信安大赛报告提纲

基于知识图谱的网络安全威胁预警系统

1. 简介
   1. 背景分析

越来越多的计算机曾遭受过勒索病毒的洪范攻击，因此关于勒索病毒的防范措施越来越

引起人们的注意，但传统的病毒防范方式因为其杀毒软件的商业性质所决定的大多代码不可开源、用户自定义功能较差、特别是对于杀毒软件病毒库的更新周期较长的特点难以适应网络环境中新病毒的出现速度。

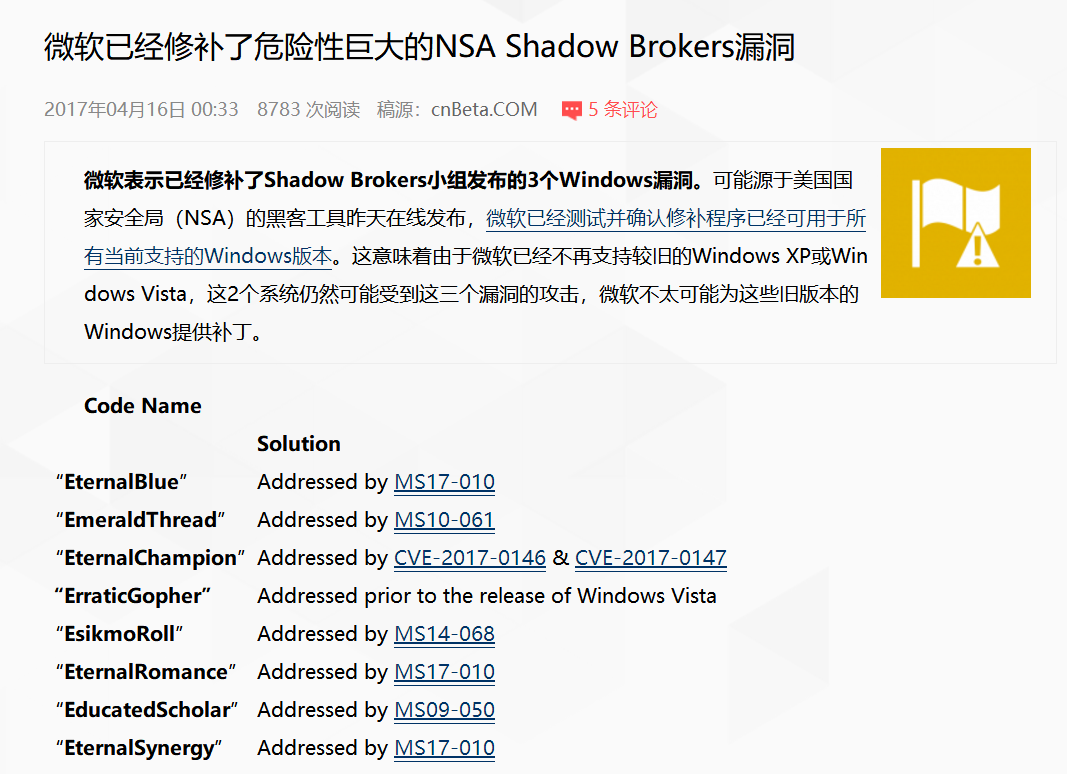
* 1. 相关工作

目前的病毒防范尤其是新病毒的防范措施主要由操作系统（如微软）公司修补新漏洞，也有极少数极客在网上分享自制杀毒软件或相应简单措施的经验教程，以及相关应对网络安全威胁措施的研究报告。我们在分析了以下解决方案的优劣之后提出了我们的解决方案——基于知识图谱的网络安全威胁预警系统。

1、国内外现有的解决方案

1. 操作系统公司修补新漏洞——提供系统保障。让操作系统修复自身已被发现的漏

洞。致力于打造一个以漏洞更少、安全性更高、及时更新漏洞修复补丁、为每一台使用该系统的主机提供系统安全的正版操作系统。如下图微软修补了危险性巨大的NSA Shadow Brokers漏洞。



1. 极客经验分享——提供自定义服务功能。极客在各种开源社区分享其网络安全技术知识和实战经验，通过教程教授网民小型自制杀毒软件或补丁，让网民自己定义功能服务，并开发出最适合自身需要的小型杀毒软件。当然对于大部分普通网民来说更现实易懂的方式就是上百度经验查一查教程，比如如下针对勒索病毒的简单端口关闭防范教程。



1. 应对网络安全威胁措施的研究报告

如上海交通大学的一篇硕士专业学位论文《基于数据挖掘的网络安全态势分析》，

其中提到了使用数据挖掘技术通过分析大量数据进行模型分析和攻击检测。其中指出了

利用关系型数据库记录并分析大量数据进行分析处理。

1. 现有解决方案的特点

优点：

（1）功能获取免费且简单，较快获得安全服务。微软等公司也会更新漏洞补丁发布市场，这些都是免费的，一键安装即可，大大的节省了人力物力，减少了流程，为用户减少了一定的损失。

1. 漏洞检测服务，可自定义检查周期。微软公司往往会提供漏洞检测、病毒扫描服务，帮助用户找到电脑中那些存在的且和现有最新病毒库或漏洞库相同的漏洞病毒，便于用户及时查杀或修补漏洞。
2. 维护成本低，通过微软等公司在不断更新病毒库和软件版本，微软公司不断发布新的漏洞并推出系统补丁，同时还有极客的技术分享，从操作系统公司、开源社区提供技术支持，以便用户保护其操作系统。

缺点：

1. 更新时间较慢。存在部分漏洞存在数年才解决的情况，危险性极高。一旦被黑客发现并加以利用则会造成巨大损失。
2. 过多的漏洞补丁会拖慢系统速度。就连微软公司自己也承认了这一点。过多的补丁会让电脑运行不堪重负，速度明显下降。
3. 关系型数据库的局限性。关系型数据库在面对复杂数据关系的时候应对显得吃力，即表与表之间的复杂关系出现的时候尤为明显。
4. 对未知病毒和存在的未知漏洞的防御能力低下。新的病毒总是在攻击之后才能开始思考对策进行漏洞修复，事后处理无法降低损失，更无法避免损失。
5. 对可能攻击方式缺乏逻辑上的梳理和扩展能力。承接低下的防御能力，现有机制无法将不同攻击方式，不同病毒之间的关联关系联系起来，即无法触类旁通，举一反三。倘若使用知识图谱一类的工具，则可以串起整个攻击流程图。
   1. 特色描述

