安全事件周报

安全事件周报 (12.21-12.27)

360CERT
北京奇虎科技有限公司 | 2020-12-28

报告信息

报告名称	安全事件周报（12.21-12.27）		
报告类型	安全事件周报	报告编号	B6-2020-122801
报告版本	1.0	报告日期	2020-12-28
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	2020-12-28	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 35 项

话题集中在`网络攻击`、`勒索软件`方面，涉及的组织有：`SolarWinds`、`Dell`、`Citrix`、`美国财政部`等。供应链攻击持续发酵，各大下游用户尽快进行补丁升级。

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**
FreePBX 开发商 Sangoma 遭遇 Conti 勒索软件攻击	★★★★★
货运公司 Forward Air 遭到 Hades 勒索软件攻击	★★★★
Emotet 卷土重来，每天攻击 10 万个邮箱	★★★★
攻击者使用假冒的亚马逊礼品卡发放 Dridex 木马	★★★★
佛蒙特医院证实勒索病毒攻击事件	★★★★
REvil 威胁要发布医院集团客户名人的照片	★★★
数据安全	**等级**
黑客论坛上泄露了 27 万个 Ledger 所有者的真实地址	★★★★
NetGalley 网站遭到数据泄露	★★★★
养老金供应商数据遭到泄漏	★★★
网络攻击	**等级**
美国财政部遭受严重的 SolarWinds 漏洞攻击	★★★★★
微软使用的 SolarWinds 遭到黑客入侵	★★★★
在 SolarWinds 网络攻击分析中发现了新的 SUPERNOVA 后门	★★★★
美国司法部查获了冒充制药公司的假域名	★★★★
黑客利用 0day 漏洞攻击半岛电视台员工的 iPhone	★★★★
EXMO 加密货币交易所遭黑客攻击，损失了 5%的总资产	★★★★
一个以出售宠物狗为幌子的诈骗活动	★★★★
网络钓鱼诈骗伪装成 Chase 的安全通知	★★★★
UltraRank 犯罪团伙针对更多的电子商务网站	★★★★
新的网络钓鱼电子邮件活动围绕 COVID-19 主题	★★★★
假冒美国邮政服务的网络钓鱼攻击以消费者为目标	★★★★

Citrix 证实 NetScaler 的 ADC 正在受到 DDoS 攻击	★★★★
俄罗斯加密货币交易所 Livecoin 在平安夜遭到黑客攻击	★★★★
VMware 确认在 SolarWinds 黑客攻击中遭到破坏	★★★
罗阿诺克学院在遭受网络攻击后推迟春季学期	★★★
朝鲜黑客试图窃取 COVID-19 疫苗研究成果	★★★
其他事件	**等级**
Treck TCP/IP 协议栈中严重漏洞影响了数百万的物联网设备	★★★★★
利用`FireEye`泄漏的工具可以攻击数百万台设备	★★★★★
Dell Wyse ThinOS 中的严重漏洞导致 thin 客户端被接管	★★★★
多家科技公司支持`Facebook`对`NSO Group`发起的诉讼	★★★★
网上公布了部分感染 Sunburst 恶意软件的组织名单	★★★
前"Silk Road"成员被判 8 个月监禁	★★★
VPN Bulletproof 服务在全球警察行动中被攻破	★★★
执法部门查获了泄漏信用卡的黑市	★★★
Windows 0day 漏洞的补丁被绕过	★★★
QNAP 修复了 QTS、QES 和 QTS hero 的严重漏洞	★★★

三、 事件详情

(一) 恶意程序

FreePBX 开发商 Sangoma 遭遇 Conti 勒索软件攻击

日期: 2020-12-24

等级: 高

来源: Lawrence Abrams

标签: ['Sangoma', 'Conti', 'Ransomware', 'FreePBX', 'Data Leak', 'Cyberattack']

Sangoma 透露，在遭受了`Conti`勒索软件攻击之后，该公司的文件被盗并被泄露。 Sangoma 是 IP 语音硬件和软件提供商，以流行的开源`FreePBX PBX`电话系统而闻名，该系统使组织可以在其网络上创建公司电话系统。 2020 年 12 月 24 日，`Conti`勒索软件团伙在他们的勒索软件数据泄漏站点上发布了超过 26GB 的数据，这些数据是在最近的网络攻击中从`Sangoma`窃取的。 泄漏的数据包括与公司会计，财务，收购，员工福利和薪资以及法律文件有关的文件。

详情

FreePBX developer Sangoma hit with Conti ransomware attack

https://www.bleepingcomputer.com/news/security/freepbx-developer-sangoma-hit-with-conti-ransomware-attack/

