安全事件周报

安全事件周报 (12.07-12.13)

360CERT
北京奇虎科技有限公司 | 2020-12-14

报告信息

报告名称	安全事件周报（12.07-12.13）		
报告类型	安全事件周报	报告编号	B6-2020-121402
报告版本	1.0	报告日期	2020-12-14
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	2020-12-14	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 54 项

话题集中在`漏洞修复`、`勒索软件`方面，涉及的组织有：`QNAP`、`富士康`、`FireEye`、`Starbucks`等。数据买卖、数据盗窃频发，企业信息保护不可忽视。

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
富士康遭勒索软件袭击，被勒索 3400 万美元赎金	★★★★★
勒索软件攻击受害者的备份系统	★★★★
支付卡掠取集团部署 Raccoon 恶意软件	★★★★
俄罗斯黑客将 Zebrocy 恶意软件隐藏在虚拟磁盘映像中	★★★★
Qbot 恶意软件利用 Windows 自启动	★★★★
njRAT 木马运营商使用 Pastebin 替代 C2 服务器	★★★★
StealthyTrident 行动：公司软件受到攻击	★★★★
PgMiner 僵尸网络爆破攻击 PostgreSQL 数据库	★★★★
Pay2Key 黑客窃取英特尔 Habana 实验室的数据	★★★★
TrickBot 使用被入侵的 Subway UK 营销系统进行网络钓鱼	★★★★
伊朗的 RANA Android 恶意软件监视通讯工具	★★★
勒索软件迫使托管提供商 Netgain 关闭数据中心	★★★
伊朗的 Android 间谍软件监听私人聊天	★★★
Adrozek 恶意软件在多个浏览器中将广告悄悄地注入搜索结果	★★★
数据安全	**等级**
黑客在一个暗网上出售超过 85000 个 SQL 数据库	★★★★★
25 万个被盗的 MySQL 数据库在暗网出售	★★★★★
牙科诊所供应商遭黑客攻击，暴露了 100 多万名患者的信息	★★★★★
黑客泄露了世界第三大飞机制造商 Embraer 的数据	★★★★
新泽西州传真公司泄露 56 万多封电子邮件和加密密码	★★★★
科技公司 UiPath 遭受数据泄露	★★★★
意外暴露个人信息后，Spotify 重设用户密码	★★★

网络攻击	等级
安全公司 FireEye 披露了安全漏洞	★★★★★
挪威称俄罗斯黑客组织 APT28 是 2020 年 8 月议会黑客事件的幕后黑手	★★★★
新的鱼叉式钓鱼电子邮件模仿微软域名	★★★★
黑客将窃取工具隐藏在网站的 CSS 文件中	★★★★
SideWinder APT 组织针对尼泊尔、阿富汗发起攻击	★★★★
欧洲药品管理局遭到网络攻击	★★★★
Cisco 前工程师因发起黑客攻击被判 2 年监禁	★★★★
WordPress 插件 0day 使成千上万的网站受到黑客攻击	★★★★
俄罗斯黑客利用新的 VMware 漏洞窃取数据	★★★
伪造的数据泄露告警用于窃取 Ledger 加密货币钱包	★★★
Facebook 追踪 APT32 OceanLotus 黑客到越南的 IT 公司	★★★
CISA 和 FBI 警告称黑客攻击 K-12 远程教育	★★★
其他事件	**等级**
数以百万计的物联网设备面临 TCP/IP 堆栈漏洞的风险	★★★★★
严重的 MDHexRay 漏洞影响 100 多种医疗成像系统	★★★★★
青少年承认参与 2016 年震撼互联网的 DDoS 攻击	★★★★★
Microsoft 团队报告的零点击可修复 RCE 漏洞	★★★★
PlayStation 修复了严重的远程代码执行漏洞	★★★★
D-linkvpn 路由器修复了远程命令注入漏洞	★★★★
微软 2020 年 12 月 12 日的补丁日修补了 58 个漏洞	★★★★
Adobe 安全更新修复了 Lightroom 中的严重漏洞	★★★★
Apache 修复了 Struts 2 中的代码执行漏洞	★★★★
Starbucks 修复了移动平台中发现的远程代码执行漏洞	★★★★

Valve 的 Steam 服务器漏洞让黑客劫持在线游戏	★★★★
Cisco 修复了 Jabber 里的代码执行漏洞	★★★★
QNAP 修复了能接管 NAS 设备的严重漏洞	★★★
所有 Kubernetes 版本受到未修复的中间人攻击漏洞的威胁	★★★
OpenSSL 存在严重漏洞，请立即更新	★★★
比特币交易所运营商被判 5 年监禁	★★★
Google 开源了 Atheris，一个在 Python 代码中查找安全漏洞的工具	★★★
黑客使用 WinZip 不安全的服务器连接恶意软件	★★★
Sophos 修复了 Cyberoam OS 中的 SQL 注入漏洞	★★★
Glassdoor 公司审查平台发现严重 CSRF 漏洞	★★★
NI CompactRIO 控制器漏洞可能导致生产中断	★★★

三、 事件详情

(一) 恶意程序

富士康遭勒索软件袭击，被勒索 3400 万美元赎金

日期: 2020-12-07

等级: 高

来源: Lawrence Abrams

标签: ['Foxconn', 'Ransomware', 'Electronics', 'DoppelPaymer']

2020 年 11 月 29 日左右，富士康在墨西哥的一家工厂遭遇勒索软件攻击，攻击者窃取了未加密的文件，然后对设备进行加密。 富士康是全球最大的电子制造公司，2019 年的营业收入达到 1,720 亿美元，在全球拥有超过 80 万名员工。 富士康的子公司包括 Sharp Corporation，FIH Mobile 和 Belkin。 2020 年 12 月 7 日，DoppelPaymer 勒索软件在其勒索软件数据泄漏站点上发布了属于富士康 NA 的文件。 泄漏的数据包括常规业务文档和报告，但不包含任何财务信息或员工的个人详细信息。

详情

Foxconn electronics giant hit by ransomware, $34 million ransom

https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/

勒索软件攻击受害者的备份系统

日期: 2020-12-07

等级: 高

来源: Teri Robinson

标签: ['Clay Heuckendorf', 'Backup Systems', 'Ransomware', 'Ransom']

在 Clay Heuckendorf 和他的团队成员无法预计为何某些客户的备份数据丢失之前，攻击者就已经发起了勒索软件攻击。 攻击者删除了客户的备份映像并激活了服务器中的勒索软件。恶意软件在服务器上运行了六个月，他们安装了一个密钥记录器。 备份攻击通常会在锁定和加密文件系统之前抹去组织的备份基础结构和存储快照，从而阻止备份数据的恢复，从而使攻击者能威胁公司支付赎金。

详情

Ransomware attacks target backup systems, compromising the company 'insurance policy'

https://www.scmagazine.com/home/security-news/ransomware/ransomware-attacks-target-backup-systems-compromising-the-company-insurance-policy/

支付卡掠取集团部署 Raccoon 恶意软件

日期: 2020-12-08

等级: 高

来源: Akshaya Asokan

标签: ['FakeSecurity', 'Raccoon', 'JavaScript', 'Payment Card', 'Skimming Group']

安全公司 Group-IB 称，一个名为`FakeSecurity`的`JavaScript`信用卡盗取者组织最近部署了 Raccoon 恶意软件，目的是针对电子商务网站窃取受害者的支付卡详细信息。 这些电子商务网站在 2 月至 9 月期间在四次独立的攻击中成为攻击者的目标，这些活动使用了几种策略来传递 Raccoon 恶意软件。 这些攻击主要依靠带有恶意文件的网络钓鱼邮件来传播恶意软件。

