安全事件周报

安全事件周报 (11.30-12.06)

360CERT
北京奇虎科技有限公司 | 2020-12-07

报告信息

报告名称	安全事件周报（11.30-12.06）		
报告类型	安全事件周报	报告编号	B6-2020-120701
报告版本	1.0	报告日期	2020-12-07
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	2020-12-07	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 58 项

话题集中在`勒索软件`、`网络攻击`方面，涉及的组织有：`温哥华地铁运营商`、`Kopter`、`Randstad`、`VMware`等。勒索及网络攻击数量剧增，良好的安全管理和员工安全意识提升刻不容缓。

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**
勒索软件团伙声称从 E-Land 窃取了 200 万张信用卡	★★★★★
新的 TrickBot 版本可以篡改 UEFI/BIOS 固件	★★★★★
温哥华地铁的交通系统被 Egregor 勒索软件攻击	★★★★★
勒索软件袭击直升机制造商 Kopter	★★★★★
宾夕法尼亚州特拉华县选择向 DoppelPaymer 团伙支付 50 万赎金	★★★★
Docker 恶意软件现很普遍，开发人员需要认真对待 Docker 的安全性	★★★★
DarkIRC 恶意软件利用 Oracle WebLogic 的严重漏洞	★★★★
阿拉巴马州学区因勒索软件攻击而关闭	★★★★
俄罗斯黑客组织使用 Dropbox 存储恶意软件窃取的数据	★★★★
K12 教育巨头将赎金支付给 Ryuk 组织	★★★★
攻击者使用新的恶意 NPM 软件包安装 njRAT 远程木马	★★★★
恶意软件：DeathStalker	★★★★
Egregor 勒索软件袭击人力资源巨头 Randstad	★★★★
黑客利用更新的恶意软件攻击 MacOS 用户	★★★
在勒索软件攻击后，巴尔的摩的师生被告知停用 Windows 电脑	★★★
十月勒索软件袭击，佛蒙特州医院仍在恢复当中	★★★
微软将越南政府黑客与加密挖掘恶意软件活动联系起来	★★★
具有 SSH 横向移动功能的僵尸网络	★★★
8%的 Google Play 应用程序易受旧的安全漏洞的攻击	★★★
数据安全	**等级**
法国制药分销平台泄漏 1.7 TB 以上的数据	★★★★★
尽管修复了漏洞，但 Android 应用程序仍暴露了 1 亿用户的信息	★★★★★

印度就业网站 IIMJobs 遭黑客攻击，数据库在网上泄露	★★★★★
俄罗斯黑客论坛上泄露了 850 多万条来自免版税图片网站的用户记录	★★★★★
医疗保健提供商 AspenPoint 数据泄露影响 29.5 万名患者	★★★★
Absa 银行卷入数据泄露，员工被控盗窃	★★★
Instagram 泄露未成年人的电子邮件地址	★★★
网络攻击	**等级**
黑客利用黑盒攻击从意大利的 atm 机中窃取了 80 万欧元	★★★★★
新型网络攻击可以欺骗 DNA 科学家制造危险的病毒和毒素	★★★★
信用卡分离器使用被盗的订单信息填充伪造的 PayPal 表格	★★★★
朝鲜黑客攻击了英国 COVID 疫苗制造商阿斯利康	★★★★
网络钓鱼使用 FINRA 相似域来瞄准美国经纪公司	★★★★
巴西航空工业公司遭到网络攻击	★★★★
LinkedIn 诈骗：仍然是最流行的网络钓鱼形式	★★★★
新的网络钓鱼组织的目标是 COVID-19 疫苗供应链	★★★★
一男子因攻击任天堂窃取数据被叛 3 年监禁	★★★★
黑客在社交媒体共享图标中隐藏了软件掠取器	★★★★
BlackShadow 黑客以 100 万美元勒索以色列保险公司	★★★★
伊朗黑客袭击以色列供水设施	★★★★
警方逮捕了两名盗窃国防公司敏感数据的黑客	★★★★
美国联邦调查局和国土安全部警告称，美国智库将受到攻击	★★★
HMRC 钓鱼攻击滥用邮件服务，绕过垃圾邮件过滤器	★★★
针对全球大学的网络钓鱼活动	★★★
MetaMask 网络钓鱼通过 Google 广告窃取加密货币钱包	★★★
网络雇佣兵组织 DeathStalker 使用了一个新的后门	★★★

医疗机构 Johnson & Johnson 遭受的网络攻击上升了 30%	★★★
其他事件	**等级**
Talos 报告了 WebKit 的远程代码执行漏洞	★★★★★
扫描 400 万个 Docker images 后发现：51%存在严重漏洞	★★★★★
Hacker_R_US 因炸弹威胁和 DDoS 勒索而入狱八年	★★★★
OpenClinic 程序存在共享电子病历漏洞	★★★★
谷歌白帽详解零点击蠕虫 Wi-Fi 漏洞	★★★★
TIM 红队研究（RTR）的专家发现 6 个 0day 漏洞	★★★
Gootkit 恶意软件与 REvil 勒索软件同时活跃	★★★
微软删除了 18 个恶意 Edge 扩展	★★★
最大的网络色情犯罪团伙"Nth Room"头目被判入狱 40 年	★★★
施乐 DocuShare 漏洞导致数据泄漏	★★★
IOS 中的漏洞可以让攻击者在 WIFI 覆盖范围内控制苹果手机	★★★
VMware 修复了 NSA 报告的 0day 漏洞	★★★
Google Play 源代码漏洞使应用程序易受攻击	★★★

三、 事件详情

(一) 恶意程序

勒索软件团伙声称从 E-Land 窃取了 200 万张信用卡

日期: 2020-12-03

等级: 高

来源: Lawrence Abrams

标签: ['E-Land Retail', 'Ransomware', 'Clop', 'Credit Cards']

Clop 勒索软件声称在过去的一年时间里从 E-Land Retail 盗窃了 200 万张信用卡。 E-Land Retail 是 E-Land Global 的子公司，经营着许多零售服装店，包括 New Core 和 NC 百货商店。 2020 年 10 月，E-Land Retail 在遭受 CLOP 勒索软件攻击后不得不关闭 23 个 NC 百货商店和 New Core 商店。 在被攻击之后，E-Land Retail 表示敏感的客户数据是安全的，因为它被加密存储在另一台服务器上。

详情

Ransomware gang says they stole 2 million credit cards from E-Land

https://www.bleepingcomputer.com/news/security/ransomware-gang-says-they-stole-2-million-credit-cards-from-e-land/

新的 TrickBot 版本可以篡改 UEFI/BIOS 固件

日期: 2020-12-03

等级: 高

来源: Catalin Cimpanu

标签: ['TrickBot', 'UEFI', 'BIOS', 'Malware', 'Botnet', 'MosacRegressor', 'LoJax']

TrickBot 恶意软件的运营商添加了一项新功能，可以使他们与受感染计算机的 BIOS 或 UEFI 固件进行交互。 安全公司 Advanced Intelligence 和 Eclypsium 在 2020 年 12 月 3 日发表的联合报告中说，新功能被发现在新的 TrickBot 模块的内部，该模块在 10 月底首次出现在野外。 新模块使安全研究人员感到担忧，因为其功能将使 TrickBot 恶意软件在受感染的系统上建立更持久的立足点，从而使恶意软件能够在操作系统重新安装后存活下来。

详情

New TrickBot version can tamper with UEFI/BIOS firmware

https://www.zdnet.com/article/new-trickbot-version-can-tamper-with-uefibios-firmware/

温哥华地铁的交通系统被 Egregor 勒索软件攻击

日期: 2020-12-04

等级: 高

来源: Lawrence Abrams

标签: ['Egregor', 'TransLink', 'Ransomware', 'IT', 'Payment Systems']

`Egregor`勒索软件的行动已经破坏了温哥华地铁公司的运输机构`TransLink`，网络攻击导致服务和支付系统中断。在恢复了支付系统后，TransLink 发表了一份声明，披露了勒索软

件攻击导致了 IT 问题，并且还称："我们的一些 IT 基础设施遭到勒索软件攻击，包括通过印刷信息与 TransLink 通信，"。`Global BC`记者乔丹·阿姆斯特朗（Jordan Armstrong）在推特上发布了一张勒索单的图片，并称 TransLink 打印机正在反复打印赎金单。

