安全事件周报

安全事件周报 (11.23-11.29)

360CERT
北京奇虎科技有限公司 | 2020-11-30

报告信息

报告名称	安全事件周报（11.23-11.29）		
报告类型	安全事件周报	报告编号	B6-2020-113001
报告版本	1.0	报告日期	2020-11-30
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	2020-11-30	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 51 项

话题集中在`勒索软件`、`网络攻击`方面，涉及的组织有：`GitHub`、`Advantech`、`Minecraft`、`Banijay`等。勒索泛滥，员工安全意识提升也是企业安全重要一环

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**
假冒的 Minecraft mods 用广告淹没了超过 100 万台 Android 设备	★★★★★
勒索软件攻击将使法国 IT 服务部门损失 6000 万美元	★★★★★
物联网芯片制造商 Advantech 受到勒索软件的打击，1250 万美元的赎金	★★★★★
FBI 发布了有关 Ragnar Locker 勒索软件活动的警报	★★★★
沃尔玛独家销售的 Jetstream 路由器隐藏着能控制设备的后门	★★★★
TA416 APT 使用新的 PlugX 恶意软件变种	★★★★
新的 WAPDropper 恶意软件滥用 Android 设备进行 WAP 欺诈	★★★★
Blackrota Golang 后门包严重混淆视听	★★★★
勒索软件团伙寻找税务软件，以加大对受害者的压力	★★★★
勒索软件：Egregor 新变种可能是对您的企业的下一个重大恶意软件威胁	★★★★
Bandook 后门木马	★★★★
佳能公开证实八月勒索软件攻击和数据泄露	★★★★
Banijay 被 DoppelPaymer 勒索软件击中	★★★★
Sopra Steria 估计勒索软件攻击的财务影响可能达到 5000 万欧元	★★★★
大规模威胁运动攻击开源回收开源仓库	★★★
TrickBot 恶意软件使用模糊的 Windows 批处理脚本来逃避检测	★★★
Stantinko 的 Linux 恶意软件现在伪装成 Apache Web 服务器	★★★
SSH 后门僵尸网络与"研究"感染技术	★★★
勒索软件攻击美国最大的生育网络，病人数据被盗	★★★
Dark Caracal APT 组织仍然活跃	★★★
数据安全	**等级**
黑客泄露事件管理应用程序 Peatix 的用户数据	★★★★★

百度的 Android 应用程序被发现收集和泄露敏感用户数据	★★★★★
暴露了近 50000 个易受攻击的 Fortinet VPN 的密码	★★★★★
1600 万巴西 COVID-19 患者的详细信息在网上曝光	★★★★★
网络设备供应商 Belden 披露数据泄露	★★★★
Home Depot 同意就 2014 年数据泄露达成 1750 万美元的和解	★★★
Sophos 在安全漏洞发生后提醒客户信息泄露	★★★
黑客出售数百份高管账号，每个 100 至 1500 美元	★★★
网络攻击	**等级**
巴西政府从有史以来最严重的网络攻击中恢复过来	★★★★★
黑客通过 GoDaddy 攻击加密货币平台	★★★★
使用最新密钥的 Tesla Model X 在几分钟内就被破解了	★★★★
针对 30 万以上 Spotify 用户的凭据填充攻击	★★★★
国际刑警组织逮捕了 3 名尼日利亚 BEC 诈骗犯，他们的目标超过 50 万个实体	★★★★
恶意软件在被黑客攻击的 WordPress 网站上创建诈骗在线商店	★★★
FBI：我们网站的虚假版本可用于网络攻击，因此请当心	★★★
网络巨头 Belden 公司数据在网络攻击中被盗	★★★
丹麦新闻社 Ritzau 遭勒索软件袭击，但没有支付赎金	★★★
网络钓鱼用伪造的"重返工作岗位"内部备忘录引诱员工	★★★
CISA 警告易受攻击的 Fortinet VPN 上存在密码泄漏	★★★
其他事件	**等级**
英国 NCSC 警告敦促组织修复 MobileIron CVE-2020-15505 RCE	★★★★★
VMware 修复了能让黑客瞄准企业网络的 SD-WAN 漏洞	★★★★
30%的顶级在线购物域名容易受到 SSL 攻击	★★★★
Facebook 在韩国因未经同意分享用户数据而被罚款	★★★★

工业自动化系统中的一个严重漏洞	★★★★
GitHub 修复了 Google 发现的严重安全漏洞	★★★
TikTok 补丁修复了 XSS 漏洞和点击劫持漏洞	★★★
苹果全球安全负责人因受贿指控被起诉	★★★
黑客因运行服务绕过防病毒软件而被捕	★★★
cPanel 的 2FA 绕过可能会让数千万的网站受到黑客攻击	★★★
Xbox 漏洞可能会让黑客将玩家标签与玩家的电子邮件链接起来	★★★
windows7 和 windows server 2008 的 0day 漏洞仍未修复	★★★

三、 事件详情

(一) 恶意程序

假冒的 Minecraft mods 用广告淹没了超过 100 万台 Android 设备

日期: 2020-11-23

等级: 高

来源: Ionut Ilascu

标签: ['Google', 'Minecraft', 'Fake Mods', 'Android', 'Kaspersky']

攻击者绕过 Google 对 Play 官方商店的保护，并为流行游戏 Minecraft 发布了 20 多个假 modpack。 这些应用程序只是空壳，旨在吸引想要修改其游戏玩法的儿童和青少年。 他们不提供任何恶意软件，但是一旦安装，它们几乎无法正常使用手机。 安装后，假的 modpacks 开始显示全屏广告。 该 modpacks 将每两分钟打开一个带有广告的浏览器窗口。 卡巴斯基的安全研究人员在 7 月检测到了此操作，发现最成功的假 modpack 拥有超过一百万的安装。

详情

Fake Minecraft mods swamp over 1M Android devices with ads

https://www.bleepingcomputer.com/news/security/fake-minecraft-mods-swamp-over-1m-android-devices-with-ads/

勒索软件攻击将使法国 IT 服务部门损失 6000 万美元

日期: 2020-11-26

等级: 高

来源: Prajeet Nair

标签: ['Sopra Steria', 'Ryuk', 'Ransomware', 'Attack', 'IT', 'French']

Sopra Steria 被 Ryuk 勒索软件之前未知的版本击中。 根据一份公司声明，法国 IT 服务公司 Sopra Steria 于 10 月份受到 Ryuk 勒索软件的攻击，估计该攻击将使该公司损失 4000 至 5000 万欧元（4700 万至 5900 万美元）。 10 月 21 日，Sopra Steria 承认它已使用以前未知的 Ryuk 勒索软件检测到攻击。 该公司当时指出，没有证据表明有任何客户或公司数据泄露，或者该公司管理的任何客户系统都没有损坏

