安全事件周报

安全事件周报 (04.19-4.25)

360CERT
北京奇虎科技有限公司 | 2021-04-26

报告信息

报告名称	安全事件周报（04.19-4.25）		
报告类型	安全事件周报	报告编号	B6-2021-042601
报告版本	1.0	报告日期	2021-04-26
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	2021-04-26	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 15 项

话题集中在`恶意软件`、`网络攻击`方面，涉及的组织有：`Apple`、`Passwordstate`、`Codecov`、`Homebrew`等。供应链攻击再起，各厂商注意防护。

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**
REvil 窃取苹果产品蓝图并向其勒索	★★★★★
通过 Xcode 项目传播的恶意软件现在针对苹果的 Mac	★★★★
黑客假冒微软商店、Spotify 网站来传播窃取信息的恶意软件	★★★★
Qlocker 勒索软件攻击使用 7zip 加密 QNAP 设备	★★★★
"ToxicEye"恶意软件在 Telegram 平台中泛滥	★★★★
Joker 恶意软件的目标是更多的 Android 设备	★★★★
黑客入侵安卓手机来模仿联网电视产品	★★★★
网络攻击	**等级**
Passwordstate 密码管理器被用于供应链攻击	★★★★★
Codecov 受到供应链攻击	★★★★
Lazarus APT 黑客现在使用 BMP 图像隐藏 RAT 恶意软件	★★★★
朝鲜黑客利用网络浏览器盗取比特币	★★★★
美国国家安全局发布俄罗斯黑客利用的 5 大漏洞	★★★★
黑客利用虚假的 Facebook 广告进行网络钓鱼	★★★★
其他事件	**等级**
黑客们正积极瞄准 VPN 设备漏洞	★★★★
Homebrew 远程代码执行漏洞披露	★★★★

三、 事件详情

(一) 恶意程序

REvil 窃取苹果产品蓝图并向其勒索

日期: 2021-04-20

等级: 高

来源: Sergiu Gatlan

标签: ['REvil', 'Apple']

Quanta 是一家总部位于台湾的原始设计制造商（ODM），并且是 Apple Watch，Apple Macbook Air 和 Apple Macbook Pro 的制造商。REvil 勒索软件团伙声称他们通过该公司窃取了苹果的产品蓝图，并要求苹果公司在 5 月 1 日之前支付赎金，以防止其窃取的数据被泄露。根据 Tor 付款页面，Quanta 或者苹果必须在 4 月 27 日之前支付 5,000 万美元，或者在倒计时结束后支付 1 亿美元，否则相关敏感数据将会被泄露。

详情

REvil gang tries to extort Apple, threatens to sell stolen blueprints

https://www.bleepingcomputer.com/news/security/revil-gang-tries-to-extort-apple-threatens-to-sell-stolen-blueprints/

通过 Xcode 项目传播的恶意软件现在针对苹果的 Mac

日期: 2021-04-19

等级: 高

来源: The Hacker News

标签: ['Mac', 'Xcode', 'Apple', 'M1']

一个针对 Xcode 开发者的 Mac 恶意软件已经重构，以增加对苹果新 M1 芯片的支持，并扩展其功能，从加密货币应用程序中窃取机密信息。XCSSET 在 2020 年 8 月被发现通过修改后的 Xcode IDE 项目进行传播。在构建时，这些项目被配置为执行有效负载。

详情

Malware That Spreads Via Xcode Projects Now Targeting Apple's M1

https://thehackernews.com/2021/04/malware-spreads-via-xcode-projects-now.html

黑客假冒微软商店、Spotify 网站来传播窃取信息的恶意软件

日期: 2021-04-20

等级: 高

来源: Lawrence Abrams

标签: ['Spotify', 'Info-stealing', 'Fake Site']

攻击者正模仿微软商店、Spotify 和一个在线文档转换器的网站，并通过这些虚假网站散布恶意软件，窃取保存在 web 浏览器中的信用卡和密码。攻击是通过恶意广告进行的，这些广告宣传合法的应用程序。例如，此攻击中使用的一个广告推广了一个在线象棋应用程

