ICS 35.030
CCS L 80

T/CCIA

中 国 网 络 安 全 产 业 联 盟 技 术 规 范

T/CCIA XXX—XXXX

网络安全技术 病毒防治产品互联互通接口内容和格式

Cybersecurity technology—Antivirus products interface contents and format for interconnectivity

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国网络安全产业联盟　　发 布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国网络安全产业联盟提出。

本文件由中国网络安全产业联盟归口。

本文件起草单位：北京安天网络安全技术有限公司、北京赛西科技发展有限责任公司、国家信息中心、中国电子技术标准化研究院、北京天融信网络安全技术有限公司、杭州安恒信息技术股份有限公司、深信服科技股份有限公司、北京神州绿盟科技有限公司、北京升鑫网络科技有限公司、启明星辰信息技术集团股份有限公司、北京山石网科信息技术有限公司、江苏省未来网络创新研究院。

本文件主要起草人：孙洪伟、张瑜、许玉娜、张伟坤、匡贺、杨博麟、韩耀光、黄磊、王志鹏、张宁、赵新强、陈韵然、李彦峰、闫桂勋、安高峰、王龑、陈星、田丽丹、孙凌、王彦磊、卞建超、胡月、蒋发群、梁伟、付巍、张广兴等。

网络安全技术 病毒防治产品互联互通接口内容和格式

1 范围

本文件规定了病毒防治产品实现互联互通的接口内容和格式。

本文件适用于指导病毒防治产品互联互通的设计、开发、应用和测试。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 37090-2018 信息安全技术 病毒防治产品安全技术要求和测试评价方法

GB/T 25069-2022 信息安全技术 术语

GB/T AAAAA.1-20XX 网络安全技术 网络安全产品互联互通 第1部分：框架

GB/T AAAAA.3-20XX 网络安全技术 网络安全产品互联互通 第3部分：告警信息格式

3 术语和定义

GB/T 37090-2018和GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

病毒防治产品 antivirus products

用于检测发现或阻止恶意代码的传播以及对主机操作系统、应用软件和用户文件的篡改、窃取和破坏等的产品。

4 概述

病毒防治产品通过定制或使用内置的接口服务，实现与安全管理系统的信息共享和安全功能指令协同。病毒防治产品与安全管理系统互联互通的信息为告警信息，互联互通的功能指令包括恶意代码检测和恶意代码处理，示意图见图1。

病毒防治产品互联互通的通信接口见附录A。

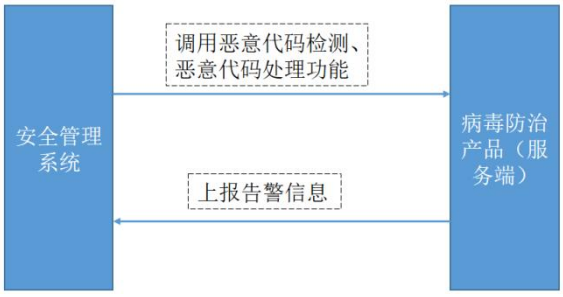

图 1 病毒防治产品互联互通示意图

5 字段类型取值

信息属性结构表中，字段类型的取值见表1。

表 1 字段类型的取值

字段类型	说明
字符型（string）	一种以字母、数字、汉字和其他字符形式表达的数据类型。
整型（int）	一种用任意实数表达的数据类型。
日期时间型（datetime）	一种通过 YYYY-MM-DD hh：mm：ss 的形式表达时间的值的类型。
数组型（array）	一系列类似数据的集合。

6 病毒防治产品报送的信息内容和格式

6.1 概述

病毒防治产品与安全管理系统互联互通的告警信息由通用信息和专有信息组成，通用信息是描述各类告警的共性信息，专有信息是描述不同类别告警的信息，包括告警分类基础信息和告警子类扩展信息。

