# 安全事件周报

## 安全事件周报 (04.12-4.18)



360CERT
北京奇虎科技有限公司 | 2021-04-19

# 报告信息

| | | | |
|---|---|---|---|
| 报告名称 | 安全事件周报（04.12-4.18） | | |
| 报告类型 | 安全事件周报 | 报告编号 | B6-2021-041901 |
| 报告版本 | 1.0 | 报告日期 | 2021-04-19 |
| 报告作者 | 360CERT | 联系方式 | cert@360.cn |
| 提供方 | 北京奇虎科技有限公司 | | |
| 接收方 | | | |

# 报告修订记录

| 报告版本 | 日期 | 修订 | 审核 | 描述 |
|---|---|---|---|---|
| 1.0 | 2021-04-19 | 360CERT | 360CERT | 撰写报告 |

# 目录

# 一、 事件概览


本周收录安全事件 19 项

话题集中在`恶意软件`、`漏洞信息`方面，涉及的组织有：`伊朗核电站`、`Valve`、`HUAWEI`、`Chrome`等。多个严重漏洞曝光，各厂商注意及时修复。

对此，360CERT 建议：

1. 使用 360 安全卫士进行病毒检测、
2. 使用 360 安全分析响应平台进行威胁流量检测，
3. 使用 360 城市级网络安全监测服务 QUAKE 进行资产测绘，
4. 做好资产自查以及预防工作，以免遭受黑客攻击。

# 二、 事件档案

| **恶意程序** | **等级** |
| --- | --- |
| 勒索软件的发展影响了法医学分析 | ★★★★ |
| BRATA 恶意软件冒充 Android 安全扫描程序 | ★★★★ |
| 50 万华为用户感染了 Joker Android 恶意软件 | ★★★★ |
| 新的 Linux，macOS 恶意软件隐藏在假冒的 Browserify NPM 包中 | ★★★★ |
| Capcom 勒索事件攻击报告 | ★★★★ |
| 黑客通过网站联系表格来传递 IcedID 恶意软件 | ★★★★ |
| 休斯顿火箭队调查勒索软件攻击 | ★★★★ |
| Monero 加密货币活动利用 ProxyLogon 缺陷 | ★★★★ |
| **网络攻击** | **等级** |
| 伊朗核电站遭遇网络攻击 | ★★★★ |
| 美国和英国指责俄罗斯情报部门黑客发动重大网络攻击 | ★★★★ |
| **其他事件** | **等级** |
| Valve 游戏引擎漏洞影响多个旗下游戏 | ★★★★ |
| NAME:WRECK DNS 漏洞影响超过 1 亿台设备 | ★★★★ |
| 美国国家安全局发现了影响 Microsoft Exchange 服务器的新漏洞 | ★★★★ |
| 研究人员发布 Chrome，Edge，Brave，Opera 的 0day POC | ★★★★ |
| 第二个 Chrome 0day 漏洞在 twitter 上被删除 | ★★★★ |
| SAP 修复了 Business Client、Commerce 和 NetWeaver 中的漏洞 | ★★★★ |
| 美国因 SolarWinds 网络攻击制裁俄罗斯并驱逐 10 名外交官 | ★★★★ |
| 未修补的 MS Exchange 服务器受到加密劫持恶意软件攻击 | ★★★★ |
| 工业系统以太网/IP 堆栈中报告严重错误 | ★★★★ |

# 三、 事件详情

## (一) 恶意程序

### 勒索软件的发展影响了法医学分析

日期: 2021-04-12

等级: 高

来源: Bradley Barth

标签: ['the Active Directory', 'Orrick']

网络安全界密切关注勒索组织在过去一年中不断升级的商业策略，包括双重勒索、组成卡特尔和直接联系受害者。但是，不能忽视一些新的工具和技术战略，这些新的工具和技术战略是最近为阻碍和复杂化法医调查而增加的。Palo Alto 公司 Crypsis 集团副总裁布雷特·帕德雷斯（Bret Padres）指出，在虚拟机上设置 Active Directory 和域控制器的情况下，攻击者会对虚拟机环境进行整体加密，这将进一步减缓法医学分析的速度。