解决上述产品或者针对病毒的新型病毒的侦测的解决途径存在的问题我们研发了基于知识图谱的网络安全威胁预警系统，它是一个支持大数据平台的基于知识图谱的网络安全威胁预警系统，既为用户提供高效可靠的大规模数据搜集分析处理能力，又为用户提供可能出现新病毒的预警信息，还有友好而简单的操作界面。本系统采用最适合的国密算法SM2与SM4进行混合数据加密，保障了病毒攻击情况数据和服务器反馈和数据信息的安全性。相较于上述的解决方案，本系统的主要优势如下：

1. 基于flume+kafka+storm的高效大数据平台架构，保证大量攻击情报数据的即时传

输与处理。用户在使用时可以将其部署在服务器上，用于检测服务器提供服务的整个集群的病毒攻击情况并加以分析。如果出现数据库中未知病毒攻击情况则及时更新到病毒库中。

1. 可自学习、自生成的知识图谱与实时更新的自适应识别算法，保障对于未知病毒

的提前预警作用。利用知识图谱，我们使网络安全威胁预警系统具有了知识推理的逻辑结构能力，即可以分析不同可能攻击方式攻击路径之间的关联关系；同时实体、属性、关系能更好的理解语义范围域，使整体结构更加清晰易懂且易扩展，提升上层应用例如搜索和攻击方式匹配的准确率。通过知识图谱的建立，整理出现有病毒的特征和攻击流程，并提前列出大量可能的攻击步骤，每次攻击时记录下攻击步骤的触发情况并记录下一段时间内的频率，当未来某时刻出现了疑似攻击行为但并未产生受攻击警报时，可以通过匹配以往受攻击步骤触发的频率进行匹配，若相似度较高则将其是做新的病毒并纳入病毒库以实现动态扩充病毒库的功能。

（3）可追踪溯源的黑客发现策略。通过分析网络报文段中首部的ip地址分析出攻击来源，如果是肉机发起攻击可以分析肉机方面收到的报文信息通过追踪算法查找到攻击者源ip，减少损失，增大破获攻击案件的成功率。找到源ip后对其发出警告，并联系网络警方加以监督管控。并将从源ip及肉机ip发出的消息皆视为黑名单，以后与其他正常信息区别对待。

（4）采用SM2 和SM4 国密算法混合加密传输数据。当服务器检测到攻击并将攻击数据上传到处理系统、处理系统返回处理消息、处理系统连接数据库传输数据时，本系统随机生成一个SM4 算法的随机密钥key，用SM4 算法对需传送的明文数据加密，然后再用SM2 算法对该密钥key 进行加密。然后再进行点对点分布式网络中完成版权信息和侵权记录的传输，保证了攻击信息传输及分析处理过程的数据安全性。

1.4 应用前景分析

[可参考]未来工作方向补充：  
 可将态势感知的模块放到大型运营商如中国移动的服务器上，可以监测所有经过其旗下的服务器的攻击信息，锁定其ip。

二、作品设计与实现

2.1 系统概述

2.2 系统架构设计

2.2.1 系统层次架构设计

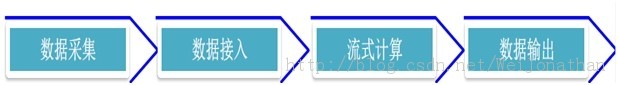
2.2.2 系统模拟攻击架构设计

2.2.3 系统入侵检测架构设计

2.3 系统核心技术

2.3.1 基于flume+kafka+storm的高效大数据平台架构

目前大数据处理与分析已经成为全球性问题，大数据充斥在网络的每一个角落。计算机中的各个应用、各个服务时时从上一个节点获取数据并从本地上传数据，需要获取计算机每个时刻所发生的数据行为，无疑，数据量已达到一定的量化程度。故本系统选择基于大数据平台。大数据平台一般包括数据源、数据采集、数据分析、数据存储等方面，系统分为以下模块（如下图）：

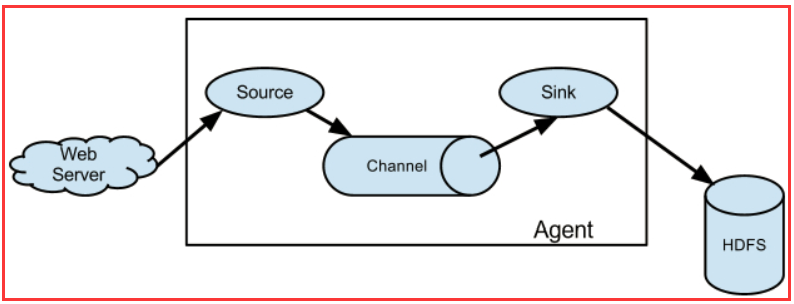


根据模块对应的需求和功能，系统最终采用了当前主流的技术日志分析系统Flume、消息队列处理系统Kafka、实时计算系统Storm来实现，以下做详细说明：

1. 数据采集

负责从各节点上实时采集数据，数据量大，选用cloudera的日志分析系统flume来实现

Flume:一个分布式、可靠、和高可用的海量日志采集、聚合和传输的系统。支持在日志系统中定制各类数据发送方，用于收集数据。Flume 运行的核心是 Agent，通过三个基本组件source、channel、sink来收集、暂时储存、处理传输数据的基本单位event，如图



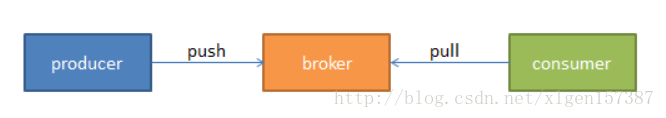
Flume原理示意图

Flume的传输具有可靠性，引入了确认机制，当确认数据成功发送后才会删除channel中的缓存数据。并且flume具有可恢复性，其中的File Channel 是一个持久化的隧道它持久化所有的事件，并将其存储到磁盘中。因此，即使 服务器宕掉，或者操作系统崩溃或重启，也不会造成采集到的病毒攻击数据和其他数据丢失。