货运公司 Forward Air 遭到 Hades 勒索软件攻击

日期: 2020-12-21

等级: 高

来源: Lawrence Abrams

标签: ['Forward Air', 'Hades', 'Ransomware', 'Cyberattack']

货运物流公司`Forward Air`遭受了 Hades 勒索软件团伙的攻击，这对该公司的业务运营产生了影响。 `Forward Air`是一家位于美国田纳西州的领先货运和空运物流公司。该公司 2019 年的收入为 14 亿美元，拥有员工 4300 多人。 2020 年 12 月 19 日，FreightWaves 报告说，Forward Air 遭受了网络攻击，迫使他们关闭系统以防止攻击蔓延。 Forward Air 随后在向 BleepingComputer 的声明中确认了此攻击。

详情

Trucking giant Forward Air hit by new Hades ransomware gang

https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-hit-by-new-hades-ransomware-gang/

Emotet 卷土重来，每天攻击 10 万个邮箱

日期: 2020-12-23

等级: 高

来源: Tara Seals

标签: ['Emotet', 'Botnet', 'Ransomware', 'Banking Trojan']

经过将近两个月的休整之后，`Emotet`僵尸网络卷土重来，它更新了`payload`，并发起了一场每天攻击 10 万个邮箱的网络攻击活动。 Emotet 于 2014 年以银行木马的身份诞生，并不断发展成为提供全方位服务的威胁传递机制。 它可以在受害者机器上安装一系列恶意软件，包括信息窃取工具，电子邮件收集器，自动传播机制和勒索软件。

详情

Emotet Returns to Hit 100K Mailboxes Per Day

https://threatpost.com/emotet-returns-100k-mailboxes/162584/

攻击者使用假冒的亚马逊礼品卡发放 Dridex 木马

日期: 2020-12-24

等级: 高

来源: Akshaya Asokan

标签: ['Europe', 'Dridex', 'Evil Corp', 'Amazon Gift Cards', 'Phishing']

据网络安全公司`Cybereason`报道，网络犯罪份子正以美国和西欧的网上购物者为目标，使用假冒的亚马逊礼品卡，发放`Dridex`银行木马。 Cybereason 的研究人员表示，自 2020 年 12 月起，攻击者已经将美国和西欧国家的数千名受害者作为目标，亚马逊在这些国家很受欢迎。 攻击者通过发送钓鱼邮件，声称收件人得到了免费的亚马逊礼品卡。 礼品卡包含在一个恶意附件中，收件人一旦下载，即可触发`Dridex`木马。

详情

Fake Amazon Gift Cards Deliver Dridex Trojan

https://www.databreachtoday.com/fake-amazon-gift-cards-deliver-dridex-trojan-a-15663

佛蒙特医院证实勒索病毒攻击事件

日期: 2020-12-27

等级: 高

来源: Pierluigi Paganini

标签: ['Vermont Hospital', 'Ransomware']

总部位于伯灵顿的佛蒙特大学健康网络承认勒索软件是十月袭击的幕后黑手。2020 年 10 月，黑客袭击了布鲁克林的威科夫高地医疗中心和佛蒙特大学健康网络。这起网络攻击发生在 10 月 28 日，并中断了乌云医学中心和附属设施的服务。一个月后，佛蒙特大学医学中心瘫痪的系统慢慢恢复。12 月初，医院首席执行官斯蒂芬·莱夫勒博士宣布，10 月下旬发生在佛蒙特大学医疗中心计算机系统上的攻击事件每天给医院造成约 150 万美元的损失。

详情

Vermont Hospital confirmed the ransomware attack

https://securityaffairs.co/wordpress/112694/malware/vermont-hospital-ransomware-attack.html

REvil 威胁要发布医院集团客户名人的照片

日期: 2020-12-26

等级: 中

来源: Pierluigi Paganini

标签: ['Hospital Group', 'REvil', 'Sodinokibi']

`REvil`勒索软件团伙，又名`Sodinokibi`，入侵了英国整形外科中心，并威胁要发布名人客户前后的照片。这家医院集团有 11 家诊所，专门从事减肥手术、隆胸、乳头矫正和鼻子调整，其客户不乏名人。该医院集团已经确认了勒索软件攻击，并将安全漏洞告知了信息专员。

详情

REvil gang threatens to release intimate pictures of celebs who are customers of The Hospital Group

https://securityaffairs.co/wordpress/112637/cyber-crime/the-hospital-group-revil.html