详情

Ransomware's evolving tools & technical tactics confuse forensic analysis

https://www.scmagazine.com/home/security-news/ransomware/ransomwares-evolving-tools-and-technical-tactics-confuse-forensic-analysis/

### BRATA 恶意软件冒充 Android 安全扫描程序

日期: 2021-04-12

等级: 高

来源: The Hacker News

标签: ['Android', 'BRATA']

BRATA（Brazilian Remote Access Tool Android）最开始是一个具有屏幕记录功能的巴西恶意软件，之后逐渐演变成银行特洛伊木马。近期，它被发现冒充官方游戏商店的安全扫描程序，分发一个能够收集敏感信息的后门。这些有争议的应用程序是针对巴西、西班牙和美国的用户设计的，其中大多数应用程序的安装量在 1000 到 5000 次之间。另一款名为 DefenseScreen 的应用程序在去年从 Play Store 中被删除之前，已经安装了 10000 次。

详情

BRATA Malware Poses as Android Security Scanners on Google Play Store

https://thehackernews.com/2021/04/brata-malware-poses-as-android-security.html

### 50 万华为用户感染了 Joker Android 恶意软件

日期: 2021-04-13

等级: 高

来源: BALAJI N

标签: ['Joker Android Malware', 'Android', 'Huawei']

Doctor Web 的分析师宣称，他们最近在华为设备的官方应用商店 AppGallery 中发现了 Joker Android 恶意软件，该恶意软件被认定为 Android 多功能木马。Joker 家族会诱骗

Android 用户为其所有的移动服务付费，据报道，超过 50 万的华为智能手机用户从该公司的官方 Android 商店下载了受感染的应用程序。

详情

500,000 Huawei Users Infected with Joker Android Malware

https://gbhackers.com/500000-huawei-users-infected-with-joker-android-malware/

## 新的 Linux，macOS 恶意软件隐藏在假冒的 Browserify NPM 包中

日期: 2021-04-13

等级: 高

来源: Ax Sharma

标签: ['Linux', 'macOS', 'npm']

在 npm 注册中心发现了一个新的恶意软件包，目标是使用 Linux 和 applemacos 操作系统的 NodeJS 开发者。这个恶意软件包被称为"webbrowserify"，它模仿了流行的 browserify npm 组件，此外，到目前为止，该组件中包含的 ELF 恶意软件在所有主流杀毒引擎中的检测率均为零。

详情

New Linux, macOS malware hidden in fake Browserify NPM package

https://www.bleepingcomputer.com/news/security/new-linux-macos-malware-hidden-in-fake-browserify-npm-package/

## Capcom 勒索事件攻击报告

日期: 2021-04-13

等级: 高

来源: Ionut Ilascu

标签: ['Capcom', 'Ragnar Locker', 'VPN']

CapCom 是日本电视游戏软件公司，旗下有《街头霸王》、《洛克人》、《生化危机》等有名气的作品。该公司在 2020 年 11 月遭遇 Ragnar Locker 勒索病毒攻击，被窃取 1TB 敏感数据，并被索要 1100 万美元作为赎金，该公司一直都未曾主动联系过黑客协商赎金支付问题，其数据也在被勒索的几周后被泄露。
近日，该公司宣布，经过研究人员对网络设备的分析调查，此次攻击事件黑客是通过攻击 Capcom 位于北美加州子公司的一个旧 VPN 备份进入了 Capcom 的内部。2020 年 11 月 1 日，攻击者从该设备转向美国和日本办公设备。

对数据泄露的最终评估为 15649 人将受到该事件影响，涉及到的数据包括姓名、地址、电话号码、电子邮件地址等公司和个人数据。

详情

Capcom: Ransomware gang used old VPN device to breach the network

https://www.bleepingcomputer.com/news/security/capcom-ransomware-gang-used-old-vpn-device-to-breach-the-network/

