对异常行为的检测目的。为实现这一目标，在云端需要建立与边缘设备的协调机制，以实现对海量终端日志数据的传输、同步等。该协调机制可以根据场景需求，采用不同的调度策略，如负载均衡、定制优先级、动态调整等，以提高系统针对不同应用环境的效率和稳定性。

云服务器检测到某个终端存在异常活动或终端设备之间存在异常通信时，可以通过下发策略管控指令实现对指定终端设备的监管。这需额外配置定制化的终端设备管控策略与异常行为检测策略，如定期数据备份、软件监管、异常检测规则库、异常行为检测模型等，以保障终端设备的安全性，并降低因员工安全意识薄弱导致的勒索病毒入侵现象，减少内部财产损失。

2. 勒索软件防护策略

2.1 安全预防策略

借助于云端设备高效的协调能力，可以实现对终端集群的实时策略下发，完成对终端设备的统一管控。云服务器可以通过下发多种预防策略，实现对勒索软件的预防，降低因员工安全意识不足导致的勒索病毒入侵现象。以下列举了部分可以通过云端服务器下发统一的预防策略：

■备份策略

通过下发数据备份策略，定期实现对终端设备重要数据（例如文档、图片、视频等）的增量或差异备份，将备份数据存储至云端或其他离线设备等安全的地方，以减少因数据丢失或被加密造成的风险。

■补丁策略

及时下发补丁策略，及时更新系统和应用程序的安全补丁，例如 Windows 更新、杀毒软件更新、浏览器更新等，修复已知的漏洞，防止勒索软件利用旧漏洞入侵系统；制定和执行补丁的管理流程，例如确定补丁的优先级和安装顺序，制定补丁的备份和恢复计划。

■权限限制

通过云端控制终端用户访问设备的权限，使用最低权限原则，为用户和程序分配合适的权限，避免不必要的访问和操作，减少勒索软件的影响范围；限制网络和设备的访问权限，例如使用防火墙和 VPN 等技术来保护网络的安全，禁止或监控外部设备的连接和使用，隔离或隐蔽重要的服务器或数据。

■行为监管

限制终端用户可以访问的外部网站以及使用的软件，避免用户进入钓鱼网站或者开放高危端口。此外，还可以安装可靠的防病毒软件和防火墙，定期扫描和拦截可疑的文件和网络流量，防止勒索软件感染；禁止客户端修改或删除系统或应用程序的重要文件或设置，例如注册表、启动项、服务等。

■安全培训

大部分安全隐患都源自人们安全知识的匮乏。基于云端设备对终端的统一管控，可以定期下发安全宣传内容，例如，警示员工避免点击或下载可疑的链接、附件、网站等，不要随意支付赎金或与攻击者沟通，及时报告并应对勒索软件攻击。提高用户和员工对勒索软件的认识和警惕，增强员工安全意识。

2.2 异常检测策略

当勒索病毒通过零日漏洞或社工手段入侵终端设备后，云端服务器将对各终端产生的系统内核日志进行实时分析，通过识别异常行为模式发现可疑活动。异常行为检测方法大致可以分为基于专家经验定

