基于APT攻击链的网络安全态势感知

吴鹏，皇甫涛

（中国移动通信集团重庆有限公司，重庆 401420）

摘　要　为提升应对APT攻击的安全防御能力，信息网络安全态势感知技术越来越被关注，以实现安全事件的预测与预防。文章从该角度出发分析网络安全态势感知研究的必要性，从网络安全态势感知研究框架出发，详细阐述目前国内外网络安全态势感知研究的体系结构和主要方法，对网络安全态势感知技术进行了归纳总结并对未来感知技术的趋势进行了展望。

关键词　态势感知；APT攻击链；态势评估；态势预测

中图分类号　TN918　　**文献标识码**　A　　**文章编号**　1008-5599（2015）12-0043-05

DOI:10.13992/j.cnki.tetas.2015.12.011

1　网络安全态势感知定义及处理流程

网络安全态势感知定义：基于网络安全态势及安全日志记录的检测和分析，对未来某段时间内的网络安全状态进行预测、预警及展示的安全技术。网络态势感知概念于 1999 年被 TimBass 等人首次提出，从建立网络空间态势感知框架，利用入侵检测分布式传感器实施数据融合，对网络安全态势实施评估，再不断衍生出其它模型，网络安全态势感知系统关键技术、框架模型被不断地改进、细化和完善。

网络安全态势感知处理流程如图 1 所示。

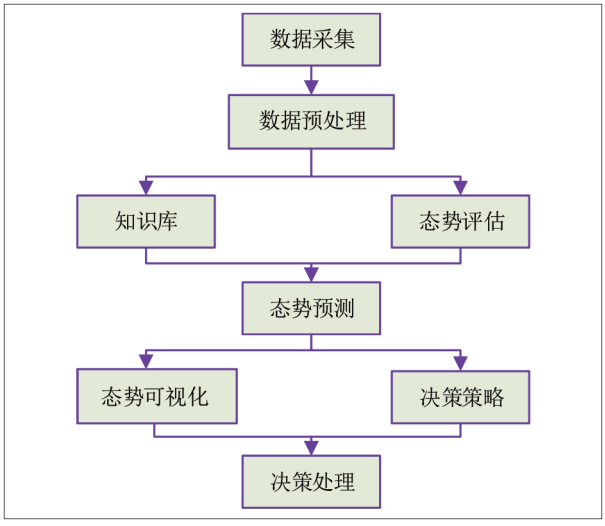

图1　网络安全态势感知处理流程

2　网络安全态势感知现状

网络安全态势感知作为安全研究领域新热点之一，对网络环境内安全要素进行采集、分析，并预测未来发展趋势。网络安全态势感知已在数据融合、评估方法、体系结构等领域取得相应研究成果，但基本属于理论学术层面偏多，实际应用案例偏少。

收稿日期：2015-11-16

随着 APT 攻击越发多样化和复杂化，新常态下的安全威胁可利用的攻击面越来越宽，可覆盖网络、操作系统、数据库、Web、APP 等各种层面和应用，依靠传统入侵检测提供的安全检测信息难以满足现阶段需要，伴随互联网业务的多样化、个性化发展，尤其是对于互联网上新业务新技术的不断应用，更需要通过大数据分析方式来采集、分析并判断或预测网络威胁行为，更为直观地给展现出 APT 攻击的整个动态过程。

3 网络安全态势感知的关键技术研究

按照网络安全态势感知的实现步骤，分析每个流程，阐述当前安全态势感知的研究方法及关键技术。

3.1 网络安全态势的常用体系结构

网络安全态势体系结构主要有 B-S、C-S、基于 Agent 的模型、基于云计算的感知模式等。

目前应用较广泛的是基于 Agent 的模型，具有异步计算、并行求解、动态执行、智能化路由等优点，可极大提高态势感知的速度和效率。

基于云计算的网络安全态势感知模型，可有效解决网络态势信息生成准确性低和节点处理能力不足的问题。云计算的并行计算方法和分布式文件存储方法能很好解决大规模数据的高效处理及存储问题。基于云计算的网络安全态势感知模型研究属于本领域的新方向之一，从技术层面来讲还处于研究阶段。