相关安全建议

1. 软硬件提供商要提升自我防护能力，保障供应链的安全
2. 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
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. 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
6. 各主机安装 EDR 产品，及时检测威胁

(二) 数据安全

黑客论坛上泄露了 27 万个 Ledger 所有者的真实地址

日期: 2020-12-21

等级: 高

来源: Lawrence Abrams

标签: ['Ledger', 'Hacker Forum', 'Cryptocurrency', 'Leaked']

攻击者在黑客论坛上泄漏了`Ledger`加密货币钱包用户的失窃电子邮件和邮寄地址。Ledger 是用于存储，管理和出售加密货币的硬件加密货币钱包。 保存在这些钱包里的资金是通过一个 24 个单词的恢复短语和一个只有所有者知道的可选密钥来保护的。

详情

Physical addresses of 270K Ledger owners leaked on hacker forum

https://www.bleepingcomputer.com/news/security/physical-addresses-of-270k-ledger-owners-leaked-on-hacker-forum/

NetGalley 网站遭到数据泄露

日期: 2020-12-24

等级: 高

来源: Lawrence Abrams

标签: ['NetGalley', 'Data Breach', 'Personal information', 'Database']

12 月 21 日，NetGalley 图书推广网站遭遇数据泄露，攻击者能够访问包含会员个人信息的数据库。 该数据库包含`NetGalley`会员的个人信息，包括他们的账号，密码，用户名和电子邮件地址。 数据库中可能包含的其他可选信息包括用户的邮寄地址，生日，公司名称和`Kindle`电子邮件地址。 NetGalley 允许作者和出版商向有影响力的读者和行业专业人士宣传其书籍，希望他们能向他们的读者推荐这些书籍。

详情

NetGalley discloses data breach after website was hacked

https://www.bleepingcomputer.com/news/security/netgalley-discloses-data-breach-after-website-was-hacked/

养老金供应商数据遭到泄漏

日期: 2020-12-22

等级: 中

来源: Matthew Hughes

标签: ['UK', 'Pensions', 'NOW', 'Data Leakage']

目前，英国的养老金提供商`NOW`已经给一些英国的客户发了电子邮件，警告由于承包商错误而导致的数据泄漏问题。 该电子邮件声称服务提供商无意间将用户的数据发布到了一个未命名的公共软件论坛。 这些数据包括个人资料（姓名，电子邮件地址和出生日期）以及国民保险号码。

详情

UK firm NOW: Pensions tells some customers a 'service partner' leaked their data all over 'public software forum'

https://www.theregister.com/2020/12/22/now_pensions_data_breach/

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. 及时检查并删除外泄敏感数据
3. 合理设置服务器端各种文件的访问权限
4. 软硬件提供商要提升自我防护能力，保障供应链的安全

(三) 网络攻击

美国财政部遭受严重的 SolarWinds 漏洞攻击

日期: 2020-12-22

等级: 高

来源: Mathew J. Schwartz

标签: ['Democratic', 'SolarWinds', 'US Treasury', 'Supply Chain Attack']

一位资深民主党参议员说，美国财政部遭受了大规模的`SolarWinds`供应链攻击，数十个美国财政部电子邮件帐户被盗。 根据美国财政部工作人员的说法，美国财政部自 2020 年 7 月开始遭受严重破坏，其严重程度尚不清楚。

详情

US Treasury Suffers 'Significant' SolarWinds Breach

https://www.databreachtoday.com/us-treasury-suffers-significant-solarwinds-breach-a-15641

微软使用的 SolarWinds 遭到黑客入侵

日期: 2020-12-21

等级: 高

来源: GURUBARAN S

标签: ['SolarWinds', 'Microsoft', 'Orion', 'Cloud']

2020 年 12 月 21 日，gbhackers 报道了一个与此次 SolarWinds 黑客事件有关的受害者微软公司。 微软公司是 SolarWinds 产品 Orion（网络管理软件）的用户。 知情人士称，微软自己的产品也已遭到破坏，并被攻击者用来攻击受害者。 据报道，这些黑客利用了微软的云服务，但并没有影响微软公司的基础设施。截止 2020 年 12 月 21 日，微软尚未对此问题发表评论。

详情

Microsoft Breached in Suspected Russian Hack Using SolarWinds

https://gbhackers.com/microsoft-cyberattack-solarwinds/

在 SolarWinds 网络攻击分析中发现了新的 SUPERNOVA 后门

日期: 2020-12-21

等级: 高

来源: Ionut Ilascu

标签: ['Orion', 'SolarWinds', 'Backdoor', 'SUPERNOVA', 'Webshell', 'Trojan']

