安全事件周报

安全事件周报 (11.09-11.15)

360CERT
北京奇虎科技有限公司 | 2020-11-16

报告信息

报告名称	安全事件周报（11.09-11.15）		
报告类型	安全事件周报	报告编号	B6-2020-111602
报告版本	1.0	报告日期	2020-11-16
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	2020-11-16	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 40 项

话题集中在`勒索软件`、`数据泄露`方面，涉及的组织有：`X-Cart`、`Cencosud`、`EA Games`、`Vertafore`等。勒索事件频发，数据保护是企业安全防护的重中之重。

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
新的"Ghimob"恶意软件可以监视 153 个 Android 移动应用程序	★★★★★
ModPipe 后门攻击了酒店行业使用的 POS 软件	★★★★★
RansomEXX 勒索软件现在可以针对 Linux 系统	★★★★
勒索软件团伙入侵 Facebook 账户发布勒索广告	★★★★
Play Store 被确定为大多数 Android 恶意软件的主要分发媒介	★★★★
Costarito APT：网络攻击者使用不知名恶意软件	★★★★
勒索软件攻击电子商务平台 X-Cart	★★★
勒索软件运营商使用伪造的微软团队更新部署 Cobalt Strike	★★★
恶意 NPM 项目窃取了浏览器信息和 Discord 帐户	★★★
Darkside 勒索软件发起联盟计划	★★★
生物技术研究公司 Miltenyi Biotec 遭 Mount Locker 勒索软件攻击	★★★
零售业巨头 Cencosud 遭遇 Egregor 勒索软件攻击	★★★
Jupyter 恶意软件窃取浏览器数据	★★★
新的 TroubleGrabber 恶意软件针对 Discord 用户	★★★
数据安全	**等级**
全球数百万酒店客人遭遇大规模数据泄露	★★★★★
Animal Jam 儿童虚拟世界遭遇数据泄露，影响 4600 万用户	★★★★★
Vertafore 数据泄露案曝光 2770 万德州司机信息	★★★★★
580 万 RedDoorz 用户记录在黑客论坛上出售	★★★★
COVID-19 数据共享应用泄露医护人员信息	★★★★
私人社交网络泄露的色情照片、视频和音频超过 13 万个	★★★★
ShinyHunters 入侵冥王星电视服务，320 万个账户被曝光	★★★★

Cobalt Strike 工具包的反编译源代码在网上泄露	★★★
网络攻击	**等级**
黑客通过 CVE-2020-14882 漏洞攻击 WebLogic 服务器	★★★★
UVM 健康网络遭受网络攻击，化疗预约功能受阻	★★★★
特朗普网站指称亚利桑那州选举舞弊曝光选民数据	★★★★
黑客从加密货币服务 Akropolis 窃取 200 万美元	★★★★
Microsoft Exchange 攻击暴露了新的 XUNT 后门	★★★
攻击者使用图像反转技术绕过 Office 365 过滤机制	★★★
超过 2800 家电子商店运行过时的 Magento 软件	★★★
North Face 网站遭遇了证书填充攻击	★★★
其他事件	**等级**
微软前工程师因盗窃 1000 万美元被判 9 年监禁	★★★★★
微软发布了 112 个安全漏的洞修复程序	★★★★★
Windows 10、iOS、Chrome、Firefox 等在天府杯比赛中被安全人员攻破	★★★★
严重的权限提升漏洞导致 Intel 发布更新	★★★★
世界上最大的 Android 电视中发现严重漏洞	★★★★
Google 解决了两个新的 Chrome 0day 漏洞	★★★★
Bug hunter 因 DOD 账户接管漏洞获得"月度最佳研究员"奖	★★★
更新 Windows 10 以修补 Microsoft Store 游戏中的漏洞	★★★
EA Games 的 Origin 客户端包含特权升级漏洞	★★★
现在修补的 Ubuntu 桌面漏洞允许权限提升	★★★

三、 事件详情

(一) 恶意程序

新的“Ghimob”恶意软件可以监视 153 个 Android 移动应用程序

日期: 2020-11-10

等级: 高

来源: Catalin Cimpanu

标签: ['Android', 'Banking Trojan', 'Ghimob', 'Malware', 'Kaspersky']

安全研究人员发现了一种新的 Android 银行木马，它可以从 153 个 Android 应用程序中窃取数据。 据安全公司卡巴斯基(Kaspersky)2020 年 11 月 9 日发布的一份报告称，这款名为 Ghimob 的木马被认为是由 Windows 恶意软件 Astaroth (Guildma)背后的同一个组织开发的。 卡巴斯基说，新的 Android 木马已经被打包在网站和服务器上的恶意 Android 应用程序中提供下载。

详情

New 'Ghimob' malware can spy on 153 Android mobile applications

https://www.zdnet.com/article/new-ghimob-malware-can-spy-on-153-android-mobile-applications/

ModPipe 后门攻击了酒店行业使用的 POS 软件

日期: 2020-11-12

等级: 高

来源: MartinSmolár

标签: ['ModPipe', 'POS', 'Backdoor', 'ESET', 'Modular']

`ESET`的研究人员发现了`ModPipe`，这是一个模块化的后门，可以让运营商访问存储在运行`ORACLE MICROS`餐厅企业系列（RES）3700 POS 的设备中的敏感信息，这是一个管理软件套件，被全球数十万家酒吧、餐厅、酒店和其他酒店机构使用。 后门的独特之处在于它的可下载模块及其功能。其中一个名为`GetMicInfo`的算法包含一个算法，通过从`Windows`注册表值中解密来收集数据库密码。这表明后门的作者对目标软件有很深的了解，他们选择了这种复杂的方法，而不是通过一个更简单但更明显的方法收集数据，如键盘记录。

详情

Hungry for data, ModPipe backdoor hits POS software used in hospitality sector

https://www.welivesecurity.com/2020/11/12/hungry-data-modpipe-backdoor-hits-pos-software-hospitality-sector/

