李刚,陈述新,赵洪壮,等地震行业网络安全全流量监控系统建设与应用[J].地震工程学报,2018,40(增刊):205-213.doi:10.3969/j.issn.1000-0844.2018.Supp.205

LI Gang,CHEN Shuxin,ZHAO Hongzhuang,et al.Construction and Application of a Full-Flow Monitoring System for Seismic Network Safety[J].China Earthquake Engineering Journal,2018,40(Supp):205-213.doi:10.3969/j.issn.1000-0844.2018.Supp.205

地震行业网络安全全流量监控系统建设与应用

李 刚[1],陈述新[2],赵洪壮[3],张 颖[4],李永红[5],丁 晶[1]

(1. 天津市地震局,天津 300201;2. 新疆维吾尔自治区地震局,新疆 乌鲁木齐 830011;
3.中国地震台网中心,北京 100045;4. 四川省地震局,四川 成都 610041;5. 山东省地震局,山东 济南 250014)

摘要:介绍地震行业网络安全全流量监控系统的设计、建设与应用效果,阐述全流量监控系统对于网络安全防护工作的重要性与实际意义。研究对于大型信息网络系统的安全防护工作具有参考价值。

关键词:网络;安全;防护;全流量;监控;ElasticSearch

中图分类号:P315;TP393.08 **文献标志码**:A **文章编号**:1000-0844(2018)增刊-0205-09

DOI:10.3969/j.issn.1000-0844.2018.Supp.205

Construction and Application of a Full-Flow Monitoring System for Seismic Network Safety

LI Gang[1], CHEN Shuxin[2], ZHAO Hongzhuang[3], ZHANG Ying[4], LI Yonghong[5], DING Jing[1]

(1. *Earthquake Agency of Tianjin Municipality, Tianjin* 300201, *China*;
2. *Earthquake Agency of Xinjiang Uygur Autonomous Region, Urumqi* 830011, *Xinjiang, China*;
3. *China Earthquake Networks Center, Beijing* 100045, *China*;
4. *Earthquake Agency of Sichuan Province, Chengdu* 610041, *Sichuan, China*;
5. *Earthquake Agency of Shandong Province, Jinan* 250014, *Shandong, China*)

Abstract: The full-flow analysis of network security is an important approach for new-generation network security protection. This approach can detect attacks from multiple angles, all directions, and repeated backtracking. It can find known and unknown security threats, i.e. fault host, vulnerability exploitation, advanced Trojan horse communication, APT attacks, and data theft. It can also locate and obtain evidence of network attacks and help users improve safety analysis and response. This work introduced the design, construction, and application of a seismic network safety full-flow monitoring system. It also described the importance and practical necessity of full-flow monitoring systems for network security protection. In addition, it provided an important reference for the security protection of large-scale information network systems.

Keywords: network; security; protection; full flow; monitoring; Elastic Search

收稿日期:2018-08-04

基金项目:中国地震信息网络安全防护项目

第一作者简介:李刚(1978-),男,山西襄汾人,高级工程师,主要从事地震信息网络规划建设与网络安全工作。

E-mail:ligang@tjdzj.com。

0 引言

中国地震信息网络系统始建于“九五”时期,在“十五”期间系统进行了扩建,建成包括 1 个国家中心、46 个省级和直属单位网络中心。近千个三级信息节点的行业网络系统。实现了“网络到台站 IP 到仪器”的数字化地震观测系统,地震信息网络也成为地震行业数据传输交换、信息发布与数据共享工作的基础信息平台,为各类地震观测、震害防御、应急救援、科普宣传等业务提供支撑与保障。

但随着信息化技术的发展,地震信息网络系统的安全问题日显突出,“注重网络系统规模,忽视网络安全设计”的早期网络建设模式给地震信息网络安全带来重大风险。2016 年初地震信息网络系统遭受了一次大范围木马病毒攻击。据统计,全网有近 600 余台计算机服务器被破解入侵,成功入侵次数超过 4 000 次,地震行业网络安全形势处于重度高危状态。中国地震局对此高度重视,决定进行中国地震信息网络安全防护工作,任务重点目标即包括初步实现信息网络全流量安全监控和基本的安全防护能力,以下将详细介绍地震行业网络全流量监控系统的建设方案与建设应用情况。

1 方案设计

1.1 原有系统存在的问题

地震信息网络系统因建设时间早,网络内各节点间采用信任机制互联,节点间没有防护措施,全国网络如同一个交换网。虽然有部分单位加强了本区域的安全防护,但每个区域间不均衡的安全防护能力仍使得跨区域的网络攻击事件频发,在系统中存在众多安全问题和风险隐患[1],主要包括:

(1) 网络安全管理、监控与运维能力严重不足,没有有效手段进行安全问题监控与控制,安全问题难发现、难定位、难取证,网络安全保障能力严重不足,特别是无法有效阻止同类安全问题的再次发生[2];

