ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 40652—2021

信息安全技术
恶意软件事件预防和处理指南

Information security technology—
Guide to malware incident prevention and handling

2021-10-11 发布　　2022-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国科学院大学、西安电子科技大学、国家计算机病毒应急处理中心、中国科学院信息工程研究所、奇安信科技集团股份有限公司、北信源软件股份有限公司、中国航空综合技术研究所。

本文件主要起草人：张玉清、何远、刘奇旭、王鹤、杨毅宇、王文杰、王基策、陈建民、付安民、李学俊、钟力、刘兴安、张翀斌、张永印、林玥、孙鸿宇、刘新建。

信息安全技术
恶意软件事件预防和处理指南

1 范围

本文件在GB/T 20985.1—2017和GB/T 20985.2—2020的基础之上，针对恶意软件事件的预防和处理过程给出了进一步指南。

本文件适用于计算机系统管理人员、网络管理人员、安全事件响应小组等预防和处理恶意软件事件。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 20985.1—2017 信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理

GB/T 20985.2—2020 信息技术 安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

恶意软件 malware

被专门设计用来损害或破坏系统，对保密性、完整性或可用性进行攻击的软件。

注：病毒和木马是恶意软件的例子。

[来源：ISO/IEC 27033-1:2015,3.22]

3.2

恶意软件事件 malware incident

由恶意软件引起，并造成保密性、完整性或可用性破坏的信息安全事件。

3.3

防病毒软件 antivirus software

监控主机和网络的程序，通过恶意软件的特征、白名单和异常行为等检测恶意软件，并能识别和清除恶意软件。

注：防病毒软件又称为反病毒软件、杀毒软件。

3.4

病毒 virus

在计算机程序中插入破坏计算机功能或者数据，影响计算机使用并且能自我复制的一组计算机指令或程序代码。

[来源：GB/T 31499—2015,3.6]

3.5

勒索软件　ransomware

采取加密或屏蔽用户操作等方式劫持用户对系统或数据的访问权，并借此向用户索取赎金的恶意软件。

3.6

后门　backdoor

可以绕过系统的权限管理机制，接收并执行来自特定端口请求的恶意软件。

3.7

恶意移动代码　malicious mobile code

带有恶意意图并能够通过远程主机传播到本地主机，无需用户主动触发就可以在本地自动执行的代码。

3.8

间谍软件　spyware

从计算机窃取用户隐私或保密信息的恶意软件。

注：信息可能包括最频繁访问的网站或密码之类的更敏感信息的事项。

[来源：ISO/IEC 27032:2012，4.43]

3.9

Rootkit 恶意软件　rootkit malware

隐藏在目标系统内部，能够以内核态或用户态权限运行，并对系统功能调用请求进行拦截和篡改，以及秘密收集目标系统信息的恶意软件。

3.10

默认拒绝　deny by default

防火墙或路由器的配置项，除了明确允许通过的网络数据外，在默认情况下拒绝其他所有网络数据。

3.11

事件响应小组　incident response team；IRT

由组织中具备适当技能且可信的成员组成的团队，负责在事件生存周期中处理事件。

注：IRT 通常被称为 CERT(计算机应急响应小组)和 CSIRT(计算机安全事件响应小组)。

[来源：GB/T 20985.1—2017，3.2]

4　缩略语

下列缩略语适用于本文件。

BIOS：基本输入输出系统(Basic Input/Output System)

DDoS：分布式拒绝服务攻击(Distributed Denial of Service)

HTTP：超文本传输协议(Hypertext Transfer Protocol)

IDS：入侵检测系统(Intrusion Detection System)

IoT：物联网(Internet of Things)

IP：网际互连协议(Internet Protocol)

IPS：入侵防御系统(Intrusion Prevention System)

USB：通用串行总线(Universal Serial Bus)

5 规划和准备

5.1 概述

GB/T 20985.1—2017 的 5.2 和 GB/T 20985.2—2020 的第 4 章～第 11 章的指南适用。并且，以下事件响应小组、基本预防措施、安全意识教育、脆弱性防范、恶意软件防范等特定的指南适用。

5.2 事件响应小组

5.2.1 概述

在 GB/T 20985.1—2017 中 5.2 的 c)、d)和 GB/T 20985.2—2020 的第 7 章基础上给出如下进一步指南。组建事件响应小组时应综合考虑以下内容。

5.2.2 小组职责

组织宜依托事件响应小组，负责恶意软件事件的响应工作，制定针对恶意软件事件的处理流程，并参照事件处理流程对安全事件响应小组成员分配不同的角色。经常对小组成员进行安全培训，保证小组成员能及时准确地对恶意软件事件做出反应及进行处理。

5.2.3 人员技能

恶意软件事件处理人员宜掌握以下技能。

a) 了解已知的典型恶意软件感染和传播的主要特征。

b) 熟悉组织配备的恶意软件检测工具和相关配置情况，会使用所配备的工具，能分析相关数据并确认特定的威胁。

c) 有一名以上事件处理人员熟练使用计算机取证工具。

d) 对信息技术广泛了解，能预判恶意软件事件对组织带来的威胁或影响，为遏制、根除恶意软件事件的威胁或影响，以及恢复信息系统正常工作做出对应的决策。恶意软件事件的常见场景见附录 A。

e) 有一名以上具备高级语言编程能力的维护人员。

5.2.4 安全服务外包要求

组织无法满足恶意软件事件响应人员的技能要求和团队要求时，宜考虑安全服务外包，并满足以下要求：

a) 与外包服务商签订相关协议，确保能及时处理恶意软件事件；

b) 外包服务商无法及时达到现场处理时，可实施远程指导；

c) 外包服务商平时给予定期或不定期安全检查；

d) 外包服务商了解各项业务功能及其之间的相关性，确定支持各种业务功能的相关信息系统资源及其他资源，明确相关信息的保密性、完整性和可用性要求；

e) 外包服务商应协助用户建立适当的应急响应策略，能及时对业务中断、系统宕机、网络瘫痪等突发安全事件造成的影响进行评估，并在事件发生后提出快速有效的恢复信息系统运行的方法；