3.2 基于 APT 攻击链的网络安全态势体系结构

从具体的内容角度上讲，我们将基于 APT 攻击链的网络安全态势体系结构的内容分为 3 个方面。

（1）全新调整传统漏洞、安全威胁的规则划分维度，解决单一告警、单一事件无状态统计的局面，起到重新按照事件划分攻击链的作用。

（2）采用数据处理中心或专业云对规则新分类告警进行日志分析，从大数据分析角度实现智能化处理。

（3）APT 攻击整个过程可分阶段、动态化、直观地予以展现。

3.3 基于 APT 攻击链的数据采集技术

数据采集技术主要分为单一要素和多源数据，基于 APT 攻击链的网络安全态势感知模型也属于多源异质融合的类型，通过部署 IDS（入侵检测系统）、防火墙、流量监控、漏洞扫描器等网络安全设备，融合多个类型的传感器数据，采用被动收集网络安全日志和主动获取网络配置信息相结合的方式，结合数据处理中心或专业云端对各类数据进行一系列融合处理，以实现大数据关联分析。建立了具有攻击行为、网络安全服务和安全态势 3 个层次的网络安全态势感知模型。

对于态势感知而言，多数据源信息采集方式的感知误差率小于单源采集方式，但其信息融合技术、数据处理的难度却更大。当前网络安全态势感知的数据采集来源主要有设备配置信息、设备运行日志信息、安全工具警报信息及日志信息等。以上信息基本涵盖全部所需的安全信息。有效要素选取和信息提取方式，对态势感知研究将起到决定性作用。

为构建新常态下的威胁感知态势，结合海量数据的分析，形成以新规则为主导，以新分类为依据，以攻击链为引领的新型网络安全态势感知分析模型；随着网络攻击行为的变化、升级形成颠覆式的有状态的攻击行为检测预警方案；以客观的多元化的攻击形态为基础，彻底改变固有思维模式中的“一攻一报”的单点威胁告警模式，从大数据挖掘的角度出发，通过智能化的数据分析，真正超越传统 IDS 检测告警的形态，形成新常态下安全威胁感知态势的解决思路。

3.4 基于 APT 攻击链的数据预处理技术

数据预处理工作主要分为以下两个方面。

（1）数据格式统一，将采集的所有不同类型的文件转换为统一格式的文件或数据结构。

（2）对转换格式的数据进行分析，在海量数据中排除与安全态势感知无关的噪声数据，将重复的属性数据进行合并，实现数据的合并和约减。针对 APT 攻击链所引发出的海量攻击信息，为达到及时、全面、高效的数据预处理，应部署数据处理中心或专业云端，并通过

配置数据预处理策略来实施操作。

3.5 基于 APT 攻击链的态势评估

网络安全态势评估有两层含义。

（1）对采集信息实施实时地数据融合和关联分析，及时有效展现网络的实际运行状况。

（2）采取合理的技术及方式对历史数据进行分析，以预测潜在的网络攻击，即态势预测。

针对 APT 攻击链的构建和威胁感知的效果，应从不同层次、不同角度建立层次性指标体系，细化各类指标信息，层次化评估网络安全态势。为适应新攻击行为和攻击手法将规则分为 5 个攻击阶段：探测扫描阶段、渗透攻击阶段、攻陷入侵阶段、安装工具阶段和恶意行为阶段。

（1）探测扫描阶段：包括了攻击者在攻击前对目标的扫描，包括网络扫描、系统扫描、端口、漏洞扫描等，扫描行为是攻击入侵的前期准备阶段，通过信息收集，掌握目标机器的系统，漏洞信息，对进一步进行入侵攻击有事半功倍的效果。

（2）渗透攻击阶段：该阶段是已经对目标机器做了扫描，或是直接对目标机器进行攻击，包括利用栈、堆方面的漏洞，利用 Web 系统平台方面的漏洞，逻辑配置错误方面的漏洞，内存破坏方面的漏洞等，对目标主机发起攻击。