详情

Ransomware Attack Will Costs French IT Services $60 Million

https://www.databreachtoday.com/ransomware-attack-will-costs-french-services-60-million-a-15465

物联网芯片制造商 Advantech 受到勒索软件的打击，1250 万美元的赎金

日期: 2020-11-27

等级: 高

来源: Sergiu Gatlan

标签: ['Conti', 'Advantech', 'Ransomware', 'Steal Data']

`Conti`勒索软件团伙袭击了工业自动化和工业物联网（IIoT）芯片制造商`Advantech`的系统，目前要求 1400 万美元赎金，以解密受影响的系统，并停止泄露被盗的公司数据。`Advantech`是全球领先的医疗保健设备和解决方案制造商，拥有超过 8000 人的嵌入式计算机和服务器。2018 年，该公司以 34%的 WW 市场份额成为世界工业计算领域的领导者，2019 年公司的年销售收入超过 17 亿美元。

详情

IIoT chip maker Advantech hit by ransomware, $12.5 million ransom

https://www.bleepingcomputer.com/news/security/iiot-chip-maker-advantech-hit-by-ransomware-125-million-ransom/

FBI 发布了有关 Ragnar Locker 勒索软件活动的警报

日期: 2020-11-23

等级: 高

来源: Pierluigi Paganini

标签: ['Ragnar Locker', 'Ransomware', 'FBI']

美国联邦调查局（FBI）发布了紧急警报（MU-000140-MW），以警告私营行业合作伙伴。自 2020 年 4 月确认袭击以来，Ragnar Locker 勒索软件活动有所增加。 MU-000140-MW 紧急警报包括检测与该勒索软件团伙相关联的妥协指标。 FBI 于 2020 年 4 月首次观察到 Ragnar Locker 勒索软件，当时未知的参与者使用它对一家大公司的文件进行加密，获得大约 1100 万美元的赎金，并威胁要释放 10 TB 的敏感公司数据。 从那时起，Ragnar Locker 就针对越来越多的受害者进行了部署，其中包括云服务提供商，通信，建筑，旅行和企业软件公司。

详情

FBI issued an alert on Ragnar Locker ransomware activity

https://securityaffairs.co/wordpress/111286/malware/ragnar-locker-ransomware-fbi-alert.html

沃尔玛独家销售的 Jetstream 路由器隐藏着能控制设备的后门

日期: 2020-11-23

等级: 高

来源: Bernard Meyer

标签: ['Walmart', 'Jetstream', 'Router', 'Backdoors']

在 CyberNews 高级信息安全研究员 Mantas Sasnauskas 与研究人员 James Clee 和 Roni Carta 的合作下，在 Jetstream 路由器中发现了可疑后门，该路由器在沃尔玛专门出售，作为其 wifi 路由器系列。 该后门使攻击者不仅可以远程控制路由器，而且可以远程控制与该网络连接的任何设备。 CyberNews 与 Walmart 进行了联系，以征询他们的意见，并了解他们是否知道 Jetstream 后门，以及他们打算如何保护客户。 在 CyberNews 发送了有关受影响的 Jetstream 设备的信息后，沃尔玛发言人告知 CyberNews， 沃尔玛正在研究该问题以了解更多信息。有问题的商品目前无货，沃尔玛没有计划进行补充。

详情

Walmart-exclusive router and others sold on Amazon & eBay contain hidden backdoors to control devices

https://cybernews.com/security/walmart-exclusive-routers-others-made-in-china-contain-backdoors-to-control-devices/

TA416 APT 使用新的 PlugX 恶意软件变种

日期: 2020-11-23

等级: 高

来源: Lindsey O'Donnell

标签: ['TA416', 'Golang', 'PlugX', 'Malware', 'Spear-phishing Attacks']

TA416 高级持续威胁（APT）在其一个月的不活动之后，该组织被发现使用了从未见过的`PlugX`恶意软件加载程序`Golang`变体来发动鱼叉式网络钓鱼攻击。 TA416，也称为“Mustang Panda”和“ RedDelta”，最近在针对与梵蒂冈和中国共产党建交的实体以及缅甸实体的运动中被发现（所有这些都是先前报道的运动 ）。 在对这些攻击的进一步分析中，研究人员发现该组织已更新了其工具集-特别是对其 PlugX 恶意软件变种进行了改进。 PlugX 远程访问工具（RAT）以前曾用于针对政府机构的攻击，并允许远程用户未经许可或授权即可盗窃数据或控制受影响的系统。

详情

TA416 APT Rebounds With New PlugX Malware Variant

https://threatpost.com/ta416-apt-plugx-malware-variant/161505/

新的 WAPDropper 恶意软件滥用 Android 设备进行 WAP 欺诈

日期: 2020-11-24

等级: 高

来源: Catalin Cimpanu

标签: ['Android', 'WAPDropper', 'Southeast Asia', 'Check Point', 'Android']

安全研究人员发现一种新的 Android 恶意软件目前正在野外传播，主要针对东南亚地区的用户。 这款名为 WAPDropper 的恶意软件被安全公司 Check Point 发现，目前正在通过托管在第三方应用商店的恶意应用程序传播。 Check Point 表示，一旦恶意软件感染了用户，它就会开始让用户注册付费电话号码，为各种服务收取高额费用。 最终的结果是，所有感染病毒的用户每个月都会收到大量的电话账单，直到他们取消了付费号码的订阅，或者向他们的移动提供商报告了这个问题。

详情

New WAPDropper malware abuses Android devices for WAP fraud

https://www.zdnet.com/article/new-wapdropper-malware-abuses-android-devices-for-wap-fraud/

Blackrota Golang 后门包严重混淆视听

日期: 2020-11-24

等级: 高

来源: Lindsey O'Donnell

标签: ['Golang', 'Blackrota', 'Backdoor', 'Heavy Obfuscation Punch']

研究人员发现了一种新的用 Go 编程语言（Golang）编写的后门程序，由于其严重的混淆程度，该程序让他们大吃一惊。 名为`Blackrota`的后门最初是在研究人员拥有的蜜罐中发现的，该后门试图利用 Docker Remote API 中的未授权访问漏洞。 后门之所以与众不同，是因为它使用了广泛的反检测技术，这使得该恶意软件极难分析，研究人员说，基于 Golang 的恶意软件并不常见。

详情

Blackrota Golang Backdoor Packs Heavy Obfuscation Punch

https://threatpost.com/blackrota-golang-backdoor-obfuscation/161544/

勒索软件团伙寻找税务软件，以加大对受害者的压力

日期: 2020-11-24

等级: 高

来源: Bradley Barth

标签: ['Mount Locker', 'TurboTax', 'Sophos', 'PowerShell', 'Ransomware']

