安全事件周报

安全事件周报 (12.14-12.20)

360CERT
北京奇虎科技有限公司 | 2020-12-21

报告信息

报告名称	安全事件周报（12.14-12.20）		
报告类型	安全事件周报	报告编号	B6-2020-122101
报告版本	1.0	报告日期	2020-12-21
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	2020-12-21	360CERT	360CERT	撰写报告

目录

一、 事件概览 1
二、 事件档案 2
三、 事件详情 4
(一) 恶意程序 4
(二) 数据安全 9
(三) 网络攻击 11
(四) 其他事件 14
四、 产品侧解决方案 20
(一) 360 网络空间测绘系统 20
(二) 360 安全分析响应平台 20
(三) 360 安全卫士 21
附录 A 事件等级说明 22
附录 B 事件类型说明 24

一、 事件概览

本周收录安全事件 40 项

话题集中在`网络攻击`、`勒索软件`方面，涉及的组织有：`SolarWinds`、`美国能源部`、`Microsoft`、`美国核安全局`等。供应链攻击爆发，软件及设备提供商要大力提升自我的安全能力。

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**
Symrise 在 Clop 勒索软件攻击后停止了生产	★★★★★
黑客组织滥用 Google 和 Facebook 服务部署恶意软件	★★★★
勒索软件攻击导致密苏里市账单延迟	★★★★
挪威邮轮公司 Hurtigruten 遭到勒索软件袭击	★★★★
Gitpaste-12 蠕虫扩大了攻击范围	★★★★
Goontact：新的针对 Android 和 iOS 用户的恶意软件	★★★★
Ryuk，Egregor 勒索软件攻击利用 SystemBC 后门	★★★★
安装量超过三百万次的恶意扩展仍在应用商店中	★★★★
DoppelPaymer 勒索软件正骚扰拒绝付款的受害者	★★★★
Agenttela 恶意软件更新了数据收集功能	★★★★
伊朗国家黑客与 Pay2Key 勒索软件有关联	★★★★
勒索软件伪装成《赛博朋克 2077》手机版	★★★★
新的 Windows 木马程序窃取浏览器凭据、Outlook 文件	★★★
Credential Stealer 针对美国、加拿大银行客户	★★★
数据安全	**等级**
美国临时人力资源机构 440GB 的数据被泄露	★★★★★
世界各地医院的 4500 万次医疗扫描记录被泄漏	★★★★★
电力供应商 People's Energy 被黑，泄露 25 万客户信息	★★★★
Azure Blob 暴露 CRM50 万的客户机密文档	★★★★
网络攻击	**等级**
FireEye 确认 SolarWinds 供应链攻击	★★★★★
SignSight 行动：针对东南亚认证机构的供应链攻击	★★★★★

黑客使用移动模拟器窃取数百万美元	★★★★★
网络钓鱼活动使用 Outlook 迁移邮件	★★★★
Subway 三明治忠诚卡用户遭钓鱼诈骗	★★★★
用于加密货币供应链攻击的恶意 RubyGems 软件包	★★★★
美国核武器局在 SolarWinds 攻击中遭到黑客入侵	★★★★
诈骗利用移动设备模拟器从网上银行账户盗取数百万美元	★★★★
微软称其系统也遭到 SolarWinds 供应链攻击破坏	★★★
其他事件	**等级**
微软和科技公司合作攻击了 SolarWinds 黑客使用的关键域	★★★★★
Medtronic MyCareLink 的漏洞可让黑客接管植入心脏的设备	★★★★★
安装了 500 万次的 WordPress 插件存在严重漏洞	★★★★★
PoS 终端存在任意代码执行漏洞	★★★★
Firefox 修补了严重漏洞，该漏洞同样影响 Chrome	★★★★
惠普公司披露了服务器管理软件中的 0day 漏洞	★★★★
Bouncy Castle 修复了 API 身份验证绕过漏洞	★★★★
SoReL-20M:一个包含 2000 万个恶意软件样本的数据集	★★★
严重的 Golang XML 解析器漏洞可以绕过 SAML 身份验证	★★★
苹果修复了 iOS 和 iPadOS 中的多个代码执行漏洞	★★★
研究人员把 RAM 变成 WiFi 卡，从未联网的系统中窃取数据	★★★
Facebook 因欺诈性 VPN 行为被 ACCC 告上法庭	★★★
美国航空监管机构发布了安全更新	★★★

三、 事件详情

(一) 恶意程序

Symrise 在 Clop 勒索软件攻击后停止了生产

日期: 2020-12-20

等级: 高

来源: Lawrence Abrams

标签: ['Symrise', 'Clop', 'Ransomware']

2020 年 12 月，Symrise 遭受了一次 Clop 勒索软件攻击，据称攻击者窃取了 500GB 的未加密文件，并加密了近 1000 台设备。`Symrise`是全球 30000 多个产品中使用的香料和香料的主要开发商，包括雀巢、可口可乐和联合利华的产品。2019 年，Symrise 实现了 34 亿欧元的收入，员工超过 10000 人。

详情

Flavors designer Symrise halts production after Clop ransomware attack

https://www.bleepingcomputer.com/news/security/flavors-designer-symrise-halts-production-after-clop-ransomware-attack/

