安全事件周报

安全事件周报 (10.19-10.25)

360CERT
北京奇虎科技有限公司 | 2020-10-26

报告信息

报告名称	安全事件周报（10.19-10.25）		
报告类型	安全事件周报	报告编号	B6-2020-102601
报告版本	1.0	报告日期	2020-10-26
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	2020-10-26	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 48 项

话题集中在`网络攻击`、`勒索软件`方面，涉及的组织有：`Discord`、`Ubisoft`、`Google`、`QNAP`等。漏洞频发，各大厂商积极推送升级补丁。

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**
GravityRAT：间谍软件	★★★★
勒索软件团伙将部分赎金捐赠给慈善组织	★★★★
Maze 勒索软件	★★★★
新的 Windows RAT 可以通过 Telegram 频道进行控制	★★★★
xmrig 挖矿恶意软件	★★★★
台湾政府 2020 年 4 月遭多起网络攻击	★★★★
新恶意软件使用远程覆盖攻击劫持您的银行帐户	★★★
蒙特利尔的 STM 公共交通系统遭到勒索软件攻击	★★★
LockBit 勒索软件在网络上悄无声息地攻击	★★★
法国 IT 外包商 Sopra Steria 疑遭 Ryuk 勒索软件网络攻击	★★★
Boyne Resorts 滑雪和高尔夫胜地运营商遭到 WastedLocker 勒索软件袭击	★★★
新的 Emotet 攻击使用一个新的 Microsoft Word 模板	★★★
数据安全	**等级**
网络电话服务提供商泄漏了 3.5 亿客户记录	★★★★★
Albion 网络游戏制造商数据被泄露	★★★★
Nefilim 勒索软件团伙公布了 Luxottica 的数据	★★★★
房贷交易平台曝光房贷文件	★★★★
Kleenheat 客户名称和地址因系统漏洞而泄漏	★★★
网络攻击	**等级**
美国国安局：中国黑客常用的 25 大漏洞	★★★★★
Ryuk 勒索软件团伙使用 Zerologon 漏洞进行闪电般的攻击	★★★★
黑客在 SS7 移动攻击中劫持 Telegram、电子邮件帐户	★★★★

MMO 游戏街头黑帮因严重漏洞泄露 190 万用户数据	★★★★
俄罗斯黑客攻击美国政府网络	★★★★
网络钓鱼组织通过伪造的选民登记表收集用户数据、电子邮件和银行密码	★★★★
与伊朗有关的 APT 袭击了中东的组织	★★★★
《看门狗:军团》游戏成为黑客的目标	★★★
美国起诉六名俄罗斯军官	★★★
网络钓鱼诈骗使用重定向来窃取 Office 365、Facebook 凭据	★★★
管理员帐户遭到入侵两周后，OpenDev 关闭了 Gerrit 代码检查工具	★★★
MobileIron 企业 MDM 服务器受到 DDoS 团伙的攻击	★★★
黑客针对思科设备中的 CVE-2020-3118 漏洞	★★★
钓鱼攻击者利用恶意的 SharePoint 和 OneDrive 链接	★★★
勒索软件摧毁了佐治亚州的选民数据库	★★★
其他事件	**等级**
Google 补丁修复了 Chrome 浏览器的 0day 漏洞	★★★★★
WordPress 对流行插件进行了强制的安全更新	★★★★★
Discord 桌面应用程序漏洞链触发远程代码执行攻击	★★★★
Oracle 发布 2020 年 10 月安全公告	★★★★
新的 Gitjacker 工具允许您查找在线公开的.git 文件夹	★★★
微软是钓鱼邮件中被模仿最多的品牌	★★★
Bug bounty 提供者利用别人的漏洞获利	★★★
七款易受地址栏欺骗攻击的移动浏览器	★★★
谷歌删除了两个收集用户数据的 Chrome 广告拦截器	★★★
Lightning Network 披露 `concerning` 加密漏洞	★★★
Mozilla 发布了 Firefox、Firefox ESR 和 Thunderbird 的安全更新	★★★

VMware 修复了其 ESXi、Workstation、Fusion 和 NSX-T 中的几个缺陷	★★★
台湾厂商 QNAP 就 Zerologon 漏洞发布咨询	★★★
Nvidia 警告玩家 GeForce 存在严重的漏洞	★★★
美国财政部对支持 Triton 恶意软件的俄罗斯研究机构实施制裁	★★★
谷歌的 Waze 可以让黑客识别和跟踪用户	★★

三、 事件详情

(一) 恶意程序

GravityRAT：间谍软件

日期: 2020-10-19

等级: 高

作者:

标签: ['Trojan', 'Android', 'GravityRAT', 'Malware']

2018 年，思科 Talos 的研究人员发布了一篇关于间谍软件 GravityRAT 的帖子，该软件被用来攻击印度军队。印度计算机应急响应小组(CERT-IN)于 2017 年首次发现了该木马。它的创建者被认为是巴基斯坦的黑客组织。根据 securelist 的信息，这个活动至少从 2015 年就开始了，之前的目标是 Windows 电脑。

详情

GravityRAT: The spy returns

https://securelist.com/gravityrat-the-spy-returns/99097/

勒索软件团伙将部分赎金捐赠给慈善组织

日期: 2020-10-20

等级: 高

作者: ,Catalin Cimpanu

标签: ['Bitcoin', 'Darkside', 'Children International', 'The Water Project', 'Donate Money']

一个勒索软件组织已将部分勒索要求的一部分从受害者那里勒索到了慈善组织。目前的接受者包括国际儿童基金会（非营利组织，该组织为极端贫困儿童提供赞助）和水源项目（该组织旨在为整个撒哈拉以南非洲地区提供清洁可靠的水源）。根据比特币区块链上的交易，每个组织收到 0.88 比特币（约 10,000 美元）。发送者是一个勒索软件团体，名称为 Darkside。 Darkside 小组自 2020 年 8 月活跃至今，是一个典型的"大型游戏猎人"，它专门研究大型公司网络，加密其数据并要求数百万美元的巨额赎金。

详情

Ransomware gang donates part of ransom demands to charity organizations

https://www.zdnet.com/article/ransomware-gang-donates-part-of-ransom-demands-to-charity-organizations/

Maze 勒索软件

日期: 2020-10-21

等级: 高

作者:

标签: ['Maze', 'Ransomware', 'Malware', 'ChaCha']

在过去的一年里，`Maze`勒索软件已经成为威胁企业和大型组织的最臭名昭著的恶意软件家族之一。几十个组织已经成为这个恶意软件的受害者，包括`LG`、`Southwire`和彭萨科

拉市。该勒索软件的历史始于 2019 年上半年，当时没有任何明显的品牌烙印,勒索字样中包含标题`0010 System Failure 0010`，被研究人员简称为`ChaCha 勒索软件`。

详情

Life of Maze ransomware

https://securelist.com/maze-ransomware/99137/

新的 Windows RAT 可以通过 Telegram 频道进行控制

日期: 2020-10-22

等级: 高

作者: Catalin Cimpanu

标签: ['Trojan', 'Telegram', 'T-RAT', 'Hacking Forums']

