安全事件周报

安全事件周报 (10.05-10.11)

360CERT
北京奇虎科技有限公司 | 2020-10-12

报告信息

报告名称	安全事件周报（10.05-10.11）		
报告类型	安全事件周报	报告编号	B6-2020-101201
报告版本	1.0	报告日期	2020-10-12
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	2020-10-12	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 35 项

话题集中在`网络攻击`、`勒索软件`方面，涉及的组织有：`Facebook `、`Apple`、`Chowbus `、`阿联酋国际航空公司`等。网络扫描器积极利用 1day、Nday 进行无差别攻击，更新不及时，内网两行泪。

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**
勒索软件迫使保险公司关闭了 200 个管理员帐户	★★★★★
加密挖掘蠕虫增加了 Linux 密码窃取功能	★★★★
第二次在野发现 UEFI rootkit	★★★★
无文件恶意程序注入 Windows 错误报告服务	★★★★
一种被称为 SLOTHFULMEDIA 的新的远程木马	★★★
勒索软件威胁激增，Ryuk 约每周攻击 20 家公司	★★★
勒索软件攻击健康科技公司，扰乱了 COVID-19 医学试验	★★★
新的 HEH 僵尸网络可能会擦除磁盘	★★★
Software AG 受勒索软件的攻击：攻击者泄露了工作人员的护照	★★★
新的 MalLocker.B 勒索软件能显示赎金笔记	★★★
嘉年华证实数据泄露是 8 月勒索软件攻击的结果	★★★
泰勒科技公司最终向勒索软件支付了赎金	★★★
不要低估 FONIX 勒索软件服务	★★★
CISA 警告美国政府机构遭受 Emotet 攻击	★★
数据安全	**等级**
澳大利亚社交新闻平台泄露 8 万条用户记录	★★★★
阿联酋国际航空公司的数据泄露至暗网	★★★
网络攻击	**等级**
美国公司 1500 万美元网络抢劫案剖析	★★★★★
黑客从瑞士大学窃取了 6 位数的金额	★★★★
新一波的网络钓鱼电子邮件以选举为诱饵	★★★★
国际海事组织（IMO）遭受网络攻击	★★★★

外卖服务 Chowbus 遭黑客攻击，超过 40 万名客户受到影响	★★★★
黑客团伙现利用严重的 Windows 漏洞进行攻击	★★★★
国土安全部：不明黑客袭击了美国人口普查局网络	★★★★
基于 Mirai 的 IoT 木马传播了两个 0day 漏洞	★★★
Fullz House 入侵 Boom!的网站	★★★
Wisepay 的"停机"源于食堂支付业务对入侵者攻击的阻止	★★★
Comcast 遥控器可被入侵用于监听对话	★★★
WordPress 漏洞为 Zerologon 攻击提供通道	★★★
黑客组织出售间谍和虚假新闻服务	★★★
亚马逊黄金日，网络钓鱼和欺诈攻击激增	★★★
Fitbit gallery 可用于分发恶意应用程序	★★★
其他事件	**等级**
流行的反病毒软件漏洞让攻击者可以升级特权	★★★
Bugcrowd 在 2020 年末选出最值得关注的 Bugs	★★★
在苹果各种服务中发现 55 个安全漏洞	★★★
Facebook 首次推出漏洞赏金	★★★

三、 事件详情

(一) 恶意程序

勒索软件迫使保险公司关闭了 200 个管理员帐户

日期: 2020-10-06

等级: 高

作者: Gareth Corfield

标签: ['The Register', 'Ardonagh Group', 'Ransomware', 'Accounts']

知情人士向 The Register 透露，随着"cyber incident"在其 IT 领域的发展，Ardonagh Group 保险公司被迫暂停 200 个具有管理员特权的内部帐户。英国《金融时报》称，作为英国第二大私有保险经纪公司，Ardonagh Group 2020 年以来一直在收购其它公司。 最近一次袭击发生的时机很不幸：据报道，Ardonagh 最近公布了财务报告，显示损失 9400 万英镑。Ardonagh 的发言人 KellyAnnKnight 没有否认公司遭受的"cyber incident"是勒索软件，但没有证实任何细节。

详情

Insurance firm Ardonagh Group disabled 200 admin accounts as ransomware infection took hold

https://www.theregister.com/2020/10/06/ardonagh_group_ransomware/

加密挖掘蠕虫增加了 Linux 密码窃取功能

日期: 2020-10-05

等级: 高

作者: Sergiu Gatlan

标签: ['Docker', 'Monero', 'Password Stealing', 'Mimipy', 'Mimikatz', 'TeamTNT']

`TeamTNT`最近更新了密码挖掘设备，使其更容易通过网络传播其他的密码挖掘设备。虽然该组织主要以主动锁定 Docker 实例为目标，使用受损系统进行未经授权的 Monero（XMR）挖掘而闻名，但该组织现在改变了策略，将其加密劫持恶意软件升级为收集用户凭证。`Unit 42`的研究人员发现，`TeamTNT`正在努力增强其恶意软件的能力，这次是通过`mimipy`(支持 Windows/Linux/macOS)和`mimipenguin`(支持 Linux)增加内存密码抓取功能，这两款`Mimikatz`开源软件都是针对`NIX`桌面的。Unit 42 给这种蠕虫命名为 Black-T，它会收集在被攻击系统内存中找到的任何明文密码，并将其发送给 TeamTNT 的命令和控制服务器。