黑客组织滥用 Google 和 Facebook 服务部署恶意软件

日期: 2020-12-14

等级: 高

来源: Ionut Ilascu

标签: ['Molerats', 'Phishing', 'Gaza Cyber\u200b\u200bgang', 'SharpStage', 'DropBook']

`Molerats`网络黑客组织在最近的鱼叉式钓鱼活动中一直使用依赖`Dropbox`，`Google Drive`和`Facebook`的新的恶意软件，通过该恶意软件能执行命令、存储被盗的数据。 该黑客组织从 2012 年就开始活跃。 Molerats 在最近的钓鱼攻击中使用了两个新的后门，`SharpStage`和`DropBook`，以及`MoleNet`。

详情

Hacking group's new malware abuses Google and Facebook services

https://www.bleepingcomputer.com/news/security/hacking-group-s-new-malware-abuses-google-and-facebook-services/

勒索软件攻击导致密苏里市账单延迟

日期: 2020-12-15

等级: 高

来源: Lawrence Abrams

标签: ['The City of Independence', 'Ransomware', 'Attack']

密苏里州独立市 2020 年 12 月 7 日遭遇勒索软件攻击，迫使他们在攻击中关闭自己的 IT 系统。 研究人员表示，他们正在执行完整的系统扫描，并从可用备份中还原被加密的计算机。 还原的过程正在进一步恢复城市的服务，包括发送公用事业账单和在线支付等服务。

详情

Ransomware attack causing billing delays for Missouri city

https://www.bleepingcomputer.com/news/security/ransomware-attack-causing-billing-delays-for-missouri-city/

挪威邮轮公司 Hurtigruten 遭到勒索软件袭击

日期: 2020-12-15

等级: 高

来源: Pierluigi Paganini

标签: ['Hurtigruten', 'Norwegian', 'Cruise Company', 'Ransomware', 'Cyberattack']

挪威邮轮公司 Hurtigruten 的首席数字官在一份声明中说：“Hurtigruten 的整个全球数字基础设施都受到了勒索软件的攻击，这是一次严重的攻击。” 该公司在 2020 年 12 月 12 日晚发现了这次攻击，该公司的系统被一个勒索软件感染。 该公司的网站被攻击后显示一条消息，“抱歉，该网站目前无法正常工作”。

详情

Norwegian cruise company Hurtigruten was hit by a ransomware

https://securityaffairs.co/wordpress/112320/malware/cruise-company-hurtigruten-ransomware.html

Gitpaste-12 蠕虫扩大了攻击范围

日期: 2020-12-15

等级: 高

来源: Lindsey O'Donnell

标签: ['GitHub', 'Monero', 'Gitpaste-12', 'Worm', 'Pastebin']

`Gitpaste-12`僵尸网络蠕虫主要针对 Web 应用程序，IP 摄像机和路由器。 `Gitpaste-12`是在 2020 年 10 月下旬针对基于`Linux`的服务器和物联网（`IoT`）设备的攻击中首次发现的，该僵尸网络利用`GitHub`和`Pastebin`存储恶意组件代码，拥有至少 12 个不同的攻击模块，并包括一个针对`Monero`加密货币的模块。

详情

Gitpaste-12 Worm Widens Set of Exploits in New Attacks

https://threatpost.com/gitpaste-12-worm-widens-exploits/162290/

Goontact：新的针对 Android 和 iOS 用户的恶意软件

日期: 2020-12-16

等级: 高

来源: Catalin Cimpanu

标签: ['Android', 'iOS', 'Lookout', 'Goontact', 'Malware']

安全研究人员发现了一种新的具有间谍和监视功能的恶意软件，目前存在于`Android`和`iOS`系统中。 这个名为`Goontact`的恶意软件能够从受害者那里收集数据，例如电话联系人、短信、照片和位置信息等。 移动安全公司`Lookout`检测到`Goontact`恶意软件目前通过第三方站点进行分发，这些第三方站点推广免费即时消息传递应用程序。

详情

New Goontact spyware discovered targeting Android and iOS users

https://www.zdnet.com/article/new-goontact-spyware-discovered-targeting-android-and-ios-users/

Ryuk，Egregor 勒索软件攻击利用 SystemBC 后门

日期: 2020-12-16

等级: 高

来源: Lindsey O'Donnell

标签: ['SystemBC', 'Tor', 'Ransomware', 'C2']

商品恶意软件后门`SystemBC`现已发展到可以自动化利用，并使用匿名化的 Tor 平台，一旦勒索软件被执行，勒索软件参与者就会使用后门在受害者系统上建立一个持久的连接。这使得网络犯罪攻击者更容易部署后门，并且能够隐藏命令和控制（C2）服务器通信的地址。 SystemBC 是一种代理和远程管理工具，于 2019 年首次被发现。

详情

Ryuk, Egregor Ransomware Attacks Leverage SystemBC Backdoor

https://threatpost.com/ryuk-egregor-ransomware-systembc-backdoor/162333/

安装量超过三百万次的恶意扩展仍在应用商店中

日期: 2020-12-16

等级: 高

来源: Sergiu Gatlan

标签: ['Edge', 'Microsoft', 'Malicious Extensions', 'Phishing Sites', 'Redirect']

