安全事件周报

安全事件周报 (10.12-10.18)

360CERT
北京奇虎科技有限公司 | 2020-10-19

报告信息

报告名称	安全事件周报（10.12-10.18）		
报告类型	安全事件周报	报告编号	B6-2020-101903
报告版本	1.0	报告日期	2020-10-19
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	2020-10-19	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 37 项

话题集中在`网络攻击`、`勒索软件`方面，涉及的组织有：`Amazon`、`Intcomex`、`Seyfarth Shaw`、`Barnes`等。VPN 攻击事件频发，线上工作的安全保障至关重要。

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
ESET 参与全球运营以破坏 Trickbot 僵尸网络	★★★★
“柠檬鸭”加密矿僵尸网络的活动突然激增	★★★★
IAmTheKing 和 SlothfulMedia 恶意软件家族	★★★★
NPM nukes NodeJS 恶意软件使用 Windows，Linux 反向 shell	★★★★
新型不加密文件的 Android 勒索软件	★★★
BazarLoader 曾在高价值目标上部署 Ryuk 勒索软件	★★★
著名律师事务所 Seyfarth Shaw 遭到勒索软件攻击	★★★
新的 Emotet 攻击使用虚假的 Windows Update 为诱饵	★★★
数据安全	**等级**
迈阿密的科技公司遭受了 1TB 的客户和业务数据泄露	★★★★★
2020 年卫生数据泄露事件大多数为勒索所致	★★★★
研究人员发现了据称是北约和土耳其的敏感文件	★★★
卡丁论坛上发布了 300 万迪基客户的信用卡详细信息	★★★
Crytek 遭 Egregor 勒索软件击，育碧数据被泄露	★★★
网络攻击	**等级**
黑客利用 VPN 漏洞访问美国政府选举支持系统	★★★★
哈克尼遭到黑客网络攻击	★★★★
挪威称俄罗斯黑客是 8 月议会袭击的幕后黑手	★★★★
Clop 勒索软件攻击了 Software AG	★★★★
随着勒索活动的猖獗，Travelex 和其他机构面临 DDoS 威胁	★★★★
伊朗国家黑客组织与勒索软件部署有关	★★★★
严重的 Magento 代码执行漏洞威胁在线商店	★★★★

亚马逊优惠日购物者要小心欺诈网站！	★★★
Canva 设计平台被黑客用于钓鱼	★★★
据报道，5 万个家庭摄像头被黑客攻击，视频被传到网上	★★★
Barnes&Noble 受到网络攻击，可能暴露了客户数据	★★★
对伦敦议会的网络攻击仍有"重大影响"	★★★
波多黎各消防局的服务器遭到攻击	★★★
伊朗黑客组织再次以大学为目标	★★★
另一个威胁组织加入勒索软件诈骗	★★★
嘉年华公司勒索软件攻击影响了三家邮轮公司	★★★
Twitter 黑客诱使员工放弃 VPN 证书	★★★
其他事件	**等级**
SonicWall VPN 高危漏洞导致 DoS、Worming RCE	★★★★★
可以滥用 Windows Update 来执行恶意文件	★★★★
微软 10 月补丁日修复 87 个漏洞，公开披露 6 个漏洞	★★★★
Adobe 解决了 Adobe Flash Player 中的一个严重漏洞	★★★★
谷歌、英特尔警告基于 linux 的物联网设备的内核错误	★★★
Talos 专家披露了 Allen-Bradley 适配器中未修补的 DoS 漏洞	★★★
Zoom 现在支持端到端加密（E2EE）调用	★★★

三、 事件详情

(一) 恶意程序

ESET 参与全球运营以破坏 Trickbot 僵尸网络

日期: 2020-10-12

等级: 高

作者:

标签: ['ESET', 'Microsoft', 'Trickbot', 'Botnets']

ESET 已与微软、`Lumen`旗下的黑莲花实验室(`Black Lotus Labs`)、`NTT Ltd`.等合作伙伴展开合作，试图破坏`Trickbot`僵尸网络。`Trickbot`是最流行的银行恶意软件家族之一，ESET 通过提供技术分析、统计信息、已知的命令、控制服务器域名和 IP 为该项目做出了贡献。长期以来，Trickbot 一直是互联网用户的主要困扰。 ESET 于 2016 年底首次检测到 Trickbot。在这些年中，Trickbot 的漏洞不断地被报道，使其成为目前规模最大，寿命最长的僵尸网络之一。

详情

ESET takes part in global operation to disrupt Trickbot

https://www.welivesecurity.com/2020/10/12/eset-takes-part-global-operation-disrupt-trickbot/

“柠檬鸭”加密矿僵尸网络的活动突然激增

日期: 2020-10-15

等级: 高

作者:

标签: ['Cisco Talos', 'Lemon Duck', 'Botnet', 'Cryptomining', 'XMR', 'Monero', 'Covid-19']

Cisco Talos 的研究人员警告说，“柠檬鸭”加密矿僵尸网络的活动突然激增。Cisco Talos 的一份报告称，可以感染 Windows 和 Linux 设备的僵尸网络，旨在通过使用加密恶意软件`XMR`挖掘`monero`加密货币。 尽管僵尸网络早在 2018 年 12 月就已经存在，但研究人员一直在追踪 8 月以来激增的活动，僵尸网络感染了更多设备，扩大其恶意网络。2020 年 8 月，安全公司`Sophos`的一份报告指出，加密僵尸网络的运营商已经开始使用以`covid -19`为主题的电子邮件，诱使受害者打开含有恶意软件的附件。

