安全事件周报

安全事件周报 (11.16-11.22)

360CERT

360CERT
北京奇虎科技有限公司 | 2020-11-23

报告信息

报告名称	安全事件周报（11.16-11.22）		
报告类型	安全事件周报	报告编号	B6-2020-112301
报告版本	1.0	报告日期	2020-11-23
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	2020-11-23	360CERT	360CERT	撰写报告

360CERT

目录

360CERT

一、 事件概览

本周收录安全事件 38 项

话题集中在`网络攻击`、`勒索软件`方面，涉及的组织有：`Capcom`、`Manchester United`、`Americold`、`Mitsubishi`等。漏洞扫描肆掠，快速实施补丁升级是重中之重。

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**
Capcom 游戏玩家信息数据泄露	★★★★
成人网站用户被 ZLoader 恶意软件通过假 Java 更新进行攻击	★★★★
Chaes 恶意软件攻击拉丁美洲最大电子商务平台的客户	★★★★
WFH 导致针对制药公司的移动网络钓鱼和恶意软件攻击激增	★★★★
REvil 勒索软件攻击 Managed.com 主机提供商，五十万赎金	★★★★
研究人员发现新的 Grelos skimmer 变种	★★★★
韩国的供应链遭到 Lazarus 攻击	★★★
COVID-19 抗原公司受到恶意软件攻击	★★★
Egregor 勒索软件攻击受害者的打印机	★★★
Qbot Banking 特洛伊木马程序现在正在部署 Egregor 勒索软件	★★★
TrickBot turns 100：最新发布的具有新功能的恶意软件	★★★
数据安全	**等级**
暴露的数据库显示有超过 10 万个 Facebook 账户被泄露	★★★★
Liquid 货币交易所称黑客进入内部网络，窃取用户数据	★★★★
新南威尔士州预计网络攻击将使其损失 700 万澳元的法律和调查费用	★★★
网络攻击	**等级**
三菱电机公司受到新的网络攻击	★★★★★
针对 Intel SGXSecurity 事务的基于硬件的故障注入攻击	★★★★
装有 Epsilon 框架主题的 WordPress 网站成为大规模攻击的目标	★★★★
office365 钓鱼活动使用重定向 url 和检测沙箱来逃避检测	★★★★
乔·拜登的"Vote Joe"网站被土耳其黑客攻击	★★★★
曼联遭遇网络攻击	★★★★

360CERT

网络攻击使圣约翰市的 IT 基础设施瘫痪	★★★★
新的 skimer 攻击使用 WebSockets 来逃避检测	★★★
冷库巨头 Americold 服务受到网络攻击的影响	★★★
黑客组织利用 ZeroLogon 在汽车行业发动攻击	★★★
黑客攻击 49000 多个存在漏洞的 Fortinet VPN	★★★
其他事件	**等级**
警告：GO SMS Pro 应用程序中未修补的漏洞会暴露数百万条媒体消息	★★★★★
Ticketmaster 因数据安全故障被罚款 170 万美元	★★★★
超过 245000 个 Windows 系统仍然容易受到 BlueKeep RDP 漏洞的攻击	★★★★
多家工业控制系统供应商警告存在严重漏洞	★★★★
Facebook Messenger 漏洞可以让黑客在你接电话之前监听你	★★★★
AWS 漏洞允许攻击者查找用户的 Access Codes	★★★★
交友网站 Bumble 为 1 亿用户提供了不安全的刷卡服务	★★★
澳大利亚 BitConnect 发起人因涉嫌密码诈骗被起诉	★★★
macOS Big Sur 上的某些 Apps 绕过了内容过滤器和 VPN	★★★
Cisco 在 PoC 攻击代码发布后修补了严重漏洞	★★★
Cisco Webex 漏洞允许攻击者作为虚假用户加入会议	★★★
防范 DNS 欺骗:发现缓存投毒漏洞	★★★
VMware 修复了天府杯白帽黑客大赛上发现的 hypervisor 漏洞	★★★

360CERT

三、 事件详情

(一) 恶意程序

Capcom 游戏玩家信息数据泄露

日期: 2020-11-16

等级: 高

来源: Lawrence Abrams

标签: ['Capcom', 'Game Giant', 'Japanese', 'Ragnar Locker', 'Ransomware', 'Data Breach']

日本游戏巨头 Capcom 在确认攻击者在最近的一次勒索软件攻击中窃取了用户和员工的敏感信息后，宣布发生数据泄露事件。 如果你是玩街机游戏或电子游戏长大的，那么 Capcom 就是知名游戏的开发商，包括《街头霸王》、《生化危机》、《幽灵与妖精》、《鬼泣》和《洛克人》。 在 2020 年 11 月 2 日，Capcom 受到了网络攻击，导致他们关闭了部分网络以阻止病毒的传播。一名安全研究人员发现了用于攻击的恶意软件样本后，很快就得知 Ragnar Locker 勒索软件行动导致了 Capcom 的网络攻击。

详情

Capcom confirms data breach after gamers' info stolen in cyberattack

https://www.bleepingcomputer.com/news/security/capcom-confirms-data-breach-after-gamers-info-stolen-in-cyberattack/

成人网站用户被 ZLoader 恶意软件通过假 Java 更新进行攻击

日期: 2020-11-17

等级: 高

来源: Ionut Ilascu

标签: ['ZLoader', 'Malsmoke', 'Malware', 'Fake Java update']

自 2020 年年初以来一直在进行的恶意软件运动最近改变了策略，从漏洞利用工具包转变为社会工程学，以成人内容消费者为目标。 运营商使用一种古老的技巧来分发 ZLoader 恶意软件的变种，这是一种银行木马，在缺席了将近两年之后于 2020 年早些时候卷土重来，现在用作信息窃取。 该活动被安全研究人员命名为 Malsmoke，主要针对人流量高的成人网站，例如 xHamster，吸引了数亿每月的访问者。 另一个网站是 Bravo Porn Tube，每月有超过 800 万的访问者。