Chrome 和 Edge 浏览器的恶意扩展程序安装量超过 300 万，其中大多数仍可在`Chrome Web Store`和`Microsoft Edge`附加组件门户上安装，它们能够窃取用户的信息并将其重定向到钓鱼网站。 Avast 威胁情报研究人员发现恶意软件扩展被设计成看起来像`Instagram`、`Facebook`、`Vimeo`和其他知名在线平台的附加组件。 虽然`Avast`在 2020 年 11 月就发现了这些扩展，但他们估计这些扩展可能已经存在多年，因为一些`Chrome`应用商店的评论者称，从 2018 年 12 月开始，链接就被劫持。

详情

Malicious Chrome, Edge extensions with 3M installs still in stores

https://www.bleepingcomputer.com/news/security/malicious-chrome-edge-extensions-with-3m-installs-still-in-stores/

DoppelPaymer 勒索软件正骚扰拒绝付款的受害者

日期: 2020-12-16

等级: 高

来源: Catalin Cimpanu

标签: ['DoppelPaymer', 'FBI', 'Ransomware', 'Ransom']

美国联邦调查局说，它们已经监测到`DoppelPaymer`勒索软件团伙采取了匿名电话的方式，通过恐吓强迫受害者支付赎金，勒索团伙对受害者公司的其员工甚至亲属的威胁不断

升级。 美国联邦调查局称，`Doppelpaymer`是最早的勒索软件变体之一。 美国联邦调查局建议受害者保护他们的网络，以防止被入侵，在被攻击后，建议受害者通知当局，并尽量避免支付赎金，因为这会激励攻击者进行新的入侵，使他们轻松获利。

详情

FBI says DoppelPaymer ransomware gang is harassing victims who refuse to pay

https://www.zdnet.com/article/fbi-says-doppelpaymer-ransomware-gang-is-harassing-victims-who-refuse-to-pay/

Agenttela 恶意软件更新了数据收集功能

日期: 2020-12-16

等级: 高

来源: Prajeet Nair

标签: ['AgentTesla', 'Cofense', 'Information Stealing', 'Credentials']

据安全公司`Cofense`发布的一份报告称，`AgentTesla`信息窃取软件的升级版本拥有额外的数据收集功能，包括锁定更多浏览器和电子邮件客户端的能力。 `AgentTesla`最初是在 2014 年被安全研究人员发现的。研究人员在 8 月份发现，该恶意软件现在可以从 vpn、网络浏览器、FTP 文件和电子邮件客户端窃取凭证。

详情

AgentTesla Malware Has Updated Data Harvesting Capabilities

https://www.databreachtoday.com/agenttesla-malware-has-updated-data-harvesting-capabilities-a-15617

伊朗国家黑客与 Pay2Key 勒索软件有关联

日期: 2020-12-17

等级: 高

来源: Sergiu Gatlan

标签: ['Fox Kitten', 'Pay2Key', 'Israel', 'Ransomware']

伊朗国家黑客`Fox Kitten`与`Pay2Key`勒索软件联系在一起，该组织最近开始针对以色列和巴西的组织。 威胁情报公司`ClearSky`表示，他们表示大概率的情况下，`Pay2Key`是由伊朗`APT`团体`Fox Kitten`运营的，该组织于 2020 年 11 月至 12 月开始了新一波的攻击，涉及数十家以色列公司。

详情

Iranian nation-state hackers linked to Pay2Key ransomware

https://www.bleepingcomputer.com/news/security/iranian-nation-state-hackers-linked-to-pay2key-ransomware/

勒索软件伪装成《赛博朋克 2077》手机版

日期: 2020-12-17

等级: 高

来源: Lawrence Abrams

标签: ['Windows', 'Android', 'Cyberpunk 2077', 'CoderWare', 'Ransomware']

攻击者正在为《赛博朋克 2077》游戏分发伪造的`Windows`和`Android`安装程序，该《赛博朋克 2077》会安装一个自称为`CoderWare`的勒索软件。 为了诱骗用户安装恶意软件，攻击者通常将恶意软件作为游戏安装程序、作弊工具和版权软件的破解程序进行分发。

详情

Ransomware masquerades as mobile version of Cyberpunk 2077

https://www.bleepingcomputer.com/news/security/ransomware-masquerades-as-mobile-version-of-cyberpunk-2077/

新的 Windows 木马程序窃取浏览器凭据、Outlook 文件

日期: 2020-12-14

等级: 中

来源: Lindsey O'Donnell

标签: ['Microsoft', 'Windows', 'PyMicropsia', 'Trojan', 'Information Stealing']

研究人员发现了一种新的名为`PyMicropsia`的信息窃取木马，该木马是由威胁组织`AridViper`开发的，`AridViper`以针对中东的组织为目标而闻名，它的目标是`Microsoft Windows`系统，该木马具有大量的数据过滤功能，能够收集浏览器的凭据，窃取 Outlook 文件。

详情

New Windows Trojan Steals Browser Credentials, Outlook Files

https://threatpost.com/windows-trojan-steals-browser-credentials-outlook-files/162223/

Credential Stealer 针对美国、加拿大银行客户

日期: 2020-12-17

等级: 中

来源: TRENDMICRO

标签: ['AHK', 'VBA', 'Credential Stealer', 'Excel']

2020 年 12 月中旬，研究人员发现了一个散布证书窃取程序的活动，这从 2020 年初就开始了。恶意软件感染以恶意 Excel 文件开始，此文件包含 AHK 脚本编译器可执行文件、恶意 AHK 脚本文件和 Visual Basic for Applications（VBA）宏。研究人员跟踪了恶意软件的命令和控制（C&C）服务器，并确定这些服务器来自美国、荷兰和瑞典。同时，恶意软件一直针对美国和加拿大的金融机构进行攻击。