RansomEXX 勒索软件现在可以针对 Linux 系统

日期: 2020-11-09

等级: 高

来源: Prajeet Nair

标签: ['Kaspersky', 'Linux', 'RansomEXX', 'Windows', 'Ransomware']

卡巴斯基的研究人员发现了一个 Linux 版本的 RansomEXX 勒索软件，到目前为止它只针对 Windows 设备。 RansomEXX 首次被安全研究人员发现是在 2020 年 6 月。根据卡巴斯基的报告，该勒索软件与最近针对德克萨斯州运输部(Texas Department of Transportation)和柯尼卡美能达(Konica Minolta)的攻击有关。 该恶意软件因攻击大型组织而臭名昭著，并且 2020 年初活跃度最高。

详情

RansomEXX Ransomware Can Now Target Linux Systems

https://www.databreachtoday.com/ransomexx-ransomware-now-target-linux-systems-a-15332

勒索软件团伙入侵 Facebook 账户发布勒索广告

日期: 2020-11-11

等级: 高

来源: Lawrence Abrams

标签: ['Facebook Account', 'Ragnar Locker', 'Ransomware', 'Extortion Ads', 'Ransom']

一个勒索软件组织现在开始在 Facebook 上发布广告，向受害者施压，要求他们支付赎金。 2020 年 11 月 10 日，Ragnar Locker 背后的勒索软件运营商又上了一个台阶，他们侵入了一个 Facebook 广告客户的账户，并创建了他们对`Campari Group`攻击的广告。 被黑客入侵的`Facebook`帐户所有者`Chris Hodson`表示，在`Facebook`将其检测为欺诈活动之前，该广告已向 7,000 多个`Facebook`用户进行展示。

详情

Ransomware gang hacks Facebook account to run extortion ads

https://www.bleepingcomputer.com/news/security/ransomware-gang-hacks-facebook-account-to-run-extortion-ads/

Play Store 被确定为大多数 Android 恶意软件的主要分发媒介

日期: 2020-11-11

等级: 高

来源: Catalin Cimpanu

标签: ['Google', 'Android', 'Malware', 'Play Store']

在最近的一项学术研究中，官方的 Google play 商店被认为是 Android 设备上安装恶意软件的主要来源，被认为是迄今为止进行的此类恶意软件中规模最大的一种。 研究人员使用 NortonLifeLock（以前为 Symantec）提供的遥测数据，分析了在 2019 年 6 月至 2019 年 9 月的四个月中，超过 1200 万台 Android 设备上应用程序安装的起源。 研究人员总共为 790 万个独特应用程序安装了超过 3400 万个 APK（Android 应用程序）。 研究人员表示，根据 Android 恶意软件的不同分类，他们分析的应用程序中有 10%到 24%可能被描述为恶意或不需要的应用程序。

详情

Play Store identified as main distribution vector for most Android malware

https://www.zdnet.com/article/play-store-identified-as-main-distribution-vector-for-most-android-malware/

Costarito APT：网络攻击者使用不知名恶意软件

日期: 2020-11-12

等级: 高

来源: Pierluigi Paganini

标签: ['CostaRicto APT', 'South Asian', 'Blackberry', 'Undocumented Malware']

`Blackberry`的研究人员记录了一个名为`CostaRicto`的雇佣黑客组织的活动，该组织被发现使用一种以前没有记录过的恶意软件攻击南亚金融机构和全球娱乐公司。 在过去 6 个月里，`Blackberry`研究和情报团队一直在监控一场网络间谍活动，目标是全球各地不同的受害者。BlackBerry 将这一活动称为 CostaRicto，它似乎是由雇佣黑客操纵的，这是一群聪明的雇佣黑客，他们拥有定制的恶意软件工具、复杂的 VPN 代理和 SSH 隧道挖掘能力。

详情

Costaricto APT: Cyber mercenaries use previously undocumented malware
https://securityaffairs.co/wordpress/110818/apt/costaricto-apt-cyber-mercenaries.html

勒索软件攻击电子商务平台 X-Cart

日期: 2020-11-09

等级: 中

来源: Catalin Cimpanu

标签: ['X-Cart', 'Platform', 'Vulnerability']

电子商务软件供应商 X-Cart 在 10 月底遭遇勒索软件攻击，导致该公司托管平台上托管的客户商店瘫痪。 据信，这起事件发生在攻击者利用第三方软件的漏洞获取对 X-Cart 商店托管系统的访问权之后。 X-Cart 背后的公司卖方实验室营销副总裁杰夫·科恩（Jeff Cohen）表示他们已经确定了漏洞，但在他们的安全公司确认之前不希望透露该名称。 杰夫科恩说，攻击者访问了少量服务器，并对其进行了加密，摧毁了在受影响系统上运行的 X-Cart 商店。一些商店完全瘫痪了，而另一些商店则报告了发送电子邮件警报的问题。

详情

Ransomware hits e-commerce platform X-Cart
https://www.zdnet.com/article/ransomware-hits-e-commerce-platform-x-cart/

勒索软件运营商使用伪造的微软团队更新部署 Cobalt Strike

日期: 2020-11-10

等级: 中

来源: Pierluigi Paganini

标签: ['Cobalt Strike', 'Ransomware', 'Microsoft Updates', 'Cobalt Strike']

勒索软件运营商正在使用恶意的虚假`Microsoft Teams`更新来提供后门程序，这些后门程序会安装`Cobalt Strike`利用工具并破坏目标网络。 由于 COVID-19 的大流行，迫使越来越多的组织和企业使用视频会议，而攻击者正试图利用这一点。 该技术不是新技术，攻击者已经在野外攻击中加以利用。 在 2019 年，DoppelPaymer 勒索软件运营商使用此技巧在 2019 年将目标锁定为 Microsoft 用户。2020 年，WastedLocker 运营商通过使用多状态攻击链并使用签名的二进制文件来逃避检测，从而发展了该技术。

