ICS 33.040
M 16

YD

中华人民共和国通信行业标准

YD/T 2251-2011

国家网络安全应急处理平台安全信息获取接口要求

National network security emergency responsing platform interface specification for security information access

2011-06-01 发布　　2011-06-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言

本技术规定根据国家网络安全应急处置的要求，参考GB/T 2260-2007《中华人民共和国行政区划代码》、GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》、GB/T 22240-2008 《信息安全技术 信息系统安全等级保护定级指南》、YD/T 1827-2008《网络安全事件描述和交换格式》、YD/T 1729-2008《电信网和互联网安全等级保护实施指南》等相关国际国内标准，同时考虑到国内电信运营商网络安全事件管理系统或网管系统的实际情况制定而成。本技术规定主要由网络安全事件分类分级、事件数据格式交换要求组成。

本技术规定的附录A和附录B作为规范性目录，附录C作为资料性附录。

本技术规定由中国通信标准化协会提出并归口。

本技术规定起草单位：国家计算机网络应急技术处理协调中心、清华大学、中国科学院计算技术研究所、中国联合网络通信集团有限公司、中国电信集团公司、中国移动通信集团公司、北京启明星辰信息安全技术有限公司、北京天融信公司、中兴通讯股份有限公司、东软集团股份有限公司、哈尔滨安天科技股份有限公司。

本技术规定主要起草人：袁春阳、孙东红、周勇林、舒　敏、焦绪录、殷丽华、林　平、何清林、张　超、王健斌、汤泰鼎、刘仁勇、李青山、徐晓琳、肖新光、纪玉春、徐　原、赵　阳、刘　楠。

国家网络安全应急处理平台安全信息获取接口要求

1 范围

本标准规定了网络安全应急处理平台与基础电信网络或重要信息系统的集中式网络安全事件管理系统或网管系统的接口，包括接口的功能要求和接口协议。

本标准主要适用于网络安全应急处理平台、集中式网络安全事件管理系统及网管系统。

2 规范性引用文件

下列文件中的条款通过本技术规定的引用而成为本技术规定的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本技术规定。然而，鼓励根据本技术规定达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本技术规定。

GB/T 2260-2007　　中华人民共和国行政区划代码

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全事件　Security Event

由计算机信息系统或者网络中的各种计算机设备，例如主机、网络设备、安全设备等发现并记录下的各种可疑活动以及产生的各类故障事件等。

3.2

网络设备　Network Device

承担网络通信的设备，主要包括路由器、交换机等。

3.3

安全设备　Security Device

承担某种安全职责的传统设备，主要包括防火墙、入侵检测系统等。

3.4

操作系统　Operating System

在服务器或客户端运行的系统软件，负责管理各种系统资源，如 Windows NT/2000/XP、Linux、Unix 等。

3.5

应用系统　Application System

负责提供某种特定服务的软件系统，如 Web、Ftp、Mail、DBMS 等。

3.6

威胁　Threat

对系统、组织及其资产构成潜在破坏能力的可能性因素或者事件。

3.7

漏洞　Vulnerability

在系统的设计、实现或者运行和管理中的缺陷或弱点，这些缺陷或弱点可能会被利用，以突破系统的安全策略，其中部分具有国际上通用的CVE编号。

3.8

安全对象　Security Object

主要分为网元设备、安全基础防护系统、安全支撑系统。比如，主机服务器、交换机、路由器等为网元设备，如防火墙、入侵监测系统、反病毒系统等为安全基础防护系统；日志审计系统、账号口令管理系统、VPN系统、终端管理等为安全支撑系统。

3.9

XML模式　XML Schema

万维网联盟（World Wide Web Consortium）W3C 推荐的XML标准，用来定义XML文档和相关规范，以便提供一种灵活的方法来描述用于标记XML文档的合法构建模块。

3.10

国家网络安全应急处理平台　National Network Security Emergency Responsing Platform

为发现整体性安全事件和及时预警提供支撑的技术平台，接收来自运营商和重要信息系统等的各类安全事件，并进行综合汇总、分析。以下简称“应急处理平台”。

3.11

集中式网络安全事件管理系统　Centralized Network Security Events Management System

能够将来自网络传输设备（如路由器、交换机）、网络安全设备（如防火墙、入侵检测系统）等安全对象的安全信息进行集中分析和统一处理的管理系统。本标准中的集中式网络安全事件管理系统，是指基础电信网络或重要信息系统网络的集中式网络安全事件管理系统，如SOC中心、4A系统等。

3.12

安全管理系统　Security Management System

本标准的安全管理系统是指集中式网络安全事件管理系统、网管系统以及其他相关管理系统。

4　缩略语

下列缩略语适用于本文件。

4A	Account/Authentication/Authorization/Audit	账号/认证/授权/审计
DBMS	DataBase Management System	数据库管理系统
HIDS	Host Based Intrusion Detection	主机入侵检测系统
IDS	Intrusion Detection System	入侵检测系统
IPS	Intrusion Prevention System	入侵防护系统
NTMS	Network Traffic Management System	网络业务管理系统
NIDS	Network　Based Intrusion Detection	网络入侵检测系统
SOC	Security Operation Center	安全管理中心
TMS	Terminal Management System	终端管理系统
UTM	United Threat Management	统一威胁管理
VPN	Virtual Private Network	虚拟专用网络
XML	eXtensible Markup Language	可扩展标识语言

5 系统概述

应急处理平台与安全管理系统的接口关系如图1所示。

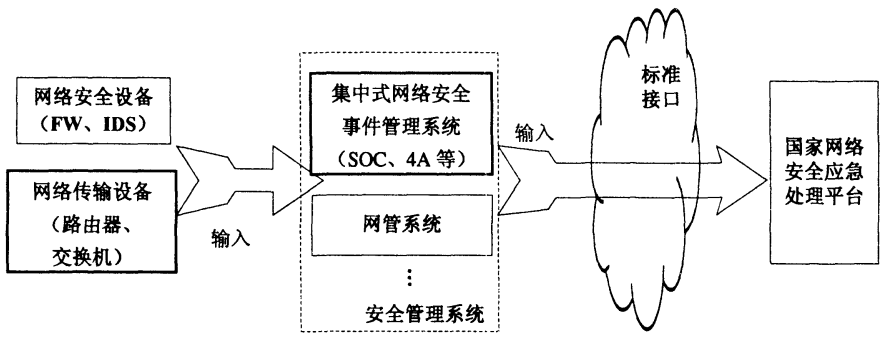


图 1 国家网络安全应急处理平台与安全管理系统的接口关系

应急处理平台从安全管理系统中获取安全事件。本标准对这些事件进行分类分级，实现统一描述，并结合跨多自治域网络安全监测需求和基础电信网安全管理的实际情况，规定安全事件的具体内容。通过本标准规定的接口，应急处理平台可以对来自多个自治域的大量网络安全事件进行综合分析、协调处置。

安全事件原始来源于基础电信网络或重要信息系统网络的 SOC、4A、网管系统、异常流量管理系统、防火墙、入侵检测系统、VPN、病毒过滤网关、防垃圾邮件系统、反病毒系统、漏洞扫描器、安全审计系统、操作系统、应用系统、交换机、路由器等系统。安全管理系统应按照本标准要求，对事件信息进行转换后，发送给应急处理平台。

应急处理平台通过本标准定义的接口，从安全管理系统获取网络安全事件，针对大规模分布式拒绝服务攻击（DDoS）、蠕虫、木马、僵尸网络等，对来自不同安全管理系统的安全事件进行汇总与分析，发现针对基础电信网络和重要信息系统的网络安全事件，整合数据并统一提供分析报表和主动预警，为相关部门的网络安全监管和决策提供依据。

6 安全事件分类

6.1 安全事件基本类型

根据安全事件之间的共性和差异，按基本类型、子类型、详细类型三个层次对安全事件进行分类。

本标准定义了 8 个，安全事件基本类型，见表 1。

表1 安全事件基本类型表

基本类型名称	分类编号	事件描述
操作记录类	1	记录各种操作事件，包括访问、配置变更、软件安装、申请、设备操作命令等
状态信息类	2	说明系统、应用、网络等运行的安全状态
信息刺探类	3	通过扫描、嗅探、业务模拟等方式获得系统及网络信息的各类事件，也包括可能伴随的掩护和躲避行为所产生的事件
恶意代码类	4	与威胁到系统安全的程序相关的事件，具体子类型定义见 6.3
攻击入侵类	5	利用系统及网络缺陷实施攻击的事件以及攻击造成的结果事件，具体子类型定义见 6.4
信息危害类	6	通过各种手段（如：欺骗、垃圾信息、篡改等），危害到了信息的保密性、完整性、可用性等安全属性的事件，具体子类型定义见 6.5
设备设施故障类	7	设备、系统、应用及网络的故障报告、异常报告等相关事件，具体子类型定义见 6.6
其他类	0	不属于以上几类的其他事件

操作记录类、信息刺探类安全事件主要针对系统或网络内部的维护，一般不会对基础电信网络或重

要信息系统造成严重的安全影响。应急处理平台主要接收与网络安全攻击相关的状态信息类、恶意代码类、攻击入侵类、信息危害类和设备设施故障类事件。本技术规定对这 5 类事件进一步划分子类型，各子类型的详细定义见 6.2、6.3、6.4、6.5 和 6.6。