详情

Metro Vancouver's transit system hit by Egregor ransomware

https://www.bleepingcomputer.com/news/security/metro-vancouvers-transit-system-hit-by-egregor-ransomware/

勒索软件袭击直升机制造商 Kopter

日期: 2020-12-05

等级: 高

来源: Catalin Cimpanu

标签: ['Kopter', 'LockBit', 'Ransomware', 'Helicopter']

直升机制造商 Kopter 已经成为勒索软件攻击的受害者，因为黑客入侵了它的内部网络并加密了公司的文件。在 Kopter 拒绝与黑客接触后，勒索软件团伙在互联网上公布了该公司的一些文件。Kopter 的数据已经发表在 dark web 上的一个博客上，该博客由 LockBit 勒索软件团伙运营。在这个网站上共享的文件包括商业文件，内部项目，以及各种航空航天和国防工业标准。

详情

Ransomware hits helicopter maker Kopter

https://www.zdnet.com/article/ransomware-hits-helicopter-maker-kopter/

宾夕法尼亚州特拉华县选择向 DoppelPaymer 团伙支付 50 万赎金

日期: 2020-11-30

等级: 高

来源: Pierluigi Paganini

标签: ['Delaware County', 'Pennsylvania', 'DoppelPaymer', 'Ransomware']

在 2020 年 11 月 28 日成为 DoppelPaymer 勒索软件攻击的受害者之后，宾夕法尼亚州的特拉华县选择支付 500,000 美元的赎金。 消息人士告诉《行动新闻》，网络犯罪分子在 2020 年 11 月 28 日控制了网络加密文件，包括警方报告、工资、采购和其他数据库。 然而，起诉证据并未受到影响。这次感染并未影响选举局和县紧急服务部。

详情

Delaware County, Pennsylvania, opted to pay 500K ransom to DoppelPaymer gang

https://securityaffairs.co/wordpress/111654/cyber-crime/delaware-county-doppelpaymer-ransomware.html

Docker 恶意软件现很普遍，开发人员需要认真对待 Docker 的安全性

日期: 2020-11-30

等级: 高

来源: Catalin Cimpanu

标签: ['Docker', 'Kubernetes', 'Cloud', 'Misconfiguring']

2017 年底，恶意软件领域发生了重大变化。随着基于云的技术越来越流行，网络犯罪团伙也开始瞄准 Docker 和 Kubernetes 系统。 这些攻击大多遵循一种非常简单的模式，即攻击者扫描配置错误、管理界面暴露在网上的系统，以接管服务器并部署加密货币挖掘恶意软件。 在过去的三年里，这些攻击不断升级，针对 Docker(和 Kubernetes)的新恶意软件种类和攻击者正在定期被发现。十一月末，中国安全公司奇虎 360（qihoo360）发现了这些最新的恶意软件。 但是，尽管对 Docker 服务器的恶意软件攻击实际上现已司空见惯，但许多 Web 开发人员和基础架构工程师仍未吸取教训，并且仍在错误配置 Docker 服务器，使它们容易受到攻击。

详情

Docker malware is now common, so devs need to take Docker security seriously

https://www.zdnet.com/article/docker-malware-is-now-common-so-devs-need-to-take-docker-security-seriously/

DarkIRC 恶意软件利用 Oracle WebLogic 的严重漏洞

日期: 2020-12-01

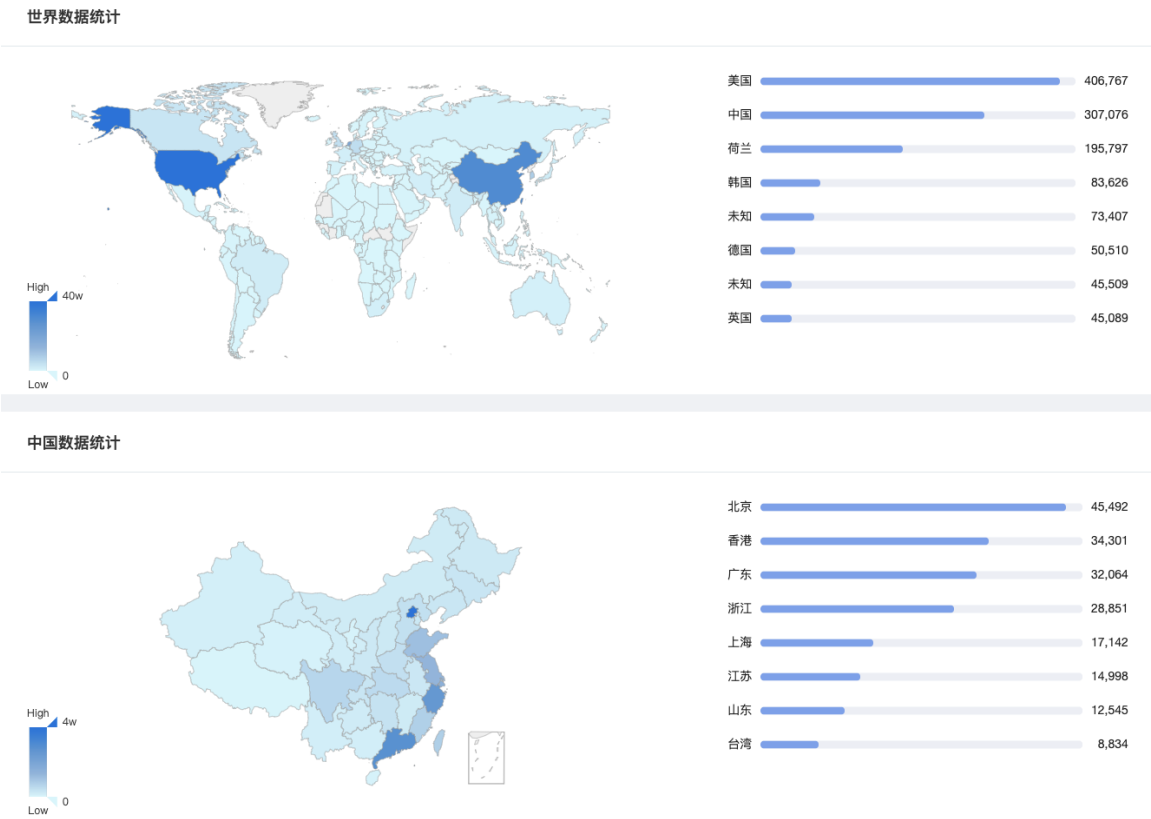
等级: 高

来源: Sergiu Gatlan

标签: ['Oracle WebLogic', 'DarkIRC', 'Botnet', 'Shodan', 'RCE', 'Vulnerability']

一个名为 DarkIRC 的僵尸网络正在主动针对成千上万个暴露的 Oracle WebLogic 服务器进行攻击，这些攻击旨在利用 Oracle 两个月前修复的 CVE-2020-14882 远程代码执行（RCE）漏洞。 根据瞻博网络威胁实验室的报告，基于 Shodan 的统计信息，可以通过 Internet 访问近 3,000 台 Oracle WebLogic 服务器，并允许未经身份验证的攻击者在目标服务器上执行远程代码。 攻击者目前使用至少五种不同的有效载荷来攻击 WebLogic 服务器，DarkIRC 恶意软件目前在黑客论坛上以 75 美元的价格出售。

目前 weblogic 的具体分布如下图，数据来自于 360 QUAKE



详情

Critical Oracle WebLogic flaw actively exploited by DarkIRC malware

https://www.bleepingcomputer.com/news/security/critical-oracle-weblogic-flaw-actively-exploited-by-darkirc-malware/

阿拉巴马州学区因勒索软件攻击而关闭

日期: 2020-12-01

等级: 高

来源: Lawrence Abrams

标签: ['Huntsville City School', 'Alabama', 'Ransomware', 'Shut Down']

勒索软件运营商袭击了阿拉巴马州的亨茨维尔市学区，迫使他们在 2020 年 12 月所剩余的时间关闭学校。 亨茨维尔市学区是阿拉巴马州第六大学区，拥有近 24,000 名学生，2,300 名员工和 37 所学校。 由于 COVID-19，学区既提供了在校教学又提供了完全的在线学习体验。 11 月 30 日，就在学生们从感恩节假期回来的时候，由于网络攻击破坏了他们的 IT 系统，学校给学生提前放学。 为防止勒索软件传播到借给学生和教职员工的设备，学区要求关闭所有学区发行的设备，并保持关闭状态，直至另行通知。

