安全事件周报

安全事件周报 (03.29-04.04)

360CERT
北京奇虎科技有限公司 | 2021-04-06

报告信息

报告名称	安全事件周报（03.29-04.04）		
报告类型	安全事件周报	报告编号	B6-2021-040601
报告版本	1.0	报告日期	2021-04-06
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	2021-04-06	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 11 项

话题集中在`数据泄露`、`网络攻击`方面，涉及的组织有：`Asteelflash`、`Facebook`、`PHP SRC`、`Activision`等。PHP 代码被植入后门，Facebook 遭遇用户数据泄露。

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**
Asteelflash 电子制造商遭遇勒索软件攻击	★★★★
《使命召唤：战区》恶意软件	★★★★
一种 Android 恶意软件隐藏为系统更新应用程序来监视你	★★★★
数据安全	**等级**
Facebook5.33 亿用户数据被发布	★★★★★
MobiKwik 遭遇重大漏洞，350 万用户 KYC 数据曝光	★★★★★
网络攻击	**等级**
针对安全研究人员的最新网络攻击	★★★★★
PHP 代码被植入后门	★★★★★
针对加密货币的自动攻击行为	★★★★
其他事件	**等级**
伪造的 jQuery 文件会在 WordPress 网站上加载被混淆的恶意软件	★★★★
VMware 修补程序关键的 vRealize 操作平台漏洞	★★★★
成千上万的项目受到 netmask npm 包漏洞的影响	★★★★

三、 事件详情

(一) 恶意程序

Asteelflash 电子制造商遭遇勒索软件攻击

日期: 2021-04-02

等级: 高

来源: Lawrence Abrams

标签: ['Asteelflash', 'REvil']

法国领先的电子制造服务公司 Asteelflash 遭到了 REvil 勒索软件团伙的网络攻击，该团伙要求支付 2400 万美元的赎金，REvil 允许攻击者访问 Tor 协商页面进行网络攻击。

详情

Asteelflash electronics maker hit by REvil ransomware attack

https://www.bleepingcomputer.com/news/security/asteelflash-electronics-maker-hit-by-revil-ransomware-attack/

《使命召唤：战区》恶意软件

日期: 2021-04-02

等级: 高

来源: Becky Bracken

标签: ['Activision', 'Call of Duty', 'RAT']

《使命召唤：战区》（Call of Duty:Warzone）背后的公司 Activision 发布警告称，一名攻击者发布了一款作弊工具的广告，结果发现这是远程访问特洛伊木马（RAT）。Activision 在警告中说，该木马于 3 月份首次出现，当时一名网络攻击者发布了一款免费的游戏辅助工具。作弊指南通常会要求用户以最高的权限运行，并禁用或卸载防病毒软件和主机防火墙、内核代码签名等。该工具发布贴收到了 1 万多次浏览和 260 条回复，这篇帖子随后在评论中又添加了说明，并链接到了一个 YouTube 视频，该视频的浏览量达到了 5000 次。

详情

Call of Duty Cheats Expose Gamers to Malware

https://threatpost.com/call-of-duty-cheats-gamers-malware/165209/

一种 Android 恶意软件隐藏为系统更新应用程序来监视你

日期: 2021-03-29

等级: 高

来源: Charlie Osborne

标签: ['Android', 'Trojan']

研究人员发现了一种新的"复杂的"安卓间谍软件应用程序，将自己伪装成软件更新。该恶意软件是一种远程访问特洛伊木马（RAT），能够窃取 GPS 数据和短信、联系人列表、通话日志、获取图像和视频文件、秘密录制基于麦克风的音频、劫持移动设备的摄像头拍

照、查看浏览器书签和历史记录、窃听电话、窃取手机上的操作信息，包括存储统计数据和已安装应用程序的列表，即时通讯内容也面临风险。

详情

This Android malware hides as a System Update app to spy on you

https://www.zdnet.com/article/this-android-malware-hides-as-a-system-update-app-to-spy-on-you/

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. 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

(二) 数据安全

Facebook5.33 亿用户数据被发布

日期: 2021-04-03

等级: 高

来源: Larry Dignan

标签: ['Facebook']

5.53 亿 Facebook 用户的数据，包括电话号码、Facebook id、全名、出生日期和其他信息都被发布在网上。安全公司哈德逊洛克（hudsonrock）的首席技术官阿隆•加尔在推特上发布了这个数据。加尔公布了受影响用户的国家名单，根据他的名单，美国有 3230 万受影响用户，英国有 1150 万。

详情

Facebook data on 533 million users posted online

https://www.zdnet.com/article/facebook-data-on-533-million-users-posted-online/

MobiKwik 遭遇重大漏洞，350 万用户 KYC 数据曝光

日期: 2021-03-29

等级: 高

来源: The Hacker News

标签: ['MobiKwik', 'KYC', 'India', 'Payments Service']

印度移动支付服务 MobiKwik 在 2021 年 3 月初发现重大数据泄露事件后，数百万用户共 8.2TB 的数据开始在暗网上流传。

泄露的数据包括敏感的个人信息，如：客户姓名、散列密码、电子邮件地址、住宅地址等。

详情

MobiKwik Suffers Major Breach — KYC Data of 3.5 Million Users Exposed
https://thehackernews.com/2021/03/mobikwik-suffers-major-breach-kyc-data.html