详情

Payment Card Skimming Group Deployed Raccoon Infostealer

https://www.databreachtoday.com/payment-card-skimming-group-deployed-raccoon-infostealer-a-15549

俄罗斯黑客将 Zebrocy 恶意软件隐藏在虚拟磁盘映像中

日期: 2020-12-09

等级: 高

来源: Ionut Ilascu

标签: ['Zebrocy', 'APT28', 'VHD', 'Malware', 'Spear Phishing']

俄罗斯黑客将 Zebrocy 恶意软件打包在虚拟硬盘（VHD）中以避免被发现。 这种技术在最近`APT28` (Fancy Bear, Sofacy, Strontium, Sednit) 发起的鱼叉式钓鱼活动中被发现，钓鱼的最终目的是用`Zebrocy`工具的变体感染目标系统。 `Zebrocy`支持多种编程语言（AutoIT，C ++，C＃，Delphi，Go，VB.NET）。在最近的钓鱼活动中，攻击者选择了基于 Golang 的版本，而不是更常见的 Delphi 版本。

详情

Russian hackers hide Zebrocy malware in virtual disk images

https://www.bleepingcomputer.com/news/security/russian-hackers-hide-zebrocy-malware-in-virtual-disk-images/

Qbot 恶意软件利用 Windows 自启动

日期: 2020-12-09

等级: 高

来源: Sergiu Gatlan

标签: ['Qbot', 'Windows', 'Autostart', 'Cobalt Strike', 'Egregor']

Qbot 恶意软件的最新版本会在受感染的 Windows 设备关闭之前激活自身的持久性机制，并在系统重启或唤醒时自动删除所有痕迹。 Qbot（也称为 Qakbot，Quakbot 和 Pinkslipbot）是一种 Windows 银行木马，具有蠕虫功能，至少从 2009 年开始活跃，用于窃取银行凭证，个人信息和财务数据。 该恶意软件存在键盘记录功能，可以在受感染计算机上安装后门、部署 Cobalt Strike、提供 ProLock 和 Egregor 勒索软件的 payload。

详情

Qbot malware switched to stealthy new Windows autostart method

https://www.bleepingcomputer.com/news/security/qbot-malware-switched-to-stealthy-new-windows-autostart-method/

njRAT 木马运营商使用 Pastebin 替代 C2 服务器

日期: 2020-12-10

等级: 高

来源: Charlie Osborne

标签: ['C2', 'Pastebin', 'njRAT', 'Trojan', 'Payload', 'Botnet']

njRAT 远程访问木马（RAT）的运营商正在利用`Pastebin C2`隧道来避免网络安全研究人员的审查。 2020 年 12 月 8 日，Palo Alto Networks 公司的 42 号网络安全小组发现，`njRAT`（也称为`Bladabindi`）从`Pastebin`下载并执行`payload`，替代了传统的命令控制（C2）服务器。 利用`.NET`开发的`njRAT`是一种广泛使用的特洛伊木马，它能够远程劫持受损机器，能够执行的功能有截屏、数据过滤、键盘记录等。

详情

njRAT Trojan operators are now using Pastebin as alternative to central command server
https://www.zdnet.com/article/njrat-trojan-operators-are-now-using-pastebin-as-alternative-to-central-command-server/

StealthyTrident 行动：公司软件受到攻击

日期: 2020-12-10

等级: 高

来源: MathieuTartare

标签: ['Able Desktop', 'Mongolia', 'HyperBro', 'Backdoor', 'LuckyMouse', 'TA428']

ESET 研究人员发现，聊天软件 Able Desktop 是蒙古流行的业务管理软件的一部分，被蒙古 430 个政府机构使用，该聊天软件是用来给 HyperBro 提供后门的，研究人员还发现了与`ShadowPad`后门的连接，该连接现在至少被五个不同的攻击者使用。 研究人员认为`Able`更新系统自 2020 年 6 月以来一直遭到破坏。

详情

Operation StealthyTrident: corporate software under attack
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

PgMiner 僵尸网络爆破攻击 PostgreSQL 数据库

日期: 2020-12-13

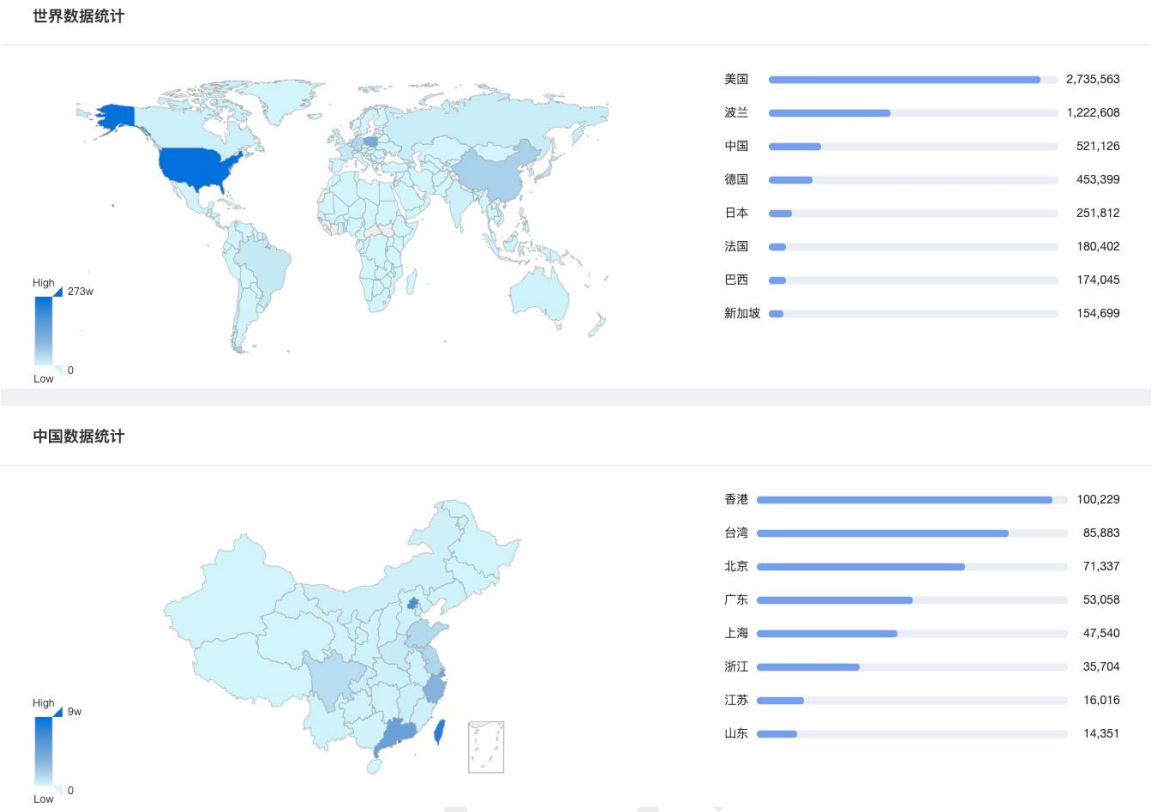
等级: 高

来源: Catalin Cimpanu

标签: ['PgMiner', 'PostgreSQL', 'Brute Force', 'Miner']

安全研究人员发现了一个僵尸网络操作，它针对 PostgreSQL 数据库安装加密货币 miner，被命名为 PgMiner。据研究人员称，僵尸网络的运作方式是对 internet 可访问的 PostgreSQL 数据库执行暴力攻击。僵尸网络随机选择一个公共网络范围（例如，18.xxx.xxx.xxx)然后遍历该范围内的所有 IP 地址，搜索在线公开 PostgreSQL 端口（端口 5432）的系统。如果 PgMiner 发现了一个活动的 PostgreSQL 系统，僵尸网络将从扫描阶段移动到它的暴力破解阶段，试图猜测`postgres`用户的密码。