详情

Alabama school district shut down by ransomware attack

https://www.bleepingcomputer.com/news/security/alabama-school-district-shut-down-by-ransomware-attack/

俄罗斯黑客组织使用 Dropbox 存储恶意软件窃取的数据

日期: 2020-12-02

等级: 高

来源: Sergiu Gatlan

标签: ['Turla', 'Russian', 'Crutch', 'Hacking Group', 'Malware']

俄罗斯支持的黑客组织图拉（Turla）在针对欧盟国家外交部等知名目标的网络间谍活动中，利用一个此前未经证实的恶意软件工具集部署后门，窃取敏感文件。 这个之前未知的恶意软件框架被作者命名为 Crutch，被用于从 2015 年到 2020 年初的活动中。 Turla 的 Crutch 恶意软件旨在帮助收集和泄露敏感文件以及俄罗斯黑客组织控制的 Dropbox 帐户感兴趣的其他各种文件。

详情

Russian hacking group uses Dropbox to store malware-stolen data

https://www.bleepingcomputer.com/news/security/russian-hacking-group-uses-dropbox-to-store-malware-stolen-data/

K12 教育巨头将赎金支付给 Ryuk 组织

日期: 2020-12-02

等级: 高

来源: Pierluigi Paganini

标签: ['K12 Inc.', 'Ryuk', 'Ransom', 'Education', 'Data Leak']

在线教育巨头 K12 在 2020 年 11 月中旬遭到了 Ryuk 勒索软件的攻击，现在已经支付了赎金以避免数据泄露。 K12 公司是一家销售在线教育和课程的盈利性教育公司。K12 是一个教育管理组织(EMO)，为公立学校的学生提供从幼儿园到 12 年级的在线教育，公开交易的 K12 是注册人数最多的 EMO。 K12 2020 年 12 月初公开披露了勒索软件攻击，该事件发生在 2020 年 11 月中旬，迫使公司关闭其系统，以防止恶意软件的传播。

详情

K12 education giant paid the ransom to the Ryuk gang

https://securityaffairs.co/wordpress/111824/malware/k12-ryuk-ransomware.html

攻击者使用新的恶意 NPM 软件包安装 njRAT 远程木马

日期: 2020-12-03

等级: 高

来源: GURUBARAN S

标签: ['Remote Access Trojan', 'NMP Packages', 'njRAT', 'jdb.js', 'db-json.js', 'Phishing']

RAT（远程访问木马）是一种恶意软件，攻击者可以利用它来控制受感染的系统，执行任意命令，运行键盘记录程序以及谨慎进行其他监视活动。 在感恩节，Sonatype 在 npm 注册表中发现了一种新的恶意软件。 恶意数据包是`jdb.js`和`db-json.js`，均由同一作者发布。 经过进一步调查，发现`jdb.js`背后的作者发布了另一个恶意的 npm 软件包`db-json.js`。 `jdb.js`是一个恶意软件包，与`njRAT(Bladabindi)`捆绑在一起，该软件包在 2014 年导致 Microsoft 关闭了 400 万个站点。 njRAT 的变种最近通过 Youtube 上的比特币骗局和 Excel 钓鱼邮件传播。

详情

New malicious NPM packages Used by Attackers Install njRAT Remote Access Trojan
https://gbhackers.com/new-malicious-npm-packages-used-by-attackers-install-njrat-remote-access-trojan/

恶意软件：DeathStalker

日期: 2020-12-03

等级: 高

来源: Pierre Delcher

标签: ['DeathStalker', 'Malware', 'Phishing', 'Securelist', 'PowerShell', 'Backdoor']

DeathStalker 是一个恶意软件，从 2012 年开始活跃，该恶意软件在 2018 年引起了 securelist 团队的注意，因为其独特的攻击特征不符合通常的网络犯罪或国家赞助的活动，使 securelist 团队认为 DeathStalker 是一家"黑客招募"公司。 从基于 Python 和 VisualBasic 的 Janicab，到基于 PowerShell 的 Powersing，DeathStalker 多年来利用了数种恶意软件攻击手段，并通过了基于 JavaScript 的 Evilnum。 为了启动感染，DeathStalker 通常依赖带有附件的鱼叉式网络钓鱼电子邮件、或指向公共文件共享服务的链接、或基于 Windows 快捷方式的脚本执行。

详情

What did DeathStalker hide between two ferns?
https://securelist.com/what-did-deathstalker-hide-between-two-ferns/99616/

Egregor 勒索软件袭击人力资源巨头 Randstad

日期: 2020-12-04

等级: 高

来源: Lawrence Abrams

标签: ['Egregor', 'Randstad', 'Ransomware', 'Data Breach', 'Staffing Agency']

人事代理公司`Randstad`宣布他们的网络被 Egregor 勒索软件入侵，他们在攻击中窃取了未加密的文件。`Randstad`是全球最大的人事代理机构，在 38 个市场设有办事处，并拥有著名的就业网站`Monster.com.` Randstad 拥有超过 38000 名员工，2019 年实现收入 237 亿欧元。Egregor 勒索软件公布了窃取的 1%的数据。这些泄露的数据是一个 32.7MB 的档案，包含 184 个文件，包括会计电子表格、财务报告、法律文件和其他杂项业务文档。

详情

Largest global staffing agency Randstad hit by Egregor ransomware
https://www.bleepingcomputer.com/news/security/largest-global-staffing-agency-randstad-hit-by-egregor-ransomware/

黑客利用更新的恶意软件攻击 MacOS 用户

日期: 2020-11-30

等级: 中

来源: Danny Palmer

标签: ['MacOS', 'OceanLotus', 'APT32', 'Backdoor']

一个新的恶意软件正以苹果 MacOS 用户为目标，研究人员称这与国家支持的黑客行动有关。 Trend Micro 的网络安全分析师详细介绍了这一活动，他们已将其与 OceanLotus（也称为 APT32）相关联，该组织是一个与越南政府有联系的黑客组织。 OceanLotus 的目标客户是在越南工作的外国组织。MacOS 后门为攻击者提供了进入受感染计算机的窗口，使他们能够窥探并窃取机密信息。

详情

Hackers are targeting MacOS users with this updated malware

https://www.zdnet.com/article/hackers-are-targeting-macos-users-with-this-updated-malware/

在勒索软件攻击后，巴尔的摩的师生被告知停用 Windows 电脑

日期: 2020-11-30

等级: 中

来源: Sergiu Gatlan

标签: ['Baltimore County Public Schools', 'Windows PC', 'Google', 'Ransomware', 'Baltimore', 'Chromebook']

巴尔的摩县学区是美国第 25 大学校系统。巴尔的摩县公立学校（BCPS）敦促学生和教职员工停止使用学校发行的 Windows 计算机，并在勒索软件攻击于 2020 年 11 月 25 日袭击该地区的网络后，仅使用 Chromebook 和 Google 帐户。 勒索软件攻击迫使 BCPS 关闭其大部分网络，原因是事件期间受影响的系统数量众多。如果员工和学生的信息也从学区系统中泄露，这起事件也可能导致数据泄露。

详情

Baltimore students told to ditch Windows PCs after ransomware attack

https://www.bleepingcomputer.com/news/security/baltimore-students-told-to-ditch-windows-pcs-after-ransomware-attack/

十月勒索软件袭击，佛蒙特州医院仍在恢复当中

日期: 2020-11-30

等级: 中

来源: Lawrence Abrams

标签: ['The University of Vermont Health Network', 'Ryuk', 'Ransomware']

2020 年 10 月，佛蒙特大学医院遭受 Ryuk 勒索软件攻击，在其卫生网络中的所有 7 家医院中都不同程度地影响了服务。现佛蒙特大学健康网络仍在恢复，其服务慢慢恢复在线。袭击发生时，仅 UVM Medical Center 的患者护理受到影响，一些选手术已重新安排。 不过，大多数医院都受到 IT 中断的影响，例如无法获得 EPIC 病历，MyChart 患者门户，电子邮件和电话系统。 2020 年 11 月 27 日，佛蒙特大学健康网络大学发布了勒索软件攻击的更新，解释了正在恢复的服务。