## 黑客通过网站联系表格来传递 IcedID 恶意软件

日期: 2021-04-14

等级: 高

来源: BALAJI N

标签: ['Microsoft', 'IcedID']

微软的安全研究人员最近发现，黑客不断滥用合法的公司联系表格发送钓鱼电子邮件，这样黑客就可以通过合法的诉讼威胁目标企业，不仅如此，黑客还试图通过 IcedID 信息窃取恶意软件影响目标企业。

详情

Hackers Abuse Website Contact forms to Deliver IcedID Malware

https://gbhackers.com/icedid-malware/

## 休斯顿火箭队调查勒索软件攻击

日期: 2021-04-16

等级: 高

来源: Doug Olenick

标签: ['NBA', 'Houston Rockets']

NBA 休斯顿火箭队报道称，他们最近遭到勒索软件攻击，巴布克网络团伙为此承担了责任。巴布克团伙在其勒索网站上的一篇现已被删除的帖子中，放置了一张据称已从火箭队网络中删除的纸条和文件。该团伙声称已经删除了 500GB 的数据，包括第三方合同以及公司、客户、员工和财务信息。巴布克的报告说："公布这些信息可能会导致法律问题，并引起客户的担忧。"。

详情

Houston Rockets Investigate Ransomware Attack

https://www.databreachtoday.com/houston-rockets-investigate-ransomware-attack-a-16415

## Monero 加密货币活动利用 ProxyLogon 缺陷

日期: 2021-04-18

等级: 高

来源: Pierluigi Paganini

标签: ['ProxyLogon', 'Microsoft Exchange', 'Monero']

Sophos 研究人员报告说，攻击者利用 ProxyLogon 漏洞，攻击 Exchange 服务器并部署恶意 Monero cryptominer。攻击始于 PowerShell 命令，该命令从另一台受感染服务器的 Outlook Web Access 登录路径（/owa / auth）检索名为 win_r.zip 的文件。然后该脚本调用 Windows 内置的 certutil.exe 程序来下载另外两个文件，即 win_s.zip 和 win_d.zip，之后下放病毒。

详情

Monero Cryptocurrency campaign exploits ProxyLogon flaws

https://securityaffairs.co/wordpress/116955/cyber-crime/proxylogon-flaws-cryptocurrencyminer.html

## 相关安全建议

1. 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
2. 做好资产收集整理工作，关闭不必要且有风险的外网端口和服务，及时发现外网问题
3. 条件允许的情况下，设置主机访问白名单
4. 及时对系统及各个服务组件进行版本升级和补丁更新
5. 包括浏览器、邮件客户端、vpn、远程桌面等在内的个人应用程序，应及时更新到最新版本
6. 各主机安装 EDR 产品，及时检测威胁

# (二) 网络攻击

## 伊朗核电站遭遇网络攻击

日期: 2021-04-12

等级: 高

来源: Prajeet Nair

标签: ['Israeli', 'Iranian']

以色列公共媒体《菅直人报》援引情报人士的话称，以色列政府发动的网络攻击导致伊朗一座核电站关闭，伊朗称这是"蓄意破坏"的行为，此次攻击拖延了伊朗浓缩提炼铀进度。

详情

Iranian Nuclear Site Shut Down by Apparent Cyberattack

https://www.databreachtoday.com/iranian-nuclear-site-shut-down-by-apparent-cyberattack-a-16382

## 美国和英国指责俄罗斯情报部门黑客发动重大网络攻击

日期: 2021-04-15

等级: 高

来源: Danny Palmer

标签: ['Russian', 'SolarWinds']

据美国和英国称，为俄罗斯对外情报局工作的黑客是太阳风攻击、针对 Covid-19 研究设施等的网络间谍活动的幕后黑手。美国的指控来自国家安全局（NSA）、网络安全和基础设施安全局（CISA）和联邦调查局（FBI）的联合咨询，其中还描述了俄罗斯对外情报局（SVR）正在利用 VPN 服务中的五个众所周知的漏洞。英国也将这些袭击归咎于俄罗斯情报部门。

