ICS 33.040
M 21

YD

中华人民共和国通信行业标准

YD/T 2707-2014

互联网主机网络安全属性描述格式

Host network security attribute description format

2014-10-14 发布　　2014-10-14 实施

中华人民共和国工业和信息化部　发布

目　录

前　言

本标准由中国通信标准化协会提出并归口。

本标准起草单位：国家计算机网络应急技术处理协调中心、北京神州绿盟科技有限公司、华为技术有限公司。

本标准主要起草人：徐　原、姚　力、朱芸茜、周勇林、何清林、强　倩、王明华、纪玉春、王营康、李　佳、何世平、郑礼雄。

引　言

近年来，网络恶意程序肆虐传播，地下黑色产业链发展迅速。国家互联网应急中心（CNCERT）监测发现黑客利用网页挂马、攻击入侵等手段攻击了大量的互联网主机，并植入木马、僵尸网络等恶意程序对其进行控制，导致大量用户个人隐私信息、个人财产、国家机密数据被窃取。黑客还利用这些被控主机发动大规模拒绝服务攻击。这些行为对互联网网络安全甚至社会安全造成了严重危害。

全面掌握互联网主机的网络安全属性对遏制恶意程序传播有重要意义。通过统一规范互联网主机的命名规则、描述规范，便于在网络安全组织、安全企业、研究机构、互联网企业之间进行信息交换和共享。对于含有恶意倾向的互联网主机信息，可以利用国家互联网应急中心的黑名单发布系统、安全企业的安全防护产品、以及媒体的传播等渠道，向广大互联网用户及时推送恶意服务器信息，防止用户访问这些恶意主机或站点，减少遭受入侵攻击的几率。同时，通过互联网主机存在漏洞的信息情况共享，能增加国家对互联网网络安全现状的了解，对可能发生的大规模网络攻击入侵事件能进行预警、及时防范。

互联网主机网络安全属性描述格式

1 范围

本标准规定了互联网主机的网络安全属性基本信息，主要包括互联网主机基本信息和所包含漏洞情况、有恶意行为的主机相关信息，如发现时间、使用的域名和IP地址、地理位置、运营商、控制主机数量、控制主机列表、控制方式等具体内容的描述格式定义。

本标准适用于网络安全组织、安全企业、研究机构等进行互联网主机网络安全属性信息的共享、交换工作，以及有恶意行为主机列表的对外发布预警。

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，仅所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。

GBZ 20986-2007 信息安全技术 信息安全事件分类分级指南

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

信息系统 Information System

由计算机硬件、软件、网络和通信设备等组成的以处理信息和数据为目的的系统。

3.1.2

漏洞 Vulnerability

信息系统中的软件、硬件或协议中存在缺陷或不适当的配置，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。

3.1.3

恶意程序 Malicious Program

在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。

3.1.4

拒绝服务攻击 Denial of Service

向某一目标信息系统发送密集的攻击包，或执行特定攻击操作，以期致使目标系统停止提供服务。

3.1.5

网页篡改 Webpage Defacement

恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容。

3.1.6

网页仿冒 Phishing

通过构造与某一目标网站高度相似的页面（俗称钓鱼网站），并通常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式发送声称来自于被仿冒机构的欺骗性消息，诱骗用户访问钓鱼网站，以获取用户个人信息（如银行账号和账户密码）。

3.1.7

网页挂马　Web-based Malware Website

通过在网页中嵌入恶意程序或链接，致使用户计算机在访问该页面时可能被植入恶意程序。

3.1.8

垃圾邮件　Spam

将不需要的消息（通常是未经请求的广告）发送给众多收件人。包括：（1）收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；（2）收件人无法拒收的电子邮件；（3）隐藏发件人身份、地址、标题等信息的电子邮件；（4）含有虚假的信息源、发件人、路由等信息的电子邮件。

3.1.9

非授权访问　Unauthorized Access

没有访问权限的用户以非正当的手段访问数据信息。非授权访问事件一般发生在存在漏洞的信息系统中，黑客利用专门的漏洞利用程序（Exploit）来获取信息系统访问权限。

3.2　缩略语

下列缩略语适用于本文件。

ASN	Autonomous System Number	自治系统号
CNVD	China National Vulnerability Database	国家信息安全漏洞共享平台
CVE	Common Vulnerabilities and Exposures	通用漏洞披露
HNSADF	Host Network Security Attribute Description Format	互联网主机安全属性描述格式
IP	Internet Protocol	互联网协议
ISP	Internet Service Provider	互联网服务提供商
MD5	Message-Digest Algorithm 5	信息摘要算法第5版
URL	Uniform / Universal Resource Locator	统一资源定位符（网页地址）
XML	Extensible Markup Language	可扩展的标记语言