详情

Ransomware operators use fake Microsoft Teams updates to deploy Cobalt Strike
https://securityaffairs.co/wordpress/110693/malware/fake-microsoft-teams-cobalt-strike.html

恶意 NPM 项目窃取了浏览器信息和 Discord 帐户

日期: 2020-11-10

等级: 中

来源: Pierluigi Paganini

标签: ['Sonatype', 'Malicious NPM', 'Discord accounts', 'Discord.dll']

Sonatype 研究人员`Ax Sharma`发现了一个名为`discord.dll`的`npm`软件包，其中包含从用户浏览器和`Discord`应用程序中窃取敏感文件的恶意代码。 恶意 JavaScript 库已上传到 npm 数据包存储库，并且已被删除。 discord.dll 项目已经可以在 NPM 门户上使用五个月，并且已被开发人员下载了一百次。 Sonatype 研究人员报告，一旦安装，恶意 discord.dll 将运行恶意代码搜索开发人员的计算机为某些应用程序，然后检索他们内部的 LevelDB 数据库。

详情

Malicious NPM project steals browser info and Discord accounts
https://securityaffairs.co/wordpress/110705/hacking/malicious-npm-project-discord-dll.html

Darkside 勒索软件发起联盟计划

日期: 2020-11-12

等级: 中

来源: Mathew J. Schwartz

标签: ['Darkside', 'Cybercrime Forums', 'Affiliate Program', 'Ransomware']

使用联营企业可以实现众包利润，但也会让运营商面临更多风险，Darkside 勒索软件团伙最近宣布，它推出了一个联盟计划，作为其努力实现收入最大化的一部分。 据以色列网络威胁情报监测公司`Kela`报道，最近几天，`Darkside`背后的运营商已进入`XSS`和`Exploit`这两个主要的俄语网络犯罪论坛，以宣布其新会员计划的详细信息。 对于每一个支付赎金的受害者，附属公司与勒索软件运营商分享所得。

详情

Darkside Ransomware Gang Launches Affiliate Program
https://www.databreachtoday.com/blogs/darkside-ransomware-gang-launches-affiliate-program-p-2968

生物技术研究公司 Miltenyi Biotec 遭 Mount Locker 勒索软件攻击

日期: 2020-11-14

等级: 中

来源: Pierluigi Paganini

标签: ['Miltenyi Biotec', 'Mount Locker', 'Ransomware', 'Biotech']

生物技术研究公司 Miltenyi Biotec 遭受了勒索软件攻击，该勒索软件攻击于 10 月发生，并影响了其全球 IT 基础设施。 Miltenyi Biotec 是一家全球生物技术公司，总部位于德国科

隆，提供的产品和服务可为科学家，临床研究人员和医师提供基础研究，转化研究和临床应用方面的支持。 该公司宣布，在袭击发生后，它已完全恢复了系统，但是在某些国家，地区，本地员工仍面临邮件和电话系统的问题。

详情

Biotech research firm Miltenyi Biotec hit by Mount Locker ransomware

https://securityaffairs.co/wordpress/110900/malware/miltenyi-biotec-ransomware-attack.html

零售业巨头 Cencosud 遭遇 Egregor 勒索软件攻击

日期: 2020-11-14

等级: 中

来源: Lawrence Abrams

标签: ['Cencosud', 'Egregor', 'Ransomware', 'Cyberattack']

总部位于智利的跨国零售公司 Cencosud 遭受了 Egregor 勒索软件行动的网络攻击，影响了商店的服务。 Cencosud 是拉丁美洲最大的零售公司之一，拥有超过 14 万名员工，2019 年收入 150 亿美元。 2020 年 11 月 14 日，Cencosud 遭到勒索软件攻击，加密了整个零售店的设备，影响了公司的运营。阿根廷出版商 Clarín 称，零售店仍在营业，但一些服务受到影响。

详情

Retail giant Cencosud hit by Egregor Ransomware attack, stores impacted

https://www.bleepingcomputer.com/news/security/retail-giant-cencosud-hit-by-egregor-ransomware-attack-stores-impacted/

Jupyter 恶意软件窃取浏览器数据

日期: 2020-11-13

等级: 中

来源: Ionut Ilascu

标签: ['Jupyter', 'Malware', 'Browser', 'Backdoor']

俄国黑客一直在使用一种新的恶意软件来从受害者中窃取信息。 该恶意软件为`Jupyter`，他的威胁一直没有受到重视，并受益于快速的开发周期。 虽然 Jupyter 的目的是收集各种软件的数据，但支持其传输的恶意代码也可以用来在受感染的系统上创建后门。 2019 年 10 月，在美国一所大学的事件响应活动中出现了该恶意软件的变体，但数据表明，早前版本从 5 月就已开发出来。 网络安全公司 Morphisec 的研究人员发现，攻击套件的开发者非常活跃，有些组件在一个月内收到了 9 次以上的更新。

详情

New Jupyter malware steals browser data, opens backdoor

https://www.bleepingcomputer.com/news/security/new-jupyter-malware-steals-browser-data-opens-backdoor/

新的 TroubleGrabber 恶意软件针对 Discord 用户

日期: 2020-11-13

等级: 中

来源: Pierluigi Paganini

标签: ['TroubleGrabber', 'Netskope', 'Discord', 'Malware']

`Netskope`安全研究人员发现了一种名为`TroubleGrabber`的盗取身份认证的恶意软件，这种恶意软件通过`Discord`附件传播，并使用`Discord`的网络`hook`将窃取的数据传输给运营商。 该恶意软件具有与其他针对`Discord 游戏玩家的恶意软件（例如`AnarchyGrabber`）所使用的相同功能，但它似乎是不同攻击者的工作。TroubleGrabber 由名为" Itroublve"的人开发，目前被多个攻击者使用。