详情

Adult site users targeted with ZLoader malware via fake Java update

https://www.bleepingcomputer.com/news/security/adult-site-users-targeted-with-zloader-malware-via-fake-java-update/

Chaes 恶意软件攻击拉丁美洲最大电子商务平台的客户

日期: 2020-11-18

等级: 高

来源: Charlie Osborne

标签: ['Chaes', 'MercadoLivre', 'Latin America', 'Malware']

在针对拉丁美洲电子商务客户的广泛攻击中，发现了此前未知的恶意软件。 该恶意软件被 Cybereason Nocturnus 研究人员称为 Chaes，目前正由攻击者在整个 LATAM 地区部署，以窃取财务信息。 网络安全团队在 2020 年 11 月 18 日的博客文章中说，该地区最大的电子商务公司 MercadoLivre 的巴西客户是信息窃取恶意软件的重点。

详情

Chaes malware strikes customers of Latin America's largest e-commerce platform

https://www.zdnet.com/article/chaes-malware-strikes-customers-of-latin-americas-largest-e-commerce-platform/

WFH 导致针对制药公司的移动网络钓鱼和恶意软件攻击激增

日期: 2020-11-18

等级: 高

来源: Danny Palmer

标签: ['Pharmaceuticals', 'COVID-19', 'Phishing', 'Malware']

网络攻击者越来越多地追击制药行业，他们针对员工开展网络钓鱼和恶意软件活动，专门利用智能手机和平板电脑的潜在安全漏洞。 目前，制药是一个极为引人注目的目标，因为制药公司试图开发一种针对 COVID-19 的疫苗，而且已经有记录表明，有国家支持的黑客活动试图窃取医学研究机构的知识产权。 移动网络安全公司 Lookout 的研究人员说，2020 年以来，针对制药员工的移动网络钓鱼攻击激增，因为网络犯罪分子试图获取敏感数据。

详情

WFH leads to surge in mobile phishing and malware attacks targeting pharmaceuticals companies

https://www.zdnet.com/article/wfh-leads-to-surge-in-mobile-phishing-and-malware-attacks-targeting-pharmaceuticals-companies/

REvil 勒索软件攻击 Managed.com 主机提供商，五十万赎金

日期: 2020-11-18

等级: 高

来源: Lawrence Abrams

标签: ['Managed.com', 'REvil', 'Hosting Provider', 'Ransom', 'Ransomware']

Web 托管提供商 Managed.com 已使其服务器和 Web 托管系统脱机，因为他们难以从 2020 年 11 月 16 日的 REvil 勒索软件攻击中恢复过来。 正如 ZDNet 最初报道的那样，Managed.com 在 2020 年 11 月 17 日披露他们受到勒索软件攻击，并且为了保护客户数据的完整性，他们决定关闭整个系统，包括客户的网站。

详情

REvil ransomware hits Managed.com hosting provider, 500K ransom

https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-managedcom-hosting-provider-500k-ransom/

研究人员发现新的 Grelos skimmer 变种

日期: 2020-11-19

等级: 高

来源: Pierluigi Paganini

标签: ['Grelos skimmer', 'Magecart', 'Malware']

RiskIQ 的安全专家发现了 Grelos skimmer 的新变种，该变种与 Magecart 集团的业务重叠。 在 Magecart 的保护伞下，黑客组织继续以电子商店为目标，利用软件窃取银行卡数据。至少自 2010 年以来，安全公司已经监控了十几个组织的活动。 这些团体的受害者名单很长，包括几个主要平台，例如英国航空，Newegg，Ticketmaster，MyPillow 和 Amerisleep，以及 Feedify。

详情

New Grelos skimmer variant reveals murkiness in tracking Magecart operations
https://securityaffairs.co/wordpress/111165/malware/grelos-skimmer.html

韩国的供应链遭到 Lazarus 攻击

日期: 2020-11-16

等级: 中

来源: AntonCherepanov

标签: ['Lazarus', 'South Korea', 'Attack', 'Malware', 'ESET']

ESET 遥测数据最近的研究人员发现，有人试图在韩国通过供应链攻击部署 Lazarus 恶意软件。为了发布恶意软件，攻击者使用了一种不同寻常的供应链机制，滥用从两家不同公司窃取的合法韩国安全软件和数字证书。 Lazarus 小组于 2016 年 2 月首次出现在诺维塔（Novetta）的报告中 ，US-CERT 和 FBI 将该组称为“HIDDEN COBRA”。

详情

Lazarus supply-chain attack in South Korea
https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/

COVID-19 抗原公司受到恶意软件攻击

日期: 2020-11-17

等级: 中

来源: Becky Bracken

标签: ['Miltenyi', 'COVID-19', 'Antigen Firm', 'Malware']

全球生物技术公司米尔特尼(Miltenyi)最近向客户披露，该公司在过去两周，一直在与针对其 IT 基础设施的恶意软件攻击作斗争。 该公司说，Miltenyi 一直在研究 COVID-19 的治疗方法，攻击事件发生后，该公司仍在努力进行电话和电子邮件通信。 公司声明称，请放心，目前已采取一切必要措施控制问题，恢复所有受影响的系统。根据该公司目前的情况来看，没有迹象表明恶意软件被分发给客户或合作伙伴。

详情

COVID-19 Antigen Firm Hit by Malware Attack
https://threatpost.com/covid-19-antigen-malware-attack/161317/

Egregor 勒索软件攻击受害者的打印机

日期: 2020-11-18

等级: 中

来源: Lawrence Abrams

标签: ['Egregor', 'Ransomware', 'Printers', 'Ransom Notes']

Egregor 勒索软件使用了一种新颖的方法来吸引受害者的注意力，从所有可用的打印机中打印出勒索的纸条。 勒索软件团伙知道，许多企业宁愿将勒索软件攻击隐藏起来，也不愿公开，包括对员工，因为担心消息会影响股价和他们的声誉。 为了提高公众对这次袭击的认识，并迫使受害者付钱，Egregor 在攻击公司后，会在所有可用的网络和本地打印机上反复打印赎金。