f) 外包服务商提供相关的培训服务，以提高用户的安全意识，便于相关责任人明确自己的角色和责任，了解常见的安全事件和入侵行为，熟悉应急响应策略。

5.2.5 工具和资源

安全事件响应小组成员宜配备必要的工具和资源，具体如表 1 所示。

表 1 恶意软件事件处理工具和资源

工具/资源	说明
恶意软件事件处理人员的通讯方式	
联络信息	组织内部和外部小组成员的联络信息（例如，电话号码、邮件地址、手机号码等），以及防病毒软件提供商和其他事件响应小组的联络信息等
在线设备	提供给组织内其他小组的即时更新信息、升级信息等
互联网连接替补方案	遭遇严重恶意软件事件以致网络无法连接时，需要使用其他方法来寻找有关新威胁的信息、下载补丁和实时更新
分析恶意软件事件的软件和硬件工具	
便携式计算机	用于分析恶意代码样本、主机日志及网络流量数据
备用服务器、网络设备	用来在独立环境中测试恶意软件；如果安全事件响应小组无法确定额外设备的代价，可以考虑使用测试实验室中的设备，或者使用操作系统仿真软件建立虚拟实验室
存储设备	用来保存和传输恶意软件样本的存储设备，如 USB 盘、光盘等
分析工具	分别用来抓取数据包和分析网络流量的包嗅探器和协议分析仪；最新的未被感染的操作系统和分析工具；用来检测可能存在恶意软件感染的软件（例如，防病毒软件、恶意软件专杀工具、系统管理软件、网络取证工具）
恶意软件事件分析资源	
端口列表	包括常用端口和已知木马和后门端口号
相关文档	包含操作系统、应用程序、协议、反病毒和入侵检测标记等信息的文档
关键资源目录	关键资源的图标和目录，如网站、电子邮件和文件传输服务器
基线	网络、系统和应用程序活动的预期基线
恶意软件事件处理软件	
工具软件	包括操作系统启动盘、操作系统安装盘、应用程序安装盘等
安全补丁	操作系统和应用程序供应商提供的安全补丁
镜像软件	操作系统、应用程序、存储在辅助存储设备中的备份镜像

5.3 基本预防措施

在 GB/T 20985.1—2017 的 5.2 c)和 GB/T 20985.2—2020 的 6.4 a)基础上给出如下进一步指南。制定基本预防措施时应综合考虑以下内容：

a) 限制用户使用管理员级别的特权；

b) 及时升级操作系统和应用程序的版本，并及时下载、安装补丁修复相关漏洞；

c) 指明哪种类型的系统（例如文件服务器、电子邮件服务器、代理服务器）和应用程序（例如电子邮件客户端、浏览器）需要哪些对应类型的安全预防软件（如防病毒软件、恶意软件专杀工具），同时为配置和维护软件列出相关要求（比如软件更新频率、系统扫描范围）；

d) 通过组织安全管理部门的批准，方可访问其他网络（包括互联网）；
e) 对防火墙宜进行统一管理、监测和审计；
f) 对终端设备设置 BIOS 口令；
g) 及时备份重要数据和文件，备份系统与原系统隔离；
h) 保存资产清单，以便及时了解需要保护的内容并对其进行漏洞评估。

5.4 安全意识教育

在 GB/T 20985.1—2017 的 5.2 g）和 GB/T 20985.2—2020 的第 10 章基础上给出如下进一步指南。安全意识教育相关内容如下：

a) 不宜打开未知来源的电子邮件或者电子邮件附件，不通过电子邮件发送或接收可执行文件；
b) 不宜使用与业务不相关的软件；
c) 不宜点击可疑的浏览器弹出式窗口；
d) 不宜点击可疑的网络地址链接；
e) 不宜访问可能含有恶意内容的网站；
f) 不宜打开可能与恶意软件相关联的文件；
g) 不宜关闭防病毒软件、恶意软件专杀工具、防火墙等安全软件；
h) 不宜使用管理员级别的账户进行常规操作；
i) 不宜下载或执行来自不可信任（如陌生网站）来源的应用程序；
j) 不宜通过电子邮件回复金融或个人信息，组织不宜通过电子邮件要求得到这些信息；
k) 在回复电子邮件或自动弹出式窗口时不应提供任何账号、密码或者其他登录凭证，只在组织内部网站中使用这些信息；
l) 如果收到可疑的附件（如陌生人发送的邮件），宜通过电话等方式联系发送者确认附件的真实性；
m) 不宜回复任何陌生的或无法确认的电子邮件；
n) 宜定期对自己的账户密码进行修改并注意加强密码强度，并实施有效的权限管理机制，结合生物特征识别等技术手段对账户信息进行加密保护；
o) 不宜在互联网上随意登录组织内部的邮箱，宜对垃圾邮件进行及时过滤或清理。

5.5 脆弱性防范

5.5.1 概述

在 GB/T 20985.1—2017 的 5.2 f）和 GB/T 20985.2—2020 的 6.4 a）基础上给出如下进一步指南。进行脆弱性防范时应综合考虑以下内容。

5.5.2 补丁管理

补丁管理宜做到以下几点：

a) 从官方渠道获取补丁；
b) 评估补丁对系统的影响，在安全隔离的环境（对其他设施或系统不造成影响的环境）测试补丁，并记录补丁的评估和决策过程；
c) 及时测试新补丁并对漏洞进行修复，确认软件漏洞没有对应补丁的情况下，宜利用其他的脆弱性缓解技术或安全防御技术来预防恶意软件事件的发生；
d) 测试补丁的可利用性时，满足补丁对组织中每一个易受攻击的系统都有效，特别是远程系统（例如远程办公系统等）。

5.5.3 最小特权原则

使用最小特权原则宜做到以下几点：

a) 对组织内的信息系统优先利用最小特权原则；

b) 对组织内的服务器、网络设备、应用程序等，进行用户分级管理，对不同级别的用户赋予满足需求的最低权限。

5.5.4 其他预防措施

除了利用安全软件等预防恶意软件，组织宜用如下措施加强预防：

a) 卸载/禁用与业务无关的服务或端口，如 445 端口等；

b) 删除不安全的文件共享；

c) 删除或者更改操作系统和应用程序的默认用户名和密码；

d) 使用网络服务之前对使用者进行身份验证；

e) 通过修改操作系统配置项，禁止自动运行二进制文件和脚本程序，关闭自动播放策略。

5.6 恶意软件防范

5.6.1 概述

在 GB/T 20985.1—2017 的 5.2 f)和 GB/T 20985.2—2020 的 6.4 a)基础上给出如下进一步指南。进行恶意软件防范措施时应综合考虑以下内容。

