安全事件周报

安全事件周报 (2.15-2.21)

360CERT

360CERT
北京奇虎科技有限公司 | 2021-02-22

报告信息

报告名称	安全事件周报（2.15-2.21）		
报告类型	安全事件周报	报告编号	B6-2021-022201
报告版本	1.0	报告日期	2021-02-22
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	2021-02-22	360CERT	360CERT	撰写报告

360CERT

目录

360CERT

一、 事件概览

本周收录安全事件 11 项

话题集中在`网络攻击`方面，涉及的组织有：`Singtel`、`Microsoft`、`EXMO`、`Android`等。Exchange 部分源码遭窃，供应链攻击效率显著。

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。

360CERT

二、 事件档案

恶意程序	**等级**
保险商实验室（UL）认证巨头遭勒索	★★★★★
安卓应用程序的安全漏洞未修补，下载量达 10 亿次	★★★★
Masslogger 特洛伊木马变种窃取 Outlook、Chrome 凭据	★★★★
数据安全	**等级**
新加坡电信公司遭遇信息泄露	★★★★
Clop 勒索团伙在暗网上泄露 Jones Day 律师事务所数据	★★★★
网络攻击	**等级**
DDoS 攻击关闭 EXMO 加密货币交换服务器	★★★★
Malvertisers 利用浏览器漏洞将用户重定向至诈骗页面	★★★★
错误配置的婴儿监视器泄露在线视频流	★★★★
Microsoft 内部 SolarWoinds 调查结果	★★★★
黑客滥用 Google Apps 脚本窃取信用卡	★★★★
网络钓鱼更改电子邮件超链接前缀以绕过防御	★★★★

360CERT

三、 事件详情

(一) 恶意程序

保险商实验室（UL）认证巨头遭勒索

日期: 2021-02-19

等级: 高

来源: Lawrence Abrams

标签: ['UL LLC', 'Ransomware']

保险商实验室（UL LLC）遭到勒索软件攻击，黑客对其服务器进行加密，并导致服务器宕机。UL 是美国最大、历史最悠久的安全认证公司，在 40 多个国家拥有 14000 名员工和办事处。UL 标志遍布在各电器、笔记本电脑、电视遥控器、灯泡，甚至你的苹果 USB 充电器的背面。据消息人士称，UL 决定不支付赎金，而是从备份中恢复系统。

详情

Underwriters Laboratories (UL) certification giant hit by ransomware

https://www.bleepingcomputer.com/news/security/underwriters-laboratories-ul-certification-giant-hit-by-ransomware/

安卓应用程序的安全漏洞未修补，下载量达 10 亿次

日期: 2021-02-16

等级: 高

来源: Catalin Cimpanu

标签: ['Android', 'SHAREit', 'RCE']

一个下载超过 10 亿次的 Android 应用程序--SHAREit，包含未修补的漏洞。SHAREit 是一款允许用户与朋友或个人设备之间共享文件的移动应用程序。攻击者通过中间人网络攻击，可以向 SHAREit 应用程序发送恶意命令，并劫持其合法功能来运行自定义代码、覆盖应用程序的本地文件，或者在用户不知情的情况下安装第三方应用程序。

详情

Security bugs left unpatched in Android app with one billion downloads

https://www.zdnet.com/article/security-bugs-left-unpatched-in-android-app-with-one-billion-downloads/

Masslogger 特洛伊木马变种窃取 Outlook、Chrome 凭据

日期: 2021-02-18

等级: 高

来源: Charlie Osborne

标签: ['Chrome', 'Outlook', 'Trojan', 'Phinshing']

Masslogger 特洛伊木马变种正在尝试窃取 Outlook、Chrome 凭据。该木马利用网络钓鱼邮件伪装成与业务相关的查询，并包含.RAR 附件。 如果受害者打开附件，将提取已编译的 HTML 文件.CHM 文件，其中还包含带有嵌入式 JavaScript 代码的 HTML 文件。最终导

致部署包含 Masslogger 加载器的 PowerShell 脚本。

详情

Masslogger Trojan reinvented in quest to steal Outlook, Chrome credentials
https://blog.talosintelligence.com/2021/02/masslogger-cred-exfil.html

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. 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
6. 及时备份数据并确保数据安全
7. 各主机安装 EDR 产品，及时检测威胁

(二) 数据安全

新加坡电信公司遭遇信息泄露

日期: 2021-02-17

等级: 高

来源: Eileen Yu

标签: ['Singtel', 'FTA']

新加坡电信公司 Singtel 证实，12.9 万名客户的个人数据被泄露，其中包括他们的身份证号码以及其他一些数据，包括姓名、出生日期、手机号码和实际地址。28 名前 Singtel 员工的银行账户信息和一家使用 Singtel 移动电话的企业客户的 45 名员工的信用卡信息也被泄露。此外，包括供应商、合作伙伴和企业客户在内的 23 家企业的"部分信息"也遭到泄露。

详情

Singtel breach compromises data of customers, former employees
https://www.zdnet.com/article/singtel-breach-compromises-data-of-customers-former-employees/

Clop 勒索团伙在暗网上泄露 Jones Day 律师事务所数据

日期: 2021-02-17

等级: 高

来源: Deeba Ahmed

标签: ['Jones Day', 'Clop', 'Leak Data', 'Dark Web']

Clop 勒索软件团伙在暗网上泄露了从美国律师事务所 Jones Day 窃取的数据。 Jones Day 是一家备受瞩目的美国律师事务所，代表美国前总统唐纳德·特朗普（Donald Trump）对法律进行了全面的调查。就总收入而言，它是美国第十大公司。它的一些客户包括摩根大通公司，宝洁公司，Alphabet Inc.的 Google，沃尔玛公司和麦当劳。黑客在网站上发布消息称，他们从 Jones Day 盗走了大约 100GB 的文件，数据包括电子邮件和法律文件。

