面向大数据的网络安全策略研究

□ 郑晨阳 / 南京政治学院上海校区军事信息管理系 上海 200433

摘要: 大数据时代的到来,给传统的网络安全带来了新的问题。文章在分析面向大数据网络安全隐患的基础上,分析用户行为特征、网络流量特征和高级持续性攻击特征,提出大数据应具备网络安全感知能力、网络安全融合能力和网络安全服务能力的网络安全策略,以全面保障大数据环境下的网络安全。

关键词: 大数据, 网络安全, 网络安全策略

DOI: 10.3772/j.issn.1673—2286.2014.02.002

大数据时代的到来,给传统的网络信息安全带来了新的问题。大规模网络生产、分享和应用数据的时代给人们的生活、工作带来极大的便利,人们在微博、论坛等社交网络上沟通、记录和分享信息,人们在网上搜索、查询获取知识资源,人们在网上无国界和时间限制享受购物,由此产生的海量数据也带来了极大的安全问题。

1 面向大数据的网络安全隐患

美国“棱镜”计划包括两个秘密监视项目,一是监视、监听民众电话的通话记录;二是监视民众的网络活动。主要监控电子邮件、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间、社交网络等信息资源。计划涉及美国的微软、雅虎、谷歌、苹果等互联网公司。情报部门利用强大的分析处理工具,对这些从互联网公司搜集来的海量数据进行检索、比对和分析,可以还原每一个人的真实身份信息、社会关系,在侵犯个人的隐私的同时危及国家的政治、经济和军事的安全。

1.1 大数据的数据存储隐患

大数据时代带来信息的集中存储和管理。“大数据”存在的初衷,是希望通过获得大量的用户行为数据,进行精准的分析,可以更加高效地为用户服务。但大数据在提供更全面更精准更加客观的数据分析的同

时,所搜集的海量数据和潜在价值更吸引人们,特别是黑客和美国的情报部门。由于大数据的来源途径复杂,获得的大数据类型繁多,包括文本、图片、声音、视频、日志文件等等,除了少部分传统的结构化数据外,绝大部分数据属于半结构化和非结构化的数据,而各种非结构化的数据又增加了大数据存储的复杂性。

使用非关系型数据库NoSQL存储数据,能够存储大量不同类型的结构化数据和非结构化数据,有效解决大数据存储的可扩展性和可用性,以及数据存储的灵活性。但NoSQL不同于传统的数据库技术,不能通过传统的SQL语言进行数据访问,缺乏一套严格的访问控制机制。同时NoSQL使用新代码,意味着系统本身在一段时期内仍然存在各种安全漏洞的风险。

1.2 大数据的数据分析隐患

大数据超强的数据分析能力尤其是预测趋势分析带给人们极大的惊喜,是企业营销的法宝。但“棱镜”计划的暴露,发现涉及的思科、IBM、谷歌、高通、英特尔、苹果、甲骨文、微软对网络安全的危害更为巨大。通过这些公司获取的海量数据看起来是分散游离的,但看似无关的数据经过整理和分析都可能成为极为重要的商业机密数据和国家机密数据,危及国家的政治和经济安全。例如,一个普通百姓的消费数据几乎没有价值,但是如果一个亿、甚至几个亿的普通百姓消费数据被整合起来,就可能关系到整个国家经济发展的核心指标。

大数据使用的数据挖掘和数据分析技术在带来商业价值的同时,也被黑客用来发起攻击。黑客大量收集社交网络、电子邮件、电话、微博和家庭住址等信息,精准地进入和控制成千上万的电脑组成僵尸网络,在适当的时机发起大规模的僵尸网络攻击。而平时僵尸网络是很难被发现的,黑客们通常隐蔽地、远程控制着分散在网络中的傀儡电脑,而这些电脑的主人并不知道已经被控制成为僵尸网络的成员。

1.3 自主知识产权缺失隐患

“棱镜门”挑战的是国家安全,暴露了我国基础网络设施的安全存在很大的隐患。我国各类硬件和软件如芯片、交换机、操作系统、数据库等产品高度依赖国外产品,尤其是“棱镜门”所涉及的微软、甲骨文、思科公司的产品在我国占据很大的市场份额,使得大量机密数据被这些公司所掌握,也就很容易被国外的情报机构所获取。而这些产品存在一些尚未公开的安全漏洞,更是对我国的网络安全造成极大的威胁。