详情

Crypto-mining worm adds Linux password stealing capability

https://www.bleepingcomputer.com/news/security/crypto-mining-worm-adds-linux-password-stealing-capability/

第二次在野发现 UEFI rootkit

日期: 2020-10-05

等级: 高

作者: Sergiu Gatlan

标签: ['UEFI', 'MosacRegressor', 'rootkit', 'LoJax']

安全研究人员在围绕 2019 年针对两个非政府组织（NGO）的攻击展开的调查中发现了第二个在野使用的`UEFI rootkit`。 UEFI（统一可扩展固件接口）固件允许高度持久的恶意软件，因为它安装在焊接到计算机主板的 SPI 闪存中，因此无法通过重新安装 OS 或更换硬盘来摆脱它。 `UEFI bootkit`被发现它的卡巴斯基研究人员`Mark Lechtik`和`Igor Kuznetsov`称为`MosacRegressor`，是一个模块化、多阶段的恶意软件框架，被讲中文的黑客用于数据窃取和间谍活动。目前只知道另一个在野外使用的`UEFI bootkit`实例，即 2018 年由 ESET 发现的`rootkit LoJax`。`LoJax`是由讲俄语的`APT28`黑客组织在`legit LoJack`防盗软件中以补丁`UEFI`模块的形式注入的。攻击者通过注入多个可用于在目标设备上部署恶意软件的恶意模块来修改恶意 UEFI 固件映像。`MosaicRegressor`具有几个下载器，有时还有多个中间加载程序，其最终目标是在目标计算机上下载和执行恶意负载。

详情

MosaicRegressor: Second-ever UEFI rootkit found in the wild

https://www.bleepingcomputer.com/news/security/mosaicregressor-second-ever-uefi-rootkit-found-in-the-wild/

无文件恶意程序注入 Windows 错误报告服务

日期: 2020-10-07

等级: 高

作者:

标签: ['Malwarebytes', 'Vietnam', 'APT32', 'Inject', 'Phishing']

研究人员发现了一种新的攻击策略，即攻击者直接将无文件恶意软件注入 Windows 错误报告服务中，作为规避防御检测手段。这次攻击是以一个网络钓鱼邮件开始的，它使用的主题是"Your Right to Compensation"，邮件中包含一个 zip 文件，里面有一个标签为"Compensation manual.doc"的文件，文件说它是加密的，并要求受害者启用编辑功能。报告称，当这个过程完成后，受害者会被带到一个网站，在那里无文件恶意软件被加载到 Windows 错误报告系统中。

详情

Fileless Malware Injected in Windows Error Reporting Service

https://www.databreachtoday.com/fileless-malware-injected-in-windows-error-reporting-service-a-15129

一种被称为 SLOTHFULMEDIA 的新的远程木马

日期: 2020-10-05

等级: 中

作者:

标签: ['CISA', 'SLOTHFULMEDIA', 'Malware', 'Dropper', 'RAT']

美国国防部网络国家任务部队(CNMF)和国土安全部网络安全和基础设施安全局(CISA)发布了一份恶意软件分析报告，提供了一种名为 SLOTHFULMEDIA 的新型恶意软件的技术细节。与其他 MAR 分析一样，该报告提供了有关这一威胁的技术细节，包括妥协指标、应对行动建议以及预防感染的建议。"该示例是一个 dropper，在执行时会部署两个文件。

第一个是名为" mediaplayer.exe"的远程访问工具（RAT），该工具专门用于受害计算机系统的命令和控制（C2）。 分析确定了 RAT 具有终止进程，运行任意命令，进行屏幕截图，修改注册表以及修改受害者计算机上文件的能力。" 报告中写到。

详情

SLOTHFULMEDIA RAT, a new weapon in the arsenal of a sophisticated threat actor
https://securityaffairs.co/wordpress/109092/malware/slothfulmedia-rat-report.html

勒索软件威胁激增，Ryuk 约每周攻击 20 家公司

日期: 2020-10-06

等级: 中

作者: Ionut Ilascu

标签: ['Maze', 'Ryuk', 'REvil', 'Check Point', 'Ransomware', 'Malware']

监控勒索软件威胁的恶意软件研究人员注意到，与 2020 年前六个月相比，过去几个月此类攻击急剧增加。根据`Check Point`和`IBM Security X-Force`事件响应小组最近公布的数据，排在榜首的勒索软件有`Maze`、`Ryuk`和`REvil` (Sodinokibi)。两家公司都注意到，2020 年 6 月至 9 月，全球范围内的勒索软件事件激增，其中一些威胁比其他威胁更为活跃。来自`Check Point`的数据显示，2020 年第三季度，`Maze`和`Ryuk`是最常见的勒索软件家族，后者平均每周攻击 20 家公司。 根据检查点 2020 年 10 月 6 日的报告，`Ryuk`在 7 月份增加了活动，并主要关注医疗保健机构，这些机构已经承受了疫情带来的巨大压力，无法承受系统瘫痪的后果。

详情

Ransomware threat surge, Ryuk attacks about 20 orgs per week
https://www.bleepingcomputer.com/news/security/ransomware-threat-surge-ryuk-attacks-about-20-orgs-per-week/