详情

Credential Stealer Targets US, Canadian Bank Customers

https://www.trendmicro.com/en_us/research/20/l/stealth-credential-stealer-targets-us-canadian-bank-customers.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. 主机集成化管理，出现威胁及时断网
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. 各主机安装 EDR 产品，及时检测威胁
9. 移动端不安装未知应用程序、不下载未知文件

(二) 数据安全

美国临时人力资源机构 440GB 的数据被泄露

日期: 2020-12-14

等级: 高

来源: Edvardas Mikalauskas

标签: ['Automation Personnel Services', 'Data Leaked', 'Ransom', 'Hacker Forum']

美国人力资源机构(Automation Personnel Services)的 440GB 档案在一个黑客论坛上被泄露。 Automation Personnel Services 公司表示，目前正在进行调查，受影响数据的范围和性质尚未得到确认。 被泄漏的文件包含公司的机密数据、用户信息、合作伙伴和员工有关的敏感文件，例如薪资数据以及各种法律文件。 该归档文件于 11 月 24 日被泄露，被泄漏的原因是 Automation Personnel Services 拒绝支付赎金。

详情

440GB of data from US-based temporary staffing agency leaked on hacker forum
https://cybernews.com/security/440gb-of-data-from-us-based-temporary-staffing-agency-leaked-on-hacker-forum/

世界各地医院的 4500 万次医疗扫描记录被泄漏

日期: 2020-12-15

等级: 高

来源: Gareth Corfield

标签: ['CybelAngel', 'Data Leaked', 'Medical Scans', 'X-rays']

整个 2020 年，有 2000 台医疗服务器处于未授权的状态，服务器包含 4500 万张 X 射线图像和其他医学扫描图像，没有任何安全保护措施，可以被任意访问。 其中，泄漏的数据包括患者的姓名，出生日期，地址，身高，体重，诊断的个人健康信息等。 研究人员称，不仅敏感的个人信息被泄漏，而且恶意攻击者还访问了这些服务器并且在服务器上安装了恶意软件。

详情

45 million medical scans from hospitals all over the world left exposed online for anyone to view – some servers were laced with malware • The Register

https://www.theregister.com/2020/12/15/dicom_45_million_medical_scans_unsecured/

电力供应商 People's Energy 被黑，泄露 25 万客户信息

日期: 2020-12-17

等级: 高

来源: Paul Kunert

标签: ['People's Energy', 'Steal Data']

可再生电力和天然气供应商人民能源公司（People's Energy）告诉其 25 万多名客户，其 IT 系统漏洞被攻击者利用，客户信息已被泄漏。这些数据包括会员姓名、家庭住址、电子邮件地址、电话号码、出生日期、人们的能源账户号码、电价详情和电表识别号。

详情

Ethical power supplier People's Energy hacked, 250,000 customers' personal info accessed

https://www.theregister.com/2020/12/17/peoples_energy_hacked/

Azure Blob 暴露 CRM50 万的客户机密文档

日期: 2020-12-18

等级: 高

来源: Gareth Corfield

标签: ['Azure Blob', 'Unsecured Database']

一家商业应用开发商的`Microsoft Azure Blob`未做安全认证，导致超过 50 万的客户机密和敏感文件暴露于公共互联网中。泄漏的信息包括职业健康评估，伦敦劳埃德（Lloyds of London）承保的美国公司的保险索赔文件，以及大律师对申请晋升的初级同事的私人意见，以及联邦快递的运输安全文件，食品公司 Huel，投资管理公司的内部投诉以及无数其他文件。

详情

Unsecured Azure blob exposed 500,000+ highly confidential docs from UK firm's CRM customers

https://www.theregister.com/2020/12/18/probase_unsecured_azure_blob/

相关安全建议

1. 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
2. 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
3. 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
4. 及时备份数据并确保数据安全

5. 发生数据泄漏事件后，及时进行密码更改等相关安全措施

(三) 网络攻击

FireEye 确认 SolarWinds 供应链攻击

日期: 2020-12-14

等级: 高

来源: Catalin Cimpanu

标签: ['SolarWinds', 'Orion', 'US', 'FireEye', 'Malware']

美国安全公司 FireEye 2020 年 12 月 14 日表示，黑客已经破坏了软件提供商 SolarWinds`，然后在其`Orion`软件部署了带有恶意软件的更新程序，以感染多家美国公司和政府网络。`FireEye` 的报告是在`美国财政部`和`美国商务部国家电信与信息管理局`（NTIA）遭到入侵之后发布的。此次`SolarWindows`供应链攻击也是黑客入侵`FireEye`网络的手段。

详情

FireEye confirms SolarWinds supply chain attack

https://www.zdnet.com/article/fireeye-confirms-solarwinds-supply-chain-attack/

SignSight 行动：针对东南亚认证机构的供应链攻击

日期: 2020-12-17

等级: 高

来源: IgnacioSanmillan

标签: ['SignSight', 'Southeast Asia', 'Supply- chain Attack', 'Backdoor']