在分析来自 SolarWinds Orion 供应链攻击的工件时，安全研究人员发现了另一个后门，该后门很可能来自第二个攻击者。 该恶意软件名为`SUPERNOVA`，是植入 Orion 网络和应用程序监视平台代码中的`Webshell`，它使攻击者能够执行任意代码。 该 webshell 是 SolarWinds 的 Orion 软件中存在的合法.NET 库（`app_web_logoimagehandler.ashx.b6031896.dll`）的木马变体，攻击者对其进行了修改，使其可以逃避自动防御机制。

详情

New SUPERNOVA backdoor found in SolarWinds cyberattack analysis

https://www.bleepingcomputer.com/news/security/new-supernova-backdoor-found-in-solarwinds-cyberattack-analysis/

美国司法部查获了冒充制药公司的假域名

日期: 2020-12-21

等级: 高

来源: Prajeet Nair

标签: ['Moderna', 'Regeneron', 'Fake Domains', 'COVID-19', 'Phishing']

据美国司法部说，联邦调查人员已经查获了两个假冒制药公司`Moderna`和`Regeneron`的域名。 据美国检察官办公室称，2020 年 12 月初对这两个站点进行了调查，发现攻击者冒充了两家制药公司的域名并使用欺诈网站窃取可用于进行网络钓鱼活动和传播恶意软件的身份。

详情

DOJ Seizes Fake Domains Impersonating Moderna, Regeneron

https://www.databreachtoday.com/doj-seizes-fake-domains-impersonating-moderna-regeneron-a-15638

黑客利用 0day 漏洞攻击半岛电视台员工的 iPhone

日期: 2020-12-21

等级: 高

来源: Pierluigi Paganini

标签: ['Al Jazeera', 'iOS', 'Zero Day', 'Pegasus', 'Kismet', 'NSO Group']

2020 年 7 月和 2020 年 8 月，政府工作人员使用`Pegasus`间谍软件入侵了半岛电视台的 36 部属于记者，制片人，主持人和执行人员的个人电话。 位于伦敦的`Al Araby TV`的一名记者的个人电话也遭到了黑客攻击。攻击者利用了`iOS`的`0day`漏洞来入侵员工的`iPhone`。 攻击者使用了名为`Kismet`的漏洞利用链，该链是`Pegasus`武器库的一部分，该武器库由`NSO Group`公司出售。

详情

Zero-day exploit used to hack iPhones of Al Jazeera employees

https://securityaffairs.co/wordpress/112500/malware/al-jazeera-zeroday-hack.html

EXMO 加密货币交易所遭黑客攻击，损失了 5%的总资产

日期: 2020-12-21

等级: 高

来源: Sergiu Gatlan

标签: ['EXMO', 'Cryptocurrency', 'Hot Wallets']

英国加密货币交易所`EXMO`透露，匿名攻击者在对其热钱包进行攻击后，提取了近 5%的总资产。 热钱包是连接互联网的，与没有互联网连接的冷钱包(也称为离线钱包或硬件钱包)不同，热钱包被交易所用来临时存储正在进行的交易和转移的资产。 EXMO 表示，从 12 月 21 日世界标准时间 2:27:02 开始，在检测到可疑的大额提款后，该交易所已暂停所有提款。

详情

EXMO cryptocurrency exchange hacked, loses 5% of total assets

https://www.bleepingcomputer.com/news/security/exmo-cryptocurrency-exchange-hacked-loses-5-percent-of-total-assets/

一个以出售宠物狗为幌子的诈骗活动

日期: 2020-12-22

等级: 高

来源: Becky Bracken

标签: ['German', 'Bitcoin', 'Fake Puppy', 'Con', 'COVID-19']

研究人员发现了一种以比特币出售伪造的德国牧羊犬幼犬的活动，多数买家遭到欺诈。 该骗局是由`Anomali`的一位研究人员发现的。 据`Amomali`报告，这些骗子自 2018 年 11 月以来一直在运营诈骗网站，他们发现有 17 个与该组织相关的网站，该组织销售鸟类，猫和精油。 与其他骗局一样，`Fodjie Bobga`会出售狗和其他动物，收取定金并建立假的销售渠道。 假冒的运输公司会联系受害者并告诉他们，由于`COVID-19`，他们需要支付额外的钱才能交货，之后进一步敲诈更多的钱。

详情

Holiday Puppy Swindle Has Consumers Howling

https://threatpost.com/holiday-puppy-swindle-consumers-howling/162565/

网络钓鱼诈骗伪装成 Chase 的安全通知

日期: 2020-12-23

等级: 高

来源: Lawrence Abrams

标签: ['Chase', 'Phishing Emails', 'Account']