勒索软件攻击健康科技公司，扰乱了 COVID-19 医学试验

日期: 2020-10-06

等级: 中

作者:

标签: ['eResearchTechnology', 'COVID-19', 'Ransomware', 'Medical Trials']

总部位于费城的医疗科技公司 eResearchTechnology（ERT）遭遇勒索软件攻击，但没有患者受到影响。几周前有报道称，德国一家名为杜塞尔多夫大学医院（University hospital Düsseldorf，UKD）的勒索软件袭击导致一名患者死亡。如今，总部位于费城的医疗科技公司 eResearchTechnology（ERT）透露，该公司遭到勒索软件攻击。该机构向医疗机构销售软件，用于开发测试和治疗，目前，该公司的软件正在用于创建并测试`COVID-19`疫苗。然而，勒索软件的攻击并没有破坏任何临床试验，而是干扰和减缓了一些试验。

详情

Ransomware attack on health tech firm disrupted COVID-19 medical trials
https://www.hackread.com/ransomware-attack-health-tech-firm-disrupted-covid-19-trials/

新的 HEH 僵尸网络可能会擦除磁盘

日期: 2020-10-07

等级: 中

作者:

标签: ['Netlab', 'HEH', 'Botnet', 'Wipes Devices']

来自中国科技巨头奇虎 360 网络安全部门`Netlab`的研究人员发现了一个新的僵尸网络，被追踪为 HEH，其中包含清除被感染系统（如路由器、物联网设备和服务器）的所有数据的代码。它是用 Go 开源编程语言编写的，以 SSH 端口（23 和 2323）为目标，通过发起暴力攻击，将 SSH 端口（23 和 2323）暴露在网络上

详情

New HEH botnet wipes devices potentially bricking them
https://securityaffairs.co/wordpress/109186/hacking/heh-botnet.html

Software AG 受勒索软件的攻击：攻击者泄露了工作人员的护照

日期: 2020-10-09

等级: 中

作者: Gareth Corfield

标签: ['Software AG', 'German', 'Ransomware', 'Passports', 'Leaked']

德国软件公司(`Software AG`)似乎受到了勒索软件的攻击，这家德国 IT 巨头称该国股市受到了恶意软件攻击的影响。恶意软件攻击的消息迟迟未能渗透到盎格鲁文化圈(`Anglosphere`)，尽管德国通讯社新闻专线(`newswire`)昨日晚间发表了一份简短报告，并在一些不知名的投资网站上转载。该报告还说，Software AG 服务器和员工笔记本的数据被下载。`El Reg`看到的攻击者勒索网页的屏幕截图显示了员工护照、内部账单以及一个基于 windows 系统的内部目录。文件夹的名称表明，内容可能涉及在美国和加拿大的 Software AG 客户。

详情

Software AG hit with ransomware: Crooks leak staffers' passports, want millions for stolen files
https://www.theregister.com/2020/10/09/software_ag_ransomware/

新的 MalLocker.B 勒索软件能显示赎金笔记

日期: 2020-10-09

等级: 中

作者:

标签: ['Microsoft', 'Android', 'Home', 'MalLocker.B', 'Ransomware', '']

微软发现了一种名为 MalLocker.B 的 Amdroid 勒索软件。当用户按下 Home 键时激活。微软(Microsoft)的研究人员发现，这种新的安卓勒索软件滥用了来电通知和锁定受害者手机屏幕的 Home 键背后的机制。 AndroidOS 的 MalLocker.B 通过受污染的 Android 应用程序分发，可在在线论坛和第三方网站上下载。 新的变体还设法规避了许多可用的保护，针对安全解决方案的检测率较低。为了避免感染 MalLocker.B 和类似的恶意软件，建议用户避免从第三方商店或论坛安装 Android 应用程序。

详情

New MalLocker.B ransomware displays ransom note in innovative way
https://securityaffairs.co/wordpress/109263/malware/mallocker-b-android-ransomware.html

嘉年华证实数据泄露是 8 月勒索软件攻击的结果

日期: 2020-10-10

等级: 中

作者:

标签: ['Carnival Corporation', 'Data Breach', 'Ransomware', 'Citrix']

全球最大的邮轮运营商嘉年华公司（Carnival Corporation）证实，8 月份勒索软件攻击导致数据泄露。勒索软件运营商在攻击中窃取了客户、员工和船员的个人信息。嘉年华公司是一家英美邮轮运营商，目前是世界上最大的旅游休闲公司，拥有 10 个邮轮品牌的 100 多艘船只。

详情

Carnival confirms data breach as a result of the August ransomware attack
https://securityaffairs.co/wordpress/109308/data-breach/carnival-data-breach.html

泰勒科技公司最终向勒索软件支付了赎金

日期: 2020-10-11

等级: 中

作者:

标签: ['Tyler Technologies', 'Ransom', 'Decryption Key']

泰勒科技公司最终决定支付赎金以获得解密密钥，恢复在最近一次勒索软件攻击中加密的文件。泰勒技术公司是美国公共部门最大的软件供应商。9 月底，该公司披露了一起勒索软件攻击事件，其客户报告称在他们的网络上发现了可疑的登录和以前看不到的远程访问工具。勒索软件攻击事件发生在 9 月 23 日，威胁者攻破了该公司的网络并部署了该恶意软件。