在`Able Desktop`软件的供应链攻击发生几周之后，越南政府认证局（VGCA）的网站上就发生了另一起类似的攻击，攻击者修改了两个可以从该网站下载的软件安装程序，并添加了后门程序。 `ESET`的研究人员于 2020 年 12 月上旬发现了这种新的供应链攻击，并通知了受感染的组织和`VNCERT`。 VGCA 表示，他们已经意识到了这次攻击，并通知了下载该木马软件的用户。

详情

Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia

https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/

黑客使用移动模拟器窃取数百万美元

日期: 2020-12-17

等级: 高

来源: Akshaya Asokan

标签: ['IBM', 'Mobile Emulators', 'Spoof Banking', ' Hacking Group']

`IBM Trusteer`报告说，一个黑客组织正在使用移动模拟器来欺骗银行客户的移动设备，并从美国和欧洲的银行中窃取了数百万美元。 `IBM Security`的执行安全顾问`Limor Kessem`说，尽管已经通知了受到黑客攻击的银行，但第二波攻击可能已经开始。 开发人员通常使

用移动模拟器来测试各种设备类型上的应用程序和功能。 在 IBM 调查的案例中，攻击者使用了 20 个移动模拟器，欺骗了超过 1.6 万部设备。

详情

Hackers Use Mobile Emulators to Steal Millions

https://www.databreachtoday.com/hackers-use-mobile-emulators-to-steal-millions-a-15623

网络钓鱼活动使用 Outlook 迁移邮件

日期: 2020-12-14

等级: 高

来源: Akshaya Asokan

标签: ['Microsoft', 'Outlook', 'Abnormal Security', 'Phishing']

`Abnormal Security`的研究人员表示，一场旨在获取`Office 365`证书的钓鱼活动使用微软`Outlook`迁移信息。 报告称，这些被设计成看起来像是来自受害者组织 IT 部门的钓鱼邮件称，收件人必须更新到最新版本的`Microsoft Outlook`。 当受害者点击网络钓鱼邮件中的链接时，他们将被重定向到一个恶意域，该域显示一个旧版本的`Outlook`登录页面，该页面能窃取用户名和密码等凭据。

详情

Phishing Campaign Uses Outlook Migration Message

https://www.databreachtoday.com/phishing-campaign-uses-outlook-migration-message-a-15587

Subway 三明治忠诚卡用户遭钓鱼诈骗

日期: 2020-12-15

等级: 高

来源: Becky Bracken

标签: ['Subway', 'Sophos', 'Loyalty Card', 'Phishing', ' U.K.', 'Ireland']

Subway 三明治的忠诚卡会员是最近网络犯罪的受害者之一。 `Sophos`的研究人员发现，网络钓鱼攻击的目标是英国和爱尔兰的`Subway`忠诚卡会员，目的是诱骗他们下载恶意软件。 此次钓鱼攻击的手段是让受害者改变他们`Excel`安全设置，允许恶意行为者运行宏并向受害者的设备发送恶意软件。 该代码从隐藏的文件表创建`URL`，然后`URL`抓取恶意软件。

详情

Subway Sandwich Loyalty-Card Users Suffer Ham-Handed Phishing Scam

https://threatpost.com/subway-loyalty-card-phishing-scam/162308/

用于加密货币供应链攻击的恶意 RubyGems 软件包

日期: 2020-12-16

等级: 高

来源: Lawrence Abrams

标签: ['RubyGems', 'Supply Chain Attack', 'Packages', 'Ruby', 'GEM']

新的恶意软件包 RubyGems 正在利用供应链攻击，并从毫无防备的用户那里窃取加密货币。 RubyGems 是 Ruby 编程语言的软件包管理器，允许开发人员下载其他人开发的代码并将其集成到他们的程序中。 由于任何人都可以将`Gem`上传到`RubyGems`存储库，因此攻击者可以将恶意软件包上传到存储库。

详情

Malicious RubyGems packages used in cryptocurrency supply chain attack

https://www.bleepingcomputer.com/news/security/malicious-rubygems-packages-used-in-cryptocurrency-supply-chain-attack/

美国核武器局在 SolarWinds 攻击中遭到黑客入侵

日期: 2020-12-17

等级: 高

来源: Tara Seals

标签: ['NNSA', 'FERC', 'SolarWinds']

美国能源部及其负责维持美国核储备的国家核安全局（NNSA）遭受到 SolarWinds 供应链攻击。美国能源部官方消息人士称，他们的部门受到了攻击者的渗透，包括对国家核安全局（NNSA）、联邦能源管理委员会（FERC）、华盛顿和新墨西哥州的桑迪亚和洛斯阿拉莫斯国家实验室，以及能源部里士兰办事处。

详情

Nuclear Weapons Agency Hacked in Widening Cyberattack – Report

https://threatpost.com/nuclear-weapons-agency-hacked-cyberattack/162387/

诈骗利用移动设备模拟器从网上银行账户盗取数百万美元

日期: 2020-12-20

等级: 高

来源: Pierluigi Paganini

标签: ['Fraud Operation', 'Online Bank', 'Mobile Device Emulators']

IBM Trusteer 的研究人员发现了一个大规模的欺诈行为，罪犯利用移动设备仿真器网络，在几天内从网上银行账户盗取数百万美元。这些网络犯罪分子使用了大约 20 个移动设备模拟器来模拟 16000 多个客户的手机，这些客户的移动银行账户已经被泄露。据专家称，这是有史以来规模最大的银行欺诈行动之一。