5.6.2 安全软件部署和管理

组织部署和管理安全软件时宜考虑以下要点。

a) 安装好操作系统后立即安装防病毒软件，更新最新的病毒特征库，并安装防病毒软件补丁。

b) 正确配置防病毒软件，确保防病毒软件可以持续有效地检测和阻止恶意软件攻击。

c) 对统一集中管理的计算机，由安全管理员定期监测防病毒软件的运行情况。管理员通常负责获取、测试、核实、发布病毒特征库，并在组织内进行更新。

d) 安全管理员进行定期检查，确保系统配置正确并正在使用最新的防病毒软件。

e) 部署集中管理的防病毒软件时，组织确保网络和服务器可以满足日常更新和峰值更新时的需求。

f) 为预防服务器漏洞造成的影响，组织宜考虑使用不同的操作系统平台搭建防病毒服务器，而不是使用与组织中大多数服务器和工作站相同的操作系统。

g) 为提高预防恶意软件的能力，在关键系统(例如电子邮件服务器)中使用多种防病毒产品。

h) 对组织的远程连接网点，组织宜考虑改造为统一集中管理。无法统一管理时，及时发送消息给远程用户，提醒用户及时更新病毒特征库。

i) 对用户进行安全知识培训，出现重大威胁时本地系统管理员和远程用户可有效配合执行操作。

j) 为集中化管理和监测，组织决定应用程序如何分布、配置和维护，以及如何去监控恶意软件的活动。

k) 用户不宜在系统中禁用或卸载防病毒软件，也不宜更改任何关键设置。

l) 用户在使用防病毒软件时宜根据系统提示或安全管理员的要求及时升级软件、更新病毒特征库等。

5.6.3 防病毒软件

组织内部署防病毒软件时，防病毒软件宜提供以下保护功能：

a) 扫描系统的关键组件，例如启动文件和引导记录等；
b) 自动对外部存储设备（如移动硬盘、USB 盘等）和电子邮件附件进行扫描；
c) 实时检查系统中的可疑活动，例如扫描所有电子邮件附件防止已知病毒通过电子邮件传播；
d) 监测常见的应用程序，例如浏览器、文件传输程序以及即时通讯软件的行为；
e) 防病毒软件能监测可能被用于感染系统和向其他系统传播恶意软件的应用程序的活动；
f) 定期扫描所有硬盘驱动器，以便确认系统是否受感染；支持选择性地扫描其他存储设备，可以按需求对外部存储设备执行手动扫描；
g) 检测恶意软件，包括病毒、蠕虫、木马、勒索软件、间谍软件等；
h) 清理注册表、恶意锁定主页等被恶意软件修改的启动选项；
i) 隔离可疑对象；
j) 定时自动更新病毒库；
k) 监测在系统启动时自动加载的进程和程序。

5.6.4 恶意软件专杀工具

恶意软件专杀工具宜具备以下功能：

a) 对特定的恶意软件目标，能够快速识别和定位，缓解恶意软件影响，从系统中根除恶意软件；
b) 定期扫描文件，内存和配置文件等，检测可能存在的特定恶意软件；
c) 针对某些传播速度快、容易多次感染的恶意软件（例如 USB 盘病毒、勒索病毒等）提供免疫功能；
d) 针对某些对操作系统功能造成破坏（例如映像劫持、安全模式禁用、任务管理器禁用、注册表管理器禁用、桌面菜单右键显示损坏、命令行工具禁用、无法修改浏览器主页、显示文件夹选项禁用等）的恶意软件，提供修复功能；
e) 针对某些感染文件造成文件损坏的恶意软件，提供修复文件功能。

5.6.5 终端安全软件

终端安全软件能限制主机出入网络的活动，既能阻止主机受感染又能阻止主机向外传播恶意软件。配置终端安全软件时宜做到以下几点：

a) 为预防恶意软件事件，基于主机的防火墙对流入的数据采用默认拒绝规则，推荐组织结合实际情况对流出的数据采用默认拒绝规则；
b) 开启阻止网页浏览器弹出窗口、抑制服务器缓存文件（Cookies）以及识别网页和电子邮件中的潜在信息泄漏等功能；

注：Cookies 是指服务器发给客户端，并保存在客户端中的小型文本文件。

c) 正确配置终端安全软件，能实时更新最新的病毒特征库和软件模块；
d) 为预防网络蠕虫和其他威胁，可以通过终端安全软件来保护可直接访问网络的系统。

5.6.6 应用程序设置

预防恶意软件事件宜考虑的应用程序设置如下：

a) 阻止打开和运行可疑电子邮件的附件中的文件；
b) 过滤可疑内容，如过滤垃圾邮件和网站有害内容；
c) 限制可疑内容，如限制网页浏览器的服务器缓存文件（Cookies）；
d) 拦截网页浏览器的弹出式窗口；
e) 防止自动启动宏应用，如办公软件中的软件宏语言自动运行。

5.6.7 区域边界防病毒设备

组织宜在网络区域边界部署网络防火墙或IDS、IPS。配置网络防火墙或IPS时宜做到以下几点：

a) 基于网络流量识别已知和未知恶意攻击，提供网络流量过滤功能，阻止异常流量的入侵；
b) 有效监测出攻击应用程序（如电子邮件服务器、网络服务器）的恶意活动；
c) 识别蠕虫活动和其他形式的恶意软件，以及像后门和电子邮件生成器这样的攻击；
d) 开启默认拦截功能，但在特定条件下，设置允许使用或禁止使用拦截功能；
e) 为预防恶意软件事件，设置默认拒绝规则集，拒绝任何没有被允许进出的数据通过；
f) 为降低蠕虫的传播速度，考虑对外部系统（例如远程办公的家用系统、商业合作伙伴系统）的网络制定限制措施；
g) 网络防火墙对进入和流出的数据包进行过滤，并确保每一条规则有效，定期审查网络防火墙控制访问列表，删除无效规则；
h) 应配置网络地址转换功能，将内部网络的私有地址映射成连接到互联网中的一个或多个公共地址，有利于阻止蠕虫攻击组织内部主机；
i) 发生防病毒软件和入侵防御系统不能监测的重大恶意软件事件时，更改防火墙规则以阻止基于网络服务的恶意软件扩散；
j) 阻止木马等恶意软件访问外部主机IP地址。

6 发现和报告

6.1 概述

GB/T 20985.1—2017的5.3和GB/T 20985.2—2020的6.4 b)、6.5、6.6、6.9中的指南适用。并且，以下恶意软件事件发现特定的指南适用。

6.2 恶意软件事件发现

在GB/T 20985.1—2017的5.3 c)基础上给出如下进一步指南。提前发现恶意软件事件的途径如下。

a) 恶意软件预警公告。防病毒软件提供商和其他安全相关组织发布的有关新的重大恶意软件或威胁情报预警的公告。
b) 安全设备告警。恶意软件的运行会导致防病毒软件等安全设备产生相关告警，这些告警意味着可能会发生恶意软件事件。

针对常见恶意软件，表2列出了恶意软件事件最有可能的迹象。获得管理员权限的恶意软件的迹象没有在表2中列出。

表2 恶意软件迹象

迹象	恶意软件类型										
	复合型病毒	宏病毒	网络服务蠕虫	垃圾邮件蠕虫	特洛伊木马	恶意移动代码	后门	按键记录	Rootkit	恶意浏览器插件	邮件生成器
安全设备											
防病毒软件告警	√	√	√	√	√	√	√	√	√	√	√