勒索软件的参与者正在针对税收软件文件，以期挖掘高度敏感的数据并增强对受害者的影响力，其中包括小型企业，这些企业的纳税合规性可能会受到严重破坏。 据报道，2020 年 11 月 20 日左右，安全研究人员 Vitali Kremez 向 BleepingComputer 透露，最近发现的勒索软件程序 Mount Locker 一直以具有 TurboTax 软件相关扩展名的文件为目标。 就在 2020 年 10 月，Sophos 分别报告说，LockBit 勒索软件参与者一直在使用 PowerShell 工具在受到破坏的网络上寻找税收软件，以便找到可能被勒索的目标。

详情

Ransomware gangs hunt for tax software to ratchet up pressure on victims

https://www.scmagazine.com/home/security-news/ransomware/ransomware-gangs-hunt-for-tax-software-to-ratchet-up-pressure-on-victims/

勒索软件：Egregor 新变种可能是对您的企业的下一个重大恶意软件威胁

日期: 2020-11-25

等级: 高

来源: Danny Palmer

标签: ['Egregor', 'Digital Shadows', 'Ransomware', 'Variant', 'Bitcoin']

随着网络犯罪分子将勒索软件作为一种加密易受攻击网络的首选手段，试图利用受害者的比特币，勒索软件的一种新形式正变得越来越多产。 Egregor 勒索软件最早出现在 9 月份，但在几起备受瞩目的事件之后，包括针对书商 Barnes & Noble 以及视频游戏公司 Ubisoft 和 Crytek 的攻击，已经变得臭名昭著。 根据 Digital Shadows 的网络安全研究人员的说法，Egregor 勒索软件已经在全球 19 个不同行业中夺走了至少 71 名受害者，而且其背后的团队很可能只是在精心策划了其活动之后才刚刚开始。

详情

Ransomware: This new variant could be the next big malware threat to your business

https://www.zdnet.com/article/ransomware-this-new-variant-could-be-the-next-big-malware-threat-to-your-business/

Bandook 后门木马

日期: 2020-11-26

等级: 高

来源: CHECKPOINT

标签: ['Trojan', 'Bandook', 'Backdoor', 'Kazakh', 'Lebanese']

Check Point Research 最近观察到一股针对全球各种目标的新浪潮，利用了一种名为`Bandook`的 13 年前的后门木马。 Bandook 在 2015 年和 2017 年的活动中几乎消失，分别被称为"Manul 行动"和"Dark Caracal"。电子前沿基金会(EFF)和瞭望台发现，这些行动被认为是由哈萨克和黎巴嫩政府实施的。 在过去的一年里，这个曾经的商品恶意软件的几十个数字签名变体开始重新出现在威胁领域，重新点燃了人们对这个古老的恶意软件家族的兴趣。

详情

Bandook: Signed & Delivered

https://research.checkpoint.com/2020/bandook-signed-delivered/

佳能公开证实八月勒索软件攻击和数据泄露

日期: 2020-11-27

等级: 高

来源: Pierluigi Paganini

标签: ['Canon', 'Cloud', 'Ransomware', 'Data Breach']

佳能公司最终证实，它是 8 月初勒索软件攻击的受害者，攻击者也从其服务器中窃取了数据。 该漏洞最初是由 Bleepingcomputer 报告的，该事件跟踪了佳能 image.canon 云照片和视频存储服务的可疑中断。 据媒体报道，此事件导致免费 10GB 存储功能用户的数据丢失。

详情

Canon publicly confirms August ransomware attack and data breach

https://securityaffairs.co/wordpress/111523/malware/canon-confirms-ransomware-attack.html

Banijay 被 DoppelPaymer 勒索软件击中

日期: 2020-11-27

等级: 高

来源: Sergiu Gatlan

标签: ['Banijay', 'DoppelPaymer', 'Ransomware']

法国跨国生产和分销公司 Banijay Group SAS 遭到 DoppelPaymer 勒索软件攻击，敏感信息在事件中被勒索软件运营商窃取。目前，该集团在 22 个地区拥有 120 多家制作公司，并运营一些最大的全球娱乐品牌。Banijay 的品牌包括主厨、幸存者、老大哥、卡戴珊家族、憨豆先生、黑镜等等

详情

MasterChef, Big Brother producer hit by DoppelPaymer ransomware

https://www.bleepingcomputer.com/news/security/masterchef-big-brother-producer-hit-by-doppelpaymer-ransomware/

Sopra Steria 估计勒索软件攻击的财务影响可能达到 5000 万欧元

日期: 2020-11-29

等级: 高

来源: Pierluigi Paganini

标签: ['Sopra Steria', 'Ryuk', 'Ransomware']

法国 IT 外包商`Sopra Steria`遭到勒索软件攻击。虽然该公司没有透露感染其系统的恶意软件家族，但当地媒体猜测，这起勒索软件与`Ryuk`有关。这家欧洲 IT 公司在全球 25 个国家拥有 46000 名员工。它提供广泛的 It 服务，包括软件开发和咨询。现在该公司估计，最近的勒索软件攻击将对财务造成 4000 万欧元（4800 万美元）到 5000 万欧元（6000 万美元）不等的财务影响

详情

Sopra Steria estimates financial Impact of ransomware attack could reach €50 Million

https://securityaffairs.co/wordpress/111632/malware/sopra-steria-ransomware-losses.html

大规模威胁运动攻击开源回收开源仓库

日期: 2020-11-23

等级: 中

来源: Pierluigi Paganini

标签: ['Sonatype', 'CursedGrabber', 'npm', 'xpc.js', 'Machine Learning']

Sonatype 在 npm 注册表中发现了更多的恶意软件，根据 Sonatype 的分析和多个网络威胁情报报告，已经发现一个新的、大规模的恶意软件运动利用开源生态系统。 2020 年 11 月 20 日，Nexus Intelligence 研究服务发现了名为" xpc.js"的恶意软件，该服务包括下一代机器学习算法，可自动检测与开源生态系统相关的潜在恶意活动。

详情

Massive threat campaign strikes open-source reposSecurity Affairs

https://securityaffairs.co/wordpress/111321/malware/cursedgrabber-malware-campaign.html

TrickBot 恶意软件使用模糊的 Windows 批处理脚本来逃避检测

日期: 2020-11-24

等级: 中

来源: Ax Sharma

标签: ['TrickBot', 'Windows', 'Evade Detection', 'Batch Script']

随着`TrickBot`的第 100 版发布，该恶意软件配备了新的和先进的回避功能。 其中一种功能是使用混淆的批处理脚本启动器来启动恶意可执行文件。 批处理脚本不需要解析器，而是 Microsoft Windows 的内置命令提示符，这使得这种逃避技术变得自成体系且简约。 TrickBot 是一种恶意软件感染，通常通过恶意网络钓鱼电子邮件或其他恶意软件来安装。 安装后，TrickBot 将在受害者的计算机上安静地运行，同时下载其他模块以执行不同的任务。