近年来,国内先后推出了龙芯等国产芯片、推出麒麟操作系统、达梦数据库、华为的交换机等通讯设备,但仍然难以和国外的产品所抗衡。微软的操作系统渗透到各行各业和千家万户的电脑中。美国的通信公司思科参与了我国几乎所有大型网络项目的建设,涉及政府、海关、邮政、金融、铁路、民航、军警等要害部门,以及中国电信、中国联通等电信运营商的网络基础建设。而华为和中兴公司虽然已是全球第二大和第五大通信设备供货商,但美国以安全威胁为由,禁止华为和中兴在美购买资产,以及为任何通信网络项目提供设备。

2 面向大数据的网络安全特征分析

2.1 用户行为特征分析

用户行为特征分析是通过日志文件分析正常用户和攻击用户在访问行为上的差异,提取适当的异常特征,进而进行访问行为的比对实现异常检测。即用户在网络上进行搜索、浏览、参与讨论、社交交流、好友互动等行为都会留下个体用户的行为特征,将这些鲜明的用户特征提取出来,整理、归类形成用户行为特征库。

黑客行为主要是指黑客攻击者出于不正当的目的对网络进行一系列的非法获取主机的内部信息资源、破

坏主机的正常运行、传输异常网络数据包等活动。在搜集到的海量用户行为数据基础上,分析非法窃取信息的行为、破坏系统的行为、假冒合法用户行为、恶意安装程序行为、非法破解口令账号行为、修改日志行为等等黑客行为特征数据,对这些数据进行分析整理,归类建立能够充分反应黑客各种行为特征的特征库。

在用户对网络进行访问时,通过对其行为和用户行为特征库、黑客攻击行为特征库进行检测、分析和匹配,以评估用户行为安全状况,识别用户的身份、访问时间、访问站点、访问操作、访问内容类型、访问操作造成的数据流量,以区别正常的用户访问行为和异常的黑客攻击行为,从而保障网络的安全。

2.2 网络流量特征分析

分布式拒绝服务攻击(DDoS)通过控制分散且数量巨大的电脑作为攻击平台,对一个或多个目标发动拒绝服务攻击,达到成倍的攻击威力。DDoS攻击通过大量合法的被控制主机向被攻击的服务器发送大量的连接请求,导致服务器端无法正常应答而瘫痪,或伪造虚假的IP地址发送连接请求,使得服务器端的连接应答无法送回,造成高流量无用数据,导致网络瘫痪。DDoS攻击的典型特征就是网络数据流量发生了异常。

通常正常的网络访问发出请求的数据包一般很小,但返回数据包由于是网页,包含图片、声音、视频等往往比较大,就会出现下行流量远大于上行流量的特征。而木马程序正好相反,被控端为服务器,控制端发送命令,被控端执行,形成上行流量远大于下行流量的特征。

基于点对点通信(P2P)网络实现独立的计算机之间对等的、双向的、实时的信息资源的共享,其网络流量特征和非正常网络流量特征非常相似,即上行流量大于下行流量。和传统的DDoS攻击不同,P2P网络不需要通过服务器,不存在网络瓶颈的问题,被控用户可以无限扩充,这也成为DDoS攻击的重要平台。可以通过增加分析网络连接特征和自启动特征来避免误判,弥补网络流量特征分析的不足。即P2P网络连接特征是P2P对多用户提供在线资源共享,与用户的连接数量比较多,而DDoS攻击网络连接特征是被控制端一般只和一个控制端进行连接。DDoS攻击具有自启动特征,即控制程序潜伏入驻被控制端后,在每次重新启动后为了能够继续获得控制权,就会想方设法采用各种自启动手段来重新启动控制程序。

2.3 APT攻击特征分析

高级持续性威胁 (APT) 网络攻击已经成为信息安全保障领域的巨大威胁。APT攻击通常是经过周密策划和实施, 针对特定对象进行长期的、有计划的攻击, 具有高度的隐蔽能力、潜伏期长、攻击路径和渠道不确定的特征。

