DOI:10.19353/j.cnki.dzsj.2020.18.011

基于等级保护的新型终端安全防护技术

国家电网公司西北分部　李　欣　智　远
国网陕西省电力公司信息通信公司　刘　颖　姚亚强　李　霖

随着数据量的增长，加密数据流的应用以及APT风险长期潜伏，传统终端安全防护已经不能适应当前的终端环境。而且传统的防护技术在系统资源占用越来越高的同时效率却在下降，并且主要局限在终端单点安全防护。随着国家对信息安全技术与网络安全保护迈入2.0时代以及信息技术的发展，基于机器学习的大数据分析技术可以实现快速响应、降低误报，有效处置终端安全防护问题。

计算机终端从发明到全面普及，安全问题始终伴随其发展史。随着互联网、工业网、物联网及5G技术的普及，病毒、木马、恶意软件也已经完全不同于以往，这不但影响了系统的正常运行，同时给企业和个人带来了不小的经济损失。传统的静态特征库、启发式杀毒、黑白名单等技术已经无法应对，现今各样的病毒木马，新兴的机器学习及端点检测与响应安全防护技术可能会成为未来一段时间内端点安全防护技术的主要发展方面。

本文从安全建设方面出发，对建立安全可信的计算环境做了初步的研究，提出了终端安全防护的技术方向。

1　终端安全防护现状

目前，终端安全防护主要面临两个方面的问题。

从外部环境来说，传统终端安全防护已经不能适应当前的终端环境，终端硬盘存储空间往往是TB级的数据量，保存有百万甚至千万级的音频文件、视频文件、照片、各类文档、系统文件等。网络速度不断提升，网络视频、音频、超大邮件附件等数据，都在占用终端流量。终端商各种应用软件P2P、VPN、HTTPS、SSL VPN等加密数据流量，可能携带病毒或恶意软件，使得无法对数据流进行安全评估。同时，病毒木马的工具化、流程化生产，导致新的病毒和木马等恶意软件变种速度越来越快，杀毒软件特征库越来越大，而且误报率越来越高。

从安全防护技术来说，一是当前终端防护技术落后，传统的病毒特征库，采取静态特征对抗静态代码，低效误报率高；二是新型病毒木马的行为也越来越复杂和多样性，安全分析技术需要越来越复杂的分析逻辑，系统资源占用越来越高；三是高级持续威胁（APT）具有更高级、更持续、更隐蔽，更有针对性，潜伏期更长等特点，传统仅基于端点的安全防护技术难以发现和拦截；四是终端安全技术主要局限在终端自身单点安全防护，而很少关注大规模的终端日志、网络事件流量、网络数据流向等宏观数据所能挖掘和发现的安全风险。并且未形成一体化防护，防护能力分散，兼容性与普适性不达标，不同系统主机需采用不同的防护方案，导致管理维护工作量大。

随着国家对信息安全技术与网络安全保护迈入2.0时代以及信息技术的发展，TB级别的大数据分析、机器学习也被引入到安全领域以解决所面临的困境。其将在我国推行信息安全等级保护制度的过程中起到非常重要的作用,指导用户开展信息系统安全等级保护的建设整改、等级测评等工作。

2　终端安全防护技术

2.1　高级持续威胁(Advanced Persistent Threat,APT)防护

由于高级持续威胁（APT）的特殊性，使得其较难被发现。要发现未知系统安全风险，需要通过挖掘海量的大数据，主要包括：主机和服务器日志、应用系统日志、安全设备和网络设备日志、网络流量信息、网络访问路径信息等，结合正常用户日志和网络访问行为，用机器学习的方法定义新的安全检测模型来检测未知的攻击行为。利用不断积累的海量大数据，进行持续不断的机器学习，对正常用户的行为建立正常用户模型，从而发现内部用户的异常操作行为。

2.2　端点检测与响应（Endpoint Detection amd Response,EDR）

端点检测与响应是近来出现的一种端点安全防御新思路。与传统的端点安全防护技术不同，其主要以大数据和人工智能的威胁分析来解决传统依赖于杀毒软件、防火墙、各种终端助手、端点准入技术所所无法解决的互联网新型恶意软件。该框架形成基于终端资产的预防、防御、检测、响应的自适应、可视化、持续闭环的体系。面对来自外部威胁、内部威胁、高级威胁、业务异常等终端风险闭环管理的完整性方面，能进行实时的检测分析，提前预