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



详情

PgMiner botnet attacks weakly secured PostgreSQL databases

https://www.zdnet.com/article/pgminer-botnet-attacks-weakly-secured-postgresql-databases/

Pay2Key 黑客窃取英特尔 Habana 实验室的数据

日期: 2020-12-13

等级: 高

来源: Pierluigi Paganini

标签: ['Habana Labs', 'Intel', 'Pay2key', 'Chipmaker']

英特尔旗下的人工智能芯片制造商 Habana 实验室遭到 Pay2key 勒索软件运营商的黑客攻击，攻击者在推特上声称窃取了敏感数据，其中包括一种代号为高迪（Gaudi）的新型人工智能芯片的信息。黑客共享了一个泄漏目录的链接，以及源代码和属于被黑客公司的内部进程的图像。黑客还声称已经进入了公司的域控制器，如果这是真的，这将表明他们能够破坏公司的所有组织网络。

详情

Pay2Key hackers stole data from Intel's Habana Labs

https://securityaffairs.co/wordpress/112258/data-breach/pay2key-hacked-habana-labs.html

TrickBot 使用被入侵的 Subway UK 营销系统进行网络钓鱼

日期: 2020-12-13

等级: 高

来源: Pierluigi Paganini

标签: ['Subway UK', 'TrickBot', 'Excel', 'Phishing']

黑客入侵了英国地铁公司的一个营销系统，并利用它发送网络钓鱼信息，向客户发送恶意软件。该恶意电子邮件内容是处理所谓的地铁订单，其中包括一个链接，指向一个恶意的 Excel 文档，这些 Excel 文档将安装最新版本的 TrickBot 恶意软件。英国地铁公司立即启动事件响应程序，并向受影响的客户发送预警通知电子邮件。

详情

Hacked Subway UK marketing system used in TrickBot phishing campaign

https://securityaffairs.co/wordpress/112248/data-breach/subway-uk-trickbot-phishing.html

伊朗的 RANA Android 恶意软件监视通讯工具

日期: 2020-12-07

等级: 中

来源: The Hacker News

标签: ['Android', 'Iranian', 'FBI', 'RANA']

2020 年 12 月 7 日，一组研究人员公布了一款以前未公开的 `Android` 间谍软件植入功能，该软件是由伊朗一个受制裁的黑客开发的。 该软件可以让攻击者监视流行即时通讯应用的私人聊天，强制 Wi-Fi 连接，自动接听特定号码的来电，以便窃听通话。

详情

Iranian RANA Android Malware Also Spies On Instant Messengers

https://thehackernews.com/2020/12/iranian-rana-android-malware-also-spies.html

勒索软件迫使托管提供商 Netgain 关闭数据中心

日期: 2020-12-08

等级: 中

来源: Lawrence Abrams

标签: ['Netgain', 'Cloud', 'Ransomware', 'Take Down ', 'Cyberattack']

2020 年 11 月下旬，云托管和 IT 服务提供商 Netgain 在遭遇勒索软件攻击后，其部分数据中心下线。 Netgain 为医疗保健和会计行业的公司提供托管和云 IT 解决方案，包括托管 IT 服务和桌面即服务环境。 Netgain 声称他们是 2020 年 11 月 24 日勒索软件攻击的受害者。12 月 4 日，客户开始收到来自`Netgain`的电子邮件，邮件里说由于主机托管提供商受到网络攻击，他们可能会遭遇系统宕机。

详情

Ransomware forces hosting provider Netgain to take down data centers

https://www.bleepingcomputer.com/news/security/ransomware-forces-hosting-provider-netgain-to-take-down-data-centers/

伊朗的 Android 间谍软件监听私人聊天

日期: 2020-12-09

等级: 中

来源: Prajeet Nair

标签: ['Android', 'ReversingLabs', 'APT 39', 'Spyware', 'Iranian']

根据安全公司 ReversingLabs 的报告，Android 间谍软件背后的黑客组织增加了新的功能，包括侦听`Skype`，`Instagram`和`WhatsApp`上的私人聊天。 涉嫌开发该恶意软件的组织被称为`APT 39`，也称为`Chafer Remexi`，`Cadelspy`和`ITG`。 该组织被认为与伊朗政府有联系，`APT 39`和一家名为`Rana Intelligence Computing Co.`的联营公司均由伊朗情报和安全部控制。

详情

Iranian-Linked Android Spyware Sneaks Into Private Chats

https://www.databreachtoday.com/iranian-linked-android-spyware-sneaks-into-private-chats-a-15556

Adrozek 恶意软件在多个浏览器中将广告悄悄地注入搜索结果

日期: 2020-12-11

等级: 中

来源: Pierluigi Paganini

标签: ['Microsoft', 'Adrozek', 'Browser', 'Extensions']

微软警告称，一种名为`Adrozek`的新恶意软件会感染设备，并通过改变浏览器设置，在搜索结果页面中插入广告来劫持 Chrome、Edge 和 Firefox 浏览器。用户被重定向到欺诈域，在那里他们被诱骗安装了受污染的软件。攻击者通过附属广告项目赚取收入，这些项目按赞助附属网页的流量付费。

详情

Adrozek malware silently inject ads into search results in multiple browsers

https://securityaffairs.co/wordpress/112166/malware/adrozek-malware-campaign.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. 减少外网资源和不相关的业务，降低被攻击的风险
3. 及时对系统及各个服务组件进行版本升级和补丁更新
4. 包括浏览器、邮件客户端、vpn、远程桌面等在内的个人应用程序，应及时更新到最新版本
5. 注重内部员工安全培训
6. 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
7. 不盲目信任云端文件及链接

8. 移动端不安装未知应用程序、不下载未知文件
9. 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
10. 网段之间进行隔离，避免造成大规模感染

(二) 数据安全

黑客在一个暗网上出售超过 85000 个 SQL 数据库

日期: 2020-12-10

等级: 高

来源: Catalin Cimpanu

标签: ['SQL', 'Databases', 'Dark Web', 'ZDNet', 'Selling']

目前有超过 85,000 个 SQL 数据库在暗网上出售，每个数据库的价格只需 550 美元。 该网站是 ZDNet 的安全研究人员于 2020 年 12 月 10 日发现的，本次泄漏是自 2020 年初以来一直在进行的数据库勒索计划的一部分。 黑客已经攻击了 SQL 数据库，从数据库中下载数据，删除数据库原始文件，并留下赎金记录，以让服务器所有者联系攻击者，以取回他们的数据。

详情

Hackers are selling more than 85,000 SQL databases on a dark web portal

https://www.zdnet.com/article/hackers-are-selling-more-than-85000-sql-databases-on-a-dark-web-portal/

25 万个被盗的 MySQL 数据库在暗网出售

日期: 2020-12-10

等级: 高

来源: Ionut Ilascu

标签: ['BleepingComputer', 'Databases', 'MySQL', 'Dark Web']

黑客在暗网上建立了一个拍卖网站，出售从数万个被入侵的 MySQL 服务器中窃取的 25 万个数据库。 整个数据库的大小为 7TB，是数据库勒索业务的一部分，该业务自 2020 年 10 月以来急剧增加。 早在 2020 年 5 月份，BleepingComputer 就报告说，一个攻击者正在从网上商店窃取 SQL 数据库，并威胁受害者，如果他们不支付比特币，就讲他们的数据公开。

详情

250,000 stolen MySQL databases for sale on dark web auction site

https://www.bleepingcomputer.com/news/security/250-000-stolen-mysql-databases-for-sale-on-dark-web-auction-site/

牙科诊所供应商遭黑客攻击，暴露了 100 多万名患者的信息

日期: 2020-12-10

等级: 高

来源: Marianne Kolbasuk McGee

标签: ['Florida', 'Dental Practices', 'Data Breach', 'Support Services']