详情

TrickBot malware uses obfuscated Windows batch script to evade detection

https://www.bleepingcomputer.com/news/security/trickbot-malware-uses-obfuscated-windows-batch-script-to-evade-detection/

Stantinko 的 Linux 恶意软件现在伪装成 Apache Web 服务器

日期: 2020-11-24

等级: 中

来源: Catalin Cimpanu

标签: ['Stantinko', 'Linux', 'Malware', 'Botnets', 'Apache Web']

Stantinko 是目前仍在运行的最古老的恶意软件僵尸网络之一，已推出对其 Linux 恶意软件类别的更新，将其木马升级为合法的 Apache Web 服务器进程（httpd），以使对受感染主机的检测更加困难。 安全公司 Intezer Labs 发现了这些升级，这证实了尽管在代码更改方面有一段时间处于不活跃状态，但 Stantinko 僵尸网络现在仍在运行。 Stantinko 僵尸网络于 2012 年首次被发现。该恶意软件背后的组织开始通过将`Stantinko`木马作为应用程序捆绑的一部分或通过盗版应用程序进行分发来进行操作。

详情

Stantinko's Linux malware now poses as an Apache web server

https://www.zdnet.com/article/stantinkos-linux-malware-now-poses-as-an-apache-web-server/

SSH 后门僵尸网络与“研究”感染技术

日期: 2020-11-26

等级: 中

来源: Pierluigi Paganini

标签: ['SSH Backdoor ', 'Botnet', 'Research', 'Discord CDN']

安全专家 Tolijan Trajanovski 分析了 SSH 后门僵尸网络，该僵尸网络实现了一种有趣的“研究”感染技术。 在最近的一条推文中，恶意软件研究员`@0xrb`共享了一个列表，其中包含最近捕获的 IoT 僵尸网络示例的 URL。 在链接中，有一个不常见的示例，`Discord CDN`后面的`URL`（如 IoT 恶意软件研究人员@_lubiedo 所指出的那样）可能难以阻止。

详情

SSH-backdoor Botnet With ‘Research’ Infection Technique

https://securityaffairs.co/wordpress/111477/malware/ssh-backdoor-botnet.html

勒索软件攻击美国最大的生育网络，病人数据被盗

日期: 2020-11-26

等级: 中

来源: Sergiu Gatlan

标签: ['US Fertility', 'Ransomware', 'Encrypted', 'Attack']

美国最大的生育中心网络 US Fertility 表示，两个月前，也就是 2020 年 9 月，该公司的一些系统在勒索软件攻击中被加密。 US Fertility 的网络由 10 个州的 55 个地点组成，2018

年通过其诊所和 80 多名医生完成了近 25000 个试管婴儿周期。 2020 年 9 月 14 日，USF 经历了一次 IT 安全事件由于恶意软件的感染，他们网络上的某些计算机系统无法访问。在对 11 月 13 日结束的攻击过程中访问的所有文件进行审查后，USF 确定未知勒索软件组过滤的文件包含每个受影响个人的各种类型的信息，包括姓名、地址、出生日期、MPI 编号和社会保险号码。

详情

Ransomware hits largest US fertility network, patient data stolen

https://www.bleepingcomputer.com/news/security/ransomware-hits-largest-us-fertility-network-patient-data-stolen/

Dark Caracal APT 组织仍然活跃

日期: 2020-11-29

等级: 中

来源: Pierluigi Paganini

标签: ['Trojan', 'Dark Caracal', 'Bandook', 'APT']

研究人员发现了一系列针对多个行业的新攻击，这些攻击来自`Dark Caracal`，`Dark Caracal`是一个与黎巴嫩总司令部有关联的 APT 组织，在最近的攻击中，它使用了一个名为 Bandook 的 13 年前的后门木马的新版本，该木马执行主要分为三个阶段。第一阶段利用一个微软 Word 文档（例如"认证文档.docx）在 ZIP 文件中传递。打开存档文件后，会下载恶意宏，然后继续删除并执行原始 Word 文档中加密的第二阶段 PowerShell 脚本。在攻击的最后阶段，PowerShell 脚本从合法的云存储服务（如 Dropbox 或 Bitbucket）下载编码的可执行部分，然后组装 Bandook 加载器，将 RAT 注入新的 internet explorer 进程中

详情

Operators behind Dark Caracal are still alive and operational

https://securityaffairs.co/wordpress/111617/apt/dark-caracal-still-active.html

相关安全建议

1. 注重内部员工安全培训
2. 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
3. 移动端不安装未知应用程序、不下载未知文件
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. 及时对系统及各个服务组件进行版本升级和补丁更新
6. 不盲目信任云端文件及链接
7. 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
8. 网段之间进行隔离，避免造成大规模感染

9. 各主机安装 EDR 产品，及时检测威胁

(二) 数据安全

黑客泄露事件管理应用程序 Peatix 的用户数据

日期: 2020-11-24

等级: 高

来源: Catalin Cimpanu

标签: ['Peatix', 'Alexa', 'Instagram stories', 'Telegram', 'Leaked']

2002 年 11 月，一名黑客泄露了在活动组织平台 Peatix 上注册的 420 多万用户的数据。 Peatix 目前是 Alexa 网站中最受欢迎的 3500 个网站之一。 该网站的用户数据可通过 Instagram stories，Telegram 频道以及几个不同的黑客论坛上发布的广告获得。 根据 ZDNet 看到的 Peatix 数据样本，泄露的信息包括全名、用户名、电子邮件以及加密和散列的密码。

详情

Hacker leaks the user data of event management app Peatix

https://www.zdnet.com/article/hacker-leaks-the-user-data-of-event-management-app-peatix/

百度的 Android 应用程序被发现收集和泄露敏感用户数据

日期: 2020-11-24

等级: 高

来源: The Hacker News

标签: ['Android', 'Baidu', 'Baidu Maps', 'Baidu Search Box', 'Google', 'the Play Store', 'Palo Alto', 'Leaked']

2020 年 10 月，中国科技巨头百度（Baidu）的两款热门安卓（Android）应用程序在收集用户敏感信息时被发现，已被从谷歌 Play 商店中删除。 被调查的两款应用程序百度地图和百度搜索框被发现在用户不知情的情况下收集设备标识符，如国际移动用户标识（IMSI）号码或 MAC 地址，从而使它们有可能在网上被追踪。 这项发现是由网络安全公司 Palo Alto Networks 发现的，该公司将其发现通知了百度和 Google，之后，搜索公司于 10 月 28 日以"未指定的侵权行为"为由撤消了这些应用。