详情

'Lemon Duck' Cryptominer Activity Spikes

https://www.databreachtoday.com/lemon-duck-cryptominer-activity-spikes-a-15186

IAmTheKing 和 SlothfulMedia 恶意软件家族

日期: 2020-10-15

等级: 高

作者:

标签: ['CISA', 'SlothfulMedia', 'IAmTheKing', 'Malware', 'Securelist', 'DHS CISA']

2020 年 10 月 1 日，`DHS-CISA`机构发布了一个名为`SlothfulMedia`的恶意软件家族的信息。2018 年 6 月，`securelist`基于未知家族的恶意软件样本中发现的恶意软件字符串，发布了有关名为`IAmTheKing`的新活动集群的第一份报告。随着时间的推移，`securelist`发现了这一攻击者使用的三种不同的恶意软件，其中之一是`SlothfulMedia`。这篇博客文章的目的是介绍所有这些攻击，并提供`securelist`能够收集到的关于攻击者兴趣的数据。

详情

IAmTheKing and the SlothfulMedia malware family

https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/

NPM nukes NodeJS 恶意软件使用 Windows，Linux 反向 shell

日期: 2020-10-16

等级: 高

作者:

标签: ['NPM', 'NodeJS', 'Malware', 'Malicious Packages', 'Sonatype']

最近，NPM 删除了其存储库上的多个包，这些包建立了与远程服务器的连接，并泄露了用户数据。 这 4 个软件包在过去的几个月里已经收集了超过 1000 总下载，直到 2020 年 10 月 15 日被 NPM 删除。 尽管 NPM 发现并删除了恶意程序包，但我能够深入到 Sonatype 的自动恶意软件检测系统档案中，以获得它们的源代码副本，因为它已经存在于 NPM 下载中。

详情

NPM nukes NodeJS malware opening Windows, Linux reverse shells

https://www.bleepingcomputer.com/news/security/npm-nukes-nodejs-malware-opening-windows-linux-reverse-shells/

新型不加密文件的 Android 勒索软件

日期: 2020-10-12

等级: 中

作者:

标签: ['Microsoft', 'Android', 'Ransomware', 'Unencrypted']

微软检测到具有新攻击技术和行为的新 Android 勒索软件，这体现了移动勒索软件的发展。 大部分勒索软件是用来加密文件的，但这个新的勒索软件不会加密文件，相反，它会通过显示一个警告屏幕来阻止访问设备。 Android 勒索软件使用一个特殊的权限系统警报窗口，在其他应用程序的顶部显示勒索通知，点击任何按钮就可以解除。 这个权限是用来通知用户的系统警报或错误，但是 Android 威胁滥用它来获得对显示器的访问。

详情

New Sophisticated Android Ransomware that Doesn't Encrypt Files

https://gbhackers.com/new-android-ransomware/

BazarLoader 曾在高价值目标上部署 Ryuk 勒索软件

日期: 2020-10-12

等级: 中

作者: Lawrence Abrams

标签: ['TrickBot', 'BazarLoader', 'Ryuk', 'Active Directory', 'Ransomware']

在部署 Ryuk 勒索软件之前，黑客团伙越来越多地使用新型的 BazarLoader 木马瞄准高价值目标。多年来，TrickBot 帮派一直使用其木马来入侵企业网络，方法是下载用于特定行为（例如窃取密码，传播到其他计算机甚至窃取域的 Active Directory 数据库）的不同软件模块。随着时间的流逝，这些模块已经得到了大量的分析，安全解决方案变得更加擅长检测这些模块。 英特尔高级安全研究人员在一份新报告中解释说，攻击者现在不再使用众所周知的`TrickBot`特洛伊木马烧死受害者，而是选择使用`BazarBackdoor`作为攻击高价值企业目标的首选工具。

详情

BazarLoader used to deploy Ryuk ransomware on high-value targets
https://www.bleepingcomputer.com/news/security/bazarloader-used-to-deploy-ryuk-ransomware-on-high-value-targets/

著名律师事务所 Seyfarth Shaw 遭到勒索软件攻击

日期: 2020-10-13

等级: 中

作者:

标签: ['Seyfarth Shaw', 'Law Firm', 'Ransomware', 'Attack']

全球领先的法律公司之一 Seyfarth Shaw 宣布，它受到了恶意软件的攻击，很可能是勒索软件的攻击。Seyfarth Shaw LLP 是一家国际 AmLaw 百强律师事务所，总部位于美国伊利诺斯州芝加哥，其客户包括财富 500 强中的 300 多家公司，其业务几乎反映了经济的各个行业和部门。Seyfarth Shaw 公司宣称自己受到了恶意软件的攻击，媒体立即报道了勒索软件的感染，该公司随后证实了此事。 根据该公司发布的一份声明，这次攻击发生在 2020 年 10 月 10 日。

详情

Leading Law firm Seyfarth Shaw discloses ransomware attack
https://securityaffairs.co/wordpress/109435/malware/seyfarth-shaw-ransomware-attack.html

新的 Emotet 攻击使用虚假的 Windows Update 为诱饵

日期: 2020-10-15

等级: 中

作者: ,Catalin Cimpanu

标签: ['Emotet', 'Botnet', 'Malspam', 'MaaS', 'Windows Update', 'lures']

