安全事件周报

安全事件周报 (01.11-01.17)

360CERT
北京奇虎科技有限公司 | 2021-01-18

报告信息

报告名称	安全事件周报（01.11-01.17）		
报告类型	安全事件周报	报告编号	B6-2021-011801
报告版本	1.0	报告日期	2021-01-18
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	2021-01-18	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 37 项

话题集中在`恶意程序`、`漏洞修复`方面，涉及的组织有：`联合国`、`西门子`、`Microsoft`、`Adobe`等。蠕虫病毒突袭，员工安全意识建设不可或缺。

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**
Sunburst 后门与俄罗斯 APT 恶意软件共享功能	★★★★★
在 SolarWinds 供应链攻击中发现的第三种恶意软件	★★★★★
Incaseformat 蠕虫病毒威胁	★★★★★
用来攻击 Qui Cellmate 用户的恶意软件源代码被泄露	★★★★
地下论坛出售的恶意软件称可以完全控制 Android 手机	★★★★
Facebook 起诉恶意 Chrome 扩展的制造商恶意窃取数据	★★★★
利用 Telegram 机器人的新型诈骗	★★★★
Windows Finger 命令被网络钓鱼滥用以下载恶意软件	★★★★
勒索软件攻击了苏格兰环境保护局	★★★★
数据安全	**等级**
联合国泄露了超过 10 万个环境规划署的工作人员记录	★★★★★
数据管理公司泄漏了数百万个人资料	★★★★★
Capcom：39 万人可能受到勒索软件数据泄露的影响	★★★★★
暗网 Juspay 泄漏 3500 万客户卡数据	★★★★★
新西兰储备银行的数据被黑客窃取	★★★★
Ubiquiti 公司披露数据泄露	★★★★
黑客泄露了被盗的辉瑞 COVID-19 疫苗数据	★★★★
网络攻击	**等级**
水坑行动利用了 0day 漏洞	★★★★★
Spalax：针对哥伦比亚实体的持续恶意软件活动	★★★★★
Mimecast 表示，黑客滥用其证书来访问 Microsoft 账户	★★★★
网络钓鱼中常见的假冒品牌	★★★★

基于电报的网络钓鱼服务 Classiscam 登陆欧洲市场	★★★★
其他事件	**等级**
全球最大的暗网非法市场被关闭	★★★★★
安全公司 Bitdefender 发布了 Darkside 勒索软件的免费解密器	★★★★
Typeform 修复了 Zendesk Sell 应用的数据劫持漏洞	★★★★
微软 2021 年 1 月补丁日修复了 83 个漏洞，包括 1 个 0day 漏洞	★★★★
Adobe 在安全更新中修复了 7 个严重漏洞	★★★★
在 CMX 软件中发现了严重的 Cisco 漏洞	★★★★
认证的推特账户在"Elon Musk"加密骗局中被黑，涉案金额达 58 万美元	★★★★
未公开的 Apache Velocity XSS 漏洞影响政府网站	★★★★
西门子修复数字工业软件产品中的多个漏洞	★★★★
最大的贩卡市场 Joker's Stash 宣布关闭	★★★★
Orbit Fox WordPress 插件中的漏洞允许攻击者接管站点	★★★★
未经授权的 RAC 员工非法入侵计算机系统并将数据出售	★★★
俄罗斯黑客因黑客攻击被判刑十二年	★★★
Microsoft Sysmon 现在可以检测恶意软件进程篡改的操作	★★★
新的克隆技术以绕过以 Google 的 2FA 密钥	★★★
研究人员在 F5 BIG-IP 系统中发现了一个 DoS 漏洞	★★★

三、 事件详情

(一) 恶意程序

Sunburst 后门与俄罗斯 APT 恶意软件共享功能

日期: 2021-01-11

等级: 高

来源: Sergiu Gatlan

标签: ['Kaspersky', 'Sunburst', 'SolarWinds', 'Kazuar', 'Russian']

卡巴斯基研究人员发现，`Sunburst`后门程序（在`SolarWinds`供应链攻击期间部署的恶意软件）显示出与`Kazuar`的功能重叠，`Kazuar`是暂时与俄罗斯`Turla`黑客组织联系在一起的`.NET`后门程序。
`Turla`（又名`VENOMOUS BEAR`和`Waterbug`）早在 1996 年就一直在协调信息盗窃和间谍活动，并且是针对五角大楼和`NASA`、美国中央司令部和芬兰外交部的袭击的主要嫌疑犯。
`Kazuar`是`Turla`过去的运营中使用的工具之一，据卡巴斯基称，`Kazuar`与`SolarWinds`黑客背后的组织（`UNC2452`和`DarkHalo`）创建的恶意软件共享一些功能。

详情

Sunburst backdoor shares features with Russian APT malware

https://www.bleepingcomputer.com/news/security/sunburst-backdoor-shares-features-with-russian-apt-malware/

在 SolarWinds 供应链攻击中发现的第三种恶意软件

日期: 2021-01-12

等级: 高

来源: Catalin Cimpanu

标签: ['CrowdStrike', 'SolarWinds', 'Malware', 'Supply Chain Attack', 'Sunspot']