（3）攻陷入侵阶段：该阶段表示了目标主机已经不被黑客成功攻陷，接下来攻击者可以做他想做的事情，攻陷阶段的表现形式如 FTP 登录成功、Telnet 猜测成功等。

（4）安装工具阶段：指在攻击者成功进入目标主机后在目标主机中安装恶意软件，木马程序或是直接挂马等，通过这些恶意的工具实现与黑客的控制链接，下载其它恶意软件等。

（5）恶意行为阶段：即攻击者在目标主机安装完恶意软件后，恶意软件在目标主机产生的恶意行为包括控制链接，对主机进行恶意操作等。

新型规则攻击分类如图 2 所示。

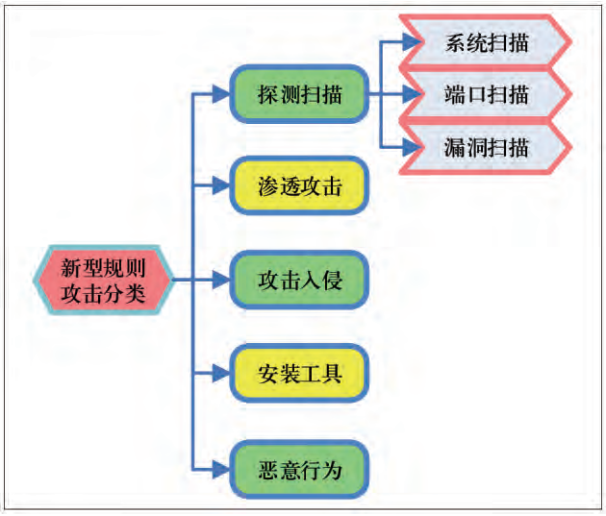

图2 新型规则攻击分类

对应以上各个阶段建立的候选指标，按层次、信息来源、需求提炼出宏观性质的二级综合性指标，有机组织原先设定的候选指标并进一步抽象，建立态势感知的指标体系。从攻击目的、攻击手段、漏洞信息等角度分别来进一步指标体系。

针对所建立的指标体系，采用纵向数据融合和横向信息关联的方式，运用一定的数学模型和先验知识进行关联分析和理解，给出一个可信的态势值。可以采用的工具包括贝叶斯网络理论、隐马尔可夫模型、D-S 证据理论、模糊逻辑等，采用多种评估相结合的方法，如利用模糊识别和 D-S 证据理论，较好地解决多样本识别的不一致问题，有效地对识别结果进行融合。

3.6 基于 APT 攻击链的态势预测

态势预测是态势评估的最后步骤，目前预测方法较多，如灰色理论、时间序列分析、神经网络和支持向量机等，很多技术和方法都是相辅相成的。

综合 APT 攻击链多样性特点，以及网络安全态势预测算法的优缺点，采用多种预测方式相结合的方式对态势进行预测。对此提出一种支持向量机和神经算法相结合的网络安全态势预测模型。

利用支持向量机作为融合技术，能对基于 APT 安全感知模型的多源、多属性信息进行融合，从而产生对态势的感知，结合神经网络方法，能进一步完善对网络安全态势预测的精准度。

3.7 基于 APT 攻击链的态势可视化

网络安全态势可视化，即利用可视化方式展现网络当前状态和未来趋势的一种技术，可更直观地展示相关信息。可视化技术的 3 个重要要素是数据、设计和沟通。可视化技术目前发展迅速，已实现动态视图实时显示、多视图切换等，用户对可视化技术的需求和依赖程度也越来越高。