序，然而，当用户点击广告时，他们会被带到一个假冒的微软商店页面，上面有一个假冒的"Xchess3"在线象棋应用程序，而该程序就是精心构造的恶意软件。

详情

Fake Microsoft Store, Spotify sites spread info-stealing malware

https://www.bleepingcomputer.com/news/security/fake-microsoft-store-spotify-sites-spread-info-stealing-malware/

Qlocker 勒索软件攻击使用 7zip 加密 QNAP 设备

日期: 2021-04-21

等级: 高

来源: Lawrence Abrams

标签: ['QNAP', 'Qlocker']

一场针对全球 QNAP 设备的大规模勒索活动正在进行。这个勒索软件被称为 Qlocker，并于 2021 年 4 月 19 日开始针对 QNAP 设备。攻击者使用 7-zip 将 QNAP 设备上的文件移动到受密码保护的加密档案中。当文件被锁定时，QNAP 资源监视器将显示许多"7z"进程，这些进程是 7zip 命令行可执行文件。勒索软件完成后，QNAP 设备的文件将存储在受密码保护的 7-zip 档案中，以.7z 扩展名结尾。

详情

Massive Qlocker ransomware attack uses 7zip to encrypt QNAP devices

https://www.bleepingcomputer.com/news/security/massive-qlocker-ransomware-attack-uses-7zip-to-encrypt-qnap-devices/

"ToxicEye"恶意软件在 Telegram 平台中泛滥

日期: 2021-04-22

等级: 高

来源: Elizabeth Montalbano

标签: ['Telegram', 'ToxicEye']

一项新的研究发现，黑客正在利用广受欢迎的电报信息应用程序，将其代码嵌入名为 ToxicEye 的远程访问特洛伊木马（RAT）中。ToxicEye 恶意软件可以接管文件系统，安装勒索软件，并从受害者的电脑中泄露数据。

详情

Telegram Platform Abused in 'ToxicEye' Malware Campaigns

https://threatpost.com/telegram-toxiceye-malware/165543/

Joker 恶意软件的目标是更多的 Android 设备

日期: 2021-04-22

等级: 高

来源: Akshaya Asokan

标签: ['Android', 'Huawei']

据安全公司 Doctor Web 称，Joker 恶意软件通过华为官方应用商店 AppGallery 中的恶意应用锁定了全球超过 50 万台 Android 设备。这些恶意小丑应用程序已被下载 53.8 万次。

一旦安装在 Android 设备上，攻击者就可以使用恶意软件一次向设备订阅多达 10 个高级移动服务。攻击者拥有受害者在不知情的情况下订阅的海外"高级服务"，然后通过受害者的电话账单收取移动服务费。一旦安装了恶意应用程序，当用户与其交互时，特洛伊木马会连接到攻击者的命令和控制服务器，并下载其他组件。下载的组件会自动为 Android 设备用户订阅高级移动服务。

详情

Joker Malware Targets More Android Devices
https://www.databreachtoday.com/joker-malware-targets-more-android-devices-a-16450

黑客入侵安卓手机来模仿联网电视产品

日期: 2021-04-24

等级: 高

来源: Deeba Ahmed

标签: ['Android', 'Pareto', 'Botnet']

网络安全公司 Human Security（原 White Ops）发现了一个高度复杂的基于僵尸网络的欺诈行动，黑客成功感染了 100 多万台 Android 移动设备，来窃取了广告商的收入。这些被入侵的设备被用来通过电视广告进行诈骗，模仿电视产品的恶意软件被植入 android 设备中，以生成虚假的广告浏览量。据研究人员称，僵尸网络模拟超过 6000 个 CTV 应用程序，每天至少提供 6.5 亿条广告请求。

详情

Hacked Android phones mimicked connected TV products to generate fake ad views
https://www.hackread.com/hacked-android-phones-connected-tv-products-malware/