详情

New TroubleGrabber malware targets Discord users
https://securityaffairs.co/wordpress/110887/malware/troublegrabber-discord-malware.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. 不盲目信任云端文件及链接
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. 及时对系统及各个服务组件进行版本升级和补丁更新
5. 网段之间进行隔离，避免造成大规模感染
6. 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
7. 注重内部员工安全培训
8. 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

(二) 数据安全

全球数百万酒店客人遭遇大规模数据泄露

日期: 2020-11-09

等级: 高

来源: Tara Seals

标签: ['S3', 'Cloud', 'Amazon Bucket', 'Hotel', 'Data Breach']

一个被广泛使用的酒店预订平台已经曝光了世界各地不同酒店的 1000 万份与客人相关的文件，这是由于一个错误配置的 Amazon Web Services S3 bucket。这些记录包括敏感数据，包括信用卡细节。 酒店使用`Prestige Software`的`Cloud Hospitality`将其预订系统与在线预订网站（如 Expedia 和 Booking.com）集成。 Planet 安全团队称，该事件影响了总计 24.4 GB 的数据。 许多记录包含单个预订将多个酒店客人分组在一起的数据，因此，研究人员说，暴露的人数很可能超过 1000 万。

详情

Millions of Hotel Guests Worldwide Caught Up in Mass Data Leak
https://threatpost.com/millions-hotel-guests-worldwide-data-leak/161044/

Animal Jam 儿童虚拟世界遭遇数据泄露，影响 4600 万用户

日期: 2020-11-11

等级: 高

来源: Lawrence Abrams

标签: ['Animal Jam', 'WildWorks', 'Data Breach', 'Virtual World', 'Hacker Forum']

`Animal Jam`是`WildWorks`创建的虚拟世界，孩子们可以在这里和其他成员一起玩在线游戏。Animal Jam 面向 7 至 11 岁的儿童用户，由儿童创造的动物角色超过 3 亿，每 1.4 秒就会有新玩家注册。 2020 年 11 月 10 日，一个攻击者在一个黑客论坛上免费共享了两个属于`Animal Jam`的数据库，他们说这些数据库是由知名网站黑客`ShinyHunters`获得的。这两个被盗的数据库名为`game_accounts`和`users`，包含约 4600 万被盗用户记录。

详情

Animal Jam kids' virtual world hit by data breach, impacts 46M accounts
https://www.bleepingcomputer.com/news/security/animal-jam-kids-virtual-world-hit-by-data-breach-impacts-46m-accounts/

Vertafore 数据泄露案曝光 2770 万德州司机信息

日期: 2020-11-13

等级: 高

来源: Catalin Cimpanu

标签: ['Vertafore', 'Texas', 'Data Breach', 'Without Authorization']

保险软件提供商`Vertafore`2020 年 11 月 13 日披露了一起数据泄露事件，承认第三方获取了 2770 万德克萨斯州司机的详细信息。 这起事件发生在 3 月 11 日，由于人为错误，三个数据文件意外存储在一个不安全的外部存储服务中。 Vertafore 表示，这些文件于 8 月 1 日从外部存储系统中删除，但经过调查，他们发现这些文件在未经授权的情况下被访问。

详情

Info of 27.7 million Texas drivers exposed in Vertafore data breach
https://www.zdnet.com/article/info-of-27-7-million-texas-drivers-exposed-in-vertafore-data-breach/

580 万 RedDoorz 用户记录在黑客论坛上出售

日期: 2020-11-10

等级: 高

来源: Lawrence Abrams

标签: ['RedDoorz', 'User Records', 'Hacking Forum', 'Sale']

在 9 月份遭遇数据泄露后，一名攻击者正在一个黑客论坛上出售一个包含 580 万条用户记录的 RedDoorz 数据库。RedDoorz 是一家位于新加坡的酒店管理和预订平台，在东南亚拥有超过 1000 家酒店。通过网站或手机应用，用户可以注册一个账户，浏览可用的经济型酒店并预订。 2020 年 9 月底，RedDoorz 披露，由于一名未经授权的人访问了他们的

一个数据库，他们遭受了数据泄露。不过，当时据其所知，`RedDoorz`的财务信息或密码都没有被泄露。 攻击者 2020 年 11 月 9 日开始销售包含 580 万用户记录的数据库，该记录在 RedDoorz 数据泄露期间被盗。

详情

5.8 million RedDoorz user records for sale on hacking forum

https://www.bleepingcomputer.com/news/security/58-million-reddoorz-user-records-for-sale-on-hacking-forum/

COVID-19 数据共享应用泄露医护人员信息

日期: 2020-11-11

等级: 高

来源: Elizabeth Montalbano

标签: ['COVID-19', 'Data Leak', 'Philippines', 'Vulnerability', 'COVID-KAYA']

菲律宾医护人员使用的一个共享 COVID-19 病例数据的平台包含多个漏洞，暴露了医护人员的数据，可能泄露了患者数据。 根据多伦多大学 Citizen Lab 研究人员的报告，COVID-KAYA 平台的网络和 Android 应用程序中都存在漏洞，未经授权的用户可以访问有关该平台用户的私人数据以及潜在的患者数据。 COVID-KAYA 于 6 月 2 日部署，使菲律宾的一线医疗人员能够自动收集和与该国卫生部共享冠状病毒病例信息。 该应用程序具有 Web，iOS 和 Android 版本，并使用 Cordova（跨平台应用程序开发框架）构建，该框架允许开发人员使用 Web 技术构建应用程序，然后将相同的代码部署到 Web 和移动平台。

详情

COVID-19 Data-Sharing App Leaked Healthcare Worker Info

https://threatpost.com/covid-19-data-leaked-healthcare-worker-info/161108/

私人社交网络泄露的色情照片、视频和音频超过 13 万个

日期: 2020-11-11

等级: 高

来源: Bernard Meyer

标签: ['CyberNews', 'Leaked', 'Database', 'Bucket', 'Photo', 'Covid-19']