6.2 状态信息类安全事件分类

状态信息类事件是说明系统、应用、网络等安全状态的信息。

状态信息类安全事件子类型定义见表2。

表2 状态信息类安全事件子类型

子类型名称	子类型编号
漏洞告警信息	201
其他	202

6.3 恶意代码类安全事件分类

恶意代码类安全事件是指蓄意制造、传播恶意代码，或是因受到恶意代码的影响而导致的告警事件。恶意代码是指插入到信息系统中的一段程序，危害系统中数据、应用程序或操作系统的保密性、完整性或可用性，或影响信息系统的正常运行。

恶意代码类安全事件子类型定义见表3。

表3 恶意代码类安全事件子类型

子类型名称	子类型编号
计算机病毒	401
网络蠕虫	402
僵尸软件	403
木马	404
网页挂马	405
跨站脚本 XSS	406
其他	409

6.4 攻击入侵类安全事件分类

攻击入侵类安全事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的安全事件。

攻击入侵类安全事件子类型定义见表4。

表4 攻击入侵类安全事件子类型

子类型名称	子类型编号
拒绝服务攻击	501
漏洞攻击	502
蠕虫攻击	503
后门攻击	504
猜测口令	505
非法访问	506
域名劫持	507
CGI攻击（包括注入攻击等）	508
其他	599

6.5 信息危害类安全事件分类

信息危害类安全事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的安全事件。

信息危害类安全事件子类型定义见表5。

表5 信息危害类安全事件子类型

子类型名称	子类型编号
网页篡改	601
网络仿冒（钓鱼）	602
垃圾信息（如垃圾邮件）	603
信息泄露与窃取（未授权用户无意或有意获取信息）	604
其他	609

6.6 设备设施故障类安全事件分类

设备设施故障类安全事件是指设备、系统、应用及网络的故障报告、异常报告等相关事件，如：路由器瘫痪、互联网链路故障等。

设备设施故障类安全事件子类型定义见表6。

表6 设备设施故障类安全事件子类

子类型名称	子类型编号
设备故障（如设备自身异常等）	701
通信线路故障（如通信链路异常等）	702
系统功能失效（某些系统功能失效）	703
运行环境故障（如温度异常、电源异常等）	704
性能门限告警（如CPU、内存、硬盘等超过额定限度等）	705
处理故障（如录入、配置故障等）	706
其他	709

6.7 安全事件详细分类

针对安全事件子类型中的某些事件，可进一步细分。事件详细分类见表 7。

表7 事件详细分类

事件名称	详细类型编号	子类型编号	协议类型
HTTP Flood	501001	501	9
ICMP Flood	501002	501	6
UDP Flood	501003	501	4
TCP SYN Flood	501004	501	5
TCP Flood	501005	501	5
MultiPro Flood	501006	501	3
Connection-Flood	501007	501	
其他拒绝服务	501008	501	

7 安全事件分级

7.1 信息系统和网络分级

根据信息系统和网络所承载的业务对国家安全、经济建设、社会生活的重要性以及业务对信息系统和网络的依赖程度，在本标准中将信息系统和网络按重要程度划分为三级，包括特别重要、重要和一般。

——特别重要

按照 GB/T 22240-2008 定级为 4 级及其以上的信息系统在本标准中属于特别重要系统；

或按照 YD/T 1729-2008 定级为 4 级及其以上的系统和网络在本标准中定为特别重要的系统和网络。

——重要

按照 GB/T 22240-2008 定级为 3 级的信息系统在本标准中属于重要系统；

或按照 YD/T 1729-2008 定级为 3.1 和 3.2 级的系统和网络在本标准中属于重要系统和网络。

——一般

其他的系统和网络其重要性属于一般。

7.2 安全事件级别定义

依据安全事件对安全对象造成损失的程度、威胁以及涉及信息系统和网络的重要程度等因素，参考 GB/Z 20986-2007 中对安全事件级别的定义，在本标准中将安全事件的级别分为 4 级，包括：

——非常重要事件

对于特别重要系统的重大（II 级）及以上事件、重要系统的特别重大（I 级）事件，级别为非常重要；

——重要级别事件

对于特别重要系统的较大（III 级）事件、重要系统的重大（II 级）事件，级别为重要；

——中等级别事件

对于特别重要系统的一般（IV 级）事件、重要系统的较大（III 级）事件、一般系统的重大（II 级）事件，级别为中等；

——一般级别事件

对于重要系统的一般（IV 级）事件、一般系统的较大（III 级）和一般（IV 级）事件，级别为一般。

8 安全事件统一描述格式

对网络安全事件的统一描述格式见表 8。该格式中的信息主要由报送信息的设备、产生告警的系统信息和事件本身的信息三部分组成。

表8 网络安全事件统一描述格式

数据项名称	名 称	数据类型	是否必需	说 明
event _id	发送时安全事件的唯一标识	varchar(52)	是	由安全管理系统产生的，用于标识安全事件的唯一编号。应急处理平台可用该号追踪事件来源。编码方式建议为“安全事件来源单位编码+自由编码”的形式，其中安全事件来源单位编码见附录 A.2
senddev_ip	发送安全事件的设备地址	varchar（15）	是	发送该事件的设备地址
senddev_mac	发送安全事件的设备的 MAC 地址	varchar（17）	否	以分隔符隔离的 6 字节地址
send_dev_type_id	发送安全事件的系统类型	varchar(4)	是	该设备的设备类型名称：见附录 A.3 设备类型编码方式
warn_sys_locate	报警系统位置	varchar(7)	是	产生事件告警信息的系统位置由省市份四位和单位编码三位组成。具体编码见附录 A.2

表 8（续）

数据项名称	名　称	数据类型	是否必需	说　明
warn_sys_id	报警系统 ID	varchar(6)	是	产生事件告警信息的系统 ID 由系统类型两位和手工填写四位构成
warn_sys_ip	报警系统 IP 地址	varchar（15）	是	产生该事件告警的设备地址。例如防火墙产生的事件则填写防火墙管理 IP
warn_sys_name	报警系统名称	varchar(50)	否	产生事件告警信息的系统名称
warn_antivirus_sys_id	反病毒系统名称 ID	smallint unsigned	否	为明确病毒命名，该字段说明反病毒系统名称。对于病毒事件类必须填写。反病毒系统称 ID 编码见附录 A.4
warn_sys_netcode	报警系统网络编号	varchar(10)	是	说明产生事件告警信息的系统属于哪个网际网络（即自治域号）。如无自治域号，可以按邮编编写
event_type_id	基本安全事件类型 ID	smallint unsigned	是	见表 9。
event_detail_type_id	详细事件类型 ID	smallint unsigned	否	见 6.7
vuln_id	漏洞编号	varchar(13)	否	即漏洞信息的 CVE 编号，如 CVE-2009-055
name	事件名称	varchar(50)	是	格式如 “HTTP_读命令”
protocol_id	协议类型	smallint unsigned	否	涉及网络协议的事件必填。参照常用协议类型表，未列出的自行填写
feature	特征串	varchar(256)	是	详细事件特征串
range	匹配范围	smallint(5) unsigned	是	匹配前多少个字节
srcip	事件源 IP	int(10) unsigned	否	按网络字节序存
dstip	事件目的 IP	int(10) unsigned	是	按网络字节序存。在病毒、蠕虫类事件中，为感染这些恶意代码的系统 IP
srcport	事件源端口	smallint(5) unsigned	否	按网络字节序存
dstport	事件目的端口	smallint(5) unsigned	否	按网络字节序存
invol	发送流量	bigint(20) unsigned	否	发送的流量。异常流量事件必填。
outvol	接收流量	bigint(20) unsigned	否	接收的流量。异常流量事件必填
inunit	发送流量单位	Smallint(3) unsigned	否	如有发送流量，必填。其中，0：kB；1：MB
outunit	接收流量单位	smallint(3) unsigned	否	如有发送流量，必填。其中，0：kB；1：MB
inpktnum	进入数据包数	bigint(20) unsigned	否	接收数据包数量。异常流量事件必填

表 8（续）

数据项名称	名　称	数据类型	是否必需	说　明
outpktnum	离开数据包数	bigint(20) unsigned	否	发送数据包数量。异常流量事件必填
fail_time	故障发生时间	datetime	是	设备发生故障的时间
isdeal	是否处理	smallint(3) unsigned	否	0 为未处理，1 为已删除，2 为已隔离，3 为其他已处理情况
url	事件相关域名和 URL	varchar(256)	否	网页挂马、域名劫持、CGI 攻击、网络仿冒等涉及域名和 URL 的事件必填
rank	原始危害等级	smallint unsigned	否	直接取原始事件中的某个字符串在初始化部分赋给它即可
merge_count	归并数量	smallint(5) unsigned	是	多个事件归并的数量
time_start	事件归并的开始时间	datetime	是	如为归并事件必填；若事件未归并，则表示事件发生或被发现的时间。
time_end	事件归并的结束时间	datetime	是	如为归并事件必填
event_content	事件内容	text	是	事件内容描述(从原始日志中提取得关键字)，例如 syslog 包所有原始内容
注：“是否必需”字段为上报安全事件时是否应填写的内容				