详情

A massive fraud operation used mobile device emulators to steal millions from online bank accounts

https://securityaffairs.co/wordpress/112487/cyber-crime/massive-fraud-operation.html

微软称其系统也遭到 SolarWinds 供应链攻击破坏

日期: 2020-12-17

等级: 中

来源: The Hacker News

标签: ['SolarWinds', 'Microsoft', 'Supply Chain']

微软证实其受到了 SolarWinds 供应链攻击的影响，目前来看，此事件的范围，复杂程度和影响可能比以前想象的要广泛得多。路透社还援引知情人士的话称，微软沦陷的产品随后被利用来打击其他受害者。不过，微软否认了该攻击已渗透到其生产系统中，其客户不会受到影响

详情

Microsoft Says Its Systems Were Also Breached in Massive SolarWinds Hack
https://thehackernews.com/2020/12/microsoft-says-its-systems-were-also.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. 主机集成化管理，出现威胁及时断网
4. 如果允许，暂时关闭攻击影响的相关业务，积极对相关系统进行安全维护和更新，将损失降到最小
5. 移动端不安装未知应用程序、不下载未知文件

(四) 其他事件

微软和科技公司合作攻击了 SolarWinds 黑客使用的关键域

日期: 2020-12-15

等级: 高

来源: Catalin Cimpanu

标签: ['Microsoft', 'SolarWinds', 'ZDNet']

2020 年 12 月 15 日，微软和科技公司联盟，攻破了 SolarWinds 黑客事件中起着核心作用的域。 该域名是`avsvmcloud.com`。它作为命令和控制（C&C）服务器，通过公司`Orion`应用程序的木马更新向大约 18,000 个`SolarWinds`客户发送了恶意软件。`SolarWinds Orion`在 2020 年 3 月至 2020 年 6 月之间发布了从 2019.4 到 2020.2.1 的更新版本，其中包含一种名为`SUNBURST`（也称为`Solorigate`）的恶意软件。

详情

Microsoft and industry partners seize key domain used in SolarWinds hack
https://www.zdnet.com/article/microsoft-and-industry-partners-seize-key-domain-used-in-solarwinds-hack/

Medtronic MyCareLink 的漏洞可让黑客接管植入心脏的设备

日期: 2020-12-15

等级: 高

来源: Pierluigi Paganini

标签: ['Medtronic', 'Cardiac Devices', 'Vulnerability']

美敦力公司（Medtronic）的`MyCareLink Smart 25000 Patient Reader Reader`产品存在漏洞，攻击者可以利用该漏洞控制配对心脏的设备。 MyCareLink Smart 25000 Patient Reader 是 Medtronic 设计的平台，可从患者植入的心脏设备中收集数据并将其传输到 Medtronic CareLink 网络。 研究人员发现了三个漏洞，可以利用这些漏洞来修改或伪造从植入的心脏设备接收到的数据。 这些漏洞还可能使远程攻击者能够控制配对的心脏设备，并在 MCL 智能患者读取器上执行任意代码。

详情

Flaws in Medtronic MyCareLink can allow attackers to take over implanted cardiac devices
https://securityaffairs.co/wordpress/112328/hacking/medtronic-mycarelink-flaws.html