4　网络安全属性描述格式

4.1　主机的描述方法

对于每个本标准所定义的类(Class)，首先给出其语义，并用类图来表现和其他类之间的关系，然后用XML的文档结构定义模式（Schema）给出该类的具体描述格式。

对于每个类的描述包括五个部分：

——类说明：简要描述类的具体含义

——类图：以图形的方式说明类的构成

——子类：描述该类所包含的子类，是否是必须的，存在实例个数及其简要说明

——属性：用于说明该类所具有的属性名，及其含义

——Schema定义：给出该类XML Schema实现片段

4.2 版本（HNSADF-Document）

类说明

HNSADF-Document类在HNSADF数据模型是顶层类，所有HNSADF文档都是HNSADF-Document类的实例，在此显示了版本号。

类图（如图1所示）

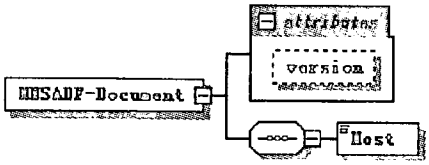


图1 版本类图

子类

Host：包括一个或多个实例。包含所有与互联网主机安全属性信息相关的互联网主机类。

属性

version：必选。字符串。指出HNSADF文档所遵循的描述格式的版本号。本标准以下定义的格式是第一个版本，版本号为01。

Schema定义

```
<xsd:element name="HNSADF-Document">
        <xsd:complexType mixed="true">
            <xsd:sequence>
                <xsd:element ref="Host"/>
            </xsd:sequence>
            <xsd:attribute name="version" type="xsd:string" fixed="04"/>
        </xsd:complexType>
</xsd:element>
```

4.3 互联网主机（Host）

类说明

每一个报告或处理的互联网主机，由Host类的一个实例来描述。Host类为通常交换的互联网主机数据提供一个标准的表示法，并且把所描述的活动和一个惟一的标识符联系起来。

Host类概述互联网主机安全属性信息，也对构成Host类的安全属性进行分类。

类图（如图2所示）

子类

BasicInfo：存在一个实例。主机的基本信息；

SecurityAttribute：存在一个或多个实例。主机的网络安全属性信息；

AdditionalData：存在零个或多个实例。使用不能在其他地方描述的信息来扩展数据模型的区域；

Contact：存在一个或多个实例。与主机有关的参与方的联系信息；

Assessment：最多存在一个实例。评估互联网主机活动影响的描述。

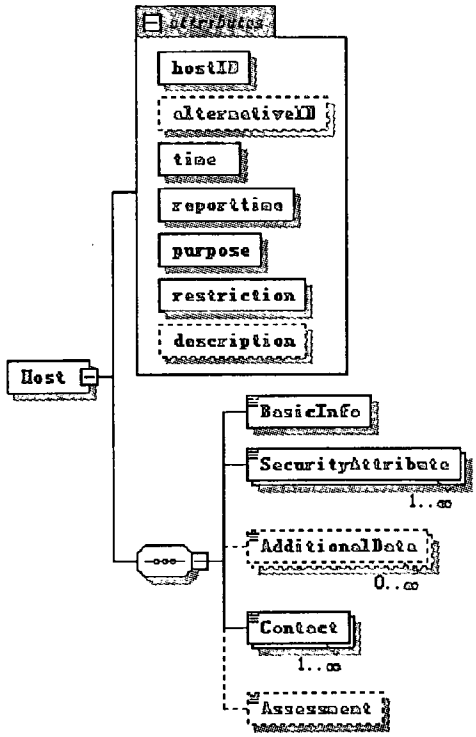


图2　互联网主机类图

属性

HostID：必选。文档的产生方指派给该主机的跟踪号，或者是惟一标识符；

AlternativeID：可选。由其他单位用来引用文档中所描述的同一活动的一列主机跟踪号；

Time：必选。发生时间；

Rreporttime：必选。报告时间；

Purpose：必选。枚举类型；指出HNSADF文档的目的。本属性被定义为一个枚举列表：

——handling：发送本HNSADF-文档的目的是期望接收者处理互联网主机；

——statistics：发送本HNSADF-文档，只用于统计目的；

——warning：发送本HNSADF-文档，只是作为一个警告；

——other：发送HNSADF-文档目的将在AdditionalData元素中指明。

restriction：必选。枚举类型；指出HNSADF-文档的发送者期望接收者应该遵守的保密原则，由文档的接收者自由决定是否遵守这个原则。逻辑上，子类可以继承父类的这个属性值。由于多数高层类都有restriction属性，这就有可能设置细粒度的保密策略。如果子类加紧或者放松保密规则，子类可以不考虑父类的保密规则。对一个没有指定restriction属性值的类，可以在其指定了restriction属性值的最邻近的祖先类中得出该类的restriction属性值。restriction属性被定义为一个枚举类型值，缺省值为“private”：

——public：对信息没有任何级别的限制；

——need-to-know：信息可以被和互联网主机有关的其他方共享（举例来说，多个受害站点能够相互通告）；

——private：信息不能被共享；

——default：按照通信各方预先安排的信息保密规则，决定是否可共享信息。

description：可选。字符串类型。互联网主机的自由形式的文本描述。

Schema定义

```
<xsd:element name="Host">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="BasicInfo"/>
            <xsd:element name="SecurityAttribute" maxOccurs="unbounded"/>
            <xsd:element name="AdditionalData" minOccurs="0" maxOccurs="unbounded"/>
            <xsd:element name="Contact" maxOccurs="unbounded"/>
            <xsd:element name="Assessment" minOccurs="0"/>
        </xsd:sequence>
            <xsd:attribute name="hostID" use="required"/>
            <xsd:attribute name="alternativeID"/>
            <xsd:attribute name="time" use="required"/>
            <xsd:attribute name="reporttime" type="NTPTIMESTAMP" use="required"/>
            <xsd:attribute name="purpose" type="xs:string" use="required"/>
            <xsd:attribute name="restriction" type="xs:string" use="required"/>
            <xsd:attribute name="description"/>
    </xsd:complexType>
</xsd:element>
```