详情

SolarWinds: US and UK blame Russian intelligence service hackers for major cyber attack

https://www.zdnet.com/article/solarwinds-us-and-uk-blame-russian-intelligence-service-hackers-for-major-cyber-attack/

## 相关安全建议

1. 积极开展外网渗透测试工作，提前发现系统问题
2. 及时对系统及各个服务组件进行版本升级和补丁更新
3. 包括浏览器、邮件客户端、vpn、远程桌面等在内的个人应用程序，应及时更新到最新版本
4. 注重内部员工安全培训

# (三) 其他事件

## Valve 游戏引擎漏洞影响多个旗下游戏

日期: 2021-04-12

等级: 高

来源: Ionut Ilascu

标签: ['CS:GO', 'RCE', 'HackerOne']

一组被称为秘密俱乐部的安全研究人员在 Twitter 上报告了 Valve 开发的源 3D 游戏引擎中的远程代码执行漏洞，该引擎用于构建拥有数千万玩家的游戏。由于该漏洞存在于游戏引擎中，因此所有使用源代码构建的产品都会受到影响，并且需要一个补丁来消除对用户的风险。该组织的一名研究人员说，他们大约两年前就披露了其脆弱性，但它仍然影响着《反击：全球进攻》（CS:GO）的最新版本。

详情

CS:GO, Valve Source games vulnerable to hacking using Steam invites

https://www.bleepingcomputer.com/news/security/cs-go-valve-source-games-vulnerable-to-hacking-using-steam-invites/

## NAME:WRECK DNS 漏洞影响超过 1 亿台设备

日期: 2021-04-13

等级: 高

来源: Ionut Ilascu

标签: ['TCP/IP', 'NAME:WRECK', 'Siemens', 'DNS']

2021 年 4 月 13 日，安全研究人员披露了九个漏洞，这些漏洞影响在至少 1 亿个设备上运行的 TCP / IP 网络通信堆栈中的域名系统协议的实现。主要为以下设备
- FreeBSD（漏洞版本：12.1）：BSD 系列中最流行的操作系统之一
- IPnet（漏洞版本：VxWorks 6.6）：由 Interpeak 最初开发，由 WindRiver 维护，并由 VxWorks 实时操作系统（RTOS）使用
- NetX（漏洞版本：6.0.1）：是 ThreadX RTOS 的一部分，是 Microsoft 维护的一个开源项目，名称为 Azure RTOS NetX
- Nucleus NET（漏洞版本：4.3）：由西门子业务 Mentor Graphics 维护的 Nucleus RTOS 的一部分，用于医疗，工业，消费类，航空航天和物联网设备

详情

NAME:WRECK DNS bugs affect over 100 million devices

https://www.bleepingcomputer.com/news/security/name-wreck-dns-bugs-affect-over-100-million-devices/

## 美国国家安全局发现了影响 Microsoft Exchange 服务器的新漏洞

日期: 2021-04-13

等级: 高

来源: The Hacker News

标签: ['Microsoft', 'NAS']

在 4 月份发布的一系列修补程序中，微软针对总共 114 个安全漏洞推出了修补程序，其中包括一个被积极利用的 0day 漏洞和 Exchange 服务器中的四个远程代码执行漏洞。在 114 个安全漏洞中，19 个被评为严重，88 个被评为高危，1 个被评为中危。其中最主要的是 CVE-2021-28310，这是 Win32k 中的一个权限提升漏洞，据说该漏洞正受到攻击，攻击者可以通过在目标系统上运行恶意代码来提升权限。

详情

NSA Discovers New Vulnerabilities Affecting Microsoft Exchange Servers

https://thehackernews.com/2021/04/nsa-discovers-new-vulnerabilities.html

## 研究人员发布 Chrome，Edge，Brave，Opera 的 0day POC

日期: 2021-04-13

等级: 高

来源: Deeba Ahmed

标签: ['POC', 'Chromium']