相关安全建议

1. 严格控制数据访问权限
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. 及时检查并删除外泄敏感数据

(三) 网络攻击

针对安全研究人员的最新网络攻击

日期: 2021-04-01

等级: 高

来源: Adam Weidemann

标签: ['SecuriElite', 'Security Researchers', 'North Korean']

2021 年 1 月，威胁分析小组记录了一次黑客攻击活动，并将其归因于朝鲜政府支持的一个针对安全研究人员的实体。
3 月 17 日，这些黑客为一家名为“ SecuriElite”的假公司建立了一个具有相关社交媒体资料的新网站。
该网站谎称自己是一家位于土耳其的红队安全公司，可提供渗透测试，软件安全评估和漏洞利用。
与这些黑客以前创建的网站一样，该网站在页面底部也有指向其 PGP 公钥的链接。

详情

Update on campaign targeting security researchers
https://blog.google/threat-analysis-group/update-campaign-targeting-security-researchers/

PHP 代码被植入后门

日期: 2021-03-29

等级: 高

来源: PHP

标签: ['PHP', 'Backdoor', 'Zlib']

2021 年 3 月 28 日，PHP 团队的 git.php.net 服务器上维护的 php-src Git 存储库中被提交了两个恶意文件。恶意文件是以创建者的名义提交的，目前尚不清楚这一攻击是如何发生的，但是所有线索都表明这次攻击是针对 git.php.net 服务器的（而不是个人 git 帐户）。通过分析恶意代码，发现其目的是为了给安装该版本 PHP 的网站植入后门并方便远程执行代码（RCE）。目前尚不清楚该事件的影响情况，但是 git.php.net 服务器已停用，其源代码存储库现已迁移到 GitHub。

Github Commit 地址
- https://github.com/php/php-src/commit/c730aa26bd52829a49f2ad284b181b7e82a68d7d
- https://github.com/php/php-src/commit/c730aa26bd52829a49f2ad284b181b7e82a68d7d

详情

PHP 代码被植入后门

https://news-web.php.net/php.internals/113838

针对加密货币的自动攻击行为

日期: 2021-04-03

等级: 高

来源: Ax Sharma

标签: ['GitHub', 'GitHub Actions', 'Cryptocurrency']

攻击者滥用 GitHub Actions，并在攻击中使用 GitHub 的服务器来挖掘加密货币。GitHub Actions 是一个 CI / CD 解决方案，可轻松实现所有软件工作流程的自动化和定期任务的设置。
这种特殊的攻击将恶意的 GitHub Actions 代码添加到了合法代码的分叉存储库中，并进一步为原始存储库维护者创建了一个 Pull Request，以将代码合并回去，合法项目的维护者不需要执行操作就可以使攻击成功，以此来更改原始代码。

详情

Automated attack abuses GitHub Actions to mine cryptocurrency

https://www.bleepingcomputer.com/news/security/automated-attack-abuses-github-actions-to-mine-cryptocurrency/

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. 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. 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

(四) 其他事件

伪造的 jQuery 文件会在 WordPress 网站上加载被混淆的恶意软件

日期: 2021-03-31

等级: 高

来源: Ax Sharma

标签: ['JavaScript', 'WordPress', 'JQuery Migrate']

JQuery Migrate 插件的假冒版本被注入了数十个网站，其中包含用于加载恶意软件的模糊代码。攻击者可以获得各种各样的能力，包括用于信用卡浏览的 Magecart 诈骗，以及将用户重定向到诈骗网站，用户可能会被引导到虚假调查，技术支持诈骗，被要求订阅垃圾邮件通知或下载不需要的浏览器扩展。

详情

Fake jQuery files load obfuscated malware on WordPress sites

https://www.bleepingcomputer.com/news/security/fake-jquery-files-load-obfuscated-malware-on-wordpress-sites/

VMware 修补程序关键的 vRealize 操作平台漏洞

日期: 2021-03-31

等级: 高

来源: Charlie Osborne

标签: ['VMware', 'VRealize']

VMware 修补了一对可能导致 vRealize 中管理员凭据被盗的严重漏洞，这些漏洞是由 Positive Technologies 渗透测试人员 Egor Dimitrenko 私下向 VMware 报告的，可允许具有网络访问权限的攻击者执行 SSRF 攻击并窃取管理员凭据。

详情

VMware patches critical vRealize Operations platform vulnerabilities

https://www.zdnet.com/article/vmware-patches-critical-vrealize-operations-vulnerabilities/

成千上万的项目受到 netmask npm 包漏洞的影响

日期: 2021-03-30

等级: 高

来源: Pierluigi Paganini

标签: ['CVE-2021-28918', 'Npm', 'Netmask', 'SSRF', 'Vulnerability']

netmask npm 软件包中的漏洞（编号为 CVE-2021-28918）可能使专用网络遭受多种攻击。
该漏洞是由于 netmask npm 软件包中八进制字符串的输入验证不正确引起的，它影响了 1.1.0 版本。

在广泛使用的 netmask npm 包 v1.1.0 及以下版本中，不正确的八进制字符串输入允许未经身份验证的远程攻击者对许多依赖的包执行 SSRF、RFI 和 LFI 攻击。

详情

Hundreds of thousands of projects affected by a flaw in netmask npm package
https://securityaffairs.co/wordpress/116126/hacking/netmask-npm-package-flaw.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

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