基于 APT 攻击链的威胁感知效果。

3.7.1 按 APT 攻击分阶段性的展示方式

为了更好、更直观的展现 APT 攻击的各个阶段和各事件的持续时间、时序，可采用如图 3 所示的形式进行展示。

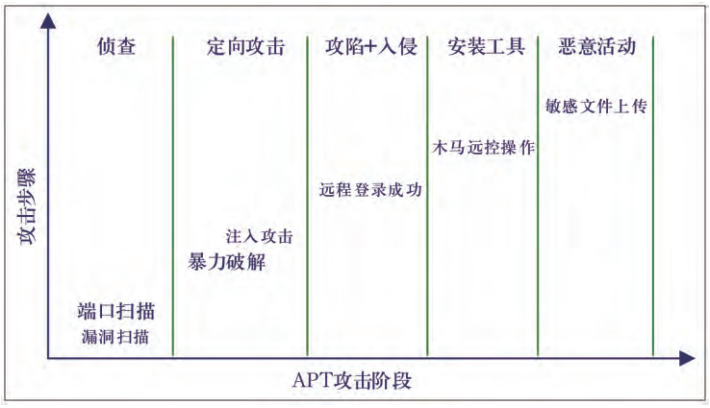

图3 APT攻击阶段性展示形式

3.7.2 大数据分析下的威胁感知效果

为让用户更加直观感知攻击态势，大数据处理中心或专业云端形成了多种呈现方式的效果图，从时间和攻击数量上动态感知网络攻击的行为，如图 4 所示。

为了给用户呈现更多的攻击信息，将攻击的告警信息分类成了不同的事件，也包括了一对一攻击、一对多攻击、多对一攻击等形式，同时展示单位时间内的攻击次数，攻击事件等信息。为用户及时了解、掌握攻击的整体态势提供可视化的显示模式。如图 5 所示。

不同的攻击行为在不同时间段的攻击特征形成的攻击曲线如图 6 所示。

针对目标主机进行的一系列攻击行为，通过对告警日志的分析，将攻击行为在不同时间 5 个不同阶段做了可视化分析展示，直观感受受影响系统的被攻击的各种行为。图 6 中不同颜色代表了不同的攻击阶段，通过图形化的表示模式能清楚的了解目标主机受攻击的状态。

动态感知着眼于全球范围的攻击行为，通过专业化、智能化的大数据挖掘，分析、发现、溯源、还原整个攻击过程，找到安全薄弱点，最终能够部署对抗措施，提升覆盖已知威胁和未知威胁的主动防御能力，将安全隐患消灭于萌芽状态。

数据处理中心或专业云端以全球多点支撑，分类告警日志为核心，侧重数据可视化、支持网络架构多级数据提取，从攻击源、攻击类型、攻击目标等多角度展示网络风险态势，提供全面纵深的威胁态势感知预警，也为用户及时做出应对策略提供帮助。