佛罗里达州的一家为 20 个州的数百家牙科诊所提供支持服务的公司表示遭到了黑客攻击，暴露了 100 多万名患者的信息，包括支付卡号。 该公司在其网站上称自己是美国规模最大、历史最悠久的牙科支持机构之一。 若联邦监管机构确认细节，该事件将是 2020 年迄今为止报道的最大的健康数据泄露事件之一。 根据提交给缅因州总检察长办公室的一份泄露通知报告，2020 年 10 月 11 日，总部位于佛罗里达州萨拉索塔的`Dental Alliance Care 11`发现了这起黑客事件。

详情

Vendor to Dental Practices Hacked: 1 Million Affected

https://www.databreachtoday.com/vendor-to-dental-practices-hacked-1-million-affected-a-15566

黑客泄露了世界第三大飞机制造商 Embraer 的数据

日期: 2020-12-07

等级: 高

来源: Catalin Cimpanu

标签: ['Embraer', 'Leak Data ', 'RansomExx', 'Dark Web']

巴西航空工业公司（Embraer）是继波音和空客之后的第三大飞机制造商，在 2020 年 11 月遭到勒索软件攻击。 2020 年 12 月 7 日，由于巴西航空工业公司拒绝支付赎金，参与入侵的黑客泄露了一些公司的私人文件，作为报复。 巴西航空工业公司的文件泄漏在了一个暗网的网站上，该网站由勒索软件集团（RansomExx，也称为 Defray777）管理。

详情

Hackers leak data from Embraer, world's third-largest airplane maker

https://www.zdnet.com/article/hackers-leak-data-from-embraer-worlds-third-largest-airplane-maker/

新泽西州传真公司泄露 56 万多封电子邮件和加密密码

日期: 2020-12-08

等级: 高

来源: Bernard Meyer

标签: ['Fax Express', 'Russian', 'New Jersey', 'Leaked', 'Database']

新泽西州的传真公司`Fax Express`在一个俄罗斯的黑客论坛上泄露了超过 56 万客户的电子邮件和经过过滤的明文密码。 `Fax Express`是一家总部位于新泽西州的海洋公司，主要销售传真机、复印机、打印机、碎纸机和相关物品。`Fax Express`自 1980 年开始运营，至今已有 40 年历史。

详情

New Jersey fax company leaks 560k+ emails and dehashed passwords

https://cybernews.com/security/new-jersey-fax-company-leaks-560k-emails-dehashed-passwords/

科技公司 UiPath 遭受数据泄露

日期: 2020-12-10

等级: 高

来源: Catalin Cimpanu

标签: ['UiPath', 'ZDNet', 'Robotics', 'Leaked']

科技公司 UiPath 是一家生产机器人自动化软件的初创公司，目前正在通过电子邮件向用户发送有关安全事件的信息，告知他们的个人信息在网上被泄露的安全事件。 该公司在 2020 年 12 月 10 日发给用户的一封电子邮件中写道：“2020 年 12 月 1 日，UiPath 发现了一起安全事件，该安全事件导致泄露了包含有关`UiPath Academy`用户的个人信息文件。”该文件包括真实姓名、电子邮件地址、用户名、公司名称、国家地点，以及 UiPath 在线学习平台 UiPath Academy 注册用户的 UiPath 认证详细信息。

详情

Tech unicorn UiPath discloses data breach

https://www.zdnet.com/article/robotics-unicorn-uipath-discloses-data-breach/

意外暴露个人信息后，Spotify 重设用户密码

日期: 2020-12-11

等级: 中

来源: Pierluigi Paganini

标签: ['Spotify', 'Vulnerability', 'Data Breach']

Spotify 通知用户，他们的个人信息可能在几个月内被无意中与某些业务合作伙伴共享。公司向加州司法部长提交了一份报告中称，2020 年 11 月 12 日，Spotify 系统中发现了一个漏洞，该漏洞无意中将您的 Spotify 帐户注册信息暴露给 Spotify 的某些业务伙伴，这些信息可能包括电子邮件地址、首选显示名、密码、性别和出生日期。”

详情

Spotify reset user passwords after accidentally personal information exposure

https://securityaffairs.co/wordpress/112215/data-breach/spotify-personal-information-exposure.html

相关安全建议

1. 及时备份数据并确保数据安全
2. 合理设置服务器端各种文件的访问权限
3. 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
4. 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
5. 及时检查并删除外泄敏感数据
6. 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
7. 严格做好主机的权限控制

(三) 网络攻击

安全公司 FireEye 披露了安全漏洞

日期: 2020-12-08

等级: 高

来源: Catalin Cimpanu

标签: ['FireEye', 'Hacking Tools', 'State-sponsored Attack']

全球最大的安全公司之一，FireEye 2020 年 12 月 8 日表示，它遭到了黑客攻击，攻击者访问了其内部网络，并窃取了 FireEye 用于测试其客户网络的黑客工具。 在 2020 年 12 月 8 日的新闻发布中，FireEye 首席执行官 Kevin Mandia 表示，攻击者还搜索了与该公司某些政府客户有关的信息。 曼迪亚（Mandia）将攻击者描述为"高度复杂的攻击者"，其纪律，操作和技术使他们相信这是国家资助的黑客攻击。

详情

FireEye, one of the world's largest security firms, discloses security breach

https://www.zdnet.com/article/fireeye-one-of-the-worlds-largest-security-firms-discloses-security-breach/

挪威称俄罗斯黑客组织 APT28 是 2020 年 8 月议会黑客事件的幕后黑手

日期: 2020-12-08

等级: 高

来源: Catalin Cimpanu

标签: ['Russia', 'the Norwegian Parliament', 'Norwegian', 'APT28', 'Parliament']

挪威警察特勤局（PST）2020 年 12 月 8 日称，APT28 是俄罗斯的军事黑客组织之一，很可能是该组织的黑客入侵了挪威议会的电子邮件帐户。 挪威议会(Stortinget)的黑客事件在 2020 年 9 月 1 日被披露。 当时，Stortinget 主管 Marianne 说，黑客侵入了议会的电子邮件系统，并进入了 Stortinget 员工和政府当选官员的收件箱。

详情

Norway says Russian hacking group APT28 is behind August 2020 Parliament hack

https://www.zdnet.com/article/norway-says-russian-hacking-group-apt28-is-behind-august-2020-parliament-hack/

新的鱼叉式钓鱼电子邮件模仿微软域名

日期: 2020-12-08

等级: 高

来源: Prajeet Nair

标签: ['Office 365', 'Microsoft', 'Ironscales', 'Spear Phishing', 'Domain']

据安全公司 Ironscales 称，鱼叉式网络钓鱼活动正在模仿`Microsoft.com`官方域名，并以该公司`Office 365`套件的用户为目标。 截止 2020 年 12 月 8 日，钓鱼邮件已经被在几千个邮箱中被发现，Ironscales 的报告发现，近 2 亿 office365 用户可能面临危险，因为这些邮件来自一个完全复制`Microsoft.com`域名的欺骗域。 这些钓鱼电子邮件已经针对金融服

务，医疗保健，保险，制造业，公用事业和电信行业中的 Office 365 用户。 在此次钓鱼攻击中，攻击者试图获取用户的凭据。

详情

Fresh Spear-Phishing Email Spoofs Microsoft Domain

https://www.databreachtoday.com/fresh-spear-phishing-email-spoofs-microsoft-domain-a-15547

黑客将窃取工具隐藏在网站的 CSS 文件中

日期: 2020-12-09

等级: 高

来源: Catalin Cimpanu

标签: ['JavaScript', 'Web Skimmer', 'CSS', 'Magecart', 'Credit Card']