详情

Vermont hospitals still recovering from October ransomware attack

https://www.bleepingcomputer.com/news/security/vermont-hospitals-still-recovering-from-october-ransomware-attack/

微软将越南政府黑客与加密挖掘恶意软件活动联系起来

日期: 2020-12-01

等级: 中

来源: Catalin Cimpanu

标签: ['Vietnamese', 'Microsoft', 'Bismuth', 'Government-Backed Hackers']

微软在 2020 年 11 月 30 日以报告表示，越南政府支持的黑客最近被发现在他们的常规网络间谍工具包中部署加密货币、挖掘恶意软件。 该报告强调了网络安全行业的增长趋势，越来越多的国家支持的黑客组织也将目光投向了常规的网络犯罪活动，这使得更加难以区分财务动机的犯罪与情报收集活动。 该越南小组被 Microsoft 追踪为 Bismuth，自 2012 年以来一直活跃，并以代号 APT32 和 OceanLotus 等闻名。

详情

Microsoft links Vietnamese state hackers to crypto-mining malware campaign

https://www.zdnet.com/article/microsoft-links-vietnamese-state-hackers-to-crypto-mining-malware-campaign/

具有 SSH 横向移动功能的僵尸网络

日期: 2020-12-02

等级: 中

来源: Pierluigi Paganini

标签: ['Weblogic', 'Monero XMR Miner', 'Tsunami', 'Cloud', 'Botnet', 'SSH Lateral Movement']

一位安全研究人员 0xrb 分享了使用 Weblogic 漏洞进行传播的僵尸网络示例。 该僵尸网络也是在 2020 年 11 月 28 日被 BadPackets 发现的，截至 2020 年 12 月 1 日，它仍处于活动状态。该僵尸网络带有两个有效载荷：1）Monero XMR Miner 二进制文件； 2）Tsunami 二进制文件。 该僵尸网络以云服务器为目标。 2020 年 9 月，AWAKE Security 的帕特里克·奥尔森（Patrick Olsen）调查并报告了仅携带 XMR Miner 有效载荷的僵尸网络的早期版本。

详情

Multi-Vector Miner+Tsunami Botnet with SSH Lateral Movement

https://securityaffairs.co/wordpress/111761/malware/multi-vector-miner-tsunami-botnet.html

8%的 Google Play 应用程序易受旧的安全漏洞的攻击

日期: 2020-12-03

等级: 中

来源: Catalin Cimpanu

标签: ['Android', 'Check Point', 'Google Play', 'Vulnerability', 'Play Core']

根据安全公司 Check Point 2020 年秋天进行的一项扫描，大约 8%的官方 Google Play 商店提供的 Android 应用程序，容易受到流行的 Android 库中的安全漏洞的攻击。 该安全漏洞存在于旧版本的 Play Core 中，该版本是 Google 提供的 Java 库，开发人员可以将其嵌入其应用程序中以与官方的 Play 商店门户进行交互。 Google 修补了 2020 年 3 月份发布的 Play Core 1.7.2 中的漏洞，但根据 Check Point 2020 年 12 月 3 日发布的新发现，并非所有开发人员都已更新了其应用附带的 Play Core 库，这就使得用户容易从安装在其设备上的恶意应用中遭受数据窃取攻击。

详情

8% of all Google Play apps vulnerable to old security bug
https://www.zdnet.com/article/8-of-all-google-play-apps-vulnerable-to-old-security-bug/

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. 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
3. 减少外网资源和不相关的业务，降低被攻击的风险
4. 各主机安装 EDR 产品，及时检测威胁
5. 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
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. 主机集成化管理，出现威胁及时断网
8. 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
9. 注重内部员工安全培训
10. 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

(二) 数据安全

法国制药分销平台泄漏 1.7 TB 以上的数据

日期: 2020-12-01
等级: 高
来源: Edvardas Mikalauskas
标签: ['CyberNews', 'ElasticSearch', 'Apodis Pharma', 'France', 'Leaking']

`CyberNews`调查小组发现了`ElasticSearch`数据库的一个不安全的、可公开访问的`Kibana`仪表板，该数据库包含属于法国软件公司`Apodis Pharma`的机密数据。 Apodis Pharma 是一家为药房，医疗机构，制药实验室和健康保险公司提供数字化供应链管理平台和其他软件解决方案的公司。 CyberNews 发现的数据库包含超过 1.7 TB 的与业务相关的机密数据，包括药品销售数据，Apodis Pharma 合作伙伴和员工的全名，客户仓库库存统计信息，药品装运位置和地址等。

详情

French pharma distribution platform leaking 1.7+ TB of data
https://cybernews.com/security/french-pharmaceuticals-distribution-platform-leaking-1-7-tb-confidential-data/

尽管修复了漏洞，但 Android 应用程序仍暴露了 1 亿用户的信息

日期: 2020-12-01

等级: 高

来源: Sergiu Gatlan

标签: ['GO SMS Pro', 'Android', 'Bug Fix', 'Trustwave']

GO SMS Pro 是一个 Android 即时消息应用程序，安装量超过 1 亿，尽管开发人员已经为修复数据泄漏背后的漏洞进行了将近两个星期的努力，但它仍在公开数百万用户的私人共享消息。 该漏洞由 Trustwave 的研究人员三个月前发现并于 11 月 19 日公开披露，该漏洞使未经身份验证的攻击者可以不受限制地访问 GO SMS Pro 用户私下共享的语音消息，视频和照片。

详情

Android app still exposing messages of 100M users despite bug fix

https://www.bleepingcomputer.com/news/security/android-app-still-exposing-messages-of-100m-users-despite-bug-fix/

印度就业网站 IIMJobs 遭黑客攻击，数据库在网上泄露

日期: 2020-12-01

等级: 高

来源: Waqas

标签: ['IIMJobs', 'Leaked', 'Hacking Forum ', 'Highorbit Careers']

根据 Alexa 流量分析，IIMJobs 是印度访问量最大的 700 家网站之一。印度就业委员会 IIMJobs 的数据库在一个著名的黑客论坛上被泄露。 根据 Hackread.com 网站分析，该数据库于 2020 年 11 月 23 日被泄露，其中包含多达 46GB 的数据，这些数据来自于在 IIMJobs 注册的求职者和招聘人员。 可以证实，IIMJobs 网站约 140 万注册用户受到数据泄露的影响。

详情

Indian job portal IIMJobs hacked; database leaked online

https://www.hackread.com/indian-job-portal-iimjobs-hacked-database-leaked/

俄罗斯黑客论坛上泄露了 850 多万条来自免版税图片网站的用户记录

日期: 2020-12-02

等级: 高

来源: Edvardas Mikalauskas

标签: ['Russian', 'Inmagine', 'Hacker Forum', 'Database', '123RF.com']

一个免版税的图片网站，最近在一个俄罗斯黑客论坛上被泄露。 123RF.com 公司是一家位于马来西亚的数字股票内容代理公司，销售免版税的图片、录像和音频。 它是 Inmagine 集团的一部分，每月有超过 1200 万活跃用户（包括苹果、谷歌、亚马逊和微软等）。 存储在数据库泄露部分的 8500246 个用户记录包括用户的全名、电子邮件地址、IP 地址、位置、使用 MD5 哈希算法进行哈希处理的密码等。

详情

8.5+ million user records from royalty-free image website leaked on Russian hacker forum
https://cybernews.com/security/8-5-million-user-records-from-royalty-free-image-website-leaked-on-russian-hacker-forum/

医疗保健提供商 AspenPoint 数据泄露影响 29.5 万名患者

日期: 2020-11-30

等级: 高

来源: Sergiu Gatlan

标签: ['AspenPointe', 'Data Breach', 'Healthcare Provider']

美国医疗保健提供商 AspenPointe 通知患者，由于 2020 年 9 月的一次网络攻击，攻击者能够窃取受保护的健康信息（PHI）和个人识别信息（PII）。 AspenPointe 是一个非营利组织，由医疗补助、州、联邦和地方政府的合同以及捐款资助，管理着 12 个组织，每个组织为 5 万多个个人和家庭提供服务。 AspenPointe 最近发现了在 2020 年 9 月 12 日至 2020 年 9 月 22 日之间对其网络进行未经授权的访问。 该组织聘请了外部安全专家来调查此事件，并找出影响其网络的信息泄露范围。