几个重要子类的安全事件填写指南和实例参见附录 C。

9　数据交换的相关要求

9.1　应上报的安全事件子类型及其基本信息

应急处理平台重点针对 DDoS 攻击、僵尸网络和蠕虫等事件进行综合分析和协调处置，关注危害级别较高的安全事件。安全管理系统向应急处理平台上报的安全事件子类型见表 9。

表9　应上报的安全事件子类型

子类型编号	子类型名称	子类型编号	子类型名称
201	漏洞告警信息	505	猜测口令
401	计算机病毒	506	非法访问
402	网络蠕虫	507	域名劫持
403	僵尸软件	508	CGI 攻击（含注入攻击）
404	木马	601	网页篡改
405	网页挂马	602	网络仿冒
406	跨站脚本 XSS	603	垃圾邮件
501	拒绝服务攻击	604	信息泄露与窃取
502	漏洞攻击	701	设备故障
503	蠕虫攻击	702	通信线路故障
504	后门攻击	703	系统功能失效

9.2　安全事件子类型上报时需填写的基本信息

下面定义每类事件上报时填写的基本信息。

上报的漏洞告警信息事件信息见表 10。

表10 漏洞告警信息上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
漏洞 CVE 编号	vuln-id	否
漏洞名称	name	是
原始严重级别	rank	是
扫描出漏洞的资产 IP	dstip	是
扫描出漏洞的端口	dstport	否
协议类型	protocol_id	否
漏洞扫描产品信息	warn_sys_name	是
漏洞发现时间	time_start	是
漏洞描述	event_content	是

上报的计算机病毒事件信息见表 11。

表11 计算机病毒事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
病毒名称	name	是
反病毒系统名称 ID	warn_antivirus_sys_id	是
传播病毒的 IP 地址	srcip	否
感染病毒的 IP 地址	dstip	是
病毒传播端口号	srcport	否
病毒感染端口号	dstport	否
病毒特征串	feature	是
匹配范围	range	否
原始危害等级	rank	是
病毒描述	event_content	是
是否已清除（消除对系统的影响，如隔离、删除等）	isdeal	否

上报的网络蠕虫事件信息见表 12。

表12 网络蠕虫事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
蠕虫名称	name	是
协议类型	protocol_id	是
传播蠕虫的 IP 地址	srcip	否
感染蠕虫的 IP 地址	dstip	是
蠕虫传播端口号	srcport	否
蠕虫感染端口号	dstport	否
蠕虫特征串	feature	是
匹配范围	range	否
原始危害等级	rank	是
蠕虫描述	event_content	是
是否已清除（消除对系统的影响，如隔离、删除等）	isdeal	否

上报的僵尸软件事件信息见表 13。

表13 僵尸软件报警事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
僵尸软件名称	name	是
协议类型	protocol_id	是
传播僵尸软件的 IP 地址	srcip	否
感染僵尸软件的 IP 地址	dstip	是
僵尸软件感染端口号	dstport	否
僵尸软件特征串	feature	是
匹配范围	range	否
原始危害等级	rank	是
僵尸软件描述	event_content	是
是否已清除（消除对系统的影响，如隔离、删除等）	isdeal	否

上报的木马事件信息见表 14。

表14 木马事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
木马名称	name	是
协议类型	protocol_id	是
传播木马的 IP 地址	srcip	否
感染木马的 IP 地址	dstip	是
木马感染端口号	dstport	否
木马特征串	feature	是
匹配范围	range	否
原始危害等级	rank	是
木马描述	event_content	是
是否已清除（消除对系统的影响，如隔离、删除等）	isdeal	否

上报的网页挂马事件信息见表 15。

表15 网页挂马事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必须
事件名称	name	是
协议类型	protocol_id	否
挂马网页 IP 地址	dstip	否
挂马网页端口号	dstport	否
挂马特征串	feature	是
匹配范围	range	否
包含恶意代码网页的 URL	url	是
原始危害等级	rank	是
描述	event_content	是

上报的跨站脚本 XSS 事件信息见表 16。

表16 跨站脚本 XSS 事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必须
事件名称	name	是
包含跨站脚本的网站 IP 地址	dstip	是
脚本特征串	feature	是
匹配范围	range	否
原始危害等级	rank	是
描述	event_content	是

上报的拒绝服务攻击事件信息见表 17。

表17 拒绝服务攻击事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
事件名称	name	是
协议类型	protocol_id	是
被攻击对象 IP 地址	dstip	是
被攻击对象端口号	dstport	否
发送流量	invol	是
接收流量	outvol	是
发送流量单位	inunit	是
接收流量单位	outunit	是
进入数据包数	inpktnum	是
离开数据包数	outpktnum	是
原始危害等级	rank	是
描述	event_content	是

上报的漏洞攻击事件信息见表 18。

表18 漏洞攻击事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
事件名称	name	是
协议类型	protocol_id	是
被攻击设备 IP 地址	dstip	是
被攻击设备端口号	dstport	否
漏洞攻击特征串	feature	是
匹配范围	range	否
原始危害等级	rank	是
描述	event_content	是

上报的蠕虫攻击事件信息见表 19。

表19 蠕虫攻击事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
事件名称	name	是
协议类型	protocol_id	是
被攻击设备 IP 地址	dstip	是
被攻击设备端口号	dstport	否
蠕虫攻击特征串	feature	是
匹配范围	range	否
原始危害等级	rank	是
描述	event_content	是

上报的后门攻击事件信息见表 20。

表20 后门攻击事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
事件名称	name	是
协议类型	protocol_id	是
攻击源 IP 地址	srcip	是
攻击目标 IP 地址	dstip	是
攻击源端口号	srcport	否
攻击目标端口号	dstport	否
原始危害等级	rank	是
后门攻击事件描述	event_content	是

上报的猜测口令事件信息见表 21。

表21 猜测口令事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
事件名称	name	是
协议类型	protocol_id	是
猜测者 IP 地址	srcip	是
被猜测者 IP 地址	dstip	是
猜测者端口号	srcport	否
被猜测者端口号	dstport	否
原始危害等级	rank	是
恶意猜测口令描述	event_content	是

上报的非法访问事件信息见表 22。

表22 非法访问事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
事件名称	name	是
协议类型	protocol_id	是
非法访问源 IP 地址	srcip	是
非法访问目的 IP 地址	dstip	是
非法访问源端口号	srcport	否
非法访问目的端口号	dstport	否
原始危害等级	rank	是
非法访问事件描述	event_content	是

上报的域名劫持事件信息见表 23。

表23 域名劫持事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
事件名称	name	是
协议类型	protocol_id	否
被劫持的域名	url	是
劫持目标的源 IP 地址	srcip	是
劫持后的 IP 地址	dstip	是
原始危害等级	rank	是
域名劫持事件描述	event_content	是

上报的CGI攻击（含注入攻击）事件信息见表24。

表24 CGI攻击事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必须
事件名称	Name	是
协议类型	protocol_id	是
被攻击网站IP地址	Dstip	是
被攻击的具体URL	url	是
原始危害等级	Rank	是
描述	event_content	是

上报的网页篡改事件信息见表25。

表25 网页篡改事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
事件名称	Name	是
协议类型	protocol_id	否
被篡改网页的IP地址	Dstip	否
被篡改网页的URL	url	是
原始危害等级	rank	是
网页篡改事件描述	event_content	是

上报的网络仿冒事件信息见表26。

表26 网络仿冒事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
事件名称	name	是
协议类型	protocol_id	否
被仿冒网站的IP地址	srcip	是
运行仿冒网站主机的IP地址	dstip	是
被仿冒后的网站URL	url	是
原始危害等级	rank	是
网络仿冒事件描述	event_content	是

上报的垃圾邮件事件信息见表27。

表27 垃圾邮件事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
事件名称	name	是
协议类型	protocol_id	否
垃圾邮件发送源IP地址	srcip	是
垃圾邮件特征串	feature	是
匹配范围	range	否
原始危害等级	rank	是
垃圾邮件描述	event_content	是

上报的信息泄露与窃取事件信息见表28。

表28 信息泄露与窃取事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
事件名称	name	是
协议类型	protocol_id	否
发生信息泄露或窃取设备的 IP 地址	dstip	是
设备端口号	dstport	否
原始危害等级	rank	是
事件描述	event_content	是

上报的设备设施故障类事件信息见表 29。

表29 设备设施故障类事件上报基本信息

基本信息	统一描述格式中的对应字段	是否必需
故障名称	name	是
故障类型	protocol_id	否
故障设备 IP 地址	dstip	是
故障设备端口号	dstport	否
故障发生时间	fail_time	是
事件描述	event_content	是

9.3 应上报的安全事件级别

应急处理平台重点关注危害级别较高的安全事件。安全管理系统凡符合本标准中第 7 章定义的非常重要事件、重要级别事件、中等级别的事件，以及重要系统和特别重要系统发生的设备设施故障类信息都应上报给应急处理平台。应急处理平台可以根据需要动态调整应上报安全事件的级别。

9.4 事件归并要求

为减少传输的数据量，安全管理系统在上报安全事件时，应在规定时间内对某类安全事件依据归并条件进行归并。不同类型事件的归并条件见表 30。对某类事件进行归并时，应满足归并条件的要求。安全管理系统应具有支持归并条件增、删、改的调整能力。