在过去的两年中，网络犯罪组织使用了各种各样的技巧来将信用卡盗窃代码（也称为网络窃取工具或`Magecart`脚本）隐藏在在线商店的各个位置，以防止被发现。 过去发现的窃取工具的地方包括内部图像，例如网站图标或者社交媒体网络的图像、附加到流行的 JavaScript 库（如 jQuery，Modernizr 和 Google 跟踪代码管理器）或隐藏在网站小部件（例如实时聊天窗口）中。 在最新的攻击中，黑客将窃取工具隐藏在网站的 CSS 文件中。

详情

Hackers hide web skimmer inside a website's CSS files

https://www.zdnet.com/article/hackers-hide-web-skimmer-inside-a-websites-css-files/

SideWinder APT 组织针对尼泊尔、阿富汗发起攻击

日期: 2020-12-09

等级: 高

来源: Tara Seals

标签: ['SideWinder', 'Pakistan', 'Afghanistan', 'Phishing', 'Malware']

SideWinder APT 组织利用印度，尼泊尔和巴基斯坦之间最近的争端作为诱饵，发起了新的网络钓鱼攻击、传播恶意软件。 目标是收集位于尼泊尔和阿富汗的目标敏感信息。 这次攻击主要利用看上去合法的`webmail`登录页面，目的是获取登陆凭证。 趋势科技的研究人员表示，这些网页是从受害者实际的邮件登录页面复制过来的，然后经过修改，变成了钓鱼网站。

详情

SideWinder APT Targets Nepal, Afghanistan in Wide-Ranging Spy Campaign

https://threatpost.com/sidewinder-apt-nepal-afghanistan-spy-campaign/162086/

欧洲药品管理局遭到网络攻击

日期: 2020-12-09

等级: 高

来源: Pierluigi Paganini

标签: ['The European Medicines Agency', 'Cyberattack', 'COVID-19']

欧洲药品管理局（EMA）已成为网络攻击的目标。 EMA 没有提供有关攻击的技术细节，也没有表明此次攻击是否对其运营生产`COVID-19`疫苗产生影响。 欧洲药品管理局在整个欧盟的`COVID-19`疫苗生产环节中起着至关重要的作用，它可以访问敏感和机密信息，包括试验产生的质量，安全性和有效性数据。

详情

European Medicines Agency targeted by cyber attack

https://securityaffairs.co/wordpress/112125/intelligence/european-medicines-agency-cyberattack.html

Cisco 前工程师因发起黑客攻击被判 2 年监禁

日期: 2020-12-10

等级: 高

来源: Prajeet Nair

标签: ['Cisco', 'Ex-Cisco Engineer', 'Prison', 'AWS']

美国司法部 200 年 12 月 9 日宣布，前 Cisco 工程师被判入狱两年，此前他被控告黑客入侵 Cisco，总共造成 140 万美元的损失。 据负责监管此案的美国加州北区检察官办公室称，2020 年 8 月，31 岁的苏迪什·卡萨巴·拉梅什(Sudhish Kasaba Ramesh)承认了一项指控，即在未经授权的情况下，故意访问受保护的计算机，并不顾后果地造成损害。`Ramesh`从 2016 年 8 月至 2018 年 4 月在 Cisco 工作。离开公司后，他重新获得了对 Amazon Web Services 上 Cisco 托管的云基础架构的访问权限，并删除了 450 多个虚拟机，这给 Cisco 的 Webex 客户造成了停机问题。

详情

Ex-Cisco Engineer Sentenced to 2 Years in Prison for Hacking

https://www.databreachtoday.com/ex-cisco-engineer-sentenced-to-2-years-in-prison-for-hacking-a-15564

WordPress 插件 0day 使成千上万的网站受到黑客攻击

日期: 2020-12-12

等级: 高

来源: Pierluigi Paganini

标签: ['Easy WP SMTP', 'WordPress', '0day']

黑客正积极利用流行的`WordPress`插件`Easy WP SMTP`中的 0day 漏洞来重置管理员帐户的密码。该插件安装在超过 500000 个站点上，尽管安全补丁已经发布，但是许多站点还没有被修补。WP-SMTP WordPress 插件允许您通过 SMTP 服务器配置和发送所有传出的电子邮件，防止电子邮件进入收件人的垃圾邮件/垃圾邮件文件夹。

详情

WordPress Easy WP SMTP zero-day potentially exposes hundreds of thousands of sites to hack

https://securityaffairs.co/wordpress/112218/hacking/easy-wp-smtp-wordpress-plugin-flaw.html

俄罗斯黑客利用新的 VMware 漏洞窃取数据

日期: 2020-12-07

等级: 中

来源: Sergiu Gatlan

标签: ['NSA', 'Russian', 'VMware', 'CVE-2020-4006', 'Webshell', 'Vulnerability']

美国国家安全局(NSA)警告称，俄罗斯政府支持的黑客正在利用最近修补过的 VMware 漏洞，在易受攻击的服务器上部署 web shell，以窃取敏感信息。 美国国防部情报机构说：“国家安全局鼓励国家安全系统（NSS），国防部（DoD）和国防工业基地（DIB）网络管理员优先考虑缓解受影响服务器上的漏洞。” CVE-2020-4006 最初被评为严重漏洞，但 VMware 在发布补丁后，公开了利用限制：需要配置程序管理员帐户的有效密码。之后将评级从严重级别降低至高危。

详情

NSA: Russian state hackers exploit new VMware vulnerability to steal data

https://www.bleepingcomputer.com/news/security/nsa-russian-state-hackers-exploit-new-vmware-vulnerability-to-steal-data/

伪造的数据泄露告警用于窃取 Ledger 加密货币钱包

日期: 2020-12-10

等级: 中

来源: Lawrence Abrams

标签: ['Ledger', 'Fake Data Breach', 'Phishing', 'Cryptocurrency', 'Email']

一个网络钓鱼活动正在进行，该网络钓鱼攻击针对 Ledger 钱包用户，发送带有伪造的数据泄露通知，用于从收件人那里窃取加密货币。 Ledger 是一个硬件加密货币钱包，可让用户存储，管理和出售加密货币。 从 2020 年 10 月开始，Ledger 用户开始收到来自 Ledger 的有关数据泄露的虚假电子邮件。 电子邮件中指出，用户已受到违规行为的影响，因此他们应该安装最新版本的 Ledger Live，以使用新的密码保护其资产。

详情

Fake data breach alerts used to steal Ledger cryptocurrency wallets

https://www.bleepingcomputer.com/news/security/fake-data-breach-alerts-used-to-steal-ledger-cryptocurrency-wallets/

Facebook 追踪 APT32 OceanLotus 黑客到越南的 IT 公司

日期: 2020-12-10

等级: 中

来源: The Hacker News

标签: ['Facebook', 'OceanLotus', 'Vietnam', 'APT', 'CyberOne Group']

Facebook 的网络安全研究人员正式将越南 APT 组织`海莲花`与该国的一家 IT 公司联系起来，因为该组织被发现滥用其平台入侵人们的账户并分发恶意软件，自 2012 年以来，这些间谍活动的目标是促进越南的战略利益。Facebook 安全政策负责人纳撒尼尔·格莱彻（Nathaniel Gleicher）和网络威胁情报经理迈克·德维利亚斯基（Mike Dvilyanski）称：“调查将 APT32 与越南的一家 IT 公司 CyberOne Group（也称为 CyberOne Security、CyberOne Technologies、Hánh Tinh company Limited、Planet and Diacauso）有关。”

详情

Facebook Tracks APT32 OceanLotus Hackers to IT Company in Vietnam
https://thehackernews.com/2020/12/facebook-tracks-apt32-oceanlotus.html

CISA 和 FBI 警告称黑客攻击 K-12 远程教育

日期: 2020-12-11

等级: 中

来源: Pierluigi Paganini

标签: ['FBI', 'K-12', 'Distance Learning Education']