详情

Healthcare provider AspenPointe data breach affects 295K patients
https://www.bleepingcomputer.com/news/security/healthcare-provider-aspenpointe-data-breach-affects-295k-patients/

Absa 银行卷入数据泄露，员工被控盗窃

日期: 2020-12-02

等级: 中

来源: Charlie Osborne

标签: ['Absa', 'Bank', 'Data Leak', 'Financial Services Group']

Absa 已经通知客户数据泄露，可能会危及他们的个人信息。 总部位于南非约翰内斯堡的金融服务集团（financial services group）提供个人和商业银行业务以及财富管理服务，已将安全事件的矛头指向一名员工。 Absa 在整个非洲大陆的 12 个国家/地区设有分支机构，约有 42,000 名员工。

详情

Absa bank embroiled in data leak, rogue employee accused of theft
https://www.zdnet.com/article/absa-bank-embroiled-in-data-leak-rogue-employee-accused-of-theft/

Instagram 泄露未成年人的电子邮件地址

日期: 2020-12-03

等级: 中

来源: Jeremy Kirk

标签: ['David Stier', 'Instagram', 'Leaking', 'HTML']

在 2020 年 11 月，旧金山的数据科学家 David Stier 发现 Instagram 在用户个人资料的网络版本的 HMTL 中泄漏了孩子的电子邮件地址。David Stier 还称，Instagram 在 HTML 源代

码中包含个人身份信息的方式与一年半前完全相同，社交媒体平台需要更好的保障措施社交网络给未成年人带来特殊风险。 目前 Instagram 已经修复了这个漏洞。

详情

Why Did Instagram Leak Minors' Email Addresses Again?

https://www.databreachtoday.com/did-instagram-leak-minors-email-addresses-again-a-15452

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. 严格控制数据访问权限
4. 发生数据泄漏事件后，及时进行密码更改等相关安全措施
5. 及时备份数据并确保数据安全
6. 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

(三) 网络攻击

黑客利用黑盒攻击从意大利的 atm 机中窃取了 80 万欧元

日期: 2020-12-01

等级: 高

来源: GURUBARAN S

标签: ['Italian', 'Black Box Attack', 'ATMs', 'Cyberattacks ']

一个犯罪组织利用一种新的黑匣子攻击技术，从意大利的至少 35 台自动取款机中盗取钱财。 意大利执法机构证实，该网络犯罪组织利用 ATM 黑盒攻击，在短短 7 个月内窃取了约 80 万欧元。 在这种攻击中，黑盒设备(如移动设备或覆盆子)与 ATM 物理连接，攻击者利用它向机器发送命令，然后从自动取款机中提取所有现金。

详情

Hackers Steal 800,000€ from ATMs in Italy Using Black Box attack

https://gbhackers.com/hackers-steal-money/

新型网络攻击可以欺骗 DNA 科学家制造危险的病毒和毒素

日期: 2020-11-30

等级: 高

来源: Charlie Osborne

标签: ['Cyberattack', 'DNA', 'Dupe', 'Viruses', 'Toxins']

一种新形式的网络攻击已经被开发出来，凸显了未来针对生物研究领域的数字攻击可能产生的后果。 2020 年 11 月 30 日，内盖夫本-古里安大学(Ben-Gurion University)的学者们描述了"不知情的"生物学家和科学家如何可能成为网络攻击的受害者，这些攻击旨在将生物战提升到另一个水平。 在全球科学家正在推动研发潜在疫苗以对抗 COVID-19 的时候，本·古里安的研究小组表示，攻击者不再需要物理接触"危险"物质即可生产或提供它。相反，攻击者可以通过针对性的网络攻击来诱骗科学家生产毒素或合成病毒。

详情

This new cyberattack can dupe DNA scientists into creating dangerous viruses and toxins

https://www.zdnet.com/article/this-new-cyberattack-can-dupe-scientists-into-creating-dangerous-viruses-toxins/

信用卡分离器使用被盗的订单信息填充伪造的 PayPal 表格

日期: 2020-11-30

等级: 高

来源: Sergiu Gatlan

标签: ['PayPal', 'JavaScript', 'Card Skimmers', 'Magecart', 'Iframe']

新的信用卡分离器使用一种创新技术来注入有效的 PayPal iframe，并在受到破坏的在线商店上劫持结帐流程。 信用卡分离器是基于 JavaScript 的脚本，Magecart 网络犯罪团伙将其作为 Web 窃取（也称为电子窃取）攻击的一部分，进行黑客攻击后，注入到电子商务网站的结帐页面中。 攻击者的最终目标是收集被入侵商店的客户提交的付款和个人信息，并将其发送到受其控制的远程服务器上。

详情

Credit card skimmer fills fake PayPal forms with stolen order info

https://www.bleepingcomputer.com/news/security/credit-card-skimmer-fills-fake-paypal-forms-with-stolen-order-info/

朝鲜黑客攻击了英国 COVID 疫苗制造商阿斯利康

日期: 2020-12-02

等级: 高

来源: GURUBARAN S

标签: ['AstraZeneca', 'North Korean', 'COVID Vaccine', 'LinkedIn', 'WhatsApp']

英国制药公司阿斯利康（AstraZeneca）是开发 COVID-19 疫苗的领先制造商之一，已成为朝鲜黑客的目标。 两名知情人士向路透社透露，2020 年 11 月至 12 月，有疑似朝鲜黑客试图侵入阿斯利康的系统。 黑客冒充 LinkedIn 和 WhatsApp 上的招聘人员，向阿斯利康员工提供虚假工作机会。 该报告称，那些声称是职务说明的文件都带有旨在访问受害者计算机的恶意代码。

详情

North Korean Hackers Targeted COVID Vaccine Maker AstraZeneca

https://gbhackers.com/covid-vaccine-maker-targeted/

网络钓鱼使用 FINRA 相似域来瞄准美国经纪公司

日期: 2020-12-02

等级: 高

来源: Sergiu Gatlan

标签: ['US', 'FINRA', 'Phishing', 'Domain Spoofing', 'Securities']

美国证券业监管机构 FINRA 在 2020 年 12 月初的时候警告经纪公司，他们使用最近注册的网络域名欺骗合法的 FINRA 网站，不断进行网络钓鱼攻击。 金融业监管局（Financial Industry Regulatory Authority）是一个由美国证券交易委员会（SEC）监管的非盈利组织，负责监管美国境内所有公开活动的交易所市场和证券公司。 这个独立的、非政府的证券监管机构还监管着全美 62.4 万多家券商，每天都要审查数十亿起市场事件。

详情

Phishing targets US brokerage firms using FINRA lookalike domain

https://www.bleepingcomputer.com/news/security/phishing-targets-us-brokerage-firms-using-finra-lookalike-domain/

巴西航空工业公司遭到网络攻击

日期: 2020-12-02

等级: 高

来源: Angelica Mari

标签: ['Brazilian', 'Embraer', 'Cyberattack', 'Aerospace']

巴西航空防务集团巴西航空工业公司（Embraer）受到网络攻击，影响了公司的运营。 根据这家公司 2020 年 11 月 30 日发表的一份声明，这次攻击导致了该公司的数据泄漏，并且该网络攻击已于 2020 年 11 月 25 日被发现，因此无法访问该公司的单个系统环境。

详情

Brazilian aerospace firm Embraer hit by cyberattack

https://www.zdnet.com/article/brazilian-aerospace-firm-embraer-hit-by-cyberattack/

LinkedIn 诈骗：仍然是最流行的网络钓鱼形式

日期: 2020-12-02

等级: 高

来源: Chris Stokel-Walker

标签: ['LinkedIn', 'Phishing', 'Social Platforms']

LinkedIn 是世界上最有影响力的社交平台之一，也是业务和职业发展的重要场所。 但是，随着经济衰退开始加剧，人们继续努力攀登职业阶梯，LinkedIn 成为了诈骗者试图欺骗毫无戒心的受害者，并移交其个人详细信息的主要方式之一。 点击量最高的 LinkedIn 钓鱼邮件包括这样的主题:"你出现在新的搜索中!"、"人们在看你的 LinkedIn 资料"、"请把我加入你的 LinkedIn 网络"以及"在 LinkedIn 上加入我的网络"。 几乎有一半关于 LinkedIn 的钓鱼邮件被打开。