详情

Baidu's Android Apps Caught Collecting and Leaking Sensitive User Data

https://thehackernews.com/2020/11/baidus-android-apps-caught-collecting.html

暴露了近 50000 个易受攻击的 Fortinet VPN 的密码

日期: 2020-11-25

等级: 高

来源: Ax Sharma

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

一名黑客泄露了近 5 万个易受攻击的 Fortinet vpn 的密码。 据 BleepingComputer 报道，2020 年 11 月 21 日，一名黑客发布了一份清单，列出了存在 CVE-2018-13379 漏洞的设

备，用以从这些设备窃取 VPN 证书。 利用严重的 FortiOS 漏洞 CVE-2018-13379，攻击者可以从 Fortinet VPN 中访问敏感的" sslvpn_websession"文件。 这些文件包含与会话有关的信息，但最重要的是，这些文件可能会显示 Fortinet VPN 用户的纯文本用户名和密码。

详情

Passwords exposed for almost 50,000 vulnerable Fortinet VPNs

https://www.bleepingcomputer.com/news/security/passwords-exposed-for-almost-50-000-vulnerable-fortinet-vpns/

1600 万巴西 COVID-19 患者的详细信息在网上曝光

日期: 2020-11-27

等级: 高

来源: Pierluigi Paganini

标签: ['Brazilian', 'COVID-19', 'Albert Einstein Hospita', 'GitHub']

由于巴西医院工作人员的失误，超过 1600 万巴西 COVID-19 患者的个人和健康详细信息在网上意外暴露。 圣保罗阿尔伯特爱因斯坦医院的一名员工在 GitHub 上上传了一份包含用户名、密码和敏感政府系统访问密钥的电子表格。 该电子表格包含用于多个系统的登录凭据，包括用于管理 COVID-19 患者数据的 E-SUS-VE 和 Sivep-Gripe 应用程序。

详情

Details of 16 million Brazilian COVID-19 patients exposed online

https://securityaffairs.co/wordpress/111534/data-breach/brazilian-covid-19-patients-leak.html

网络设备供应商 Belden 披露数据泄露

日期: 2020-11-27

等级: 高

来源: Catalin Cimpanu

标签: ['Belden', 'Networking Equipment', 'Data Breach', 'American']

美国网络设备供应商 Belden 表示，它在 2020 年 11 月 24 日早些时候发布的新闻稿中遭到黑客入侵。 Belden 表示，黑客侵入了有限数量的文件服务器后，就发生了安全漏洞。 在公司的 IT 人员检测到涉及受感染服务器的异常活动之后，才检测到入侵。 随后的调查显示，入侵者复制了一些现任和前雇员的数据，以及有关某些商业伙伴的有限公司信息。 Belden 目前正在通知其认为数据在事件中被泄露的客户和员工。

详情

Networking equipment vendor Belden discloses data breach

https://www.zdnet.com/article/networking-equipment-vendor-belden-discloses-data-breach/

Home Depot 同意就 2014 年数据泄露达成 1750 万美元的和解

日期: 2020-11-25

等级: 中

来源: Charlie Osborne

标签: ['Home Depot', 'Data Breach', 'Settlement', 'MageCart']

家得宝(Home Depot)同意支付 1750 万美元和解金，以了结 2014 年该公司遭受的数据泄露事件。 特拉华州总检察长凯西·詹宁斯（Kathy Jennings）2020 年 11 月 24 日宣布了和解协议，根据该协议，共有 46 个州以及哥伦比亚特区与美国零售商达成了和解。 2014 年，Home Depot 确认其付款系统发生了网络攻击，影响了美国和加拿大的客户。

详情

Home Depot agrees to $17.5 million settlement over 2014 data breach

https://www.zdnet.com/article/home-depot-agrees-to-17-5m-settlement-over-2014-data-breach/

Sophos 在安全漏洞发生后提醒客户信息泄露

日期: 2020-11-26

等级: 中

来源: Sergiu Gatlan

标签: ['Sophos', 'British', 'Personal Information']

英国网络安全和硬件公司 Sophos 向一小群客户发送电子邮件，提醒他们，他们的个人信息在 2020 年 11 月 24 日发现安全漏洞后被曝光。 未经授权的攻击者可以访问暴露的客户数据，这是由于公司使用了错误配置的"工具"来存储与公司支持团队联系的用户的信息。 Sophos 没有提供任何信息，没有说明是谁发现并泄露了这个不安全的存储工具，也没有透露有多少客户的个人信息因为这个安全漏洞而被泄露。

详情

Sophos alerts customers of info exposure after security breach

https://www.bleepingcomputer.com/news/security/sophos-alerts-customers-of-info-exposure-after-security-breach/

黑客出售数百份高管账号，每个 100 至 1500 美元

日期: 2020-11-28

等级: 中

来源: Pierluigi Paganini

标签: ['Exploit.in', 'Executives Info']

黑客正以每帐户 100 至 1500 美元的价格提供访问数百名 C 级主管的电子邮件帐户的权限。 在 Exploit.in 上可以访问数百位 C 级主管的电子邮件帐户，每个帐户的费用为 100 到 1500 美元。 Exploit.in 是一个流行的针对俄语俄语的地下论坛，与其相似的论坛还有 fuckav.ru，Blackhacker，Omerta 和 L33t。

详情

Hundreds of C-level executives credentials available for $100 to $1500 per account

https://securityaffairs.co/wordpress/111588/cyber-crime/executives-credentials-dark-web.html

相关安全建议

1. 条件允许的情况下，设置主机访问白名单
2. 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
3. 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
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. 及时备份数据并确保数据安全
7. 严格控制数据访问权限

(三) 网络攻击

巴西政府从有史以来最严重的网络攻击中恢复过来

日期: 2020-11-23

等级: 高

来源: Angelica Mari

标签: ['Brazilian', 'STJ', 'Ransomware', 'Cyberattack', 'Recovers']

在遭受了针对巴西公共部门机构有史以来最严重的网络攻击后，面临中断两周多的高级选举法院(STJ，葡萄牙语首字母缩写)终于设法让其系统恢复运行。 在 11 月 3 日发生勒索软件攻击后，STJ 的系统有 26 个小时完全不可用，因此联邦警察可以收集证据。 调查过程还包括联邦数据处理服务公司 Serpro 和美国陆军网络防御单位，目前仍在进行中。在 11 月 20 日系统全面重建之前，最高法院在处理紧急案件时只能发挥有限的功能。 STJ 的总统部长恩里克•马丁斯(Henrique Martins)表示，就规模和复杂性而言，这是巴西政府机构遭遇的"有史以来最严重的"网络攻击。

详情

Brazilian government recovers from "worst-ever" cyberattack

https://www.zdnet.com/article/brazilian-government-recovers-from-worst-ever-cyberattack/