详情

Egregor ransomware bombards victims' printers with ransom notes

https://www.bleepingcomputer.com/news/security/egregor-ransomware-bombards-victims-printers-with-ransom-notes/

Qbot Banking 特洛伊木马程序现在正在部署 Egregor 勒索软件

日期: 2020-11-20

等级: 中

来源: Lawrence Abrams

标签: ['Qbot', 'ProLock', 'Egregor', 'Ransomware']

Qbot 银行木马已经放弃了 ProLock 勒索软件，取而代之的是 Egregor 勒索软件，后者在 9 月份突然活跃起来。 Qbot，也被称为 QakBot 或 QuakBot，是一种 Windows 恶意软件，它窃取银行证书、Windows 域证书，并为安装勒索软件的攻击者提供远程访问。 类似于 Ryuk 与 TrickBot 和 DoppelPayme 一起使用以访问网络的方式类似，ProLock 勒索软件在历史上一直与 Qbot 一起获得对受感染网络的访问。

详情

QBot partners with Egregor ransomware in bot-fueled attacks

https://www.bleepingcomputer.com/news/security/qbot-partners-with-egregor-ransomware-in-bot-fueled-attacks/

TrickBot turns 100：最新发布的具有新功能的恶意软件

日期: 2020-11-20

等级: 中

来源: Lawrence Abrams

标签: ['TrickBot']

网络犯罪团伙发布了第一百个版本的`TrickBot`恶意软件，并附加了一些功能来逃避检测。TrickBot 是一种恶意软件感染，通常通过恶意钓鱼电子邮件或其他恶意软件安装。安装后，TrickBot 将安静地运行在受害者的计算机上，同时下载其他模块来执行不同的任务。这些模块执行广泛的恶意活动，包括窃取域的 Active Directory 服务数据库、在网络上横向传播、屏幕锁定、窃取 Cookie 和浏览器密码以及窃取 OpenSSH 密钥。

详情

TrickBot turns 100: Latest malware released with new features

https://www.bleepingcomputer.com/news/security/trickbot-turns-100-latest-malware-released-with-new-features/

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. 各主机安装 EDR 产品，及时检测威胁
3. 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
4. 网段之间进行隔离，避免造成大规模感染
5. 及时对系统及各个服务组件进行版本升级和补丁更新
6. 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
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. 注重内部员工安全培训

(二) 数据安全

暴露的数据库显示有超过 10 万个 Facebook 账户被泄露

日期: 2020-11-16

等级: 高

来源: Lindsey O'Donnell

标签: ['Facebook', 'Database', 'Accounts', 'Cybercriminals']

研究人员发现，欺诈者使用一个不安全的数据库存储至少 10 万名受害者的用户名和密码，这之后，他们发现了一个针对 Facebook 用户的大范围全球骗局。 研究人员说，该骗局背后的网络犯罪分子通过使用一种假装透露谁在访问他们的个人资料的工具，诱使 Facebook 受害者提供其帐户登录凭据。 vpnMentor 的研究人员 2020 年 11 月 13 日表示，诈骗者利用盗取的登录凭证，通过受害者的账户在 Facebook 帖子上分享垃圾评论，引导人们进入他们的诈骗网站网络。

详情

Exposed Database Reveals 100K+ Compromised Facebook Accounts

https://threatpost.com/exposed-database-100k-facebook-accounts/161247/

Liquid 货币交易所称黑客进入内部网络，窃取用户数据

日期: 2020-11-18

等级: 高

来源: Catalin Cimpanu

标签: ['Liquid', 'Cryptocurrency', 'Database']

Liquid 是当今 20 大加密货币交易门户之一，2020 年 11 月 18 日披露了一个安全漏洞。该公司在其网站上的一篇博客文章中说，11 月 13 日，一名黑客成功地侵入了员工的电子邮件账户，并转向其内部网络。 该公司表示，在黑客窃取任何资金之前就已检测到入侵，但随后的调查显示，攻击者能够从 Liquid 的数据库中收集存储用户详细信息的个人信息。

详情

Liquid crypto-exchange says hacker accessed internal network, stole user data
https://www.zdnet.com/article/liquid-crypto-exchange-says-hacker-accessed-internal-network-stole-user-data/

新南威尔士州预计网络攻击将使其损失 700 万澳元的法律和调查费用

日期: 2020-11-17

等级: 中

来源: Asha Barbaschow

标签: ['Service NSW', 'Cyberattack', 'MyService', 'Email Accounts']

新南威尔士州服务中心是新南威尔士州政府提供一站式服务的机构，它在 2020 年 4 月遭遇了一次网络攻击，导致 18.6 万名客户的信息被盗。 在从 4 月开始的为期四个月的调查之后，新南威尔士州服务局（Service NSW）表示，它从 47 个员工电子邮件帐户中盗窃了 738GB 的数据，其中包括 380 万份文档。 新南威尔士州服务局保证，没有证据表明 MyService 的个人帐户数据或服务新南威尔士州数据库在攻击期间受到损害。

详情

Service NSW expecting cyber attack to set it back AU$7m in legal and investigation costs
https://www.zdnet.com/article/service-nsw-expecting-cyber-attack-to-set-it-back-au7m-in-legal-and-investigation-costs/

相关安全建议

1. 及时备份数据并确保数据安全
2. 及时检查并删除外泄敏感数据
3. 发生数据泄漏事件后，及时进行密码更改等相关安全措施
4. 合理设置服务器端各种文件的访问权限
5. 统一 web 页面报错信息，避免暴露敏感信息

(三) 网络攻击

三菱电机公司受到新的网络攻击

日期: 2020-11-20

等级: 高

来源: Pierluigi Paganini

标签: ['Mitsubishi Electric Corp.', 'Cyberattack', 'Vulnerability', 'Zero Day']