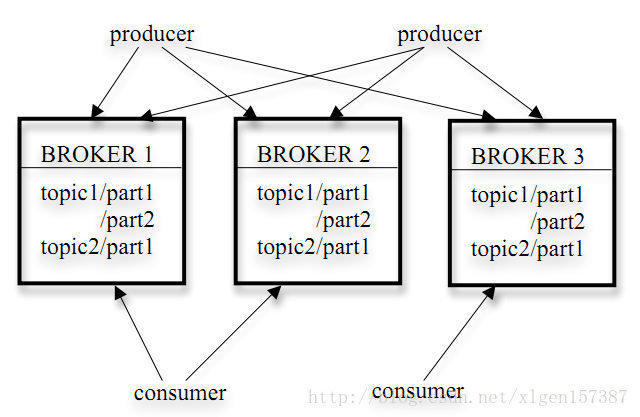
2）.数据接入

由于采集数据的速度和数据处理的速度不一定同步，因此添加一个消息中间件来作为缓冲，采用高吞吐量的分布式发布订阅消息系统kafka。

Kafka:  一种高吞吐量的分布式发布订阅消息系统，用来解决典型的生产者和消费者问题。如下图所示，Kafka作为producer和consumer的中间人，并采用生产者push、消费者pull的策略很好的解决了生产消费不匹配的问题。在此系统中，事件的数据往往是高并发的，吞吐量巨大，采集的数据每秒可达到几万条，但在分析处理时并没有那么高的速率，kafka很好的解决了这一问题。



Kafka可以是一台服务器，也可以是服务器集群，统称为broker。每条发布到Kafka集群的消息都有一个类别，被称为topic。而每个topic下对应了物理地址中多个partition,此系统中便根据Ip归属或者事件类型对采集的数据很好的进行了分类管理，同时也保证了为病毒分析提供了准确无冗杂的数据，保证了负载均衡。

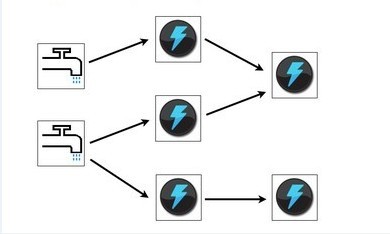


Kafka原理示意图

3）.流式计算

对采集到的数据进行实时分析，选择apache的分布式、高容错的实时计算系统storm。

Storm：一个分布式、高容错的实时计算系统storm。全量数据处理使用的大多是鼎鼎大名的hadoop，作为一个批处理系统，hadoop以其吞吐量大、自动容错等优点，在海量数据处理上得到了广泛的使用。但是，hadoop不擅长实时计算。而storm带着流失计算的标签在当前成为了实时计算的主流。Storm主要分为两种组件Nimbus和Supervisor，Nimbus负责在集群里面发送代码，分配工作给机器。而Supervisor会监听分配给它那台机器的工作，根据需要启动/关闭工作进程Worker。Storm提交运行的程序称为Topology，采取的事件信息在这里被作为最小的消息单位是一个Tuple，也就是一个任意对象的数组。Topology由Spout和Bolt构成。Spout发出Tuple， Bolt可以随意订阅某个Spout或者Bolt发出的Tuple并进行处理。数据由storm进行处理以后进行4）数据输出，输出到后台数据库进行储存。



Topology设计逻辑图

本系统具有严格的及时性，收集到的事件数据应当及时被分析处理，来做出根据当前分析情况的预警。选择storm来进行实现是最佳的选择。

Flume+kafka+storm小结：

根据病毒分析系统的数据量大，实时分析，极需计算能力的特点，系统采

用了主流的大数据平台构架Flume+kafka+storm。如图所示，flume获取数据，作为生产者；kafka作为中间人解决生产消费矛盾；storm则充当消费者实时地处理数据。

Consumer

Broker

Producer

Flume kafka storm

系统整合了三个工具系统的优点特性。Flume具有可靠性、可恢复性，kafka保证了数据的有序性和高吞吐量具有实时性，storm具有高容错性，易扩展性，并且拥有高效的性能，保证了十分的延迟。使得此系统也具有高效的性能，可靠性和实时性。

2.3.2 基于国密SM2 和SM4 混合算法的数据传输协议

此算法用于传输攻击流程中的攻击情报数据以及交互的信息。提高对中间人攻击等网络攻击方式的抵御能力。通过两端的公私密钥，使得数据能够安全有效且高速的传递。

在受攻击记录和受攻击情况的传输过程中，我们利用SM4算法加密速度快和SM2算法加密安全性高、密钥管理简单的特点，使用国密SM2和SM4混合算法对受攻击态势进行加密。首先，随机生成一个SM4 算法的随机密钥key，用SM4 算法对需传送的明文数据加密；然后，使用SM2 算法对该密钥key 进行加密，在保证数据安全的同时又提高了加/解密的速度。

SM2 密钥协商算法与SM4 算法

在本系统中，使用SM4算法加密需要发送的数据明文，SM4算法将明文和密文

均看成4个32比特字，我们表示为：

明文：

密文：

轮密钥：

反序变换：

加密变换：

 。对方接收到数据时，解密解密变换与加密变换结构相同，不同的仅是轮密钥的使用顺序，在本系统中SM4算法的方法和描述如表：

表 SM4算法主要方法

|  |  |  |
| --- | --- | --- |
| 方法 | 返回值 | 描述 |
| dncryptData\_CBC | String | 使用CBC模式解密 |
| encryptData\_CBC | void | 使用CBC模式加密 |
| decryptData\_ECB | String | 使用ECB模式解密 |
| encryptData\_ECB | String | 使用ECB 分组模式加密 |
| sm4.setSecretKey | void | 设置SM4密钥 |

本系统使用SM4算法对明文数据进行加密，但SM4算法的缺点是消息安全取决于对密钥的保护，泄漏密钥就意味着已加密信息可能被破解。因此，系统同时使用了SM2密钥协商算法对SM4算法生成密钥key进行加密。SM2算法属于非对称密钥算法，使用公钥进行加密，私钥进行解密，已知公钥求私钥在计算上不可行。发送方用接收者的公钥将消息加密成密文，接收方用自已的私钥对收到的密文进行解密还原成原始消息。使用SM2算法的方法及描述见表：