在当今的网络安全领域，`Emotet`僵尸网络是`malspam`的最大来源之一。`malspam`是指发送带有恶意软件附件的电子邮件。`malspam`是支撑僵尸网络的基础，为`Emotet`机器提供新的受害者，这是一种租用给其他犯罪集团的"恶意软件即服务"(MaaS)网络犯罪活动。为了防止安全公司把他们的电子邮件标记为"恶意"或"垃圾邮件"，`Emotet`团队会定期改变这些电子邮件的发送方式以及文件附件的外观。在最近的`Emotet`活动中发送的文件附件显示一条来自 Windows 更新服务的消息，告诉用户需要更新 Office 应用程序。根据

Cryptolaemus 集团的最新消息，自 2020 年 10 月 14 起，这些`Emotet`诱饵被大量垃圾邮件发送给世界各地的用户。

详情

New Emotet attacks use fake Windows Update lures
https://www.zdnet.com/article/new-emotet-attacks-use-fake-windows-update-lures/

相关安全建议

1. 移动端不安装未知应用程序、不下载未知文件
2. 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
3. 如果允许，暂时关闭攻击影响的相关业务，积极对相关系统进行安全维护和更新，将损失降到最小
4. 网段之间进行隔离，避免造成大规模感染
5. 如果不慎勒索中招，务必及时隔离受害主机、封禁外链 ip 域名并及时联系应急人员处理
6. 条件允许的情况下，设置主机访问白名单
7. 减少外网资源和不相关的业务，降低被攻击的风险
8. 各主机安装 EDR 产品，及时检测威胁

(二) 数据安全

迈阿密的科技公司遭受了 1TB 的客户和业务数据泄露

日期: 2020-10-13
等级: 高
作者:
标签: ['Intcomex', 'Data Leak', 'Russian', 'Database', 'Hacker Forum']

位于迈阿密的增值解决方案和技术产品公司`Intcomex`遭遇重大数据泄露，近`1TB`的用户数据泄露。泄露的数据包括信用卡、护照和执照扫描、个人数据、工资单、财务文档、客户数据库、员工信息等。 部分数据是在俄罗斯一个流行的黑客论坛上免费泄露的，第一部分于 2020 年 9 月 14 日公开，第二部分于 2020 年 9 月 20 日公开。

详情

Miami-based tech company suffers massive 1TB customer and business data leak
https://cybernews.com/security/miami-based-tech-company-suffers-massive-1tb-data-leak/

2020 年卫生数据泄露事件大多数为勒索所致

日期: 2020-10-13
等级: 高

作者:

标签: ['Blackbaud', 'Magellan Health', 'Ransomware', 'Data Breach', 'HIPAA']

涉及勒索软件攻击的黑客事件继续占据 2020 年健康数据泄露的主导地位，Blackbaud 和 Magellan health 这两家公司的事件导致了他们客户的大量泄露。 截至 2020 年 10 月 13 日，美国卫生与公众服务部(Department of Health and Human Services)的 HIPAA 泄漏报告工具网站显示，2020 年迄今为止最大的健康数据泄露事件中，绝大多数是勒索软件攻击。 在联邦政府公布的 2020 年迄今为止 10 起最大的健康数据黑客事件中，有 9 起与勒索软件事件有关，涉及筹款软件提供商 Blackbaud 和管理健康公司 Magellan Health。

详情

Health Data Breaches in 2020: Ransomware Incidents Dominate

https://www.databreachtoday.com/health-data-breaches-in-2020-ransomware-incidents-dominate-a-15170

研究人员发现了据称是北约和土耳其的敏感文件

日期: 2020-10-12

等级: 中

作者:

标签: ['Cyble', 'NATO', 'Turkey', 'Leaked', 'Havelsan']

来自美国 Cyble 公司的研究人员最近发现了一个匿名威胁者分享的帖子，他在网上的名字是 Spectre123，据说他泄露了北约和 Havelsan(土耳其军事/国防制造商)的敏感文件。Cyble 分析了泄露的敏感文件，并报告说，这些文件包括工作文件、建议书、合同、3d 设计、简历、包含原材料信息的 excel 表和财务报表。目前尚不清楚这些攻击者是出于网络间谍目的还是黑客行动主义的目的，泄露信息的内容表明这是黑客活动分子的工作，但不能排除这是民族国家行为的结果。

详情

Researchers found alleged sensitive documents of NATO and Turkey

https://securityaffairs.co/wordpress/109386/breaking-news/nato-turkey-data-leak.html

卡丁论坛上发布了 300 万迪基客户的信用卡详细信息

日期: 2020-10-15

等级: 中

作者: ,Catalin Cimpanu

标签: ["Dickey's barkerpit", "Joker's Stash", 'Card', 'Gemini Advisory']

美国最大的烧烤连锁店迪基烧烤坑（`Dickey's barkerpit`）超过 300 万顾客的信用卡详细信息已被公布在一个名为`Joker's Stash`的卡片作假市场上。这一发现是由追踪金融欺诈的网络安全公司`Gemini Advisory`发现的。这些信用卡数据似乎是在 2019 年 7 月至 2020 年 8 月期间收集的。支付卡记录大多是针对使用过时磁条技术的卡，以每张卡 17 美元的中间价出售。

详情

Card details for 3 million Dickey's customers posted on carding forum

https://www.zdnet.com/article/card-details-for-3-million-dickeys-customers-posted-on-carding-forum/

Crytek 遭 Egregor 勒索软件击，育碧数据被泄露

日期: 2020-10-15

等级: 中

作者: ,Lawrence Abrams

标签: ['Crytek', 'Ubisoft', 'Egregor', 'Ransomware', 'Data leaked']