安全研究人员在俄语的地下黑客论坛上发现了一种新的远程访问木马(RAT)。
这款名为 T-RAT 的恶意软件售价仅为 45 美元，它的主要卖点是能够通过`Telegram`频道而不是基于网络的管理面板来控制受感染的系统。
它的作者声称，这使得购买者可以更快速、更容易地从任何位置访问受感染的电脑，使得攻击者可以在受害者被感染后，在 RAT 被发现之前，启动数据窃取功能。

详情

New Windows RAT can be controlled via a Telegram channel

https://www.zdnet.com/article/new-windows-rat-can-be-controlled-via-a-telegram-channel/

xmrig 挖矿恶意软件

日期: 2020-10-22

等级: 高

作者:

标签: ['XMRig', 'Ransomware', 'C', 'Miner']

随着保护方法的改进，挖矿恶意软件的开发人员不得不增强他们自己的创造，常常转向重要的解决方案。securelist 在分析开源挖矿软件 XMRig 时发现了几个这样的解决方案。
除了通过数据盗窃和勒索软件赚钱的知名组织(例如，涉嫌最近攻击`SK Hynix`和`LG`电子的`Maze`)，许多潜在的攻击者也被网络犯罪的高调成功所吸引。
在技术能力方面，这些业余勒索者远远落后于有组织的团体，因此使用公开的勒索软件，目标是普通用户，而不是企业部门。这类攻击的花费通常非常小，因此这些不法分子不得不采取各种策略，从每台被感染的机器上获得最大的收益。

详情

xmrig miner

https://securelist.com/miner-xmrig/99151/

台湾政府 2020 年 4 月遭多起网络攻击

日期: 2020-10-22

等级: 高

作者:

标签: ['DLP', 'Waterbear Loader', 'Malware', 'Taiwan', 'Government']

2020 年 4 月，台湾多个政府机构发现高度恶意的网络活动。仅在一个环境中，在扫描的数千个端点中，有 30 个端点被确认感染，10 个高风险端点被这些受损端点连接。在这些复杂的有针对性的攻击中发现了 10 个严重的恶意软件，其中大多数是`Waterbear Loader`恶意软件。攻击者发现并利用可信和常用的数据丢失预防（DLP）软件中的一个弱点来触发恶意软件并持久化。

详情

Taiwan government targeted by multiple cyberattacks in April 2020

https://cybernews.com/security/taiwan-government-targeted-by-multiple-cyberattacks-in-april-2020/

新恶意软件使用远程覆盖攻击劫持您的银行帐户

日期: 2020-10-19

等级: 中

作者: ,Charlie Osborne

标签: ['Brazilian', 'Vizom', 'IBM', 'Bank', 'DLL hijacking', 'Remote Overlay']

研究人员发现了一种新的恶意软件，它利用远程覆盖攻击手段攻击巴西的银行账户持有人。这种新的恶意软件变种，被 IBM 称为 Vizom，正在巴西各地活跃，旨在通过在线的金融服务入侵银行账户。
2020 年 10 月 13 日，IBM 安全研究人员陈纳曼、奥泽尔和凯塞姆表示，这些恶意软件使用特殊的策略来隐藏并实时危及用户设备，即远程覆盖技术和 DLL 劫持攻击。
Vizom 通过基于垃圾邮件的网络钓鱼活动传播，并伪装成流行的视频会议软件。

详情

This new malware uses remote overlay attacks to hijack your bank account

https://www.zdnet.com/article/this-new-malware-uses-remote-overlay-attacks-to-hijack-your-bank-account/

蒙特利尔的 STM 公共交通系统遭到勒索软件攻击

日期: 2020-10-21

等级: 中

作者: ,Lawrence Abrams

标签: ['Société de transport de Montréal', 'RansomExx', 'Montreal', 'Ransomware', 'Attack']

近日，蒙特利尔 Societe de transport de Montreal (STM)公共交通系统遭遇 RansomExx 勒索软件攻击，服务和在线系统受到影响。10 月 19 日，STM 遭受了一次中断，影响了它的 IT 系统、网站和客户支持。虽然这些中断没有影响到公共汽车或地铁系统的运行，但由

于 STM 使用的是在线注册系统，依赖 STM 挨家挨户的辅助运输服务的残疾人受到了影响。

详情

Montreal's STM public transport system hit by ransomware attack

https://www.bleepingcomputer.com/news/security/montreals-stm-public-transport-system-hit-by-ransomware-attack/

LockBit 勒索软件在网络上悄无声息地攻击

日期: 2020-10-21

等级: 中

作者: ,Ionut Ilascu

标签: ['LockBit', 'RaaS', 'Ransomware', 'Network', 'PowerShell']

一旦 LockBit 勒索软件登陆受害者网络，它只需五分钟就可以在目标系统上部署加密程序。LockBit 于 2019 年 9 月加入勒索软件服务（RaaS）业务，它由自动化流程驱动，在受害者网络中快速传播，识别有价值的系统并锁定它们。当恶意软件加载到系统内存中，日志和支持文件在执行时会被删除，LockBit 攻击会留下很少的痕迹用于取证分析。

详情

LockBit ransomware moves quietly on the network, strikes fast

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-moves-quietly-on-the-network-strikes-fast/

法国 IT 外包商 Sopra Steria 疑遭 Ryuk 勒索软件网络攻击

日期: 2020-10-22

等级: 中

作者: Gareth Corfield

标签: ['Sopra Steria', 'Ryuk', 'Cyberattack', 'Ransomware']

总部位于法国的 IT 外包商`Sopra Steria`遭到网络攻击，据报道与`Ryuk`勒索软件团伙有关。该公司拒绝透露发生了什么，但法国媒体报道称，`Sopra Steria`的`Active Directory`基础设施遭到了攻击，似乎是与`Ryuk`恶意软件团伙有关联的黑客所为。

详情

French IT outsourcer Sopra Steria hit by 'cyberattack', Ryuk ransomware suspected

https://www.theregister.com/2020/10/22/sopra_steria_ryuk_ransomware_reports/

Boyne Resorts 滑雪和高尔夫胜地运营商遭到 WastedLocker 勒索软件袭击

日期: 2020-10-24

等级: 中

作者:

标签: ['WastedLocker', 'Boyne Resorts', 'Ransomware', 'Attack']

美国的滑雪和高尔夫度假胜地运营商`Boyne Resorts`的系统感染了`WastedLocker`勒索软件，该事件影响了预订系统。`Boyne Resorts`度假村汇集了从不列颠哥伦比亚省到缅因州

的山地和湖滨度假村，滑雪场和景点。该公司拥有并经营 11 家物业，以及一个户外生活设备，服装零售部门，在密歇根州的各个城市设有商店。勒索软件最初侵入了公司办公室，然后横向移动，瞄准了他们经营的度假村的 IT 系统。由于这次攻击，该公司被迫关闭了部分网络，以防止勒索软件的传播。公司的客户无法在公司经营的度假村预订房间。

详情

Boyne Resorts ski and golf resort operator hit with WastedLocker ransomware

https://securityaffairs.co/wordpress/109933/hacking/boyne-resorts-wastedlocker-ransomware.html

新的 Emotet 攻击使用一个新的 Microsoft Word 模板

日期: 2020-10-25

等级: 中

作者:

标签: ['Microsoft Office', 'Microsoft Word', 'Emotet', 'COVID-19']

研究人员最近观察到`Emotet`攻击采用了一个新模板，该模板伪装成`Microsoft Office`消息，敦促收件人更新其`Microsoft Word`以添加新功能。
Emotet 垃圾邮件利用模板欺骗受害者，使其启用宏来启动感染。安装恶意软件后，`Emotet`会在机器上下载额外的`payloads`，包括勒索软件，并用它发送垃圾邮件。

详情

New Emotet attacks use a new template urging recipients to upgrade Microsoft Word

https://securityaffairs.co/wordpress/109950/cyber-crime/emotet-microsoft-word-template.html

相关安全建议

1. 注重内部员工安全培训
2. 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
3. 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
4. 严格做好 http 报文过滤
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
6. 网段之间进行隔离，避免造成大规模感染
7. 主机集成化管理，出现威胁及时断网
8. 及时备份数据并确保数据安全

(二) 数据安全

网络电话服务提供商泄漏了 3.5 亿客户记录

日期: 2020-10-19

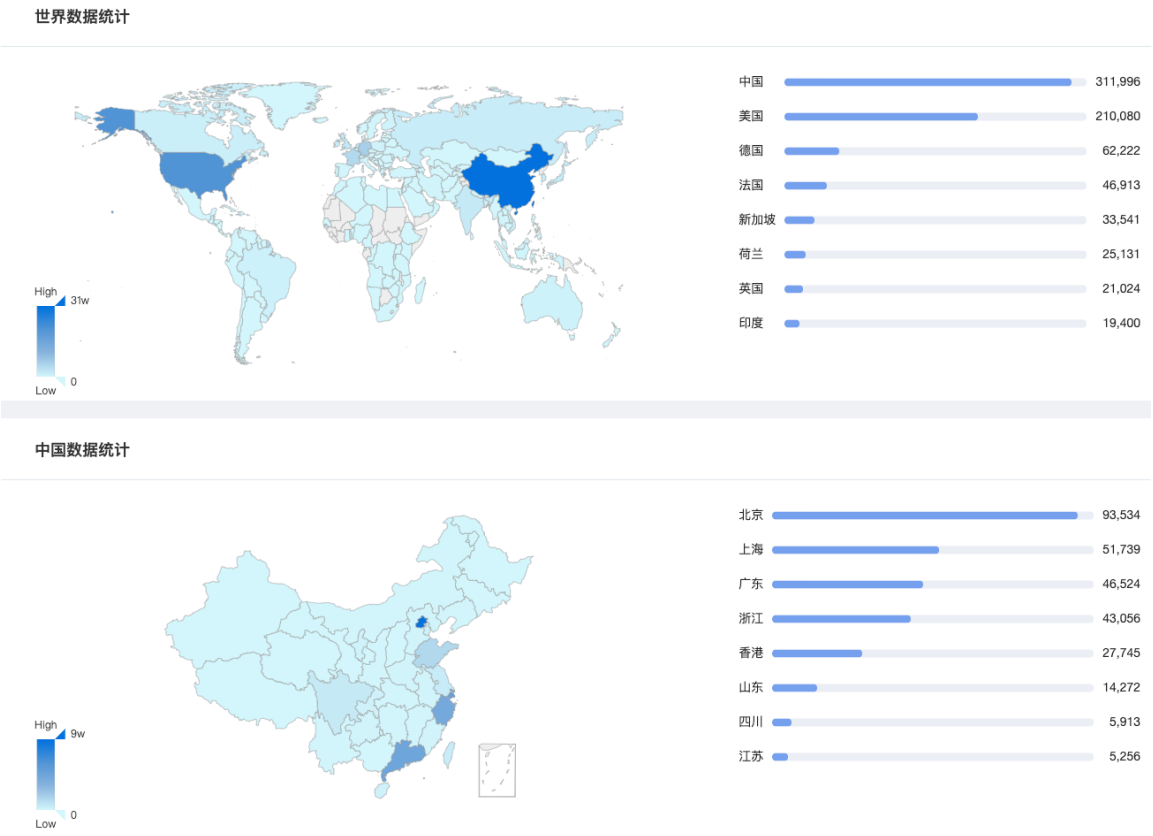
等级: 高

作者:

标签: ['Broadvoice', 'Elasticsearch', 'Unsecured', 'Data Breach']

一个有超过 3.5 亿客户记录的数据库，属于互联网语音协议公司`Broadvoice`，暴露在了不安全的 Elasticsearch 集群中。
10 月 1 日，安全研究员`Bob Diachenko`发现了这个泄露的数据库。他观察到，未受保护的`Elasticsearch`集群包含了一些敏感信息。
该数据库泄露了 3.5 亿份客户记录，包括呼叫者姓名、电话号码和地点。其中一个数据库被发现包含数十万封语音邮件以及其它信息，如医疗处方和金融贷款。

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



详情

VOIP Service Provider Exposes 350M Customer Records
https://gbhackers.com/voip-data-expose/

Albion 网络游戏制造商数据被泄露

日期: 2020-10-19

等级: 高

作者: ,Catalin Cimpanu

标签: ['Albion Online', 'Game Maker', 'Password Hashes', 'Sandbox Interactive']

游戏开发商 2020 年 10 月 17 日透露，一名黑客入侵了流行的免费中世纪幻想 MMORPG Albion Online 论坛，并窃取了用户名和密码哈希值。
"入侵者能够访问论坛用户的资料，包括连接到这些论坛帐户的电子邮件地址，"Albion Online 背后的公司 Sandbox Interactive 说到。
攻击者还获取了加密的密码。Sandbox Interactive 表示，这些密码通过 Bcrypt 密码散列函数进行散列，然后再加入随机数据，以加大攻击者逆转和破解密码的难度。
由于这次未经授权的入侵，游戏开发商在 2020 年 10 月 17 日通过论坛帖子要求用户重新设置密码，并向所有受影响的用户发送电子邮件。

详情

Albion Online game maker discloses data breach

https://www.zdnet.com/article/albion-online-game-maker-discloses-data-breach/

Nefilim 勒索软件团伙公布了 Luxottica 的数据

日期: 2020-10-20

等级: 高

作者:

标签: ['Nefilim', 'Italian', 'Luxottica', 'CVE-2019-19781', 'Citrix ADX', 'Data Breach']

Nefilim 勒索软件运营商发布了一长串文件，这些文件看似属于意大利眼镜和眼保健巨头 Luxottica，大量的文件似乎与人事办公室和财务部门有关。 对泄露的文件进行分析后发现，这些文件包含有关招聘过程，专业简历的机密信息，以及有关集团人力资源部门内部结构的信息。 公开的财务数据包括预算，市场预测分析和其他敏感数据。。Luxottica Group S.p.A.是一家意大利眼镜企业集团，也是眼镜行业中全球最大的公司，拥有超过 80,000 名员工，2019 年创造了 94 亿美元的收入。

详情

Nefilim ransomware gang published Luxottica data on its leak site

https://securityaffairs.co/wordpress/109778/data-breach/luxottica-data-leak-ransomware.html

房贷交易平台曝光房贷文件

日期: 2020-10-20

等级: 高

作者:

标签: ['Maxex', 'Home Loan', 'Data Leak']

总部位于亚特兰大的住宅抵押贷款交易公司 Maxex 公开了 9GB 的内部数据，其中大部分用于其贷款交易平台的软件开发。 但它也包括机密银行文件，系统登录凭证，电子邮件，数据泄露事件响应策略，甚至包括几年前进行的渗透测试的报告。 另外，该公司泄漏了新

泽西州和宾夕法尼亚州至少 23 个人的完整抵押文件。每个人的按揭文件从 400 到 600 页不等。这些 pdf 文件包含了受影响者数量惊人的个人和金融数据。这 23 份文件与 2013 年前后的抵押贷款有关，其中包括提交抵押贷款申请前几年的个人文件。这些文件包括完整的纳税申报单、美国国税局(IRS)的成绩单、主要机构的信用报告、银行账户对账单、出生证扫描、护照、驾照、雇主来信、离婚记录、学业成绩单，甚至还有抵押贷款申请人和他们孩子的社会安全号码。

详情

Home Loan Trading Platform Exposes Mortgage Documentation

https://www.databreachtoday.com/blogs/home-loan-trading-platform-exposes-mortgage-documentation-p-2959

Kleenheat 客户名称和地址因系统漏洞而泄漏

日期: 2020-10-19

等级: 中

作者: ,Asha Barbaschow

标签: ['Australian', 'Kleenheat', 'Data Breach', 'DDos']

澳大利亚天然气生产商克莱恩霍特(Kleenheat)警告多家客户，称之前发生的网络攻击可能导致姓名和地址等信息被泄露。这家位于珀斯的零售商和分销商认为，入侵事件发生在 2014 年，发生在第三方系统上。`ZDNet`平台了解该系统已不再使用。
该公司在给客户的一封电子邮件中写道:"`Kleenheat`最近在一次例行数据安全检查中发现了可能的泄露，并没有发生在公司的内部系统中。"
`Kleenheat`将存在潜在风险的数据称为"一般联系信息"，并确认其中包括姓名、居住地址和电子邮件地址。`Kleenheat`保证电话号码、出生日期、银行、信用卡和账户数据没有泄露。

详情

Kleenheat customer names and addresses exposed in system breach

https://www.zdnet.com/article/kleenheat-customer-names-and-addresses-exposed-in-system-breach/

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. 发生数据泄漏事件后，及时进行密码更改等相关安全措施

3. 数据库数据，尤其是密码等敏感信息需进行加密存储
4. 使用 Git 等同步存储工具时，注意信息的过滤，避免上传敏感文件
5. 严格控制数据访问权限
6. 及时检查并删除外泄敏感数据
7. 条件允许的情况下，设置主机访问白名单
8. 及时备份数据并确保数据安全

(三) 网络攻击

美国国安局：中国黑客常用的 25 大漏洞

日期: 2020-10-20

等级: 高

作者: ,Sergiu Gatlan

标签: ['NSA', 'Vulnerability', 'DoD', 'DIB', 'Chinese']

在 2020 年 10 月 20 日发布的一份报告中，美国国家安全局表示，它知道中国政府支持的黑客针对国家安全系统(NSS)、美国国防工业基地(DIB)和国防部(DoD)信息网络的针对性攻击。
作为这些攻击的一部分，美国国家安全局已经发现了 25 个公开的漏洞，这些漏洞被用来访问网络，部署恶意移动应用，并通过横向传播，同时攻击者窃取敏感数据。
美国国家安全局建议所有机构立即给易受攻击的设备打补丁，以防止导致数据盗窃、银行欺诈和勒索软件攻击的网络攻击。

详情

NSA: Top 25 vulnerabilities actively abused by Chinese hackers
https://www.bleepingcomputer.com/news/security/nsa-top-25-vulnerabilities-actively-abused-by-chinese-hackers/

Ryuk 勒索软件团伙使用 Zerologon 漏洞进行闪电般的攻击

日期: 2020-10-19

等级: 高

作者:

标签: ['Ryuk', 'Phishing', 'Encryption', 'Zerologon', 'Cobalt Strike', 'CVE-2020-1472']

Ryuk 勒索软件团伙再次发起攻击，从发送网络钓鱼邮件到对受害者网络的加密在 5 小时内完成。研究人员说，这种惊人的速度部分是由于团伙使用了 Zerologon 权限升级漏洞（CVE-2020-1472）。微软称，Zerologon 漏洞允许未经身份验证的攻击者通过网络访问域控制器，完全危害所有 Active Directory 身份服务。它在 2020 年 8 月份被修补，但许多组织仍然未修复该漏洞。
根据 2020 年 10 月 18 日发布的 DFIR 报告研究人员的分析，在这次特定的攻击中，在攻击者使用 Zerologon 提升权限后，他们使用各种黑客工具，如 Cobalt Strike、AdFind、WMI 和 PowerShell 来实现目标。

详情

Ryuk Ransomware Gang Uses Zerologon Bug for Lightning-Fast Attack
https://threatpost.com/ryuk-ransomware-gang-zerologon-lightning-attack/160286/

黑客在 SS7 移动攻击中劫持 Telegram、电子邮件帐户

日期: 2020-10-19

等级: 高

作者: ,Ionut Ilascu

标签: ['Pandora Security', 'SS7', 'Telegram', 'Hijack', '2FA']

通过接入用于连接全球移动网络的 7 号信令系统(SS7)，黑客能够获取加密货币业务中知名人士的 Telegram 和电子邮件数据。
在这次有针对性的攻击中，黑客通过受害者手机供应商的短信息系统发送了双因素认证(2FA)登录代码。
黑客发动 SS7 攻击，可以通过更新合法接收方的设备位置来拦截短信和呼叫，就好像设备已注册到另一个网络(漫游场景)。
这次攻击发生在 9 月，针对的对象是 Partner Communications Company（以前称为 Orange Israel）的至少 20 个订户，他们全部都参与了更高级别的加密货币项目。

详情

Hackers hijack Telegram, email accounts in SS7 mobile attack
https://www.bleepingcomputer.com/news/security/hackers-hijack-telegram-email-accounts-in-ss7-mobile-attack/

MMO 游戏街头黑帮因严重漏洞泄露 190 万用户数据

日期: 2020-10-20

等级: 高

作者:

标签: ['Street Mobster', 'SQL Injection', 'BigMage Studios', 'Databases']

研究人员发现，由于 SQL 注入严重漏洞，MMO 游戏`街头黑帮`正在泄漏 190 万用户的数据。攻击者可以利用 SQL 注入漏洞来破坏游戏数据库并窃取用户数据。`街头黑帮`(Street Mobster)是一款免费游戏，基于浏览器的黑手党帝国类型的在线游戏，玩家管理一个虚构的犯罪企业，由保加利亚开发公司`BigMage Studios`创建。攻击者可以通过在游戏网站上发起 SQL 注入（SQLi）攻击来访问该数据库。利用 Street Mobster 中的 SQLi 漏洞可以获取包括玩家的用户名、电子邮件地址和密码，以及存储在数据库中的其他游戏相关数据。

详情

MMO game Street Mobster leaking data of 1.9 million users due to critical vulnerability
https://securityaffairs.co/wordpress/109788/data-breach/street-mobster-data-leak.html