表 SM2算法主要算法

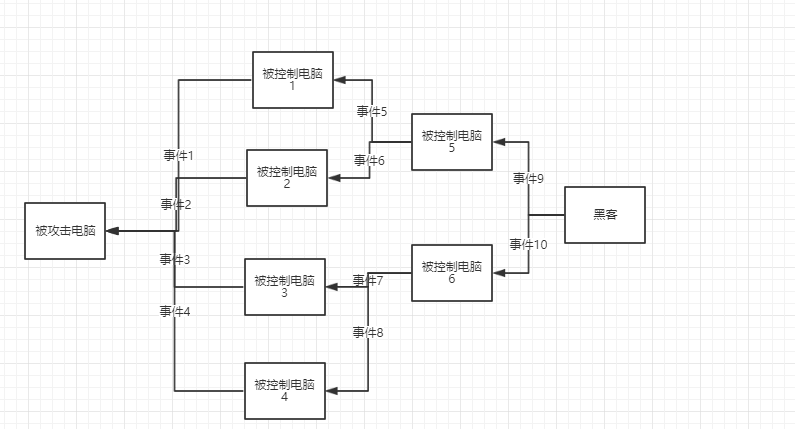
|  |  |  |
| --- | --- | --- |
| 方法 | 返回值 | 描述 |
| encrypt | static byte[] | SM2加密 |
| decrypt | static byte[] | SM2解密 |
| sign | static byte[] | 标签展示 |
| verifySign | Static boolean | 检验标签 |

2.3.3 基于Neo4j的知识图谱和基于MySQL的数据库平台

2.3.4 实时更新的自适应识别病毒算法

2.3.5 可追踪溯源的黑客发现策略

黑客在攻击其他计算机传播病毒时，往往不是通过自己的主机直接发布病毒攻击他人，而是通过控制一定数量的肉机进行攻击来保证自自身的安全和提升传播速度。肉机。肉机又被称为傀儡机，是指被黑客远程控制的计算机。在追寻病毒传播路径的时候，通常很能追踪到黑客本身。而本系统中，采取的黑客发现策略能够在有限层数内，追踪到黑客的原始机。主要采用了对比—剥离的方法策略，计算机中每个交互事件有源IP和目的IP，利用大数据平台的优势，我们将记录下攻击事件的源IP和目的IP。在出现病毒攻击后，触发追踪方法，查询这个知识图谱一系列事件的源IP，然后在根据多源IP查询全库的目的IP，将多台受攻击的计算机的事件源IP不断进行比较，剥离出发送攻击事件的源IP，然后一步一步定位到一个IP，即黑客



攻击层数示意图

如图所示，当我们的被攻击电脑瘫痪后，马上查询事件1-4的来源，得到被控制电脑1-4的IP。再以他们的IP作为目的IP查询到事件5-8，对比事件的源IP地址得到更近一层的傀儡机5-8的IP地址，依次向上追踪最终查找一切的源IP，即黑客。

2.4 系统功能设计

2.4.1 用户模块

2.4.1.1 登陆功能

2.4.1.2 注册功能

2.4.1.3 修改信息功能

2.4.2 权限模块

2.4.2.1 普通用户权限

2.4.2.2 管理员权限

2.4.3 病毒防御模块

2.4.3.1 勒索病毒检测

2.4.3.2 建立基于知识图谱的安全规则库

2.4.4 大数据平台实时事件处理

系统引入了大数据平台做实时的事件处理，能够在数据量极大的情况下仍然保持着对数据的实时处理的功能。采用了流行的flume+kafka+storm作为数据平台的构架。系统中，flume从管理下的数以万计的计算机的防火墙和监控软件中获取数据，作为生产者，将数据可靠地发送给消息队列处理系统kafka；kafka作为中间人,解决生产消费速率不匹配问题；storm则充当消费者实时地处理数据。

数据源

Source

channel

sink

Source

channel

sink

Source

channel

sink

Flume agent

event event event

Kafka集群

Topic

Partition1 Partition2

Topic

Partition1 Partition2

Topic

Partition1 Partition2

1 2 3

Spout tuple Spout tuple

bolt bolt bolt bolt

bolt bolt

Storm集群

输出分析数据

可从图中得知flume、kafka和storm三个系统都有自己独立的一套结构和功能，同时三个系统能很好地合作连接到一块来作为一个整体。此大数据平台中的数据流向在图中能很好地体现出来，具体如下：

1．数据源

每台计算机中的防火墙能保护脆弱的服务，控制对系统的访问，它几乎对计算机所有的与外界的网络往来就有着严密的记录。因此我们把每台计算机的防火墙作为数据源，能够准确高效的获得计算机的网络往来记录。同时，监控软件也作为了我们获取数据的数据源，帮助信息更完善和准确。

2.数据流向flume

每个flume agent从数据源不断地获取数据，得到数据后将数据暂时存储在channel中，在sink中将数据分为一条条的基本单位event发向kafka集群中。Flume处理的数据具有可靠性。

3.event到达kafka集群

数据被作为event推向kafka后，根据不同的类型被分往不同的topic中，并储存在物理内存中。物理内存中以partition作为单位存储，等待storm来消费。传输时每条数据拥有自己的offset，并采用相应的机制来保证了有序性和传输可靠性。

4.storm‘消费’

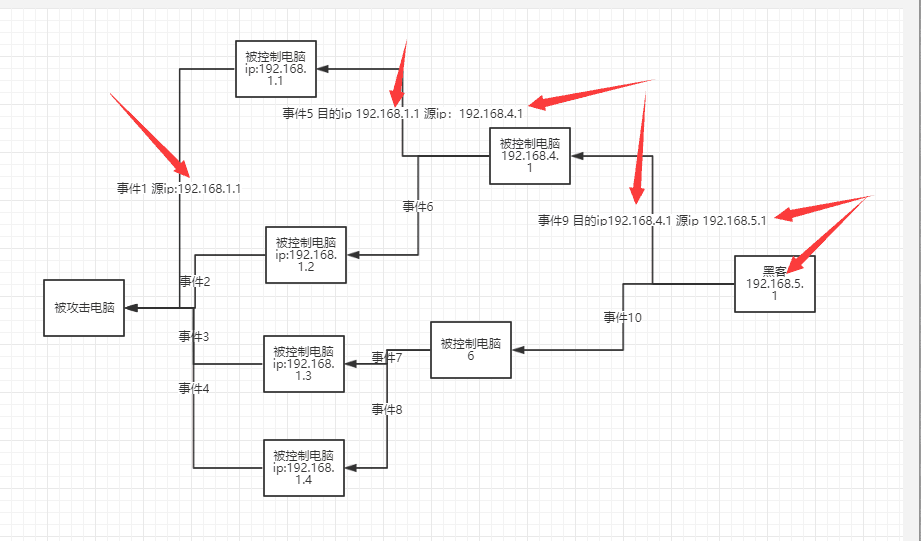
Storm从Kafka中消费到信息后。其中的组件Nimbus则会根据当前系统的繁忙情况和数据量，将处理信息的作业分给相对空闲的Bolt进行处理。保证了系统的高效运行和负载均衡。