警防范并及时响应对应的安全策略；能自动化智能化的阻止攻击、修补漏洞、隔离风险、取证分析、追溯攻击源头。端点检测与响应技术基于防护技术系统、资产管理体系、安全运营和威胁响应体系的融合，更好地识别安全风险，通过平台、产品和模块的自动联动更高效解决问题和保护各类资产的安全性。

端点检测与响应的实际应用已经趋于成熟，国内外有多家安全厂商开始推广EDR技术的终端安全防护方案。企业采取主动防御的方式进行终端安全防护也越来越有必要。

2.3 基于机器学习的优势

机器学习涉及到多门交叉学科，是人工智能（AI）领域的心机，通过基于模式的机器学习算法来模拟人类的认知过程，在大数据的分析和挖掘时，自动分析发现多种因素作用下的内在的规律，从而进行一定程度的判断和预测。只有通过机器学习技术的应用，结合端点检测与响应（EDR）的技术构架，才可能实现当前环境下病毒、木马和各种恶意软件及高级持续威胁（APT）的有效防护，可以说机器学习是EDR技术的核心。

(1)在端点检测与响应（EDR）中，机器学习主要应用于端点用户和系统的正常操作行为和异常行为的提取，通过捕获大量的端点静态和动态的用户和软件行为特征向量，采用机器学习的思想进行端点用户和系统行为的训练建模和分类检测，得出该使用场景下用户和系统的正常和异常行为模型。利用该模型可以更加高效地检测出端点的异常操作行为。

对于终端本地大量的文件，通过建立文件信誉机制，包括本地信誉、全网信誉、云端信誉解决黑白名单问题，实现快速发现高风险文件，降低文件重复检测的资源占用，同时利用云端大数据分析平台和云端的威胁情报系统，做到风险的提前防护。

(2)利用人工智能，进行大数据的深度学习建立数千维度的算法模型，多维度的检测技术，发现高检出率和低误报率的模型并不断完善算法和训练，通过持续学习、自我进化，实现不依赖于静态特征码的无特征病毒检测，有效鉴定未知病毒。利用云端威胁情报及时对区域热点病毒家族进行特征基因提取，通过机器学习和沙盒行为分析，快速应对检测病毒的各种新变异、新变种。

使用基于大数据分析的文件信誉技术、人工智能的恶意文件检测技术、流行病毒的基因特征检测技术、病毒恶意行为的行为链规则检测技术，对已知文件进行快速过滤，重点提升未知威胁文件的检测能力，构建完善的防御体系，全面预防、有效检测。

2.4 端点检测与响应技术的应用

EDR 的暴力破解检测方案将端点探针（Agent）部署在终端上，端点探针将会在终端上持续监控密码的爆破行为日志，如果发现了有人进行密码的爆破，将可以设置对特定IP 进行一段时间的自动封停，同时，支持对暴力破解事件攻击源IP加入黑名单，已加入黑名单的IP无法访问网内所有终端，避免终端被爆破成功。

传统的后门文件检测是基于特征码的检测技术，严重依赖于特征库，很难及时检测新的变种，检测效率也随着特征库的变大而迅速降低。采用机器学习的检测方法，通过先利用语法分析器生成语法树，基于语法树提取出危险特征以及正常特征，特征包含数量统计特征、比率特征、覆盖面特征、字符串熵、运算符号统计等，在学习已标记样本特征数据来构建检测模型，然后利用此模型对样本进行检测判定，该方法不仅可以正确检测出已有样本数据，对未知样本也有很好的检测效果。

对后门文件的检测综合利用文件信誉库、静态分析、机器学习、运行行为分析等手段对文件进行判断，相比流量侧的防御，检测方案将会更全面地分析文件。可根据需要进行后门定时扫描任务一旦发现后门文件，可以立刻自动隔离或仅上报不隔离。

总结：EDR利用于云计算和机器学习技术实现异常行为分析、海量文件检测、未知病毒检测、高级持续威胁检测等，完整覆盖端点安全防御全生命周期，同时实现主动发现和清除来自外部或内部的安全威胁，显著提升终端应对APT和未知威胁的主动防御能力，满足终端安全控制点的要求，帮助用户实现等级保护建设。此外，通过统一的EDR控制端下发针对不同终端的安全策略，通过统一终端管控平台，可对各类型终端统一进行安全基线管理。

当前高速互联网和大数据应用环境下的终端安全防护，区别于传统的终端安全防御技术，安全工作任重而道远，依法依规开展安全防护工作，以守法底线之不变应对安全形势之万变，才能在瞬息万变的网络安全复杂环境下占据主动。