详情

LinkedIn scams: Still the most popular form of phishing

https://cybernews.com/security/linkedin-scams-still-the-most-popular-form-of-phishing/

新的网络钓鱼组织的目标是 COVID-19 疫苗供应链

日期: 2020-12-03

等级: 高

来源: Charlie Osborne

标签: ['Phishing', 'COVID-19', 'Vaccine', 'Supply Chains', 'Cold Chains']

一个新的全球网络钓鱼攻击的重点是破坏供应链，该供应链使 COVID-19 疫苗组件保持低温。 2020 年 12 月 3 日，IBM Security X-Force 团队的研究人员表示，与 COVID-19 冷链相关的组织已成为攻击者的目标，COVID-19 冷链是确保潜在疫苗在适当温度下安全存储和保存的供应链的一部分。 当这些疫苗需要在`-70°C`下保存以保持其功效时，维持和保护供应链的冷藏组件至关重要。不幸的是，这正是新的攻击浪潮着眼于破坏的领域。

详情

This phishing group is targeting COVID-19 vaccine supply chains

https://www.zdnet.com/article/this-phishing-group-is-targeting-covid-19-vaccine-supply-chains/

一男子因攻击任天堂窃取数据被叛 3 年监禁

日期: 2020-12-03

等级: 高

来源: Akshaya Asokan

标签: ['Ryan Hernandez', 'Phishing', 'Confidential Data', 'Nintendo']

美国司法部宣布，一名 21 岁的加利福尼亚男子因屡次入侵游戏公司任天堂、窃取机密数据而被判有期徒刑三年。 据美国司法部称，从 2016 年开始，当时还是未成年的埃尔南德斯就试图利用钓鱼技术侵入任天堂服务器，窃取公司员工的证书。 有一次，埃尔南德斯泄露了有关预期的 Nintendo Switch 控制台的信息。 根据法庭文件，2017 年，FBI 特工在父母的家中与埃尔南德斯协商，他同意停止对任天堂进行黑客攻击，以换取联邦当局不提出指控。 联邦检察官说，在 2018 年 6 月至 2019 年 6 月期间，埃尔南德斯再次侵入任天堂，包括该公司开发者的门户，试图窃取更多的公司数据和开发者工具。

详情

3 Years in Prison

https://www.databreachtoday.com/nintendo-hackers-sentence-3-years-in-prison-a-15508

黑客在社交媒体共享图标中隐藏了软件掠取器

日期: 2020-12-04

等级: 高

来源: Pierluigi Paganini

标签: ['Sansec', 'Software Skimmer', 'Icons', 'Social Media']

安全研究人员发现了一种新技术，在结账页面上插入一个软件掠取器，将恶意软件隐藏在社交媒体按钮中。 Sansec 的安全专家详细介绍了攻击者将软件掠取器注入结帐页面的新技术。 当黑客入侵电子商务网站，并植入旨在窃取支付卡数据或个人身份信息（PII）的恶意代码时，就会发生电子窃听。

详情

Hackers hide software skimmer in social media sharing icons
https://securityaffairs.co/wordpress/111872/malware/software-skimmer-social-share-icon.html

BlackShadow 黑客以 100 万美元勒索以色列保险公司

日期: 2020-12-04

等级: 高

来源: Lawrence Abrams

标签: ['Israeli', 'insurance Company', 'Bitcoin', 'Leaking', 'BlackShadow']

攻击者正在敲诈一家以色列保险公司，索要近 100 万美元的比特币，以停止泄露该公司被盗的数据。 2020 年 11 月 30 日，一个自称`BlackShadow`的网络犯罪组织在推特上说，他们入侵了以色列`Shirbit`保险公司，并在攻击中窃取了文件。 这些被盗数据包括文件、电子邮件 PST 文件、扫描文件、录音和护照图像。 2020 年 12 月 3 日，攻击者最终发布了一份勒索要求，声称 Shirbit 有 24 小时的时间发送 50 个比特币（约合 100 万美元），他们将停止泄露数据。 攻击者警告说，如果不支付报酬，他们将继续每 24 小时泄露一次数据。

详情

BlackShadow hackers extort Israeli insurance company for $1 million
https://www.bleepingcomputer.com/news/security/blackshadow-hackers-extort-israeli-insurance-company-for-1-million/

伊朗黑客袭击以色列供水设施

日期: 2020-12-04

等级: 高

来源: Pierluigi Paganini

标签: ['Iranian', 'ICS', 'Israeli', 'Water Facility', 'HMI']

研究人员透露，一群伊朗黑客侵入了以色列供水设施的一个未受保护的`ICS`。黑客在 2020 年 12 月 1 日晚发布的一段视频中声称，他们已经攻破了以色列的一处供水设施，很可能是循环水系统。水库的 HMI 系统直接连接到互联网上，没有任何安全设备保护或限制访问。此外，系统在访问时没有使用任何身份验证方法。这使得攻击者能够轻松地访问系统，并能够修改系统中的任何值，例如，允许他们篡改水压、改变温度等。

详情

Iranian hackers access unsecured HMI at Israeli Water Facility
https://securityaffairs.co/wordpress/111934/ics-scada/israeli-water-facility-breached.html

警方逮捕了两名盗窃国防公司敏感数据的黑客

日期: 2020-12-06

等级: 高

来源: Pierluigi Paganini

标签: ['Italian', 'Defense Company', 'Leonardo', 'Steal Data']

意大利警方逮捕了两名窃取国防公司`Leonardo S.p.A.`10GB 机密数据和军事机密的黑客。这两人是 Leonardo SpA 公司 IT 安全管理部门的前雇员、目前在监狱中的 Arturo D'Elia 和 Leonardo 的 CERT（网络紧急准备小组）负责人安东尼奥·罗西（Antonio Rossi）。列奥纳多是一家国有跨国公司，也是世界上最大的国防承包商之一。意大利警方发布的新闻稿称，这两人对莱昂纳多 SpA 航空结构部门和飞机部门的 IT 结构进行了严重攻击。

详情

Police arrest two people over stealing sensitive data from defense giant
https://securityaffairs.co/wordpress/111965/cyber-crime/leonardo-data-theft.html

美国联邦调查局和国土安全部警告称，美国智库将受到攻击

日期: 2020-12-02

等级: 中

来源: Sergiu Gatlan

标签: ['FBI', 'U.S.', 'DHS-CISA', 'Think Tanks', 'APT']

美国联邦调查局（FBI）和国土安全局（DHS-CISA）在 2020 年 12 月 1 日晚间发表的一份联合咨询报告中警告说，有国家支持的黑客组织将矛头指向美国智库组织。 根据这两个联邦机构的说法，高级持续威胁（APT）攻击者经常将攻击指向此类组织和个人，这些组织和个人在塑造美国政策和国际事务中可以发挥重要作用。 FBI 和 DHS-CISA 还提供了一套的缓解措施，由智库组织的领导人、工作人员和 IT 人员立即实施，以加强他们的安全态势，抵御国家黑客组织正在进行的攻击。

详情

FBI and Homeland Security warn of APT attacks on US think tanks
https://www.bleepingcomputer.com/news/security/fbi-and-homeland-security-warn-of-apt-attacks-on-us-think-tanks/

HMRC 钓鱼攻击滥用邮件服务，绕过垃圾邮件过滤器

日期: 2020-12-02

等级: 中

来源: Ax Sharma

标签: ['SendGrid', 'HMRC Phishing', 'Mailing Service', 'Bypass Spam Filters']

攻击者正在利用合法的 SendGrid 邮件服务发送 HMRC 网络钓鱼电子邮件，以欺骗绕过垃圾邮件过滤器。 这个公开的漏洞已经多次被攻击者利用来逃避电子邮件安全产品的检测，但是还没有找到具体的修复方案。 SendGrid 是一家电子邮件传递公司，提供用于发送新闻通讯，促销电子邮件和运营业务电子邮件（例如运输通知）的基础结构。

详情

HMRC phishing scam abuses mail service to bypass spam filters
https://www.bleepingcomputer.com/news/security/hmrc-phishing-scam-abuses-mail-service-to-bypass-spam-filters/

针对全球大学的网络钓鱼活动

日期: 2020-12-04

等级: 中

来源: Prajeet Nair

标签: ['Shadow Academy', 'Universities', 'Phishing']