该系统的实现策略和采用的技术很好的解决了需求。数据来源全面可靠、flume的可靠性和可恢复性、Kafka的有序性以及storm的高效性和负载均衡性是该系统大数据实时处理功能的基础和关键。

2.4.5 病毒发现和自增加策略

2.4.6 黑客发现策略

黑客发现是该系统的一大创新点功能，能在有限的攻击层数范围之内追根溯源，有效的辨别出黑客控制的肉机，发现此病毒的始作俑者。主要采取递归查询的方法策略，即以受攻击的电脑的ip作为目的IP地址查询出发布攻击事件的傀儡计算机，并通过其他若干台的计算机所查询出的傀儡机进行IP对比，得到此肉机属于病毒感染的第几层。再以此肉机的IP为目的IP地址查到源IP地址，再进行对比，不断重复此操作，最终得到一切的源头，即黑客。下面对该功能的流程做具体说明：

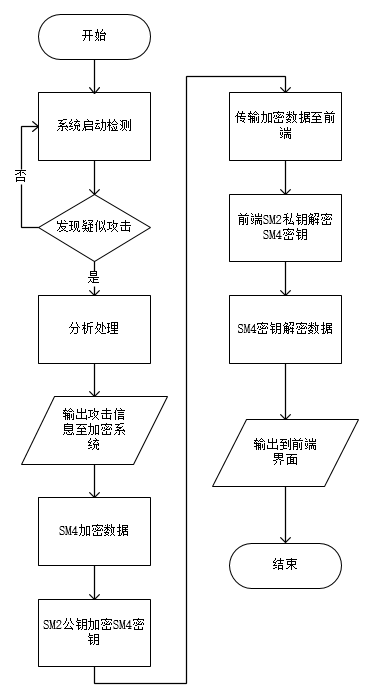


递归查询流程图

如图所示，当我们的电脑被攻击瘫痪后，立刻查询我们的病毒知识图谱，查出攻击事件1-4，查到发送事件1-4的电脑源IP192.168.1.1、192.168.1.2、192.168.1.3和192.168.1.4。此时再查询我们的病毒知识图谱，得到攻击事件5-8，以查到的源IP地址，查出发送事件5-8的电脑的源IP地址，可得到电脑6的IP和IP地址192.168.4.1。同理，若中间还有许多层的傀儡机，通过此方法最终得到黑客地址192.168.5.1。此功能需要大量的数据和查询计算，大数据平台为我们提供了良好的保障。

2.4.7 数据传输加解密

在数据传输加解密模块中，系统先通过部署在服务器上的探针检测到可能的攻击行为，并将其处理转换为字符串格式，输送给加密端。先使用SM4加密，并将密钥通过SM2用公钥当做数据进行加密，进行传输，接收到后再在前端通过SM2私钥进行解密得到SM4密钥，并用此解密SM4传递的数据。加解密流程如下：