Egregor 勒索软件团伙对游戏开发商 Crytek 发起了一场勒索软件攻击，并泄露了他们声称从育碧网络窃取的文件。育碧和`Crytek`都是著名的游戏开发商，公司总部分别位于法国和德国。`Egregor`勒索软件游戏发布了包含未加密文件的档案，声称这些档案是在不相关的攻击中从`Ubisoft`和`Crytek`窃取的。

详情

Crytek hit by Egregor ransomware, Ubisoft data leaked

https://www.bleepingcomputer.com/news/security/crytek-hit-by-egregor-ransomware-ubisoft-data-leaked/

相关安全建议

1. 及时检查并删除外泄敏感数据
2. 严格控制数据访问权限
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

(三) 网络攻击

黑客利用 VPN 漏洞访问美国政府选举支持系统

日期: 2020-10-12

等级: 高

作者: Sergiu Gatlan

标签: ['US', 'VPN', 'Elections', 'Govt', 'Vulnerability', 'Zerologon']

黑客通过将 VPN 漏洞和最近的 Windows CVE-2020-1472 安全漏洞结合在一起，攻击并获得了对美国选举支持系统的访问权。美国网络安全和基础设施安全局(CISA)表示，高级持续威胁(APT)参与者经常使用这种漏洞组合策略，来攻击联邦和 SLTT(州、地方、部落和领土)政府网络，以及选举组织和基础设施。

详情

Hackers used VPN flaws to access US govt elections support systems

https://www.bleepingcomputer.com/news/security/hackers-used-vpn-flaws-to-access-us-govt-elections-support-systems/

哈克尼遭到黑客网络攻击

日期: 2020-10-13

等级: 高

作者: Gareth Corfield

标签: ['Hackney Council', 'the National Cyber Security Centre', 'Cyberattack', 'London']

位于伦敦东部的哈克尼委员会（Hackney Council）宣布已受到了"网络攻击"，但当局和国家网络安全中心（NCSC）的官员对实际发生的事情仍然守口如瓶。当地市长菲利普·格兰维尔（Philip Glanville）于 2020 年 10 月 13 日在议会网站上发表声明说："哈克尼委员会一直是网络攻击的目标，这正影响哈克尼的许多服务和 IT 系统。"令公众担忧的是，该委员会和 NCSC 似乎都无法控制上述"网络攻击"。

详情

Hackers hack Hackney: Local government cries 'cyberattack' while UK infosec officials rush to figure out what happened

https://www.theregister.com/2020/10/13/hackney_council_hacked_hackers_cyberhack/

挪威称俄罗斯黑客是 8 月议会袭击的幕后黑手

日期: 2020-10-13

等级: 高

作者: Sergiu Gatlan

标签: ['Norway', 'Russia', 'Cyberattack', 'Parliament']

挪威外交部长伊恩·埃里克森·瑟里德在 2020 年 10 月 13 日说，俄罗斯是 2020 年 8 月挪威议会遭到网络攻击的幕后黑手。瑟里德在 2020 年 10 月 13 日早些时候发布的新闻稿中说："8 月 24 日，挪威议会宣布他们的电子邮件系统出现数据泄露"，此前的简报也包括国防部长弗兰克·巴克克·詹森。"根据政府拥有的信息基础，他们认为俄罗斯是这一活动的幕后黑手。"瑟里德还说："这是一个严重的事件，影响到挪威最重要的民主制度。"

详情

Norway says Russian hackers were behind August Parliament attack

https://www.bleepingcomputer.com/news/security/norway-says-russian-hackers-were-behind-august-parliament-attack/

Clop 勒索软件攻击了 Software AG

日期: 2020-10-13

等级: 高

作者:

标签: ['Software AG', 'Cloud', 'Ransomware', 'Clop', 'Data Leak']

Clop 和该组织的标志性恶意软件再次发动攻击，这次攻击的目标是德国软件集团公司(software AG`)。据报道，到目前为止，该公司并没有支付 2300 万美元的巨额赎金。2020 年 10 月 11 日，该公司证实，这些攻击者正在公布公司数据。 10 月初，网络攻击者成功侵入了该公司的系统。该公司在 10 月 5 日发布了一份声明，公开承认了这次攻击，并补充说，"尽管为其客户提供的服务（包括基于云的服务）不受影响，但是，Software AG 已按照受控方式关闭了内部系统，遵守公司的内部安全规定"。

详情

Software AG Data Released After Clop Ransomware Strike - Report
https://threatpost.com/software-ag-data-clop-ransomware/160042/

随着勒索活动的猖獗，Travelex 和其他机构面临 DDoS 威胁

日期: 2020-10-14

等级: 高

作者:

标签: ['Travelex', 'DDoS', 'BTC', 'Email', 'Orgs']

世界各地的公司不断收到勒索电子邮件，威胁在其网络上发动分布式拒绝服务（DDoS）攻击，除非他们支付赎金，据报道，英国外汇公司`Travelex`是最近备受关注的威胁接收者之一。研究人员说，自 8 月中旬以来，已经有几家公司收到电子邮件，警告称他们的公司网络将在大约一周内受到 DDoS 攻击。研究人员说，最初的赎金要求定为 20 BTC（在撰写本文时约合 23 万美元），网络犯罪分子威胁说，如果没有支付赎金，每天的赎金将增加 10 BTC。

详情

Travelex, Other Orgs Face DDoS Threats as Extortion Campaign Rages On
https://threatpost.com/travelex-ddos-extortion-campaign/160110/

伊朗国家黑客组织与勒索软件部署有关

日期: 2020-10-15

等级: 高

作者: ,Catalin Cimpanu

标签: ['Thanos', 'Iranian', 'Ransomware', 'MuddyWater', 'Phishing']