据 RiskIQ 的研究人员称，2020 年一个黑客组织针对全球 20 所大学和学校进行了一系列旨在窃取证书的网络钓鱼攻击。据报道，这些网络钓鱼邮件使用了各种各样的主题作为诱饵，其中包括可能来自学校图书馆、学生门户网站或经济援助部门的信息。这些信息包含一个指向黑客创建的恶意链接。

详情

Phishing Campaign Targeted Universities Worldwide

https://www.databreachtoday.com/phishing-campaign-targeted-universities-worldwide-a-15518

MetaMask 网络钓鱼通过 Google 广告窃取加密货币钱包

日期: 2020-12-04

等级: 中

来源: Ionut Ilascu

标签: ['Google', 'MetaMask']

`MetaMask`加密货币钱包的用户一直在遭受网络钓鱼诈骗的损失，该诈骗通过谷歌搜索广告吸引潜在受害者。MetaMask 拥有超过 100 万用户的社区。该网站通过浏览器扩展在浏览器中提供以太坊加密货币钱包，允许分布式应用程序从区块链读取数据。2020 年 12 月开始 MetaMask 收到大量的投诉，所有的投诉都描述了同一个场景：在尝试安装 MetaMask 浏览器扩展之后，钱都没了。MetaMask 向其社区发出了该骗局的警报，并建议使用与合法网站的直接链接元掩码.io 网址和远离赞助广告

详情

MetaMask phishing steals cryptocurrency wallets via Google ads

https://www.bleepingcomputer.com/news/security/metamask-phishing-steals-cryptocurrency-wallets-via-google-ads/

网络雇佣兵组织 DeathStalker 使用了一个新的后门

日期: 2020-12-05

等级: 中

来源: Pierluigi Paganini

标签: ['DeathStalker', 'PowerShell', 'PowerPepper', 'Cyber Mercenaries Group']

网络雇佣兵组织`DeathStalker`在最近的攻击中使用了一个新的 PowerShell 后门。卡巴斯基的专家发现了一个以前不为人所知的后门，被称为 PowerPepper，该组织从 7 月中旬开始在攻击中使用。"PowerPepper 是一个 Windows 内存 PowerShell 后门程序，可以执行远程发送的 shell 命令。"DeathStacker 是卡巴斯基发现的一个黑客雇佣组织，自 2012 年以来，它一直针对全世界的组织，主要是律师事务所和金融实体。

详情

Cyber mercenaries group DeathStalker uses a new backdoor

https://securityaffairs.co/wordpress/111945/hacking/deathstalker-powerpepper-backdoor.html

医疗机构 Johnson & Johnson 遭受的网络攻击上升了 30%

日期: 2020-12-05

等级: 中

来源: Pierluigi Paganini

标签: ['Healthcare', 'Johnson & Johnson', 'COVID-19']

医疗保健机构`强生公司`观察到，在 COVID-19 流感大流行期间，由国家资助的黑客发动的网络攻击激增。据《华尔街日报》报道，“北韩黑客袭击了美国、英国和韩国的至少六家从事 COVID-19 治疗的制药公司”。这些公司包括强生公司（Johnson&Johnson）和总部位于马里兰州的诺瓦克斯公司（Novax Inc.），这两家公司都在研发实验性疫苗

详情

COVID-19 – Johnson & Johnson saw a 30% uptick in cyber-attacks

https://securityaffairs.co/wordpress/111960/hacking/covid-19-johnson-johnson-cyber-attacks.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. 若系统设有初始口令，建议使用强口令，并且在登陆后要求修改。
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. 登陆入口增加验证码功能。
6. 减少外网资源和不相关的业务，降低被攻击的风险
7. 注重内部员工安全培训
8. 移动端不安装未知应用程序、不下载未知文件
9. 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
10. 不盲目安装未知的浏览器扩展

(四) 其他事件

Talos 报告了 WebKit 的远程代码执行漏洞

日期: 2020-12-01

等级: 高

来源: Pierluigi Paganini

标签: ['Talos', 'WebKit', 'Browser Engine', 'Apple', 'Cisco', 'Vulnerability', 'RCE']

思科的 Talos 团队发现了 WebKit 浏览器引擎中的安全漏洞，这些漏洞的严重性很高，其中包括可以由远程攻击者利用的安全漏洞，通过诱使用户访问恶意网站来实现代码执行。WebKit 是由 Apple 开发的浏览器引擎，主要用于其 Safari Web 浏览器以及所有 iOS Web

浏览器。 BlackBerry Browser、PlayStation 控制台、Tizen 移动操作系统以及 Amazon Kindle 电子书阅读器随附的浏览器都使用的 WebKit。

详情

Talos reported WebKit flaws in WebKit that allow Remote Code Execution
https://securityaffairs.co/wordpress/111698/hacking/webkit-browser-engine-flaws.html

扫描 400 万个 Docker images 后发现：51%存在严重漏洞

日期: 2020-12-03

等级: 高

来源: Pierluigi Paganini

标签: ['Docker Hub', 'Docker images', 'Vulnerability', 'Dependencies']

容器安全公司 Prevasio 分析了 Docker Hub 上托管的 400 万个公共 Docker 容器的 images，发现其中大多数具有严重漏洞。 在 400 万个 Docker images 中，有 51%包含具有至少一个严重漏洞的程序包或应用程序依赖项，而 13%的 images 具有严重级别的漏洞。 动态分析还揭示了 6,432 个恶意或潜在有害的容器 images，占 Docker Hub 所有公开可用 images 的 0.16%。

详情

A scan of 4 Million Docker images reveals 51% have critical flaws
https://securityaffairs.co/wordpress/111833/hacking/docker-hub-scan-analysis.html

Hacker_R_US 因炸弹威胁和 DDoS 勒索而入狱八年

日期: 2020-12-01

等级: 高

来源: Catalin Cimpanu

标签: ['DDoS', 'Apophis Squad', 'Hacker_R_US', 'Timothy Dalton Vaughn', 'Prison']

美国一名法官判处一名 22 岁的黑客 8 年监禁，罪名是参与 DDoS 勒索计划，对世界各地的公司和学校制造假炸弹威胁，以及拥有儿童色情材料。 黑客被确定为北卡罗来纳州温斯顿·塞勒姆（Winston-Salem）居民蒂莫西·道尔顿·沃恩（Timothy Dalton Vaughn），该黑客于 2019 年 2 月被捕，于同年 11 月认罪，2020 年 11 月 30 日被判处 95 个月监禁，此前他因 COVID-19 而推迟量刑。 沃恩以" Hacker_R_US"和" WantedbyFeds"的身份上网，是黑客组织 Apophis Squad 的成员，该组织在 2018 年前八个月引起轰动，然后在执法镇压后逐渐消失。

详情

'Hacker_R_US' gets eight years in prison for bomb threats and DDoS extortion
https://www.zdnet.com/article/hacker-r-us-gets-eight-years-in-prison-for-bomb-threats-and-ddos-extortion/

OpenClinic 程序存在共享电子病历漏洞

日期: 2020-12-01

等级: 高

来源: Tara Seals

标签: ['OpenClinic', 'XSS', 'Management Software', 'Path Traversal']

`OpenClinic` 应用程序中发现了四个用于共享电子病历的漏洞。 其中最令人担忧的是，允许未经身份验证的远程攻击者从应用程序读取患者的个人健康信息（PHI）。 OpenClinic 是开源的健康记录管理软件； Bishop Fox 的研究人员称，其最新版本是 2016 年发布的 0.8.2，因此这些漏洞仍未得到修复。 根据研究人员的说法，这些漏洞涉及缺少身份验证、 文件上传不安全、跨站点脚本（XSS）和路径遍历。 严重性最高的漏洞（CVE-2020-28937）缺少对医学检验信息请求的身份验证检查。

详情

Electronic Medical Records Cracked Open by OpenClinic Bugs
https://threatpost.com/electronic-medical-records-openclinic-bugs/161722/

谷歌白帽详解零点击蠕虫 Wi-Fi 漏洞

日期: 2020-12-01

等级: 高

来源: The Hacker News

标签: ['Google', 'iOS', 'Apple', 'iPhone', 'Wormable', 'Wi-Fi', 'Vulnerability']