2.4.8 安全态势可视化展示

三、作品测试与分析

3.1 测试方案

3.2 测试环境及测试设备

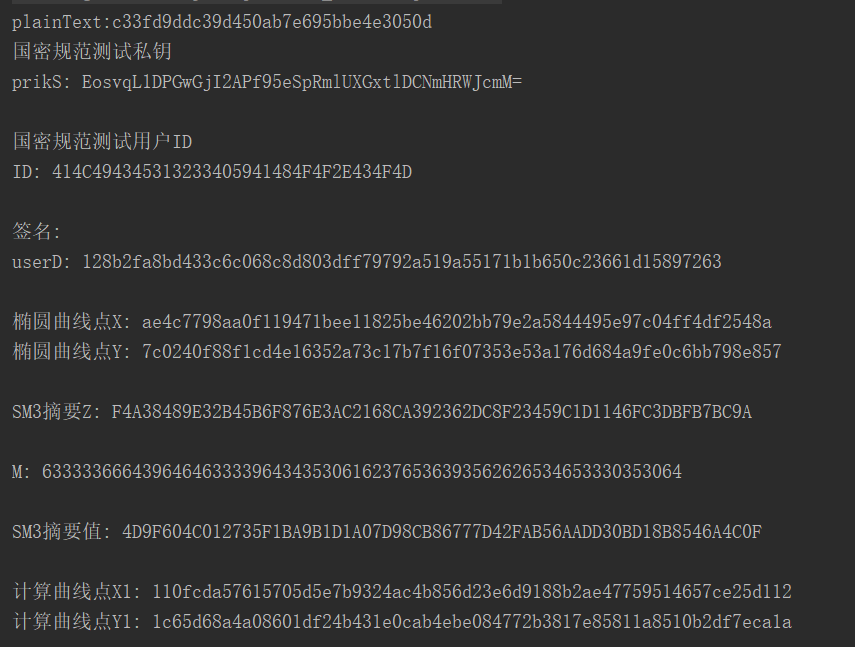
3.3 算法测试

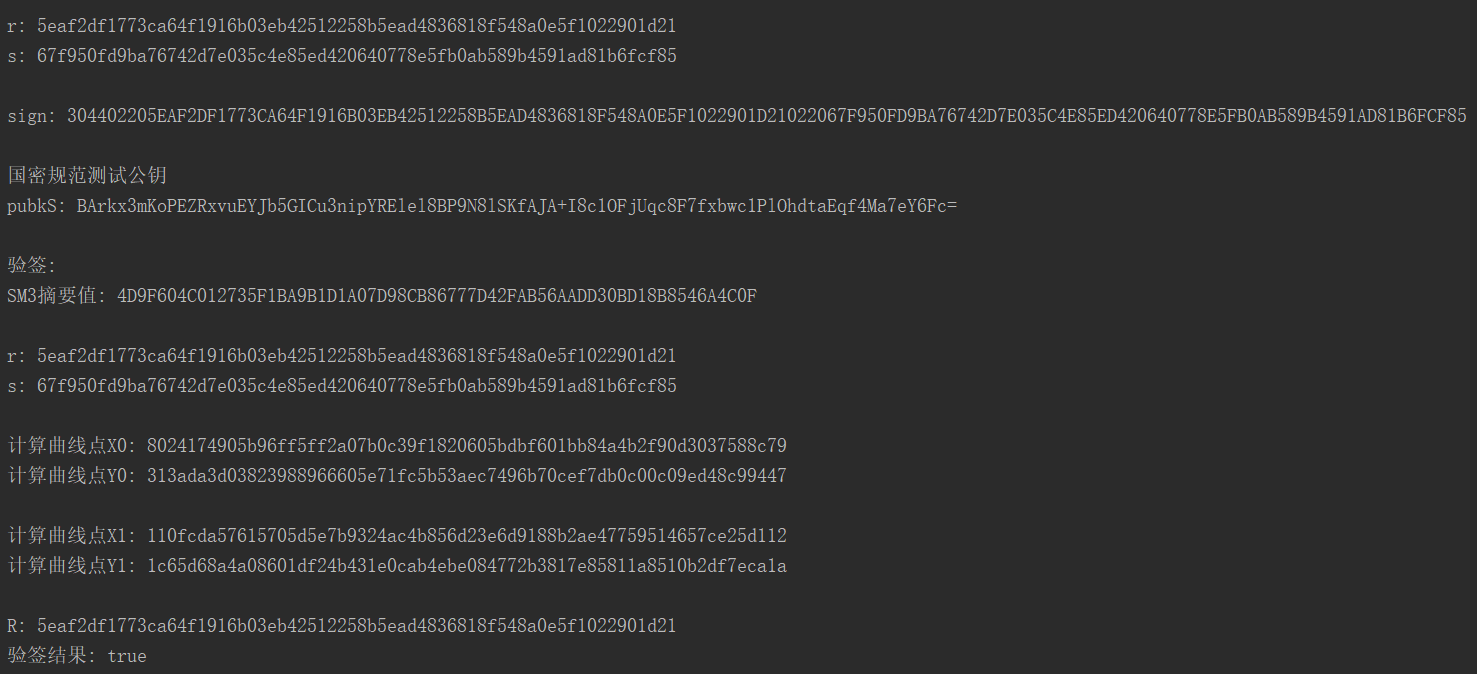
国密SM2 算法的测试用例如表3-2，输入数据来源于国密规范测试私钥和国密规范测试公钥以及随手输入的较长字符串。

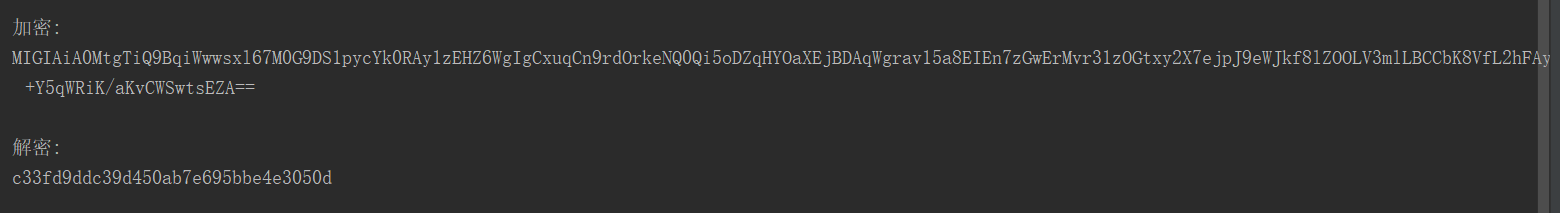
3.3.1 国密SM2 算法测试

|  |  |  |  |
| --- | --- | --- | --- |
| 用例编号 | No.1 | 模块名称 | SM2算法 |
| 测试方法 | 黑盒测试 | 测试日期 | 2018.5.11 |
| 测试说明 | 根据国密规范测试私钥和国密规范测试公钥，判断SM2加解密算法能否正常运行及实现密钥协商 | | |
| 预置条件 | 系统将要进行数据传输 | | |
| 判断准则 | 输入的字符串为随机输入，可多次重复实验，对比加解密后字符串数据是否一致。 | | |
| 测试输入 | plainText:c33fd9ddc39d450ab7e695bbe4e3050d  国密规范测试私钥  prikS: EosvqL1DPGwGjI2APf95eSpRmlUXGxtlDCNmHRWJcmM=  国密规范测试公钥  pubkS: BArkx3mKoPEZRxvuEYJb5GICu3nipYRElel8BP9N8lSKfAJA+I8c1OFjUqc8F7fxbwc1PlOhdtaEqf4Ma7eY6Fc= | | |
| 测试输出 | sign: 3044022040F1EC59F793D9F49E09DCEF49130D4194F79FB1EED2CAA55BACDB49C4E755D102206FC6DAC32C5D5CF10C77DFB20F7C2EB667A457872FB09EC56327A67EC7DEEBE7  R: 40f1ec59f793d9f49e09dcef49130d4194f79fb1eed2caa55bacdb49c4e755d1  验签结果: true  加密:  MHYCIAR9YwJMudf/t74d5wYwKjY/dS5p7RO3B6cy0kZ/XAdcAiBDVSSrzpzPdwnDzdk3vDMU6euXtEo68i6g/P0os5MhxwQgrgWjwx1o8lmMh74ec1TxPs+gL34ZOmTAgZ+0S2Vgr2UEDlV8ogXiOt2mXJRR2UFO  解密:c33fd9ddc39d450ab7e695bbe4e3050d | | |
| 测试评价 | 测试通过，SM2 算法能够正常运行 | | |

测试结果如图







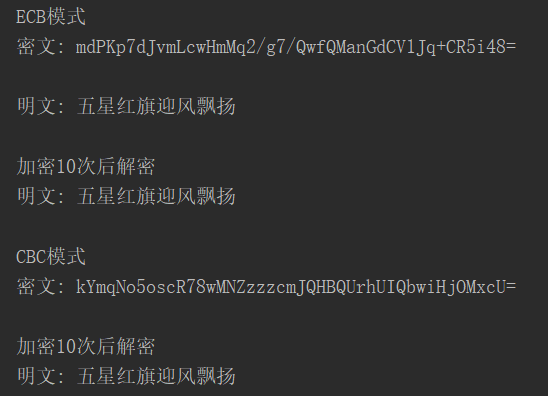
发送方和接受方在数据传输前进行密钥协商，结果如图所示，与预期结果一致，表明通过SM2 算法测试。