网络安全公司`CrowdStrike`是直接调查`SolarWinds`供应链攻击的公司之一，该公司 2021 年 1 月 12 日表示，它已经发现了与此次黑客攻击直接相关的第三种恶意软件。
该恶意软件命名为`Sunspot`，为先前发现的`Sunburst`（`Solorigate`）和`Teardrop`恶意软件增色不少。
但`Crowdstrike`表示，该恶意软件实际上是第一个被使用的恶意软件。
在 2021 年 1 月 12 日发布的一份报告中，`Crowdstrike`说`Sunspot`于 2019 年 9 月部署，当时黑客首次破坏了`SolarWinds`的内部网络。

详情

Third malware strain discovered in SolarWinds supply chain attack

https://www.zdnet.com/article/third-malware-strain-discovered-in-solarwinds-supply-chain-attack/

Incaseformat 蠕虫病毒威胁

日期: 2021-01-13

等级: 高

来源: 360CERT

标签: ['Incaseformat', 'Worm']

360 检测到蠕虫病毒 incaseformat 大范围爆发，病毒感染用户机器后会通过 U 盘自我复制感染到其他电脑，导致电脑中磁盘文件被删除，给用户造成极大损失。用户电脑中毒后，病毒文件通过 DeleteFileA 和 RemoveDirectory 代码实施了删除文件和目录的行为。此病毒启动后将自身复制到 C:WINDOWS say.exe 并创建启动项退出，等待重启运行，下次开机启动后约 20s 就开始删除用户文件。360 安全卫士已支持对该病毒的查杀用户可以通过安装 360 安全卫士或通过软件管家下载 incaseformat 专杀工具。

详情

Incaseformat 蠕虫病毒威胁

https://cert.360.cn/warning/detail?id=39a713a8612444993801f654e5ed9ed8

用来攻击 Qui Cellmate 用户的恶意软件源代码被泄露

日期: 2021-01-11

等级: 高

来源: Pierluigi Paganini

标签: ['Qiui Cellmate', 'ChastityLock', 'Source Code', 'Malware', 'Leaked']

用来攻击`Qiui Cellmate`成人玩具用户的`ChastityLock`勒索软件的源代码现在已经公开。
勒索软件代码的泄露最早是由用户`@vx-underground`在推特上披露的。
2020 年 10 月，Pen Test Partners 的研究人员发布了一份报告，其中提供了有关影响他们的安全漏洞的详细信息，而 Qiui Cellmate 成为头条新闻。
攻击者威胁称，如果受害者不支付赎金，就会无限期锁定设备。

详情

Source code for malware that targets Qiui Cellmate device was leaked online

https://securityaffairs.co/wordpress/113251/hacking/qiui-cellmate-ransomware.html

地下论坛出售的恶意软件称可以完全控制 Android 手机

日期: 2021-01-12

等级: 高

来源: Danny Palmer

标签: ['Android', 'Underground Forums', 'Remote Administration Tool', 'Malware']

地下论坛上正在出售一种由两种旧恶意软件新组成的恶意软件，让黑客可以访问用户在 Android 手机上的所有操作，价格低至`29.99`美元，即使是低级别的网络犯罪分子也能窃取敏感的个人数据。
这种远程木马通过键盘记录感染受害者，使攻击者能够轻松监控网站和应用程序的使用情况，从而窃取用户名和密码以及财务数据。
恶意软件的低成本反映了犯罪生态系统的日益复杂，这使得那些技术水平有限的想要成为罪犯的人有可能获得工具来发动攻击。

详情

This Android malware claims to give hackers full control of your smartphone
https://www.zdnet.com/article/this-android-malware-claims-to-give-hackers-full-control-of-your-smartphone/

Facebook 起诉恶意 Chrome 扩展的制造商恶意窃取数据

日期: 2021-01-14

等级: 高

来源: Sergiu Gatlan

标签: ['Facebook', 'Chrome Web Store', 'Scraping Data', 'Malicious Chrome Extensions']

`Facebook`已经针对恶意 Chrome 扩展程序的制造商采取了法律行动，这些扩展未经授权从 `Facebook` 网站和用户系统中窃取用户资料和其他信息。
两名被告通过 Chrome 网上应用店分发了恶意浏览器扩展程序，这些扩展程序以`Oink and Stuff`公司为名。
所有这四个扩展程序仍可在 Google 的 Chrome 网上应用店中下载，并且已有 54,000 多名用户安装了这些扩展程序。

详情

Facebook sues makers of malicious Chrome extensions for scraping data
https://www.bleepingcomputer.com/news/security/facebook-sues-makers-of-malicious-chrome-extensions-for-scraping-data/

利用 Telegram 机器人的新型诈骗

日期: 2021-01-14

等级: 高

来源: Lindsey O'Donnell

标签: ['Telegram Bot', 'European', 'Scam-as-a-Service', 'Classiscam']

一种新型自动欺诈技术出现，该技术利用`Telegram`机器人从欧洲受害者那里窃取钱财和付款数据。
该骗局被研究人员称为`Classiscam`，目前网络犯罪分子作为一项服务出售，并已被至少 40 个独立的网络帮派使用。
截止 2020 年，网络犯罪分子使用该服务的总收入至少为 650 万美元。