三菱电机(Mitsubishi Electric Corp.)再次受到大规模网络攻击，可能导致其业务合作伙伴的相关信息泄露。 公司管理人员 11 月 20 日表示，他们正在检查与之有业务往来的 8653 个账户，以确定是否有与其他方银行账户相关的信息以及其他信息泄露。 入侵发生在 2019 年 6 月 28 日，该公司于 2019 年 9 月展开了调查。在两家当地报纸《朝日新闻》(Asahi Shimbun)和《日本经济新闻》(Nikkei)报道了安全漏洞之后，三菱电机才披露了这一安全事件。属 于国防部门、铁路和电力供应组织的高度机密信息显然被盗。

详情

Mitsubishi Electric Corp. was hit by a new cyberattack
https://securityaffairs.co/wordpress/111201/hacking/mitsubishi-electric-cyberattack.html

针对 Intel SGXSecurity 事务的基于硬件的故障注入攻击

日期: 2020-11-17

等级: 高

来源: Pierluigi Paganini

标签: ['VoltPillager', 'Intel', 'SGXSecurity', 'CPU', 'Fault injection']

伯明翰大学的六位研究人员组成的小组设计了一种名为`VoltPillager`的新攻击技术，该技术可以通过控制 CPU 内核电压来破坏`Intel Software Guard Extensions（SGX）`专用区的机密性和完整性。 该攻击利用了一种低成本工具，该工具用于在 CPU 和主板上的电压调节器之间的串行电压识别总线上注入串行电压识别（SVID）数据包。 注入的数据包允许研究人员完全控制 CPU 核心电压和执行故障注入攻击。

详情

Hardware-based fault injection attacks against Intel SGXSecurity Affairs
https://securityaffairs.co/wordpress/111033/hacking/voltpillager-attack-intel-sgx.html

装有 Epsilon 框架主题的 WordPress 网站成为大规模攻击的目标

日期: 2020-11-18

等级: 高

来源: Pierluigi Paganini

标签: ['WordPress', 'Epsilon Framework', 'Function Injection']

Wordfence 威胁情报小组的专家发现，攻击者正在扫描互联网，寻找安装了 Epsilon 框架主题的 WordPress 网站，以利用函数注入攻击。 据专家称，有超过 15 万个网站安装了这些易受攻击的主题。 到目前为止，Wordfence 已经针对来自这些漏洞的超过 150 万个站点发起了超过 750 万次攻击，这些站点来自 18,000 多个 IP 地址。

详情

Large-scale campaign targets vulnerable Epsilon Framework WordPress themes
https://securityaffairs.co/wordpress/111104/hacking/epsilon-framework-themes-attacks.html

office365 钓鱼活动使用重定向 url 和检测沙箱来逃避检测

日期: 2020-11-18

等级: 高

来源: Pierluigi Paganini

标签: ['Microsoft', 'Office 365', 'Redirector URL', 'Sandbox', 'Phishing']

Microsoft 正在跟踪针对企业的 Office 365 网络钓鱼活动，这些攻击能够检测沙盒解决方案并逃避检测。 该活动使用与远程工作相关的诱饵，如密码更新、会议信息、帮助台票等。 活动背后的攻击者利用重定向 URL 来检测来自沙箱环境的传入连接。 在检测到沙箱的连接后，重定向器会将它们重定向到合法站点以逃避检测，而来自真正的潜在受害者的连接会被重定向到钓鱼页面。

详情

Office 365 phishing campaign uses redirector URLs and detects sandboxes to evade detection

https://securityaffairs.co/wordpress/111120/cyber-crime/office-365-phishing-campaign.html

乔·拜登的“Vote Joe”网站被土耳其黑客攻击

日期: 2020-11-20

等级: 高

来源: Ax Sharma

标签: ['Turkish', 'Vote Joe', 'Joe Biden', 'RootAyyıldız', 'Defaced']

2020 年 11 月 20 日，由拜登·哈里斯（Biden-Harris）总统竞选活动建立的`Vote Joe`网站遭到了土耳其黑客`RootAyyıldız`的入侵和诽谤。 根据证据和该站点的存档快照，本次入侵和破坏似乎已经持续了超过 24 小时。 据互联网档案馆的`Wayback Machine`称，直到 11 月 9 日左右，即 2020 年美国总统大选之后的几天，`vote.joebiden.com`网站将重定向到`iwillvote.com`。

详情

Joe Biden's 'Vote Joe' website defaced by Turkish Hackers

https://www.bleepingcomputer.com/news/security/joe-bidens-vote-joe-website-defaced-by-turkish-hackers/

曼联遭遇网络攻击

日期: 2020-11-21

等级: 高

来源: Pierluigi Paganini

标签: ['Manchester United', 'Cyberattack', 'IT']

曼联足球俱乐部的系统遭到了网络攻击，目前还不知道其球迷的个人数据是否被泄露。目前，曼联俱乐部已经迅速采取行动遏制袭击，并正与专家顾问合作，调查这起事件，尽量减少持续的 IT 干扰。曼联俱乐部已通知英国当局，包括新闻专员办公室，联合对事件展开调查

详情

Manchester United hit by ‘sophisticated’ cyber attack

https://securityaffairs.co/wordpress/111231/hacking/manchester-united-cyber-attack.html

网络攻击使圣约翰市的 IT 基础设施瘫痪

日期: 2020-11-22

等级: 高

来源: Pierluigi Paganini

标签: ['Saint John', 'Cyberattack', 'IT Infrastructure']

加拿大圣约翰市遭到大规模网络攻击，整个 IT 市政基础设施瘫痪。网络攻击导致整个市政网络关闭，包括城市网站、在线支付系统、电子邮件和客户服务应用程序。圣约翰市正与联邦和省政府合作，以求从网络攻击中恢复过来。据估计，该市可能需要几周时间才能从这次攻击中完全恢复。