3.3.2 国密SM4 算法测试

|  |  |  |  |
| --- | --- | --- | --- |
| 用例编号 | No.2 | 模块名称 | SM4算法 |
| 测试方法 | 黑盒测试 | 测试日期 | 2018.5.11 |
| 测试说明 | 通过预设的公钥和输入数据，分别加密1 次和10次，再进行解密 | | |
| 预置条件 | 系统将要进行数据传输 | | |
| 判断准则 | 使用SM4 算法加解密，与输入的明文进行对比，判断是否一致 | | |
| 测试输入 | 明文：五星红旗迎风飘扬  密钥：JeF8UygsiOMfs2Y8 | | |
| 测试输出 | CBC模式  加密1 次后解密明文：五星红旗迎风飘扬  加密10次后解密明文：五星红旗迎风飘扬  ECB模式：  加密1 次后解密明文：五星红旗迎风飘扬  加密10次后解密明文：五星红旗迎风飘扬 | | |
| 测试评价 | 测试通过，SM4 算法实现了数据稳定地加解密 | | |

测试SM4 算法时的加解密状态，通过国家密码局推荐的公钥以及自定义的一句话作为加密数据，分别加密1 次和10 次，最后进行解密。

得到的结果都是输入数据，表现出SM4 算法的正确性与稳定性。

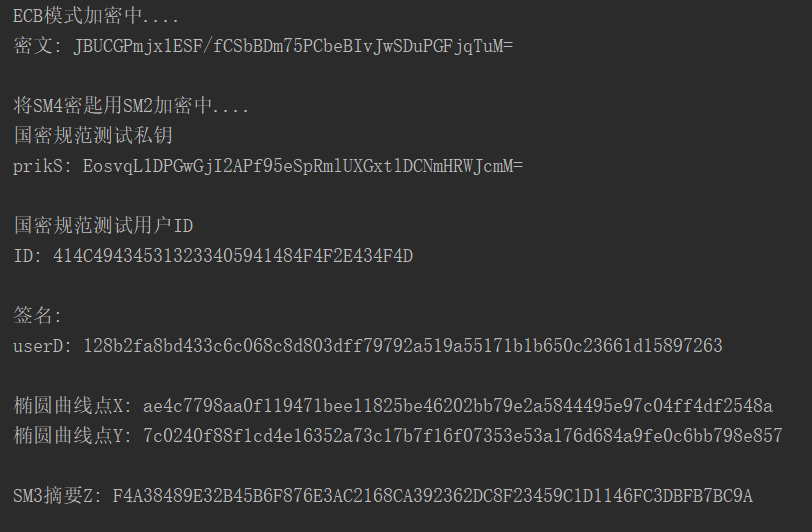


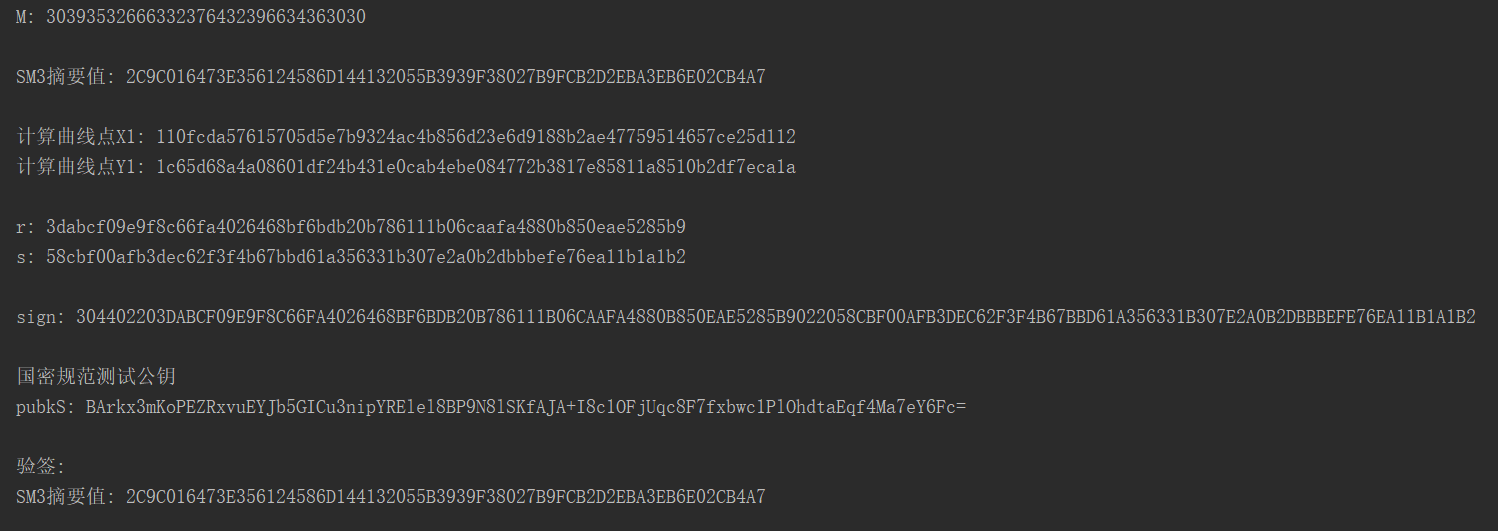
3.3.3 基于国密SM2 和SM4 混合算法的数据传输协议测试

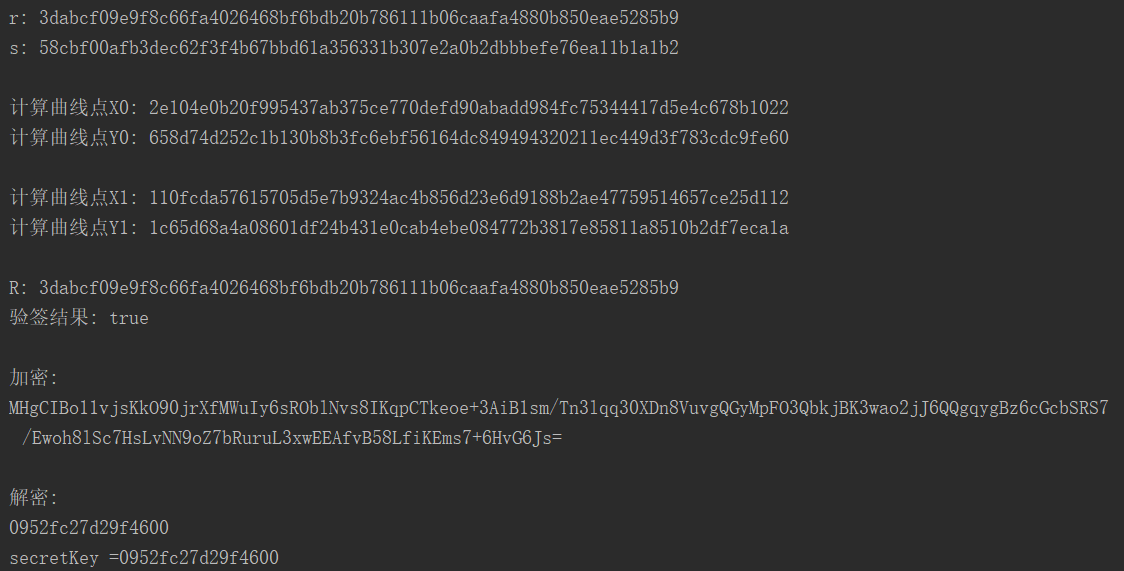
测试SM2 和SM4 混合算法时，选取设计好的版权信息区块链的数据作为输入数据，使用SM4 算法加密数据明文，SM2 算法加密密钥，如下表是SM2 和SM4 混合算法的测试用例：

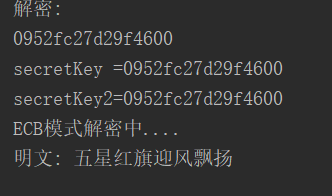
|  |  |  |  |
| --- | --- | --- | --- |
| 用例编号 | No.3 | 模块名称 | SM2 和SM4 混合算  法 |
| 测试方法 | 黑盒测试 | 测试日期 | 2018.5.11 |
| 测试说明 | 使用SM2 和SM4 混合算法对版权信息区块进行加解密 | | |
| 预置条件 | 在进行攻击情报传递时，需要对情报内容数据加密 | | |
| 判断准则 | 对比加密前和解密后数据的一致性判断算法的正确性 | | |
| 测试输入 | 数据明文：五星红旗迎风飘扬  国密规范测试私钥  prikS: EosvqL1DPGwGjI2APf95eSpRmlUXGxtlDCNmHRWJcmM=  国密规范测试公钥  pubkS: BArkx3mKoPEZRxvuEYJb5GICu3nipYRElel8BP9N8lSKfAJA+I8c1OFjUqc8F7fxbwc1PlOhdtaEqf4Ma7eY6Fc= | | |
| 测试输出 | 验签结果: true  secretKey =dccfec8a27854208  secretKey2=dccfec8a27854208  解密出明文: 五星红旗迎风飘扬 | | |