网络新闻调查小组最近发现了一个不安全的数据库，其中包含 13 万多张极其敏感、非常露相的私人照片、视频和录音。 该数据库似乎属于一个私人社交网络，很有可能是在中国。幸运的是，在`cybernews`第一次联系亚马逊两天后，也就是 11 月 6 日，亚马逊关闭了这个不安全的存储`bucket`。

详情

130k+ extremely NSFW sexual photos, video and audio leaked by ‘private social network’

https://cybernews.com/security/130k-nsfw-photos-video-audio-leaked-private-social-network/

ShinyHunters 入侵冥王星电视服务，320 万个账户被曝光

日期: 2020-11-15

等级: 高

来源: Pierluigi Paganini

标签: ['Pluto TV', 'ShinyHunters', 'Accounts', 'Television Service']

一名黑客在一个黑客论坛上免费分享了 320 万冥王星电视用户账户，他声称这些账户是被 ShinyHunters 的攻击者窃取的。 冥王星电视是美国的互联网电视服务，它是广告商支持的视频点播（AVOD）服务，主要通过旨在模拟传统广播节目体验的数字线性频道提供一系列节目内容。该服务有超过 2800 万会员。 数据泄露似乎是由著名的攻击者 ShinyHunters 的工作造成的，后者是许多其他安全漏洞的背后原因，其中包括微软私有 GitHub 存储库，流行的数字银行应用`Dave.com`和`Animal Jam`的黑客入侵。

详情

ShinyHunters hacked Pluto TV service, 3.2M accounts exposed

https://securityaffairs.co/wordpress/110931/data-breach/pluto-tv-database-shinyhunters.html

Cobalt Strike 工具包的反编译源代码在网上泄露

日期: 2020-11-11

等级: 中

来源: Pierluigi Paganini

标签: ['Cobalt Strike', 'GitHub', 'Source Code', 'Leaked']

Cobalt Strike 开发后工具包的反编译源代码据称已经在 GitHub 的一个资源库中在线泄露。 Cobalt Strike 是一个合法的渗透测试工具包和威胁仿真软件，允许攻击者在受损害的设备上部署`payloads`，称为`beacons`，以远程创建`shell`，执行`PowerShell`脚本，执行权限升级，或生成一个新的会话，以在受害系统上创建侦听器。 Cobalt Strike 被广泛应用于攻击者，他们使用破解版本获得对目标网络的持久远程访问。

详情

The alleged decompiled source code of Cobalt Strike toolkit leaked online

https://securityaffairs.co/wordpress/110782/hacking/cobalt-strike-source-code.html

相关安全建议

1. 管控内部员工数据使用规范，谨防数据泄露并及时做相关处理
2. 对于托管的云服务器(VPS)或者云数据库，务必做好防火墙策略以及身份认证等相关设置
3. 敏感数据建议存放到 http 无权限访问的目录
4. 及时备份数据并确保数据安全
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. 条件允许的情况下，设置主机访问白名单
7. 建议加大口令强度，对内部计算机、网络服务、个人账号都使用强口令

(三) 网络攻击

黑客通过 CVE-2020-14882 漏洞攻击 WebLogic 服务器

日期: 2020-11-09

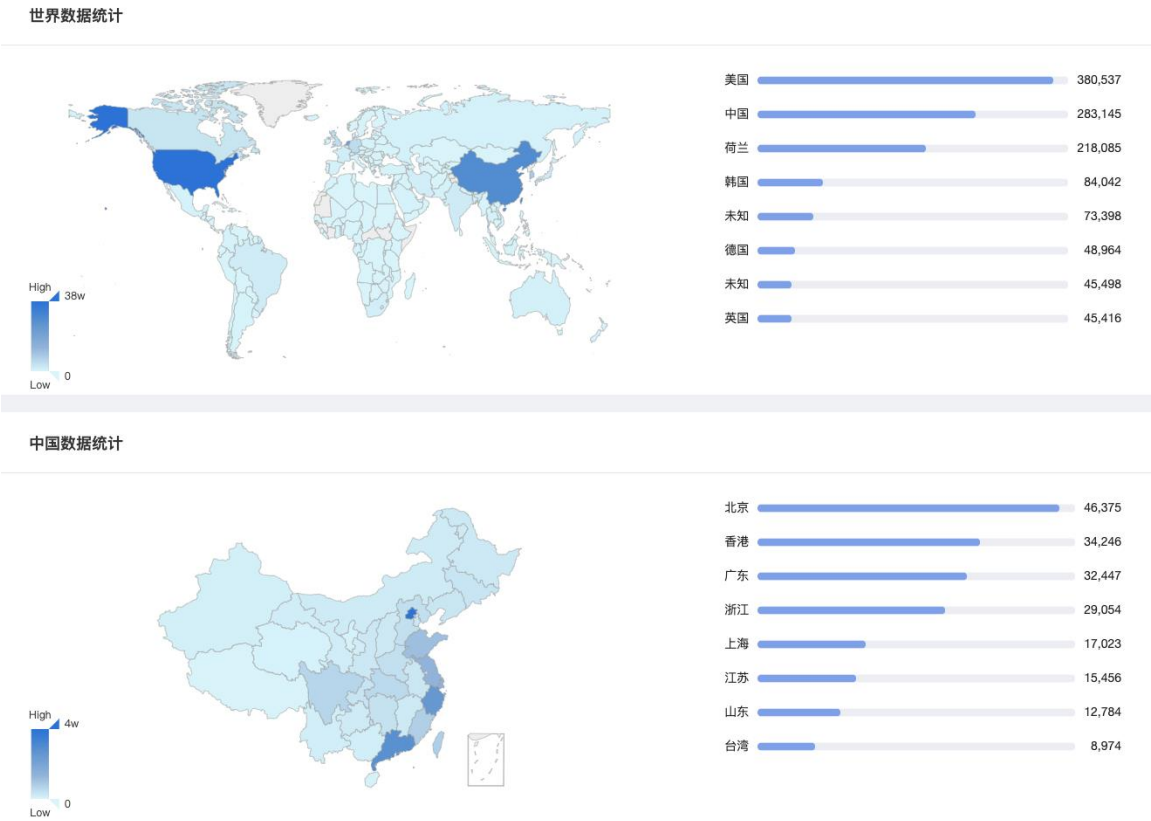
等级: 高

来源: GURUBARAN S

标签: ['Oracle WebLogic Servers', 'Cobalt Strike', 'Vulnerability', 'Crypto-Mining ']