安全研究人员说，他们发现了将最近的袭击和 Thanos 勒索软件和伊朗国家资助的黑客组织联系起来的线索。ClearSky 和 Profero 的安全研究人员在调查几家以色列知名组织的安全事件时表示，他们将这次入侵与`MuddyWater`联系了起来，后者是一个由伊朗政府支持的黑客组织。`MuddyWater`将使用带有恶意`Excel`或`PDF`文件的钓鱼邮件，这些邮件打开后将从黑客的服务器下载并安装恶意软件。在第二种情况下，`MuddyWater`将扫描 Internet 上未打补丁的 Microsoft Exchange 电子邮件服务器，利用 CVE-2020-0688 漏洞，在服务器上安装 Web Shell，然后下载并安装以前看到的相同恶意软件。

详情

Iranian state hacker group linked to ransomware deployments
https://www.zdnet.com/article/iranian-state-hacker-group-linked-to-ransomware-deployments/

严重的 Magento 代码执行漏洞威胁在线商店

日期: 2020-10-15

等级: 高

作者:

标签: ['Magento', 'Adobe', 'Magecart', 'Vulnerability', 'Code Execution']

Adobe 电子商务平台 Magento 经常成为 Magecart 威胁组织等攻击者的攻击目标。Magento 的两个严重漏洞可能使受影响的系统能够任意执行代码。从亚马逊优惠日(Amazon Prime Day)到 11 月的 Black Friday，零售业将在未来几个月内迎来繁荣。这将给 Adobe 带来压力，迫使其迅速修补流行的`Magento`开源平台上的漏洞。其中最严重的漏洞包括允许任意代码执行的漏洞。 该问题源于使用"allow list"方法检查文件扩展名时应用程序未验证完整文件名。 这可能使攻击者可以绕过验证并上传恶意文件。

详情

Critical Magento Holes Open Online Shops to Code Execution
https://threatpost.com/critical-magento-holes-online-shops-code-execution/160181/

亚马逊优惠日购物者要小心欺诈网站!

日期: 2020-10-13

等级: 中

作者:

标签: ['Amazon', 'Phishing', 'Fraudulent Sites', 'Prime day']

Amazon Prime Day 交易将于 2020 年 10 月 14 日开始，然而攻击者使用 Amazon 品牌和徽标进行了网络钓鱼和欺诈活动。 最近几天，使用亚马逊品牌和标志的欺诈网站注册数量激增，据研究人员在过去 30 天里的研究数据显示，注册的包含"亚马逊"一词的域名比 2020 年 9 月增加了 21%。 安全研究人员称，8 月份亚马逊新的钓鱼和欺诈网站急剧增加，9 月份又增加了 2.5 倍。攻击者试图复制亚马逊网站的页眉和页脚布局、字体和尺寸来欺骗购物者。黑客试图引诱受害者，他们窃取最敏感的数据，如信用卡信息、姓名、生日、电子邮件和实际地址以及其他详细信息。

详情

Amazon Prime Day shoppers Beware!- Attackers Creating Fraudulent Sites
https://gbhackers.com/amazon-prime-day-scams/

Canva 设计平台被黑客用于钓鱼

日期: 2020-10-14

等级: 中

作者: Lawrence Abrams

标签: ['Canva', 'Platform', 'Phishing', 'HTML']

免费的图形设计网站 Canva 被攻击者滥用，以创建和托管复杂的网络钓鱼登陆页面。Canva 是一个图形设计平台，它允许用户创建海报、信头、节日贺卡和其他数字媒体，然后可以下载为图像，通过可点击的链接以 HTML 格式共享或打印。作为其服务的一部分，设计师可以生成可共享的 url，以便朋友和同事可以在 canva.com 上查看他们的作品。当共享设计时，点击链接的用户将看到一个完整的页面，并能够与任何嵌入的链接或表单交互。 在网络安全公司 Cofense 的一份新报告中，攻击者越来越多地使用 Canva 来创建托管的 HTML 登录页，然后用于将钓鱼受害者重定向到伪造的登录表单。

详情

Canva design platform actively abused in credentials phishing
https://www.bleepingcomputer.com/news/security/canva-design-platform-actively-abused-in-credentials-phishing/

据报道，5 万个家庭摄像头被黑客攻击，视频被传到网上

日期: 2020-10-14

等级: 中

作者:

标签: ['ESET', 'Home Cameras ', 'Singapore', 'Private Video']

一个黑客团队声称，他们已经攻破了 5 万多个家庭安全摄像头，并将其中一些视频上传到了网上。虽然相当一部分视频似乎来自新加坡，但泰国、韩国和加拿大的人们似乎也受到了侵犯。一些视频的长度从一到二十分钟不等，展示了不同年龄段的人在不同的姿势或不同的脱衣阶段，已经被上传到色情网站。报道这一消息的新报纸援引不具名的黑客组织的话说，他们已经与 70 多名会员分享了这些视频片段，这些成员支付了 150 美元终身使用这些赃物。

详情

50,000 home cameras reportedly hacked, footage posted online

https://www.welivesecurity.com/2020/10/14/50000-home-cameras-reportedly-hacked-footage-posted-online/

Barnes&Noble 受到网络攻击，可能暴露了客户数据

日期: 2020-10-14

等级: 中

作者: Lawrence Abrams

标签: ['Barnes & Noble', 'Cyberattack', 'BleepingComputer', 'Customer Data']