详情

A cyberattack crippled the IT infrastructure of the City of Saint John
https://securityaffairs.co/wordpress/111259/cyber-crime/saint-john-cyber-attack.html

新的 skimer 攻击使用 WebSockets 来逃避检测

日期: 2020-11-16

等级: 中

来源: Pierluigi Paganini

标签: ['Akamai', 'Skimmer', 'WebSockets', 'Payment Cards']

来自 Akamai 的研究人员发现了一种新的 skimmer 攻击，该攻击针对多个电子商店，采用了一种过滤数据的新技术。 攻击者使用伪造的信用卡论坛和 WebSockets 窃取用户的财务和个人信息。 在线商店越来越多地将其付款流程外包给第三方供应商，这意味着他们不处理商店内部的信用卡数据。 为了解决这个问题，攻击者创建了一张虚假的信用卡表格，并将其注入应用程序的结帐页面。

详情

New skimmer attack uses WebSockets to evade detection
https://securityaffairs.co/wordpress/110982/hacking/skimmer-attack-websockets.html

冷库巨头 Americold 服务受到网络攻击的影响

日期: 2020-11-16

等级: 中

来源: Lawrence Abrams

标签: ['Americold', 'Cold Storage', 'Cyberattack']

冷库巨头 Americold 目前正在应对影响其运营的网络攻击，包括电话系统，电子邮件，库存管理和订单履行。 Americold 是领先的温度控制仓库运营商，为零售商，食品服务提供商和生产商提供供应链服务和库存管理。 Americold 在全球管理 183 个仓库，拥有大约 13,000 名员工。 2020 年 11 月 16 日，Americold 遭受了一次网络攻击，导致他们关闭了自己的计算机系统以防止攻击的扩散。

详情

Cold storage giant Americold services impacted by cyberattack
https://www.bleepingcomputer.com/news/security/cold-storage-giant-americold-services-impacted-by-cyberattack/

黑客组织利用 ZeroLogon 在汽车行业发动攻击

日期: 2020-11-18

等级: 中

来源: Charlie Osborne

标签: ['Cicada', 'APT10', 'Stone Panda', 'Cloud Hopper', 'ZeroLogon']

研究人员发现了一个全球范围内的活动，目标是使用最近披露的 ZeroLogon 漏洞的企业。这次主动的网络攻击被认为是 Cicada 的杰作，被追踪的还有 APT10、Stone Panda 和 Cloud Hopper。 赛门铁克研究人员记录了 17 个地区的公司及其子公司，涉及汽车、制药、工程和管理服务提供商(MSP)行业，它们最近成为 Cicada 的目标。

详情

Hacking group exploits ZeroLogon in automotive, industrial attack wave

https://www.zdnet.com/article/cicada-hacking-group-exploits-zerologon-launches-new-backdoor-in-automotive-industry-attack-wave/

黑客攻击 49000 多个存在漏洞的 Fortinet VPN

日期: 2020-11-22

等级: 中

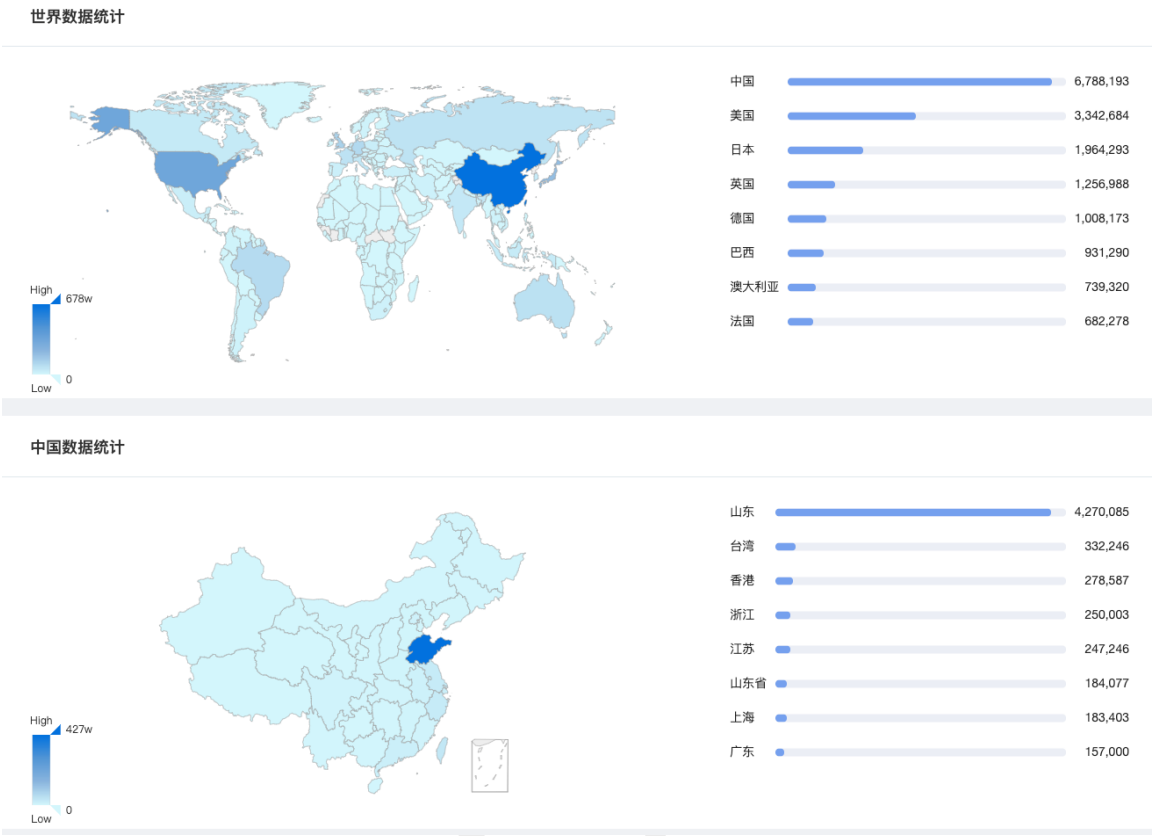
来源: Ax Sharma

标签: ['VPN', 'Fortinet VPN', 'CVE-2018-13379']