4.3.1 基本信息（BasicInfo）

类说明

描述该主机的基本信息。

类图（如图3所示）

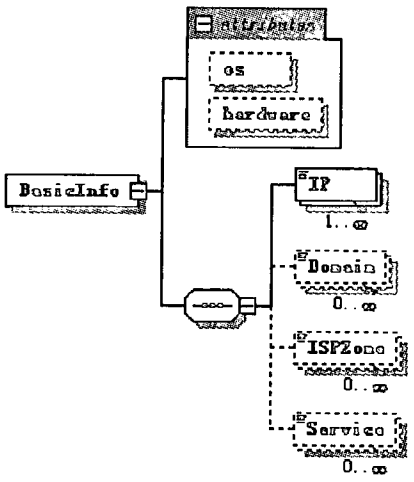


图 3 基本信息类图

子类

IP：存在一个或多个实例。描述该主机的所有IP地址；

Domain：存在零个或多个实例。描述该主机的所有域名信息；

ISPZone：存在零个或多个实例。描述该主机所处的运营商区域信息；

Service：存在零个或多个实例。描述该主机提供的服务信息。

属性

Os：可选。描述该主机使用的操作系统信息。

Hardware：可选。描述该主机的硬件信息。

Schema定义

```
<xsd:element name="BasicInfo">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="IP" maxOccurs="unbounded"/>
            <xsd:element name="Domain" minOccurs="0" maxOccurs="unbounded"/>
            <xsd:element name="ISPZone" minOccurs="0" maxOccurs="unbounded"/>
            <xsd:element name="Service" minOccurs="0" maxOccurs="unbounded"/>
        </xsd:sequence>
        <xsd:attribute name="os"/>
        <xsd:attribute name="hardware"/>
    </xsd:complexType>
</xsd:element>
```

4.3.1.1 地址(IP)

类说明

描述主机的网络地址信息。

类图（如图4所示）

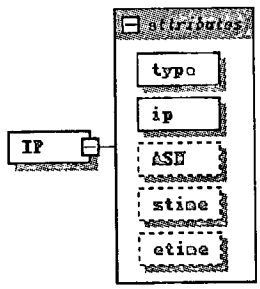


图 4 IP 地址类图

子类

无。

属性

Type：必选。表明是IPv4还是IPv6的地址；

Ip：必选。IP值；

ASN：可选。IP地址所在自治系统的惟一标识号；

Stime：可选。该IP在此主机上使用的开始时间；

Eime：可选。该IP在此主机上使用的结束时间。

Schema定义

```
<xsd:element name="IP">
        <xsd:complexType>
            <xsd:attribute name="type" use="required"/>
            <xsd:attribute name="ip" use="required"/>
            <xsd:attribute name="ASN"/>
            <xsd:attribute name="stime"/>
            <xsd:attribute name="etime"/>
        </xsd:complexType>
    </xsd:element>
```

4.3.1.2 域名（Domain）

类说明

描述主机的域名信息。

类图（如图5所示）

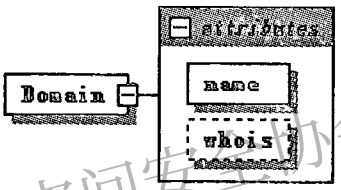


图5 域名类图

子类

无。

属性

Name：必选。域名名称；

Whois：可选。域名的whois信息。

Schema定义

```
<xsd:element name="Domain">
    <xsd:complexType>
        <xsd:attribute name="name" use="required"/>
        <xsd:attribute name="whois"/>
    </xsd:complexType>
</xsd:element>
```

4.3.1.3 ISP 区域信息（ISPZone）

类说明

描述主机所处的ISP运营商名称及所在区域信息。

类图（如图6所示）

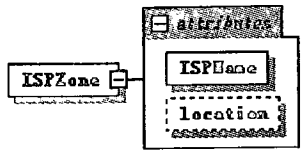


图6 ISP区域信息类图

子类

无。

属性

ISPName：必选。运营商名称；

Location：可选。运营商所在地。

Schema定义

```
<xsd:element name="ISPZone">
    <xsd:complexType>
        <xsd:attribute name="ISPName" use="required"/>
        <xsd:attribute name="location"/>
    </xsd:complexType>
</xsd:element>
```