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. 做好资产收集整理工作，关闭不必要且有风险的外网端口和服务，及时发现外网问题
3. 及时对系统及各个服务组件进行版本升级和补丁更新
4. 包括浏览器、邮件客户端、vpn、远程桌面等在内的个人应用程序，应及时更新到最新版本
5. 各主机安装 EDR 产品，及时检测威胁
6. 注重内部员工安全培训
7. 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
8. 勒索中招后，应及时断网，并第一时间联系安全部门或公司进行应急处理

(二) 网络攻击

Passwordstate 密码管理器被用于供应链攻击

日期: 2021-04-23

等级: 高

来源: Sergiu Gatlan

标签: ['ClickStudios', 'Passwordstate']

Passwordstate 是一种本地密码管理解决方案，已被全球 29,000 家公司的 370,000 多名安全和 IT 专业人员使用。它的客户名单中有许多 500 强企业，包括政府，国防，金融，航空，零售，汽车，医疗保健，法律和媒体。Passwordstate 密码管理器背后的公司 Click Studios 通知客户，攻击者破坏了该应用程序的更新机制，在破坏其网络后以供应链攻击的形式传播恶意软件。在 4 月 20 日至 4 月 22 日期间下载了升级程序的客户可能已经中招。

详情

Passwordstate password manager hacked in supply chain attack

https://www.bleepingcomputer.com/news/security/passwordstate-password-manager-hacked-in-supply-chain-attack/

Codecov 受到供应链攻击

日期: 2021-04-19

等级: 高

来源: Pierluigi Paganini

标签: ['Codecov', 'Bash']

软件公司 Codecov 遭遇网络攻击，攻击者破坏了其一个工具的供应链，此前攻击者破坏了其基础架构，以将凭据收集器代码注入其名为 Bash Uploader 的工具中。

详情

Codecov was a victim of a supply chain attack

https://securityaffairs.co/wordpress/116967/hacking/codecov-supply-chain-attack.html

Lazarus APT 黑客现在使用 BMP 图像隐藏 RAT 恶意软件

日期: 2021-04-19

等级: 高

来源: The Hacker News

标签: ['North Korean', 'Malwarebytes', 'Lazarus']

2021 年 4 月 13 日，malwarebytes 发现了 Lazarus 针对韩国的攻击，疑似通过分发附带恶意文档的钓鱼邮件作为初始攻击媒介，有趣的是，攻击者将恶意 HTA 对象嵌入到 BMP 文件中以释放 RAT Loader，完成后续攻击。
malwarebytes 在报告中对本次攻击的样本及过程进行了分析。报告地址：
https://blog.malwarebytes.com/malwarebytes-news/2021/04/lazarus-apt-conceals-malicious-code-within-bmp-file-to-drop-its-rat/

详情

Lazarus APT Hackers are now using BMP images to hide RAT malware

https://thehackernews.com/2021/04/lazarus-apt-hackers-are-now-using-bmp.html

朝鲜黑客利用网络浏览器盗取比特币

日期: 2021-04-20

等级: 高

来源: Ionut Ilascu

标签: ['Lazarus', 'JavaScript', 'Bitcoin']

2020 年 7 月，Sansec 发表了一篇攻击者使用 JavaScript 嗅探器（JS-sniffers）对美国和欧洲在线商店进行攻击的文章。文章中，研究人员将" clientToken ="攻击活动归因于一个被称为 Lazarus 的 APT 组织。
Group-IB 的威胁情报团队对这些活动进行了更加深入的研究，并锁定了另一个具有相同基础架构的攻击活动。攻击者表现出了以前的攻击习惯——使用从未见过的工具窃取加密货币。Lazarus 攻击了在线商店，在网页中植入恶意 JS 嗅探器：JS 嗅探器经过重新设计以窃取加密货币。实际上，Sansec 识别出的受害者中，有一些并没有受到"clientToken ="攻击活动的影响，而是成为了另一个没有报道过的攻击活动的受害者，Group-IB 的研究人员将这个攻击活动命名为 BTC Changer 。Group-IB 的研究人员将其命名为 BTC Changer。
Group-IB 的 TI&A 团队在其中识别出了 Lazarus 使用的 BTC 地址，并分析了来往业务。结果发现了 Lazarus 参与其中的额外证据。