(2) 行业网络结构采用的信任互联机制使得行业网络内跨区域的网络攻击事件频发,小的安全漏洞也可对全网造成严重影响,全网预警、检测与防范能力不足[3];

(3) 新型网络安全检测能力与手段不足,对已知和未知安全事件分析、排查等都过多依赖人员经验,效率不高,能力不强,无法满足全网安全防护工作需要。

1.2 建设目标

根据以上情况,中国地震信息网络安全防护项目将网络全流量安全监控系统的建设目标设定为:在解决网络安全监控与防护的基础上,对各类已知与未知的网络窃密、攻击行为可具备监控、发现、分析、回溯追踪的能力,可为安全事件响应提供数据支撑与证据线索,并实现新形势下网络安全防护与保障能力[4]。系统要向新型网络安全防护体系过渡,提高全网安全工作的“可视、可管、可控、可监测、可落地、及时响应、提前预测、重点防御”能力[5-7]。

1.3 系统结构设计

网络安全全流量监控系统要满足各区域网络中心对本区域内信息的监控与回溯分析,可对各类安全问题进行定位,同时相关网络运行、安全状态等重要信息要通过地震行业网络汇集到全流量数据分析中心进行综合处理与应用,实现全网安全状态统一管理。在安全策略管理上,可通过数据分析中心对全网安全策略进行统一下发和管理,实现全网策略统一化、标准化,实现全网防护能力集中控制。

而在地震信息网络系统内,网络数据交换与传输经过①地震台站、大中城市与市县地震信息节点、②省级中心、③国家中心三级系统,之后在行业骨干网进行全网交换[8-9]。国家中心和省级中心是行业网络数据交换的主体,因此本次全流量系统的建设要实现国家中心、省级和直属单位网络中心的区域级流量监控与安全防护能力,而各单位可根据实际需求在后期再进行系统的扩展与延伸,同时在行业内建立全流量数据分析中心,实现监控数据汇集分析应用与统一安全服务[10]。

地震行业网络安全全流量系统部署结构如图 1 所示。

1.4 全流量采集分析系统设计

(1) 采集分析系统的分析功能需求设计

采集分析系统安装于各区域中心,要至少具备 4 路数据接口,以分别接入互联网区域、行业网互联区域和局域网区域,实现区域内所有网络流量采集功能,同时采集分析系统要具备以下安全检测与分析能力:

① 具备 L2~L7 层网络流量可视化的能力

网络协议的鉴别能力是进行安全检测的基础[11],对网络流量的掌握情况决定了是否能够准确鉴别出网络异常行为[12]。系统可实现网络 L2~L7 层的流量可视化[13],可从 MAC、IP、会话、协议、应

用等维度分析网络行为，支持 TCP/UDP 会话日志的长期保存，其协议与数据包分析能力要具备 Sniffer、WireShark 等工具的能力。

② 具备快速感知各类网络威胁的能力

采集分析系统要具备多种网络威胁检测能力，能够对各类蠕虫、漏洞利用攻击、DDoS 攻击、暴力破解等已知威胁进行检测；可通过内置的异常流量行为模型库或自定义可疑行为模型，对远程控制、木马心跳、可疑长连接、隐蔽信道通信、可疑加密通信等异常行为进行快速检测，发现未知威胁的痕迹并进行有效预警和防护[14]。

③ 具备快速定位问题主机降低事件影响的能力

能将网络日志与数据分析中心[15]下发的各类黑域名、黑 IP 等威胁情报信息进行比对，能够快速识别和定位遭受攻击的主机、问题主机、甚至是失陷主机，为果断采取处置措施提供依据，能防止攻击在网络内的扩散，并同步对可疑或问题事件开展定性分析，高效、精准定位事件原因，可快速消除问题隐患，防止威胁在网络内造成更严重的影响，并可对安全事件进行关联分析[16]，对事件的影响进行有效评估，向行业系统提供类似事件防护建议，以杜绝或降低同类事件的再次发生。

④ 具备安全事件回溯分析的能力

采集分析系统要能够长时间保留原始数据包、统计数据、网络会话、警报信息等关键网络数据，并具备基于 IP 地址、域名、流量特征值、DNS 解析记录、异常行为模型等多维度回查功能，可对网络数据包进行还原，实现数据包级分析工作的可视化，进而对网络安全事件具备“知其然，更能知其所以然”的回溯分析能力，可对事件还原及追踪溯源工作提供有效保障[17]。

