安全事件周报

安全事件周报 (04.26-05.02)

360CERT
北京奇虎科技有限公司 | 2021-05-03

报告信息

报告名称	安全事件周报（04.26-05.02）		
报告类型	安全事件周报	报告编号	B6-2021-050601
报告版本	1.0	报告日期	2021-05-06
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	2021-05-06	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 13 项

话题集中在`恶意软件`、`数据泄露`方面，涉及的组织有：`Reverb`、`Apple`、`PHP SRC`等。黑客利用近期漏洞大肆攻击，各厂商注意防护

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**
RotaJakiro: Linux 秘密后门	★★★★★
FluBot 间谍软件遍布欧洲	★★★★
黑客利用 SonicWall 0Day 漏洞部署 FiveHands 勒索软件	★★★★
卡巴斯基发现了具有后门功能的中情局恶意软件	★★★★
云托管提供商瑞士云遭遇勒索软件攻击	★★★★
数据安全	**等级**
黑客曝光 2.5 亿美国户口记录	★★★★
Reverb 泄露音乐家个人信息	★★★★
150 万条与政府有关的电子邮件记录遭遇泄露	★★★★
网络攻击	**等级**
黑客利用 0day 漏洞攻击 MacOS 计算机	★★★★★
First Horizon 银行在线帐户被黑客窃取客户资金	★★★★
其他事件	**等级**
一个新的 PHP Composer 漏洞可能导致广泛的供应链攻击	★★★★★
Apple 修补了 macOS Gatekeeper 被绕过的漏洞	★★★★
F5 BIG-IP 易受 Kerberos KDC 欺骗漏洞攻击	★★★★

三、 事件详情

(一) 恶意程序

RotaJakiro: Linux 秘密后门

日期: 2021-04-29

等级: 高

来源: Netlab

标签: ['Linux', 'Backdoor', 'RotaJakiro']

360 NETLAB 的 BotMon 系统标记了具有 0 VT 检测的可疑 ELF 文件（MD5 = 64f6cfe44ba08b0babdd3904233c4857），该文件与 TCP 443（HTTPS）上的 4 个域通信，但流量不是 TLS / SSL。仔细查看该样本，发现它是针对 Linux X64 系统的后门程序，该家族已经存在至少 3 年了，根据它的行为将其命名为 RotaJakiro。RotaJakiro 使用多种加密算法非常注意隐藏其踪迹，包括使用 AES 算法对样本中的资源信息进行加密，C2 通信使用的组合 AES、XOR、ROTATE encryption 和 ZLIB compression。

详情

RotaJakiro: A long live secret backdoor with 0 VT detection
https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en/

FluBot 间谍软件遍布欧洲

日期: 2021-04-28

等级: 高

来源: Doug Olenick

标签: ['Proofpoint', 'Europe']

Proofpoint 的研究人员称，警方逮捕了四名涉嫌参与这一活动的嫌疑人，但之后 FluBot Android 间谍软件再次在欧洲各地蔓延。这家安全公司报告说，这些恶意软件的运营商正在有条不紊地工作，利用他们控制下的数千台设备发送恶意钓鱼短信，一个接一个地袭击不同的国家。

详情

FluBot Spyware Spreads Across Europe
https://www.databreachtoday.com/flubot-spyware-spreads-across-europe-a-16480

黑客利用 SonicWall 0Day 漏洞部署 FiveHands 勒索软件

日期: 2021-04-30

等级: 高

来源: The Hacker News

标签: ['FIVEHANDS', 'UNC2447', 'CVE-2021-20016']

一个金融黑客组织在 SonicWall VPN 设备中发现了一个 0Day 漏洞，该组织利用此漏洞进行攻击，并部署一种名为 FIVEHANDS 的新型勒索软件。CVE-2021-20016 是 SonicWall

SSLVPN SMA 产品系列中的 SQL 注入漏洞，未经身份验证的攻击者可利用该漏洞获取访问登录凭据（用户名，密码）以及会话信息，从而获取 SMA100 设备的控制权。