印度一名安全研究人员 Rajvardhan Agarwal 发布了一个 PoC，该漏洞主要影响 web 浏览器。它是 v8javascript 中的一个远程代码执行漏洞，影响除 Chrome 之外的所有 Chromium 浏览器，如 MS-Edge、Brave 和 Opera。这个漏洞在 Pwn2Own 2021 黑客竞赛中被证明，最初是由来自 Dataflow Security 的 Bruno Keith 和 Niklas Baumstark 发现的。两人因利用这个漏洞在 Chrome 和 Edge 上运行恶意代码而获得 10 万美元的奖金。

详情

Researcher release PoC exploit for 0-day in Chrome, Edge, Brave, Opera

https://www.hackread.com/poc-exploit-for-0-day-chrome-edge-brave-opera/

## 第二个 Chrome 0day 漏洞在 twitter 上被删除

日期: 2021-04-14

等级: 高

来源: Lawrence Abrams

标签: ['Twitter', 'Google Chrome', 'Microsoft Edge']

Twitter 上发布了第二个 chromiumzero-day 远程代码执行漏洞，该漏洞会影响当前版本的 googlechrome、microsoftedge，以及其他可能基于 Chromium 的浏览器。一位名为 frust 的安全研究人员在 Twitter 上发布了一个 PoC 漏洞，该漏洞是基于 Chromium 的 0day 漏洞，导致 Windows 记事本应用程序打开。frust 的远程代码执行漏洞也无法逃脱 Chromium 的沙盒安全功能。Chromium 的沙盒是一种安全特性，可以防止攻击者在主机

上执行代码或访问文件。除非攻击者使用未修补的沙盒逃逸漏洞将新的 0day 漏洞连接起来，否则处于当前状态的新 0day 漏洞不会伤害用户，除非用户禁用沙盒。

详情

Second Google Chrome zero-day exploit dropped on twitter this week

https://www.bleepingcomputer.com/news/security/second-google-chrome-zero-day-exploit-dropped-on-twitter-this-week/

## SAP 修复了 Business Client、Commerce 和 NetWeaver 中的漏洞

日期: 2021-04-14

等级: 高

来源: Ionut Ilascu

标签: ['SAP', 'Business Client', 'CVE']

SAP 的安全更新解决了多个漏洞。其中最严重的影响该公司的业务客户产品。该公司的另外两款产品更新了针对严重漏洞的修补程序，这些漏洞允许未经授权的用户访问配置对象并允许远程代码执行。

详情

SAP fixes critical bugs in Business Client, Commerce, and NetWeaver

https://www.bleepingcomputer.com/news/security/sap-fixes-critical-bugs-in-business-client-commerce-and-netweaver/

## 美国因 SolarWinds 网络攻击制裁俄罗斯并驱逐 10 名外交官

日期: 2021-04-15

等级: 高

来源: The Hacker News

标签: ['US', 'SolarWinds', 'Russia', 'SVR']

美国和英国正式将 IT 基础设施管理公司 SolarWinds 的"供应链攻击"归因于为俄罗斯外国情报服务（SVR）工作的政府工作人员。英国政府在一份声明中说："无论是在网络空间、在选举中的干涉还是在情报部门的侵略行动中，俄罗斯在世界范围内的恶行模式都表明，对英国的国家和集体安全来说，俄罗斯仍然是最严重的威胁。"为此，美国财政部对俄罗斯实施了全面制裁，理由是俄罗斯"破坏了美国自由公正选举和民主体制的运作"，并对其在助长蔓延的 SolarWinds 黑客攻击方面发挥了作用，同时还禁止国内 6 家为俄罗斯情报部门运营的网络项目提供支持的科技公司。这些公司包括 ERA Technopolis、Pasit、联邦州自治科学机构科学研究所、专业安全计算设备和自动化（SVA）、Neobit、Advanced System Technology 和 Pozitiv Teknolodzhiz（积极技术），最后三家是 IT 安全公司，其客户包括俄罗斯情报机构。此外，拜登政府还驱逐了 10 名俄罗斯驻华盛顿外交使团成员，包括其情报部门的代表。