一名黑客发布了一份攻击列表，信息为从近 5 万台 FortineVPN 设备中窃取的 VPN 凭据。在易受攻击的目标名单上，有着世界各地商业银行和政府组织。黑客使用的漏洞为`CVE-2018-13379`，这是一个路径遍历漏洞，影响大量未修补的 FortiNet FortiOS SSL VPN 设备。通过利用此漏洞，未经验证的远程攻击者可以通过巧尽心思构建的 HTTP 请求访问系统文件。

360CERT

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



详情

Hacker posts exploits for over 49,000 vulnerable Fortinet VPNs

https://www.bleepingcomputer.com/news/security/hacker-posts-exploits-for-over-49-000-vulnerable-fortinet-vpns/

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. 减少外网资源和不相关的业务，降低被攻击的风险
4. 若系统设有初始口令，建议使用强口令，并且在登陆后要求修改。
5. 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

(四) 其他事件

警告：GO SMS Pro 应用程序中未修补的漏洞会暴露数百万条媒体消息

日期: 2020-11-19

等级: 高

来源: The Hacker News

标签: ['GO SMS Pro', 'Android', 'Vulnerability', 'Google Play']

Android 上安装了超过 1 亿的流行短信应用程序 GO SMS Pro 被发现存在一个未修补的安全漏洞，该漏洞会暴露用户之间的媒体传输，包括私人语音信息、照片和视频。
Trustwave 高级安全顾问 Richard Tan 在与 The Hacker News 分享的一份报告中说：“这意味着该 Messenger 应用程序的用户之间共享的任何敏感媒体都有被未经身份验证的攻击者或好奇的用户破坏的危险。” 根据 Trustwave SpiderLabs 的说法，该漏洞存在于该应用程序的 7.91 版本中，该版本于 2020 年 2 月 18 日在 Google Play 商店中发布。

详情

WARNING: Unpatched Bug in GO SMS Pro App Exposes Millions of Media Messages
https://thehackernews.com/2020/11/warning-unpatched-bug-in-go-sms-pro-app.html

Ticketmaster 因数据安全故障被罚款 170 万美元

日期: 2020-11-16

等级: 高

来源: Mathew J. Schwartz

标签: ['Ticketmaster', 'UK', 'Britain', 'EU', 'Fined']

在收到潜在欺诈的警报后，Ticketmaster 花了 9 周时间才发现这一重大漏洞。
Ticketmaster UK 已被英国隐私监管机构罚款 125 万英镑(约合 170 万美元)，原因是该公司严重违反遵守欧盟的《一般数据保护条例》。 监管机构表示，该公司未能正确保护它选择在支付页面上运行的聊天机器人软件，攻击者对其进行了破坏，从而使他们能够窃取支付卡信息。 据称，即使在首次警惕其网站上存在可疑的信用卡欺诈事件后，Ticketmaster UK 仍未能在九个星期内缓解该问题。

详情

Ticketmaster Fined $1.7 Million for Data Security Failures
https://www.databreachtoday.com/ticketmaster-fined-17-million-for-data-security-failures-a-15369

超过 245000 个 Windows 系统仍然容易受到 BlueKeep RDP 漏洞的攻击

日期: 2020-11-17

等级: 高

来源: Catalin Cimpanu

标签: ['BlueKeep', 'RDP', 'Windows', 'SMBGhost']

在微软披露 BlueKeep 漏洞影响 windowsrdp 服务一年半后，仍有超过 245000 个 Windows 系统未修补，易受攻击。 在 2019 年 5 月的第一次扫描中，这个数字代表了最初发现易受 BlueKeep 攻击的 950000 个系统中的 25%。类似地，超过 103000 个 Windows 系统也仍然容易受到 SMBGhost 的攻击，SMBGhost 是服务器消息块 v3（SMB）协议中的一个漏洞，该协议与 Windows 的最新版本一起发布，于 2020 年 3 月披露。这两个漏洞都允许攻击者远程接管 Windows 系统，并被认为是过去几年 Windows 中披露的一些最严重的漏洞。

详情

More than 245,000 Windows systems still remain vulnerable to BlueKeep RDP bug
https://www.zdnet.com/article/more-than-245000-windows-systems-still-remain-vulnerable-to-bluekeep-rdp-bug/

多家工业控制系统供应商警告存在严重漏洞

日期: 2020-11-17

等级: 高

来源: Tom Spring

标签: ['Real Time Automation', 'Paradox', 'Vulnerability']

工业控制系统公司 Real Time Automation 和 Paradox 2020 年 11 月 17 日警告称，系统存在严重漏洞，可能遭到恶意攻击者的远程攻击。 根据行业标准的常见漏洞评分系统(Common Vulnerability Scoring System)，漏洞的严重程度为 9.8 分(满分 10 分)。该漏洞可以追溯到 Claroty 生产的一个部件。 在 RTA 的 499ES ENIP 堆栈中发现了一个堆栈溢出漏洞，所有版本都在 2.28 之前，这是最广泛使用的 OT 协议之一，Claroty 在 2020 年 11 月 17 日公开披露了这个漏洞。

详情

Multiple Industrial Control System Vendors Warn of Critical Bugs
https://threatpost.com/ics-vendors-warn-critical-bugs/161333/

Facebook Messenger 漏洞可以让黑客在你接电话之前监听你

日期: 2020-11-20

等级: 高

来源: The Hacker News

标签: ['Facebook Messenger', 'Android', 'Google', 'Vulnerability']