示例1：以恶意程序告警中的病毒告警为例，其描述格式为：告警通用信息（表3）+恶意程序告警基础信息格式（表4）+计算机病毒告警扩展信息格式（表5）。

示例2：以其他告警中的根工具包告警为例，其描述格式为：告警通用信息（表3）+恶意程序告警基础信息格式（表4）+根工具包告警扩展信息格式（表12）。

告警信息格式示例参见附录B.1。

6.2 告警信息分类代码表

病毒防治产品涉及的互联互通告警信息分类代码见表2。

表 2 告警信息分类代码表

告警信息分类	告警信息子类	英文名称	分类代码
恶意程序告警	计算机病毒告警	computer virus alarm	01001
	网络蠕虫告警	cyber worm alarm	01002
	特洛伊木马告警	trojan horse alarm	01003
	黑客工具告警	Hacktool alarm	01004
	灰色软件告警	grayware alarm	01005
	勒索软件告警	ransomware alarm	01006
	挖矿软件告警	miner virus alarm	01007
其他恶意程序告警	风险软件告警	riskware alarm	99001
	根工具包告警	rootkit alarm	99002
	引导工具包告警	bootkit alarm	99003
	包裹炸弹告警	archive bomb alarm	99004

	其他告警子类	Other alarm	999999

6.3 告警通用信息

告警通用信息格式见表3。

表 3 告警通用信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	告警时间	alarmTime	告警发生时间，例 2024-10-28 11:32:23	日期时间型	是
2	告警等级	alarmLevel	1-低危 2-中危 3-高危	整型	是
3	告警名称	alarmName	告警信息名称	字符型	是
4	告警描述	alarmDesc	对告警的详细描述、说明	字符型	是
5	告警类型	alarmCategory	1-恶意程序告警，2-网络攻击告警，3-数据安全告警，4-异常行为告警，5-其他告警	整型	是
6	告警子类	alarmSubCategory	告警子类，见表 2	字符型	是
7	产品类型	devType	D201-主机恶意代码防治，C202-网络恶意代码防范	字符型	是
8	产品地址	devIp	病毒防治产品 IP 地址	字符型	是
9	受害对象 IP	victimIP	受害对象的 IP 地址，支持 ipv4、ipv6 格式	字符型	是
10	受害对象端口	victimPort	受害对象所被利用的端口，例 8080	字符型	否
11	资产标识	assetId	资产所属组织分配的资产标识信息	字符型	是
12	处置方式	disposeType	1-已处理 2-待处理	整型	是
13	是否加密	encryption	告警所采集的网络安全信息是否加密，1-非加密，2-加密	整型	是
14	产品型号	devID	病毒防治产品硬件型号	字符型	是
15	产品版本	devVer	病毒防治产品软件版本	字符型	是
16	产品厂商	devVenodor	病毒防治产品厂家名称	字符型	是
17	告警所属网络	alarmArea	告警所属的网络区域，如互联网、内网等	字符型	否
18	源 IP	sourceIP	对受害对象发起攻击或访问的 IP 地址，支持 ipv4、ipv6 格式	字符型	否
19	源端口	sourcePort	对受害对象发起攻击或访问的的端口	字符型	否
20	协议	protocol	承载的传输层协议或应用层协议	字符型	否
21	状态	state	攻击是否成功的状态，1-失败,2-成功,3-尝试，4-未知	整型	否
22	是否上报	report	告警信息是否需要上报有关主管部门，1-需要,2-不需要	整型	否
23	扩展字段	-	在完整告警信息之后可增加自定义扩展字段	-	否

6.4 告警专用信息

6.4.1 恶意程序告警基础信息

恶意程序告警基础信息格式见表4。

表 4 恶意程序告警基础信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	恶意程序名称	programName	恶意程序的名称	字符型	是
2	文件地址	filePath	恶意程序在计算机中的存放位置	字符型	是
3	哈希值	fileHash	恶意程序固定长度散列值	字符型	是
4	运行环境	platform	恶意程序的运行环境	字符型	是
5	家族	family	恶意程序的家族名称	字符型	是
6	变种	Variant	同一恶意程序家族的变种	字符型	否
7	行为标签	behavior	恶意程序的风险与行为标签	字符型	否
8	黑客组织	organization	恶意程序相关黑客或组织	字符型	否