详情

US Sanctions Russia and Expels 10 Diplomats Over SolarWinds Cyberattack

https://thehackernews.com/2021/04/us-sanctions-russia-and-expels-10.html

## 未修补的 MS Exchange 服务器受到加密劫持恶意软件攻击

日期: 2021-04-15

等级: 高

来源: Waqas

标签: ['Sophos', 'Exchange', 'Microsoft']

根据 Sophos 网络安全研究人员的报告，黑客正在寻找易受攻击、未修补的 Microsoft Exchange 服务器，并在其上安装加密货币挖掘恶意软件。调查进一步显示，这一新发现的活动旨在秘密利用受损系统的处理能力牟利。

详情

Unpatched MS Exchange servers hit by cryptojacking malware
https://www.hackread.com/ms-exchange-servers-cryptojacking-malware/

## 工业系统以太网/IP 堆栈中报告严重错误

日期: 2021-04-16

等级: 高

来源: The Hacker News

标签: ['CISA', 'Claroty', 'Dos', 'CIP']

美国网络安全和基础设施安全局（CISA）发布警告称，开放式以太网/IP 协议栈中存在多个漏洞，可能使工业系统遭受拒绝服务（DoS）攻击、数据泄漏和远程代码执行。2021 年 2 月 10 日之前的所有版本都会受到影响。

详情

Severe Bugs Reported in EtherNet/IP Stack for Industrial Systems
https://thehackernews.com/2021/04/severe-bugs-reported-in-ethernetip.html

## 相关安全建议

1. 及时对系统及各个服务组件进行版本升级和补丁更新
2. 包括浏览器、邮件客户端、vpn、远程桌面等在内的个人应用程序，应及时更新到最新版本
3. 受到网络攻击之后，积极进行攻击痕迹、遗留文件信息等证据收集

# 四、 产品侧解决方案

## （一）360 网络空间测绘系统

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或(quake#360.cn)获取对应产品。


## （二）360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或(shaoyulong#360.cn)获取对应产品。

## （三）360 安全卫士

针对本次安全更新，Windows 用户可通过 360 安全卫士实现对应补丁安装，其他平台的用户可以根据修复建议列表中的产品更新版本对存在漏洞的产品进行更新。如有其他问题可联系相关产品负责人或（360safe-ent#360.cn）。

# 附录 A 事件等级说明

| 高 | |
|---|---|
| 星级 | ★★★★/★★★★★ |
| 评定标准 | 1. 事件影响面十分广泛，受关注度高<br>2. 事件涉及的漏洞等级为严重/高危<br>3. 事件涉及机密/重要/核心数据，<br>4. 事件涉及数据量巨大<br>5. 事件涉及大型/常用厂商与组件<br>6. 事件涉及金额数目庞大/相关受害者损失高<br>7. 已知/潜在受害者数量庞大<br>8. 与日常生活/工作联系紧密 |
| 修复建议 | 建议在 3 个工作日内采取相关安全措施，并做好资产自测及预防工作 |

| 中 | |
|---|---|
| 星级 | ★★/★★★ |
| 危害结果 | 1. 事件影响面一般，受关注度中等<br>2. 事件涉及的漏洞等级为中危<br>3. 事件涉及数据机密性/重要性一般，<br>4. 事件涉及数据量中等<br>5. 事件涉及小型/常用厂商与组件<br>6. 事件涉及金额数目中等/相关受害者损失一般<br>7. 已知/潜在受害者数量中等<br>8. 与日常生活/工作联系一般 |
| 修复建议 | 建议在 7 个工作日内采取相关安全措施，并做好资产自测及预防工作 |

| 低 |
|---|

| | |
|---|---|
| 星级 | ★ |
| 危害结果 | 1. 事件影响面局限，受关注度低<br>2. 事件涉及的漏洞等级为低危<br>3. 事件涉及数据机密性/重要性低，<br>4. 事件涉及数据量低<br>5. 事件涉及小型/非常用厂商与组件<br>6. 事件涉及金额数目少/相关受害者损失低<br>7. 已知/潜在受害者数量少<br>8. 与日常生活/工作联系较小 |
| 修复建议 | 建议在 12 个工作日内采取相关安全措施，并做好资产自测及预防工作 |