谷歌 Project Zero 的白帽黑客伊恩·比尔（Ian Beer）2020 年 12 月 1 日披露了一个现已修补的严重"可蠕虫" iOS 漏洞的详细信息，该漏洞可能使远程攻击者可以通过 Wi-Fi 完全控制附近的任何设备。 贝尔在一篇冗长的博客文章中详细介绍了这个漏洞，他表示利用此漏洞，可查看所有照片，阅读所有电子邮件，复制所有私人消息并实时监视设备上发生的一切。

详情

Google Hacker Details Zero-Click 'Wormable' Wi-Fi Exploit to Hack iPhones
https://thehackernews.com/2020/12/google-hacker-details-zero-click.html

TIM 红队研究（RTR）的专家发现 6 个 0day 漏洞

日期: 2020-11-30

等级: 中

来源: Pierluigi Paganini

标签: ['TIM's Red Team', 'Massimiliano Brolli', 'Vulnerability', 'StruxureWare', 'Schneider Electric']

2020 年 11 月 30 日，由 Massimiliano Brolli 领导的 TIM 红队研究发现了施耐德电气的 StruxureWare 产品中的 6 个新漏洞。 施耐德电气已在 2020 年 4 月至 2020 年 11 月之间修复了这些漏洞。 施耐德电气是专门从事能源和自动化产品（如 ICS，SCADA 和 IoT 产品）的供应商。 StruxureWare 是与物理设备集成的软件，用于对能源，照明，消防安全和 HVAC 进行集成监视，控制和管理。

详情

Exclusive: Experts from TIM's Red Team Research (RTR) found 6 zero-days
https://securityaffairs.co/wordpress/111692/hacking/schneider-electric-zero-days.html

Gootkit 恶意软件与 REvil 勒索软件同时活跃

日期: 2020-11-30

等级: 中

来源: Lawrence Abrams

标签: ['Gootkit', 'Trojan', 'REvil', 'Germany', 'Ransomware']

时隔一年，Gootkit 信息窃取特洛伊木马又重新活跃起来，与 REvil 勒索软件一起发起了针对德国的新活动。 Gootkit 木马是一种基于 javascript 的恶意软件，它会产生各种恶意行为，包括键盘记录、录制视频、窃取电子邮件、密码，以及注入恶意脚本以窃取网上银行凭证。 2019 年，Gootkit 攻击者将 MongoDB 数据库暴露在互联网上，其后 MongoDB 数据库遭受了数据泄漏。 这次破坏之后，人们以为 Gootkit 已经关闭了他们的行动，直到其在 2020 年 11 月初又突然活跃。

详情

Gootkit malware returns to life alongside REvil ransomware

https://www.bleepingcomputer.com/news/security/gootkit-malware-returns-to-life-alongside-revil-ransomware/

微软删除了 18 个恶意 Edge 扩展

日期: 2020-12-01

等级: 中

来源: Catalin Cimpanu

标签: ['Microsoft', 'Ads Injection', 'Edge', 'Malicious Edge Extensions']

微软已经从 Edge Add-ons 门户网站上删除了 18 个 Edge 浏览器扩展，因为这些扩展被发现在用户的 web 搜索结果页面中插入广告。 在 Microsoft 通过 Reddit 收到用户的多次投诉后，这些扩展在 11 月 20 日至 11 月 25 日期间被删除。 即使用户基数很小，Edge 已经激起了网络犯罪集团的兴趣，这些犯罪团伙在过去十年里一直在 Chrome 和 Firefox 的扩展商店中充斥着恶意插件。随着浏览器的使用量持续增长，这些类型的事件预计将变得更加常见。

详情

Microsoft removes 18 malicious Edge extensions for injecting ads into web pages

https://www.zdnet.com/article/microsoft-removes-18-malicious-edge-extensions-for-injecting-ads-into-web-pages/

最大的网络色情犯罪团伙“Nth Room”头目被判入狱 40 年

日期: 2020-12-02

等级: 中

来源: Waqas

标签: ['Cho Ju-Bin', 'Nth Room', 'Sextortion', 'Jailed']

韩国的 Cho Ju-bin 被指控强迫至少 74 名女性，包括 16 名未成年人，在 Nth Room 制作和销售露骨的色情内容。 25 岁的 Nth Room 头目 Cho Ju-bin 被判入狱 40 年，而不是无期徒刑。 据报道，Nth Room 是韩国迄今发现的最大的性交易网络之一。Cho Ju-bin 是网上性虐待网络的主谋。

详情

Leader of biggest online sextortion ring 'Nth Room' jailed for 40 years
https://www.hackread.com/nth-room-online-sex-trafficking-ringleader-jailed/

施乐 DocuShare 漏洞导致数据泄漏

日期: 2020-12-02

等级: 中

来源: Tom Spring

标签: ['Xerox', 'DocuShare', 'Vulnerability', 'Sensitive Data']

施乐发布了针对两个漏洞的修复程序，这些漏洞影响了其市场领先的 DocuShare 企业文档管理平台。 这些漏洞如果被利用，可能会使 DocuShare 用户遭受攻击，从而导致敏感数据丢失。 网络安全与基础设施安全局（CISA）2020 年 12 月 2 日发布了安全公告，敦促用户和管理员应用补丁，以修补 Xerox DocuShare 的最新发行版本（6.6.1、7.0 和 7.5）中的两个严重安全漏洞。

详情

Xerox DocuShare Bugs Allows Data Leaks
https://threatpost.com/xerox-docushare-bugs/161791/

IOS 中的漏洞可以让攻击者在 WIFI 覆盖范围内控制苹果手机

日期: 2020-12-03

等级: 中

来源: Liam Tung

标签: ['Google', 'iPhone', 'iOS', 'Apple', 'Wi-Fi', 'Vulnerability']

负责 iPhone 安全的谷歌 Project Zero (GPZ)漏洞研究者近日透露，iOS 系统中存在一个漏洞，可以让攻击者在 Wi-Fi 覆盖的范围内完全控制苹果手机。 GPZ 是谷歌的一个安全研究小组，其任务是发现所有流行软件的漏洞，包括微软的 Windows 10、谷歌 Chrome 和 Android，以及苹果的 iOS 和 macOS。 专门研究 iOS 黑客的 GPZ 黑客 Ian Beer 说，他在 2020 年新冠疫情期间发现的漏洞，允许 Wi-Fi 范围内的攻击者查看所有 iPhone 的照片和电子邮件，并复制 Messages 中的所有私人消息。

详情

Google researcher: I made this 'magic' iPhone Wi-Fi hack in my bedroom, imagine what others could do
https://www.zdnet.com/article/google-researcher-i-made-this-magic-iphone-wi-fi-hack-in-my-bedroom-imagine-what-others-could-do/

VMware 修复了 NSA 报告的 0day 漏洞

日期: 2020-12-04

等级: 中

来源: Sergiu Gatlan

标签: ['VMware', 'Security Updates', 'CVE-2020-4006', 'Vulnerability', 'Command Injection']

VMware 发布了安全更新，以解决 VMware Workspace One Access、Access Connector、Identity Manager 和 Identity Manager Connector 中的 0day 漏洞。 该漏洞

是一个命令注入漏洞，被追踪为 CVE-2020-4006，于 2020 年 11 月 20 日公开披露。 如果成功利用此漏洞，攻击者可以升级权限并在主机 Linux 和 Windows 操作系统上执行命令。

详情

VMware fixes zero-day vulnerability reported by the NSA

https://www.bleepingcomputer.com/news/security/vmware-fixes-zero-day-vulnerability-reported-by-the-nsa/

Google Play 源代码漏洞使应用程序易受攻击

日期: 2020-12-05

等级: 中

来源: Akshaya Asokan

标签: ['Play Core Library', 'Google Play', 'CVE-2020-8913']

Google Play store 平台中的一个源代码漏洞可能使攻击者能够执行远程代码，从而在应用程序上盗用凭证。该漏洞被追踪为 CVE-2020-8913，是 Android Play Core 库中的一个代码执行漏洞，该库允许从应用程序内部与 Google Play 服务进行交互。研究人员指出，攻击者可以利用该漏洞注入恶意代码，这将使攻击者能够窃取银行凭证、窃取双重身份验证码、监视受害者并从即时消息应用程序中窃取消息。

详情

Google Play Source Code Flaw Makes Apps Vulnerable

https://www.databreachtoday.com/google-play-source-code-flaw-makes-apps-vulnerable-a-15526

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