`Barnes&Noble`透露，他们是一次网络攻击的受害者，该攻击可能暴露了客户的数据。`Barnes&Noble`是美国最大的零售连锁书店，以大型的实体零售书店闻名。 在一封 2020 年 10 月 14 日深夜发给客户的电子邮件中，BleepingComputer 看到了 Barnes&Noble 披露，他们在 2020 年 10 月 10 日遭受了一次网络攻击。作为这次攻击的一部分，攻击者获得了公司使用的公司系统的访问权。Barnes&Noble 表示，目前还没有披露任何支付细节，但目前还不确定黑客是否访问了其他个人信息。

详情

Barnes&Noble Noble hit by cyberattack that may have exposed customer data

https://www.bleepingcomputer.com/news/security/barnes-and-noble-hit-by-cyberattack-that-may-have-exposed-customer-data/

对伦敦议会的网络攻击仍有“重大影响”

日期: 2020-10-15

等级: 中

作者: ,Steve Ranger

标签: ['London', 'Cyberattack', 'Council']

2020 年 10 月早些时候，北伦敦议会表示，它受到了严重的网络攻击，许多服务和 it 系统受到影响。这次袭击继续对市政服务产生重大影响，议会要求居民除非绝对必要，否则不要与议会联系。

详情

Cyberattack on London council still having 'significant impact'

https://www.zdnet.com/article/cyber-attack-on-london-council-still-having-significant-impact/

波多黎各消防局的服务器遭到攻击

日期: 2020-10-15

等级: 中

作者:

标签: ['Puerto Rico', 'Firefighting Department', 'Ransom', 'Encrypted']

据国防部主任阿尔贝托·克鲁兹说，该部应对紧急情况的能力没有受到袭击的影响。国防部收到了一封来自攻击者的电子邮件，通知他们已经加密了服务器，并要求支付赎金才能释放他们。当地警方对此事件展开调查，而该部门决定不支付赎金。

详情

Crooks hit Puerto Rico Firefighting Department Servers

https://securityaffairs.co/wordpress/109551/hacking/puerto-rico-firefighting-department-attack.html

伊朗黑客组织再次以大学为目标

日期: 2020-10-15

等级: 中

作者:

标签: ['Iran', 'U.S.', 'Malwarebytes', 'TA407', 'Cobalt Dickens', 'Silent Librarian']

据安全公司 Malwarebytes 的研究人员称，一个被怀疑与伊朗政府有关联的黑客组织再次将美国和世界各地的大学作为攻击目标。 “沉默的图书馆员”，也被称为 TA407 和 Cobalt Dickens，目标是学术机构窃取知识产权和研究文件。Malwarebytes 的报告称，黑客组织的活动始于 2013 年，通常从 9 月新学年开始。 Malwarebytes 报告指出，由于许多学校和大学在 2020 年秋天提供虚拟课程，黑客组织已经修改了其钓鱼邮件和其他技术，以攻击远程学生和大学工作人员。

详情

Iranian Hacking Group Again Targets Universities

https://www.databreachtoday.com/iranian-hacking-group-again-targets-universities-a-15182

另一个威胁组织加入勒索软件诈骗

日期: 2020-10-15

等级: 中

作者:

标签: ['FireEye Mandiant', 'FIN11', 'Clop', 'Ransomware', 'Malware']

据火眼 Mandiant 的研究人员称，一个名为“FIN11”的新发现的以经济为动机的威胁集团正在部署`Clop`勒索软件，从目标那里窃取数据，以进行敲诈。 Mandiant 威胁情报公司（Mandiant Threat Intelligence）的分析师吉纳维耶夫·斯塔克（Genevieve Stark）说，

FIN11 最近增加了活动，并扩展到勒索软件、数据盗窃和勒索活动（参见：更多勒索软件团伙以数据泄露威胁受害者）。斯塔克说："虽然 FIN11 没有表现出高度的技术成熟度，但这并没有阻止它们影响到许多跨行业和地理区域的组织。"。多年来，FireEye Mandiant 观察到了从 FIN11 开始的突发性活动，然后是可以持续数月的平静期。例如，在 3 月至 5 月期间，该组织似乎停止了所有的计划。但现在，黑客在一周内进行了多达 5 次的恶意攻击。

详情

Another Threat Group Joins Ransomware Extortion Racket

https://www.databreachtoday.com/another-threat-group-joins-ransomware-extortion-racket-a-15183

嘉年华公司勒索软件攻击影响了三家邮轮公司

日期: 2020-10-15

等级: 中

作者:

标签: ['Carnival Corp', 'Ransomware', 'Cruise Lines', 'Attack']

据有关官员证实，8 月 15 日，美国嘉年华公司(Carnival Corp.)遭遇勒索软件攻击，黑客侵入了三家邮轮品牌以及该公司赌场业务的客人、员工和船员的个人信息。 该公司最近在最新情况中表示，嘉年华邮轮公司、荷兰美洲邮轮公司和 Seabourn 是受袭击影响的品牌，嘉年华仍在调查中。 嘉年华一直在与网络安全顾问合作，以恢复其文件，并认为"滥用数据的可能性很小"。 嘉年华在事件发生两天后，也就是 8 月 17 日，就已经透露自己成了勒索软件攻击的目标。当时，该公司承认黑客侵入并加密了某品牌的部分信息技术系统，以及从该公司下载的数据文件。

详情

Carnival Corp. Ransomware Attack Affects Three Cruise Lines

https://threatpost.com/carnival-corp-ransomware-attack-cruise/160134/

Twitter 黑客诱使员工放弃 VPN 证书

日期: 2020-10-16

等级: 中

作者:

标签: ['Twitter', 'VPN', 'Phishing', 'IT']

2020 年 7 月入侵`Twitter`的攻击者假装从`Twitter`的 IT 部门打电话询问 VPN 问题，然后说服员工在一个看起来与真实 VPN 登录站点完全相同的网站上输入他们的证书。纽约金融服务部(NYDFS)的一份报告发现，黑客们的说法是可信和成功的，因为 Twitter 的员工都在使用 VPN 连接工作，经常会遇到需要 IT 支持的 VPN 问题。 Twitter 黑客似乎还进行了研究，以确定 Twitter 员工的基本职能和职务，以便他们可以更好地模仿 Twitter 的 IT 部门。

详情

Twitter hackers lured employees to give up VPN Credentials

https://www.scmagazine.com/home/security-news/twitter-hackers-lured-employees-to-give-up-vpn-credentials/

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. 注重内部员工安全培训
3. 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
4. 如果允许，暂时关闭攻击影响的相关业务，积极对相关系统进行安全维护和更新，将损失降到最小
5. 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
6. 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
7. 积极开展外网渗透测试工作，提前发现系统问题
8. 做好文件（尤其是新修改的文件）检测
9. 统一 web 页面报错信息，避免暴露敏感信息
10. 合理设置服务器端各种文件的访问权限

(四) 其他事件

SonicWall VPN 高危漏洞导致 DoS、Worming RCE

日期: 2020-10-14

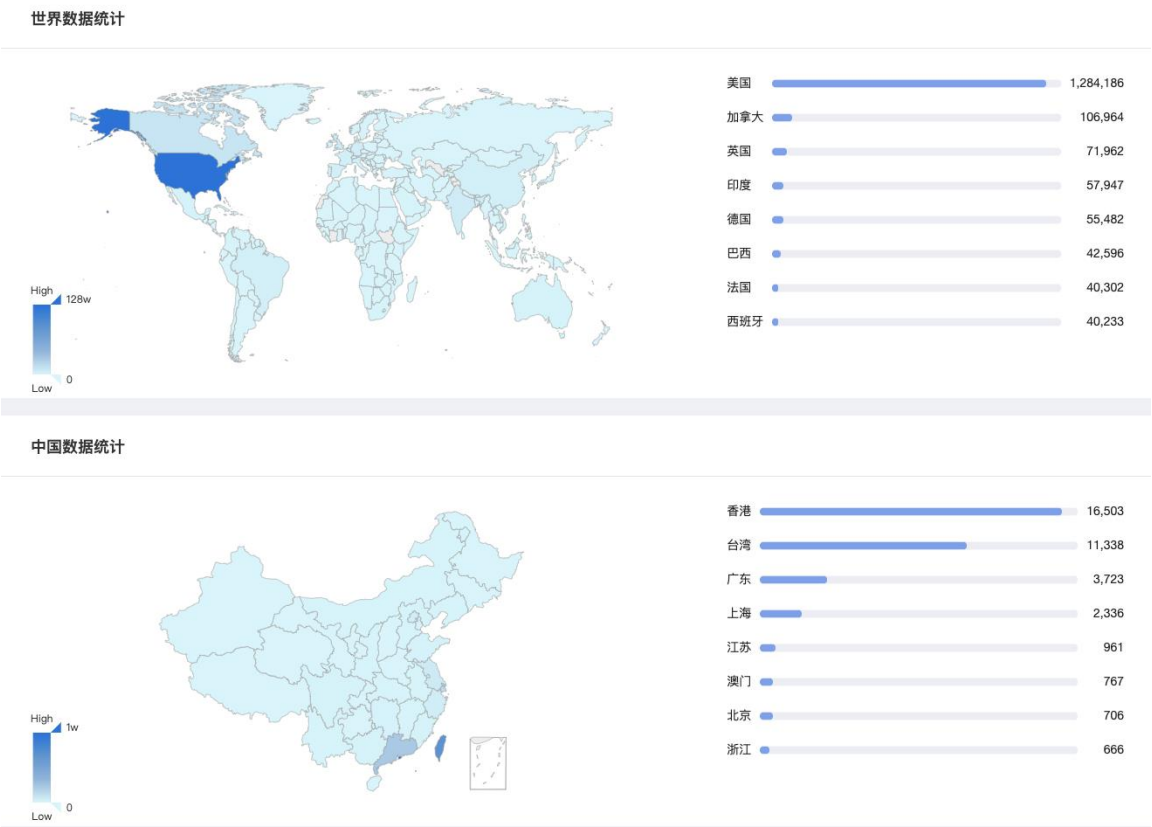
等级: 高

作者:

标签: ['RCE', 'Vulnerability', 'SonicWall VPN', 'SSLVPN', 'Buffer Overflow']

SonicWall VPN 中的一个高危安全漏洞可用于使设备崩溃并阻止用户连接到公司资源。研究人员说，它还可以打开远程代码执行（RCE）的大门。该漏洞（CVE-2020-5135）是`SonicWall Network Security Appliance（NSA`中基于堆栈的缓冲区溢出。据`Tripwire`的研究人员发现，该漏洞存在于用于产品管理和`sslvpn`远程访问的`HTTP/HTTPS`服务中。

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



详情

Critical SonicWall VPN Portal Bug Allows DoS, Worming RCE
https://threatpost.com/critical-sonicwall-vpn-bug/160108/