详情

Telegram Bots at Heart of Classiscam Scam-as-a-Service
https://threatpost.com/telegram-bots-classiscam-scam/163061/

Windows Finger 命令被网络钓鱼滥用以下载恶意软件

日期: 2021-01-15

等级: 高

来源: Lawrence Abrams

标签: ['Finger Command', 'Windows', 'Backdoor', 'Malware', 'MineBridge']

攻击者使用通常无害的 `Windows Finger` 命令在受害者的设备上下载并安装恶意后门。
`Finger`命令是源自 Linux/Unix 操作系统的实用程序，它允许本地用户检索远程计算机上的

用户列表或有关特定远程用户的信息。
除`Linux`外，`Windows`还包含执行相同功能的`finger.exe`命令。

详情

Windows Finger command abused by phishing to download malware

https://www.bleepingcomputer.com/news/security/windows-finger-command-abused-by-phishing-to-download-malware/

勒索软件攻击了苏格兰环境保护局

日期: 2021-01-15

等级: 高

来源: Mathew J. Schwartz

标签: ['Scottish', 'Ransomware', 'Environment Protection Agency', 'Conti']

苏格兰环境保护局说，2020 年 12 月的勒索软件攻击造成了严重的网络中断，并且攻击者还偷走了一些数据。
SEPA 是苏格兰政府的主要环境监管机构，负责保护国家环境。
这个非部门的公共机构，由大约 1,200 名员工组成。
该组织表示，他们仍在处理勒索软件攻击，该攻击继续破坏服务，因为攻击者要求该组织支付赎金，以换取解锁其系统密钥的保证，并承诺停止在线泄露被盗信息。

详情

Ransomware Disrupts Scottish Environment Protection Agency

https://www.databreachtoday.com/ransomware-disrupts-scottish-environment-protection-agency-a-15768

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. 条件允许的情况下，设置主机访问白名单
3. 如果不慎勒索中招，务必及时隔离受害主机、封禁外链 ip 域名并及时联系应急人员处理
4. 各主机安装 EDR 产品，及时检测威胁
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. 注重内部员工安全培训

(二) 数据安全

联合国泄露了超过 10 万个环境规划署的工作人员记录

日期: 2021-01-11

等级: 高

来源: Ax Sharma

标签: ['UNEP', 'Data Breach', 'Vulnerability', 'Git Repositories']

2021 年 1 月 11 日，研究人员揭露了一个安全漏洞，利用该漏洞可以访问联合国环境规划署(UNEP)超过 10 万名私人雇员的信息记录。
数据泄露源于公开的 Git 目录和凭据，这使研究人员可以克隆 Git 存储库并收集与 10 万多名员工相关的大量个人身份信息（PII）。
泄漏的数据暴露了联合国工作人员的旅行历史，包含：雇员 ID，姓名，雇员组，旅行理由，开始和结束日期，批准状态，目的地和停留时间。

详情

United Nations data breach exposed over 100k UNEP staff records

https://www.bleepingcomputer.com/news/security/united-nations-data-breach-exposed-over-100k-unep-staff-records/

数据管理公司泄漏了数百万个人资料

日期: 2021-01-11

等级: 高

来源: Tara Seals

标签: ['SocialArks', 'Facebook', 'Instagram', 'LinkedIn', 'Safety Detectives', 'Elasticsearch', 'Personally Identifiable Information']

2.14 亿社交媒体用户的超过 400GB 的公开和私人资料数据已经暴露于互联网上。
据安全侦探（Safety Detectives）的研究人员称，此次泄密源于中国社交媒体管理公司`SocialArks`的一个配置错误的`ElasticSearch`数据库，该数据库包含来自`Facebook`，`Instagram`，`LinkedIn`和其他平台的用户的个人身份信息。

详情

Millions of Social Profiles Leaked by Chinese Data-Scrapers

https://threatpost.com/social-profiles-leaked-chinese-data-scrapers/162936/

Capcom：39 万人可能受到勒索软件数据泄露的影响

日期: 2021-01-12

等级: 高

来源: Lawrence Abrams

标签: ['Capcom', 'Ragnar Locker', 'Data Breach', 'Ransomware', 'Cyberattack']

Capcom 发布了一份最新的数据泄露调查报告，并表示去年 11 月份的勒索软件攻击可能会影响多达 39 万人。
2020 年 11 月 2 日，`Capcom`遭到`Ragnar Locker`勒索软件运营商的网络攻击，勒索软件运营商声称他们从公司窃取了 1TB 数据。
勒索软件运营商要求 1100 万美元的比特币赎金。
Capcom 表示，他们已经确认有 16415 人的个人信息被曝光，可能受影响的总人数为 39 万人。

详情

Capcom: 390,000 people may be affected by ransomware data breach

https://www.bleepingcomputer.com/news/security/capcom-390-000-people-may-be-affected-by-ransomware-data-breach/

暗网 Juspay 泄漏 3500 万客户卡数据

日期: 2021-01-13

等级: 高

来源: Waqas

标签: ['Juspay', 'Data Sold', 'Dark Web', 'Card']