俄罗斯黑客攻击美国政府网络

日期: 2020-10-23

等级: 高

作者:

标签: ['Russian', 'U.S.', 'APT', 'Government']

CISA 和 FBI 发布了一份联合警报，详细说明了俄罗斯政府资助的高级持续威胁组织（APT）在针对各种美国政府网络以窃取敏感数据。
自 2010 年以来，俄罗斯政府资助的 APT 组织如`Berserk Bear`, `Energetic Bear`, `TeamSpy`, `Dragonfly`, `Havex`, `Crouching Yeti`, `Koala`等活跃于美国各州，地方，地区和部落(SLTT)政府网络，以及航空网络。
根据联合警告，该组织已经侵入了许多政府网络，并获得了访问敏感文件的权限。

详情

Russian Hackers Attack U.S. Government Networks
https://gbhackers.com/russian-state-sponsored-attackers/

网络钓鱼组织通过伪造的选民登记表收集用户数据、电子邮件和银行密码

日期: 2020-10-23

等级: 高

作者: Catalin Cimpanu

标签: ['US Presidential Election', 'KnowBe4', 'Proofpoint', 'Phishing', 'EAC']

在美国总统大选举行前的几天，垃圾邮件组织趁热打铁，利用与选民登记相关的链接来诱骗人们访问虚假的政府网站并泄露其个人数据，有时他们甚至直接询问银行和电子邮件密码。
电子邮件安全公司`KnowBe4`和`Proofpoint`发现了这些活动，这些活动正在假冒美国选举协助委员会(`EAC`)的身份。`EAC`是美国政府机构，负责管理选民登记指南。
根据`Proofpoint`的说法，这些网站都是假的，通常都是被黑客入侵的`WordPress`网站。如果用户没有注意到错误的网址，他们最终会把自己的个人资料提供给犯罪集团。

详情

Phishing groups are collecting user data, email and banking passwords via fake voter registration forms
https://www.zdnet.com/article/phishing-groups-are-collecting-user-data-email-and-banking-passwords-via-fake-voter-registration-forms/

与伊朗有关的 APT 袭击了中东的组织

日期: 2020-10-23

等级: 高

作者:

标签: ['Seedworm', 'Iran', 'APT', 'MuddyWater', 'Middle East']

与伊朗有关的网络间谍组织`Seedworm`(又名 MuddyWater MERCURY 和 Static Kitten)被发现在新一轮攻击中使用了一种新的下载器。安全专家指出，攻击者开始实施破坏性的攻

击。
专家称此次行动为`MuddyWater`，被用于攻击阿富汗、阿塞拜疆、柬埔寨、伊拉克、以色列、格鲁吉亚、土耳其和越南的政府、教育、石油和天然气、房地产、技术和电信组织。

详情

Iran-Linked Seedworm APT target orgs in the Middle East
https://securityaffairs.co/wordpress/109911/apt/iran-seedworm-middle-east.html

《看门狗:军团》游戏成为黑客的目标

日期: 2020-10-19

等级: 中

作者:

标签: ['Watch Dogs: Legion', 'Egregor', 'Albion', 'Source Code', 'Ubisoft']

2020 年 10 月刚刚出现的一个名为`Egregor`的勒索软件团伙声称已经入侵了即将发布的游戏《看门狗：军团》（`watchdogs:Legion`）的源代码。《看门狗：军团》将于 10 月 29 日发布，这是一个备受期待的发布，这要归功于它的 4K 视觉效果。`Egregor gang`声称已经从游戏发行商`Ubisoft`取走了代码和一些专有文件。

详情

Game Titles Watch Dogs: Legion, Albion Both Targeted by Hackers
https://threatpost.com/hackers-source-code-theft-watch-dogs-legion-albion/160268/

美国起诉六名俄罗斯军官

日期: 2020-10-19

等级: 中

作者:

标签: ['The United States', 'Russian', 'NotPetya', 'Ukranian', 'Sandworm', 'Telebots']

美国司法部宣布匹兹堡大陪审团诉格鲁情报局的六名俄罗斯人，指控他们参与了一系列袭击，给私营部门造成了数十亿美元的损失。这些俄罗斯人是一个叫做`Sandworm`或`Telebots`的组织的，他们以`NotPetya`恶意程序闻名，袭击了奥运会以及摧毁了乌克兰的电网。

详情

U.S. indicts six Russian officers for NotPetya, Ukrainian blackouts, other attacks
https://www.scmagazine.com/home/security-news/u-s-indicts-six-russian-officers-for-notpetya-ukrainian-blackouts-other-attacks/

网络钓鱼诈骗使用重定向来窃取 Office 365、Facebook 凭据

日期: 2020-10-19

等级: 中

作者:

标签: ['Facebook Messenger', 'Office 365', 'Phishing', 'Senior Executives', 'Finance Personnel']

研究人员最近警告说，有两项大规模的网络钓鱼行为，共同针对成千上万的用户，一次是攻击 Office 365 等商业服务的凭据，另一次是滥用 Facebook Messenger，以攻击大约 45 万名社交媒体的帐户持有者，高级管理人员和财务人员已被确定为行动的目标之一，此次钓鱼行动从 10 月 15 日开始大幅增加。

详情

Phishing scams use redirects to steal Office 365, Facebook credentials

https://www.scmagazine.com/home/security-news/phishing/phishing-scams-use-redirects-to-steal-office-365-facebook-credentials/

管理员帐户遭到入侵两周后，OpenDev 关闭了 Gerrit 代码检查工具

日期: 2020-10-21

等级: 中

作者: ,Simon Sharwood

标签: ['OpenStack', 'Gerrit', 'Backdoored', 'GitHub']

OpenDev.org 网站 2020 年 10 月 20 日，在意识到被秘密黑客入侵后，关闭了它的 Gerrit 部署。该网站要求用户审查最近提交给他们的项目，以确保他们不包含任何后门或其他恶意代码。
OpenDev 托管了许多其他基于 git 的存储库，与 GitHub 和类似的源代码托管机构非常相似。它使用 google 构建的 Gerrit 为团队提供了一个基于 web 的环境，让团队可以审查彼此的工作，批准或拒绝对代码库的更改，或者在编程项目上进行协作。

详情

OpenStack haven OpenDev yanks Gerrit code review tool after admin account compromised for two weeks

https://www.theregister.com/2020/10/21/opendev_gerrit_attack/

MobileIron 企业 MDM 服务器受到 DDoS 团伙的攻击

日期: 2020-10-21

等级: 中

作者: ,Catalin Cimpanu

标签: ['MobileIron', 'MDM', 'Attack', 'Orange Tsai', 'Vulnerability']

一个月前，一种用于管理大量移动设备的服务器的三个严重漏洞的细节被公布，现在，多个攻击者正在利用这些漏洞接管企业服务器，甚至策划对公司网络的入侵。这些攻击的目标是软件制造商 MobileIron 的 MDM 服务器。MDM 代表移动设备管理。MDM 系统用于企业内部，通过允许系统管理员部署证书、应用程序、访问控制列表和清除中央服务器上被盗的手机，从而允许企业管理员工的移动设备。