表 2　恶意软件迹象（续）

迹象	恶意软件类型										
	复合型病毒	宏病毒	网络服务蠕虫	垃圾邮件蠕虫	特洛伊木马	恶意移动代码	后门	按键记录	Rootkit	恶意浏览器插件	邮件生成器
安全设备											
专杀工具告警					√	√				√	
防火墙或 IPS 告警			√	√			√				
终端安全软件告警					√				√		
可观察到的主机活动											
系统无法启动	√								√		
系统启动时显示错误信息	√								√		
系统不稳定，并发生崩溃		√	√		√		√		√		
程序启动缓慢，运行缓慢，或无法运行	√	√	√		√				√	√	
系统启动项出现未知进程					√		√	√			√
非常规的端口开放							√				
发送和接受的邮件数量突然增加		√		√					√		
文字处理软件、电子表格等模板更改		√									
浏览器配置更改，如主页更改或出现新的工具条						√				√	
文件删除、崩溃或无法访问	√	√			√				√		
屏幕出现异常图案，如奇怪的消息、图像、重叠或叠加消息框		√				√			√		√
出现意外的对话框，请求允许运行程序						√				√	
观察到的网络活动											
网络流量明显增加			√	√			√				√
脆弱服务（如打开 windows 共享）的端口扫描和失败的连接尝试			√				√				
主机和未知远程系统存在网络连接			√		√	√	√	√	√	√	√

事件处理人员在确认恶意软件事件时宜做到以下几点。

a）　事件处理人员首先验证事件源是否为恶意软件。在事件源不能轻易确认的情况下，通常假设事件是由恶意软件引起并采取对应响应措施，如果随后确定不是恶意软件引起可以更改处理措施。

b）　事件处理人员与网络管理人员等合作，以便于确定数据来源。除了常规的数据来源，事件处理人员了解并熟练使用防火墙和路由器日志文件、邮件服务器和 IPS 的日志文件。

c）　在不产生额外威胁前提下，事件处理人员可以在一个被感染的正常系统或者一个恶意软件测试系统中来研究恶意软件的行为。

d）　分析人员准备一个移动存储设备，存放最新的检测工具（例如防病毒软件、恶意软件专杀工具）

等，并避免该移动存储设备被恶意软件感染。

e) 一旦事件处理人员检测了数据源，确定相关威胁的特性后，处理人员在防病毒服务提供商的恶意软件数据库中寻找这些特性，并以此确定具体是哪种恶意软件。可以参考的恶意软件特性如下：
   1) 被攻击的服务和端口；
   2) 被利用的漏洞；
   3) 邮件主题、附件名称、附件大小、主体内容；
   4) 可能会受影响的操作系统、设备、应用程序等；
   5) 恶意软件如何感染系统(例如通过漏洞、错误的配置)；
   6) 恶意软件如何影响被感染的系统，包括被感染文件的名称和位置、被更改的配置、被安装后门的端口等；
   7) 恶意软件如何传播以及如何遏制；
   8) 如何从系统中清除该恶意软件。

f) 当新的安全威胁没有出现在恶意软件数据库中时，事件处理人员参考其他信息来源以尽快做出响应。

7 评估和决策

GB/T 20985.1—2017 的 5.4 和 GB/T 20985.2—2020 的 6.4 c)中的指南适用。制定评估和决策措施时应考虑其中内容。

8 响应

8.1 概述

GB/T 20985.1—2017 的 5.5 和 GB/T 20985.2—2020 的 6.4 d)中的指南适用。并且，以下恶意软件事件响应计划、恶意软件事件遏制、识别被感染主机、恶意软件根除、恶意软件事件溯源和系统恢复特定的指南适用。

8.2 恶意软件事件响应计划

制定恶意软件事件响应计划时宜考虑如下因素：

a) 恶意软件如何进入系统，以及使用何种传输机制；
b) 全面评估恶意软件事件的传播范围，以及带来的影响和损失；
c) 通过分析得到的其他结论，如恶意软件的来源；
d) 服务对象的业务和重点决策过程；
e) 服务对象的业务连续性；
f) 确定受害系统的范围后，将被害系统和正常的系统进行隔离，断开或暂时关闭被攻击的系统；
g) 确定恶意软件类型(例如病毒、蠕虫和特洛伊木马)；
h) 确定恶意软件的隐藏位置；
i) 持续监视系统和网络活动，记录异常流量的远程 IP、域名、端口；
j) 如果恶意软件事件没有被遏制，预判在接下来的几分钟、几小时、几天内的被感染情况。

8.3 恶意软件事件遏制

遏制恶意软件常用技术见附录 B，通过工具软件遏制恶意软件事件，宜结合以下措施：

a) 需停止或删除系统非正常账号、隐藏账号并更改口令，加强口令的安全级别；
b) 挂起或结束未被授权的可疑的应用程序或进程；
c) 关闭存在的非法服务和不必要的服务；
d) 删除系统各用户“启动”目录下未授权的自启动程序；
e) 使用命令行管理工具或第三方工具停止所有开放的共享服务；
f) 使用防病毒软件或其他安全工具检查文件，扫描硬盘上所有的文件，隔离或清除病毒、木马、蠕虫和后门等恶意软件文件；
g) 在相关法律规定范围内设置陷阱，如蜜罐系统或者反击攻击者的系统；
h) 通过防病毒软件等自动检测并遏制；
i) 通过配置实现拒绝接收具有某些特性的邮件或附件，阻断恶意软件通过邮件传播；
j) 根据恶意软件的特性，通过防火墙、IPS 或终端安全软件遏制恶意软件；
k) 暂时关闭恶意软件使用的服务来遏制恶意软件，清除恶意软件后再恢复服务；
l) 无法使用关闭服务进行遏制的恶意软件，可在对恶意软件的特征进行分析后，通过重新配置网络把被感染主机从网络中断开；
m) 事件处理人员无法遏制恶意软件时，宜及时与专业部门联系并获得支持。

8.4 识别被感染主机

8.4.1 常规识别

常规识别被感染主机时宜结合以下工具或数据。

a) 恶意软件查杀工具。如防病毒软件、恶意软件专杀工具、终端安全软件等。
b) 网络设备日志。防火墙、路由器和其他过滤设备，它们记录了网络连接活动。
c) 攻击特征收集路由器（例如 Sinkhole 路由器）数据，它记录了所有的网络流量。

注：Sinkhole 路由器是通过特殊配置后，专门用来记录攻击流量特征的特殊路由器。

d) 应用程序服务器日志。如电子邮件和 HTTP 服务器等。
e) 网络取证工具。如网络取证分析工具和数据包嗅探器。

8.4.2 主动识别

主动识别恶意软件宜使用如下方法。

a) 通过编写本地脚本识别一些恶意软件。
b) 自定义防火墙、IPS 或 IDS 特征。制定一个自定义的防火墙、IPS 或者 IDS 特征，可以有效检测恶意软件。
c) 包嗅探器。配置包嗅探器并寻找特定恶意软件威胁对应的数据包，可以有效识别被感染主机。
d) 漏洞评估软件。用来识别主机漏洞的软件也可以检测一些已知的恶意软件。
e) 主机扫描器。如果某个恶意软件在被感染主机中安装后门，这些后门程序在运行时会使用某个特定端口，使用主机扫描器就可以有效识别被感染主机。
f) 其他扫描器。除了主机扫描器外，一些特殊的配置或者大小特定的系统文件都可能暗示主机被感染。