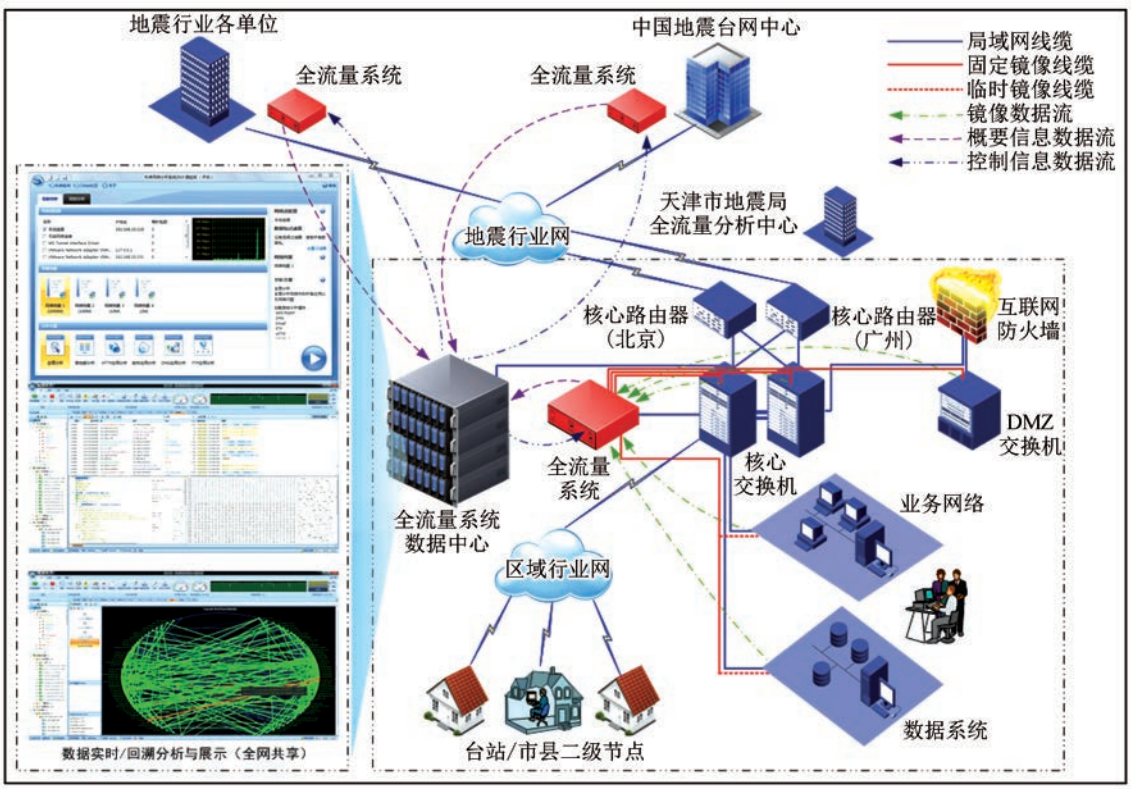

图 1　网络全流量系统部署结构示意图

(2) 采集分析系统的存储能力设计

全流量系统监控能力中的一个重要技术指标是网内流量数据的存储能力，因全流量系统可存储监控区域内所有的网络数据，因此其数据占用空间极大。根据行业网络安全工作要求，此次全流量系统要具备存储监控区域 15 天全网数据能力（不包括各类视频监控的流量），即在安全事件出现后，安全人员可通过系统追溯到 15 天内所有的网络流量信息。根据此项属性要求，作者与行业内相关单位网络管理人员进行了现有网络系统流量情况的分析计算，并以 15 天为存储标准，分析监控系统所需存储空间。

地震行业网络流量分为行业网、互联网和单位内部局域网流量三类，即：

网络通讯总流量＝行业网流量＋互联网流量＋局域网流量

作者通过地震信息网络系统建立的流量带宽监控系统查找到各单位的行业网和互联网流量数据，但在局域网流量上没有详细数据可查。作者按照地震系统局域网工作的特点，对局域网流量进行了统一估算，估算公式如下：

局域网流量≈(行业网流量＋互联网流量)×1.2

局域网流量是指网络通讯中源 IP 和目的 IP 都为局域网范围 IP 的通信流量。

表 1 是作者统计与计算出的流量信息与 15 天存储需求分析表。从中可以看出，地震行业网络系统的流量可分为三种情况，即国家中心 32TB 级、一类省级中心 16TB 级、其他单位 8TB 级。

表 1 地震系统部分单位网络平均流量与全流量存储空间计算表

单位	网络类型	各类网络平均流量统计与计算数据/(Mb·s^{-1})				15 天存储所需空间/TB	监控系统存储空间/TB
		行业网	互联网	局域网	总计		
台网中心*	国家中心	50.00	42.00	110.40	202.40	31.27	32
广东局	省级中心	16.00	31.00	56.40	103.40	15.97	16
河北局	省级中心	14.00	35.00	58.80	107.80	16.65	16
天津局	省级中心	9.00	27.00	43.20	79.20	12.24	16
山东局	省级中心	12.00	22.00	40.80	74.80	11.56	16
四川局	省级中心	14.60	31.00	54.72	100.32	15.50	16
新疆局	省级中心	11.00	22.90	40.68	74.58	11.52	16
地球所*	直属单位	5.00	43.00	57.60	105.60	16.31	16
安徽局	省级中心	2.40	20.00	26.88	49.28	7.61	8
海南局	省级中心	1.20	9.00	12.24	22.44	3.47	8
重庆局	省级中心	1.70	17.40	22.92	42.02	6.49	8
湖南局	省级中心	1.00	10.00	13.20	24.20	3.74	8
地质所	直属单位	1.50	22.00	28.20	51.70	7.99	8