详情

Tyler Technologies finally paid the ransom to receive the decryption key
https://securityaffairs.co/wordpress/109334/cyber-crime/tyler-technologies-paid-ransom.html

不要低估 FONIX 勒索软件服务

日期: 2020-10-11

等级: 中

作者:

标签: ['FONIX', 'Ransomware', 'RaaS', 'Windows']

FONIX 是一个相对较新的勒索软件服务(RaaS)，由 Sentinel 实验室的研究人员分析，它的运营商以前专门从事二进制密码，封装器的开发。FONIX 于 2020 年 7 月首次出现在威胁领域，幸运的是，与此威胁相关的感染数量仍然很小。 专家指出，勒索软件的作者不需要支付费用就可以成为该服务的附属公司，运营商只保留其附属网络中任何赎金的一部分。专家认为，然而，如果安全公司和当局低估了 FONIX RaaS，它会很快变得猖獗。

详情

Underestimating the FONIX - Ransomware as a Service could be an error
https://securityaffairs.co/wordpress/109369/cyber-crime/fonix-raas.html

CISA 警告美国政府机构遭受 Emotet 攻击

日期: 2020-10-07

等级: 中

作者:

标签: ['CISA', 'US', 'Emotet', 'Phishing']

`网络安全与基础设施安全局（CISA）`发布警报，警告称，自 8 月以来，针对美国多个州和地方政府的 Emotet 攻击激增。在此期间，CISA 的入侵检测系统已经检测到大约 16000 个与 Emotet 活动相关的警报。据专家称，Emotet 攻击的目标是美国政府实体。

详情

CISA alert warns of Emotet attacks on US govt entities
https://securityaffairs.co/wordpress/109166/malware/cisa-alert-emotet.html

相关安全建议

1. 各主机安装 EDR 产品，及时检测威胁
2. 及时对系统及各个服务组件进行版本升级和补丁更新
3. 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
4. 及时备份数据并确保数据安全
5. 明确每个服务功能的角色访问权限
6. 条件允许的情况下，设置主机访问白名单
7. 网段之间进行隔离，避免造成大规模感染

(二) 数据安全

澳大利亚社交新闻平台泄露 8 万条用户记录

日期: 2020-10-05

等级: 高

作者:

标签: ['Cybernews', 'Australian', 'Snewpit', 'Bucket', 'Amazon Web Services']

网络新闻调查小组发现了一个暴露的数据`bucket`，属于澳大利亚新闻分享平台`Snewpit`。这个不安全的`bucket`包含近`80000`条用户记录，包括用户名、全名、电子邮件地址和个人资料图片。包含这些记录的文件存储在一个可公开访问的 `Amazon Web

Services(AWS)` 服务器上，这意味着任何直接访问这些文件的人都可以访问并下载这些未公开的数据。9 月 24 日，`Snewpit bucket`中的敏感文件已被公司保护，不再可访问。

详情

Australian social news platform leaks 80,000 user records
https://securityaffairs.co/wordpress/109108/data-breach/snewpit-leaks-80000-records.html

阿联酋国际航空公司的数据泄露至暗网

日期: 2020-10-08

等级: 中

作者:

标签: ['Airlink International UAE', 'Dark Web', 'Leaked Data', 'Kelvinsectteam']

网络安全研究人员发现，一名黑客在暗网的两个平台上免费共享`阿联酋国际航空公司`的泄露数据。暗网上数据的可用性可能给组织带来严重的风险，攻击者可以利用这些数据进行多次恶意攻击。`Airlink International U.A.E.`是满足任何旅行和物流要求的领先公司。它有 200 多名员工，收入约 2.5 亿美元。数据泄漏是由一个错误配置的服务器造成的，该服务器包含 60 个目录，每个目录大约有 5000 个文件。

详情

Data from Airlink International UAE leaked on multiple dark web forums
https://securityaffairs.co/wordpress/109237/data-breach/airlink-international-uae-data-leak.html

相关安全建议

1. 严格控制数据访问权限
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. 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

(三) 网络攻击

美国公司 1500 万美元网络抢劫案剖析

日期: 2020-10-06

等级: 高

作者: Ionut Ilascu

标签: ['US', 'Email', 'Fraudsters']

经验丰富的网络攻击者通过邮件诈骗从一家美国公司偷走了 1500 万美元，这起诈骗案件耗时 2 个月。这名网络罪犯在获取了一笔商业交易的电子邮件对话后，精准地执行了他们

的计划。他们在交易中插足，转移了钱，并得以将偷窃行为隐瞒了足够长的时间，从而拿到了钱。尽管研究人员调查了一个受害者的事件，但他们发现的线索表明，建筑、零售、金融和法律行业的数十家企业都在他们的目标名单上。在确定目标后，他们花了大约两周的时间试图访问电子邮件账户。

详情

The anatomy of a $15 million cyber heist on a US company

https://www.bleepingcomputer.com/news/security/the-anatomy-of-a-15-million-cyber-heist-on-a-us-company/

黑客从瑞士大学窃取了 6 位数的金额

日期: 2020-10-05

等级: 高

作者:

标签: ['Swiss', 'the University of Basel', 'Salary', 'Phishing', 'Attack']