`Juspay`大约五个月前就遭受数据泄露，现在的调查显示，大约有 3500 万`Juspay`客户受到了影响。
值得注意的是，`Juspay`属于`Hackread.com`在 2021 年 1 月 2 日报告的数据泄露报告的 26 家公司之一。
目前，黑客正在出售 3.65 亿条用户记录，其中包括`Juspay`。被泄露的数据包括公司存储支付数据的客户的姓名、银行名称和手机号码。

详情

Juspay data breach 35 million customers' card data sold on dark web

https://www.hackread.com/juspay-data-breach-card-data-sold-dark-web/

新西兰储备银行的数据被黑客窃取

日期: 2021-01-11

等级: 高

来源: Lawrence Abrams

标签: ['The Reserve Bank', 'New Zealand', 'Data Breach']

新西兰储备银行`Te Pūtea Matua`在攻击者入侵第三方托管合作伙伴后，遭受数据泄露。
储备银行是新西兰的中央银行，负责制定货币政策以稳定该国的物价。
2021 年 1 月 10 日，储备银行披露，攻击者非法访问了其存储在第三方主机提供商的数据后，他们的数据遭到了泄露。

详情

New Zealand Reserve Bank suffers data breach via hacked storage partner

https://www.bleepingcomputer.com/news/security/new-zealand-reserve-bank-suffers-data-breach-via-hacked-storage-partner/

Ubiquiti 公司披露数据泄露

日期: 2021-01-11

等级: 高

来源: Pierluigi Paganini

标签: ['American', 'Ubiquiti Networks', 'Cloud Provider', 'Database']

美国技术供应商`Ubiquiti Networks`遭受数据泄露，并正在向其客户发送通知电子邮件，要求他们更改密码并为其帐户启用`2FA`策略。
该公司发现一些由第三方云提供商管理的系统在被未经授权地访问，但没有迹象表明用户的帐户存在未经授权的活动。
且还不知道其用户数据是否被公开，这些数据可能包括姓名，电子邮件地址和帐户的单向加密密码。

详情

Ubiquiti discloses a data breach
https://securityaffairs.co/wordpress/113296/data-breach/ubiquiti-discloses-data-breach.html

黑客泄露了被盗的辉瑞 COVID-19 疫苗数据

日期: 2021-01-12

等级: 高

来源: Sergiu Gatlan

标签: ['The European Medicines Agency', 'Pfizer', 'COVID-19', 'Leak', 'Vaccine Data']

欧洲药品管理局(EMA)2021 年 1 月 12 日透露，2020 年 12 月黑客从辉瑞生物科技公司服务器窃取的部分`COVID-19`疫苗数据已经被泄露到了网上。
网络安全情报界的消息人士称，泄露的数据包括电子邮件屏幕截图，`EMA`同行审阅评论，`Word`文档，`PDF`和`PowerPoint`演示文稿。

详情

Hackers leak stolen Pfizer COVID-19 vaccine data online
https://www.bleepingcomputer.com/news/security/hackers-leak-stolen-pfizer-covid-19-vaccine-data-online/

相关安全建议

1. 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
2. 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
3. 及时检查并删除外泄敏感数据
4. 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。
5. 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

(三) 网络攻击

水坑行动利用了 0day 漏洞

日期: 2021-01-13

等级: 高

来源: Akshaya Asokan

标签: ['Google', 'ProjectZero', 'Zero Day', 'Windows', 'Linux']

Google 的 ProjectZero 安全团队发现了 2020 年的一个复杂的水坑行动，该行动使用了四个 0day 漏洞来攻击`Windows`和`Android`移动设备。
攻击已在 2020 年第一季度发现并停止，但 ProjectZero 以及 Google 威胁分析小组直到现在才透露详细信息，因为分析复杂的操作需要花费数月的时间。
据 Google 报道，攻击行动背后的攻击者使用了两个攻击服务器，一个针对`Android`设备，另一个针对`Windows`设备，每个都使用了单独的攻击链。

详情

Watering Hole Operation Leveraged Zero-Day Exploits

https://www.databreachtoday.com/watering-hole-operation-leveraged-zero-day-exploits-a-15757

Spalax：针对哥伦比亚实体的持续恶意软件活动

日期: 2021-01-14

等级: 高

来源: Pierluigi Paganini

标签: ['ESET', 'Operation Spalax', 'Colombian', 'Malware']

来自`ESET`的安全专家揭露了一场名为`Spalax 行动`(Operation Spalax)的针对哥伦比亚政府机构和私人公司的攻击活动。
此次攻击针对政府机构和私人公司，其中大多数在能源和冶金领域。
该运动至少自 2020 年以来一直很活跃，在此次活动中，攻击者利用远程木马监视受害者。

详情

Operation Spalax, an ongoing malware campaign targeting Colombian entities

https://securityaffairs.co/wordpress/113429/hacking/operation-spalax-malware.html

Mimecast 表示，黑客滥用其证书来访问 Microsoft 账户

日期: 2021-01-12

等级: 高

来源: Catalin Cimpanu

标签: ['Mimecast', 'Microsoft 365', 'Cloud', 'Email Management']