详情

Hackers Exploit SonicWall Zero-Day Bug in FiveHands Ransomware Attacks
https://thehackernews.com/2021/04/hackers-exploit-sonicwall-zero-day-bug.html

卡巴斯基发现了具有后门功能的中情局恶意软件

日期: 2021-04-30

等级: 高

来源: Waqas

标签: ['Purple Lambert', 'Kaspersky', 'CIA']

卡巴斯基实验室的全球研究和分析团队（GReAT）发现了一种新的恶意软件，该公司声称该软件是由美国中央情报局（CIA）开发的。据研究人员称，这些样本是在 2014 年收集的，因此很可能在 2014 年部署，最晚可能在 2015 年就已经开始部署。卡巴斯基研究人员称之为 Purple Lambert；该恶意软件具有后门功能，可以被动监听网络流量并搜索"数据包"。此外，恶意软件可以从目标系统中提取基本信息，同时执行从其操作员接收的 Payload。

详情

Kaspersky spots CIA malware with backdoor capabilities
https://www.hackread.com/kaspersky-cia-malware-backdoor-capabilities/

云托管提供商瑞士云遭遇勒索软件攻击

日期: 2021-05-02

等级: 高

来源: Pierluigi Paganini

标签: ['Swiss Cloud', 'Ransomware']

4 月 27 日，这家瑞士云主机提供商遭到勒索软件攻击，导致该公司服务器基础设施瘫痪。该公司目前在 HPE 和微软专家的帮助下，从备份中恢复操作。

详情

Cloud hosting provider Swiss Cloud suffered a ransomware attack
https://securityaffairs.co/wordpress/117433/cyber-crime/swiss-cloud-ransomware-attack.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. 及时对系统及各个服务组件进行版本升级和补丁更新

4. 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
5. 各主机安装 EDR 产品，及时检测威胁
6. 注重内部员工安全培训
7. 不轻信网络消息，不浏览不良网站、不随意打开邮件附件，不随意运行可执行程序
8. 勒索中招后，应及时断网，并第一时间联系安全部门或公司进行应急处理