8.4.3 手动识别

手动识别恶意软件宜考虑如下因素。

a) 主机多系统使得识别被感染主机非常困难。一些主机可以启动多个操作系统或者使用虚拟机软件；一个操作系统实例被感染时，如果目前正在使用另一个操作系统，那么也无法识别出来。

b) 漏洞未修复可能会影响准确识别被感染主机，由于系统存在没有修复的漏洞时，可能会再次感染。
c) 一些恶意软件会删除其他恶意软件的痕迹，这将导致部分或全部恶意软件没有被检测到。
d) 在大规模恶意软件事件发生时，利用准备阶段的资产清单，识别被感染的主机，制定有效遏制方案。
e) 没有集中管理的环境下，借助网络设备来定位被感染主机。当怀疑主机被感染时，可将其从网络中断开，然后等待该用户报告断网。
f) 先处理确定被感染的主机，对不能确定是否感染的主机，采取事先商定的措施处理。
g) 向用户提供恶意软件相关信息和工具，如被感染的迹象、防病毒软件、操作系统或应用程序补丁、扫描工具，让用户自己判断是否被感染。
h) 无法识别被感染主机，不能彻底解决恶意软件事件时，向安全服务公司寻求帮助。

8.5 恶意软件的根除

8.5.1 典型根除措施

根除恶意软件宜考虑如下措施。

a) 清理系统中存在木马、病毒、恶意代码程序。
b) 恢复被黑客篡改的系统配置，删除黑客创建的后门账号。
c) 删除异常系统服务、清理异常进程。
d) 根除恶意软件后，修复系统缺陷，关闭危险服务(如文件共享等)。
e) 如果恶意软件无法彻底根除，则重新安装操作系统、应用程序、从已知安全备份中恢复数据。
f) 部分感染会在数天、数周、数月内重复发生。事件处理人员需要周期性地进行识别工作，以继续寻找被感染的系统，并确保根除工作的成功实施。
g) 应急服务提供者使用可信的工具进行安全事件的根除处理，不得使用受害系统已有的不可信的文件和工具。
h) 根除后门等恶意软件时，需要了解攻击者入侵的方法，制定封堵策略，以防止被二次入侵感染。
i) 改变全部可能受到攻击的系统账号和口令，并增加口令的安全级别。
j) 增强防护功能。复查所有防护措施的配置，比如安装最新的防火墙和防病毒软件，并及时更新，对未受保护或者保护不够的系统增加新的防护措施。

8.5.2 Rootkit 根除

根除 Rootkit 时宜注意以下几点：

a) 对感染 Rootkit 或者极有可能感染 Rootkit 的系统，通过重新安装和配置操作系统及应用程序实现根除；
b) 一个或多个攻击者得到系统管理员级别访问权限，考虑可能感染 Rootkit；
c) 任何人都可以通过一个后门得到非授权管理员级别访问权限，利用蠕虫或其他方式创建不安全共享，可按感染 Rootkit 进行处理；
d) 系统文件被特洛伊木马、后门、Rootkit、攻击工具等替换，按感染 Rootkit 进行处理；
e) 使用防病毒软件、恶意软件专杀工具完成根除工作后，系统不稳定或者运行出现异常，按感染 Rootkit 进行处理。

8.6 恶意软件事件溯源

恶意软件事件跟踪溯源时宜注意以下几点：

a) 当检测到恶意软件攻击事件时，需记录攻击源 IP、攻击发生的时间、恶意软件类型、被攻击的目标、攻击导致的影响，并向上级部门报告；
b) 通过协议分析工具进行网络流量分析，查找疑似的恶意软件命令控制服务器，然后对命令控制服务器作进一步的探测；
c) 在本机使用诸如进程查看工具等相关主机行为监测分析工具，结合系统日志等信息，获取恶意软件产生的攻击痕迹；
d) 如果获得恶意软件样本，可通过静态分析、动态调试等方法，或在沙箱中对恶意软件样本进行分析，获取恶意软件可能使用的域名、IP 地址、通信端口等信息，以及其攻击方式和执行流程，并进一步探测其攻击源头；
e) 将上述恶意软件相关信息，结合威胁情报、知识库等信息，实现恶意软件事件的追踪溯源。

8.7 系统恢复

系统恢复时宜注意以下几点：
a) 感染恶意软件后，如果操作系统功能正常，用防病毒软件根除恶意软件；
b) 对于破坏性强的恶意软件，造成系统数据文件或驱动程序被删除，处理这些事件时先重建系统或从一个完好的备份中恢复系统，随后采取一些安全措施以保证系统不会再次感染；
c) 事件响应小组考虑可能遇到的最坏情况，并考虑这些情况下如何恢复系统，确定谁执行恢复工作，估计所要花费的时间，决定恢复活动的先后顺序；
d) 恶意软件根除后，取消遏制措施，如果无法确定取消遏制措施后是否会被再次感染，宜继续执行遏制措施，直到威胁解除为止。

9 经验总结

GB/T 20985.1—2017 的 5.6 和 GB/T 20985.2—2020 的 6.4 e)、第 12 章中的指南适用。并且，以下恶意软件特定的指南适用。

恶意软件事件处理完毕后，结合网络流量、系统日志、Web 日志记录、应用日志、数据库日志以及安全产品数据，调查造成安全事件的原因，确定安全事件的威胁和破坏的严重程度。根据整个事件的情况撰写恶意软件事件应急响应报告，文档中阐述整个安全事件的现象、处理过程、处理结果、事件原因，并给出相应的安全建议。最后根据事件的处理过程总结经验。

a) 改进安全策略。例如，以.scr 结尾的邮件附件常被用来传播恶意软件，通过更改安全策略阻止这类邮件就可以预防系统被再次感染。
b) 提高用户安全认知，更新安全认知培训内容，使用户能够正确报告事件并协助处理事件。
c) 更改操作系统或应用程序的设置，以支持新的安全策略。
d) 部署新的检测系统或软件。如果原有的系统或软件无法有效防御恶意软件事件，则可以考虑更新对应的检测系统或软件。
e) 重新配置恶意软件的检测系统或软件。检测系统或软件可能需要按照不同方式重新配置。例如：
   1) 加快软件和特征库的更新速度；
   2) 改进检测的准确性(如更少的误报和漏报)；
   3) 增加监控的范围(如监控额外的传输机制监控额外的文件和系统文件)；
   4) 根据检测到的恶意软件改变自动执行活动。