详情

MobileIron enterprise MDM servers under attack from DDoS gangs, nation-states

https://www.zdnet.com/article/mobileiron-enterprise-mdm-servers-under-attack-from-ddos-gangs-nation-states/

黑客针对思科设备中的 CVE-2020-3118 漏洞

日期: 2020-10-21

等级: 中

作者:

标签: ['Cisco', 'Cisco IOS XR Software', 'Attack', 'CVE-2020-3118']

Cisco 警告说，针对`CVE-2020-3118`高严重性漏洞的攻击会影响运行`Cisco IOS XR`软件的多个运营商级路由器。该漏洞存在于`Cisco IOS XR`软件的`Cisco Discovery Protocol`实现中，允许未经验证的相邻攻击者执行任意代码或重新加载受影响的设备。该漏洞存在于 Cisco IOS XR 软件的 Cisco Discovery Protocol 实现中，允许未经验证的相邻攻击者执行任意代码或重新加载受影响的设备。

详情

Hackers are targeting CVE-2020-3118 flaw in Cisco devices

https://securityaffairs.co/wordpress/109816/hacking/cisco-cve-2020-3118-flaw-attacks.html

钓鱼攻击者利用恶意的 SharePoint 和 OneDrive 链接

日期: 2020-10-22

等级: 中

作者:

标签: ['Microsoft', 'SharePoint Online', 'OneDrive', 'Phishing']

攻击者正在利用基于云的协作服务(如微软的 SharePoint Online 和 OneDrive)作为一种社交工程工具，诱骗用户点击恶意链接，其目的通常是进行网络欺诈或供应链欺诈。
在最近的一项分析中，网络安全公司`Proofpoint`透露，在 2020 年上半年，它收集了大约 590 万封带有恶意`SharePoint Online`和`OneDrive`链接的电子邮件。虽然这些电子邮件只占所有含有恶意网址的邮件的 1%，但却占所有用户点击的 13%以上。

详情

Malicious SharePoint and OneDrive links are a phishing scammer's dream

https://www.scmagazine.com/home/security-news/phishing/malicious-sharepoint-and-onedrive-links-are-a-phishing-scammers-dream/

勒索软件摧毁了佐治亚州的选民数据库

日期: 2020-10-23

等级: 中

作者:

标签: ['Georgia', 'the Gainesville Times', 'Hall County', 'DoppelPaymer', 'Ransomware', 'Database']

据当地报纸《盖恩斯维尔时报》报道，10 月 7 日的勒索软件攻击针对的是一个用于验证佐治亚州选民签名的数据库，不过该数据库仍未完全正常运行。 但是受勒索软件攻击影响的许多其他霍尔县系统已经恢复。
安全公司 Emsisoft 的威胁分析师布雷特·卡洛（Brett Callow）表示，DoppelPaymer 犯罪团伙是这次网络攻击事件的攻击者。 他说，这可能是首次成功的勒索软件攻击，已经影响了部分选举的基础设施。

县选民登记协调员凯·温布耶告诉《盖恩斯维尔时报》，尽管选民验证数据库存在问题，但仍然可以使用选民登记卡的复印件来验证签名。

详情

Ransomware Knocks Out Voter Database in Georgia

https://www.databreachtoday.com/ransomware-knocks-out-voter-database-in-georgia-a-15235

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. 各主机安装 EDR 产品，及时检测威胁
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
4. 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
5. 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
6. 积极开展外网渗透测试工作，提前发现系统问题
7. 减少外网资源和不相关的业务，降低被攻击的风险
8. 严格做好 http 报文过滤
9. 做好产品自动告警措施
10. 统一 web 页面报错信息，避免暴露敏感信息

(四) 其他事件

Google 补丁修复了 Chrome 浏览器的 0day 漏洞

日期: 2020-10-21

等级: 高

作者:

标签: ['Google', 'Chrome', 'FreeType', '0day', 'Sergei Glazunov', 'Vulnerability']

`Google`发布了其`Chrome`浏览器的更新程序，该更新程序修补了该软件的`FreeType`字体渲染库中的一个`0day`漏洞，该漏洞已被广泛使用。
谷歌项目的安全研究员`Sergei Glazunov`发现了这个漏洞，它被归类为一种内存损坏漏洞，在自由类型中称为堆缓冲区溢出。`Glazunov`在 2020 年 10 月 19 日通知了谷歌这个漏洞。

详情

Google Patches Actively-Exploited Zero-Day Bug in Chrome Browser

https://threatpost.com/google-patches-zero-day-browser/160393/

WordPress 对流行插件进行了强制的安全更新

日期: 2020-10-21

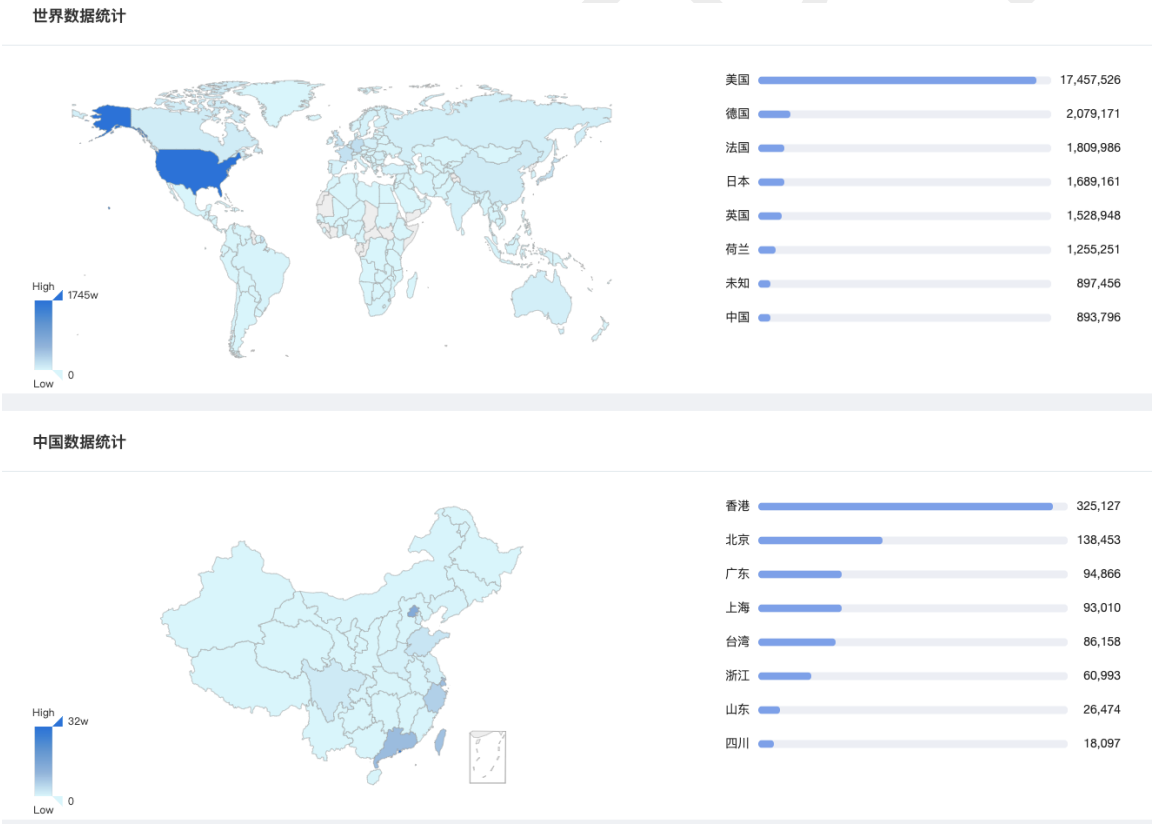
等级: 高

作者: ,Catalin Cimpanu

标签: ['WordPress', 'Plugin', 'Forced update', 'SQL Injection', 'Loginizer']