`Mimecast`是一家生产云电子邮件管理软件的公司，该公司 2021 年 1 月 12 日披露了一起安全事件，提醒客户一个攻击者获得了该公司的一个数字证书，并利用证书成功进入了一些客户的`Microsoft 365`账户。
这家总部位于伦敦的电子邮件软件公司表示，该公司的几款产品都使用这一证书连接到`Microsoft`的基础设施。
`Mimecast`表示，大约有`10%`的客户使用带有此特定证书的受影响产品。
但是，攻击者仅能访问这些客户的少数`Microsoft 365`帐户。

详情

Mimecast says hackers abused one of its certificates to access Microsoft accounts

https://www.zdnet.com/article/mimecast-says-hackers-abused-one-of-its-certificates-to-access-microsoft-accounts/

网络钓鱼中常见的假冒品牌

日期: 2021-01-14

等级: 高

来源: Danny Palmer

标签: ['Microsoft', 'Phishing', 'Mimicking Brands', 'Office 365']

`Check Point`的网络安全研究人员分析了过去三个月内发送的网络钓鱼邮件，发现 43%的仿冒品牌的网络钓鱼攻击都试图把自己伪装成来自微软的信息。
由于 `Office 365` 在企业中的分布广泛，`Microsoft` 受到了欢迎。
通过窃取这些凭据，网络攻击者试图获得对公司网络的访问权限。

详情

Phishing warning: These are the brands most likely to be impersonated by crooks, so stay alert

https://www.zdnet.com/article/phishing-warning-these-are-the-brands-most-likely-to-be-impersonated-by-crooks-so-stay-alert/

基于电报的网络钓鱼服务 Classiscam 登陆欧洲市场

日期: 2021-01-14

等级: 高

来源: Ionut Ilascu

标签: ['Scam-as-a-service', 'Classiscam']

至少有 40 个网络犯罪团伙正在使用一种`即骗即用（scam-as-a-service）`服务，这种服务依赖于 Telegram 机器人提供模仿流行分类广告、市场和送货服务的页面。2019 年夏天，IB 集团（groupib）的安全研究人员通过该公司在阿姆斯特丹的数字风险保护中首次发现了这一骗局，并将其命名为 Classiscam，并发现它在不到一年的时间内从 280 个诈骗页面增长到大约 3000 个。自发现以来，该计划扩大到后苏联和欧洲国家，如保加利亚，法国，捷克共和国，波兰和罗马尼亚。至少有 40 个组织在实施诈骗，其中最高盈利每月超过 50 万美元。

详情

Telegram-based phishing service Classiscam hits European marketplaces

https://www.bleepingcomputer.com/news/security/telegram-based-phishing-service-classiscam-hits-european-marketplaces/

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. 积极开展外网渗透测试工作，提前发现系统问题
4. 注重内部员工安全培训
5. 如果允许，暂时关闭攻击影响的相关业务，积极对相关系统进行安全维护和更新，将损失降到最小

(四) 其他事件

全球最大的暗网非法市场被关闭

日期: 2021-01-12

等级: 高

来源: Asha Barbaschow

标签: ['Europol', 'DarkMarket', 'Dark Web', 'Monero']

一项国际执法行动关闭了暗网上全球最大的非法市场。
在德国，澳大利亚，丹麦，摩尔多瓦，乌克兰，英国，美国国家犯罪局和美国（包括联邦调查局）的当局共同努力下，拥有近 50 万用户的`DarkMarket`被关闭。
欧洲刑警组织在一份声明中说，市场上有 2400 多个卖家，主要交易毒品并出售伪造的钱，被盗或伪造的信用卡详细信息，匿名 SIM 卡以及恶意软件。
一名澳大利亚公民在德国奥尔登堡市被中央刑事调查局逮捕。据称，这名 34 岁的澳大利亚男子是黑暗市场的经营者。

详情

Australian man arrested for alleged operation of now-shuttered DarkMarket

https://www.zdnet.com/article/australian-man-arrested-for-alleged-operation-of-now-shuttered-darkmarket/

安全公司 Bitdefender 发布了 Darkside 勒索软件的免费解密器

日期: 2021-01-11

等级: 高

来源: Catalin Cimpanu

标签: ['Bitdefender', 'Darkside', 'Ransomware', 'Free Decrypter', 'Tool']

网络安全公司`Bitdefender`2021 年 1 月 11 日发布了一个免费工具，可以帮助`Darkside`勒索软件的受害者免费恢复加密文件，而无需支付赎金。
该工具可从`Bitdefender`网站下载，并附有使用说明，这给那些重要文件被勒索软件锁定和勒索的公司带来了希望。

Darkside 组织自 2020 年夏季开始活跃，至今仍通过网络犯罪论坛上发布的广告开展攻击活动。

详情

Free decrypter released for victims of Darkside ransomware

https://www.zdnet.com/article/free-decrypter-released-for-victims-of-darkside-ransomware/

Typeform 修复了 Zendesk Sell 应用的数据劫持漏洞

日期: 2021-01-11

等级: 高

来源: Ax Sharma

标签: ['Typeform', 'Zendesk Sell', 'Vulnerability', 'Data Hijacking']

在线调查和表单构建软件及服务`Typeform`已修复了一个信息劫持漏洞。
`Typeform`的`Zendesk Sell`应用程序集成中存在的漏洞，可使攻击者将包含敏感数据的表单提交重定向到攻击者身上。
在线调查和表单创建工具 Typeform 允许用户创建网页，以便轻松地从用户收集数据。