攻击者正在通过 CVE-2020-14882 漏洞利用 Oracle WebLogic Server 安装 Cobalt Strike，该漏洞允许攻击者对受感染设备的持久远程访问。 除了漏洞的扫描外，还发现有少数攻击者尝试安装加密货币挖掘工具。 由于 CVE-2020-14882 和 CVE-2020-14750 很容易被未经身份验证的攻击者利用来接管存在漏洞的 WebLogic 服务器，Oracle 建议公司立即应用安全更新来阻止攻击。

目前 Weblogic 的具体分布如下图，数据来自于 360 QUAKE



详情

Hackers Attacking WebLogic Servers via CVE-2020-14882 Flaw

https://gbhackers.com/weblogic-servers-flaw/

UVM 健康网络遭受网络攻击，化疗预约功能受阻

日期: 2020-11-09

等级: 高

来源: Lindsey O'Donnell

标签: ['University of Vermont', 'Cyberattack', 'Hospital']

佛蒙特大学(University of Vermont)的医疗网络正在忙着恢复自己的系统，此前，一场网络攻击导致病患预约普遍延迟，包括化疗预约、乳房 x 光检查和活检预约。 UVM 健康网络是一个六家医院、家庭健康和临终关怀系统，包括在佛蒙特州和纽约北部的 1000 多名医生、2000 名护士和其他临床医生。 据当地报道，此次网络攻击始于 10 月 25 日的那一周，UVM 医疗中心受到的攻击最为严重。报道说，攻击通过医院的主计算机服务器，影响了整个系统。

详情

Cyberattack on UVM Health Network Impedes Chemotherapy Appointments
https://threatpost.com/cyberattack-uvm-health-network/161059/

特朗普网站指称亚利桑那州选举舞弊曝光选民数据

日期: 2020-11-09

等级: 高

来源: Becky Bracken

标签: ['Arizona', 'SQL Injection', 'Trump']

在亚利桑那州，一个用来收集当面投票欺诈证据的网站存在安全漏洞，这将为 SQL 注入和其他攻击打开大门。 这个漏洞是在特朗普竞选团队创建的 `dontpressthegreenbutton.com`网站上发现的，是由网络安全专家托德·罗辛(Todd Rossin)意外发现的。 有人使用 SQL 注入提取姓名、地址、出生日期和社会保险号的最后四个数字。

详情

Trump Site Alleging AZ Election Fraud Exposes Voter Data
https://threatpost.com/trump-site-alleging-az-election-fraud-exposes-voter-data/161068/

黑客从加密货币服务 Akropolis 窃取 200 万美元

日期: 2020-11-13

等级: 高

来源: Catalin Cimpanu

标签: ['Akropolis', 'Steals', 'Dai', 'Cryptocurrency']

加密货币借贷服务公司`Akropolis`称，黑客对其平台进行了`flash loan`攻击，并偷走了价值约 200 万美元的 Dai 加密货币。 攻击发生在 2020 年 11 月 12 日下午（格林尼治标准时间时区），Akropolis 管理员暂停了平台上的所有交易，以防止进一步损失。 Akropolis 说，虽然它聘请了两家公司来调查这一事件，但两家公司都无法查明利用该攻击的攻击载体。 对于运行 DeFi（去中心化金融）平台的加密货币服务，`Flash loan`攻击已变得很普遍，该服务允许用户使用加密货币借入或借出，推测价格变化并在类似加密货币储蓄的帐户中赚取利息。

详情

Hacker steals $2 million from cryptocurrency service Akropolis

https://www.zdnet.com/article/hacker-steals-2-million-from-cryptocurrency-service-akropolis/

Microsoft Exchange 攻击暴露了新的 XUNT 后门

日期: 2020-11-09

等级: 中

来源: Lindsey O'Donnell

标签: ['Powershell', 'Kuwait', 'Microsoft Exchange', 'Backdoors', 'xHunt', 'TriFive']

在最近，研究人员在科威特一家组织发现了对 Microsoft Exchange 服务器的攻击，发现了两个从未见过的 Powershell 后门。 该活动与已知的`xHunt`威胁组织有关，该组织于 2018 年首次被发现，此前曾针对科威特政府以及航运和运输组织发动了一系列攻击。 这次攻击使用了两种新发现的后门:一种被研究人员称为 TriFive，另一种是之前发现的基于 powershell 的后门的变种(被称为 CASHY200)，他们称之为 Snugy。

详情

Microsoft Exchange Attack Exposes New xHunt Backdoors
https://threatpost.com/microsoft-exchange-attack-xhunt-backdoors/161041/

攻击者使用图像反转技术绕过 Office 365 过滤机制

日期: 2020-11-10

等级: 中

来源: GURUBARAN S

标签: ['Microsoft', 'Office 365', 'Bypass', 'Image Inversion']

Kim Komando 说，WMC Global Analysis 研究人员发现了一个创造性的 Office 365 网络钓鱼活动，该活动是 Microsoft 帐户的合法登录页面，但使用了颜色反转以避免图像识别软件中的图案匹配。 随着图像识别软件的不断改进和准确性的不断提高，这项新技术旨在通过颠倒图像的颜色来误导扫描引擎，导致图像哈希值与原始图像不同。