大规模的网络钓鱼诈骗伪装成`Chase`发出的安全通知，邮件中声称检测到了网络诈骗活动，并且告诉收件人的账户会因此被冻结。 要"解锁"帐户，收件人需要点击电子邮件中的"立即还原"按钮。当点击"立即恢复"按钮时，收件人将被重定向到一个页面，要求他们登录自己的`Chase`账户。 如果他们输入自己的登录信息，它将被发送给攻击者，然后攻击者将有权访问该帐户。

详情

PSA: Active Chase phishing scam pretends to be fraud alerts

https://www.bleepingcomputer.com/news/security/psa-active-chase-phishing-scam-pretends-to-be-fraud-alerts/

UltraRank 犯罪团伙针对更多的电子商务网站

日期: 2020-12-23

等级: 高

来源: Akshaya Asokan

标签: ['UltraRank', 'JavaScript', 'Group-IB', 'SnifLite', 'Sniffer', 'E-Commerce Sites']

安全公司`Group-IB`称，一个名为`UltraRank`的网络犯罪团伙发起了一项新的网络攻击活动，目标至少有十二个电子商务网站，它们使用`JavaScript`嗅探器（称为`SnifLite`）窃取支付卡的数据。 此次攻击始于 2020 年 11 月。`Group-IB`的研究人员联系了所有受影响的公司，但截至 2020 年 12 月 23 日，仍有八个目标站点感染了恶意的`JavaScript`代码。 研究人员说，在过去的五年中，`UltraRank`瞄准了北美，欧洲，亚洲和拉丁美洲的 700 多个电子商务站点以及 13 个第三方供应商。

详情

'UltraRank' Targets More E-Commerce Sites

https://www.databreachtoday.com/ultrarank-targets-more-e-commerce-sites-a-15657

新的网络钓鱼电子邮件活动围绕 COVID-19 主题

日期: 2020-12-23

等级: 高

来源: Prajeet Nair

标签: ['Abnormal Security', 'COVID-19', 'Microsoft Office 365', 'Phishing', 'New York', 'State Department of Labor']

据`Abnormal Security`的研究人员称，最近一次发现的网络钓鱼活动正在窃取纽约州劳工部的信息，钓鱼邮件中声称提供 600 美元作为 COVID-19 救援计划的一部分。 此次网络钓鱼活动似乎于 2020 年 12 月初开始，到目前为止，它已经瞄准了大约 10 万个`Microsoft Office 365`帐户。 研究人员指出，攻击者通过设计围绕`COVID-19`及其经济影响的骗局，随着疫情的持续，此钓鱼邮件的收件人可能更容易相信政府正在提供额外的救济。

详情

Phishing Email Campaign Uses Updated COVID-19 Theme

https://www.databreachtoday.com/phishing-email-campaign-uses-updated-covid-19-theme-a-15653

假冒美国邮政服务的网络钓鱼攻击以消费者为目标

日期: 2020-12-23

等级: 高

来源: Steve Zurier

标签: ['Abnormal Security', 'Phishing', 'Cyberattack', 'U.S. Postal Service', 'Delivery']

`Abnormal Security`2020 年 12 月 23 日报道称，其电子邮件安全平台拦截了网络钓鱼攻击，本次钓鱼攻击假冒了美国邮政服务。 据报道称，攻击者利用了消费者希望在假期快速的收到快递的心理进行诈骗。 `CheckPoint`最近的研究指出，这类诈骗非常普遍。研究发现，2020 年 11 月，与 2020 年 10 月相比，与航运相关的钓鱼邮件数量增加了 440%。 换句话说，网络钓鱼诈骗往往与当前热点事件有关。

详情

Credential phishing attack impersonating USPS targets consumers over the holidays

https://www.scmagazine.com/home/security-news/phishing/credential-phishing-attack-impersonating-usps-targets-consumers-over-the-holidays/

Citrix 证实 NetScaler 的 ADC 正在受到 DDoS 攻击

日期: 2020-12-24

等级: 高

来源: Sergiu Gatlan

标签: ['Citrix', 'DTLS', 'ADC', 'DDos', 'Botnets', 'NetScaler']

Citrix 于 2020 年 12 月 24 日证实，一种使用`DTLS`作为放大向量的持续`DDoS 攻击模式`正在影响启用了`EDT`的`Citrix Application Delivery Controller`（ADC）网络设备。 数据报传输层安全性（`DTLS`）是一种通信协议，基于传输层安全性（`TLS`）协议，用于保护使用数据报传输的时延敏感的应用程序和服务。 该次攻击中，攻击者或僵尸程序可能会使`Citrix ADC DTLS`网络吞吐量不堪重负，有可能导致出站带宽耗尽。