详情

Typeform fixes Zendesk Sell form data hijacking vulnerability

https://www.bleepingcomputer.com/news/security/typeform-fixes-zendesk-sell-form-data-hijacking-vulnerability/

微软 2021 年 1 月补丁日修复了 83 个漏洞，包括 1 个 0day 漏洞

日期: 2021-01-12

等级: 高

来源: Lawrence Abrams

标签: ['Microsoft', 'Windows', 'Security Update', 'Microsoft Defender']

2021 年 1 月 12 日是 Microsoft 的 2021 年 1 月补丁日，它是 2021 年的第一个 Microsoft 安全更新版本。
随着 2021 年 1 月补丁日的安全更新发布，`Microsoft`已发布了针对 83 个漏洞的修复程序，其中 10 个漏洞被分类为`严重`，而 73 个漏洞分类为`重要`。
在本次更新中，还有一个 0day 漏洞和一个之前披露的漏洞得到了修复。

详情

Microsoft January 2021 Patch Tuesday fixes 83 flaws, 1 zero-day

https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2021-patch-tuesday-fixes-83-flaws-1-zero-day/

Adobe 在安全更新中修复了 7 个严重漏洞

日期: 2021-01-12

等级: 高

来源: Lindsey O'Donnell

标签: ['Windows', 'macOS', 'Linux', 'Adobe Systems', 'Vulnerability', 'Security Updates']

Adobe Systems 修复了七个严重漏洞，这些漏洞影响`Windows`，`macOS`和`Linux`用户。严重漏洞的影响有任意代码执行和敏感信息泄露等。
微软定期进行安全更新，这将影响到一系列多媒体和创意软件产品，包括 Photoshop、Illustrator 和 Adobe Bridge。

详情

Adobe Fixes 7 Critical Flaws, Blocks Flash Player Content
https://threatpost.com/adobe-critical-flaws-flash-player/162958/

在 CMX 软件中发现了严重的 Cisco 漏洞

日期: 2021-01-13

等级: 高

来源: Lindsey O'Donnell

标签: ['Cisco', 'CMX', 'Wifi', 'Vulnerability', 'CVEs']

Cisco 针对零售商的智能 Wi-Fi 解决方案中存在一个严重性很高的漏洞，该漏洞可能使远程攻击者能够更改受影响系统上任何帐户用户的密码。
该漏洞是 Cisco 在 2021 年 1 月 13 日针对 67 个高严重 CVE 发出的一系列补丁的一部分。其中包括在`Cisco AnyConnect`安全移动客户端以及`Cisco RV110W`，`RV130`，`RV130W`和`RV215W`小型企业路由器中发现的漏洞。

详情

High-Severity Cisco Flaw Found in CMX Software For Retailers
https://threatpost.com/cisco-flaw-cmx-software-retailers/163027/

认证的推特账户在“Elon Musk”加密骗局中被黑，涉案金额达 58 万美元

日期: 2021-01-14

等级: 高

来源: Lawrence Abrams

标签: ['Twitter', 'Elon Musk', 'Crypto Scam', 'Verified Account']

在最近活跃的 `Elon Musk` 加密货币骗局中，攻击者正在入侵经过认证的 Twitter 帐户。
在过去的一周里，安全研究机构 `MalwareHunterTeam`发现，在一起推广另一种假冒 `Elon Musk` 加密货币的骗局中，被黑的 Twitter 认证账户数量有所上升。
这些恶意链接指出，如果您将比特币发送到指定的地址，它们将给您寄回两倍的金额。

详情

Verified Twitter accounts hacked in $580k ‘Elon Musk’ crypto scam
https://www.bleepingcomputer.com/news/security/verified-twitter-accounts-hacked-in-580k-elon-musk-crypto-scam/