6.4.2 恶意程序告警子类扩展信息

恶意程序告警子类扩展信息格式见表5至表11。

表 5 计算机病毒告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程名	process	计算机病毒执行进程名称	字符型	是

表 6 网络蠕虫告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程名	process	蠕虫执行进程名称	字符型	是

表 7 特洛伊木马告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程名	process	木马执行进程名称	字符型	是
2	回连域名	backConnDomain	木马回连的域名	字符型	否
3	回连邮箱	backConnEmail	木马回连的邮箱	字符型	否
4	回连 IP	backConnIp	木马回连的 IP	字符型	否

表 8 黑客工具告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程名	process	黑客工具执行进程名称	字符型	是
2	分类	subType	黑客工具的分类，包括但不限于网络嗅探工具、密码破解工具、渗透测试工具等	字符型	否

表 9　灰色软件告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	分类	subType	灰色软件的分类，包括但不限于流氓软件、捆绑软件、广告件等	字符型	否

表 10　勒索软件告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程名	process	勒索软件执行进程名称	字符型	是
2	加密算法	algorithm	勒索软件使用的加密算法	字符型	否

表 11　挖矿软件告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	进程名	process	挖矿软件执行进程名称	字符型	是
2	矿池地址	miningPoolIp	矿池 IP 地址	字符型	否
3	子域名列表	subdomainList	子域名列表	字符型	否

6.4.3　其他恶意程序告警子类扩展信息

其他恶意程序告警子类扩展信息见表 12 至表 13。

表 12　根工具包告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	分类	subType	根工具类型，包括但不限于固件 rootkit、内核模式 rootkit、用户模式 rootkit、启动加载器 rootkit 等	字符型	否

表 13　引导工具包告警扩展信息格式

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	加载位置	loadLocation	引导工具的加载位置，包括但不限于 MBR、VBR、BIOS、UEFI 固件等	字符型	否

7　病毒防治产品接收的功能指令内容和格式

7.1　概述

病毒防治产品互联互通的功能指令接口为恶意代码防护功能，通过特征匹配、注册表查找等方式，检测发现病毒、木马、蠕虫等恶意代码，并对其进行清除或隔离等操作。互联互通功能指令接口数据格式示例参见附录B.2。

7.2　恶意代码检测

用于安全管理系统向病毒防治产品联动恶意代码检测功能指令，添加、删除文件或进程黑名单接口参数见表14，添加、删除文件或进程白名单接口参数见表15，下发恶意代码检测任务接口参数见表16。

表 14　添加、删除文件或进程黑名单

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	哈希值	fileHash	恶意代码固定长度散列值	字符型	是
2	进程绝对路径	process	恶意代码执行进程绝对路径	字符型	是

表 15　添加、删除文件或进程白名单

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	哈希值	fileHash	恶意代码固定长度散列值	字符型	是
2	进程绝对路径	process	恶意代码执行进程绝对路径	字符型	是

表 16　下发恶意代码检测任务

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	设备标识	uuids	要清除恶意代码的机器唯一标识集合，空数组代表全部扫描，例["deviceuuid1","deviceuuid2"]	数组型	是
2	处置方式	disposeType	1-自动处置 2-暂不处置 3-人工处置	整型	是
3	扫描方式	scanType	1-全盘扫描 2-快速扫描	整型	是