可以滥用 Windows Update 来执行恶意文件

日期: 2020-10-12

等级: 高

作者: Sergiu Gatlan

标签: ['Windows Update', 'Command', 'LoLBins', 'WDAC', 'UAC', 'Bypass']

Windows Update 客户端被添加到攻击者的远程二进制文件（LoLBins）列表，该列表可用于在 Windows 系统上执行恶意代码。LoLBins 是微软签署的可执行文件(预安装或下载)，可以被攻击者滥用，在下载、安装或执行恶意代码时逃避检测。 它们还可以被攻击者用来绕过 Windows 用户帐户控制(UAC)或 Windows 防御应用程序控制(WDAC)，并在已经受损的系统上获得持久性。

详情

Windows Update can be abused to execute malicious files
https://www.bleepingcomputer.com/news/security/windows-update-can-be-abused-to-execute-malicious-files/

微软 10 月补丁日修复 87 个漏洞，公开披露 6 个漏洞

日期: 2020-10-13

等级: 高

作者: Lawrence Abrams

标签: ['Microsoft', 'Patch Tuesday', 'Adobe', 'Windows', 'Vulnerabilities']

随着微软 2020 年 10 月补丁日安全更新发布，微软发布了其产品中 87 个漏洞的修复程序，并发布了关于 2020 年 10 月 13 日 Adobe Flash Player 更新的建议。在 2020 年 10 月 13 日修复的 87 个漏洞中，12 个被列为严重漏洞，74 个被列为重要漏洞，1 个被列为中等漏洞。

详情

Microsoft October Patch Tuesday fixes 87 bugs, six publicly disclosed

https://www.bleepingcomputer.com/news/security/microsoft-october-patch-tuesday-fixes-87-bugs-six-publicly-disclosed/

Adobe 解决了 Adobe Flash Player 中的一个严重漏洞

日期: 2020-10-13

等级: 高

作者:

标签: ['Adobe', 'Adobe Flash Player', 'Remote Code Execution', 'Vulnerability']

Adobe 发布了一个安全更新来解决 Adobe Flash Player (CVE-2020-9746)中一个严重的远程代码执行漏洞，该漏洞可能会被攻击者通过欺骗受害者访问一个网站来利用。攻击者在 HTTP 响应中插入恶意字符串后，不知情的用户访问网站，即可触发此漏洞。

详情

Adobe addresses a critical security flaw in Adobe Flash Player

https://securityaffairs.co/wordpress/109448/hacking/adobe-flash-player-critical-flaw.html

谷歌、英特尔警告基于 linux 的物联网设备的内核错误

日期: 2020-10-14

等级: 中

作者:

标签: ['Google', 'Intel', 'BlueZ', 'IoT', 'Linux', 'BleedingTooth', 'Vulnerability']

Google 和 Intel 警告 BlueZ 存在严重漏洞，BlueZ 是一个 Linux 蓝牙协议栈，为基于 Linux 的物联网（IoT）设备提供核心蓝牙层和协议支持。根据 Google 的说法，该漏洞影响到支持 BlueZ 的 5.9 版之前的 Linux 内核版本的用户。BlueZ 是一个在 GNU 通用公共许可证（GPL）下发布的开源项目，它的特点是 BlueZ 内核，从 2.4.6 版起就成为正式 Linux 内核的一部分。谷歌称之为“BleedingTooth”，改漏洞可由本地未经验证的攻击者通过精心编制的输入进行“Zero-Click”攻击。这允许攻击者在受影响设备上升级权限。

详情

Google, Intel Warn on 'Zero-Click' Kernel Bug in Linux-Based IoT Devices

https://threatpost.com/google-intel-kernel-bug-linux-iot/160067/

Talos 专家披露了 Allen-Bradley 适配器中未修补的 DoS 漏洞

日期: 2020-10-14

等级: 中

作者:

标签: ['Cisco Talos', 'Rockwell Automation', 'DoS', 'Vulnerabilities', 'Buffer Overflow']

Cisco Talos 的一名研究人员公布了，罗克韦尔自动化公司生产的工业自动化产品中，几个可远程利用的拒绝服务（DoS）漏洞的技术细节。受该漏洞影响的产品是`Allen-Bradley 1794-AENT Flex I/O series B`适配器，问题存在于以太网、IP 请求路径端口/数据、逻辑段功能中。Cisco Talos 研究人员发现了五个严重程度高的缓冲区溢出漏洞，这些漏洞影响运行 4.003 及更早版本的 Allen Bradley 设备。

详情

Talos experts disclosed unpatched DoS flaws in Allen-Bradley adapter
https://securityaffairs.co/wordpress/109480/ics-scada/allen-bradley-adapter-dos-flaws.html

Zoom 现在支持端到端加密（E2EE）调用

日期: 2020-10-15

等级: 中

作者:

标签: ['Video', 'Zoom', 'E2EE', 'Encrypted']

视频会议平台 Zoom 宣布了端到端加密（E2EE）的实现，并于 2020 年 10 月 19 日开始提供。有了 E2EE，用户将能够生成单独的加密密钥，并使用它们来保护语音或视频通话，加密保护它们不被窃听。用户使用公钥加密将密钥分发给其他会议参与者。软件将在本地存储密钥，不会与公司服务器共享。这种设计选择旨在确保变焦本身不能窃听通信。想要保护与 E2EE 的通信的用户必须更新他们的客户端，并从他们的帐户启用对 E2EE 调用的支持。

详情

Zoom now supports end-to-end encrypted (E2EE) calls
https://securityaffairs.co/wordpress/109523/security/zoom-e2ee-calls.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