APT入侵系统的途径主要包括利用智能手机、平板电脑等移动设备作为攻击的目标和对象。利用防火墙、服务器等系统漏洞获取进入系统的合法身份, 或通过锁定目标发送几可乱真的电子邮件, 以顺利植入恶意软件。这些恶意软件能够长达数年的潜伏在网络系统中, 使得各类安全防护系统不易察觉, 传统的防火墙、入侵检测系统、防病毒软件等安全措施往往很难防御。一旦潜伏下来, 就尝试各种攻击手段不断渗透和扩展到网络的各个角落, 进行各种信息的搜索和收集, 直到全面掌握攻击目标的人际关系网络、涉及的所有事件等重要情报。如“震网”(Stuxnet)病毒、“火焰”(flame)病毒等实施复杂APT攻击的恶意程序频现, 以破坏实体工业控制设备和窃取信息和收集情报为主, 均已隐蔽工作了好多年。

3 面向大数据的网络安全防御策略

面向大数据的网络安全防御充分利用大数据安全感知技术, 针对网络的通信设施、网络安全产品、网络系统软件和应用软件所存在的漏洞进行捕获、挖掘; 搜集已发生的和正在发生的网络攻击事件, 记录攻击的时间、攻击的网站, 攻击产生的流量、攻击的方法等数据。这些海量数据经过自动整合与分析, 生成漏洞特征库、黑客行为特征库、网络流量异常特征库, 进行横向和纵向的匹配关联分析, 实现大数据从网络安全技术到网络安全管理的多维度融合, 形成完整的安全防御系统。

3.1 大数据网络安全感知能力

网络安全感知能力是安全建设的基础。其可分为资产感知、脆弱性感知、安全事件感知和异常行为感知。资产感知是自动快速发现和收集大规模网络的分布情况、更新情况、属性等信息; 脆弱性感知是自动发现和挖掘网络硬件和网络软件漏洞数目和等级、网络提供的各类服务和开放的端口和端口数量等信息; 安全事件感知是指

能够确定安全事件的发生时间、地点、人物、起因、经过和结果; 异常行为感知是通过对异常行为评定, 以弥补对不可见脆弱性、未知安全事件发现的不足。

大数据的4V特征恰好可以应用于网络安全感知。即网络安全感知可以充分利用大数据量的数据存储和快速处理, 通过对各种类型数据如网络与安全设备的日志、网络运行情况信息、各类应用的日志等记录的分析获得用户的行为特征、网络流量特征和APT攻击特征, 有效识别正常的访问行为和异常攻击行为。

面向大数据的网络安全感知能力能够感知到漏洞的存在、感知到病毒的游离、感知到黑客的攻击, 感知到不断变化的应用, 感知到庞大的网络中人们的行为是否异常, 感知到网页、论坛、微博等内容是否符合规范、符合法律和法规。

3.2 大数据网络安全融合能力

大数据网络安全融合能力是网络安全建设的实现。网络安全融合主要体现在安全技术的融合, 安全与业务的融合, 安全与管理的融合。

大数据背景下, 单一的网络安全防护技术和网络安全管理手段已经不能适应, 包括终端的病毒防护、系统防火墙设置、身份识别和用户访问控制等安全防护手段; 网络边界针对IP进行的网络安全策略、网络防火墙、入侵检测技术、安全隔离、非法外连和非法接入监控, 以及病毒、垃圾邮件过滤等网关的处理。而是从用户到终端到网络边界再到数据中心, 在各个不同对象所处不同位置, 各种安全技术实现多维融合。

在终端将强调终端控制和数据保护, 强调虚拟化和安全融合; 在网络边界防护上将面对用户、应用、内容重点进行访问控制, 通过对业务系统的剖析, 对安全技术、业务、机构、流程优化整合, 充分实现安全与技术、安全与业务、安全与管理的大融合。有效实现大数据的大安全理念, 将网络安全覆盖到网络用户的终端设备(用户终端和服务器)、传输设备(网络交换机、路由器等)和数据中心的存储设备等方方面面, 形成强大的自动防御、自动修复和自动学习的网络安全防御体系。