Facebook 在其广泛安装的 Android Messenger 应用程序中修复了一个漏洞，该漏洞可能使远程攻击者可以呼叫毫无防备的目标，并在他们收到音频呼叫之前监听他们。 该漏洞是 Google Zero 项目漏洞调查团队的 Natalie Silvanovich 于 10 月 6 日发现并报告给 Facebook 的，影响到了 Android Messenger 的 284.0.0.16.11919 版本（以及更早版本）。

详情

Facebook Messenger Bug Lets Hackers Listen to You Before You Pick Up the Call
https://thehackernews.com/2020/11/facebook-messenger-bug-lets-hackers.html

AWS 漏洞允许攻击者查找用户的 Access Codes

日期: 2020-11-20

等级: 高

来源: Chinmay Rautmare

标签: ['Amazon Web Services', 'Vulnerability', 'KMS', 'SQS', 'Access Codes']

Palo Alto Networks 的 Unit 42 的研究人员称，研究人员发现了 16 种 Amazon Web Services 产品中 22 个应用程序编程接口中的漏洞，该漏洞可被利用来破坏用户的基本信息并获得各种云帐户的详细信息。 这些漏洞在 AWS 的三个区域都被发现了，包括政府服务和中国，亚马逊的简单存储服务(S3)，亚马逊的密钥管理服务(KMS)和亚马逊的简单队列服务(SQS)都很容易被滥用。

详情

AWS Flaw Allows Attackers to Find Users' Access Codes

https://www.databreachtoday.com/aws-flaw-allows-attackers-to-find-users-access-codes-a-15408

交友网站 Bumble 为 1 亿用户提供了不安全的刷卡服务

日期: 2020-11-16

等级: 中

来源: Becky Bracken

标签: ['Bumble', 'API', 'Vulnerability', 'HackerOne']

在仔细查看了流行的约会网站和应用程序 Bumble（通常由女性发起对话）的代码后，独立安全评估人员研究员 Sanjana Sarda 发现了有关 API 漏洞的信息。 这些不仅使她能够绕过 Bumble Boost 高级服务的付款，而且还能够访问该平台近 1 亿整个用户群的个人信息。Sarda 表示，这些问题很容易发现，公司对她的报告的回应表明，Bumble 需要更认真地对待测试和漏洞披露。 Sarda 花了大约两天的时间找到最初的漏洞，又花了大约两天的时间提出了一个基于同样漏洞的进一步攻击的验证概念，Sarda 在电子邮件中告诉 Threatpost 平台。尽管 API 问题不像 SQL 注入那样出名，但这些问题会造成严重的损害。

详情

Dating Site Bumble Leaves Swipes Unsecured for 100M Users

https://threatpost.com/dating-site-bumble-swipes-unsecured-100m-users/161276/

澳大利亚 BitConnect 发起人因涉嫌密码诈骗被起诉

日期: 2020-11-17

等级: 中

来源: Asha Barbaschow

标签: ['Australian', 'BitConnect', 'ASIC']

澳大利亚证券投资委员会（ASIC）宣布，`BitConnect`的前澳大利亚发起人因参与被指控欺诈数百万投资者的折叠加密货币项目而被起诉。 ASIC 表示，约翰·路易斯·安东尼·比加顿（John Louis Anthony Bigatton）在 2018 年初崩溃之前就推广了这种加密货币平台，声称从 2017 年 8 月 14 日至 2018 年 1 月 18 日，该男子是`Bitconnect`的澳大利亚国民发起人。

详情

Aussie BitConnect promoter charged over his involvement with alleged crypto scam
https://www.zdnet.com/article/aussie-bitconnect-promoter-charged-over-his-involvement-with-alleged-crypto-scam/

macOS Big Sur 上的某些 Apps 绕过了内容过滤器和 VPN

日期: 2020-11-17

等级: 中

来源: Elizabeth Montalbano

标签: ['Apple', 'Big Sur', 'Bypass', 'Content Filters', 'VPN']

安全研究人员对苹果公司的 macOS 最新 Big Sur 版本中的一项功能进行了抨击，该功能允许某些 Apple 应用程序绕过内容过滤器和 VPN。 他们说这是一种威胁，攻击者可以利用它来绕过防火墙，使他们能够访问人们的系统并暴露其敏感数据。 一个名叫 Maxwell (@mxswd)的用户在 10 月份的 Twitter 上第一个指出了这个问题。尽管安全专家存在担忧和疑问，苹果还是在 11 月 12 日向公众发布了 Big Sur。

详情

Some Apple Apps on macOS Big Sur Bypass Content Filters, VPNs
https://threatpost.com/some-apple-apps-on-macos-big-sur-bypass-content-filters-vpns/161295/

Cisco 在 PoC 攻击代码发布后修补了严重漏洞

日期: 2020-11-17

等级: 中

来源: Lindsey O'Donnell

标签: ['Cisco Security Manager', 'Patch', 'Vulnerability']

在思科安全管理器(Cisco Security Manager)中一个严重漏洞的概念验证(PoC)攻击代码发布一天后，Cisco 便发布了一个补丁。 思科安全管理器是一个面向企业管理员的端到端安全管理应用程序，它使管理员能够执行各种安全策略、解决安全事件和管理各种设备。应用程序有一个漏洞，允许远程的、未经身份验证的攻击者访问受影响系统上的敏感数据。该漏洞(CVE-2020-27130)的 CVSS 评分为 9.1 分(满分 10 分)，非常严重。

详情

Cisco Patches Critical Flaw After PoC Exploit Code Release
https://threatpost.com/critical-cisco-flaw-sensitive-data/161305/