黑客已经窃取了包括巴塞尔大学在内的几家瑞士大学的员工薪水。瑞士大学校长会议秘书长玛蒂娜·维斯解释说，根据可靠信息，瑞士有几所大学受到了影响。黑客对瑞士大学实施鱼叉式网络钓鱼攻击，试图诱骗员工提供他们的访问数据。 据《SonntagsZeitung》报道，巴塞尔检察官办公室证实，黑客侵入了大学的系统，然后威胁者通过更改受益人账户劫持了该员工的工资转账。黑客窃取了 6 位数的金额，并立即将资金转移到国外。《SonntagsZeitung》还补充说，黑客试图入侵苏黎世大学，但该大学的员工认识到网络钓鱼的企图，将其击退。

详情

Hackers stole a six-figure amount from Swiss universities

https://securityaffairs.co/wordpress/109100/hacking/swiss-universities-hacked.html

新一波的网络钓鱼电子邮件以选举为诱饵

日期: 2020-10-05

等级: 高

作者:

标签: ['Proofpoint', 'Phishing', 'Election', 'Emotet', 'Botnet']

安全研究人员警告说，新一轮的网络钓鱼电子邮件将产生一批与选举有关的诱饵，这些诱饵旨在让用户点击，从而方便散布`Emotet`僵尸网络或获取用户凭证。安全公司`Proofpoint`已经发现了数千封恶意邮件，这些邮件旨在传播来自民主党全国委员会的欺骗信息。同时，`KnowBe4`还发现了另一个欺骗美国选举援助委员会的网络钓鱼活动，该活动旨在获取凭据。`Proofpoint`称，最近的`Emotet`活动始于 10 月 1 日，这是`Emotet`背后的团伙`TA542`首次从政治角度进行网络钓鱼。

详情

Fresh Wave of Phishing Emails Use Election as a Lure

https://www.databreachtoday.com/fresh-wave-phishing-emails-use-election-as-lure-a-15117

国际海事组织（IMO）遭受网络攻击

日期: 2020-10-06

等级: 高

作者:

标签: ['The United Nations International Maritime Organization', 'IMO', 'Cyber Attack', 'IT System']

联合国国际海事组织（IMO）披露了一次网络攻击。据该机构称，9 月 30 日，第一次网络攻击后，组织的 IT 系统遭到破坏，海事组织的一些网络服务无法使用。受影响的系统包括：海事组织公共网站和其他基于网络的服务。不过包括电子邮件系统等其他内部和外部协作平台工作正常。网站 www.imo.org 已于 10 月 2 日恢复访问。

详情

A sophisticated cyberattack hit the International Maritime Organization (IMO)

https://securityaffairs.co/wordpress/109154/hacking/international-maritime-organization-imo-cyberattack.html

外卖服务 Chowbus 遭黑客攻击，超过 40 万名客户受到影响

日期: 2020-10-08

等级: 高

作者:

标签: ['Chowbus', 'Food Delivery', 'Stole Data', 'Database', 'Cyber Attack']

广受欢迎的亚洲外卖平台`Chowbus`遭到黑客攻击，黑客声称窃取了公司包含客户数据的整个数据库，攻击者将这些数据导出到一系列 Excel（CSV）文件中，并向客户发送了这些档案的链接。暴露的数据包括顾客姓名、电子邮件地址、电话号码、地址（城市、州、邮政编码）、外卖费用和 Chowbus 合作伙伴餐厅的地址。

详情

Food Delivery Service Chowbus hacked, more than 400K customer impacted

https://securityaffairs.co/wordpress/109224/data-breach/food-delivery-service-chowbus-hack.html

黑客团伙现利用严重的 Windows 漏洞进行攻击

日期: 2020-10-09

等级: 高

作者: Ionut Ilascu

标签: ['Microsoft', 'ZeroLogon', 'MuddyWater', 'TA505', 'CVE-2020-1472']

微软警告称，网络犯罪分子已经开始在他们的攻击中加入针对`ZeroLogon`漏洞的开发代码。该警告是在微软注意到网络间谍组织`MuddyWater` (SeedWorm)在 9 月下半月持续不断的攻击之后发布的。这一次，威胁者是 TA505，一个对其攻击的受害者不分皂白的对手，其历史始于 2014 年发布的 Dridex 银行木马。多年来，TA505 一直在进行攻击，传播各种恶意软件，从后门到勒索软件。最近，这个组织的入侵之后，又部署了 Clop 勒索软件，比如去年马斯特里赫特大学（Maastricht University）的袭击，导致支付了 30 比特币（约 22 万美元）的赎金。

详情

Ransomware gang now using critical Windows flaw in attacks

https://www.bleepingcomputer.com/news/security/ransomware-gang-now-using-critical-windows-flaw-in-attacks/

国土安全部：不明黑客袭击了美国人口普查局网络

日期: 2020-10-09

等级: 高

作者: Sergiu Gatlan

标签: ['US Census', 'DHS', 'Attack']

美国国土安全部在 2020 年 10 月早些时候发布的第一份国土威胁评估报告中称，2019 年美国人口普查网络遭到了不明威胁分子的袭击。 美国人口普查局是美国联邦政府最大的统计机构，负责收集有关美国经济和人口的统计数据。 然后，联邦政府利用这些数据，每年将超过 6750 亿美元的联邦基金分配给部落、地方和州政府。国土安全部说，针对美国用于支持 2020 年美国总统大选以及 2020 年美国人口普查的基础设施，国家和非国家的袭击者都可能试图破坏。