2020 年 10 月，WordPress 安全团队采取了罕见的措施，使用了一个鲜为人知的内部功能，强行为一个流行插件推送安全更新。运行 Loginizer 插件的 WordPress 站点 2020 年 10 月 20 日被强制更新到 Loginizer 版本 1.6.4。这个版本包含了一个危险的 SQL 注入错误的安全修复程序，该漏洞可能会让黑客接管运行旧版本 Loginizer 插件的 WordPress 站点。Loginizer 是当今最流行的 WordPress 插件之一，拥有超过一百万个站点。该插件为 WordPress 登录页面提供了安全增强。根据其官方描述，Loginizer 可以将访问 WordPress 登录页面的 IP 地址黑名单或白名单，可以添加双因素身份验证的支持，或者可以添加简单的验证码来阻止自动登录尝试等许多功能。

目前 Wordpress 的具体分布如下图，数据来自于 360 QUAKE



详情

WordPress deploys forced security update for dangerous bug in popular plugin

https://www.zdnet.com/article/wordpress-deploys-forced-security-update-for-dangerous-bug-in-popular-plugin/

Discord 桌面应用程序漏洞链触发远程代码执行攻击

日期: 2020-10-19

等级: 高

作者: ,Charlie Osborne

标签: ['Discord', 'APP', 'RCE', 'Vulnerability', 'Bug Bounty']

Discord 应用程序的桌面版本存在一个严重的问题，这个问题使得用户容易受到远程代码执行(RCE)攻击。
漏洞赏金猎人`Masato Kinugawa`几个月前挖掘了一个导致`RCE`的漏洞利用链，并发表了一篇博客文章，描述了该方法的技术细节。

详情

Discord desktop app vulnerability chain triggered remote code execution attacks
https://www.zdnet.com/article/discord-desktop-app-vulnerable-to-remote-code-execution-bug/

Oracle 发布 2020 年 10 月安全公告

日期: 2020-10-20

等级: 高

作者:

标签: ['Oracle', 'Critical Patch Update', 'October']

Oracle 已发布 2020 年 10 月的重要补丁更新，以解决多个产品中的 402 个漏洞。 远程攻击者可以利用其中的某些漏洞来控制受影响的系统。

网络安全和基础架构安全局（CISA）鼓励用户和管理员查看 2020 年 10 月 Oracle 重要补丁更新并应用必要的更新。

详情

Oracle Releases October 2020 Security Bulletin
https://us-cert.cisa.gov/ncas/current-activity/2020/10/20/oracle-releases-october-2020-security-bulletin-0

新的 Gitjacker 工具允许您查找在线公开的.git 文件夹

日期: 2020-10-19

等级: 中

作者: ,Catalin Cimpanu

标签: ['Gitjacker', 'Tools', '.git', 'Liam Galvin', 'Go']

一个名为`Gitjacker `的新工具可以帮助开发人员发现他们何时意外地在线上传了`/.git`文件夹，并将敏感信息暴露给攻击者。
Gitjacker 由英国软件工程师 Liam Galvin 创建，用 Go 编写，2020 年 10 月在 GitHub 上免费下载。
该工具以其最简单的形式允许用户扫描域并标识其生产系统上`/.git`文件夹的位置。

详情

New Gitjacker tool lets you find .git folders exposed online

https://www.zdnet.com/article/new-gitjacker-tool-lets-you-find-git-folders-exposed-online/

微软是钓鱼邮件中被模仿最多的品牌

日期: 2020-10-19

等级: 中

作者:

标签: ['Microsoft', 'Phishing', 'Emails', 'Coronavirus', 'Hacker Impersonations']

2020 年第三季度，在全球品牌的网络钓鱼攻击中，微软的产品和服务占据了近五分之一的份额。由于网络攻击者继续利用冠状病毒大流行造成的远程办公，根据 Check Point 的数据，这个计算机巨头从第二季度的第五位(占攻击总数的 7%)跃升至截止 9 月份的第一名。同时`Check Point`还发现，44%的钓鱼攻击是通过电子邮件进行的，其次是网络(43%)和移动(12%)。

详情

Microsoft is the Most-Imitated Brand for Phishing Emails

https://threatpost.com/microsoft-most-imitated-phishing/160255/

Bug bounty 提供者利用别人的漏洞获利

日期: 2020-10-19

等级: 中

作者: ,Ax Sharma

标签: ['HackerOne', 'Cashes Out', 'Bug Bounty', 'Plagiarized']

漏洞奖励计划已经从安全研究社区获得了越来越多的动力和兴趣，但它们也不是没有问题。
2019 年，HackerOne 支付了超过 6200 万美元的漏洞赏金，根据该平台的最新报告，2020 年这个数字超过了 1 亿美元。
不幸的是，有些人可能会为了自己的经济利益而滥用这些系统。
最近，安全专家 Guido Vranken 发现，HackerOne 运行的 Monero 漏洞奖励程序所报告的漏洞，和他之前发现的漏洞报告一模一样。
在撰写本文时，Monero 的员工在同一份 HackerOne 报告中表示，即使该漏洞是抄袭的，他们也无法收回已经支付的那笔钱。

详情

Bug bounty reporter cashes out on someone else's exploit

https://www.bleepingcomputer.com/news/security/bug-bounty-reporter-cashes-out-on-someone-elses-exploit/

七款易受地址栏欺骗攻击的移动浏览器

日期: 2020-10-20

等级: 中

作者: ,Catalin Cimpanu

标签: ['Rapid7', 'Safari', 'Opera', 'Browser', 'Address Bar Spoofing', 'Vulnerability']

"地址栏欺骗"漏洞是指 web 浏览器中的一个漏洞，该漏洞允许恶意网站修改其真实的 URL 并显示一个假的 URL—通常是合法站点的 URL。网络安全公司`Rapid7`2020 年 10 月发布的一份报告中，披露了 7 个移动浏览器应用程序中 10 个新的地址栏欺骗漏洞。受影响的浏览器包括苹果 Safari、Opera Touch 和 Opera Mini 等大牌浏览器，也包括 Bolt、RITS、UC Browser 和 Yandex Browser 等利基应用程序。

详情

Seven mobile browsers vulnerable to address bar spoofing attacks

https://www.zdnet.com/article/seven-mobile-browsers-vulnerable-to-address-bar-spoofing-attacks/

谷歌删除了两个收集用户数据的 Chrome 广告拦截器

日期: 2020-10-20

等级: 中

作者: ,Catalin Cimpanu

标签: ['Chrome Extension', 'Chrome Web Store', 'Nano-Adblocker', 'Nano-Defender', 'Collecting User Data']