黑客通过 GoDaddy 攻击加密货币平台

日期: 2020-11-23

等级: 高

来源: Prajeet Nair

标签: ['GoDaddy', 'Social Engineering', 'Cryptocurrency Platforms']

根据受害公司发布的通知，2020 年 11 月 20 日，攻击者通过访问`GoDaddy`管理的域来针对两个加密货币平台。 该域名注册公司以前曾遇到过未经授权的访问的问题。 根据安全博主`Brian Krebs`的说法，攻击者利用社会工程技术欺骗`GoDaddy`的员工暂时将对域名的控制权转移给攻击者，从而进入了这些平台。

详情

Fraudsters Target Cryptocurrency Platforms Through GoDaddy

https://www.databreachtoday.com/fraudsters-target-cryptocurrency-platforms-through-godaddy-a-15434

使用最新密钥的 Tesla Model X 在几分钟内就被破解了

日期: 2020-11-23

等级: 高

来源: Catalin Cimpanu

标签: ['Tesla Model X', 'Belgian', 'Lennert Wouters']

一位比利时安全研究人员发现了一种方法，可以覆盖和劫持 Tesla Model X 密钥卡的固件，从而使他能够窃取未运行最新软件更新的任何汽车。 该攻击仅需花费几分钟即可执行，只需要廉价的装备，由比利时鲁汶天主教大学（KU Leuven）的计算机安全和工业密码学（COSIC）研究组的博士生 Lennert Wouters 进行。 这是多年来 Wouters 的第三次 Tesla 攻击。

详情

Tesla Model X hacked and stolen in minutes using new key fob hack

https://www.zdnet.com/article/tesla-model-x-hacked-and-stolen-in-minutes-using-new-key-fob-hack/

针对 30 万以上 Spotify 用户的凭据填充攻击

日期: 2020-11-24

等级: 高

来源: Pierluigi Paganini

标签: ['Spotify', 'Credential Stuffing Attack', 'Database', 'vpnMentor', 'Botnets', 'Elasticsearch']

来自 vpnMentor 的安全专家发现了一个可能影响到一些 Spotify 账户的凭证填充攻击。这场运动背后的攻击者使用了一个包含超过 3.8 亿记录的数据库，其中包括登录凭据和 Spotify 账户的其他数据，这些数据可能来自不同的来源。 专家估计，受影响的用户数量在 30 万到 35 万之间。

详情

Credential stuffing attack targeted 300K+ Spotify users

https://securityaffairs.co/wordpress/111363/hacking/credential-stuffing-spotify.html

国际刑警组织逮捕了 3 名尼日利亚 BEC 诈骗犯，他们的目标超过 50 万个实体

日期: 2020-11-25

等级: 高

来源: The Hacker News

标签: ['Interpol', 'Nigerian', 'Malware', 'Phishing']

国际刑警组织 2020 年 11 月 24 日报道，三名涉嫌参与网络犯罪组织的尼日利亚公民在拉各斯被捕，该组织散布恶意软件，实施网络钓鱼活动，以及大规模商业电子邮件入侵(BEC)

骗局。 此次被称为"猎鹰行动"的调查，是由国际警察组织、新加坡网络安全公司 Group-IB 以及尼日利亚警察部队联合开展的。 尼日利亚警察部队是该国主要的执法机构。到目前为止，随着调查继续追踪其他嫌疑团伙成员和该集团采用的货币化方法，已经确定了约 50,000 名犯罪计划的目标受害者。

详情

Interpol Arrests 3 Nigerian BEC Scammers For Targeting Over 500,000 Entities
https://thehackernews.com/2020/11/interpol-arrest-3-nigerian-bec-scammers.html

恶意软件在被黑客攻击的 WordPress 网站上创建诈骗在线商店

日期: 2020-11-23

等级: 中

来源: Catalin Cimpanu

标签: ['WordPress', 'Brute Force', 'Hijacking', 'C&C']

一个新的网络犯罪团伙已经接管了存在漏洞的 WordPress 网站，安装隐藏的电子商务商店，目的是劫持原网站的搜索引擎排名和声誉，并推广网络诈骗。 该攻击是 2020 年 11 月初发现的，目标是由 Akamai 安全团队建立和管理的 WordPress 蜜罐。 攻击者利用暴力破解来访问网站的管理员帐户，然后重写了 WordPress 网站的主索引文件并附加了恶意代码。

详情

Malware creates scam online stores on top of hacked WordPress sites
https://www.zdnet.com/article/malware-creates-online-stores-on-top-of-hacked-wordpress-sites/

FBI：我们网站的虚假版本可用于网络攻击，因此请当心

日期: 2020-11-24

等级: 中

来源: Liam Tung

标签: ['FBI', 'Cyberattacks', 'Fake']

联邦调查局（FBI）警告公众，避免使用外观类似于其主要官方网站 www.fbi.gov 的互联网域名。 该警告涉及数十个网站，这些网站可用于定位寻求联邦调查局活动或新闻公告信息的人。 联邦调查局在 2020 年 11 月 23 日发布的公共服务公告(PSA)中表示:"联邦调查局发现，不明身份的网络行为者注册了大量域名，欺骗了联邦调查局的合法网站，这表明未来可能会有此类活动。"

详情

FBI: Fake versions of our site could be used for cyberattacks, so watch out
https://www.zdnet.com/article/fbi-fake-versions-of-our-site-could-be-used-for-cyberattacks-so-watch-out/

网络巨头 Belden 公司数据在网络攻击中被盗

日期: 2020-11-25

等级: 中

来源: Lawrence Abrams

标签: ['Belden', 'Cyberattack', 'Steal']

网络设备制造商 Belden 遭受网络攻击，攻击者可以利用该攻击窃取包含有关员工和业务合作伙伴信息的文件。 贝尔登是一家总部位于美国的网络连接设备制造商，产品包括路由器、防火墙、交换机、电缆和连接器。贝尔登在 2019 年创造了 25 亿美元的收入，雇佣了大约 9000 名员工。 贝尔登称他们最近遭受了一次网络攻击，黑客窃取了公司数据。

详情

Belden networking giant's company data stolen in cyberattack

https://www.bleepingcomputer.com/news/security/belden-networking-giants-company-data-stolen-in-cyberattack/

丹麦新闻社 Ritzau 遭勒索软件袭击，但没有支付赎金

日期: 2020-11-26

等级: 中

来源: Pierluigi Paganini

标签: ['Ritzau', 'Danish', 'Ransomware', 'Ransom']

丹麦最大的新闻社 Ritzau 受到勒索软件攻击的打击，使其服务被迫下线。 网络攻击造成了`Ritzau`100 台服务器中的四分之一收到损坏。 该机构确认已拒绝了赎金要求，但未透露金额。 Ritzaus Bureau A / S（简称 Ritzau）是由 Erik Ritzau 于 1866 年成立的丹麦新闻社。它与其他三个斯堪的纳维亚新闻社合作，提供北欧新闻（北欧新闻）。