详情

DHS: Unknown hackers targeted the US Census Bureau network

https://www.bleepingcomputer.com/news/security/dhs-unknown-hackers-targeted-the-us-census-bureau-network/

基于 Mirai 的 IoT 木马传播了两个 0day 漏洞

日期: 2020-10-05

等级: 中

作者:

标签: ['Netlab', 'Tenda', 'RAT', 'Ttint', 'DDoS']

`Netlab`发现一个新的`IoT`僵尸网络，其利用`Tenda`路由器的两个 0day 漏洞，安装远程访问特洛伊木马（`RAT`）。被称为`Ttint`的僵尸网络自 2019 年 11 月以来一直活跃，除了`DDoS`功能外，它还包括 12 个远程访问功能。攻击者利用`Tenda`路由器的 0day 漏洞（CVE-2018-14558、CVE-2020-10987）分发 Ttint 样本。基于`Mirai`代码的`Tint`远程访问特洛伊木马，包括 10 条`Mirai DDoS`攻击指令和 12 条控制指令，如路由器设备的`Socket5`代理、篡改路由器`DNS`、设置`iptables`、执行自定义系统命令。

详情

A New Mirai based IoT RAT Spreading Through 2 0-day Vulnerabilities

https://gbhackers.com/ttint-iot-botnet/

Fullz House 入侵 Boom!的网站

日期: 2020-10-06

等级: 中

作者:

标签: ['Fullz House', 'Mobile', 'Boom!', 'E-skimer']

信用卡掠夺组织`Fullz House`破坏了美国移动虚拟网络运营商（MVNO）`Boom!`的网站。Boom!移动公司为其客户提供后付费和预付费的无线服务计划，使他们能够使用美国最大

的蜂窝网络（包括 AT&T，T-Mobile 和 Verizon）的线路。Fullz House 的黑客在 Boom! 网站中注入了一个 e-skimer，不幸的是，恶意软件尚未被删除。

详情

Fullz House hacked the website of Boom! Mobile provider to steal credit cards
https://securityaffairs.co/wordpress/109144/malware/boom-mobile-e-skimmer.html

Wisepay 的“停机”源于食堂支付业务对入侵者攻击的阻止

日期: 2020-10-07

等级: 中

作者: Gareth Corfield

标签: ['UK', 'Wisepay', 'Cashless Payments', 'Outage', 'Pre-emptive']

英国无现金校园支付公司 Wisepay 发现有人恶意欺骗其信用卡支付页面，故将相关网站关闭。这家总部位于汉普郡的公司自称“允许家长和监护人向他们（孩子）的学校或大学进行在线无现金支付”，不久前该公司表示，其网站“已停止维护”。Wisepay 发言人解释，“停机”是一个先发制人的举动，目的是阻止身份不明的攻击者继续进行“网址操纵”。

详情

Wisepay 'outage' is actually the school meal payments biz trying to stop an intruder from stealing customer card details
https://www.theregister.com/2020/10/07/wisepay_outage_was_cyber_attack/

Comcast 遥控器可被入侵用于监听对话

日期: 2020-10-07

等级: 中

作者: Ionut Ilascu

标签: ['Comcast', 'XR11', 'Microsoft', 'Remotes', 'IOT', 'WarezThe Remote']

安全研究人员分析了`Comcast`的 XR11 Xfinity 语音遥控器，发现了一种无需物理访问或用户交互就能将其变成监听设备的方法。与普通的红外线遥控器不同，微软 Edge 公司的 XR11 采用了一种新的“网络捕捉”情景，它依靠射频与有线机顶盒进行通信，并配有内置麦克风，可以进行语音命令，在美国各地，有超过 1800 万个家庭中部署了该设备。

详情

Comcast cable remotes hacked to snoop on conversations
https://www.bleepingcomputer.com/news/security/comcast-cable-remotes-hacked-to-snoop-on-conversations/

WordPress 漏洞为 Zerologon 攻击提供通道

日期: 2020-10-07

等级: 中

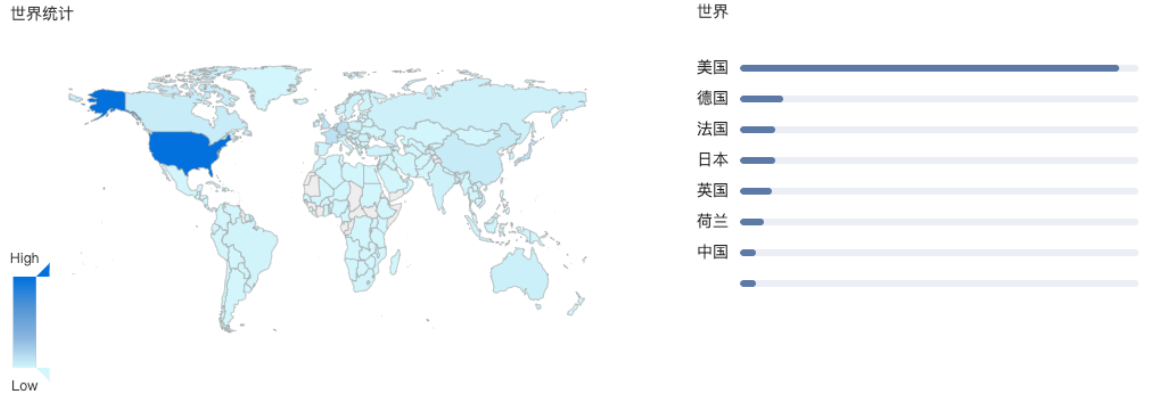
作者:

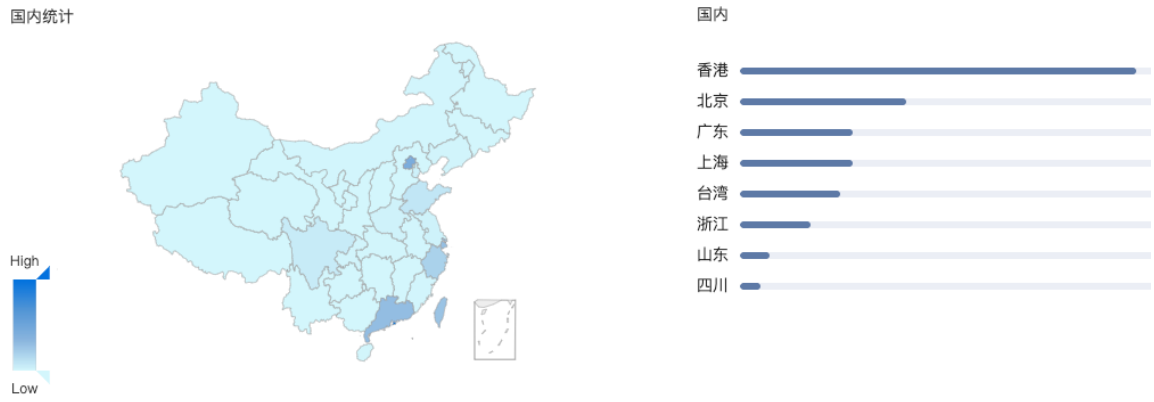
标签: ['WordPress', 'Zerologon', 'File-Manager Plugin', 'CVE-2020-25213', 'CVE-2020-1472']

不久前，Zerologon（CVE-2020-1472）成为全球的热门话题，想要利用这个漏洞的前提条件是能够连上目标域控。为了利用这个漏洞，黑客开始将其于 wordpress `File-

Manager`插件中的漏洞–CVE-2020-25213 结合使用，该漏洞允许在服务器端执行任意代码（RCE 漏洞）。攻击者通过`CVE-2020-25213`获得服务器权限之后，将建立代理隧道，并尝试执行 Zerologon 攻击。

目前 WordPress 的具体分布如下图，数据来自于 360 QUAKE





详情

Using a WordPress flaw to leverage Zerologon vulnerability and attack companies' Domain Controllers

https://securityaffairs.co/wordpress/109175/hacking/zerologon-dc-hack.html

黑客组织出售间谍和虚假新闻服务

日期: 2020-10-08

等级: 中

作者:

标签: ['Bahamut', 'BlackBerry', 'Espionage', 'Fake News Websites', 'Phishing']

安全研究人员称，一个名为`Bahamut`的黑客组织将其间谍和辟谣服务出租给出价最高的人，目标是中东和南亚的非营利组织和外交官。研究人员发现了`Bahamut`创建的几个假新闻网站，目的是推送造谣内容。他们还发现了一个网络钓鱼设施以及安装在 google play 和苹果应用商店中的恶意应用程序，这些应用程序用于针对特定的受害者和组织，由于该组织的目标不同意，黑客很可能将这项服务卖给出价最高的人。

详情

Hack-For-Hire Group Wages Espionage, Fake News Campaigns

https://www.databreachtoday.com/hack-for-hire-group-wages-espionage-fake-news-campaigns-a-15139

亚马逊黄金日，网络钓鱼和欺诈攻击激增

日期: 2020-10-08

等级: 中

作者:

标签: ['Amazon', 'Prime Day', 'Phishing', 'Malicious Websites ']

网络犯罪分子正在利用亚马逊针对订阅者的年度折扣购物活动"黄金日"。研究人员警告说，最近欺诈利用亚马逊品牌的网络钓鱼和恶意网站激增。根据一份 2020 年 10 月 8 日发布的报告报道，自 8 月份以来，每月使用亚马逊品牌创建的钓鱼和欺诈网站数量激增，这是自 3 月份疫情以来最显著的一次。研究人员分析了数以亿计的网页，以追踪使用亚马逊品牌和标识的新钓鱼和欺诈网站的数量。研究显示，威胁行为者利用亚马逊的特点和消费者行为，试图引诱网上购物者进入欺诈网站，窃取他们的凭证、财务信息和其他敏感数据。

详情

Amazon Prime Day Spurs Spike in Phishing, Fraud Attacks

https://threatpost.com/amazon-prime-day-spurs-spike-in-phishing-fraud-attacks/159960/

Fitbit gallery 可用于分发恶意应用程序

日期: 2020-10-09

等级: 中

作者: Ionut Ilascu

标签: ['Fitbit Gallery', 'Malicious Apps', 'Upload', 'Fitness']