详情

Citrix confirms ongoing DDoS attack impacting NetScaler ADCs

https://www.bleepingcomputer.com/news/security/citrix-confirms-ongoing-ddos-attack-impacting-netscaler-adcs/

俄罗斯加密货币交易所 Livecoin 在平安夜遭到黑客攻击

日期: 2020-12-25

等级: 高

来源: Pierluigi Paganini

标签: ['Russian', 'Livecoin', 'CyberAttack']

俄罗斯加密货币交易所 Livecoin 在平安夜遭到破坏，黑客入侵了它的网络，并控制了它的一些服务器。该交易所在其网站上发布消息警告客户：“亲爱的客户，我们要求您停止使用我们的服务的所有功能：不要存款，不要交易，不要使用 API。我们正受到一次精心策划的网络袭击。我们失去了对所有服务器、后端和节点的控制。”

详情

The Russian cryptocurrency exchange Livecoin hacked on Christmas Eve

https://securityaffairs.co/wordpress/112608/hacking/cryptocurrency-exchange-livecoin-hacked.html

VMware 确认在 SolarWinds 黑客攻击中遭到破坏

日期: 2020-12-21

等级: 中

来源: Sergiu Gatlan

标签: ['VMware', 'SolarWinds', 'Sunburst', 'Solarigate']

VMware 是最新一家确认其系统在最近的 SolarWinds 攻击中遭到破坏的公司。 VMware 公司表示，黑客在部署了`Sunburst`或`Solarigate`后门之后，并没有进一步的操作来利用他们的访问权限。

详情

VMware latest to confirm breach in SolarWinds hacking campaign

https://www.bleepingcomputer.com/news/security/vmware-latest-to-confirm-breach-in-solarwinds-hacking-campaign/

罗阿诺克学院在遭受网络攻击后推迟春季学期

日期: 2020-12-22

等级: 中

来源: Lawrence Abrams

标签: ['Roanoke College', 'Cyberattack', 'Delays Spring Semester']

罗阿诺克学院在遭受网络攻击影响文件和数据访问后，将春季学期的时间推迟了近一个月。 罗阿诺克学院是一所私立文理学院，位于弗吉尼亚州的塞勒姆，大约有 2000 名学生。 12 月 12 日，罗阿诺克学院遭受了一次网络攻击，导致学院无法访问文件。 学院的 IT 人员切断了学院的网络，并开始对这一事件进行调查。学院的春季学期原本安排在 2021 年 1 月 19 日，但由于 12 月 12 日的网络攻击事件和冠状病毒的传播，学院被迫将春季学期推迟到 2021 年 2 月 8 日开学。

详情

Roanoke College delays spring semester after cyberattack

https://www.bleepingcomputer.com/news/security/roanoke-college-delays-spring-semester-after-cyberattack/

朝鲜黑客试图窃取 COVID-19 疫苗研究成果

日期: 2020-12-23

等级: 中

来源: The Hacker News

标签: ['Lazarus Group', 'Kaspersky', 'North Korean', 'BookCodes']

臭名昭著的`Lazarus`等勒索团伙试图窃取`COVID-19`疫苗研究的敏感信息，以加快本国疫苗开发工作。 在这起涉及`COVID-19`疫苗的制药公司事件中，`Lazarus`团伙部署了`BookCodes`恶意软件，而最近韩国软件公司`WIZVERA`在供应链攻击中也使用了这种恶意软件，用于在目标系统上安装远程管理工具。

详情

North Korean Hackers Trying to Steal COVID-19 Vaccine Research

https://thehackernews.com/2020/12/north-korean-hackers-trying-to-steal.html

相关安全建议

1. 软硬件提供商要提升自我防护能力，保障供应链的安全
2. 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
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. 减少外网资源和不相关的业务，降低被攻击的风险
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

(四) 其他事件

Treck TCP/IP 协议栈中严重漏洞影响了数百万的物联网设备

日期: 2020-12-22

等级: 高

来源: The Hacker News

标签: ['TCP/IP', 'Treck', 'DoS', 'HTTP', 'Vulnerability']