注：表中台网中心、地球所的行业网带宽未计算测震数据汇集带宽，因此类数据在各单位节点内已统计。

根据上述分析，作者将全流量监控系统分为 4 类，除前述 3 类系统外，还增加了一种移动式采集分析系统，用于网络维护人员进行安全检查和专项维护工作。4 类系统的基本信息如表 2 所列。同时根据对各单位网络流量的估算，设计了地震行业内 47 家单位的采集分析系统部署与分配方案(表 3)。

表 2 网络全流量系统设备能力需求表

分类	安装模式	类型	接口	运行模式	存储空间/TB	存储时间/d
采集分析系统	固定式	万兆系统	4 路采集	单机	32	15
采集分析系统	固定式	千兆高端系统	4 路采集	单机	16	15
采集分析系统	固定式	千兆系统	4 路采集	单机	8	15
采集分析系统	移动式	千兆系统	1 路采集	单机	2	4

表 3 网络全流量系统设备部署情况表

分类	安装模式	类型	数量(台套)	部署位置
采集分析系统	固定式	万兆系统	1	中国地震台网中心
采集分析系统	固定式	千兆高端系统	18	中国地震局、15 家省市自治区与直辖市地震局(北京、天津、河北、山西、辽宁、福建、山东、河南、湖北、广东、四川、云南、陕西、甘肃、新疆)、2 家科研单位(地球物理研究所、第二监测中心)
采集分析系统	固定式	千兆系统	28	16 家省市自治区与直辖市地震局(内蒙古、吉林、黑龙江、上海、江苏、浙江、安徽、江西、湖南、广西、海南、贵州、西藏、重庆、青海、宁夏)、12 家科研单位(地质研究所、地壳研究所、第一监测中心、物探中心、搜救中心、工程力学研究所、地震预测研究所、强震观测中心、防灾科技学院、震害防御中心、驻深办、工程中心)
采集分析系统	移动式	千兆系统	1	天津市地震局

1.5 全流量数据分析中心与运维管理工作设计

在实现了对各单位本地的网络全流量监控与分析的基础上，要实现对全网网络安全工作的统一管理，需建设一个全流量数据分析中心，在其中实现对全网全流量系统的统一管理，包括数据集中存储管理[18]、预警信息管理、安全策略管理、系统运行管理等[19]。

(1) 全网数据集中存储管理功能

建设的分析中心要能收集处理全网 47 家单位的网络流量监控系统，包括核心关键网络指标信息和网络安全事件告警信息。

全网数据集中管理并不需要全部上传各节点监控信息，只管理相关核心指标，但对于各类监控区域内安全事件告警信息，要全部进行存储与管理，并要具备 Hadoop、ElasticSearch[20] 等大数据分析体系结构，实现海量数据的集中快速分析与服务，并具备系统平行扩展能力。本次设计中，数据分析中心要具备 2 台服务器的并行服务机制和秒级数十万条记录的查询能力，以实现全流量系统事件信息的大数据服务。

（2）全网预警信息管理功能

根据设置的警报规则，数据中心要能够集中统计显示各单位采集分析系统上报的各类警报数据，同时提供多种条件的快速检索和查询能力，并可实现在全网内同一事件的关联对比，进而实现全网预警响应。

通过此功能，可减少全网系统运维工作的压力。普通运维人员只需针对预警信息的提示，通过采集分析系统进行相关异常事件的处理，快速定位与还原安全事件发生过程，实现对各类网络异常行为的定性分析。

（3）全网安全策略管理功能

通过数据分析中心，可实现全网安全策略的下发与管理。已授权的安全管理人员可将各类安全威胁、防护信息及安全事件特征通过数据分析中心快速下发到全网的采集分析系统并即时生效，实现全网统一安全防护，减少因网络安全策略不同步部署带来的网络安全防护风险隐患。

（4）系统运行管理功能

通过数据分析中心可对行业 47 家单位的采集分析系统进行集中管理，包括设备运行状态监控、安全策略应用情况监控、用户授权信息控制等。

2　实施建设

根据设计方案要求并通过招标采购，地震系统最终采用科来 Colasoft 品牌的全流量系统进行项目建设，并达到了设计目标。

2.1　实现地震行业全流量监控全网覆盖

按照图 1、表 3 所示，在地震行业 47 家单位建成了网络全流量分析系统，在天津局建立了网络全流量数据分析中心，实现了 47 家单位的全流量分析回溯能力，实现了行业全网的安全事件统一预警、安全策略发布和统一管理，为各单位提供了强有力的网络安全事件分析、回溯系统。