7.3　恶意代码处理

用于安全管理系统向病毒防治产品联动恶意代码处理功能，主要面向上级平台对下级平台发生告警事件后的统一处理指令。下发恶意代码处理任务接口参数见表17。

表 17　下发恶意代码处理任务

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	设备标识	uuids	要清除恶意代码的机器唯一标识集合，空数组代表全部扫描，例["deviceuuid1","deviceuuid2"]	数组型	是
2	清除类型	cleanType	清除并隔离的文件标识类型,1-文件绝对路径 2-文件 hash	整型	是
3	清除集合	cleanVal	恶意代码清除集合 ["C:\\test.exe","D:\\smp.exe"]	数组型	是

附 录 A
（资料性）
病毒防治产品互联互通通信接口

A.1 病毒防治产品互联互通上报信息通信接口

病毒防治产品应支持通过接口上报互联互通信息。

A.2 病毒防治产品互联互通下发功能指令通信接口

A.2.1 通信协议

病毒防治产品通信接口和数据传输应采用统一的加密协议。当使用HTTPS协议时，应通过POST/GET/PUT/DELETE方式进行数据请求，编码格式统一为UTF-8，说明如下：

POST方法：新建操作时使用；

GET方法：查询及批量查询时使用；

PUT方法：修改及更新操作时使用；

DELETE方法：删除操作时使用。

本协议规约不改变现有HTTP标准的定义，实现者可以充分利用开发语言的HTTP工具包进行扩充。

A.2.2 请求 URL 结构

请求URL通信规约结构定义见下图。

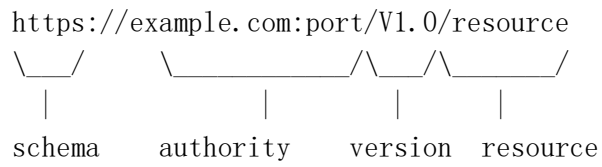

图 A.1 请求 URL 通信规约结构定义图

请求URL字段定义见下表。

表A.1 请求URL字段定义表

字段	说明	字段类型	是否必填
schema	本文件规定 schema 采用 https	字符型	是
authority	提供 API 服务的主机名称（或 ip）以及端口	字符型	是
version	版本号，如 v1、v1.0 等，可不填写	字符型	否
resource	操作的资源路径，例 addinfos 等	字符型	是

附 录 B
（资料性）
病毒防治产品互联互通接口数据格式示例

B.1 告警信息格式示例


```
{
 "alarmTime":"2021-12-21 12:33:24",
 "alarmLevel": 1,
 "alarmName": "恶意程序",
 "alarmDesc": "业务平台服务器遭受计算机病毒攻击，……",
 "alarmCategory": 1,
 "alarmSubCategory": "01001",
 "devType": " D201",
 "devIp": "1.1.1.1",
 "victimIP": "2.2.2.2",
 "victimPort": "8080",
 "assetId": "D642D4923987B9F637639AEA664512DA",
 "disposeType": "1",
 "encryption": 1,
 "devID": " ZD4000-UF ",
 "devVer": " ZD4000v2.0",
 "devVenodor": "XXX公司",
 "alarmArea": "互联网",
 "sourceIP": "51.1.1.1",
 "sourcePort": "443",
 "protocol": "TCP",
 "state": "3",
 "programName":" Voluminer ",
 "filePath": "/etc/.....",
 "fileHash": "d5744897e47fb6d78b726e9ff0c9fa70e0013a0d4f0a757af8ec0b812664b828",
 "platform": "Win32",
 "family": " Lockbit",
 "variant ": "",
 "behavior": "",
 "organization": "匿名者",
```

```
    "process":"123.exe ",
    "filePath":  "/etc/....."
  }
```


B.2 功能指令接口数据格式示例

请求样例


```
{
  "action": "allow",
  "target": {
    "fileHash": {
      "md5": "xxxxxxxxx"
    }
  },
  "args": {
    "ipv4Net": "1.2.3.0/24"
  }
    }
```


响应样例


```
{
  "statusCode ":0,
  "statusText": "success"
    }
```

参考文献

[1] GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南

[2] RFC 4627 JSON应用与媒体类型[The application/json Media Type for JavaScript Object Notation (JSON]