表30 安全事件归并条件列

事件类型编号	事件名称	归并条件
201	漏洞	事件名称，目的地址，目的端口
401	计算机病毒	事件名称，目的地址
402	蠕虫	事件名称，源地址
403	僵尸软件	事件名称，源地址
404	木马	事件名称，源地址
405	网页挂马	事件名称，源地址，目的地址
406	跨站脚本 XSS	事件名称，目的地址
501	拒绝服务攻击	事件名称，源地址，目的地址，目的端口
502	漏洞攻击	事件名称，源地址，目的地址，目的端口
503	蠕虫攻击	事件名称，源地址，目的地址
504	后门攻击	事件名称，源地址，目的地址，目的端口
505	猜测口令	事件名称，源地址，目的地址
506	非法访问	事件名称，源地址，目的地址，目的端口
507	域名劫持	事件名称，源地址，目的地址
508	CGI 攻击	事件名称，目的地址

表 30（续）

事件类型编号	事件名称	归并条件
601	网页篡改	事件名称，源地址，目的地址
602	网络仿冒	事件名称，源地址，目的地址
603	垃圾邮件	事件名称，源地址
604	信息泄露与窃取	事件名称，目的地址
701	设备故障	事件名称，目的地址
702	通信线路故障	事件名称，目的地址
703	系统功能失效	事件名称，目的地址

9.5 安全事件上报的数据格式要求

安全事件上报格式应符合附录 B 中的要求。附录 B 采用 Schema 对安全事件数据统一格式进行定义，并规定了 XML 文件的逻辑结构，定义了 XML 文件中的元素、元素属性以及元素间的关系。

9.6 安全事件实时传输要求

为向应急平台传输安全信息，安全管理中心应同时支持 9.6.1 和 9.6.2 中分别规定的两种数据传输方式。

9.6.1 安全事件传输的通信协议流程

应急处理平台和安全管理系统之间的安全事件传输方式可以采用基于 TCP 协议的 SSL 方式，数据内容为 9.5 规定的 XML 文件格式，连接的安全建立等相关问题遵循通用的 SSL 协议。

在事件传输过程中，安全管理系统应定期向应急响应平台发送保活帧，以确保数据传输时 TCP 连接的可用性，若在一定时间内未接收到保活应答帧则重新建立 TCP 连接。安全事件的上报采用客户/服务器端方式，应急处理平台做为服务器端被动接收安全管理系统发送的安全事件数据。安全管理系统在发送数据的过程中，应定期向应急处理平台发送保活帧，以检测链路状态的可用性。应急处理平台收到保活帧后，向安全管理系统发送保活应答帧。如果安全管理系统在发送保活帧后，在一定时间内未收到保活应答帧，则安全管理系统认为连接已中断，应重新建立新的 TCP 连接后再开始发送数据。

通信流程如图 2 所示。

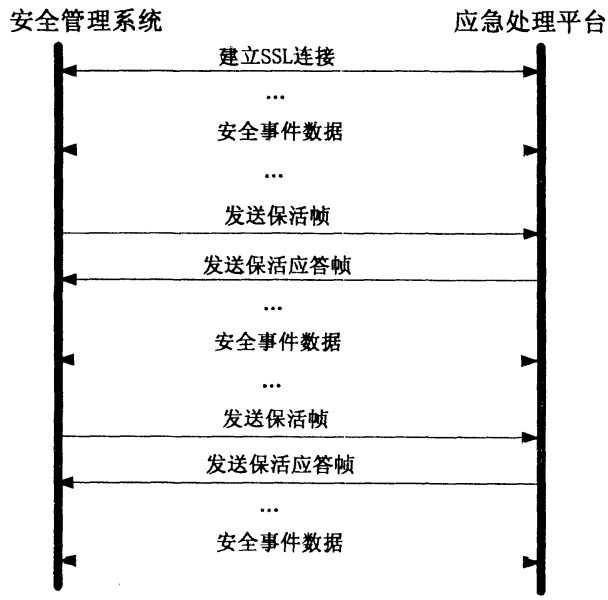
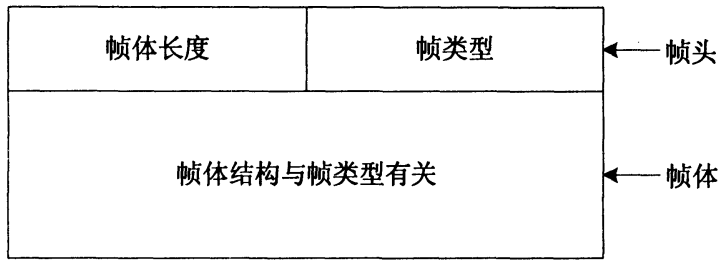


图 2 事件传输的通信协议流程

9.6.2 帧结构定义

帧结构定义见表 31。

表31 帧结构



帧头的定义见表 32。

表32 帧头定义

	字段名	数据类型	长度(字节)	字段描述
帧头	帧体长度	数值	2	不含帧头长度
	帧类型	数值	2	801—保活帧 802—保活应答帧 803—安全事件帧

保活帧的帧体长度为 0。

保活应答帧的帧体长度为 0。

安全事件帧帧体的定义见表 33。

表33 安全事件帧体定义

	字段名	数据类型	长度(字节)	字段描述
帧体	安全事件数据	字符	不限	安全事件的 XML 结构数据（其定义见附录 B）

9.7 安全事件数据的批量传输的通信协议

应急处理平台和安全管理系统之间应支持安全事件的批量传输。传输采用 SFTP 协议，在应急处理平台上建立 SFTP 服务器，安全管理系统定时向 SFTP 服务器批量传送安全事件数据。安全事件数据格式采用 XML 格式，见附录 B。

安全事件数据的传输过程见图 3。

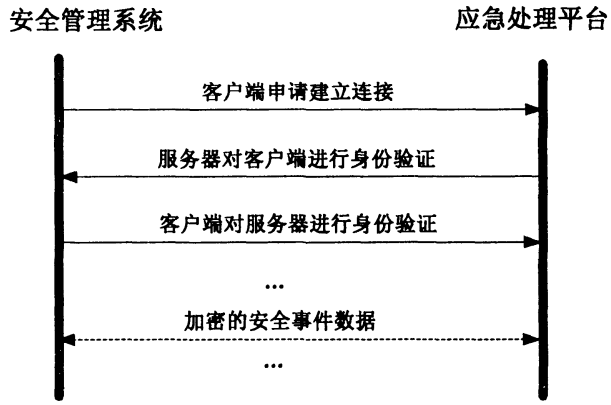


图 3 安全事件批量传输的通信协议流程

（1）SFTP 客户端申请建立连接；

（2）SFTP 服务器对 SFTP 客户端进行身份验证；

（3）SFTP 客户端对 SFTP 服务器进行身份验证；

（4）身份认证成功才可以成功建立连接；

（5）进行数据传输，传输的数据都会被加密。

附 录 A
（规范性附录）
安全事件统一描述格式中的编码规范

A.1 常用协议类型编码方式

表A.1举例说明常见的协议类型编号、名称及其常用参考端口列表，但端口号与协议并无直接对应关系。

表A.1 常用协议类型的编码

编号	协议名称	常用端口	编号	协议名称	常用端口
1	ETHER	0	20	NNTP	119
2	ARP	0	21	IRC	194
3	IP	0	24	AUTH	113
4	UDP	0	25	CHARGEN	19
5	TCP	0	26	SNMP	162
6	ICMP	0	27	ROUTE	520
7	IGMP	0	28	IMAP	143
9	HTTP	80	29	TFTP	69
10	TELNET	23	30	MSRPC	135
11	FTP	21	31	FINGER	79
12	SUNRPC	111	32	RLOGIN	513
13	DNS	53	33	NTAIL	518
14	WHOIS	43	34	ECHO	7
15	SMTP	25	35	TDS	1433
16	POP3	110	37	MSPROXY	1745
17	NETBIOS-NS	137	38	PCT	443
18	NETBIOS-SS	139	39	PPPOE	
19	NETBIOS-DG	138	99	Other	

A.2 安全事件来源单位编码方式

为明确标识安全事件来源的单位信息，对安全事件产生单位用 9 位数字编码表示，前 6 位表示地区编码，后 3 位表示单位编码。其中，地区编码使用 GB/T 2260-2007，省份具体编码见表 A.2；单位编码见表 A.3。例如：运营商集团单位表示为 000000+单位编号，如“中国移动通信集团公司”的编号为 000000002，“中国联合网通信集团有限公司”的编号为“000000004”。

各地运营商单位编号命名方式为省份编号+单位编号，例如“北京移动”的编号为 110000002，“山西联通”的编号为“140000004”。

表A.2 省份编码

省份编号	省份名称	省份编号	省份名称
000000	无归属地	410000	河南省
110000	北京市	420000	湖北省
120000	天津市	430000	湖南省

表 A.2（续）

省份编号	省份名称		省份编号	省份名称
130000	河北省		440000	广东省
140000	山西省		450000	广西壮族自治区
150000	内蒙古自治区		460000	海南
210000	辽宁省		510000	四川省
220000	吉林省		520000	贵州省
230000	黑龙江省		530000	云南省
310000	上海市		540000	西藏自治区
320000	江苏省		550000	重庆市
330000	浙江省		610000	陕西省
340000	安徽省		620000	甘肃省
350000	福建省		630000	青海省
360000	江西省		640000	宁夏回族自治区
370000	山东省		650000	新疆维吾尔族自治区