安装了 500 万次的 WordPress 插件存在严重漏洞

日期: 2020-12-17

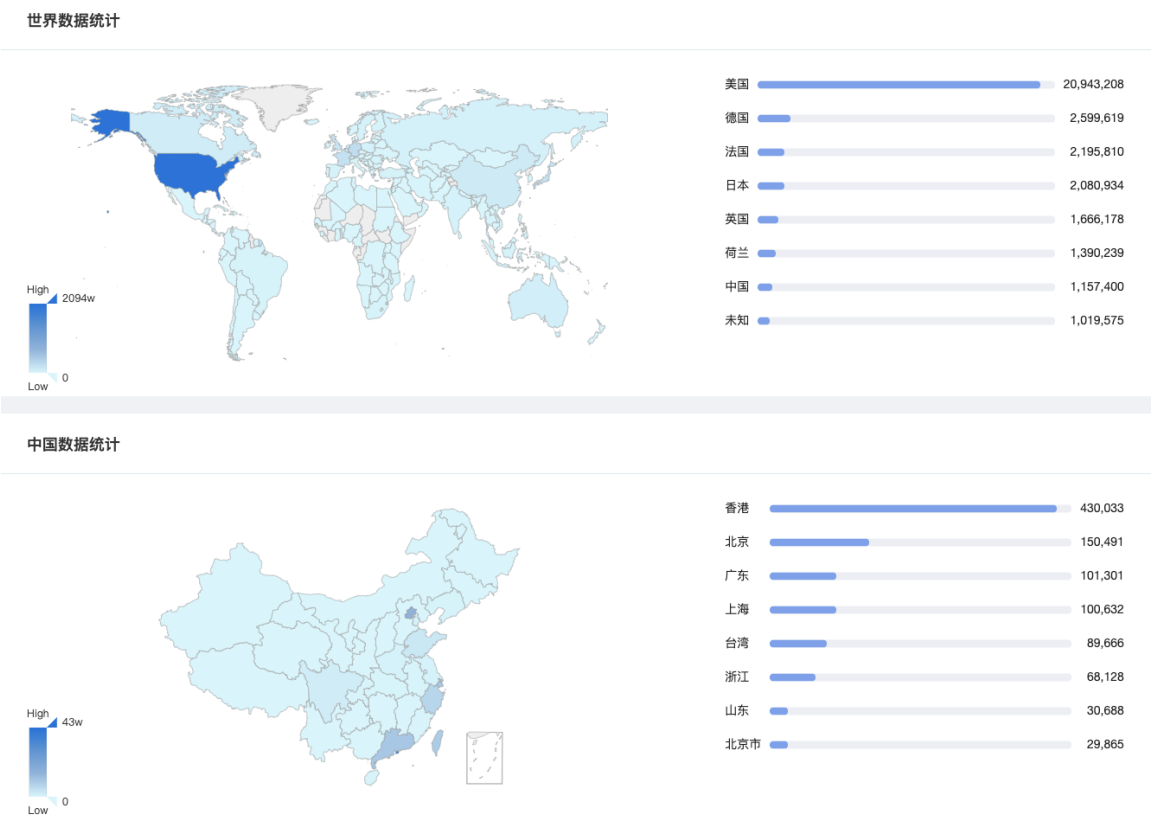
等级: 高

来源: Ax Sharma

标签: ['WordPress', 'Plugin', 'Contact Form 7', 'Patch', 'File Upload Vulnerability']

`WordPress`插件背后的团队披露了一个严重的文件上传漏洞，并发布了一个补丁。 易受攻击的插件`Contact Form 7`被安装了超过 500 万次，因此对于`WordPress`网站所有者来说，此次紧急更新是必要的。 `Contact Form 7`插件披露了一个不受限制的文件上传漏洞，攻击者可以利用该漏洞在上传文件时绕过`Contact Form 7`的文件名保护措施。

目前 Wordpress 的具体分布如下图，数据来自于 360 QUAKE



详情

WordPress plugin with 5 million installs has a critical vulnerability
https://www.bleepingcomputer.com/news/security/wordpress-plugin-with-5-million-installs-has-a-critical-vulnerability/

PoS 终端存在任意代码执行漏洞

日期: 2020-12-15

等级: 高

来源: GURUBARAN S

标签: ['PoS', 'Verifone', 'Ingenico', 'Vulnerability', 'Code Execute']

研究人员发现了两个最大的销售点（PoS）供应商`Verifone`和`Ingenico`的严重漏洞。 受影响的设备是`Verifone VX520`，`Verifone MX`系列和`Ingenico Telium 2`系列。 在使用默认密码的设备上，攻击者能够通过二进制漏洞（例如，堆栈溢出和缓冲区溢出）执行任意代码。攻击者能够利用 PoS 终端漏洞发送任意数据包、克隆卡、克隆终端并安装持久性的恶意软件。

详情

Flaws with PoS Terminals Let Attackers Execute Arbitrary Code
https://gbhackers.com/flaws-with-pos-terminals/

Firefox 修补了严重漏洞，该漏洞同样影响 Chrome

日期: 2020-12-15

等级: 高

来源: Tom Spring

标签: ['Firefox', 'Mozilla', 'Patches', 'Vulnerability']

Mozilla 基金会(Mozilla Foundation)2020 年 12 月 15 日发布的`Firefox`网络浏览器更新修复了一个严重漏洞和几个高危漏洞。 除了 CVE-2020-16042 漏洞，其余 6 个高危漏洞被修复。 Firefox 中的严重漏洞在 Chrome 浏览器安全更新中也得到了强调，该漏洞被评为严重漏洞。 Firefox 和 Chrome 仍未完全公布 CVE-2020-16042 的细节，仅将其列为内存漏洞。

详情

Firefox Patches Critical Mystery Bug, Also Impacting Google Chrome
https://threatpost.com/firefox-patches-critical-mystery-bug-also-impacting-google-chrome/162294/

惠普公司披露了服务器管理软件中的 0day 漏洞

日期: 2020-12-16

等级: 高

来源: Sergiu Gatlan

标签: ['Hewlett Packard Enterprise', 'Windows', 'Linux', 'Vulnerability', 'RCE']

惠普公司(Hewlett Packard Enterprise, HPE)披露了其 Windows 和 Linux 的专有 HPE Systems Insight Manager (SIM)软件最新版本中的 0day 漏洞。 尽管此远程代码执行

（RCE）漏洞尚未提供安全更新，但 HPE 已提供 Windows 的缓解方案，并正在努力修复该漏洞。

详情

HPE discloses critical zero-day in server management software

https://www.bleepingcomputer.com/news/security/hpe-discloses-critical-zero-day-in-server-management-software/

Bouncy Castle 修复了 API 身份验证绕过漏洞

日期: 2020-12-17

等级: 高

来源: Ax Sharma

标签: ['Bouncy Castle', 'Authentication Bypass', 'Vulnerability', 'Cryptography API']

`Bouncy Castle`是一个流行的开源密码库，该密码库中存在严重的认证绕过漏洞。 CVE-2020-28052 漏洞被成功利用后，攻击者可获得对用户帐户或管理员帐户的访问权限。`Bouncy Castle`是`Java`和`C#`/`.Net`使用的一组加密`Api`。仅`Bouncy Castle`的`.NET`版本就被下载了`1600 万`次，这说明了`Bouncy Castle`的漏洞严重性。

详情

Bouncy Castle fixes cryptography API authentication bypass flaw

https://www.bleepingcomputer.com/news/security/bouncy-castle-fixes-cryptography-api-authentication-bypass-flaw/