详情

North Korean hackers adapt web skimming for stealing Bitcoin

https://www.bleepingcomputer.com/news/security/north-korean-hackers-adapt-web-skimming-for-stealing-bitcoin/

美国国家安全局发布俄罗斯黑客利用的 5 大漏洞

日期: 2021-04-20

等级: 高

来源: BALAJI N

标签: ['CISA', 'NSA', 'FBI', 'SVR']

网络安全和基础设施安全局（CISA）与国家安全局（NSA）以及联邦调查局（FBI）最近共同发布了一份关于俄罗斯对外情报局（SVR）正在利用的五个已知漏洞的文档。美国国家安全局称，俄罗斯 SVR 正在利用这些漏洞入侵美国政府网络。这些漏洞针对公众服务，攻击者的主要动机是获取身份验证凭据。一旦攻击者得到了敏感身份凭据，他们就可以轻易地破坏美国企业网络和政府网络。

详情

NSA Released Top 5 Vulnerabilities that Exploited by Russian Hackers

https://gbhackers.com/nsa-released-top-5-vulnerabilities-that-exploited-by-russian-hackers/

黑客利用虚假的 Facebook 广告进行网络钓鱼

日期: 2021-04-21

等级: 高

来源: Waqas

标签: ['Facebook Messenger', 'Facebook', 'Phinshing']

网络安全公司 groupib 发布了一份新的报告，详细介绍了影响 80 多个国家用户的新网络钓鱼活动。攻击者在欧洲、亚洲、北美和南美以及中东创建了大约 1000 个虚假的

Facebook 个人账号，并利用这些账号发布虚假的 Facebook 广告，来宣传虚假的 Facebook Messenger，以窃取用户的登录凭据。

详情

Facebook ads used in spreading Facebook Messenger phishing scam
https://www.hackread.com/facebook-ads-facebook-messenger-phishing-scam/

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. 减少外网资源和不相关的业务，降低被攻击的风险
3. 做好产品自动告警措施
4. 及时对系统及各个服务组件进行版本升级和补丁更新
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. 注重内部员工安全培训
7. 软硬件提供商要提升自我防护能力，保障供应链的安全

(三) 其他事件

黑客们正积极瞄准 VPN 设备漏洞

日期: 2021-04-21

等级: 高

来源: Liam Tung

标签: ['FireEye', 'CISA']

网络安全公司 FireEye 和美国国土安全部网络安全和基础设施安全局（CISA）发出警告，称攻击者利用 Pulse Connect 安全 VPN 产品中新发现的漏洞进行攻击。FireEye 报告说，它一直在调查多起使用 4 月份发现的 CVE-2021-22893 漏洞的设备出现故障的事件。这起事件严重性评分为 10 分（满分为 10 分），部署的恶意软件旨在绕过双因素身份验证。

详情

Hackers are actively targeting flaws in these VPN devices. Here's what you need to do
https://www.zdnet.com/article/hackers-are-actively-targeting-flaws-in-these-vpn-devices-heres-what-you-need-to-do/

Homebrew 远程代码执行漏洞披露

日期: 2021-04-21

等级: 高

来源: reitermarkus

标签: ['Homebrew', 'Ruby', 'HackerOne']

一名安全研究人员在 Homebrew 组织的 Homebrew/homebrew-cask 存储库存储库中发现了一个漏洞，并在 HackerOne 上报告了该漏洞。在该存储库中可以通过混淆 Homebrew 项目中的库，来合并恶意请求请求。通过此漏洞，攻击者可以在使用的用户计算机上执行任意 Ruby 代码。

详情

通过破坏官方的 Cask 存储库导致 Homebrew 远程执行代码漏洞披露
https://brew.sh/2021/04/21/security-incident-disclosure/

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