2.2　网络全流量监控分析回溯能力得到实现

系统满足了设计中的各类网络流量监控、分析和回溯能力，流量数据可视化、网络威胁快速感知、问题主机的定位与快速分析功能得到有效保障，新型的网络安全防护体系得到实现。

2.3　网络流量数据 15 天存储能力得到保障

根据存储 15 天监控数据的需求，在项目建设过程中，作者与科来公司人员对网内视频数据进行了过滤，主要原理是根据相关视频协议及已知视频系统的 IP 地址，在数据包捕获阶段进行存储过滤。

以过滤天津市地震局网络中的视频监控系统为例，首先建立一个视频协议过滤规则，之后设置相关的视频系统 IP 地址，如需进行 IPv6 协议的过滤，可同时加入 IPv6 检测规则，共同形成视频系统过滤规则（图 2）。

图 2　视频数据包过滤器设置

通过对于视频数据的过滤，良好地实现了全流量监控系统的存储空间保证，实现 15 天存储需求。

2.4　ElasticSearch 分布式的全文搜索引擎的应用

全流量系统中的分析中心采用 ElasticSearch 分布式的全文搜索引擎技术[21]，通过其进行数据的存储、管理与查询服务，具备了秒级数十万条记录的查询能力，并具备快速并行扩展功能，实现了全流量系统事件信息的大数据服务。

Elasticsearch 是一个建立在全文搜索引擎 Apache Lucene(TM) 基础上的搜索引擎，它不仅包括全文搜索功能，还具备以下功能：

（1）分布式实时文件存储，并将每个字段同步

编入索引,使其可被搜索;

(2) 实现实时分析的分布式搜索引擎功能;

(3) 具备快速并行扩展能力,并行集群系统可处理 PB 级别的结构化或非结构化数据。

Elasticsearch 和关系型数据的概念对照如下:

关系数据库:数据库⇒表 ⇒ 行 ⇒ 列

Elasticsearch 系统:索引 ⇒ 类型 ⇒ 文档 ⇒ 字段

Elasticsearch 系统可以包含多个索引(数据库),每个索引中又包含多个类型(表),类型中再包含多个文档(行),每个文档中又包含不同的字段(列)。

Elasticsearch 使用的倒排索引比关系型数据库的 B-Tree 索引快,但为了提高搜索的性能,Elasticsearch 在插入/更新方面的性能有所降低。不过对于全流量系统中的预警信息、运行日志类的信息,其一次写入多次应用的模式是十分适合 Elasticsearch 应用的。

图 3 为在数据分析中心内对 2018 年 2 月 17 日—7 月 16 日间系统收集的各类日志数据进行查询分析,共找到日志信息 23 711 063 条,用时 658 ms。图 4 将检测周期缩短为 90 d 后,共找到日志信息 11 822 022 条,用时 515 ms,可以看到

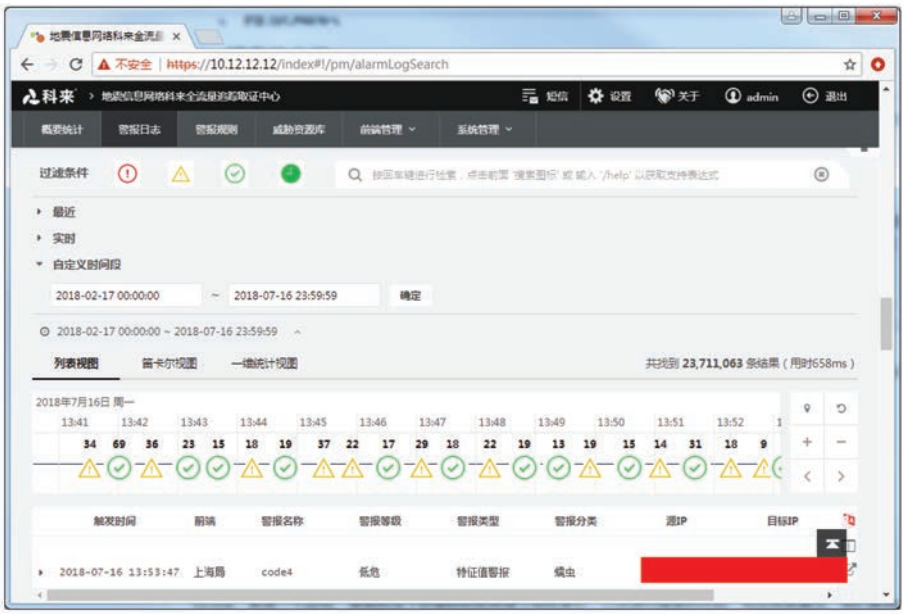

图 3 Elasticsearch 检测能力图(2 000 万条记录)