未公开的 Apache Velocity XSS 漏洞影响政府网站

日期: 2021-01-15

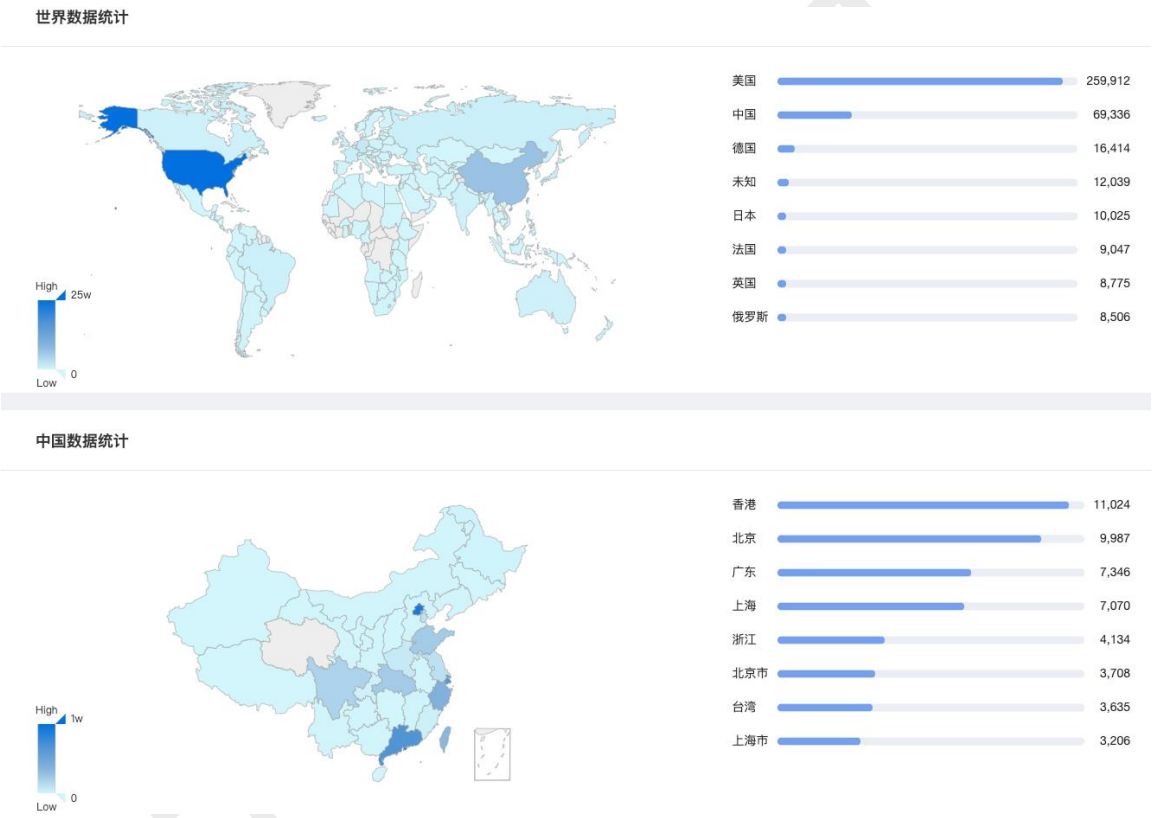
等级: 高

来源: Ax Sharma

标签: ['Apache Velocity', 'NASA', 'GOV', 'XSS', 'Vulnerability']

未经身份验证的攻击者可以利用 `Apache Velocity Tools` 中未公开的跨站点脚本（`XSS`）漏洞来针对政府站点，包括 `NASA`。
`Apache Velocity`是基于`Java`的模板引擎，开发人员可使用其在`Model-View-Controller（MVC）`架构中设计视图。
`Apache Velocity Tools`有一个未公开的 XSS 漏洞，几个月前已在`GitHub`上发布了修复程序，但该漏洞会影响其所有版本，该漏洞编号为`CVE-2020-13959`。

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



详情

Undisclosed Apache Velocity XSS vulnerability impacts GOV sites

https://www.bleepingcomputer.com/news/security/undisclosed-apache-velocity-xss-vulnerability-impacts-gov-sites/

西门子修复数字工业软件产品中的多个漏洞

日期: 2021-01-16

等级: 高

来源: Pierluigi Paganini

标签: ['Siemens', 'Siemens Digital Industries Software', 'JT2Go', 'Teamcenter', 'Solid Edge']

西门子已解决了影响西门子数字工业软件公司（Siemens Digital Industries Software）部分产品的多个漏洞。已解决的漏洞包括类型混淆，对 XML 外部实体的不恰当引用，越界写，基于堆的缓冲区溢出，基于堆栈的缓冲区溢出，不受信任的指针解除引用和越界读取。

下列产品受到西门子解决的漏洞的影响：

- JT2Go：v13.1.0 之前的所有版本
- JT2Go：版本 13.1.0。仅受 CVE-2020-26989，CVE-2020-26990，CVE-2020-26991 的影响
- Teamcenter Visualization：V13.1.0 之前的所有版本
- Teamcenter Visualization：版本 13.1.0 仅受 CVE-2020-26989，CVE-2020-26990，CVE-2020-26991 的影响

西门子还在其 Solid Edge 解决方案中解决了六个漏洞，该漏洞为 3D 设计，仿真和制造提供了软件工具。这些漏洞可能导致任意代码执行和信息泄露。

详情

Siemens fixed tens of flaws in Siemens Digital Industries Software products
https://securityaffairs.co/wordpress/113511/ics-scada/siemens-digital-industries-software-flaws.html

最大的贩卡市场 Joker's Stash 宣布关闭

日期: 2021-01-16

等级: 高

来源: Pierluigi Paganini

标签: ['Joker's Stash', 'COVID-19', 'Carding Site']

最大的在线贩卡市场`Joker's Stash`宣布其业务将于 2021 年 2 月 15 日关闭，管理员通过各种网络犯罪论坛上发布的消息宣布了这一决定。Joker's Stash 是最早的卡片售卖网站之一，它于 2014 年 10 月推出，由于其卡片的新鲜度和有效性，在地下网络犯罪中非常流行。JokerStash 称，他们的员工因新冠病毒感染而住院，大量的成员减少也降低了他们获取新卡数据的能力。卡店关闭的消息是对地下市场的重大打击。

详情

Joker’s Stash, the largest carding site, is shutting down
https://securityaffairs.co/wordpress/113493/cyber-crime/jokers-stash-shut-down.html