表 A.3 单位编码

集团编号	集团名称
001	国家计算机网络应急技术处理协调中心
002	中国移动通信集团公司
003	中国电信集团公司
004	中国联合网络通信集团有限公司
005	其他待补充

A.3 设备类型编码方式

设备类型名称见表 A.4。

表 A.4 设备类型的名称

类型编号	设备类型名称		类型编号	设备类型名称
01	Unix/Linux 类主机		13	安全管理中心 SOC
02	Windows 类主机		14	统一威胁管理系统 UTM
03	路由器/交换机		15	应用系统（如 WEB、FTP、Mail、DNS 等）
04	漏洞扫描器		16	访问控制网关 Access Control Gateway
05	防火墙		17	虚拟专用网络 VPN
06	网络入侵检测系统		18	反垃圾邮件系统
07	主机入侵检测系统		19	终端管理系统 TMS
08	反病毒系统		20	网络管理系统 Network Management System
09	4A 系统		21	认证
10	入侵防护系统 IPS		22	流量分析与响应系统
11	数据库		23	审计系统
12	网络业务管理系统 NTMS		99	其他

A.4 反病毒系统ID编码方式

由于厂商对其各类反病毒产品所发现的病毒的命名规则基本相同，因此在对反病毒系统进行编码时，本标准将按照厂商进行统一编码，见表 A.5。

表 A.5 反病毒系统 ID 编码

编 号	厂商编码	厂商名称	主要反病毒产品
1	AHN	安哲秀研究所	安博士防毒墙、防病毒软件、中央管理工具
2	ARC	ArcaBit 公司	反病毒软件
3	ASQ	Emsi 公司	反病毒软件
4	ATV	Avira 公司	防病毒软件
5	AUM	Authentium 公司	反病毒软件
6	AVA	ALWIL Software	反病毒软件
7	AVG	AVG 公司	反病毒软件
8	AVL	安天	安天防线、网络病毒监控系统、网络病毒防御系统
9	AVP	卡巴斯基公司	卡巴斯基反病毒软件、卡巴斯基全功能安全软件、防毒墙
10	BDP	bitdefender 公司	反病毒软件、全方位安全软件、互联网安全套装
11	CA	CA 公司	反病毒软件
12	CLV	Sourcefire 公司	反病毒软件
13	CMO	Comodo 公司	反病毒软件
14	CP	CP Secure 公司	蠕虫检测硬件
15	DRW	Doctor Web 公司	反病毒软件
16	FPT	F-risk 公司	反病毒软件
17	FTN	飞塔公司	终端安全产品
18	GDA	G-Data 公司	反病毒软件
19	IKR	IKARUS 公司	反病毒软件
20	KAV	金山公司	金山毒霸
21	KV	江民公司	江民杀毒软件
22	MCA	McAfee 公司	迈克菲防病毒软件
23	MIC	微软公司	反病毒软件
24	MIC	微软公司	反病毒软件
25	MKS	MKS 公司	反病毒软件
26	NAV	Symantec 公司	诺顿网络安全特警(NIS)、诺顿防病毒软件（NAV）、诺顿 360
27	NAV	Symantec 公司	赛门铁克网关
28	NOD	Eset 公司	防病毒软件
29	NPO	INCA Internet 公司	反病毒软件
30	NVC	norman 公司	反病毒软件
31	PCC	趋势科技	趋势 PC-Cillin，趋势科技杀毒专家(TAV),防毒墙(NVW)
32	PDA	Panda 软件公司	防病毒软件
33	QHT	Quick Heal 科技公司	反病毒软件
34	RAV	瑞星公司	杀毒软件、全功能安全软件、防毒墙
35	SAV	Sophos 公司	反病毒软件
36	SBT	Sunbelt 公司	反病毒与间谍软件
37	SER	F-Secure 公司	反病毒软件

表 A.5（续）

编　号	厂商编码	厂商名称	主要反病毒产品
38	THK	Hacksoft 公司	反病毒软件
39	VBT	VirusBuster 公司	反病毒软件
40	VCD	日月光华公司	光华反病毒软件
41	VCS	韩国 New Tech Wave	驱逐舰杀毒软件
42	VRB	HAURI 公司	反病毒软件
999	other	其他	

附 录 B
（规范性附录）
安全事件数据格式的 Schema 定义

本附录定义了安全事件的 XML 格式。

```
<?xml version="1.0" encoding="UTF-8" ?>
- <xs:Schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
- <xs:element name="security_event">
- <xs:complexType>
- <xs:sequence>
<xs:element name="event_id" type="xs:string" /> <!--安全事件的唯一标识-->
<xs:element name="senddev_ip" type="xs:string" /> <!--发送安全事件的设备地址-->
<xs:element name="senddev_mac" type="xs:string" minOccurs="0" /> <!--发送安全事件设备的 MAC 地址-->
<xs:element name=" send_dev_type_id" type="xs:string" /> <!--发送安全事件的系统类型-->
<xs:element name="warn_sys_locate" type="xs:string" /> <!--报警系统位置-->
<xs:element name="warn_sys_id " type="xs:string" /> <!--报警系统 ID -->
<xs:element name="warn_antivirus_sys_id " type="xs: unsignedShort " /> <!--反病毒系统名称 ID -->
<xs:element name="warn_sys_ip" type="xs:string" /><!--报警系统 IP 地址-->
<xs:element name="warn_sys_name" type=" xs: string" minOccurs="0" /> <!--报警系统名称-->
<xs:element name=" warn_sys_netcode" type="xs:string" /> <!--报警系统网络编号-->
<xs:element name="event_type_id" type=" xs:unsignedShort"/> <!--基本安全事件类型 ID -->
<xs:element name=" event_detail_type_id " type=" xs:unsignedShort"/> <!--详细事件类型 ID -->
<xs:element name="vuln_id" type=" xs: string" /><!--漏洞编号-->
<xs:element name="name" type=" xs:string" /> <!--事件名称-->
<xs:element name="protocol_id" type=" xs:unsignedInt" minOccurs="0" /> <!--协议类型-->
<xs:element name="feature" type=" xs:string" /><!--特征串-->
<xs:element name="range" type=" xs:unsignedShort"/><!--匹配范围-->
<xs:element name="srcip" type="xs:unsignedInt" minOccurs="0" /> <!--事件源 IP -->
<xs:element name="dstip" type="xs:unsignedInt" /><!--事件目的 IP -->
<xs:element name="srcport" type="xs:unsignedShort" minOccurs="0" /> <!--事件源端口-->
<xs:element name="dstport" type="xs:unsignedShort" minOccurs="0" /><!--事件目的端口-->
<xs:element name="invol" type="xs:unsingedLong" minOccurs="0"/> <!--发送流量-->
<xs:element name="outvol" type="xs:unsingedLong" minOccurs="0"/> <!--接收流量-->
<xs:element name="inunit" type="xs:unsingedShort" minOccurs="0"/> <!--发送流量单位-->
<xs:element name="outunit" type="xs:unsingedShort" minOccurs="0" /> <!--接收流量单位-->
```

```
            <xs:element name="inpktnum" type="xs:unsingedLong" minOccurs="0" /> <!--进入数据包数-->
            <xs:element name="outpktnum" type="xs:unsingedLong" minOccurs="0" /> <!--离开数据包数-->
<xs:element name=" fail_time " type=" xs:dateTime " /><!--故障发生时间-->
    <xs:element name="isdeal" type="xs:unsingedShort" minOccurs="0" /><!--是否处理-->
    <xs:element name="url" type="xs:string" minOccurs="0" /><!--事件相关域名和 URL -->
            <xs:element name="rank" type="xs:unsignedShort" minOccurs="0" /> <!--原始危害等级-->
             <xs:element name="merge_count" type="xs:unsignedShort" /> <!--归并数量-->
<xs:element name=" time_start " type=" xs:dateTime " minOccurs="0" /><!--事件归并的开始时间-->
<xs:element name=" time_end " type=" xs:dateTime " minOccurs="0" /><!--事件归并的结束时间-->
<xs:element name="event_content" type=" xs:string " /><!--安全事件内容-->
      </xs:sequence>
   </xs:complexType>
</xs:element>
</xs:Schema>
```

附 录 C
（资料性附录）
部分重点事件填写参考

C.1 状态信息类——漏洞信息

- 填写建议

— 事件主要来源：漏洞扫描系统、网络事件集中管理系统，SOC 等管理系统；

— 收集主要事件类型：关键系统或设备的漏洞信息。

- 事件填写实例

详见表 C.1。

表 C.1 漏洞信息事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.201.57.23
senddev_mac	发送安全事件的设备的 MAC 地址	00-50-56-C0-00-FF
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_0101010001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	201
vuln-id	漏洞 CVE 编号	CVE-2009-055
name	漏洞名称	Baster Rpc Exploit
protocol_id	协议类型	
dstip	存在漏洞的 IP 地址	10.201.57.188
dstport	漏洞涉及的端口号	3545
warn_sys_ip	设备地址	10.201.62.24
rank	原始危害等级	3
merge_count	归并数量	410
time_start	漏洞发现时间	2008-12-04T09:46:31
event_content	漏洞描述	CVE-2009-055
isdeal	是否已清除（消除对系统的影响，如隔离、删除等）	1