4.3.1.4 服务（Service）

类说明

Service类描述主机或网络所提供的服务。例如WWW服务、FTP服务、E-mail服务等。服务通过端口或端口列表，以及监听这些端口的服务程序来确定。

类图（如图7所示）

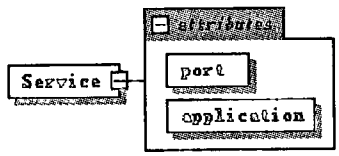


图7 服务类图

子类

无。

属性

Port：必选。描述网络服务程序所使用的端口或端口表；

Application：必选。描述端口或端口表上绑定的应用程序。

Schema定义

```
<xsd:element name="Service">
    <xsd:complexType>
        <xsd:attribute name="port" use="required"/>
        <xsd:attribute name="application"use="required"/>
    </xsd:complexType>
```

</xsd:element>

4.3.2 网络安全属性（SecurityAttribute）

类说明

实际描述主机的安全属性。本属性的子类划分参考了GBZ 20986-2007。

类图（如图8所示）

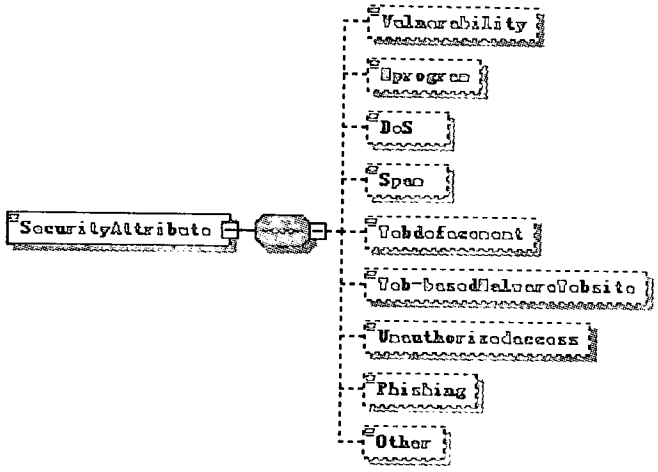


图8 网络安全属性类图

子类

Vulnerability：最多存在一个实例。描述主机存在的漏洞；

Mprogram：最多存在一个实例。描述主机是否感染、传播恶意程序；

DoS：最多存在一个实例。描述主机是否在进行DoS攻击或正遭受DoS攻击；

Spam：最多存在一个实例。描述主机是否传播垃圾邮件；

Webdefacement：最多存在一个实例。描述主机是否存在被篡改文件；

Web-basedMalwareWebsite：最多存在一个实例。描述主机是否存在挂马现象；

Unauthorizedaccess：最多存在一个实例。描述主机是否存在非授权访问；

Phishing：最多存在一个实例。描述主机是否在进行网页仿冒、钓鱼欺骗；

Other：最多存在一个实例。描述其他影响主机安全的问题。

属性

无。

Schema定义

```
<xsd:element name="SecurityAttribute">
        <xsd:complexType mixed="true">
            <xsd:sequence>
                <xsd:element ref="Vulnerability" minOccurs="0"/>
                <xsd:element ref="Mprogram" minOccurs="0"/>
                <xsd:element ref="DoS" minOccurs="0"/>
                <xsd:element ref="Spam" minOccurs="0"/>
                <xsd:element ref="Webdefacement" minOccurs="0"/>
```

```
                    <xsd:element ref="Web-basedMalwareWebsite" minOccurs="0"/>
                    <xsd:element ref="Unauthorizedaccess" minOccurs="0"/>
                    <xsd:element ref="Phishing" minOccurs="0"/>
                    <xsd:element ref="Other" minOccurs="0"/>
                </xsd:sequence>
            </xsd:complexType>
        </xsd:element>
```

4.3.2.1 漏洞（Vulnerability）

类说明

是安全属性的子类，描述漏洞相关的属性。

类图（如图9所示）

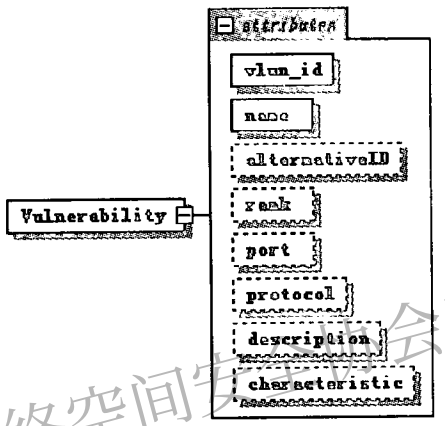


图9 漏洞类图

子类

无。

属性

Vlun_id：必选。用于标识漏洞的惟一编号：国家信息安全漏洞共享平台（CNVD）漏洞编号。

Name：必选。漏洞名称。

AtlernativeID：可选。各厂商用于给出自己对于该漏洞的惟一标识，方便进行统计、追踪。

Rank：可选。漏洞的危害级别。枚举类型，可分为高危、中危和低危。

Port：可选。该漏洞涉及的相关端口。

Protocol：可选。该漏洞涉及的相关协议。

Descritption：可选。漏洞内容的描述。

Characteristic：可选。漏洞的特征码。用于检测该漏洞。

Schema定义

```
<xsd:element name="Vulnerability">
        <xsd:complexType>
            <xsd:attribute name="vlun_id" use="required"/>
            <xsd:attribute name="name" use="required"/>
```

```
            <xsd:attribute name="alternativeID"/>
            <xsd:attribute name="rank"/>
            <xsd:attribute name="port"/>
            <xsd:attribute name="protocol"/>
            <xsd:attribute name="description"/>
            <xsd:attribute name="characteristic"/>
        </xsd:complexType>
    </xsd:element>
```