详情

Attackers Using Image Inversion Technique to Bypass Office 365 Filtering
https://gbhackers.com/image-inversion-technique/

超过 2800 家电子商店运行过时的 Magento 软件

日期: 2020-11-11

等级: 中

来源: The Hacker News

标签: ['Magento', 'Magecart', 'Software', 'Cyberattacks']

最新研究显示，2020 年 9 月初，针对运行 Magento 1.x 电子商务平台的零售商的网络攻击浪潮被归为一个黑客组织。 该组织已经进行了多种多样的 Magecart 攻击，这些攻击通常通过诸如 Adverline 事件之类的供应链攻击，或通过利用利用诸如 9 月 Magento 攻击之类的漏洞一次入侵大量网站。 这些被称为 Cardbleed 的攻击针对了至少 2806 家运行 Magento 1.x 的在线商店。

详情

Over 2800 e-Shops Running Outdated Magento Software Hit by Credit Card Hackers
https://thehackernews.com/2020/11/over-2800-e-shops-running-outdated.html

North Face 网站遭遇了证书填充攻击

日期: 2020-11-15

等级: 中

来源: Pierluigi Paganini

标签: ['The North Face', 'Credential Stuffing Attack', 'Outdoor', 'Phishing', 'Data Breaches']

户外用品零售巨头`The North Face`在 10 月 8 日和 9 日成功进行了一次伪造凭证的攻击后，迫使一些客户重新设置了密码。 凭据填充攻击涉及僵尸网络来尝试通常通过网络钓鱼攻击和数据泄露获得的被盗登录凭据。由于用户习惯于在多个服务上重用相同的密码，因此这种攻击非常有效。 这些攻击者能够访问几位客户的账户和相关的个人信息，攻击者将其注册到 enorthface.com 网站上。

详情

The North Face website suffered a credential stuffing attack
https://securityaffairs.co/wordpress/110952/data-breach/the-north-face-credential-stuffing.html

相关安全建议

1. 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
2. 积极开展外网渗透测试工作，提前发现系统问题
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. 及时检查并删除外泄敏感数据
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

(四) 其他事件

微软前工程师因盗窃 1000 万美元被判 9 年监禁

日期: 2020-11-10

等级: 高

来源: Campbell Kwan

标签: ['Microsoft', 'Engineer', 'Prison', 'Stealing', 'Volodymyr Kvashuk']

一名前微软软件工程师因从公司盗窃超过 1000 万美元被判有期徒刑 9 年。 陪审团做出的判决发现，被指控的 Volodymyr Kvashuk 犯有 18 项重罪。其中包括 5 项电信欺诈指控，6 项洗钱指控，2 项严重身份盗窃指控，2 项虚假纳税申报单指控，以及 1 项邮件欺诈、访问

设备欺诈和访问受保护的计算机以促进欺诈的指控。 Kvashuk 在 2016 年 8 月成为一名员工之前曾担任 Microsoft 承包商的工作。在该公司发现他的盗窃行为后，他于 2018 年 6 月被解雇。

详情

Former Microsoft engineer sentenced to nine years in prison for stealing $10 million

https://www.zdnet.com/article/former-microsoft-engineer-sentence-to-nine-years-in-prison-for-stealing-10-million/

微软发布了 112 个安全漏的洞修复程序

日期: 2020-11-11

等级: 高

来源: Thomas Claburn

标签: ['Microsoft', 'Patch', 'Project Zero', 'Windows', 'Vulnerability']

2020 年 11 月 10 日，微软发布了 112 个软件漏洞的补丁，其中 17 个被评为严重漏洞。 受影响的 Microsoft 产品有 15 种，包括：Microsoft Windows, Office, Internet Explorer, Edge (EdgeHTML and Chromium), ChakraCore, Exchange Server, Dynamics, Windows Codecs Library, Azure Sphere, Windows Defender, Teams, Azure SDK, Azure DevOps, 和 Visual Studio。 其中一个已修复的漏洞正在被积极利用，即 Windows 内核加密驱动程序漏洞(CVE-2020-17087)，由谷歌的 Project Zero 在上月底披露。

详情

Microsoft emits 112 security hole fixes - including the cure for a Google-disclosed vuln exploited in the wild

https://www.theregister.com/2020/11/11/patch_tuesday_updates/

Windows 10、iOS、Chrome、Firefox 等在天府杯比赛中被安全人员攻破

日期: 2020-11-09

等级: 高

来源: The Hacker News

标签: ['Tianfu Cup', 'Pwn2Own']

来自 Adobe、苹果、谷歌、微软、Mozilla 和三星的多款软件产品在 2020 天府杯(第三届国际网络安全竞赛)上获得了前所未有的成功。 天府杯与 Pwn2Own 类似，是在 2018 年开始举办的。此前，中国政府规定，出于国家安全考虑，禁止安全研究人员参加国际黑客竞赛。 奇虎 360 的企业安全和政府(ESG)漏洞研究所以 744500 美元的奖金排名第一，其次是蚂蚁金融光年安全实验室(25.8 万美元)和安全研究员彭(9.95 万美元)。

详情

Windows 10, iOS, Chrome, Firefox and Others Hacked at Tianfu Cup Competition

https://thehackernews.com/2020/11/windows-10-ios-chrome-firefox-and.html

严重的权限提升漏洞导致 Intel 发布更新

日期: 2020-11-10

等级: 高

来源: Lindsey O'Donnell

标签: ['Intel', 'Security Update', 'Vulnerability', 'AMT', 'Escalated Privileges']