谷歌在 Chrome 官方网站上删除了两个广告屏蔽扩展，这两个插件被发现在大规模收集用户数据。这两个扩展名为 Nano-Adblocker 和 Nano-Defender，在它们被拆除时，每一个都有超过 50000 个和 200000 个安装。

详情

Google removes two Chrome ad blockers caught collecting user data

https://www.zdnet.com/article/google-removes-two-chrome-ad-blockers-caught-collecting-user-data/

Lightning Network 披露 `concerning` 加密漏洞

日期: 2020-10-21

等级: 中

作者: ,Ax Sharma

标签: ['Lightning Network', 'Vulnerability', 'DoS', 'Ethreum', 'Blockchain']

Lightning Network 背后的团队已经发布了关于加密货币协议及其软件实现中发现的漏洞的大量细节。
攻击者可以利用这些漏洞来制造 DoS，并通过拦截双方签订的"智能合同"来中断加密交易。
Lightning Network 是一种运行在基于区块链的加密货币如比特币、Ethreum 等之上的支付协议。

详情

Lightning Network discloses "concerning" crypto vulnerabilities

https://www.bleepingcomputer.com/news/security/lightning-network-discloses-concerning-crypto-vulnerabilities/

Mozilla 发布了 Firefox、Firefox ESR 和 Thunderbird 的安全更新

日期: 2020-10-21

等级: 中

作者:

标签: ['Mozilla', 'Firefox', 'Firefox ESR', 'Thunderbird', 'Security Updates']

Mozilla 发布了安全更新来解决 Firefox、Firefox ESR 和 Thunderbird 中的漏洞。攻击者可以利用这些漏洞来控制受影响的系统。网络安全与基础设施安全局（CISA）鼓励用户和管理员查看 Mozilla Firefox 82、Firefox ESR 78.4 和 Thunderbird 78.4 的安全建议，并应用必要的更新。

详情

Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird

https://us-cert.cisa.gov/ncas/current-activity/2020/10/21/mozilla-releases-security-updates-firefox-firefox-esr-and

VMware 修复了其 ESXi、Workstation、Fusion 和 NSX-T 中的几个缺陷

日期: 2020-10-22

等级: 中

作者:

标签: ['VMware', 'ESXi', 'Code Execution', 'Vulnerability', 'Workstation']

VMware 修复了其 ESXi、Workstation、Fusion 和 NSX-T 产品中的几个漏洞，包括允许任意代码执行的严重漏洞。
该严重漏洞被追踪为`CVE-2020-3992`，是一个影响 ESXi 中的`OpenSLP`服务的问题。该漏洞允许远程攻击者在受影响的`ESXi`产品安装上执行任意代码。
攻击者可以利用该漏洞进行攻击，该漏洞需要位于管理网络上，并且能够访问 ESXi 计算机上的端口 427。

详情

VMware fixes several flaws in its ESXi, Workstation, Fusion and NSX-T

https://securityaffairs.co/wordpress/109843/security/vmware-critical-flaws.html

台湾厂商 QNAP 就 Zerologon 漏洞发布咨询

日期: 2020-10-22

等级: 中

作者:

标签: ['Taiwanese', 'QNAP', 'NAS', 'QTS', 'Zerologon']

台湾厂商 QNAP 发布了一则警告客户，其网络连接存储（NAS）设备的操作系统（也称 QTS）的某些版本受到 Zerologon 漏洞`（CVE-2020-1472）`的影响。
`CVE-2020-1472`漏洞是驻留在 Netlogon 中的特权提升。Netlogon 服务是 Windows 客户端身份验证体系结构中使用的一种身份验证机制，用于验证登录请求，并注册、验证和定位域控制器。企业 Windows 服务器的管理员必须在 2020 年 10 月 22 日安装 2020 年 8 月

的补丁，以减轻漏洞给网络带来的不可接受的风险。攻击者还可以利用该漏洞禁用 Netlogon 身份验证过程中的安全功能，并更改域控制器 Active Directory 上计算机的密码。

详情

Taiwanese vendor QNAP issues advisory on Zerologon flaw
https://securityaffairs.co/wordpress/109859/iot/qnap-zerologon-flaw.html

Nvidia 警告玩家 GeForce 存在严重的漏洞

日期: 2020-10-23

等级: 中

作者:

标签: ['Nvidia', 'Windows', 'GeForce', 'Vulnerability', 'Code Execution']

`Nvidia`是游戏图形处理器（`GPU`）的制造商，该公司已经修复了`Windows`版`GeForce Experience`软件的两个严重漏洞。其中最严重的漏洞（`CVE-2020-5977`）可能产生包括代码执行、拒绝服务、权限提升和信息泄露的问题。该漏洞的 `CVSS` 评分为 8.2，严重程度很高。`Nvidia`在 2020 年 10 月 24 日发布的安全建议中表示，用户可以从`GeForce`体验下载页面下载更新，或者打开客户端自动应用安全更新。

详情

Nvidia Warns Gamers of Severe GeForce Experience Flaws
https://threatpost.com/nvidia-gamers-geforce-experience-flaws/160487/

美国财政部对支持 Triton 恶意软件的俄罗斯研究机构实施制裁

日期: 2020-10-24

等级: 中

作者:

标签: ['US Treasury Department', 'Russia', 'Central Scientific Research Institute of Chemistry', 'Mechanics', 'Triton']

美国财政部宣布对俄罗斯一家研究机构实施制裁，原因是该机构涉嫌参与开发 Triton 恶意软件。
2020 年 10 月 24 日，美国财政部外国资产控制办公室(`OFAC`)根据《反美制裁法案》(CAATSA)第 224 条规定，指定一家与破坏性的`Triton`恶意软件有关的俄罗斯政府研究机构。
`Triton`是一种专门针对工业控制系统(ICS)系统设计的恶意软件，于 2017 年 12 月被`FireEye`的研究人员发现。
2017 年，该恶意软件被用于攻击沙特私人公司`Tasnee`旗下的一家沙特石化工厂，随后首次被发现。据专家称，感染引起了爆炸。

详情

US Treasury imposes sanctions on a Russian research institute behind Triton malware
https://securityaffairs.co/wordpress/109923/cyber-warfare-2/tsniikhm-sanctions-triton-malware.html

谷歌的 Waze 可以让黑客识别和跟踪用户

日期: 2020-10-20

等级: 中

作者:

标签: ['Google', 'Waze', 'Bug Bounty']

安全研究人员在 Google 的 Waze 应用程序中发现了一个漏洞，该漏洞使他能够实时跟踪附近驾驶员的具体运动，甚至可以准确地识别出他们的身份。 Waze 使用众包信息，旨在警告驾驶员可能通勤的障碍物（例如交通拥堵，建筑，事故等），然后提出绕过这些障碍物的替代且更快的路线。该应用程序还显示附近其他驾驶员的位置及其 GPS 位置。

详情

Google's Waze Can Allow Hackers to Identify and Track Users
https://threatpost.com/googles-waze-track-users/160332/

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. 使用 Git 等同步存储工具时，注意信息的过滤，避免上传敏感文件
3. 及时对系统及各个服务组件进行版本升级和补丁更新

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