SoReL-20M:一个包含 2000 万个恶意软件样本的数据集

日期: 2020-12-14

等级: 中

来源: The Hacker News

标签: ['Sophos', 'ReversingLabs', 'Dataset', 'Malware Samples']

"SoReL-20M"是一个数据集，包含用于 2000 万个`Windows .PE`文件的元数据，标签和功能。网络安全公司`Sophos`和`ReversingLabs`在 2020 年 12 月 14 日联合发布了"SoReL-20M"。这是有史以来第一个生产规模的恶意软件研究数据集，该数据集将提供给公众，旨在建立有效的防御措施并推动整个行业在安全检测和响应方面的改进。

详情

SoReL-20M: A Huge Dataset of 20 Million Malware Samples Released Online

https://thehackernews.com/2020/12/sorel-20m-huge-dataset-of-20-million.html

严重的 Golang XML 解析器漏洞可以绕过 SAML 身份验证

日期: 2020-12-14

等级: 中

来源: Ax Sharma

标签: ['Mattermost', 'Golang', 'Vulnerability', 'SAML', 'XML']

2020 年 12 月 14 日，`Mattermost`与`Golang`协作，揭示了`Go`语言的`XML`解析器中的 3 个严重漏洞。 如果攻击者成功利用这些漏洞，会影响多个基于 Go 的 SAML 实现，能够绕

过 SAML 的身份验证。 由于这些漏洞，基于 Go 的`SAML`实现在许多情况下容易被攻击者篡改，比如通过向正确签名的`SAML`消息注入恶意标记，可以伪造正确签名。

详情

Critical Golang XML parser bugs can cause SAML authentication bypass

https://www.bleepingcomputer.com/news/security/critical-golang-xml-parser-bugs-can-cause-saml-authentication-bypass/

苹果修复了 iOS 和 iPadOS 中的多个代码执行漏洞

日期: 2020-12-15

等级: 中

来源: Pierluigi Paganini

标签: ['Apple', 'iOS', 'iPadOS', 'Code Execution', 'Security Updates', 'Vulnerability']

苹果发布了安全更新，以修复其 iOS 和 iPadOS 操作系统中的多个严重的代码执行漏洞。苹果在安全更新中发布了 iOS 14.3 和 iPadOS 14.3 版本，以解决 11 个安全漏洞，包括代码执行漏洞等。 攻击者能够利用这些严重的漏洞，通过恶意字体文件在`iPhone`和`iPad`上执行恶意代码。 这些漏洞的编号包含`CVE-2020-27943`和`CVE-2020-27944`等。

详情

Apple addressed multiple code execution flaws in iOS and iPadOS

https://securityaffairs.co/wordpress/112304/security/ios-ipados-flaws.html

研究人员把 RAM 变成 WiFi 卡，从未联网的系统中窃取数据

日期: 2020-12-15

等级: 中

来源: Catalin Cimpanu

标签: ['RAM', 'WiFi', 'Air-gapped Systems', 'AIR-FI']

以色列一所大学的学者 2020 年 12 月 15 日发表了一项新的研究，详细介绍了一项技术，该技术可以将 RAM 卡转换成临时的 WIFI 发射器，并在没有 WiFi 的，未联网的计算机内传输敏感数据。 该技术名为 AIR-FI，是以色列内盖夫本古里安大学研发部负责人`Mordechai Guri`发现的。 在过去的五年里，Guri 领导了数十个研究项目，通过非常规的方法从未联网的系统中窃取数据。

详情

Academics turn RAM into WiFi cards to steal data from air-gapped systems

https://www.zdnet.com/article/academics-turn-ram-into-wifi-cards-to-steal-data-from-air-gapped-systems/

Facebook 因欺诈性 VPN 行为被 ACCC 告上法庭

日期: 2020-12-16

等级: 中

来源: Chris Duckett

标签: ['ACCC', 'Facebook', 'Onavo Protect VPN', 'Court']

澳大利亚竞争与消费者委员会（ACCC）已在澳大利亚联邦法院对`Facebook`及其两家子公司提起诉讼，指控这些公司在推广`Onavo Protect VPN`应用程序时具有虚假，误导或欺骗性行为。 ACCC 声称，在 2016 年 2 月 1 日至 2017 年 10 月之间，`Facebook`及其子公司`Facebook Israel Ltd`和`Onavo，出于商业利益而收集并使用了大量用户数据。

详情

Facebook dragged to court by ACCC over deceptive VPN conduct allegations

https://www.zdnet.com/article/facebook-dragged-to-court-by-accc-over-deceptive-vpn-conduct-allegations/

美国航空监管机构发布了安全更新

日期: 2020-12-16

等级: 中

来源: Gareth Corfield

标签: ['Boeing', 'FAA', 'Software Updates']

波音 747 客机、波音 787 客机和波音 777 客机的软件更新修复了一些漏洞，这些漏洞影响了飞行的安全性，并导致美国联邦航空局（FAA）向飞行员发布警告。 波音 777 和波音 787 自动油门系统的安全更新改变了系统的运行方式。

详情

US aviation regulator issues safety bulletins over flaws in software updates for Boeing 747, 777, 787 airliners • The Register

https://www.theregister.com/2020/12/16/boeing_software_updates_faa_warning/

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