Cisco Webex 漏洞允许攻击者作为虚假用户加入会议

日期: 2020-11-18

等级: 中

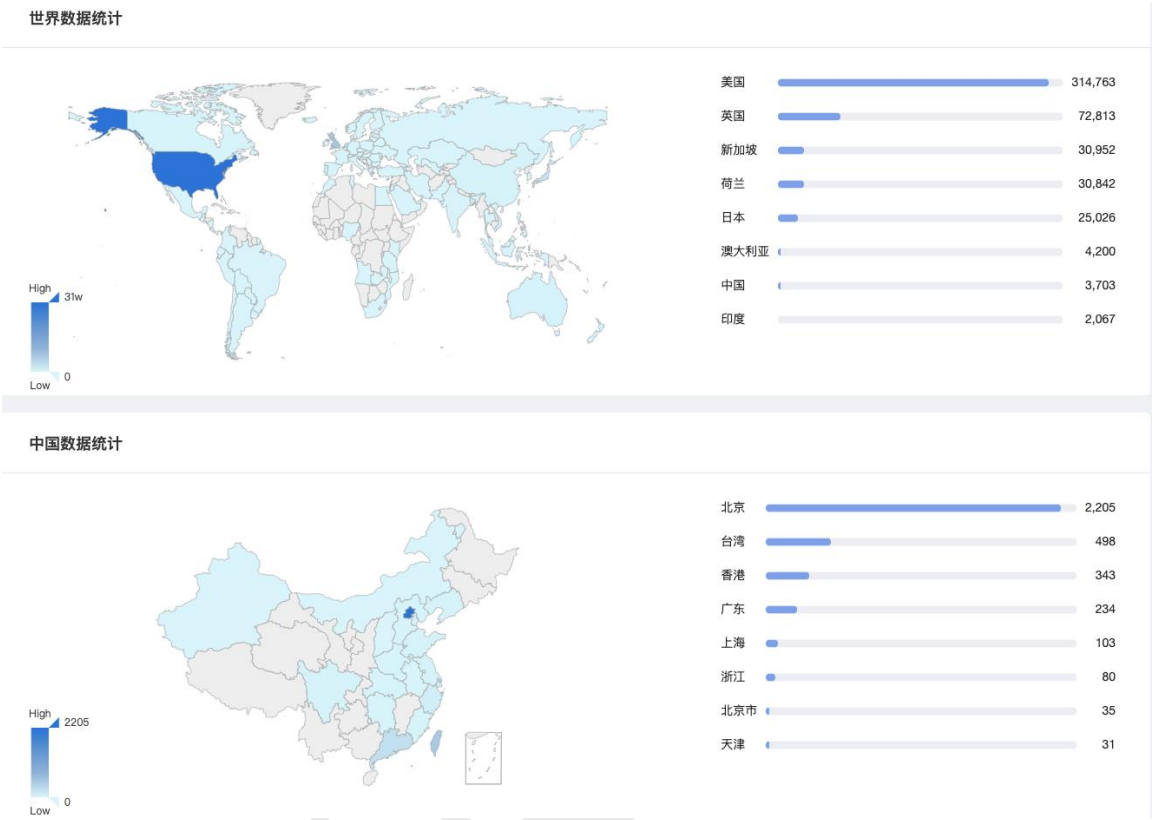
来源: Catalin Cimpanu

标签: ['Cisco', 'Webex', 'Vulnerability', 'COVID-19']

Cisco 计划修复 Webex 视频会议应用程序中的三个漏洞，这些漏洞可使攻击者以虚假用户的身份潜入并参加 Webex 会议，而其他参与者看不到。 2020 年早些时候，IBM 的安全研究人员发现了这些漏洞。他们对科技软件巨头 IBM 在冠状病毒大流行期间内部使用的远

程工作工具进行了评估。 研究人员说，当这三个漏洞结合在一起时，攻击者就可以进行攻击。

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



详情

Cisco Webex bugs allow attackers to join meetings as ghost users

https://www.zdnet.com/article/cisco-webex-bugs-allow-attackers-to-join-meetings-as-ghost-users/

防范 DNS 欺骗:发现缓存投毒漏洞

日期: 2020-11-18

等级: 中

来源: Mathew J. Schwartz

标签: ['IP', 'DNS', 'Cache Poisoning', 'Vulnerability']

互联网依靠域名系统将人类可读的域名转换为计算机可读的 IP 地址。 不幸的是，许多现代 DNS 服务容易受到欺骗性攻击，这种欺骗性攻击使攻击者可以将任何流量（最初发往特定域）重定向到他自己的服务器，然后成为中间人攻击者，从而可以进行窃听和篡改数据。来自加州大学河滨分校和北京清华大学的一组研究人员已经确定了一种新型的 DNS 缓存投毒攻击，称为"SAD DNS"，即"Side-channel AttackeD DNS"。 该漏洞是由于 Internet 控制消息协议中的速率限制控件而引起的，该协议是一种错误报告协议，网络设备（包括路由器）使用该协议将错误消息发送到已引入可利用副信道的源 IP 地址。

详情

Brace for DNS Spoofing: Cache Poisoning Flaws Discovered
https://www.databreachtoday.com/brace-for-dns-spoofing-cache-poisoning-flaws-discovered-a-15389

VMware 修复了天府杯白帽黑客大赛上发现的 hypervisor 漏洞

日期: 2020-11-20

等级: 中

来源: Simon Sharwood

标签: ['VMware', 'Hypervisor', 'Tianfu Cup', 'CVE-2020-4004', 'VMX']

VMware 披露并修复了在中国天府杯白帽黑客大赛上发现的 hypervisor 漏洞。 `CVE-2020-4004`因其在`CVSS`级别上的 9.3 而被评为`严重`，被描述为`XHCI USB 控制器漏洞`。 它允许在虚拟机上具有本地管理特权的恶意行为者在主机上运行虚拟机的 VMX 进程时执行代码。 VMX 进程在 VMkernel 中运行，并负责处理设备的`I/O`，因此存在数据泄漏的可能性。

详情

VMware reveals critical hypervisor bugs found at Chinese white hat hacking comp. One lets guests run code on hosts
https://www.theregister.com/2020/11/20/vmware_esxi_flaws/

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

360CERT

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）。

360CERT

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

360CERT

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

360CERT

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。

360CERT

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

360CERT

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