C.2 恶意代码类——计算机病毒

- 填写建议

— 事件主要来源：防病毒软件的集中管理系统，SOC 等管理系统；

— 收集主要事件类型：单一病毒大量发作（如：2h 内超过 1000 个），单一病毒无法清除大量发作（如：2h 内超过 100 个），恶意软件。

- 事件填写实例

详见表 C.2 。

表 C.2 计算机病毒事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.201.57.23
senddev_mac	发送安全事件的设备的 MAC 地址	00-50-56-C0-00-FF
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	080001
warn_antivirus_sys_id	反病毒系统名称 ID	1
warn_sys_name	产生告警信息的系统名称	SOC_0101010001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	401
name	病毒名称	WORM_MOFEI.B
protocol_id	协议类型	Anti-Virus
feature	病毒特征串	34gthbd223tgsfrs7g75sd54
range	匹配范围	6
srcip	传播病毒的 IP 地址	10.15.14.7
dstip	感染病毒的 IP 地址	10.201.57.188
srcport	病毒传播端口号	2453
dstport	病毒传播端口号	3545
warn_sys_ip	设备地址	10.201.62.24
rank	原始危害等级	3
merge_count	归并数量	410
time_start	事件归并的开始时间	2008-12-04T09:46:31
time_end	事件归并的结束时间	2008-12-04T23:11:00
event_content	病毒描述	病毒名称:WORM_MOFEI.B。病毒类型：3。染毒文件: 由损害清除服务扫描。处理结果 第一次:success;第二次:unknown
isdeal	是否已清除（消除对系统的影响，如隔离、删除等）	1

C.3 恶意代码类——蠕虫

- 填写建议

— 事件主要来源：防病毒软件的集中管理系统、入侵检测系统、防火墙系统、异常流量管理系统、SOC 等管理系统；

— 收集主要事件类型：单个或者归并的蠕虫事件。

- 事件填写实例

详见表 C.3。

表 C.3 蠕虫事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	9211454
senddev_ip	发送安全事件的设备地址	10.201.57.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-50-56-C0-00-FF
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101004
warn_antivirus_sys_id	反病毒系统名称 ID	1
warn_sys_netcode	网络编号	100180
event_type_id	基本安全事件类型 ID	402
name	蠕虫名称	熊猫烧香
protocol_id	协议类型	5
feature	蠕虫特征串	Jh4hbd223tgsfrs7g75sd54
range	匹配范围	12
srcip	传播蠕虫的 IP 地址	10.5.14.7
dstip	感染蠕虫的 IP 地址	10.0.15. 92
srcport	蠕虫传播端口号	410
dstport	蠕虫感染端口号	134
invol	发送流量	5252
outvol	接收流量	9373
inunit	发送流量单位	0
outunit	接收流量单位	0
inpktnum	进入数据包数	237883453
outpktnum	离开数据包数	352343453
warn_sys_ip	设备地址	10.201.62.24
rank	原始危害等级	3
merge_count	归并数量	0
time_start	事件归并的开始时间	2007-09-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T23:11:00
event_content	蠕虫描述	9211454|34|蠕虫|杀毒成功|2008-04-21 16:32:21|C:/windows/system32/drive.exe|26331|192.168.65.21|13|WGZX|-|-|-
isdeal	是否已清除（消除对系统的影响，如隔离、删除等）	0

C.4 恶意代码类——僵尸软件

- 填写建议

— 事件主要来源：入侵检测系统系统、SOC 等管理系统；

— 收集主要事件类型：僵尸软件事件。

- 事件填写实例

详见表 C.4。

表 C.4 僵尸软件事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.121.77.10
senddev_mac	发送安全事件的设备的MAC地址	34-50-96-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101003
warn_antivirus_sys_id	反病毒系统名称ID	1
warn_sys_netcode	网络编号	100180
event_type_id	基本安全事件类型ID	403
name	僵尸软件名称	Botnet C&Cs
protocol_id	协议类型	4
feature	僵尸软件特征串	2eweg5e5ysfrs7g75sd54
range	匹配范围	12
srcip	传播僵尸软件的IP地址	61.145.75.231
dstip	感染僵尸软件的IP地址	10.147.142.103
srcport	事件源端口	6667
dstport	僵尸软件感染端口号	3453
warn_sys_ip	设备地址	10.201.62.24
rank	原始危害等级	3
merge_count	归并数量	0
time_start	事件归并的开始时间	2008-06-22T09:27:50
time_end	事件归并的结束时间	2008-06-22T09:27:50
event_content	僵尸软件描述	僵尸网络控制服务器特有信息 Botnet C&Cs
isdeal	是否已清除（消除对系统的影响，如隔离、删除等）	0

C.5 恶意代码类——木马

- 填写建议

— 事件主要来源：入侵检测系统系统、SOC 等管理系统；

— 收集主要事件类型：单个或归并的木马事件。

- 事件填写实例

详见表 C.5。

表 C.5 木马事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.21.77.18
senddev_mac	发送安全事件的设备的 MAC 地址	E0-50-96-CD-00-FF
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_antivirus_sys_id	反病毒系统名称 ID	1
warn_sys_name	产生告警信息的系统名称	SOC_010101003
warn_sys_netcode	网络编号	100180
event_type_id	基本安全事件类型 ID	404
name	木马名称	Trojan.DL.Win32.VB.bht
protocol_id	协议类型	4
feature	木马特征串	bd22b6563tgsfrs7g75sd54
range	匹配范围	6
srcip	传播木马的 IP 地址	221.204.249.240
dstip	感染木马的 IP 地址	10.201.62.24
srcport	事件源端口	55
dstport	木马感染端口号	4324
invol	发送流量	552
outvol	接收流量	2573
inunit	发送流量单位	0
outunit	接收流量单位	0
inpktnum	进入数据包数	283453
outpktnum	离开数据包数	32343453
warn_sys_ip	设备地址	10.201.62.24
rank	原始危害等级	3
merge_count	归并数量	0
time_start	事件归并的开始时间	2008-04-21T16:32:21
time_end	事件归并的结束时间	2008-04-21T16:32:21
event_content	木马描述	9211454|34|木马|杀毒成功|2008-04-21 16:32:21||26331|221.204.249.240|13|WGZX|-|-|-
isdeal	是否已清除（消除对系统的影响，如隔离、删除等）	2

C.6 恶意代码类——网页挂马

- 填写建议

— 事件主要来源：恶意代码检测系统、入侵检测系统、SOC 等管理系统；

— 收集主要事件类型：网页挂马事件，恶意代码事件。

- 事件填写实例

详见表 C.6。

表 C.6 网页挂马事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.121.77.10
senddev_mac	发送安全事件的设备的 MAC 地址	E4-50-96-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101003
warn_sys_netcode	网络编号	100180
event_type_id	基本安全事件类型 ID	405
name	事件名称	Malware Website
protocol_id	协议类型	4
feature	挂马特征串	7gd86fg3tgsfrs7g75sd54
range	匹配范围	9
dstip	挂马网页 IP 地址	125.65.109.234
dstport	挂马网页端口号	424
warn_sys_ip	设备地址	10.201.62.24
rank	原始危害等级	3
merge_count	归并数量	0
time_start	事件归并的开始时间	2008-07-03T15:15:06
time_end	事件归并的结束时间	2008-07-03T15:15:06
event_content	描述	恶意代码服务器特有信息， url 地址: http://www.couly.com/a 域名 www.couly.com ip 地址 125.065.109.234
isdeal	是否已清除（消除对系统的影响，如隔离、删除等）	1

C.7 恶意代码类——跨站脚本XSS

- 填写建议

— 事件主要来源：恶意代码检测系统、入侵检测系统、SOC 等管理系统；

— 收集主要事件类型：跨站脚本 XSS 事件、恶意代码事件。

- 事件填写实例

详见表 C.7。

表 C.7 跨站脚本 XSS 事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.201.57.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-6A-50-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	406
name	事件名称	跨站脚本 XSS 攻击
protocol_id	协议类型	11
feature	脚本特征串	7fgd544ge55yfyh6e5y4
range	匹配范围	12
dstip	包含跨站脚本的网站 IP 地址	10.147.142.47
dstport	目的端口号	21
warn_sys_ip	设备地址	10.147.142.21
rank	原始危害等级	3
merge_count	归并数量	142
time_start	事件归并的开始时间	2007-12-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T09:46:31
event_content	描述	10.147.142.47:检测到跨站脚本 XSS 攻击