3.3 大数据网络安全服务能力

大数据网络安全服务能力是网络安全建设的保障。网络安全服务主要是围绕安全产品服务、基础安全

服务和安全运维服务。

提供可靠的安全产品服务。首要宗旨是大力发展自主知识产权的网络安全产品。我国自主研发的防火墙、入侵检测系统和入侵防御系统、漏洞扫描系统、一体化网络安全网关等网络安全产品在国内占有一定的地位。但传统的安全产品不能完全适应和消除大数据的安全隐患,尤其是对于具有潜伏性和持续性的APT网络攻击显得软弱无力。

提供可信的基础安全服务。首先提供包括可信的网络路由器、交换机等网络通讯设备,可信的计算机、服务器等网络终端设备,可信的安全操作系统、安全数据库、安全应用程序等网络软件。其次基础安全服务就是提供可靠的加密服务和身份认证机制,随着大数据环境产生的大存储量、多类型的数据存储,实施有效的加密手段,严格按照数据存储安全的要求存储,通过安全传输协议实现大数据的传输加密,为数据流的上传和下载提供有效的保护。

提供可用的安全运维服务。对整个网络环境涉及的网络设备、终端、应用系统、内容信息等实施网络安全风险评估、网络安全防护和监控、网络安全响应以及恢复、网络安全审计等服务。网络安全风险评估对网络资产、网络脆弱性、网络数据流、网络终端、网络物理环境、网络管理等方面进行全方位的评估,分析网络中存在的安全风险和缺陷,给出对应的风险等级,给出分析评估结果。依据评估结果和实际网络安全等级要求,制定网络安全策略,修补、加固和优化网络安全系统,实施网络安全检测、网络安全监控、网络安全管理。一旦发现网络攻击和破坏,及时预警、响应和恢复,同时进行全面的安全审计。

4 结语

随着移动互联网、云计算和物联网技术的日趋成熟,大数据的应用规模也愈来愈大,黑客网络攻击的手段和方法也日趋复杂,给网络安全监控和管理带来极大的挑战。传统的网络安全防御手段已经很难应对大数据本身的安全问题,而大数据技术使网络安全问题更为复杂。只有深入研究大数据和大数据技术,在充分享受大数据带给人们新的思维方式、交流方式和生活方式的同时,利用大数据技术来有效防御和解决大数据的安全问题。

参考文献

- [1] 本刊编辑部. “棱镜”折射信息安全诸多隐患[J]. 信息安全与通信保密, 2013(7):8-10.
- [2] 郭三强, 郭燕锦. 大数据环境下数据安全研究[J]. 科技广场, 2013(2):28-31.
- [3] 林龙成, 陈波, 郭向民. 传统网络安全防御面临的新威胁: APT攻击[J]. 信息安全与技术, 2013(3):20-25.
- [4] 刘鹏, 孟炎, 吴艳艳. 大规模网络安全态势感知及预测[J]. 计算机安全, 2013(3):28-35.
- [5] 吴玮. 新时代安全能力: 感知、融合、服务[J]. 网络与信息, 2012(03):62.
- [6] 刘悦, 李强, 李舟军. P2P网络安全及防御技术研究综述[J]. 计算机科学, 2013, 40(4):9-13.
- [7] 陈丽莎, 张凤荔, 王娟. 构建网络安全态势评估指标体系[J]. 重庆科技学院学报(自然科学版), 2013, 10(3):135-137.

作者简介

郑晨阳 (1961-), 南京政治学院上海校区军事信息管理系副教授, 研究方向: 信息安全、知识管理。E-mail: zhengcycn@sina.com

Research on Network Security Strategy for Big Data

Zheng Chenyang / Department of Military Information Management, Nanjing Political College Shanghai Branch, Shanghai, 200433

Abstract: The arrival of the era of Big Data has brought new problems to traditional network security. Based on the analysis of network security risks for Big Data, the paper analyzes the user behavior characteristics, the network traffic characteristics and the advanced persistent threats characteristics. Then it proposes that Big Data should possess the network security strategy which includes the ability to network security awareness, network security integration and network security services, in order to fully protect the network security of Big Data environments.

Keywords: Big data, Network security, Network security strategy

(收稿日期: 2014-01-08)