| 测试评价 | 测试通过，版权信息区块数据明文经过SM2 和SM4 混合算法加解密后数据未发生变化。 | | |

下图是测试SM2 和SM4 混合算法的输出结果。









3.3.4 未知病毒发现算法测试

3.3.5 红黑树病毒匹配算法测试

3.4 功能测试

3.4.1 未知病毒检测模块

3.4.2 攻击者追踪模块

3.4.3 实时受攻击情况展示模块

3.4.4 数据传输安全性测试

|  |  |  |  |
| --- | --- | --- | --- |
| 用例编号 | No.3 | 模块名称 | 数据传输安全性测试 |
| 测试方法 | 黑盒测试 | 测试日期 | 2018.5. |
| 测试说明 |  | | |
| 预置条件 |  | | |
| 判断准则 |  | | |
| 测试输入 |  | | |
| 测试输出 |  | | |
| 测试评价 |  | | |

3.5 性能测试

3.5.1 安全攻击负载测试

3.5.2 可视化测试

四、创新性说明

5.1 高效的大数据平台架构

此于知识图谱的网络安全威胁预警系统中所搭建的大数据平台是重要的一个组成部分，是系统的一个基本点所在，也是系统的一个创新点。大数据平台用来解决病毒感知有着他独特的优势。大数据平台是实现病毒的检索、预警等基本功能的基本，也使得我们实现自学习的、自生成的知识图谱和黑客发现等创新功能的构想得以变成现实。并且，大数据平台的很多特性成就了此系统的很多特性，它使得系统高效、快速、及时、准确。大数据平台的利用是本系统的一大创新！

5.2 可自学习、自生成的知识图谱

5.3 可追踪溯源的黑客发现策略

病毒的防护和预警是一个安全系统的基本功能，但也是基础功能。如果能直至根源地解决问题，无疑是一个更深层面的解决方案。黑客往往躲在黑暗中，把自己的主机隐藏在层层的傀儡机后面，本系统中提出的可追踪溯源的黑客发现策略便是一个解决根源的策略，系统通过不断的递归查询和比对，一步一步地识别到傀儡机，顺藤摸瓜，一层一层地往上梳理，最终达到顶层，解决病毒传播的源头来达到防护目的，无疑是病毒防护系统的一个创新。

5.4 B/S架构的通信安全

在基于知识图谱的网络安全威胁预警系统中数据的传输的安全性问题有国密SM4算法提供保护。相较于其他国际算法，如MD5,DES或者RSA，首先，使用国家密码局发福的算法更加符合国情，对于国人来说更加自主可控，安全性更高，国密SM4算法性能更加优良；其次，将国密SM4算法应用于大数据服务器的加解密中，是的数据传输过程更加安全可靠，防止内容被恶意篡改。在攻击记录和受攻击情况的传播过程中，考虑到SM4算法加密速度快和SM2算法加密安全性搞、密钥管理简单的优点，对区块中数据使用国密SM2和SM4混合算法进行加密，国密SM4算法使用SM2算法动态协商的密钥进行数据的加密，所以加密数据的安全性就依赖于国密SM2协商密钥算法的安全性，国密SM4利用分组加密的形式，在传输信道中传输效率更高，速度更快。

5.5实时更新的自适应识别算法

五、总结

参考文献

[1]基于数据挖掘的网络安全态势分析 姚钦锋 2012.06