4.3.2.2 恶意程序（Mprogram）

类说明

安全属性的子类。描述主机与恶意程序相关的属性。

类图（如图10所示）

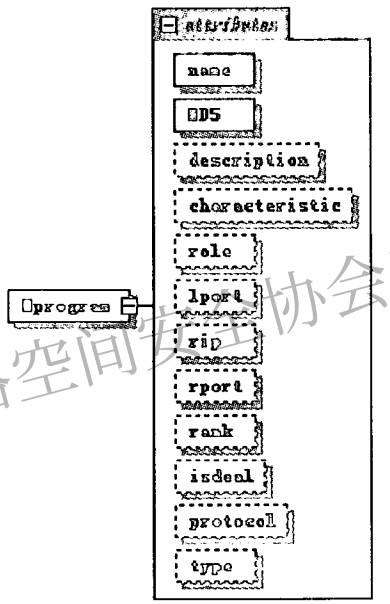


图10 恶意程序类图

子类

无。

属性

Name：必选。恶意程序名称；

MD5：必选。字符串类型。文件md5散列值；

Description：可选。字符串类型。恶意程序的详细描述；

Characteristic：可选。该恶意程序的检测特征；

Role：可选。角色。枚举类型；

——Infect：感染

——Infected：被感染

Lport：可选。本机端口；

Rip：可选。对端IP；

Rport：可选。对端端口；

Isdeal：可选。是否已经被处置；

Protocol：可选。恶意程序相关的协议；

Type：可选。恶意程序类型。木马、僵尸网络、蠕虫、病毒、其他。

Schema定义

```
<xsd:element name="Mprogram">
        <xsd:complexType>
            <xsd:attribute name="name" use="required"/>
            <xsd:attribute name="MD5" use="required"/>
            <xsd:attribute name="description"/>
            <xsd:attribute name="characteristic"/>
            <xsd:attribute name="role"/>
            <xsd:attribute name="lport"/>
            <xsd:attribute name="rip"/>
            <xsd:attribute name="rport"/>
            <xsd:attribute name="rank"/>
            <xsd:attribute name="isdeal"/>
            <xsd:attribute name="protocol"/>
            <xsd:attribute name="type"/>
        </xsd:complexType>
    </xsd:element>
```

4.3.2.3 拒绝服务攻击（DoS）

类说明

描述主机与拒绝服务攻击相关的属性。

类图（如图11所示）

子类

无。

属性

Name：必选。攻击事件名称；

Description：可选。攻击行为描述；

Role：必选。枚举类型。角色：

attack：攻击

attacked：被攻击

Type：可选。DoS攻击的类型；

Rip：可选。对端IP列表；

Rport：可选。对端端口；

Lport：可选。本机端口；

Outvol：可选。发送流量峰值；

Invol：可选。接收流量峰值；

Domain：可选。域名；

Stime：可选。开始时间；

Etime：可选。结束时间。

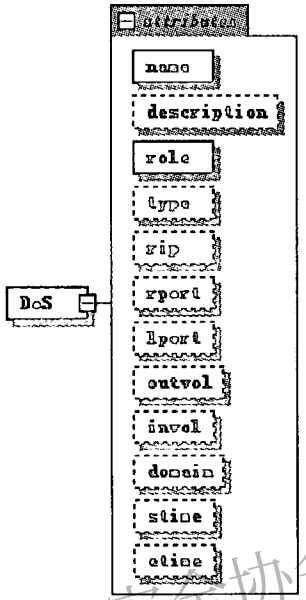


图11 拒绝服务攻击类图

Schema定义

```
<xsd:element name="DoS">
        <xsd:complexType>
            <xsd:attribute name="name" use="required"/>
            <xsd:attribute name="description"/>
            <xsd:attribute name="role" use="required"/>
            <xsd:attribute name="type"/>
            <xsd:attribute name="rip"/>
            <xsd:attribute name="rport"/>
            <xsd:attribute name="lport"/>
            <xsd:attribute name="outvol"/>
            <xsd:attribute name="invol"/>
            <xsd:attribute name="domain"/>
            <xsd:attribute name="stime"/>
            <xsd:attribute name="etime"/>
        </xsd:complexType>
    </xsd:element>
```

4.3.2.4 垃圾邮件（Spam）

类说明

描述主机是否传播垃圾邮件。

类图（如图12所示）

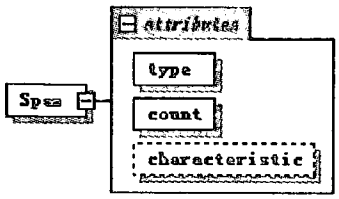


图12 传播垃圾邮件类图

子类

无。

属性

Type：必选。广告、恶意程序、色情、危害社会安全、钓鱼等。

Count：必选。拦截数量。

Characteristic：可选。垃圾邮件特征码。

Schema定义

```
<xsd:element name="Spam">
        <xsd:complexType>
            <xsd:attribute name="type" use="required"/>
            <xsd:attribute name="count" use="required"/>
            <xsd:attribute name="characteristic"/>
        </xsd:complexType>
    </xsd:element>
```