(二) 数据安全

黑客曝光 2.5 亿美国户口记录

日期: 2021-04-26

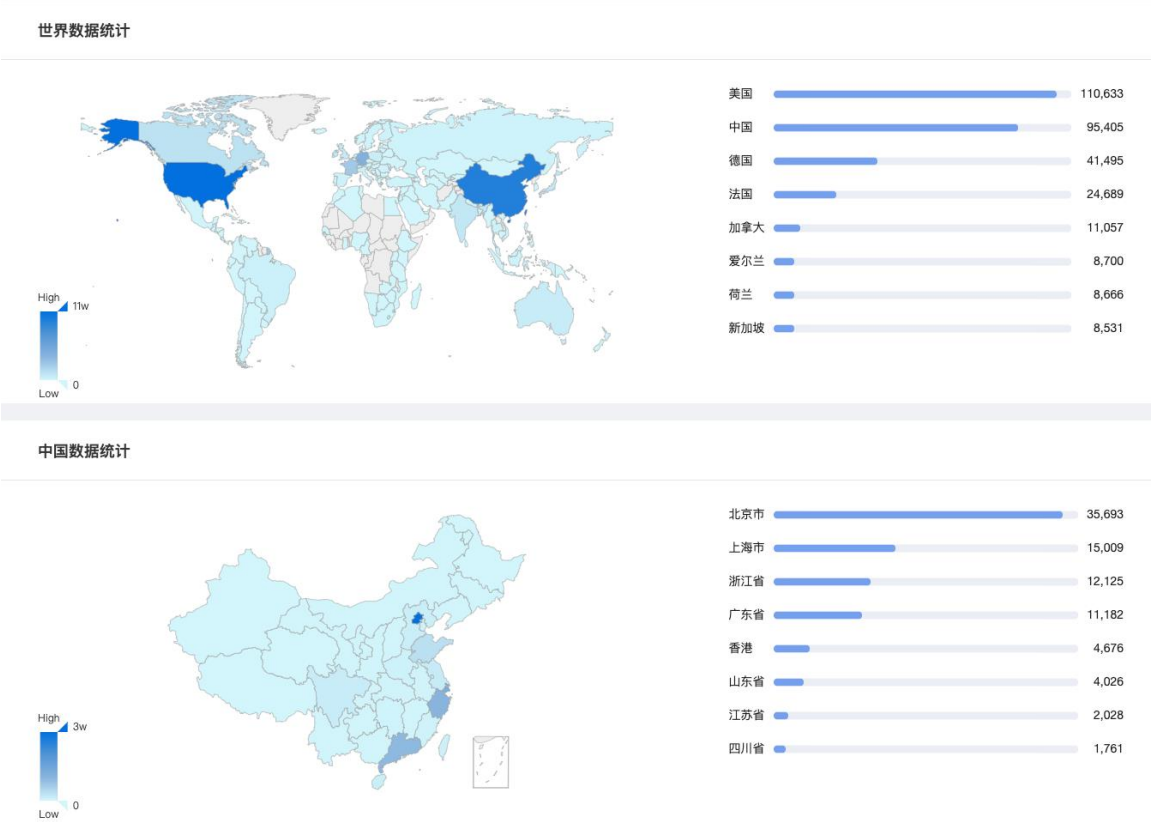
等级: 高

来源: Waqas

标签: ['American', 'Pompumurin']

2021 年 4 月 22 日，一名黑客通过 Pompumurin 泄露了一个数据库，其中包含超过 2.5 亿美国公民和居民的个人及户口数据。这个数据库包含价值 263GB 的记录，包括 1255 个 CSV 子文件，每个文件有 20 万个列表。尽管目前还不清楚是谁收集或拥有这些数据，但据消息人士透露，泄漏源来自亚马逊网络服务器上托管的开放 apache solr。

目前 Apache Solr 的具体分布如下图，数据来自于 360 QUAKE



详情

Hacker dumps sensitive household records of 250M Americans
https://www.hackread.com/hacker-dumps-household-records-of-americans/