Orbit Fox WordPress 插件中的漏洞允许攻击者接管站点

日期: 2021-01-17

等级: 高

来源: Pierluigi Paganini

标签: ['WordPress Plugin', 'Vulnerability', 'Orbit Fox', 'XSS', 'Privilege Escalation']

Wordfence 的安全专家在 Orbit Fox WordPress 插件中发现了两个安全漏洞。
这些漏洞是权限升级漏洞和存储的 XSS 漏洞，漏洞已经影响了 40,000 多次安装。

Orbit Fox 插件允许站点管理员添加注册表格和窗口小部件等功能，目前已有 40 万多个站点安装了该插件。
攻击者可以利用漏洞的将恶意代码注入网站并接管它们。

详情

Critical flaws in Orbit Fox WordPress plugin allows site takeover
https://securityaffairs.co/wordpress/113394/hacking/wordpress-orbit-fox-flaws.html

未经授权的 RAC 员工非法入侵计算机系统并将数据出售

日期: 2021-01-11

等级: 中

来源: Paul Kunert

标签: ['RAC', 'Unauthorised', 'Prison', 'Sell Data']

路边紧急救援公司 RAC 的一名雇员因未经许可入侵计算机系统，并将客户的数据卖给了事故索赔管理公司，而被判处 8 个月监禁。
法庭得知，Kim Doyle33 岁，家住英格兰西北部高惠特利村巷，在没有得到 RAC 的同意的情况下，她还是生成了道路交通事故的数据列表，包括部分姓名、手机号码和登记号码。

详情

Unauthorised RAC staffer harvested customer details then sold them to accident claims management company
https://www.theregister.com/2021/01/11/rac_staffer_unauthorised_computer_access/

俄罗斯黑客因黑客攻击被判刑十二年

日期: 2021-01-11

等级: 中

来源: Pierluigi Paganini

标签: ['U.S.', 'Russian', 'Andrei Tyurin', 'Prison']

2021 年 1 月 11 日，美国一家法院判处 37 岁的`Andrei Tyurin`12 年监禁，罪名是实施了多起针对金融机构、经纪公司、金融新闻出版商和其他美国公司的国际黑客攻击活动。
2018 年 9 月，这名俄罗斯公民被从格鲁吉亚引渡到美国，此人因在摩根大通和道琼斯大规模盗窃客户数据而受到指控。
该名男子应美国当局的要求在佐治亚州被捕，他被控多项共谋罪名，包括电汇欺诈，严重的身份盗窃和四项计算机黑客罪。

详情

Russian hacker Andrei Tyurin sentenced to 12 years in prison
https://securityaffairs.co/wordpress/113279/cyber-crime/russian-hacker-andrei-tyurin-prison.html

Microsoft Sysmon 现在可以检测恶意软件进程篡改的操作

日期: 2021-01-11

等级: 中

来源: Lawrence Abrams

标签: ['Microsoft', 'Sysmon13', 'Process Herpaderping', 'Process Hollowing', 'Security Feature']

`Microsoft`已发布了具有新安全性功能的`Sysmon 13`，它有一个新的安全特性，可以使用`process herpaderping/process hollowing`技术检测进程是否被篡改。
为了逃避安全软件的检测，攻击者将恶意代码注入到合法的`Windows`进程中。
该策略允许恶意软件执行，但是在任务管理器中，它显示为在后台运行的标准 Windows 进程。

详情

Microsoft Sysmon now detects malware process tampering attempts
https://www.bleepingcomputer.com/news/microsoft/microsoft-sysmon-now-detects-malware-process-tampering-attempts/

新的克隆技术以绕过以 Google 的 2FA 密钥

日期: 2021-01-14

等级: 中

来源: Sudais Asif

标签: ['Titan Key', 'Google', '2FA', 'Clone']

2021 年 1 月 14 日，`NinjaLab`的研究人员发明了一种新方法，通过克隆技术绕过谷歌的`Titan` 密钥（一种物理 2FA 密钥）。
该方法要求攻击者首先知道受害者的密码，然后在大约 10 个小时内就能够访问密钥本身。
此外，还需要价值 12000 美元的设备和特殊软件，以使熟练的手段进行攻击。

详情

Cloning Google's Titan Key to bypass 2FA
https://www.hackread.com/cloning-googles-titan-key-to-bypass-2fa/

研究人员在 F5 BIG-IP 系统中发现了一个 DoS 漏洞

日期: 2021-01-14

等级: 中

来源: Pierluigi Paganini

标签: ['DoS', 'CVE-2020-27716', 'F5 BIG-IP', 'Vulnerability']

一位安全研究员在 F5 BIG-IP 中发现了一个 DoS 漏洞，该漏洞为 `CVE-2020-27716`，它会影响某些版本的访问策略管理器（APM）。
F5 BIG-IP 访问策略管理器是一种安全，灵活，高性能的访问管理代理解决方案，可为您的用户，设备，应用程序和应用程序编程接口（API）提供统一的全局访问控制。
该漏洞位于流量管理微内核（TMM）组件中，该组件处理 BIG-IP 设备上的所有负载平衡的流量。

详情

Expert discovered a DoS vulnerability in F5 BIG-IP systems
https://securityaffairs.co/wordpress/113440/security/f5-big-ip-dos.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