美国`CISA`和`FBI`警告称，针对美国`K-12`教育部门的勒索软件攻击有所增加，目的是窃取数据和破坏远程教育服务。攻击事件在 2020 学年初激增。美国 FBI、CISA 和 MS-ISAC 评估，黑客的目标是幼儿园到 12 年级（K-12）的教育机构。CISA 发布的警告称，预计此类攻击将持续到 2020-2021 学年。

详情

Threat actors target K-12 distance learning education, CISA and FBI warn
https://securityaffairs.co/wordpress/112194/malware/k-12-cisa-fbi-alert.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. 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
4. 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
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. 减少外网资源和不相关的业务，降低被攻击的风险
8. 做好产品自动告警措施

(四) 其他事件

数以百万计的物联网设备面临 TCP/IP 堆栈漏洞的风险

日期: 2020-12-07

等级: 高

来源: Jeremy Kirk

标签: ['IoT', 'RCE', 'TCP/IP', 'Stack', 'Amnesia:33']

数以百万计的消费者和企业 IoT 设备在其 TCP/IP 堆栈中存在软件漏洞，该漏洞会导致远程代码执行、拒绝服务或者完全接管设备。 `Forescout` 将该漏洞称为 `Amnesia:33`。多达 150 个供应商的设备可能会受到攻击。 这些漏洞影响了各种各样的嵌入式系统，包括医疗设备、工业控制系统、路由器和交换机，实际上是任何运行脆弱的 TCP/IP 协议栈的设备。受影响的设备的最大类别是企业和消费者物联网设备。

详情

Millions of IoT Devices at Risk From TCP/IP Stack Flaws

https://www.databreachtoday.com/millions-iot-devices-at-risk-from-tcpip-stack-flaws-a-15529

严重的 MDHexRay 漏洞影响 100 多种医疗成像系统

日期: 2020-12-08

等级: 高

来源: Ionut Ilascu

标签: ['GE Healthcare', 'MDHexRay', 'Vulnerability', 'CVE-2020-25179']

用于医疗成像设备的 GE Healthcare 管理软件中存在一个严重漏洞，该漏洞可能使患者的健康隐私受到威胁，甚至可能危及他们的生命。 该漏洞被称为 MDHexRay，漏洞编号为 CVE-2020-25179。 它影响了该公司十几个产品系列中的 100 多种 CT，X 射线，MRI 设备模型。 医疗保健网络安全公司 CyberMDX 发现并命名了该漏洞。 研究人员报告了该漏洞，并一直在协助 GE Healthcare 寻找修复方案。

详情

Severe MDHexRay bug affects 100+ GE Healthcare imaging systems

https://www.bleepingcomputer.com/news/security/severe-mdhexray-bug-affects-100-plus-ge-healthcare-imaging-systems/

青少年承认参与 2016 年震撼互联网的 DDoS 攻击

日期: 2020-12-10

等级: 高

来源: Sergiu Gatlan

标签: ['Mirai', 'Botnet', 'DDos', 'Attack']

Mirai 僵尸网络背后的一名运营商承认参与了 2016 年 10 月造成互联网大规模中断的 DDoS 攻击。 多家知名网站和在线服务因 DDos 攻击被关闭，包括亚马逊、PayPal、Visa、Netflix、PlayStation Network 和 Airbnb。 该僵尸网络是 Mirai 僵尸网络的变体，是由被告在 2015 年至 2016 年 11 月期间在其他人的帮助下开发的，专门用于 DDoS 攻击游戏平台。 被告在参与攻击时还是一名未成年人。

详情

Teen who shook the Internet in 2016 pleads guilty to DDoS attacks

https://www.bleepingcomputer.com/news/security/teen-who-shook-the-internet-in-2016-pleads-guilty-to-ddos-attacks/

Microsoft 团队报告的零点击可修复 RCE 漏洞

日期: 2020-12-07

等级: 高

来源: The Hacker News

标签: ['RCE', 'Microsoft', 'Windows', 'Oskars Vegeris', 'Evolution Gaming', 'Zero-Click', 'Vulnerability']

在微软团队的桌面应用程序中，一个零点击远程代码执行(RCE)漏洞允许攻击者通过发送一条特别编写的聊天消息来执行任意代码，从而危及目标的系统，该漏洞不需要用户交互。该漏洞最终导致终端用户完全丧失对私人聊天、文件、内部网络、私人密钥和 MS 团队之外的个人数据的机密性和完整性。 2020 年 8 月 31 日，Evolution Gaming 的安全工程师 Oskars Vegeris 向 Windows 报告了这个漏洞，然后微软在 10 月底将其修复。

详情

Zero-Click Wormable RCE Vulnerability Reported in Microsoft Teams

https://thehackernews.com/2020/12/zero-click-wormable-rce-vulnerability.html

PlayStation 修复了严重的远程代码执行漏洞

日期: 2020-12-08

等级: 高

来源: Pierluigi Paganini

标签: ['PlayStation Now', 'Parsia Hakimian', 'Vulnerability', 'Remote Code Execution']

漏洞赏金猎人 Parsia Hakimian 发现 PlayStation Now (PS Now)云游戏 Windows 应用程序存在多个安全漏洞，黑客可以在有漏洞的应用程序版本的 Windows 设备上执行任意代码。 在运行 Windows7SP1 或更高版本的系统上，这些漏洞影响了 PS Now 11.0.2 和更早的版本。 自 PlayStation Now 2014 年推出以来，订阅人数已超过 220 万。

详情

Critical remote code execution fixed in PlayStation Now

https://securityaffairs.co/wordpress/112049/hacking/playstation-now-rce.html

D-linkvpn 路由器修复了远程命令注入漏洞

日期: 2020-12-08

等级: 高

来源: Ionut Ilascu

标签: ['D-link', 'VPN', 'Routers', 'Remote Command Injection', 'Vulnerability']

D-link 是为多个路由器提供 VPN 直通功能的固件，在 D-link 中存在一个漏洞，攻击者能够利用该漏洞完全控制设备。 该漏洞会影响运行固件版本 3.17 或更低版本的路由器型号 DSR-150，DSR-250/N，DSR-500 和 DSR-1000AC。 数字防御漏洞研究团队 2020 年 8 月 11 日报告称，该漏洞是 root 命令注入，如果可以通过公共互联网访问设备的"统一服务路由器"web 接口，就可以远程利用该漏洞。

详情

D-Link VPN routers get patch for remote command injection bugs

https://www.bleepingcomputer.com/news/security/d-link-vpn-routers-get-patch-for-remote-command-injection-bugs/

微软 2020 年 12 月 12 日的补丁日修补了 58 个漏洞

日期: 2020-12-08

等级: 高

来源: Catalin Cimpanu

标签: ['Microsoft', 'Patch Tuesday', 'Vulnerability', 'RCE']

微软 2020 年 12 月 8 日发布了针对 10 多种产品和服务的 58 个安全补丁，这是微软每月安全更新（称为 Patch Tuesday）的一部分。 与微软每月发布的常规 100 多个修补程序相比，2020 年 12 月的修补程序数量较少，但这并不意味着这些漏洞的严重性就没有那么高了。 2020 年 12 月的补丁中有超过三分之一被归类为远程代码执行（RCE）漏洞。 这些安全漏洞易于利用，并且无需用户通过 Internet 或跨本地网络进行交互，危害极大。

详情

Microsoft December 2020 Patch Tuesday fixes 58 vulnerabilities

https://www.zdnet.com/article/microsoft-december-2020-patch-tuesday-fixes-58-vulnerabilities/