C.8 攻击入侵类——拒绝服务类

- 填写建议

— 事件主要来源：入侵检查系统、异常流量关系系统、DOS/DDOS 清洗设备、防火墙、SOC 等管理系统；

— 收集主要事件类型：异常流量事件、入侵检查发现的 DOS/DDOS 攻击、DOS/DDOS 清洗设备拦截的攻击。

- 事件填写实例

详见表 C.8、表 C.9 和表 C.10。

表 C.8 拒绝服务攻击类事件填写实例（IPS 告警）

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.121.77.10
senddev_mac	发送安全事件的设备的 MAC 地址	34-50-96-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101002
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	501
event_detail_type_id	事件详细类型 ID	501005
name	事件名称	Botnet C&Cs
protocol_id	协议类型	5
dstip	被攻击对象 IP 地址	10.147.142.103
dstport	被攻击对象端口号	80
invol	发送流量	41552
outvol	接收流量	14573
inunit	发送流量单位	0
outunit	接收流量单位	0
inpktnum	进入数据包数	23435453
outpktnum	离开数据包数	3343543453
warn_sys_ip	设备地址	10.201.62.24
rank	原始危害等级	3
merge_count	归并数量	0
time_start	事件归并的开始时间	2007-12-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T09:46:31
event_content	描述	%IPS-ALERT-1:SENSORNAME:sensor1;SENSORIP:10.147.142.21;EVENTNAME:AIM 文件传输路径使用超长的字符串;COUNT:1;SIP:211.138.184.201; SPORT:33935; DIP:10.147.142.103;DPORT:80;TYPE:攻击;SEVERITY:高风险;PREVENTFLAG:阻断;PREVENTTYPE:动态防护 ;RELIABILITY:90;PROTOCOL:TCP;DESC:211.138.184.201 33935 -> 10.147.142.103 80 -- AIM 低于 4.1 版本的客户端在传输文件时，如果文件路径包含超长的字符串会导致系统拒绝服务

表 C.9 拒绝服务攻击类事件填写实例（异常流量清洗设备告警）

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.121.77.10
senddev_mac	发送安全事件的设备的 MAC 地址	00-60-96-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101002
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	501
event_detail_type_id	事件详细类型 ID	501003
name	事件名称	net.ipv4.sfw
protocol_id	协议类型	4
dstip	被攻击对象 IP 地址	58.210.242.20
dstport	被攻击对象端口号	29519
invol	发送流量	12288
outvol	接收流量	512000
inunit	发送流量单位	0
outunit	接收流量单位	0
inpktnum	进入数据包数	23435453
outpktnum	离开数据包数	3343543453
warn_sys_ip	设备地址	10.201.62.24
rank	原始危害等级	3
merge_count	归并数量	0
time_start	事件归并的开始时间	2007-12-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T09:46:31
event_content	描述	Attack: net.ipv4.sfw_attack_info = Connection-Flood src=202.92.162.67 dst=58.210.242.20 sport=63433 dport=29519 flag=minor:102

表 C.10 拒绝服务攻击类事件填写实例（异常流量管理系统）

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.221.37.16
senddev_mac	发送安全事件的设备的 MAC 地址	00-60-96-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101002
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	501
event_detail_type_id	事件详细类型 ID	501001
name	事件名称	anomaly TCP_SYN_Misuse
protocol_id	协议类型	5
dstip	被攻击对象 IP 地址	222.217.221.134
dstport	被攻击对象端口号	29519
invol	发送流量	0
outvol	接收流量	50000 pps
inunit	发送流量单位	0
outunit	接收流量单位	0
inpktnum	进入数据包数	5000
outpktnum	离开数据包数	0
warn_sys_ip	设备地址	219.150.59.250
rank	原始危害等级	3
merge_count	归并数量	0
time_start	事件归并的开始时间	2007-04-30T22:12:27
time_end	事件归并的结束时间	2007-04-30T22:12:27
event_content	描述	Apr 30 22:12:27 219.150.59.250 Apr 30 14:12:26 pfsp: anomaly TCP_SYN_Misuse id 38850 status done severity 3 classification medium src 0.0.0.0/0 All dst 222.217.221.134/32 Province-guangxi start 2007-04-30 13:34:52 +0000 duration 1986 percent 73.060000 rate 50000 rateUnit pps protocol tcp flags S url https://NorthTelecom-ARBOR1/alerts/anomaly/index?attack_id=38850

C.9 攻击入侵类——漏洞攻击

- 填写建议

— 事件主要来源：入侵检测系统系统、SOC 等管理系统；

— 收集主要事件类型：漏洞攻击事件。

- 事件填写实例

详见表 C.11。

表 C.11 漏洞攻击事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.31.37.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-6A-50-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101002
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	502
name	漏洞攻击名称	可疑的 MSRPC 请求
vuln-id	漏洞 CVE 编号	CVE-2009-055
protocol_id	协议类型	5
feature	漏洞攻击特征串	04ff4nge55ysfrs7gd54
range	匹配范围	12
dstip	被攻击设备 IP 地址	10.147.142.103
dstport	被攻击设备端口号	79
outvol	接收流量	50000
outunit	接收流量单位	0
inpktnum	进入数据包数	5000
warn_sys_ip	设备地址	10.147.142.21
rank	原始危害等级	3
merge_count	归并数量	1200
time_start	事件归并的开始时间	2007-12-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T09:46:31
event_content	漏洞描述	116.226.74.62:1830 -> 10.147.142.103:80, 检测到可疑的 MSRPC 请求企图利用 Microsoft NetDDE 的漏洞

C.10 恶意代码类——蠕虫攻击

- 填写建议

— 事件主要来源：防病毒软件的集中管理系统、入侵检测系统、防火墙系统、异常流量管理系统、SOC 等管理系统；

— 收集主要事件类型：单个或者归并的蠕虫攻击事件。

- 事件填写实例

详见表 C.12。

表 C.12 蠕虫攻击事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	9211454
senddev_ip	发送安全事件的设备地址	10.201.57.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-50-56-C0-00-FF
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101004
warn_sys_netcode	网络编号	100180
event_type_id	基本安全事件类型 ID	503
name	蠕虫名称	熊猫烧香
protocol_id	协议类型	5
feature	蠕虫攻击特征串	Jh4hbd223tgsfrs7g75sd54
range	匹配范围	12
srcip	源 IP 地址	10.5.14.7
dstip	被攻击设备 IP 地址	10.0.15. 92
srcport	源端口号	410
dstport	被攻击设备端口号	134
invol	发送流量	5252
outvol	接收流量	9373
inunit	发送流量单位	0
outunit	接收流量单位	0
inpktnum	进入数据包数	237883453
outpktnum	离开数据包数	352343453
warn_sys_ip	设备地址	10.201.62.24
rank	原始危害等级	3
merge_count	归并数量	0
time_start	事件归并的开始时间	2007-09-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T23:11:00
event_content	蠕虫攻击描述	被攻击设备 IP 地址为 10.0.15. 92，被攻击的端口为 134.

C.11 攻击入侵类——后门攻击

- 填写建议

— 事件主要来源：入侵检测系统系统、SOC 等管理系统；

— 收集主要事件类型：后门攻击事件。

- 事件填写实例

详见表 C.13。

表 C.13 后门攻击事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.31.37.188
senddev_mac	发送安全事件的设备的 MAC 地址	6C-6A-96-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101002
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	504
name	事件名称	检测到作为 Finger 请求发送的后门命令字符串
protocol_id	协议类型	5
feature	特征串	04ff4nge55ysfrs7gd54
range	匹配范围	12
srcip	攻击源 IP 地址	61.191.75.204
dstip	攻击目标 IP 地址	10.147.142.93
srcport	攻击源端口号	1364
dstport	攻击目标端口号	79
warn_sys_ip	设备地址	10.147.142.21
rank	原始危害等级	3
merge_count	归并数量	1200
time_start	事件归并的开始时间	2007-12-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T09:46:31
event_content	后门攻击事件描述	false:"61.191.75.204 -> 10.147.142.93:为 Finger 请求发送的后门命令字符串，一些后门程序绑定到 Finger 端口并接受来自攻击者的远程命令。如果出现这可能表示后门已经安装或者攻击者正在探测活动的后门

C.12 攻击入侵类——猜测口令

- 填写建议

— 事件主要来源：入侵检测系统系统、SOC 等管理系统；

— 收集主要事件类型：猜测口令攻击事件。

- 事件填写实例

详见表 C.14。

表 C.14 猜测口令事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.201.57.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-50-56-C0-00-FF
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010201001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	505
name	事件名称	PASS 命令的密码参数为空
protocol_id	协议类型	11
srcip	猜测者 IP 地址	61.191.75.35
dstip	被猜测者 IP 地址	10.147.142.47
srcport	猜测者端口号	1387
dstport	被猜测者端口号	21
warn_sys_ip	设备地址	10.147.142.21
rank	原始危害等级	3
merge_count	归并数量	50
time_start	事件归并的开始时间	2007-12-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T09:46:31
event_content	恶意猜测口令描述	false:"61.191.75.35 -> 10.147.142.47: 检测到客户端发送的 PASS 命令的密码参数为空，可能是在做口令猜测

C.13 攻击入侵类——非法访问

- 填写建议

— 事件主要来源：入侵检测系统系统、主机或者网络设备登录日志、SOC 等管理系统；

— 收集主要事件类型：非法访问攻击事件，单台设备在规定时间内超过特定次数（如 2h 内 100 次）的登录失败。

- 事件填写实例

详见表 C.15。

表 C.15 非法访问事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.201.57.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-6A-50-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	506
name	事件名称	客户端命令企图非法访问系统根目录
protocol_id	协议类型	11
srcip	非法访问源 IP 地址	61.191.75.35
dstip	非法访问目的 IP 地址	10.147.142.47
srcport	非法访问源端口号	1323
dstport	非法访问目的端口号	21
warn_sys_ip	设备地址	10.147.142.21
rank	原始危害等级	3
merge_count	归并数量	142
time_start	事件归并的开始时间	2007-12-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T09:46:31
event_content	非法访问事件描述	false:"61.191.75.35 -> 10.147.142.47:检测到客户端命令企图非法访问系统根目录上的某点.