# 附录 B 事件类型说明

| 网络攻击事件 | |
|---|---|
| 描述：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终端设备实施攻击，并造成终端设备异常或对终端设备当前运行造成潜在危害的信息安全事件。 | |
| 网络扫描 | 对网络边界设备及终端进行批量信息探测，包括端口扫描、服务指纹探测、DNS 查询等 |
| 漏洞利用 | 黑客使用 0day 或 nday，对系统及服务进行攻击 |
| web 攻击 | 黑客使用网络攻击技术，对 web 服务进行测试，包括 sql 注入、XSS、远程命令执行、恶意程序上传等 |
| 爆破事件 | 对网络设备及终端进暴力枚举及爆破，比如弱口令爆破、数据库爆破，系统路径爆破等 |
| 社工攻击 | 通过发送欺骗性垃圾邮件，或对目标发送构造的恶意信息，意图引诱目标给出敏感信息或者控制目标系统的攻击 |
| DDos | 使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。 |

| 恶意程序事件 | |
|---|---|
| 描述：通过网络、便携式存储设备等途径散播的，故意对终端设备等造成隐私或机密数据外泄、系统损害、数据丢失等非使用预期故障及信息安全问题的程序 | |
| 后门攻击 | 利用软件系统、硬件系统设计过程中留下的后门或有害程序所设置的后门而对信息系统实施攻击的信息安全事件 |
| 勒索软件 | 勒索程序将受害者的电脑上锁，或系统性地加密受害者硬盘上的文件，并要求受害者缴纳赎金以取回对电脑的控制权 |
| 挖矿程序 | 程序占用终端设备资源进行虚拟货币赚取，导致服务器无法正常工作 |
| 僵尸网络 | 采用一种或多种传播手段，将大量主机感染 bot 程序（僵尸程序）病毒，从而在控制者和被感染主机之间所形成的可一对多控制的网络 |
| 蠕虫病毒 | 无须计算机使用者干预即可运行的独立程序，通过不停的取得网络中（存在漏洞的）计算机的部分或全部控制权来进行传播 |
| 其它病毒 | 除上述类别以外，其余未经许可，向终端设备植入的恶意程序 |

| 数据安全事件 | |
|---|---|
| 描述：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、窃取等而导致的信息安全事件 | |
| 信息篡改 | 指未经授权，将信息系统中的信息更换为攻击者所提供的信息，而导致的信息安全事件，比如网页篡改、网页暗链等 |
| 信息假冒 | 通过假冒他人信息系统收发信息而导致的信息安全事件 |
| 信息泄漏 | 因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者，而导致的信息安全事件 |
| 信息窃取 | 未经授权用户利用可能的技术手段，主动恶意获取信息系统中信息而导致的信息安全事件 |
| 信息丢失 | 指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失而导致的信息安全事件 |
| 信息内容 | 利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件 |
| 其它信息破坏事件 | 指不能被包含在以上类别之中的信息破坏事件 |

| 其它安全事件 | |
|---|---|
| 描述：除开上述安全事件类型之外的事件 | |
| 设备设施故障 | 由于信息系统自身故障或外围保障设施故障，而导致的信息安全事件，以及人为地使用非技术手段，有意或无意的造成信息系统破坏，而导致的信息安全事件 |
| 灾害性事件 | 指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。 |
| 其它事件 | 不能归类于上述事件的安全事件 |