4.3.2.5 网页篡改（Webdefacement）

类说明

主机是否存在页面篡改。

类图（如图13所示）

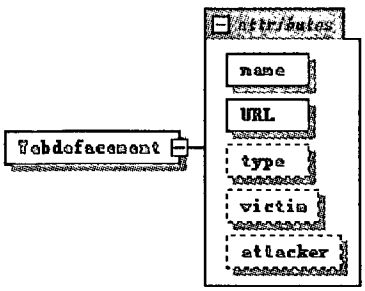


图13 页面篡改类图

子类

无。

属性

Name：必选。事件名称；

URL：必选。被篡改页面的地址；

Type：可选。夹带、内容篡改；

Victim：可选。被攻击网站名称；

Attacker：可选。攻击者。

Schema定义

```
<xsd:element name="Webdefacement">
        <xsd:complexType>
            <xsd:attribute name="name" use="required"/>
            <xsd:attribute name="URL" use="required"/>
            <xsd:attribute name="type"/>
            <xsd:attribute name="victim"/>
            <xsd:attribute name="attacker"/>
        </xsd:complexType>
    </xsd:element>
```

4.3.2.6 网页挂马（Web-based Malware Website）

类说明

描述主机是否存在网页挂马的现象、以及所利用的相关漏洞信息。

类图（如图14所示）

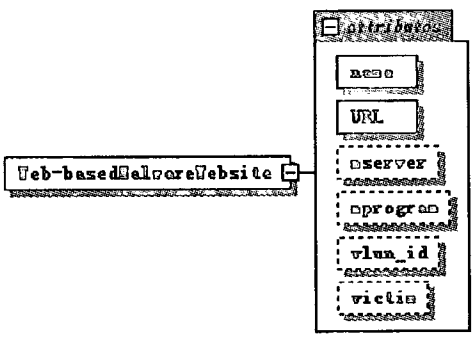


图14 网页挂马类图

子类

无。

属性

Name：必选。事件名称；

URL：必选。被挂马页面的地址；

Mserver：可选。恶意服务器域名。用于网页跳转、漏洞触发、存放恶意程序；

Mprogram：可选。相关的网马、木马、病毒、广告件等恶意程序 。恶意程序名称；

Vlun_id：可选。利用的漏洞编号；

Victim：可选。被攻击网站名称。

Schema定义

```
<xsd:element name="Web-basedMalwareWebsite">
        <xsd:complexType>
            <xsd:attribute name="name" use="required"/>
            <xsd:attribute name="URL" use="required"/>
            <xsd:attribute name="mserver"/>
            <xsd:attribute name="mprogram"/>
            <xsd:attribute name="vlun_id"/>
            <xsd:attribute name="victim"/>
        </xsd:complexType>
    </xsd:element>
```

4.3.2.7 非授权访问（Unauthorized access）

类说明

主机上是否存在非授权访问。

类图（如图15所示）

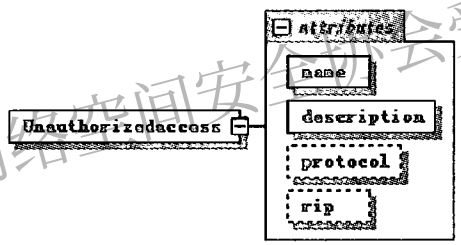


图15 非授权访问类图

子类

无。

属性

Name：必选。事件名称；

Description：必选。访问行为描述；

Protocol： 可选。涉及的相关协议；

Rip：可选。访问者IP；

Schema定义

```
<xsd:element name="Unauthorizedaccess">
    <xsd:complexType>
        <xsd:attribute name="name" use="required"/>
        <xsd:attribute name="description" use="required"/>
        <xsd:attribute name="protocol"/>
        <xsd:attribute name="rip"/>
```

```
        </xsd:complexType>
    </xsd:element>
```

4.3.2.8 网页仿冒（Phishing）

类说明

主机是否存在网页仿冒、钓鱼欺骗行为。

类图（如图16所示）

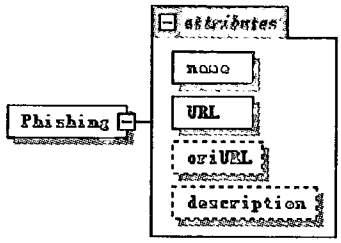


图16 网页仿冒类图

子类

无。

属性

Name：必选。事件名称；

URL：必选。网络仿冒使用的仿冒页面链接；

OriURL：可选。被仿冒的网站地址；

Description：可选。事件详细描述。

Schema定义

```
<xsd:element name="Phishing">
    <xsd:complexType>
        <xsd:attribute name="name" use="required"/>
        <xsd:attribute name="URL" use="required"/>
        <xsd:attribute name="oriURL"/>
        <xsd:attribute name="description"/>
    </xsd:complexType>
</xsd:element>
```