Reverb 泄露音乐家个人信息

日期: 2021-04-26

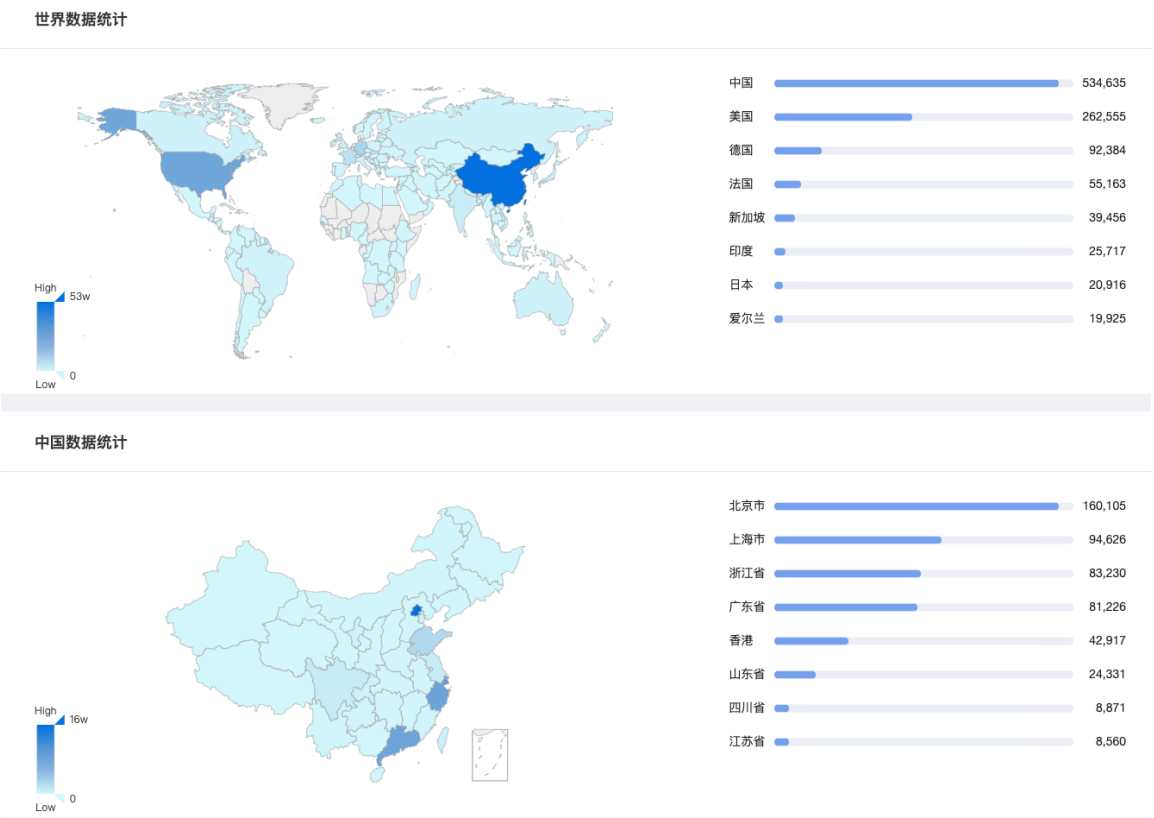
等级: 高

来源: Lawrence Abrams

标签: ['Reverb', 'Elasticsearch']

Reverb 是最大的在线市场，致力于销售乐器和设备。Reverb 遭遇数据泄露，一个未加密数据库的曝光。数据库服务器为 Elasticsearch，其中包含 560 多万条记录。每个记录都包含 Reverb.com 上特定列表的信息，包括全名、电子邮件地址、电话号码、邮寄地址、PayPal 电子邮件和列表、订单信息。

目前 Elasticsearch 的具体分布如下图，数据来自于 360 QUAKE



详情

Reverb discloses data breach exposing musicians' personal info
https://www.bleepingcomputer.com/news/security/reverb-discloses-data-breach-exposing-musicians-personal-info/

150 万条与政府有关的电子邮件记录遭遇泄露

日期: 2021-04-26

等级: 高

来源: The Hacker News

标签: ['Password', 'Government']

此次泄漏包括 1502909 个密码与来自世界各地的政府域的电子邮件地址，仅美国政府就有 625,505 个密码，其次是英国（205099），澳大利亚（136025），巴西（68535），加拿大（50726）。这一发现来自于对一个名为"COMB21"的 100GB 海量数据集的分析，这个数据集是对许多漏洞的汇总，早些时候在一个网络犯罪论坛上免费发布，它汇集了多年来发生在不同公司和组织的多起泄密事件的数据。

详情

3.2 Billion Leaked Passwords Contain 1.5 Million Records with Government Emails
https://thehackernews.com/2021/04/32-billion-leaked-passwords-contain-15.html

相关安全建议

1. 及时备份数据并确保数据安全
2. 合理设置服务器端各种文件的访问权限
3. 严格控制数据访问权限
4. 及时检查并删除外泄敏感数据
5. 发生数据泄漏事件后，及时进行密码更改等相关安全措施
6. 强烈建议数据库等服务放置在外网无法访问的位置，若必须放在公网，务必实施严格的访问控制措施

(三) 网络攻击

黑客利用 0day 漏洞攻击 MacOS 计算机

日期: 2021-04-27

等级: 高

来源: The Hacker News

标签: ['Apple', 'macOS']

苹果发布了 macOS 操作系统的更新，以解决一个被广泛利用的 0day 漏洞，该漏洞可能绕过所有安全保护，从而允许未经批准的软件在 Macos 上运行。macOS 的漏洞被识别为 CVE-2021-30657。

详情

Hackers Exploit 0-Day Gatekeeper Flaw to Attack MacOS Computers
https://thehackernews.com/2021/04/hackers-exploit-0-day-gatekeeper-flaw.html

First Horizon 银行在线帐户被黑客窃取客户资金

日期: 2021-04-30

等级: 高

来源: Sergiu Gatlan

标签: ['First Horizon']