详情

Danish news agency Ritzau hit by ransomware, but did not pay the ransom

https://securityaffairs.co/wordpress/111507/cyber-crime/ritzau-ransomware-attack.html

网络钓鱼用伪造的“重返工作岗位”内部备忘录引诱员工

日期: 2020-11-27

等级: 中

来源: Sergiu Gatlan

标签: ['COVID-19', 'Phishing', 'Steal Email', 'G Suite']

黑客试图通过伪装成公司内部“重返工作岗位”备忘录的仿冒电子邮件，盗取员工的电子邮件凭证。根据电子邮件安全公司的研究人员提供的统计数据，这些网络钓鱼邮件绕过了`G Suite`的电子邮件防御系统，成功地登陆了数千个目标个人的邮箱。考虑到在新冠疫情期间，大多数公司都会定期给员工发电子邮件，告知他们远程工作政策的变化，因此一些目标很有可能落入骗子的圈套。

详情

Phishing lures employees with fake 'back to work' internal memos

https://www.bleepingcomputer.com/news/security/phishing-lures-employees-with-fake-back-to-work-internal-memos/

CISA 警告易受攻击的 Fortinet VPN 上存在密码泄漏

日期: 2020-11-28

等级：中

来源：Akshaya Asokan

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

虽然已经快 2021 年，黑客仍然利用`CVE-2018-13379`攻击未修补的 Pulse Secure 和 Fortinet SSL VPN。安全人员在推特上发布了被曝光的 Fortinet 密码。在这条推文中，研究人员指出，泄露的密码属于与 Fortinet SSL VPN 相关的 49577 个 IP。CISA 警告说，黑客正在将漏洞（包括 FortineVPN 漏洞）与 Zerologon Windows 服务器漏洞联系起来，以攻击各地的网络

详情

CISA Warns Of Password Leak On Vulnerable Fortinet VPNs

https://www.databreachtoday.com/cisa-warns-password-leak-on-vulnerable-fortinet-vpns-a-15472

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. 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
3. 积极开展外网渗透测试工作，提前发现系统问题
4. 减少外网资源和不相关的业务，降低被攻击的风险
5. 做好产品自动告警措施
6. 及时对系统及各个服务组件进行版本升级和补丁更新
7. 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

英国 NCSC 警告敦促组织修复 MobileIron CVE-2020-15505 RCE

日期：2020-11-25

等级：高

来源：Pierluigi Paganini

标签：['CVE-2020-15505', 'MobileIron', ' RCE', 'Vulnerability', 'Orange Tsai']

英国国家网络安全中心（NCSC）发出警报，敦促组织解决 MobileIron 移动设备管理（MDM）系统中的 CVE-2020-15505 远程代码执行（RCE）漏洞，该漏洞危害严重。MDM 平台允许管理员从中央服务器远程管理组织中的移动设备群。 `CVE-2020-15505`漏洞是`MobileIron`移动设备管理（`MDM`）软件中的远程代码执行问题，该漏洞使远程攻击者可以执行任意代码并接管远程公司服务器。 安全研究员 Orange Tsai 在 3 月发现了该漏洞，MobileIron 在 6 月解决了该漏洞。

详情

UK NCSC's alert urges orgs to fix MobileIron CVE-2020-15505 RCE
https://securityaffairs.co/wordpress/111426/uncategorized/mobileiron-cve-2020-15505-alert.html

VMware 修复了能让黑客瞄准企业网络的 SD-WAN 漏洞

日期: 2020-11-23

等级: 高

来源: Pierluigi Paganini

标签: ['VMware', 'Vulnerability', 'SQL injection', 'Pass-the-Hash', 'SD-WAN']

VMware 2020 年 11 月 19 日在其`SD-WAN Orchestrator`产品中解决了六个漏洞（CVE-2020-3984，CVE-2020-3985，CVE-2020-4000，CVE-2020-4001，CVE-2020-4002，CVE-2020-4003） ，其中一些漏洞可以被攻击者用来劫持流量或关闭企业网络。 Realmode Labs 的 Ariel Tempelhof 报告了漏洞，这些漏洞可由未经身份验证的远程攻击者链接起来，以实现远程代码执行。

详情

VMware fixed SD-WAN flaws that could allow hackers to target enterprise networks
https://securityaffairs.co/wordpress/111328/security/sd-wan-orchestrator-flaws.html

30%的顶级在线购物域名容易受到 SSL 攻击

日期: 2020-11-24

等级: 高

来源: Edvardas Mikalauskas

标签: ['SSL Attack', 'Cybernews', 'Vulnerability', 'BEAST']

cybernews 分析了 2,600 多个在线购物域的 SSL 错误配置。 每个网站都应确保其服务器与用户之间的通信是加密的。 这对于在线购物和电子商务平台特别重要，该平台处理敏感的客户信息，例如身份验证凭据，信用卡号，银行数据和其他付款明细。 cybernews 发现，即使绝大多数在线商店通常遵循从优秀到良好的 SSL 配置做法，但 cybernews 分析的 Web 服务器中几乎有三分之一易受已知 SSL 漏洞的影响，而 BEAST 漏洞在在线商店中最为普遍。

详情

30% of top online shopping domains are vulnerable to BEAST SSL attack
https://cybernews.com/security/30-of-top-online-shopping-domains-are-vulnerable-to-beast-ssl-attack/

Facebook 在韩国因未经同意分享用户数据而被罚款

日期: 2020-11-26

等级: 高

来源: Cho Mu-Hyun

标签: ['Facebook', 'Share User Data', 'Fined', 'South Korea']

Facebook 在韩国被处以 67 亿韩元（约合 600 万美元）的罚款，原因是未经他们同意共享用户数据。 个人信息保护委员会（PIPC）表示，这家美国公司在 2012 年 5 月至 2018 年

6 月期间，未经其他公司同意，将其在韩国的 1800 万用户中至少 330 万的数据共享给其他公司。 该委员会表示，它还将对 Facebook 提起刑事诉讼，指控其违反了当地的个人信息法。

详情

Facebook fined in South Korea for sharing user data without consent
https://www.zdnet.com/article/facebook-fined-in-south-korea-for-sharing-user-data/

工业自动化系统中的一个严重漏洞

日期: 2020-11-29

等级: 高

来源: Pierluigi Paganini

标签: ['Automation', 'RTA', 'EtherNet/IP', 'Industrial Control Systems']