美国网络安全基础设施和安全局（`CISA`）称，`Treck`开发的`TCP/IP`协议栈中存在严重漏洞，该漏洞允许远程攻击者执行任意命令并实施拒绝服务（`DoS`）攻击。 这四个漏洞影响`Treck TCP/IP`协议栈的`6.0.1.67`以及更早的版本，并且已由英特尔报告给`Treck`公司。其中两个漏洞被评为严重。 `Treck`的嵌入式`TCP/IP`协议栈广泛应用于制造、信息技术、医疗保健和运输系统中。

详情

New Critical Flaws in Treck TCP/IP Stack Affect Millions of IoT Devices
https://thehackernews.com/2020/12/new-critical-flaws-in-treck-tcpip-stack.html

利用`FireEye`泄漏的工具可以攻击数百万台设备

日期: 2020-12-24

等级: 高

来源: Pierluigi Paganini

标签: ['Qualys', 'SolarWinds Orion', 'FireEye', 'Read Team Tool']

`Qualys`的安全专家警告说，有超过 750 万台设备可能遭受网络攻击，这些攻击利用的是`FireEye`工具中提供的漏洞。 通过分析已经确定了`FireEye Red Team`工具中存在 754 万易受攻击的实例，如果滥用这些漏洞，则会造成大范围的影响。 相关组织需要迅速采取行动，以确保自己免受这些漏洞的攻击。

详情

Millions of devices could be hacked exploiting flaws targeted by tools stolen from FireEye
https://securityaffairs.co/wordpress/112588/hacking/fireeye-tools-exploits.html

Dell Wyse ThinOS 中的严重漏洞导致 thin 客户端被接管

日期: 2020-12-21

等级: 高

来源: Ionut Ilascu

标签: ['Dell', 'Wyse', 'ThinOS', 'Thin Client']

几乎有十二种`Dell Wyse`的 thin 客户端模型易受严重漏洞攻击，远程攻击者可能会利用这些严重漏洞来运行恶意代码并获得对任意文件的访问权限。 thin 客户端是用于远程桌面连接到功能更强大的系统的小型计算机。估计有 6,000 多家组织（其中大多数来自医疗保健行业）已在其网络上部署了`Dell Wyse`thin 客户端。 该漏洞(编号为 CVE-2020-29492 和 CVE-2020-29491)存在于戴尔`Wyse`thin 客户端的操作系统`ThinOS`组件中。

详情

Critical bugs in Dell Wyse ThinOS allow thin client take over

https://www.bleepingcomputer.com/news/security/critical-bugs-in-dell-wyse-thinos-allow-thin-client-take-over/

多家科技公司支持`Facebook`对`NSO Group`发起的诉讼

日期: 2020-12-22

等级: 高

来源: Akshaya Asokan

标签: ['Microsoft', 'Google', 'Cisco', 'VMWare', 'NSO Group', 'Lawsuit', 'Pegasus']

包括微软，谷歌，思科和`VMWare`在内的几家科技公司都支持`Facebook`起诉以色列的间谍软件公司`NSO Group`。`NSO Group`被指控侵入`Facebook`拥有的`WhatsApp`即时通讯应用程序。 在 2019 年 10 月提起的联邦民事诉讼中，Facebook 指控`NSO Group`开发了一种漏洞利用程序，使政府能够监视外交官、记者和政治异见人士的`WhatsApp`消息。这起诉讼要求禁止`NSO Group`访问`WhatApp`的系统，其中赔偿的金额尚不明确。

详情

Other Tech Firms Back Facebook's Lawsuit Against NSO Group

https://www.databreachtoday.com/other-tech-firms-back-facebooks-lawsuit-against-nso-group-a-15645

网上公布了部分感染 Sunburst 恶意软件的组织名单

日期: 2020-12-21

等级: 中

来源: Catalin Cimpanu

标签: ['SolarWinds Orion', 'Sunburst', 'Organizations List', 'Malware']

2020 年 12 月 20 日，多个安全研究人员和研究团队发布了一份组织的名单，这些组织安装了`SolarWinds Orion`平台的木马版，其内部系统感染了`Sunburst`恶意软件。 该名单中含有科技公司，地方政府，大学，医院，银行和电信提供商。 安全研究人员是通过对`Sunburst`(又名`Solorigate`)恶意软件的逆向分析获取到这些列表的。

详情

Partial lists of organizations infected with Sunburst malware released online

https://www.zdnet.com/article/partial-lists-of-organizations-infected-with-sunburst-malware-released-online/

前“Silk Road”成员被判 8 个月监禁

日期: 2020-12-22

等级: 中

来源: Akshaya Asokan

标签: ['Michael Weigand', 'Silk Road', 'Shabang', 'Darknet Market', 'Prison']