Intel 2020 年 11 月进行了一次大规模的安全更新，解决了众多产品中的漏洞，最值得注意的是，未经身份验证的攻击者可以利用这些严重漏洞来获得升级的特权。 这些严重存在于与无线蓝牙相关的产品中，包括各种 Intel Wi-Fi 模块和无线网络适配器，以及其远程带外管理工具 Active management Technology (AMT)中。 总体而言，英特尔在 2020 年 11 月 10 日发布了 40 条安全公告，每条针对各种产品的严重，高危和中危漏洞。

详情

Colossal Intel Update Anchored by Critical Privilege-Escalation Bugs
https://threatpost.com/intel-update-critical-privilege-escalation-bugs/161087/

世界上最大的 Android 电视中发现严重漏洞

日期: 2020-11-12

等级: 高

来源: GURUBARAN S

标签: ['TCL', 'Android TVs', 'Vulnerability', 'Smart TVs']

电视是娱乐、广告、新闻和体育的大众传媒。随着这项技术的出现，与 Netflix、YouTube 等应用程序一起提供的内置集成。TCL 是全球第三大电视制造商，击败了众多值得关注的竞争对手。 近日，研究人员在一份安全报告中发现，TCL Android 电视存在多个严重漏洞。

详情

Critical Vulnerabilities Discovered in World's Largest Android TVs
https://gbhackers.com/critical-vulnerabilities-discovered-in-worlds-largest-android-tvs-manufacturer/

Google 解决了两个新的 Chrome 0day 漏洞

日期: 2020-11-12

等级: 高

来源: Pierluigi Paganini

标签: ['Google', 'Chrome', 'Zero Day', 'Vulnerability']

Google 发布了 Chrome 版本 86.0.4240.198，该版本解决了另外两个在野利用的 0day 漏洞。 这个 IT 巨头在短短三周内就修复了 5 个 Chrome 0day 漏洞。 匿名来源报告了两个 0day 漏洞，分别跟踪为`CVE-2020-16013`和`CVE-2020-16017`。 `Google`专家没有透露攻击中利用这些漏洞的方式。

详情

Google addresses two new Chrome zero-day flaws
https://securityaffairs.co/wordpress/110793/hacking/google-chrome-zero-day-flaws.html

Bug hunter 因 DOD 账户接管漏洞获得“月度最佳研究员”奖

日期: 2020-11-09

等级: 中

来源: Catalin Cimpanu

标签: ['DOD', 'Vulnerability', 'Takeover', 'Hijack Account']

美国国防部已经修复了一个严重影响其内部网络的漏洞，该漏洞允许攻击者通过修改发送到国防部服务器的 web 请求中的一些参数来劫持国防部账户。 该漏洞是由美国安全公司 Silent Breach 的安全研究员 Jeff Steinburg 发现的，并通过美国国防部漏洞披露计划(VDP)进行了私下报告和补丁。 这个问题的严重程度被评为"严重(9 ~ 10)"，因为这个漏洞劫持攻击者能够攻击任何国防部帐号。 尽管该漏洞是研究人员的第一篇 DOD VDP 报告，但所报告问题的严重性使 Steinburg 获得了 DOD 的"月度最佳研究员"奖。

详情

Bug hunter wins 'Researcher of the Month' award for DOD account takeover bug

https://www.zdnet.com/article/bug-hunter-wins-researcher-of-the-month-award-for-dod-account-takeover-bug/

更新 Windows 10 以修补 Microsoft Store 游戏中的漏洞

日期: 2020-11-10

等级: 中

来源: HACKREAD

标签: ['CVE-2020-16877', 'Windows Server', 'Windows 10']

CVE-2020-16877 漏洞影响了 Windows Server 和 Windows 10，该漏洞是一个高严重性特权升级漏洞。 IOActive 网络安全研究人员披露，Windows 系统存在一个特权升级漏洞，可以通过滥用上传到微软商店的游戏来加以利用。 该漏洞编号为 CVE-2020-16877，等级为严重。 它主要影响 Windows 10 和 Windows Server。

详情

Update Windows 10 to patch vulnerability in Microsoft store games

https://www.hackread.com/update-windows-10-microsoft-store-games-vulnerability/

EA Games 的 Origin 客户端包含特权升级漏洞

日期: 2020-11-10

等级: 中

来源: Gareth Corfield

标签: ['EA Games', 'Origin Client', 'Privilege Escalation', 'Botnet']

一家英国的信息安全机构在 EA Games 的 Origin 客户端中发现了特权升级漏洞。 该漏洞可能使已接通电源的攻击者获得主机设备上的系统特权，进而使主机暴露于更高级的漏洞中，例如将其转变为僵尸网络的一部分，或安装恶意软件以削弱本地用户的信誉卡详细信息，或者您可以想象犯罪分子可能会用一台刚被盗用的机器做的任何其他事情。

详情

EA Games' Origin client contained privilege escalation vuln that anyone with user-grade access could exploit

https://www.theregister.com/2020/11/10/ea_games_origin_privesc_vuln_nettitude/

现在修补的 Ubuntu 桌面漏洞允许权限提升

日期: 2020-11-11

等级: 中

来源: Tim Anderson

标签: ['GitHub', 'Ubuntu', 'Vulnerability', 'GUI', 'Patch']

GitHub 安全研究员 Kevin Backhouse 发现了 Ubuntu 20.04（一个长期支持版本）中的漏洞，该漏洞使任何桌面用户都可以获得 root 用户访问权限， 漏洞现已修复。 该漏洞仅影响桌面用户，并且需要访问 GUI，因此在大多数情况下很难利用。 也就是说，如果安装了桌面并且用户具有一定级别的访问权限，则`Ubuntu Server`原则上可能会很容易受到攻击。 根据 Ubuntu 的注释，从 16.04 LTS 到最新的 10.10 的所有发行版都将受到影响。

详情

Now-patched Ubuntu desktop vulnerability allows privilege escalation
https://www.theregister.com/2020/11/11/ubuntu_desktop_vulnerability_allows_privilege/

相关安全建议

1. 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
2. 及时对系统及各个服务组件进行版本升级和补丁更新

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