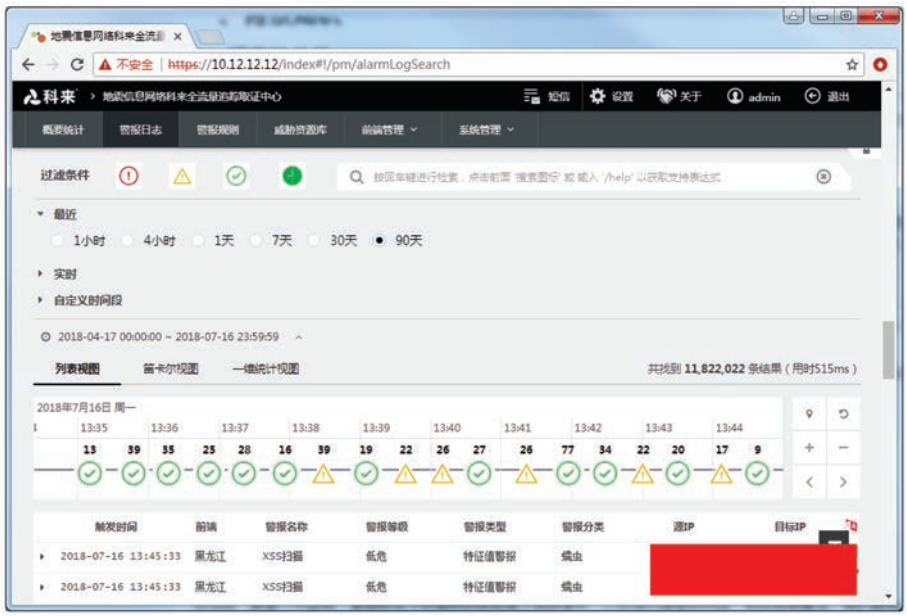

图 4 Elasticsearch 检测能力图(1 000 万条记录)

Elasticsearch 的在大数据系统中的检测能力远高于传统关系型数据库。

3　系统取得的成果与效益

网络安全全流量系统自测试应用至项目实施完成的 1 年时间内，在地震行业网络安全防护工作发挥了重要作用，主要包括以下 4 个方面。

（1）解决了网络安全事件发现难的情况

全流量系统使网络安全问题更易被发现，因为再高级的网络威胁也会产生流量。以往安全问题的发现要通过安全人员的深入分析，结合个人工作经验进行综合判断，容易出现定位不准或判断失误问题，而全流量系统通过多种网络威胁检测技术对各类已知安全问题直接产生异常告警。2017 年 11 月通过系统在地震行业内快速准确定位近 600 余台感染勒索木马或出现异常情况的计算机系统（表 4）。图 5 是某单位网络系统 445 端口的数据交换情况，可通过 445 端口快速定位勒索木马的问题线索。

表 4　地震行业网络勒索木马病毒感染或异常主机情况表

序号	单位	异常/感染主机数量/条	序号	单位	异常/感染主机数量/条
1	山东局	77	16	震防中心	5
2	福建局	71	17	黑龙江局	4
3	台网中心	63	18	西藏局	4
4	云南局	61	19	山西局	2
5	内蒙古局	48	20	湖南局	2
6	湖北局	47	21	驻深办	2
7	广东局	38	22	陕西局	2
8	安徽局	32	23	搜救中心	2
9	河北局	29	24	重庆局	1
10	江苏局	26	25	江西局	1
11	青海局	24	26	河南局	1
12	广西局	18	27	工程中心	1
13	浙江局	9	28	宁夏局	1
14	吉林局	8	29	北京局	1
15	新疆局	6	-	-	-