一位安全研究人员发现，针对 Fitbit 设备的恶意应用程序可以上传到合法的 Fitbit 域，用户可以通过私有链接安装它们。通过一些社会工程，黑客可以利用这一点，诱骗用户添加应用程序，以获取（从 Fitbit 设备传感器或手机收集的）丰富的个人信息。Fitbit 开发健身活动跟踪可穿戴设备（智能手表、腕带），为用户提供诸如步行或爬台阶数、心率、睡眠质量以及活动历史记录等指标。Fitbit 及其开发者社区的各种移动应用程序（健康、游戏、音乐、实用程序）都在 Fitbit 官方图库中发布。

详情

Fitbit gallery can be used to distribute malicious apps

https://www.bleepingcomputer.com/news/security/fitbit-gallery-can-be-used-to-distribute-malicious-apps/

相关安全建议

1. 积极开展外网渗透测试工作，提前发现系统问题

2. 域名解析使用 CDN
3. 统一 web 页面报错信息，避免暴露敏感信息
4. 减少外网资源和不相关的业务，降低被攻击的风险
5. 注重内部员工安全培训
6. 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
7. 严格做好 http 报文过滤
8. 做好产品自动告警措施
9. 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。

(四) 其他事件

流行的反病毒软件漏洞让攻击者可以升级特权

日期: 2020-10-06

等级: 中

作者:

标签: ['Windows', 'Vulnerabilities', 'Antivirus', 'DACLs', 'ProgramData']

来自 CyberARK 的安全研究人员发现了反恶意软件的安全漏洞，该软件允许攻击者升级受感染机器的权限。与其他应用程序相比，反恶意软件的漏洞带来了更高的风险，因为它具有高权限，使得攻击者能够以更高的权限运行恶意软件。根据研究人员的说法，这个`bug`的主要原因是`C:\ProgramData`目录的默认`DACLs`。在应用程序用于存储数据的 Windows 上。此进程未绑定到特定用户，任何用户都对`ProgramData`拥有读或写权限，而不是当前登录用户可以访问的`%LocalAppData%`。因此，如果一个非特权进程在`ProgramData`中创建了一个以后由特权进程使用的目录，那么可能会遇到安全问题。

详情

Flaws in Popular Antivirus Softwares Let Attackers to Escalate Privileges
https://gbhackers.com/flaws-in-popular-antivirus-softwares-let-attackers-to-escalate-privileges/

Bugcrowd 在 2020 年末选出最值得关注的 Bugs

日期: 2020-10-08

等级: 中

作者:

标签: ['Bugcrowd', 'Bugs', 'OWASP']

Bugcrowd 在 10 月 7 日发布了一篇博客，其中研究人员预测了 2020 年最后一个季度将会出现的更多的 bug。它们从 OWASP 基金会的前 10 个列表中的主要 bug 类别开始，即跨站点脚本、SQL 注入、各种身份验证流的不安全实现、敏感数据暴露、窃取敏感令牌的开放重定向以及访问控制问题。

详情

Bugcrowd picks top bugs to watch for in late 2020

https://www.scmagazine.com/home/security-news/bugcrowd-picks-top-bugs-to-watch-for-in-late-2020/

在苹果各种服务中发现 55 个安全漏洞

日期: 2020-10-09

等级: 中

作者:

标签: ['Apple', 'Vulnerabilities', 'XSS', 'RCE', 'Ethical Hackers']

一个由 5 名白帽黑客组成的团队在苹果的一系列服务中发现了总共 55 个漏洞，其中近 12 个漏洞被评为严重漏洞。这些被揭露的安全漏洞是在三个月内被发现并迅速修复的，根据苹果的窃听奖励计划，这些"白帽"黑客总共获得了 28.85 万美元的奖励。不少于 11 个漏洞被认为是严重的，29 个被认为是高危的，13 个被归类为中危，剩下的 2 个被列为低危。为了评估漏洞的严重性，团队使用了通用漏洞评分系统（CVSS）和他们对这些漏洞将产生多大的业务相关影响的知识。在这些漏洞中，有两个漏洞尤为突出：一个是远程代码执行（RCE）漏洞，它可能会让苹果杰出教育者计划（Apple Distinguished Educators）程序遭到全面破坏；另一个是一个可让威胁参与者窃取 iCloud 数据的可修复存储跨站点脚本（XSS）漏洞。

详情

55 security flaws found in various Apple services

https://www.welivesecurity.com/2020/10/09/55-security-flaws-found-various-apple-services/

Facebook 首次推出漏洞赏金

日期: 2020-10-09

等级: 中

作者:

标签: ['Facebook', 'Bug Bounty', 'Hacker Plus']

`Facebook`推出了一项忠诚度计划，旨在进一步激励研究人员发现其平台的漏洞。该忠诚计划称为" Hacker Plus"，还提供赏金奖励，让研究人员可以对更多产品和功能进行压力测试，并邀请他们参加 Facebook 年度活动。Facebook 的安全工程经理`Dan Gurfinkel`在 2020 年 10 月 9 日的帖子中说：" Hacker Plus 旨在帮助参与`facebook`的漏洞赏金计划的研究人员建立社区，此外还鼓励质量报告。"

详情

Facebook Debuts Bug Bounty 'Loyalty Program'

https://threatpost.com/facebook-bug-bounty-loyalty-program/159993/

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