详情

Clop ransomware gang leaks Jones Day law firm data on dark web
https://www.hackread.com/clop-ransomware-gang-jones-day-dark-web-data-leak/

相关安全建议

1. 及时检查并删除外泄敏感数据
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. 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
4. 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

DDoS 攻击关闭 EXMO 加密货币交换服务器

日期: 2021-02-15

等级: 高

来源: Sergiu Gatlan

标签: ['British', 'EXMO', 'DDoS']

英国加密货币交易所 EXMO 的服务器在遭到分布式拒绝服务（DDoS）攻击后暂时宕机。攻击发生后，EXMO 暂停了所有提款，并说明在此期间所有用户损失将由 EXMO 赔偿并完全退款。2021 年 2 月 17 日，EXMO 服务器恢复运行，并称："我们恢复了工作。这是一次巨大的攻击（每秒 30GB），影响了公司的整个基础架构，包括网站，API，Websocket API 和交换图表。因此，在这种情况下，任何交换中断几个小时都是很自然的。此次攻击已被击退，我们还采取了其他措施来防止这种情况再次发生。"

详情

DDoS attack takes down EXMO cryptocurrency exchange servers
https://www.bleepingcomputer.com/news/security/ddos-attack-takes-down-exmo-cryptocurrency-exchange-servers/

Malvertisers 利用浏览器漏洞将用户重定向至诈骗页面

日期: 2021-02-16

等级: 高

来源: Ionut Ilascu

标签: ['ScamClub', 'WebKit', 'CVE-2021-1801']

ScamClub 恶意组织利用 WebKit Web 浏览器引擎中的漏洞，来将用户重定向至诈骗页面。所用漏洞为 CVE-2021-1801。在过去三个月中，每天投放的恶意广告展示次数激增至 1600 万。

详情

Malvertisers exploited browser zero-day to redirect users to scams

https://blog.confiant.com/malvertiser-scamclub-bypasses-iframe-sandboxing-with-postmessage-shenanigans-cve-2021-1801-1c998378bfba

错误配置的婴儿监视器泄露在线视频流

日期: 2021-02-17

等级: 高

来源: Habiba Rashid

标签: ['RTSP', 'CCTV', 'Monitor', 'Video Stream']

SafetyDetections 网络安全团队调查显示，婴儿监视器存在一个漏洞，这是由于其配置错误，可能会导致攻击者未经授权访问摄像头的视频流。同时，不仅是婴儿监视器，其它使用 RTSP 的摄像机（如 CCTV 摄像机）已受此影响。这使攻击者能够接触到他们孩子、卧室的实时影像。

详情

Misconfigured baby monitors exposing video stream online

https://www.hackread.com/misconfigured-baby-monitors-exposing-video-stream-online/

Microsoft 内部 SolarWoinds 调查结果

日期: 2021-02-18

等级: 高

来源: MSRC

标签: ['Microsoft', 'SolarWinds', 'Azure', 'Intune', 'Exchange']

2020 年 12 月，微软遭受了 SolarWinds 供应链攻击。2021 年 2 月 18 日，微软发布此攻击事件内部调查报告。黑客获得了有限数量的源代码，主要包括
- 部分 Azure 组件源代码（服务，安全性，身份的子集）
- 部分 Intune 组件源代码
- 部分 Exchange 组件源代码

微软确定，泄露的代码不包括任何凭据。同时，微软表示会积极采用"零信任"的理念来创建优化安全模型。

详情

Microsoft Internal Solorigate Investigation – Final Update

https://msrc-blog.microsoft.com/2021/02/18/microsoft-internal-solorigate-investigation-final-update/

黑客滥用 Google Apps 脚本窃取信用卡

日期: 2021-02-18

等级: 高

来源: Sergiu Gatlan

标签: ['Google', 'CSP', 'Credit Cards']

攻击者滥用 Google 的 Apps Script 业务应用开发平台，来窃取电子商务网站客户在线购物时提交的信用卡信息。在线商店会认为 Google 的 Apps 脚本域是受信任的，并有可能将所有 Google 子域加入其站点的 CSP 配置（阻止 Web 应用程序中不受信任的代码执行的安全标准）白名单。由此，使用 script.google.com 域的恶意软件扫描引擎成功隐藏其恶意活动，并绕过内容安全策略（CSP）控件。

详情

Hackers abuse Google Apps Script to steal credit cards, bypass CSP

https://www.bleepingcomputer.com/news/security/hackers-abuse-google-apps-script-to-steal-credit-cards-bypass-csp/

网络钓鱼更改电子邮件超链接前缀以绕过防御

日期: 2021-02-19

等级: 高

来源: Bradley Barth

标签: ['Phishing', 'Bypass Defenses', 'URL Beginning']

安全研究人员称，他们已经检测到网络钓鱼利用更改电子邮件超链接前缀的方法来绕过防御。换句话说，URL 不是以"http://"开头，而是以"http://\"开头。但 URL 的其余部分保持不变。这些网址与简单的电子邮件扫描程序的已存储 ioc 不符，使得它们可以在未被发现的情况下绕过防御。

详情

Phishing campaign alters prefix in emailed hyperlinks to bypass defenses

https://www.scmagazine.com/home/security-news/phishing/phishing-campaign-alters-prefix-in-hyperlinks-to-bypass-email-defenses/

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. 软硬件提供商要提升自我防护能力，保障供应链的安全
5. 不盲目信任云端文件及链接
6. 不盲目安装官方代码仓库的第三方 Package
7. 不盲目安装未知的浏览器扩展

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）。

360CERT

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

360CERT

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。

360CERT

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

360CERT

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

360CERT