Adobe 安全更新修复了 Lightroom 中的严重漏洞

日期: 2020-12-09

等级: 高

来源: Charlie Osborne

标签: ['Adobe', 'Lightroom', 'Security Update', 'Vulnerability']

`Adobe`2020 年最后一次计划的安全更新修复了`Lightroom`、`Prelude`和`Experience Manager`中的严重漏洞。 `Adobe`的补丁修复程序于 2020 年 12 月 8 日发布，涉及四个漏洞，其中三个被认为是严重漏洞。 `Adobe`向奇虎 360 CERT 安全研究员侯敬宜致谢，该研究人员报告了漏洞。

详情

Adobe security update squashes critical vulnerabilities in Lightroom, Prelude

https://www.zdnet.com/article/adobe-security-update-squashes-critical-vulnerabilities-in-lightroom-prelude/

Apache 修复了 Struts 2 中的代码执行漏洞

日期: 2020-12-09

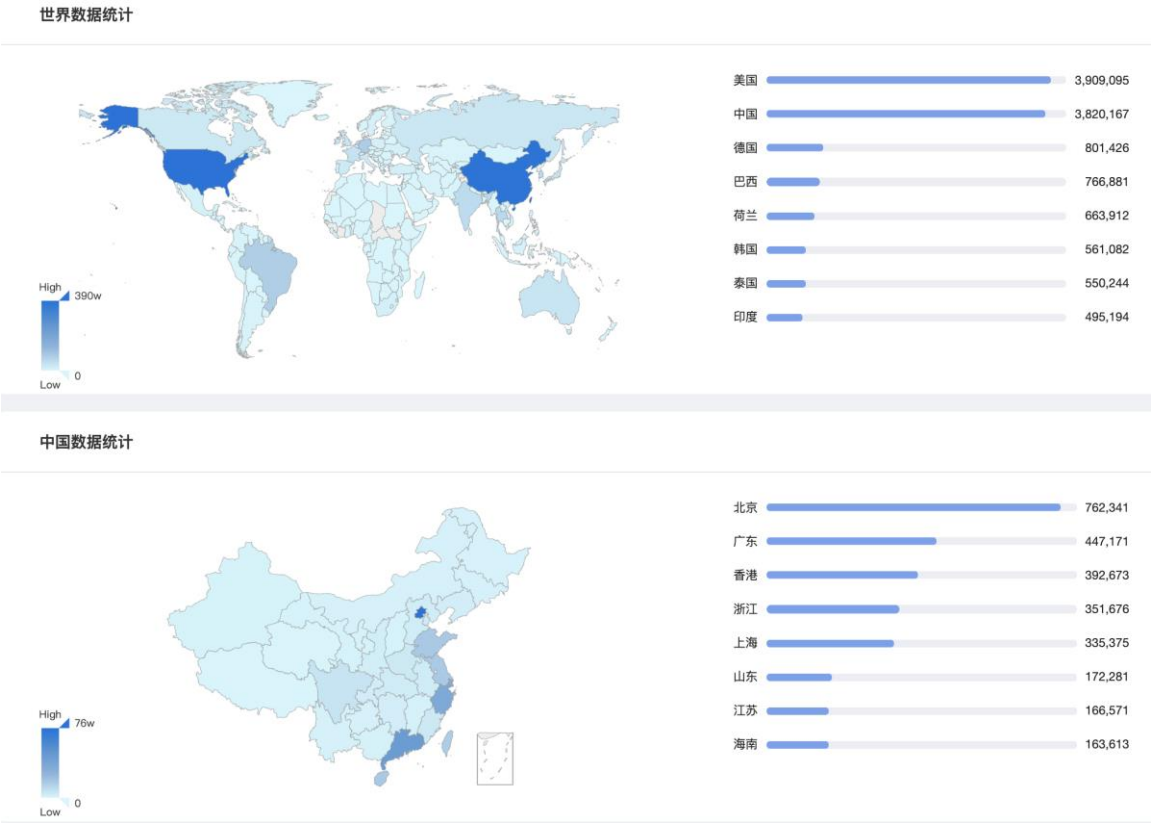
等级: 高

来源: Pierluigi Paganini

标签: ['Apache', 'Struts2', 'OGNL', 'Remote Code Execution']

Apache 在 2020 年 12 月 9 日发布了安全更新，以解决`Struts 2`中与`OGNL`技术有关的远程代码执行漏洞。 如果开发人员使用了 `%{...}` 语法，那么攻击者可以通过构造恶意的 `OGNL` 表达式，引发 `OGNL` 表达式二次解析，最终造成远程代码执行。 该漏洞影响 Struts2.0.0 到 Struts2.5.25，Struts2.5.26 的发布修复了这个漏洞。

目前 Struts2 的具体分布如下图，数据来自于 360 QUAKE



详情

Apache Software Foundation fixes code execution flaw in Apache Struts 2

https://securityaffairs.co/wordpress/112089/security/struts-2-flaw.html

Starbucks 修复了移动平台中发现的远程代码执行漏洞

日期: 2020-12-10

等级: 高

来源: Charlie Osborne

标签: ['RCE', 'Starbucks', 'HackerOne', 'Mobile', 'Vulnerability']

Starbucks 修复了移动平台中发现远程代码执行漏洞。 由`Kamil" ko2sec" OnurÖzkaleli`提交的新漏洞报告于 11 月 5 日，并于 12 月 9 日公开。该报告描述了在 mobile.starbucks.com.sg（面向新加坡用户的平台）上发现的 RCE 漏洞。 根据这份报告，`ko2sec`在`mobile.starbucks.com.sg`上发现了一个用于处理图像文件的`.ashx`上传点。但是，上传点没有限制文件类型的上传，这意味着攻击者滥用这个漏洞可以上传恶意文件并远程执行任意代码。

详情

Remote code execution vulnerability uncovered in Starbucks mobile platform

https://www.zdnet.com/article/remote-code-execution-vulnerability-uncovered-in-starbucks-mobile-platform/

Valve 的 Steam 服务器漏洞让黑客劫持在线游戏

日期: 2020-12-10

等级: 高

来源: The Hacker News

标签: ['Valve', 'Check Point', 'Steam', 'Vulnerability']

Valve 在线游戏的核心网络库中存在严重漏洞，利用该漏洞，攻击者可以远程让游戏的进程崩溃，甚至控制受影响的第三方游戏服务器。 `Valve`是一家受欢迎的美国游戏开发商和发行商，旗下拥有游戏软件发行平台`Steam`以及《半条命》、《反恐精英》、《传送门》、《胜利之日》、《军团要塞》、《求生之路》和《Dota》等多款游戏。

详情

Valve's Steam Server Bugs Could've Let Hackers Hijack Online Games

https://thehackernews.com/2020/12/valves-steam-server-bugs-couldve-let.html

Cisco 修复了 Jabber 里的代码执行漏洞

日期: 2020-12-10

等级: 高

来源: Sergiu Gatlan

标签: ['Cisco', 'RCE', 'Cisco Jabber', 'Wormable', 'Vulnerability']

Cisco 已经修复了一个严重的远程代码执行（RCE）漏洞，该漏洞影响了适用于 Windows，macOS 和移动平台的多个版本的 Cisco Jabber。Watchcom 的研究人员发现了这个可蠕虫的 RCE 漏洞。 Cisco Jabber 是使用 Chromium 嵌入式框架（CEF）构建的即时消息和网络会议桌面应用程序。

详情

Cisco fixes new Jabber for Windows critical code execution bug

https://www.bleepingcomputer.com/news/security/cisco-fixes-new-jabber-for-windows-critical-code-execution-bug/

QNAP 修复了能接管 NAS 设备的严重漏洞

日期: 2020-12-07

等级: 中

来源: Sergiu Gatlan

标签: ['NAS', 'QNAP', 'XSS', 'Command Injection ', 'Vulnerability']