C.14 攻击入侵类——域名劫持

- 填写建议

— 事件主要来源：入侵检测系统系统、主机或者网络设备日志、SOC 等管理系统；

— 收集主要事件类型：域名劫持事件、非法访问攻击事件。

- 事件填写实例

详见表 C.16。

表 C.16 域名劫持事件填写实例

字段名	中文名称	取值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.201.57.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-6A-50-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	507
name	事件名称	域名劫持事件
url	被劫持的域名	www.abc123.com.
protocol_id	协议类型	11
srcip	劫持目标的原 IP 地址	61.191.75.35
dstip	劫持后的 IP 地址	10.147.142.47
srcport	传播端口号	1323
dstport	目的端口号	21
warn_sys_ip	设备地址	10.147.142.21
rank	原始危害等级	3
merge_count	归并数量	142
time_start	事件归并的开始时间	2007-12-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T09:46:31
event_content	域名劫持事件描述	域名 www.abc123.com.被劫持。劫持后的 IP 地址为 10.147.142.47

C.15 信息危害类——网页篡改

- 填写建议

— 事件主要来源：入侵检测系统系统、主机或者网络设备日志、SOC 等管理系统；

— 收集主要事件类型：网页篡改事件、非法访问攻击事件。

- 事件填写实例

详见表 C.17。

表 C.17 网页篡改事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.201.57.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-6A-50-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	601
name	事件名称	网页篡改事件
protocol_id	协议类型	11
url	被篡改网页的 URL	http://www.xxx.com/ad.html
dstip	被篡改网页的 IP 地址	10.147.142.47
dstport	目的端口号	21
warn_sys_ip	设备地址	10.147.142.21
rank	原始危害等级	3
merge_count	归并数量	142
time_start	事件归并的开始时间	2007-12-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T09:46:31
event_content	网页篡改事件描述	IP 为 10.147.142.47 的网页被恶意篡改

C.16 信息危害类——网络仿冒

- 填写建议

— 事件主要来源：入侵检测系统系统、主机或者网络设备日志、SOC 等管理系统；

— 收集主要事件类型：网页仿冒事件、非法访问攻击事件。

- 事件填写实例

详见表 C.18。

表 C.18 网络仿冒事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.201.57.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-6A-50-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010101001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	602
name	事件名称	网站仿冒
protocol_id	协议类型	11
url	被仿冒后的网站 URL	www.sino.com
srcip	被仿冒的网站 IP 地址	61.191.75.35
dstip	运行仿冒网站主机的 IP 地址	10.147.142.47
srcport	源端口号	1323
dstport	目的端口号	21
warn_sys_ip	设备地址	10.147.142.21
rank	原始危害等级	3
merge_count	归并数量	142
time_start	事件归并的开始时间	2007-12-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T09:46:31
event_content	网络仿冒事件描述	www.sina.com 受到网络仿冒。仿冒网站的 IP 地址为 10.147.142.47。原地址为 61.191.75.35

C.17 信息危害类——垃圾邮件

- 填写建议

— 事件主要来源：垃圾邮件投诉处理系统、入侵检测系统系统、SOC 等管理系统；

— 收集主要事件类型：垃圾邮件投诉事件、垃圾邮件攻击事件。

注：垃圾邮件投诉事件一律命名为“垃圾邮件投诉”，并在源地址中填写被投诉的地址。

- 事件填写实例

详见表 C.19、表 C.20。

表 C.19 垃圾邮件事件填写实例（垃圾邮件投诉事件）

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.201.57.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-50-56-C0-00-FF
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	180001
warn_sys_name	产生告警信息的系统名称	SOC_010201001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	603
name	事件名称	垃圾邮件投诉
protocol_id	协议类型	11
feature	垃圾邮件特征串	5hgj7d544ge6ejn7
range	匹配范围	12
srcip	垃圾邮件发送源 IP 地址	125.40.170.3
warn_sys_ip	设备地址	10.201.62.24
rank	原始危害等级	3
merge_count	归并数量	120
time_start	事件归并的开始时间	2007-5-22T12:27:50
time_end	事件归并的结束时间	2007-5-22T12:27:50
event_content	垃圾邮件描述	投诉方:SpamCop 投诉 IP:125.40.170.3 所属公司:河南 投诉 ID:2295009270 投诉类型:垃圾邮件 回复地址:xusun@cnc-noc.net 影响程度:中 工单状态:已发送 回复状态:待处理 创建时间:2007-5-22 12:27:50 发件人:2295009270 发件地址:2295009270@reports.spamcop.net 发布时间:Sun,20 May 2007 05:15:19 +0200 主题:[SpamCop(125.40.170.3) id:2295009270] Paypal Notice

表 C.20　垃圾邮件事件填写实例（IPS 报告的垃圾邮件事件）

字段名	中文名称	赋　值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.36.94.245
senddev_mac	发送安全事件的设备的 MAC 地址	00-A3-50-56 -00-FF
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	100001
warn_sys_name	产生告警信息的系统名称	SOC_010201001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	507
name	事件名称	尝试发送垃圾邮件
protocol_id	协议类型	25
feature	垃圾邮件特征串	5hy67d544ge6u56
range	匹配范围	6
srcip	垃圾邮件发送源 IP 地址	221.18.132.67
warn_sys_ip	设备地址	10.147.142.21
rank	原始危害等级	2
merge_count	归并数量	120
time_start	事件归并的开始时间	2007-5-22T12:27:50
time_end	事件归并的结束时间	2007-5-22T12:27:50
event_content	垃圾邮件描述	false:" 221.18.132.67 -> 10.147.142.143:检测到一条指向本地网络服务器的 SMTP RCPT 命令,所指向的域没有位于可接受的中继主机的配置列表中,这表明有人在企图利用该服务器发送垃圾邮件,以掩盖其源地址

C.18 信息危害类——信息泄露与窃取

- 填写建议

— 事件主要来源：入侵检测系统系统、SOC 等管理系统；

— 收集主要事件类型：信息泄露与窃取事件。

- 事件填写实例

详见表 C.21。

表 C.21 信息泄漏与窃取事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.201.57.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-50-56-C0-00-FF
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	060001
warn_sys_name	产生告警信息的系统名称	SOC_010201001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	604
name	事件名称	信息泄露与窃取
dstip	发生信息泄露或窃取设备的 IP 地址	125.40.170.3
dstport	发生信息泄露或窃取的端口号	21
warn_sys_ip	设备地址	10.201.62.24
rank	原始危害等级	3
merge_count	归并数量	120
time_start	事件归并的开始时间	2007-5-22T12:27:50
time_end	事件归并的结束时间	2007-5-22T12:27:50
event_content	事件描述	信息泄露与窃取，IP 地址 125.40.170.3

C.19 设备设施故障类——设备设施故障

- 填写建议

— 事件主要来源：主机或者网络设备日志、SOC 等管理系统；

— 收集主要事件类型：设备设施故障事件。

- 事件填写实例

详见表 C.22。

表 C.22 设备设施故障事件填写实例

字段名	中文名称	赋 值
event _id	发送时安全事件的唯一标识	
senddev_ip	发送安全事件的设备地址	10.201.57.188
senddev_mac	发送安全事件的设备的 MAC 地址	00-6A-50-CD-00-7F
send_dev_type_id	发送安全事件的系统类型名称	13
warn_sys_locate	产生告警信息的系统位置	3701003
warn_sys_id	产生事件告警信息的系统 ID	130001
warn_sys_name	产生告警信息的系统名称	SOC_010101001
warn_sys_netcode	网络编号	100190
event_type_id	基本安全事件类型 ID	506
name	故障名称	设备设施故障
protocol_id	故障类型	11
dstip	故障源 IP 地址	10.147.142.47
dstport	故障设备端口号	21
warn_sys_ip	设备地址	10.147.142.21
fail_time	故障发生时间	2007-12-04T09:46:31
rank	原始危害等级	3
merge_count	归并数量	142
time_start	事件归并的开始时间	2007-12-04T09:46:31
time_end	事件归并的结束时间	2007-12-04T09:46:31
event_content	设备故障事件描述	路由器设备故障，其 IP 地址为 10.147.142.47

参 考 文 献

[1] GB/Z 20986-2007　信息安全技术 信息安全事件分类分级指南
[2] GB/T 22240-2008　信息安全技术 信息系统安全等级保护定级指南
[3] YD/T 1827-2008　网络安全事件描述和交换格式
[4] YD/T 1729-2008　电信网和互联网安全等级保护实施指南

中华人民共和国

通信行业标准

国家网络安全应急处理平台安全信息获取接口要求

YD/T 2251-2011

*

人民邮电出版社出版发行

北京市崇文区夕照寺街14号A座

邮政编码：100061

宝隆元（北京）印刷技术有限公司印刷

*

开本：880×1230 1/16　　2011年9月第1版

印张：3.5　　2011年9月北京第1次印刷

字数：89千字

ISBN 978-7-115-2395/11-346

定价：35元