根据美国司法部称，在现已关闭的`Silk Road`暗网市场中，一名主要的参与者隐瞒了网站的创建和运营，并因向联邦调查员做出虚假陈述而被判处八个月的监禁。 负责此案的纽约南区联邦检察官办公室(U.S. Attorney's Office for the Southern District of New York)报

道，网名为`Shabang`的`Michael R. Weigand`于 2020 年 12 月 18 日被判刑。 2019 年 9 月，他承认自己隐瞒了运营`Silk Road`网站。

详情

Former 'Silk Road' Associate Sentenced to 8 Months in Prison

https://www.databreachtoday.com/former-silk-road-associate-sentenced-to-8-months-in-prison-a-15643

VPN Bulletproof 服务在全球警察行动中被攻破

日期: 2020-12-22

等级: 中

来源: Pierluigi Paganini

标签: ['European', 'VPN Bulletproof Services', 'Cybercrime', 'Ransomware', 'Spear Phishing', 'E-Skimming Breaches', 'Police Operation']

美国、德国、法国、瑞士和荷兰的执法机构发起联合行动，查封了三个`VPN Bulletproof`服务使用的基础设施。 `VPN Bulletproof`服务被网络犯罪组织广泛采用，以进行恶意活动，包括勒索软件和恶意软件攻击、电子盗窃、鱼叉式网络钓鱼活动、接管账户攻击。 这三个`VPN Bulletproof`服务分别托管`insorg.org`，`safe-inet.com`和`safe-inet.net`。

详情

Bulletproof VPN services took down in a global police operation

https://securityaffairs.co/wordpress/112543/cyber-crime/bulletproof-vpn-services-takedown.html

执法部门查获了泄漏信用卡的黑市

日期: 2020-12-22

等级: 中

来源: The Hacker News

标签: ['Interpol', 'Blockchain', "Joker's Stash", 'Tor', 'Underground Forums']

美国联邦调查局（FBI）和国际刑警组织（Interpol）查获了与属于`Joker's Stash`的基于区块链的代理服务器，该服务器运行着一个臭名昭著的欺诈市场，主要在地下论坛中出售泄漏的支付卡数据。 Joker's Stash 的运营商运营着该平台的多个版本，包括区块链代理服务器域名（`.bazar`，`.lib`，`.emc`和`.coin`），这些域名负责将用户重定向到实际网站以及其他两个`Tor`（`.onion`）的变体。

详情

Law Enforcement Seizes Joker's Stash — Stolen Credit Card Marketplace

https://thehackernews.com/2020/12/law-enforcement-seizes-jokers-stash.html

Windows 0day 漏洞的补丁被绕过

日期: 2020-12-23

等级: 中

来源: Ionut Ilascu

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

早在 2020 年 6 月，`Microsoft`就针对`Windows`操作系统中的漏洞发布了修复程序，利用该漏洞攻击者能够将其权限增加到受感染计算机上的内核级别，但是补丁被绕过了。`Google Project Zero `的安全研究员`Maddie Stone`发现，微软 6 月份的补丁并没有完全修复漏洞（CVE-2020-0986），攻击者仍可以通过一些方法加以利用。 微软在 9 月 24 日收到了补丁绕过的报告，并在一天后确认了这个问题，并给它分配了编号`CVE-2020-17008`，微软告知`CVE-2020-17008`的补丁程序将在 1 月 6 日前发布。

详情

Windows zero-day with bad patch gets new public exploit code

https://www.bleepingcomputer.com/news/security/windows-zero-day-with-bad-patch-gets-new-public-exploit-code/

QNAP 修复了 QTS、QES 和 QTS hero 的严重漏洞

日期: 2020-12-23

等级: 中

来源: Sergiu Gatlan

标签: ['QNAP', 'Vulnerability', 'NAS', 'Security Updates']

QNAP 发布了安全更新，以修复多个严重的安全漏洞，这些漏洞会影响运行`QES`、`QTS`和`QuTS hero`操作系统的网络存储(NAS)设备。 QNAP 在安全更新中一共修复了六个漏洞，这些漏洞影响了其`FreeBSD`，`Linux`和基于 128 位`ZFS`的操作系统。

详情

QNAP fixes high severity QTS, QES, and QuTS hero vulnerabilities

https://www.bleepingcomputer.com/news/security/qnap-fixes-high-severity-qts-qes-and-quts-hero-vulnerabilities/

相关安全建议

1. 包括浏览器、邮件客户端、vpn、远程桌面等在内的个人应用程序，应及时更新到最新版本
2. 及时对系统及各个服务组件进行版本升级和补丁更新
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