4 总结

本文介绍了基于 APT 攻击链网络安全态势感知研

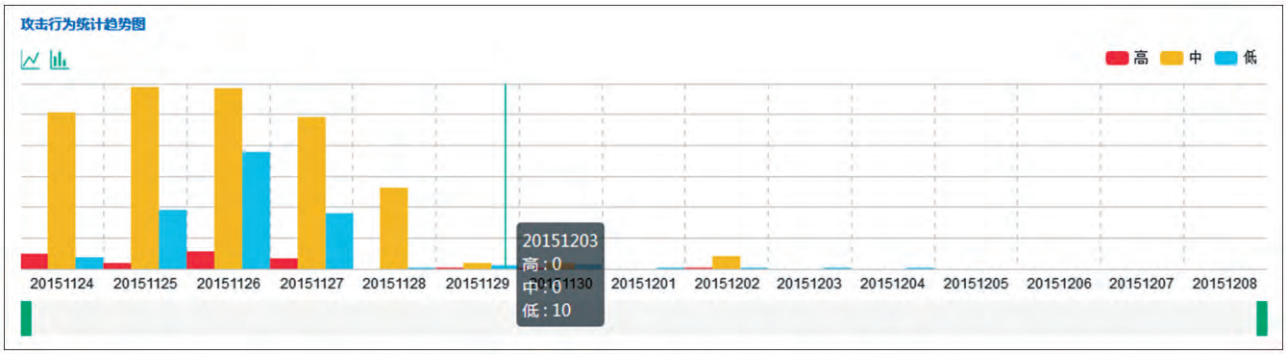

图4 大数据分析下的威胁感知效果1

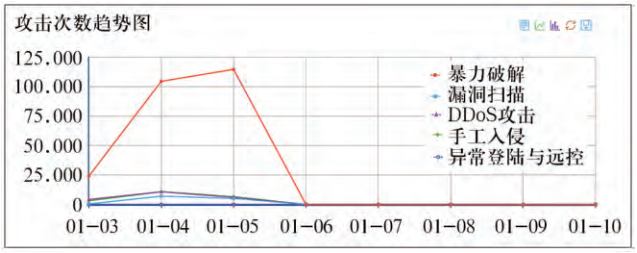

图5 大数据分析下的威胁感知效果2

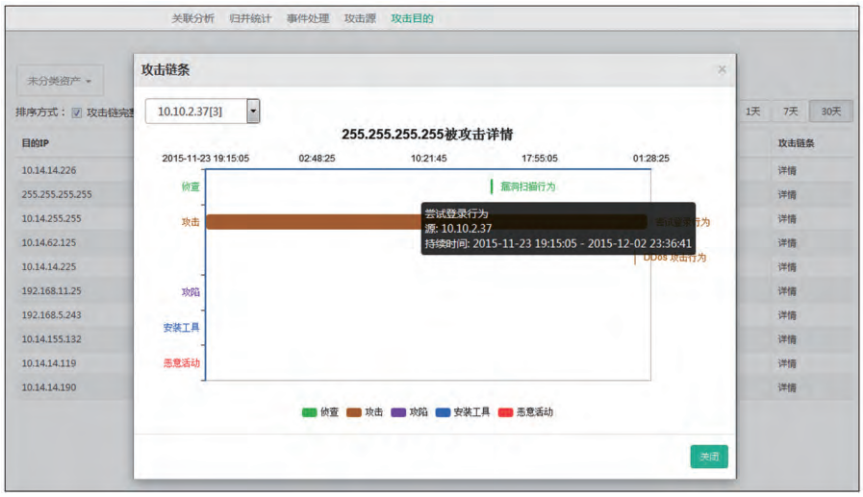

图6 大数据分析下的威胁感知效果3

究框架，从数据采集、预处理、态势评估、态势预测以及态势可视化方面，阐述针对 APT 攻击链的网络安全态势感知的体系结构、主要研究思路和关键技术方法。此类网络安全态势感知的研究对于做好 APT 攻击监测和防护具有重大意义。

伴随着互联网应用愈发广泛和深入，新业务新技术层出不穷，尤其是社会对大数据、云计算和移动互联网的深度依赖，网络安全风险空前加大，特别是 APT 攻击链越来越复杂化、多样化。传统 IDS 检测方式已不再适用万物互联状态和大数据驱动形式下的网络威胁变化。

针对 APT 攻击链，依托全新模式规则分类模型、海量数据采集、专业智能的大数据挖掘和分析模块相互融合的方式，充分利用数据驱动安全，以全量覆盖，多点上报，多级互联的形式，及时呈现可视化检测预警信息，实现“人－机－地－云”的全方位、全天候、多维度、立体式的网络安全威胁感知解决思路。

参考文献

[1] 郭方方，唐匀龙，修龙亭，等．基于云计算的网络安全态势感知模型研究[DB/OL]．http://www.paper.edu.cn/html/releasepaper/2014/01/1081/，2014-01-23．

[2] 刘效武，王慧强，赖积保，等．基于多源异质融合的网络安全态势生成与评价[J]．系统仿真学报，2010,22(6):1411－1415．

[3] 贾焰，王晓伟，韩伟红，等．YHSSAS：面向大规模网络的安全态势感知系统[J]．计算机科学，2011,38(2):4－8,37．

[4] 梁颖，王慧强，赖积保．一种基于粗糙集理论的网络安全态势感知方法[J]．计算机科学，2007,34(8):95－97,145．

[5] 陈秀真，郑庆华，管晓宏，等．层次化网络安全威胁态势量化评估方法[J]．软件学报，2006,17(4):885－897．

[6] 王娟，张凤荔，傅翀，等．网络态势感知中的指标体系研究[J]．计算机应用，2007,27(8):1907－1909,1912．

Research of cyber security situation awareness base on APT attack chain

WU Peng, HUANG Fu-tao

(China Mobile Group Chongqing Co., Ltd., Chongqing 401420, China)

Abstract In order to improve the defense ability of information security for APT attack, more and more attentions is put on the information network security situation awareness technology in order to realize the prediction and prevention of security events. This paper analyzes the necessity of studying the network security situation awareness technology. The architecture, methods and key algorithms in the existing domestic and overseas research works in this field are described in detail. Finally this paper summarizes the network security situation awareness technology and looks forward to its development trend.

Keywords situation awareness; APT attack chain; situation assess; situation prediction