附 录 A
（资料性）
恶意软件事件处理场景

A.1 概述

恶意软件引发的安全事件日渐增多，恶意软件可导致组织的信息系统运行异常、数据丢失和隐私泄漏等安全问题，对信息系统安全造成严重威胁。恶意软件事件处理的实践是提高恶意软件事件应急处理能力和发现潜在问题的有效方式。在这些实践活动中，恶意软件事件响应小组的成员将会了解恶意软件事件的基本情况，在面对一些相关的问题时，小组将会讨论出现的情况并给出最理想的解决方案。这样做的目的是明确处理人员在现实中遇到同样的问题时的处理方法，并且与推荐的策略进行比较，以查明其是否有缺点和不足。如下所列出的问题几乎适用于所有恶意软件事件处理情况，每种情况附有相对应的问题，组织宜在应急处理实践中考虑这些问题。

A.2 场景所对应的问题

场景所对应的问题如下：

a） 准备/预防：

——为了防止这种情况的发生和减小它的影响，采取了什么措施？

b） 检测和分析：

——这种恶意事件有哪些前兆呢？如果有的话，组织能检测到吗？哪种前兆将促使组织采取预防措施？

——组织能检测到哪种前兆？哪种前兆将导致人们认为恶意软件事件可能已经发生了？

——应急处理小组怎么样分析和验证这类事件？

——组织把这类事件向谁汇报呢？

——事件响应小组如何确立处理这类事件的优先顺序？

c） 遏制，清除和恢复：

——处理小组采取什么样的策略来遏制这类事件？这种策略比其他策略好在哪里？

——如果这类事件不进行遏制将出现什么情况？

d） 事后的工作：

——哪些成员要参加这次的事件的经验教训会议？

——为防止此类事件再次发生需要做什么？

——为提高检测此类事件的能力需要做什么？

e） 一般性问题：

——有多少事件响应小组成员将参与处理此事件？

——除了事件响应小组外，在组织内还有什么团体或者个人将参与处理此事件？

——小组将把事件报告给哪一外部参与方？每份报告什么时候出？每份报告将怎么做？

——在处理此事件时小组使用什么工具和资源？

——事件发生在不同日期和时间，处理的方式有何不同？

——如果事件发生在不同物理地点，处理方式有何不同？

A.3 案例

A.3.1 案例 1:蠕虫和 DDoS 代理入侵

在一个星期二早晨,一种新蠕虫被公布在互联网上。蠕虫利用两周前公开发布的 Microsoft Windows 漏洞,并且相关补丁已经发布。蠕虫通过两种方式传播:a)通过电子邮件将自身发送到能找到的受感染主机的所有地址;b)找寻打开文件共享的主机并发送自身到该主机。蠕虫为它发送的每份副本生成不同的附件名;每个附件随机生成文件名,文件名使用的是超过十几个文件扩展名中的其中一个。蠕虫也会从超过 100 个的电子邮件主题中去选择并找寻类似数量的电子邮件主体。当蠕虫感染主机时,它会获得管理权并尝试使用文件传输协议从不同 IP 地址下载 DDoS 代理(提供代理的 IP 地址数量是未知的)。虽然防病毒软件供应商会很快发出对这种蠕虫的告警,但在任何供应商发布特征库之前它传播非常迅速。在蠕虫开始传播后三小时,在防病毒特征库可用之前,组织已经被广泛感染。

下面是为此案例设置的附加问题:

a) 事件响应小组如何识别所有受感染主机?
b) 在病毒特征库发布之前组织如何去防止蠕虫进入组织?
c) 在病毒特征库发布之前组织如何去防止蠕虫由受感染主机传播?
d) 组织将会给所有易受攻击的机器打补丁吗?该怎么做?
e) 如果已经受到 DDoS 攻击的受感染主机在第二天早晨被配置去攻击另一组织的网站,将怎样去应对这一事件的变化?
f) 事件响应小组将怎样让用户知道事件的状态?如果因为蠕虫而使电子邮件服务超负荷或者不能用该怎么办?
g) 如果有的话,小组将使用什么其他措施去照看目前没有连接到网络的主机(比如旅途中的员工、偶尔拨号的外部雇员)?

A.3.2 案例 2:外部 DDoS 攻击

在一个星期日晚上,组织的网络入侵检测系统检测到大量 ping 包,并发出可疑外部 DDoS 告警。虽然事件处理人员不能确定这个告警是否正确,但他们确认此告警不和任何已知的误报相匹配。因为 DDoS 活动使用欺骗性的源 IP 地址,所以确定组织内哪一台或者哪些主机在进行此项活动需要花费相当多的时间和精力;与此同时,DDoS 活动仍在继续。调查结果显示,7 台服务器大概率生成 DDoS 通讯。

下面是此案例的附加问题:

a) 小组将怎样确认组织内哪台主机在产生此通讯量?其他哪一小组可以协助事件响应小组?
b) 在确认产生此通讯量的服务器后,小组将怎样推断出是否服务器受到恶意软件感染?

A.3.3 案例 3:远程办公安全

在一个星期六晚上,网络入侵检测软件记录到了一些来自内部的探测和扫描。一些服务器的主机入侵检测软件也记录了一些探测与扫描。入侵检测分析师断定这些内部 IP 属于这个组织的 VPN 服务器,并且联系了事件响应小组。事件响应小组查看了入侵检测记录、防火墙、VPN 服务器日志,并确定了发动攻击的外部 IP 地址,被授权的用户 ID 和相应的用户名。

下面是此案例的附加问题:

a) 假设该用户的个人电脑已经被下载的游戏中包含的木马所感染。这将怎样影响事件的处

理呢？

b） 假设该用户的个人电脑已经被一个网络服务蠕虫所感染。这将怎样影响事件的处理呢？

A.3.4 案例 4：应用程序崩溃

在一个星期一上午，该组织的咨询服务部门收到三个用户的求助，他们的电子表格应用程序在使用过程中反复崩溃。接下来，更多其他用户也反映了类似的问题。大部分的用户属于同一组或相关的组。

下面是此案例的附加问题：

a） 什么恶意软件导致了电子表格应用程序的崩溃？

b） 为了确定崩溃是恶意软件引起的需要采取哪些步骤？

A.3.5 案例 5：恶意移动代码

在一个星期五下午，几名用户联系咨询服务部门，报告陌生的弹出式窗口以及在其网络浏览器中出现的陌生工具栏。这些用户的描述很相似，因此咨询服务部门代理商认为，用户的系统被同样的东西影响，而且最可能的原因是基于 Web 的恶意移动代码。

下面是此案例的附加问题：

a） 事件响应小组如何确定什么漏洞或配置导致这种恶意代码感染系统？

b） 事件响应小组如何确定这些恶意移动代码来自哪些网站？

A.3.6 案例 6：混合恶意软件攻击

某组织采用了一个新的即时通讯平台后不久，其使用者就受到广泛的恶意软件的攻击，此恶意软件是通过使用即时消息来传播的。从安全管理员的初步报告来看，攻击似乎是由蠕虫引起的。然而后来的报告表明这种攻击也涉及 Web 服务器和 Web 客户端。即时通讯和基于网络的攻击看起来与蠕虫有关，因为它们显示相同的信息给使用者。