4.3.2.9 其他（Other）

类说明

其他（Other）作为一个扩展机制，用于描述那些不能在4.3.2的上述安全属性中描述的信息。

类图（如图17所示）

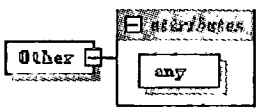


图17 其他类图

子类

无。

属性

Any：存在零个或多个实例。任何属性。

Schema定义

```
<xsd:element name="Other">
    <xsd:complexType>
        <xsd:attribute name="any" use="required"/>
    </xsd:complexType>
</xsd:element>
```

4.3.3 其他数据（AdditionalData）

类说明

其他数据（AdditionalData）类作为一个扩展机制，用于描述那些不能在数据模型中描述的信息。

类图（如图18所示）

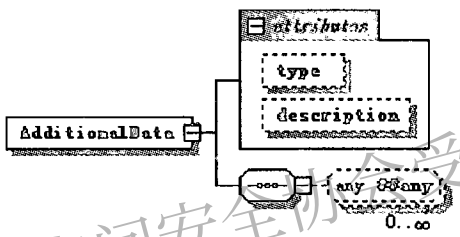


图18 其他数据类图

子类

Any：存在零个或多个实例。任何子类

属性

Type：可选。元素内容的数据类型；

Description：可选，字符串类型。该类中用户自定义的数据的语义的描述。

Schema定义

```
- <xsd:element name="AdditioanlData">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs=
"unbounded"/>
        </xsd:sequence>
        <xsd:attribute name="type"/>
        <xsd:attribute name="description"/>
    </xsd:complexType>
</xsd:element>
```

4.3.4 联系（Contact）

类说明

联系（Contact）类描述互联网主机有关的组织和个人的联系信息，Contact类封装了对有关方的命名，详细说明了能够通知到他们的联系信息，并标识了他们在互联网主机中的角色。

类图（如图19所示）

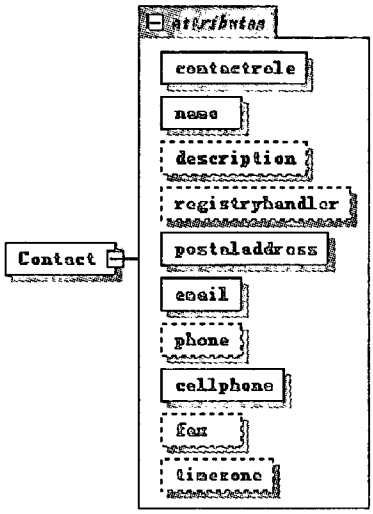


图19 联系类图

子类

无。

属性

Contactrole：必选。枚举类型；

说明：指出联系信息的角色，这个属性被定义为一个枚举列表：

creator：生成HNSADF文档的实体；

admin：主机或者网络的管理员；

tech：主机或者网络的技术联系；

irt：参与事件处理的CSIRT；

Cc：保持告知互联网主机处理的实体。

Name：必选。联系的名称。联系信息可以是一个组织，也可以是某个人；

Description：可选。联系信息的自由形式的描述。当type类型为个人时，通常是指这个人的组织头衔；

Registryhandler：可选。在注册处理机构名称（比如运营商及管理员在亚太网络信息中心APNIC注册的Handle），该子类须对接收方有意义，组织内部的处理机构名称对于组织之外的通信没有什么意义；

Postaladdress：必选。联系人或组织的邮政地址；

Email：必选。联系人或组织的电子邮件地址；

Phone：可选。固定电话号码；

Cellphone：必选。手机号码；

Fax：可选。传真号码；

Timezone：可选。联系人或组织所在的时区。

Schema定义

```
<xsd:element name="Contact">
    <xsd:complexType>
        <xsd:attribute name="contactrole" use="required"/>
        <xsd:attribute name="name" use="required"/>
        <xsd:attribute name="description"/>
        <xsd:attribute name="registryhandler"/>
        <xsd:attribute name="postaladdress" use="required"/>
        <xsd:attribute name="email" use="required"/>
        <xsd:attribute name="phone"/>
        <xsd:attribute name="cellphone" use="required"/>
        <xsd:attribute name="fax"/>
        <xsd:attribute name="timezone"/>
    </xsd:complexType>
</xsd:element>
```