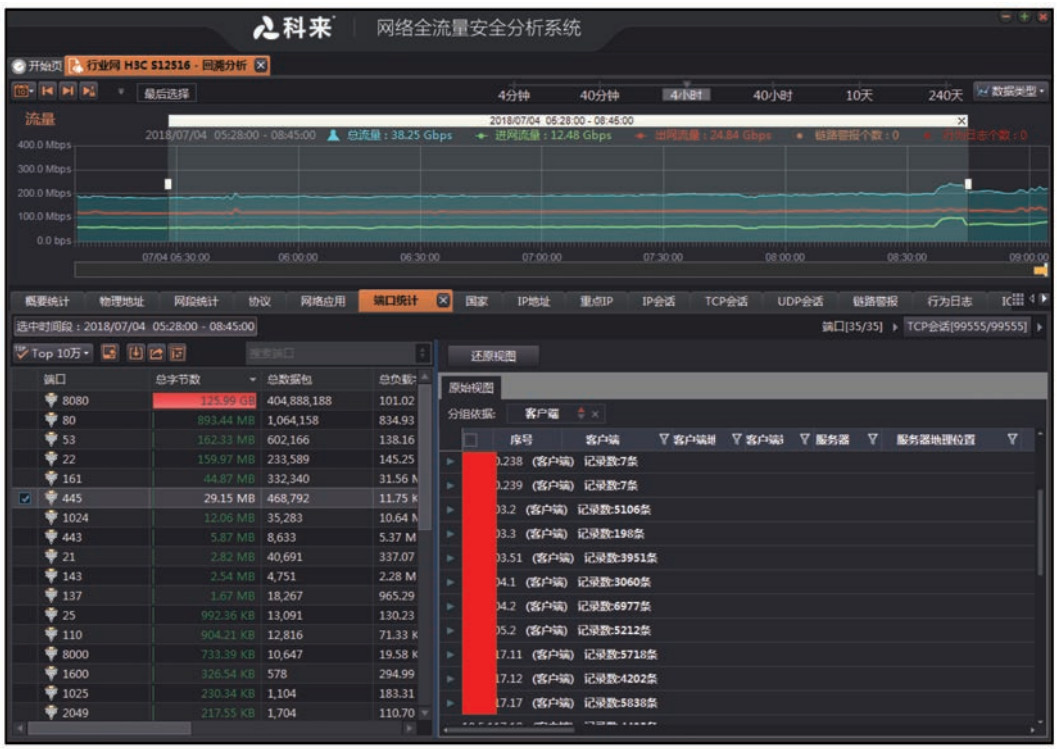

图 5　TCP445 端口数据交换情况

(2) 解决了网络安全事件回溯难的情况

网络安全事件分析与回溯是网络安全工作的一个难题,以往通过日志记录、行为分析等形式进行,分析结果往往受限于日志系统、行业记录的影响,很多情况下无法对安全事件进行复盘,丧失了对系统进行补救的机会。通过全流量系统的实施与应用,可以通过回溯功能快速还原事件过程,将事件中各类数据信息完整且可视化地展现在网络用户和安全运维人员面前,对于事件处置、风险防范和安全管理工作提供了有力保障。

图 6 是行业内某计算机系统的非法外联情况,通过 IP 矩阵图可以清晰表明事件状态。

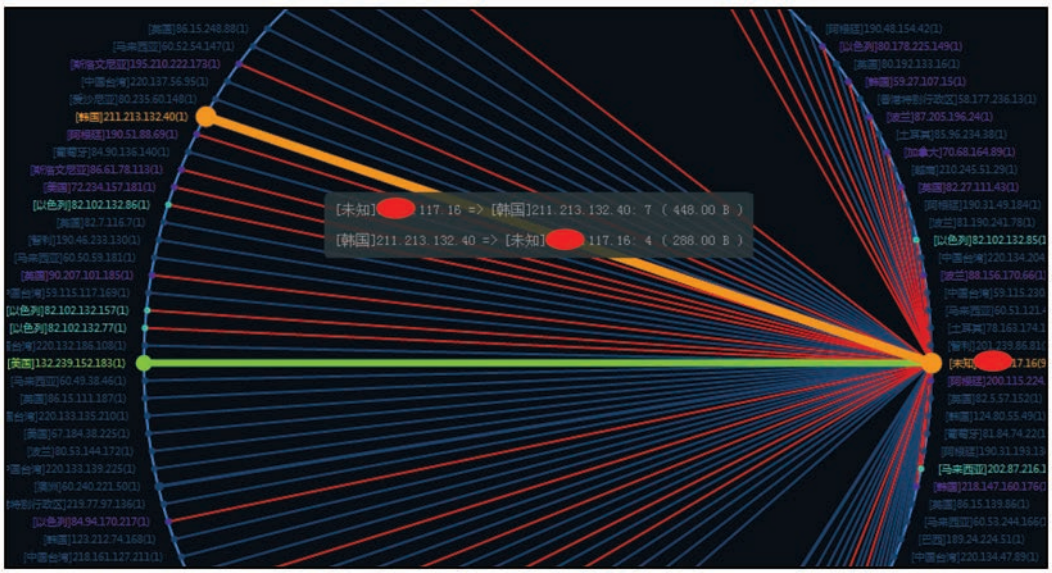

图 6 异常主机的网络连接 IP 连接矩阵图

(3) 解决了网络安全事件联动影响的问题

行业网络系统安全管理工作的重要任务之一是进行全网安全事件防范,形成统一的防护策略,建立统一的保护机制。以往出现安全问题后,全网应急时因人员技术能力、设备参数配置方式不同等原因,往往造成应急联动工作进度不一致、应急效果不佳。通过全流量系统的实施,在管理中心通过策略统一下发可以快速实现全网统一安全检测标准,对安全事件的分析与处置进行综合把握。2018 年 2—4 月间通过行业全流量系统,有效进行了“远控木马”、“挖矿木马”的全网应急响应工作,在 1 天内定位了十余家单位的木马病毒感染情况,大力提升了行业网络安全应急联动响应工作。

表 5 是网络安全全流量系统在试运行期间发现的重点安全事件,产生报警信息近 7.5 万条。

表 5 网络安全全流量系统告警信息与处理情况

序号	事件名称	报警数量/条	风险级别	处置情况
1	Agent 远控木马报警	72 530	高危	通报相关单位,完成处置
2	挖矿通信报警	1 557	高危	通报相关单位,完成处置
3	其他远控木马报警	131	高危	通报相关单位,完成处置
4	勒索木马病毒报警	2	高危	通报相关单位,完成处置
5	Ramnit 木马病毒报警	1	高危	通报相关单位,完成处置