专家们在实时自动化（RTA）499ES EtherNet/IP 栈中发现了一个严重漏洞，该漏洞可能导致黑客攻击工业控制系统。根据`CVE-2020-25159`的描述，该漏洞 CVSS 评分为 9.8（满分 10 分），并影响 2012 年 11 月 21 日发布的 2.28 版本之前的所有 EtherNet/IP 适配器源代码堆栈。受影响的产品易受基于堆栈的缓冲区溢出的攻击，这可能使攻击者发送精心构造的数据包，从而导致拒绝服务条件或代码执行。

详情

A critical flaw in industrial automation systems opens to remote hack
https://securityaffairs.co/wordpress/111646/ics-scada/automation-systems-opens-flaw.html

GitHub 修复了 Google 发现的严重安全漏洞

日期: 2020-11-23

等级: 中

来源: Liam Tung

标签: ['GitHub', 'Google Project Zero', 'Vulnerability', 'Injection Attack']

GitHub 终于修复了三个多月前由 Google Project Zero 报告给它的严重的安全漏洞。 该漏洞影响了 GitHub 的 Actions 功能，是开发人员工作流自动化工具，Google Project Zero 研究人员 Felix Wilhelm 称其极易受到注入攻击。 尽管 Google 将其描述为严重性漏洞，但 GitHub 认为这是中危安全漏洞。

详情

GitHub fixes 'high severity' security flaw spotted by Google
https://www.zdnet.com/article/github-fixes-high-severity-security-flaw-spotted-by-google/

TikTok 补丁修复了 XSS 漏洞和点击劫持漏洞

日期: 2020-11-23

等级: 中

来源: Charlie Osborne

标签: ['TikTok', 'XSS', 'Account Takeover', 'Vulnerability']

`TikTok`修复了一个`XSS`安全漏洞和一个导致帐户接管影响该公司 Web 域的漏洞。 研究人员 Muhammed" milly" Taskiran 通过漏洞赏金平台 HackerOne 报告说，第一个漏洞与`tiktok.com`域上的 URL 参数有关，该 URL 参数没有得到适当的处理。 在对平台进行 Fuzz 测试时，`bug bounty`研究员发现这个问题可能被用来实现反射跨站点脚本(XSS)，潜在地导致在用户浏览器会话中执行恶意代码。

详情

TikTok patches reflected XSS bug, one-click account takeover exploit

https://www.zdnet.com/article/tiktok-patches-reflected-xss-bug-one-click-account-takeover-exploit/

苹果全球安全负责人因受贿指控被起诉

日期: 2020-11-24

等级: 中

来源: Campbell Kwan

标签: ['Apple', 'Santa Clara County', 'Thomas Moyer', 'Indicted', 'Bribery']

加州一家大陪审团对苹果公司全球安全负责人托马斯·莫耶（Thomas Moyer）提出起诉，指控他贿赂两名圣克拉拉县警察，以获得 4 张隐藏的枪支许可证。 这些指控是在地方检察官办公室进行了为期两年的调查之后产生的，该调查发现两名警察`Rick Sung`和`James Jensen`据称暂缓发放了这些执照，并拒绝将其释放给`Moyer`，直到他提供有价值的东西为止。

详情

Apple's global security head indicted for bribery charges

https://www.zdnet.com/article/apples-global-security-head-indicted-for-bribery-charges/

黑客因运行服务绕过防病毒软件而被捕

日期: 2020-11-24

等级: 中

来源: GURUBARAN S

标签: ['CyberSeal', 'DataProtector', 'Bypass Antivirus Software', 'Romanian', 'Malware Crypting Services']

罗马尼亚警方 2020 年 11 月 24 日逮捕了两名个人，原因是他们涉嫌经营两项恶意软件加密服务，`CyberSeal`和`DataProtector`，以逃脱防病毒软件的检测。 1560 名犯罪分子购买了这些服务，用于加密几种不同类型的恶意软件，包括远程访问木马、信息窃取和勒索软件。 两人还使用了 Cyberscan 服务，该服务允许其客户端使用防病毒工具测试其恶意软件。

详情

Hackers Arrested for Running Services To Bypass Antivirus Software

https://gbhackers.com/malware-operators-arrested/

cPanel 的 2FA 绕过可能会让数千万的网站受到黑客攻击

日期: 2020-11-24

等级: 中

来源: Pierluigi Paganini

标签: ['cPanel', 'Digital Defense', 'Vulnerability', 'Bypass', '2FA']

来自 Digital Defense 的研究人员发现了 cPanel 中的一个漏洞，攻击者可能会利用该漏洞绕过 cPanel 帐户的双因素身份验证。 cPanel 是一种流行的软件套件，可简化网络托管服务器的管理。 攻击者可以利用这个漏洞绕过 cPanel 账户的双因素认证(2FA)，并接管相关网站。

详情

2FA bypass in cPanel potentially exposes tens of millions of websites to hack
https://securityaffairs.co/wordpress/111415/hacking/2fa-bypass-cpanel.html

Xbox 漏洞可能会让黑客将玩家标签与玩家的电子邮件链接起来

日期: 2020-11-25

等级: 中

来源: Catalin Cimpanu

标签: ['Microsoft', 'Xbox', 'Vulnerability', 'Bug Bounty']

微软在 Xbox 网站上修复了一个漏洞，该漏洞可能使攻击者将 Xbox 游戏玩家标签（用户名）链接到用户的真实电子邮件地址。 该漏洞是通过 Microsoft 公司最近启动的 Xbox Bug 赏金计划报告的。 Joseph"Doc"Harris 是 2020 年向微软报告该问题的几位安全研究人员之一，2020 年 11 月 24 日早些时候他与 ZDNet 分享了他的发现。 这位安全研究人员说，漏洞是在 enforcement.xbox.com 上发现的，Xbox 用户可以在该网站上查看针对其 Xbox 个人资料的攻击，如果他们觉得自己在 Xbox 网络上的行为受到了不公平的批评，还可以提交申诉。

详情

Xbox bug could have allowed hackers to link gamer tags with players' emails
https://www.zdnet.com/article/xbox-bug-could-have-allowed-hackers-to-link-gamer-tags-with-players-emails/

windows7 和 windows server 2008 的 0day 漏洞仍未修复

日期: 2020-11-26

等级: 中

来源: Pierluigi Paganini

标签: ['Windows 7', 'Windows Server 2008', 'Zero Day', 'PowerUp']

法国安全研究员 Clément Labro 发现了一个 0day 漏洞，该安全研究员正在研究更新的 Windows 安全工具。 研究人员正在开发自己的 Windows 特权升级枚举脚本，称为 PrivescCheck，它是著名 PowerUp 的一种更新和扩展版本。 专家确认，该漏洞影响 Windows 7 和 Windows Server 2008 R2 操作系统。

详情

A zero-day in Windows 7 and Windows Server 2008 has yet to be fixed
https://securityaffairs.co/wordpress/111485/hacking/windows-7-server-2008-0day.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