网络附加存储（NAS）制造商 QNAP 2020 年 12 月 7 日发布了安全更新，修复了一个严重漏洞，攻击者能够在成功利用该漏洞之后控制未修补的 NAS 设备。 QNAP 一共修复了 8 个能够影响 NAS 设备的漏洞，这些漏洞包括 XSS、命令注入漏洞等。利用命令注入漏洞可以提升权限，在受损设备或应用程序上执行任意命令，并接管底层操作系统。

详情

QNAP patches QTS vulnerabilities allowing NAS device takeover

https://www.bleepingcomputer.com/news/security/qnap-patches-qts-vulnerabilities-allowing-nas-device-takeover/

所有 Kubernetes 版本受到未修复的中间人攻击漏洞的威胁

日期: 2020-12-08

等级: 中

来源: Sergiu Gatlan

标签: ['Kubernetes', 'MiTM', 'Vulnerability', 'Google']

Kubernetes 中存在一个漏洞，该漏洞可能使攻击者能够利用中间人（MiTM）攻击拦截来自其他集群中的流量，Kubernetes 产品安全委员会已提供有关暂时阻止攻击者利用漏洞的建议。 Kubernetes（又名 K8s）最初由 Google 开发，现在由 Cloud Native Computing Foundation 维护，是一个开源系统，旨在帮助主机集群上的自动化部署。 该漏洞编号为 CVE-2020-8554，漏洞等级为中危，由 Anevia 的 Etienne Champetier 报告。

详情

All Kubernetes versions affected by unpatched MiTM vulnerability

https://www.bleepingcomputer.com/news/security/all-kubernetes-versions-affected-by-unpatched-mitm-vulnerability/

OpenSSL 存在严重漏洞，请立即更新

日期: 2020-12-08

等级: 中

来源: Pierluigi Paganini

标签: ['OpenSSL', 'TLS', 'SSL', 'Dos', 'Null Pointer']

OpenSSL 项目警告称 TLS/SSL 工具包中存在严重的安全漏洞，该漏洞让用户容易受到拒绝服务（DoS）攻击，造成的原因是空指针取消引用。 该漏洞由 Google 研究人员 David Benjamin 报告。

详情

OpenSSL is affected by a 'High Severity' security flaw, update it now

https://securityaffairs.co/wordpress/112085/security/openssl-tls-ssl-toolkit-flaw.html

比特币交易所运营商被判 5 年监禁

日期: 2020-12-08

等级: 中

来源: Akshaya Asokan

标签: ['Russian', 'France', 'Bitcoin', 'Prison', 'BTC-e']

俄罗斯公民亚历山大·文尼克（Alexander Vinnik）创立了 BTC-e 加密货币交易所，目前已经倒闭。 2020 年 12 月 7 日他由于洗钱被判处五年监禁，并必须支付 10 万欧元（12 万美元）的罚款。 据美联社报道，尽管法国法院认定 Vinnik 犯有洗钱罪，但一名法官洗清了对这位 41 岁男子的勒索和与犯罪集团有关联的额外指控。

详情

Bitcoin Exchange Operator Sentenced to 5 Years in Prison

https://www.databreachtoday.com/bitcoin-exchange-operator-sentenced-to-5-years-in-prison-a-15546

Google 开源了 Atheris，一个在 Python 代码中查找安全漏洞的工具

日期: 2020-12-09

等级: 中

来源: Catalin Cimpanu

标签: ['Google', 'Fuzz', 'Atheris', 'Python', 'Vulnerabilities']

Google 的安全专家已经开源了另一个 Fuzz 测试工具，以希望开发人员可以在发现漏洞之前先使用它来发现安全漏洞并且修复漏洞。 fuzzer(或 fuzzing 工具)和 fuzzing 技术通过向软件应用程序提供大量随机数据并分析其输出的异常和崩溃，从而给开发人员提示应用程序代码中可能存在异常的位置。 自 2013 年以来，Google 安全研究人员创建并开源了多个 Fuzz 测试工具，包括 OSS-Fuzz，Syzkaller，ClusterFuzz，Fuzzilli 和 BrokenType 之类的工具。

详情

Google open-sources Atheris, a tool for finding security bugs in Python code

https://www.zdnet.com/article/google-open-sources-atheris-a-tool-for-finding-security-bugs-in-python-code/

黑客使用 WinZip 不安全的服务器连接恶意软件

日期: 2020-12-10

等级: 中

来源: Ionut Ilascu

标签: ['WinZip', 'Malware', 'macOS', 'Android', 'iOS']

某些版本的 WinZip 文件压缩工具中的服务器与客户端通信是不安全的，可能会被修改为向用户提供恶意软件或诈骗内容。 该工具最初发布于大约 30 年前，现在已经有 macOS、Android 和 iOS 版本，以及增加协作特性的企业版。 据其网站显示，该应用程序的下载量超过 10 亿次。 WinZip 当前的版本为 25，但是较早的版本存在漏洞，可能被恶意攻击者利用。

详情

Hackers can use WinZip insecure server connection to drop malware

https://www.bleepingcomputer.com/news/security/hackers-can-use-winzip-insecure-server-connection-to-drop-malware/

Sophos 修复了 Cyberoam OS 中的 SQL 注入漏洞

日期: 2020-12-10

等级: 中

来源: Lawrence Abrams

标签: ['Sophos', 'Cyberoam', 'SQL', 'Vulnerability', 'Fix']

Sophos 已为其 Cyberoam 防火墙和路由器部署了一个修补程序，以修复 SQL 注入漏洞。Sophos 于 2014 年收购了防火墙和路由器制造商 Cyberoam Technologies，自 2019 年以来一直免费提供其 XG Firewall OS 的升级。 2020 年 12 月 10 日，Sophos 透露，Cyberoam（CROS）操作系统中修复了一个 SQL 注入漏洞，该漏洞可以远程向 CROS 设备添加帐户。

详情

Sophos fixes SQL injection vulnerability in their Cyberoam OS

https://www.bleepingcomputer.com/news/security/sophos-fixes-sql-injection-vulnerability-in-their-cyberoam-os/

Glassdoor 公司审查平台发现严重 CSRF 漏洞

日期: 2020-12-11

等级: 中

来源: Charlie Osborne

标签: ['Glassdoor', 'CSRF', 'BugBounty']

Glassdoor 是一个求职和发布匿名公司评论的网站，被曝出了一个会被利用来接管账户的严重 CSRF 问题。这可能包括在雇主帐户上建立新的管理员，删除求职者和雇主的信息，添加虚假评论，删除简历，以及发布、申请和删除工作清单，严重性评分为 9-10。

详情

Critical CSRF vulnerability found on Glassdoor company review platform

https://www.zdnet.com/article/cross-site-request-forgery-vulnerability-found-on-glassdoor-job-hunter-review-platform/

NI CompactRIO 控制器漏洞可能导致生产中断

日期: 2020-12-12

等级: 中

来源: Pierluigi Paganini

标签: ['National Instruments', 'CompactRIO', 'IIoT', 'CVE-2020-25191']

National Instruments CompactRIO 控制器中存在一个严重漏洞，允许远程攻击者破坏组织中的生产过程。该漏洞被追踪为`CVE-2020-25191`，影响 20.5 之前的驱动程序版本。National Instruments CompactRIO 产品是一款坚固耐用的实时控制器，可提供高性能的处理能力、特定于传感器的条件输入/输出以及紧密集成的软件工具链，使其成为工业物联网（IIoT）、监控和控制应用的理想之选。

详情

NI CompactRIO controller flaw could allow disrupting production

https://securityaffairs.co/wordpress/112228/ics-scada/ni-compactrio-flaw.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
3. 受到网络攻击之后，积极进行攻击痕迹、遗留文件信息等证据收集

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