4.3.5 评估（Assessment）类

类说明

评估（Assessment）类描述互联网主机活动的技术与非技术方面的影响。

类图（如图20所示）

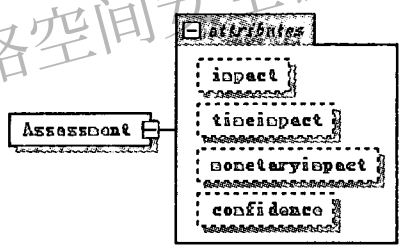


图20 评估类图

子类

无。

属性

Impact：可选。枚举类型。从技术角度评估互联网主机活动对计算机、网络等系统运营的影响，可供选取的值如下所示，该属性没有缺省值：

low：低严重性；

medium：中等程度严重性；

high：高严重性。

timeimpact：可选。枚举类型。互联网主机活动用时间度量的影响，可供选取的值如下所示，该属性没有缺省值：

short：短时间；

medium：中等时间；

long：长时间。

Monetaryimpact：可选，枚举类型。互联网主机活动用货币度量的影响，可供选取的值如下所示，该属性没有缺省值：

low：低严重性；

medium：中等程度严重性；

high：高严重性。

Confidence：可选。枚举类型。从用户的角度，对互联网主机服务能力的信心评估。可选值如下：

low：信心低；

medium：信心中；

high：信心高。

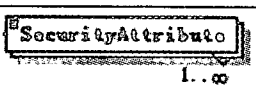
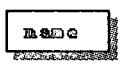
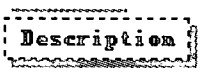
Schema定义

```
<xsd:element name="Assessment">
<xsd:complexType>
    <xsd:attribute name="impact"/>
    <xsd:attribute name="timeimpact"/>
    <xsd:attribute name="monetaryimpact"/>
    <xsd:attribute name="confidence"/>
</xsd:complexType>
</xsd:element>
```

附 录 A
（资料性附录）
类图图例说明

本标准使用类图来描述数据模型。在类图中，各符号图例含义如表A.1。

表A.1 类图的图例说明表

符号图例	含义
	类HNSADF-Document是聚合类，包含有子类
	类Host是聚合父类必须包含的单个子类，只能存在一个实例
	类SecurityAttribute是聚合父类必须包含的子类，存在一个至多个实例，个数不限
	类Assessment是聚合父类可能包含的子类，最多存在一个实例
	类AdditionalData是聚合父类可能包含的子类，存在零个或多个实例
	属性name，必须存在值
	属性Description，可以为空

附 录 B
（资料性附录）
安全属性描述格式的基础数据类型

B.1 整数

由INTEGER数据类型表示整数属性，整数数据必须以10或者16为基底编码。

以10为基底的整数编码使用阿拉伯数字‘0’到‘9’，以及可选符号‘+’或者‘-’。例如，“123”，“-456”。

以16为基底的编码使用阿拉伯数字‘0’到‘9’，以及‘a’到‘f’（或者它们的大写形式），并且在前面加上字符“0x”。例如，“0x1a2b”。

B.2 实数

由REAL数据类型来描述实数（浮点）属性。实数数据必需以10为基底编码。

实数编码和POSIX函数例库中的“strtod”一样：一个可选符号后跟一个非空的小数位数串，可选择包含一个基数字符，然后是一个可选的指数部分。一个指数部分由一个“e”或者“E”，后跟一个可选的符号，接下来是一个或者多个小数位数。例如，“123.45e02”，“-567,89e-03”。

与本标准兼容的应用程序必需支持“.”和“,”基数字符。

B.3 字符和字符串

由CHARACTER数据类型来描述单字符属性，由STRING数据类型描述已知长度的多字符属性。

字符和字符串数据没有特殊的格式要求，除了偶尔需要使用转义字符来表示特殊的字符。

B.4 字节

字节数据类型BYTE是在计算机信息技术中用于本地计量存储容量及网络传输容量的一种计量单位，1个字节是相邻的8位二进制数码。

B.5 枚举类型

由ENUM数据类型描述枚举类型，枚举类型是由可接受的值构成的一个有序列表。每一个值代表一个关键字。在本标准中，枚举类型关键字被用作属性值。

B.6 日期一时间

由本标准的DATETIME数据类型描述日期一时间串。在本标准中，日期格式为年/月/日，时间格式为时/分/秒。

B.7 端口列表

由PORTLIST数据类型描述网络端口列表，它由一个以逗号分隔的数字和范围（N-M表示端口号N至端口号M，包括M）的序列组成，可以在一个单独的序列中使用数字和范围的任意组合。例如“5-25,37,42,43,53,69-119,123-514”。

B.8 邮政地址

由POSTAL数据类型描述邮政地址。POSTAL数据格式在IETF RFC 2256 的5.17 - 5.19有详细说明。其格式如下：

建筑物，街道，邮政编码，城市，国家，或者邮政信箱，邮政编码，城市，国家。

B.9 电话和传真号码

由PHONE数据类型描述电话号码。电话和传真号码遵循ITU推荐的表达格式：

+ （国际电码）（本地代码）（电话号码）

PHONE数据类型的格式参见IETF RFC 2256的5.21。

B.10 电子邮件

由EMAIL数据类型描述电子邮件地址。EMAIL数据类型的格式参见IETF RFC 2822的3.4.1。

B.11 惟一标识

由UID数据类型描述HNSADF文档的某个特定创建者的惟一标识符。由GUID数据类型描述全局惟一的标识符。UID和GUID数据类型是由字母数字串构成。

中华人民共和国
通信行业标准
互联网主机网络安全属性描述格式
YD/T 2707-2014
*
人民邮电出版社出版发行
北京市丰台区成寿寺路11号邮电出版大厦
邮政编码：100164
宝隆元（北京）印刷技术有限公司印刷

*
开本：880×1230　1/16　　2014年11月第1版
印张：2　　2014年11月北京第1次印刷
字数：52千字
15115·495
定价：25元
本书如有印装质量问题，请与本社联系　电话：(010)81055492