下面是此案例的附加问题：

a） 由于恶意软件更像是一个混合型的攻击，那么与处理蠕虫不同，需要采取什么样的响应措施呢？

b） 组织首先控制哪种攻击向量呢？为什么？

A.3.7 案例 7：物联网恶意软件攻击

某互联网公司安全研究团队发现攻击者利用恶意软件 VPNFilter 感染了全球 54 个国家的超过 50 万台设备，品牌包括占据全球通信设备市场份额排名前几位的多家知名企业。攻击者通过被感染的路由器，向网络注入恶意负载，甚至能悄悄修改网站发送的内容。

下面是此案例的附加问题：

a） IoT 设备爆出新的漏洞，事件响应小组应采取什么措施？

b） 遇到类似事件，如何应对？

A.3.8 案例 8：通过云计算平台传播勒索软件

客户不经意通过云计算平台传播了勒索软件，招聘人员通过电子邮件接收到的简历文件感染了勒

索病毒，但该文件随后被转移到自动与云计算平台同步的文件夹，该文件通过云转发到组织内其他用户。在该简历文件被用户打开后，勒索软件会执行并加密每个设备或系统。它不只是感染最初的用户，还会快速蔓延到其他连接到云同步服务的用户和终端。导致用户的大量主机、服务器被加密、业务系统瘫痪。

下面是此案例的附加问题：

a) 遇到类似事件，事件响应小组应采取什么措施？

b) 如何阻止恶意软件进入云服务？

c) 如何阻止恶意软件在云计算平台内无限制地传播而进入云服务？

A.3.9 案例 9：勒索软件的处理

2018 年 2 月，某三甲医院遭遇勒索病毒攻击，全院所有的医疗系统均无法正常使用，正常就医秩序受到严重影响；同年 8 月，某半导体制造公司的三处重要生产基地，均因勒索病毒入侵导致生产停摆。

此案例的附加问题为：当业务系统出现无法访问、生产线停产等现象时，是否能 100％确定是服务器感染了勒索病毒？

附 录 B
（资料性）
遏制恶意软件常用技术

本附录总结了各种能有效遏制恶意软件事件的常用技术，提供了每种技术在应对不同类型恶意软件和攻击工具时的效果。为了便于描述，表 B.1 将各种环境分为两大类（可控环境和不可控环境），将各种威胁分为两大类（简单和复杂）。

a） 可控环境。指一个或多个关键群体可以控制整个组织内的服务器和工作站的操作系统以及应用程序配置。这使得在最初部署系统和提供支持、维护时，能够有效实施安全措施，并且使得组织内部能够保持一个持续的安全态势。

b） 不可控环境。指系统所有者和用户只能控制各自的系统，通常使用的是管理员权限。尽管系统最初可能使用组织的标准配置，但系统所有者和用户可以更改该配置，这将减弱其安全性。

c） 简单威胁。简单威胁只拥有几个简单的特征。例如，某个大规模邮件蠕虫只是使用固定的主题并且附件名只有三个固定的名称，那么这个蠕虫就是一个简单的威胁。如果一个后门只使用一个固定端口号并且只和固定 IP 地址通信，这个后门也算是一个简单威胁。

d） 复杂威胁。复杂威胁可能有成百上千种特征；有些复杂的威胁甚至会随即产生一些特征。例如，某大规模邮件蠕虫使用 50 个主题和 50 个文件名，并随机产生发送者地址、邮件内容和附件大小。还有一个例子是恶意移动代码，该代码从一个巨大的列表中选择 IP 地址并下载其负载。比起简单威胁，复杂威胁通常更难遏制。表 B.1 提供的是在可控环境中处理简单威胁的向导。

表 B.1 不同环境下遏制技术的效果对比

技术	简单威胁，可控环境	不可控环境下的显著差异	复杂威胁的显著差异
安全工具			
区域边界防病毒设备	能够非常有效地阻止所有企图通过网络监控点（例如网络防火墙）的已知类型恶意软件；能有效阻止一些未知恶意软件	—	—
防病毒软件	能非常有效地阻止企图感染主机的已知类型恶意软件（例如，个人电脑、服务器）；能有效阻止一些未知类型恶意软件	因为一些主机可能使用了过期的、配置错误、或功能被禁止的防病毒软件，或者没有安装防病毒软件	—
恶意软件专杀工具（通常基于主机）	能非常有效地阻止企图感染主机（例如，个人电脑、服务器）的已知特定类型恶意软件；能有效阻止一些未知类型恶意软件	因为一些主机可能使用了过期的、配置错误、或功能被禁止的防病毒软件，或者没有安装防病毒软件	—
网络入侵防御系统	能有效阻止大部分企图通过网络监控点（例如 IPS）的已知类型蠕虫；某些情况下，可以有效阻止未知蠕虫；能有效识别和阻止使用后门	—	检测准确率很低，如果威胁具有随机特征，通常无法有效检测

表 B.1　不同环境下遏制技术的效果对比（续）

技术	简单威胁，可控环境	不可控环境下的显著差异	复杂威胁的显著差异
终端安全软件	有时能有效阻止企图攻击主机的已知和未知恶意软件（例如，个人电脑，服务器）；能有效检测出企图更改关键系统文件的恶意软件	主机可能使用过期、配置错误、或功能被禁止的防病毒软件，或者没有安装防病毒软件；如果软件配置错误，也会降低检测的准确性	检测准确率很低
基于网络的垃圾邮件过滤	能够非常有效地阻止利用邮件传播的已知恶意软件	—	检测准确率很低，如果威胁具有随机特征，通常无法有效检测
基于主机的垃圾邮件过滤	能够非常有效地阻止利用邮件传播的已知恶意软件	效率不高，因为一些主机可能使用了过期的、配置错误、或功能被禁止的防病毒软件，或者没有安装防病毒软件	检测准确率很低，如果威胁具有随机特征，通常无法有效检测
基于网络的 Web 内容过滤	能有效阻止基于 Web 的已知恶意软件	—	通常效率较低，因为检测准确率很低
基于主机的 Web 内容过滤	能有效阻止基于 Web 的已知恶意软件	效率不高，因为一些主机可能使用了过期的、配置错误、或功能被禁止的防病毒软件，或者没有安装防病毒软件	通常效率较低，因为检测准确率很低
网络配置更改			
网络防火墙	可以阻止通过固定端口传播的蠕虫进入或离开网络；可以有效阻止对服务和主机的访问，能有效预防非授权主机产生的邮件离开组织的网络，能有效阻止主机访问恶意软件产生的攻击者 IP 地址，同时阻止攻击者 IP 地址对该网络的访问	—	如果需要阻止的攻击者 IP 地址太多，效率可能会受影响
终端安全软件	能非常有效地预防网络服务蠕虫感染主机（例如，工作站、服务器）；能有效预防被感染主机产生的边界活动离开主机（例如，后门、按键记录器、浏览器活动、邮件生成器）	效率不高，因为一些主机可能使用了过期的、配置错误、或功能被禁止的防病毒软件，或者没有安装防病毒软件	—
互联网边界路由器	可以有效预防利用网络服务传播的蠕虫进入组织的网络；能有效阻止主机访问恶意软件（例如，后门、恶意移动代码、按键记录器、恶意浏览器插件）产生的攻击者 IP 地址，同时阻止攻击者 IP 地址对该网络的访问	—	如果需要阻止的攻击者 IP 地址太多，效率可能会受影响