银行控股公司 FirstHorizon Corporation 披露，其部分客户的网上银行账户遭到不明攻击者的入侵。First Horizon 是一家区域性金融服务公司，拥有 840 亿美元资产，提供银行、资本市场和财富管理服务。First Horizon 在 2021 年 4 月中旬发现了这起攻击，并表示它只影响了有限数量的客户。调查期间发现，攻击者可能利用先前被盗的凭证和利用第三方软件中的漏洞，侵入客户的网上银行账户。

详情

First Horizon bank online accounts hacked to steal customers' funds

https://www.bleepingcomputer.com/news/security/first-horizon-bank-online-accounts-hacked-to-steal-customers-funds/

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. 减少外网资源和不相关的业务，降低被攻击的风险
3. 做好产品自动告警措施
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. 注重内部员工安全培训

(四) 其他事件

一个新的 PHP Composer 漏洞可能导致广泛的供应链攻击

日期: 2021-04-30

等级: 高

来源: Ravie Lakshmanan

标签: ['PHP', 'Composer', 'URL']

PHP 的软件包管理器 Composer 的维护者已发布了一个更新程序，以解决一个严重漏洞，该漏洞可能允许攻击者执行任意命令并将每个 PHP 软件包安装上后门，从而导致供应链攻击。该漏洞源于处理程序包源下载 URL 的方式，可能触发远程命令执行。

详情

A New PHP Composer Bug Could Enable Widespread Supply-Chain Attacks

https://thehackernews.com/2021/04/a-new-php-composer-bug-could-enable.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29

Apple 修补了 macOS Gatekeeper 被绕过的漏洞

日期: 2021-04-28

等级: 高

来源: Charlie Osborne

标签: ['Apple', 'Mac']

苹果发布了一系列的安全补丁，解决了一些问题，包括一个被广泛利用的 0day 漏洞和一个权限绕过漏洞。安全补丁已经发布，即 macOS Big Sur 11.3。其中一个最值得注意的修复是 Cedric Owens 发现的漏洞。该漏洞被追踪为 CVE-2021–30657，攻击者可绕过 Gatekeeper（苹果用于代码签名和验证的内置保护机制）。

详情

Apple patches macOS Gatekeeper bypass vulnerability exploited in the wild

https://www.zdnet.com/article/apple-patches-macos-gatekeeper-bypass-vulnerability-exploited-in-the-wild/

F5 BIG-IP 易受 Kerberos KDC 欺骗漏洞攻击

日期: 2021-04-28

等级: 高

来源: The Hacker News

标签: ['KDC', 'F5', 'Kerberos']

Kerberos 密钥分发中心（KDC）安全功能中存在一个新的绕过漏洞（CVE-2021-23008），影响 F5 大型 IP 应用程序交付服务。Silverfort 研究人员 Yaron Kassner 和 Rotem Zach 在一份报告中说："KDC 欺骗漏洞允许攻击者绕过 Kerberos 身份验证到大型 IP 访问策略管理器（APM），绕过安全策略，获得对敏感工作负载的不受限制的访问。"

详情

F5 BIG-IP Found Vulnerable to Kerberos KDC Spoofing Vulnerability

https://thehackernews.com/2021/04/f5-big-ip-found-vulnerable-to-kerberos.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

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 2. 事件涉及的漏洞等级为严重/高危 3. 事件涉及机密/重要/核心数据， 4. 事件涉及数据量巨大 5. 事件涉及大型/常用厂商与组件 6. 事件涉及金额数目庞大/相关受害者损失高 7. 已知/潜在受害者数量庞大 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 2. 事件涉及的漏洞等级为中危 3. 事件涉及数据机密性/重要性一般， 4. 事件涉及数据量中等 5. 事件涉及小型/常用厂商与组件 6. 事件涉及金额数目中等/相关受害者损失一般 7. 已知/潜在受害者数量中等 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 2. 事件涉及的漏洞等级为低危 3. 事件涉及数据机密性/重要性低， 4. 事件涉及数据量低 5. 事件涉及小型/非常用厂商与组件 6. 事件涉及金额数目少/相关受害者损失低 7. 已知/潜在受害者数量少 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