(4) 将网络安全问题的分析主动权掌握在自己手中

网络安全全流量系统与其他网络安全设备最大的不同是,它将网络安全问题的分析主动权掌握在自己手中,运维人员根据自己的知识、技术、分析与判断,可以从数据包级流量信息中发现问题所在,并做出响应与处置。而传统的安全设备,运维人员对于数据信息的使用范围有限,更多的是依赖设备系统提供的已知事件模型进行分析对比,即安全事件的发现依赖于设备厂商对于事件的分析能力,在时间上存在一个真空期,易错过最佳防护期。

4 总结

网络全流量安全分析系统实施后,解决了地震行业信息网络安全工作中的众多问题,也把地震行

业网络安全防护工作推向新的阶段。但在目前的应用中发现,部分单位的全流量数据采集接口不规范,导致数据采集不完整,同时对系统的运维管理也要通过相关的制度建设进行明确。要充分发挥网络全流量安全分析系统的作用,还需要建设一支高水平的安全运维团队。

同时从网络安全管控的整体工作要求来看,全流量系统还有更多功能需要建设或扩展应用,作者今后将结合《地震信息化顶层设计》和《地震信息化行动方案》等工作要求,继续优化与完善网络安全全流量监控系统,不断增强地震网络安全防护能力。

感谢:本项工作得到中国地震局监测预报司、发展财务司、中国地震台网中心及行业各单位、项目承建单位太极计算机股份有限公司、项目监理单位北京易柯森特科技有限公司、特别是成都科来软件股份有限公司的大力支持与帮助,在此表示衷心的感谢。

参考文献

[1] 周利霞,王晓磊,杨奕,等.天津地震信息网络系统的安全建设[J].震灾防御技术,2013,8(3):334-339.

[2] 郝柽,杨立庭,洪敏,等.地震信息安全管理现状及策略研究[J].西北地震学报,2013,35(增刊):201-205.

[3] 尹德录,单德华,王中.等.地震信息网络的安全运行与技术防范[J].地震地磁观测与研究,2012,33(3/4):308-312.

[4] 于宗一,曲强,邱恺,等.医院网络流量回溯分析系统应用实践[J].中国卫生信息管理杂志,2017,14(5):691-694.

[5] 任磊,杜一,马帅,等.大数据可视分析综述[J].软件学报,2014,25(9):1909-1936.

[6] 陈兴蜀,曾雪梅,王文贤,等.基于大数据的网络安全与情报分析[J].工程科学与技术,2017,49(3):1-12.

[7] 龚俭,臧小东,苏琪,等.网络安全态势感知综述[J].软件学报,2017,28(4):1010-1026.

[8] 蒋晓山,程紫燕,陈存田.地震行业骨干网“一网双平面”架构[J].地震地磁观测与研究,2017,38(4):242-245.

[9] 章熙海,万群,杨乐.地震行业地面骨干网与应急卫星通信网互联路由设计方案的探讨[J].震灾防御技术,2016,11(3):674-681.

[10] 姜立新,帅向华,关晶波,等.国家地震安全公共服务平台研究[J].震灾防御技术,2014,9(2):263-270.

[11] 闪德胜,钱叶魁.网络流量监测技术主要方法分析[J].电子测试,2017,17(9):69-70.

[12] 李轶璋,王冼,段平,等.基于历史与当前短时特征的异常流量检测[J].计算机工程,2017,43(12):73-77.

[13] 赵颖,樊晓平,周芳芳,等.网络安全数据可视化综述[J].计算机辅助设计与图形学学报,2014,26(5):687-697.

[14] 胡洋瑞,陈兴蜀,王俊峰,等.基于流量行为特征的异常流量检测[J].信息网络安全,2016(11):45-51.

[15] 王力群,黄必栋.基于日志分析平台的监控系统的设计与实现[J].计算机应用与软件,2017,34(12):158-162.

[16] 吕宗平,钟友兵,顾兆军.基于攻击链和网络流量检测的威胁情报分析研究[J].计算机应用研究,2017,34(6):1794-1797.

[17] 蒋宽,杨鹏.基于数据包回溯的软件定义网络中的故障排除[J].信息网络安全,2016(3):71-76.

[18] 李永红,周娜,赵国峰,等.云计算环境下地震数据管理与服务应用研究[J].震灾防御技术,2015,10(10):811-817.

[19] 姜海庆.统一安全管理平台在网络管理中的应用[J].通信技术,2017,50(9):2089-2093.

[20] 赵科军,葛连升,等.基于 Hadoop 和 Spark 构建可扩展的网络安全分析平台[J].华中科技大学学报(自然科学版),2016(增刊 1):25-28.

[21] 白俊,郭贺彬.基于 ElasticSearch 的大日志实时搜索的软件集成方案研究[J].吉林师范大学学报(自然科学版),2014(1):85-87.