表 B.1　不同环境下遏制技术的效果对比（续）

技术	简单威胁，可控环境	不可控环境下的显著差异	复杂威胁的显著差异
内部路由器	可以有效预防利用网络服务的蠕虫进入组织的网络；能有效阻止访问主机恶意软件产生的攻击者 IP 地址，同时阻止攻击者 IP 地址对该网络的访问；能有效阻止被感染主机产生的邮件发送活动	—	如果需要阻止的攻击者 IP 地址太多，效率可能会受影响
主机配置更改			
主机加固（包括安装补丁）	能有效阻止利用主机漏洞或不安全设置的恶意软件产生的额外感染	效率低下，因为很多主机没有打补丁或没有适当加固	—
邮件服务器设置（例如阻止邮件附件）	能有效阻止基于邮件的恶意软件使用组织的邮件服务	—	通常效率低，因为检测准确率低，如果威胁具有随机性特征，通常无法检测
组织服务器上其他服务的设置	有时可以有效阻止网络服务蠕虫	—	通常效率低，因为检测准确率低，如果威胁具有随机性特征，通常无法检测
应用程序客户端设置（例如，限制邮件客户端和浏览器中的移动代码执行）	能有效阻止特定的恶意软件	效率有限，因为用户需要完成某些设置（例如，手动更改设置，运行分发的工具或脚本）	—

表 B.2 和表 B.3 总结了表 B.1 的信息，指出了可控环境下，每种技术针对简单威胁（表 B.2）和复杂威胁（表 B.3）的效率。H 表示高效率；M 表示效率一般；L 表示低效率。

表 B.2　可控环境下对简单威胁的遏制效率

技术	恶意软件类型										
	复合型病毒	宏病毒	网络服务蠕虫	大规模邮件蠕虫	木马	恶意移动代码	后门	按键记录器	Rootkit	恶意浏览器插件	邮件生成器
安全工具											
区域边界防病毒设备	H	H	H	H	H	H	H	H	H	H	H
防病毒软件	H	H	H	H	H	H	H	H	H	H	H
恶意软件专杀工具					H	H				H	
网络入侵防御系统			M	M			L				
终端安全软件			L		M	L	L	L	M	L	L

表 B.2　可控环境下对简单威胁的遏制效率（续）

技术	恶意软件类型										
	复合型病毒	宏病毒	网络服务蠕虫	大规模邮件蠕虫	木马	恶意移动代码	后门	按键记录器	Rootkit	恶意浏览器插件	邮件生成器
基于网络的垃圾邮件过滤系统				H	L	M					H
基于主机的垃圾邮件过滤系统				H	L	M					H
基于网络的 Web 内容过滤系统					L	M				M	
基于主机的 Web 内容过滤系统					L	M				M	
网络配置更改											
网络防火墙			H	M		M	M	M		M	M
终端安全软件			H			M	M	M		M	M
互联网边界路由器			H			M	M	M		M	
内部路由器			H			M	M	M		M	L
主机配置更改											
主机加固（包括安装补丁）	L	L	M	M	M	M					
邮件服务器设置（例如，组织邮件附件）	L	L		H	M	M					H
设置组织服务器提供的其他服务			L-M								
应用程序客户端设置（例如，限制邮件客户端或浏览器执行恶意代码、限制在 word 处理器中使用宏）		M	M		M					M	

表 B.3　可控环境下对复杂威胁的遏制效率

技术	恶意软件类型										
	复合型病毒	宏病毒	网络服务蠕虫	大规模邮件蠕虫	木马	恶意移动代码	后门	按键记录器	Rootkit	恶意浏览器插件	邮件生成器
安全工具											
区域边界防病毒设备	H	H	H	H	H	H	H	H	H	H	H
防病毒软件	H	H	H	H	H	H	H	H	H	H	H
恶意软件专杀工具					H	H				H	
网络入侵防御系统			L	L			L				
终端安全软件			L		L	L	L	L	L	L	L

表 B.3　可控环境下对复杂威胁的遏制效率（续）

技术	恶意软件类型										
	复合型病毒	宏病毒	网络服务蠕虫	大规模邮件蠕虫	木马	恶意移动代码	后门	按键记录器	Rootkit	恶意浏览器插件	邮件生成器
基于网络的垃圾邮件过滤系统				L-M	L	L					L-M
基于主机的垃圾邮件过滤系统				L-M	L	L					L-M
基于网络的 Web 内容过滤系统					L	L				L	
基于主机的 Web 内容过滤系统					L	L				L	
网络配置更改											
网络防火墙			H	M		M	L-M	L-M		L-M	L-M
终端安全软件			H			M	M	M		M	M
互联网边界路由器			H			M	L-M	L-M		L-M	
内部路由器			H			M	L-M	L-M		L-M	L
主机配置更改											
主机加固(包括安装补丁)	L	L	M	M	M	M					
邮件服务器设置(例如,组织邮件附件)	L	L		L-M	L	L					L-M
设置组织服务器提供的其他服务			L-M								
应用程序客户端设置(例如,限制邮件客户端或浏览器执行恶意代码,限制在 word 处理器中使用宏)		M	M			M				M	

参 考 文 献

[1] GB/T 20275—2013 信息安全技术 网络入侵检测系统技术要求和测试评价方法

[2] GB/T 24363—2009 信息安全技术 信息安全应急响应计划规范

[3] GB/T 31499—2015 信息安全技术 统一威胁管理产品技术要求和测试评价方法

[4] ISO/IEC 27032:2012 Information technology—Security techniques—Guidelines for cybersecurity

[5] ISO/IEC 27033-1:2015 Information technology—Security techniques—Network security —Part 1: Overview and concepts

[6] NIST SP 800-28 Version 2:2008 Guidelines on Active Content and Mobile Code

[7] NIST SP 800-40 Rev.3:2013 Guide to Enterprise Patch Management Technologies

[8] NIST SP 800-61 Rev.2:2012 Computer Security Incident Handling Guide

[9] NIST SP 800-70 Rev.4:2018 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

[10] NIST SP 800-83 Version 1:2005 Guide to Malware Incident Prevention and Handling

[11] NIST SP 800-83 Rev.1:2013 Guide to Malware Incident Prevention and Handling for Desktops and Laptops