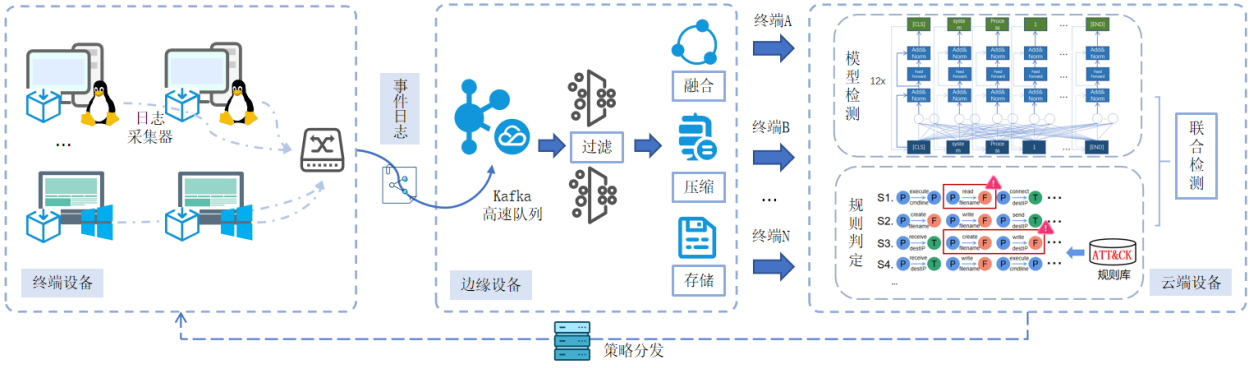


图 1 云边端架构的勒索软件防护

制的异常行为检测规则与基于机器学习模型的异常行为识别。两种方式分别具备以下优缺点：

■基于规则的勒索软件检测方案由专家根据自身专业知识，对勒索软件样本与攻击行为特征进行分析，定制一系列针对勒索病毒检测的静态与动态规则。通过将日志数据与定制的规则进行匹配以识别是否存在可疑活动。有学者对大量的勒索病毒样本执行的文件 I/O 操作进行分析，总结了 3 类勒索加密文件的 I/O 访问模式，通过监控这三类 I/O 操作来判断是否有恶意加密行为产生；还有学者定制了一款能够实时检测勒索病毒加密行为的机制，分别以文件操作行为和文件内容变化做为特征来检测恶意加密。这些基于规则的方法具备检测准确率高、误报率低的优点，但是缺点是定制的规则容易过时，不能适应恶意软件的变化和多样性，需要安全专家定期编写和维护规则或模式。

■利用机器学习模型进行勒索软件检测的方法需要从大量已标注的勒索软件和正常软件产生的日志中提取行为特征，并以此训练一个分类模型完成检测任务。例如，有文献提出结合文件熵和机器学习的方法，计算用户备份在云端的各类文件的参考熵值，作为判断后续备份的文件是否被恶意加密的依据；还有通过获取进程运行时产生的注册表、API 调用、文件等操作以及对二进制文件通过静态分析提取的部分数据作为特征，利用逻辑回归分类模型判定是否存在恶意操作。基于机器学习检测的方法的优点是能够自动学习不同勒索软件共同的行为模式，适应勒索变体的多样性，提高检测的准确性和效率，具备较强的泛化能力；缺点是需要大量的标注数据，同时可能存在过拟合和欠拟合的问题。

为实现对终端设备异常行为高效精准检测，可以结合以上两种方法，借助专家经验与 AI 模型强大的学习能力，将知识融入至模型学习的过程，提升模型在少样本情况下的学习能力，增强模型对异常行为模式的识别率。通过在云服务器中部署规则集和 AI 检测模型，借助服务器的强大计算能力，实时并行分析多终端设备产生的日志数据，可以检测出单点异常与由横向移动引发的跨终端的异常通信。

3. 结语

综合来说，基于云边端架构的勒索软件防护框架适用于企业、高校等具备一定网络规模且被勒索软件视为主要攻击对象的场景。借助于云端服务器的协同管控能力，该框架实现了对终端设备异常行为的实时监管，并将系统日志的处理、分析任务转移至边缘设备，解放了终端设备的算力；同时，通过云端一站式的策略部署、分发，可以实现对终端设备的统一管理并减少人力开销。借助云服务器对终端日志联合分析的能力，可以检测到病毒横向移动等传统单点检测无法感知的异常行为。因此，该框架实现了对于勒索软件更为精准的检测与预防。

基金项目：

浙江省教育厅一般科研项目“基于系统内核日志分析的勒索软件检测方案研究”（Y202249647）；浙江省重点研发计划项目（2021C01117）；浙江省自然科学基金/重大项目（LD22F020002）。

（浙江工业大学，浙江 杭州，310014）



