安全事件周报

安全事件周报 (03.22-03.28)

360CERT
北京奇虎科技有限公司 | 2021-03-29

报告信息

报告名称	安全事件周报（03.22-03.28）		
报告类型	安全事件周报	报告编号	B6-2021-032901
报告版本	1.0	报告日期	2021-03-29
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	2021-03-29	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 12 项

话题集中在`勒索软件`、`数据安全`方面，涉及的组织有：`壳牌`、`MangaDex`、`FBS`、`Sierra Wireless`等。钓鱼攻击袭击加州政府， 员工安全意识培训不可忽视。

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**
物联网巨头 Sierra Wireless 遭遇勒索攻击	★★★★★
BlackKingdom 勒索软件扫描 Exchange 服务器	★★★★
Purple Fox 恶意蠕虫针对 Windows 系统	★★★★
REvil 勒索软件现在可以重新启动受感染的设备	★★★★
Evil Corp 网络犯罪组织转用 Hades 勒索软件逃避制裁	★★★★
Black Kingdom 勒索团伙入侵 1500 台 Exchange 服务器	★★★★
数据安全	**等级**
能源巨头 Shell 遭遇数据泄露	★★★★★
在线交易经纪商 FBS 曝光 20TB 数据，160 亿条记录	★★★★
选举前一天，黑客泄露了数百万以色列选民的详细信息	★★★★
网络攻击	**等级**
MangaDex 漫画网站遭遇网络攻击后关闭	★★★★
微软警告绕过电子邮件网关的网络钓鱼攻击	★★★★
针对加州机构的网络钓鱼攻击锁定 9000 名员工	★★★★

三、 事件详情

(一) 恶意程序

物联网巨头 Sierra Wireless 遭遇勒索攻击

日期: 2021-03-23

等级: 高

来源: Sergiu Gatlan

标签: ['Sierra Wireless', 'Ransomware']

全球领先的物联网解决方案提供商 Sierra Wireless 披露了一起勒索软件攻击事件，迫使其停止所有基地的生产。总部位于不列颠哥伦比亚省里士满的加拿大跨国公司，在全球拥有 1300 多名员工，开发通信设备，并在北美、欧洲和亚洲设有研发中心。它的产品（包括无线调制解调器、路由器和网关）直接销售给原始设备制造商，用于各种行业，包括汽车和运输、能源、医疗保健、工业和基础设施、网络行业和安全行业。勒索软件攻击在 3 月 20 日袭击了 Sierra Wireless 的内部网络。该公司表示，这次攻击没有影响任何面向客户的服务或产品。

详情

Ransomware attack shuts down Sierra Wireless IoT maker

https://www.bleepingcomputer.com/news/security/ransomware-attack-shuts-down-sierra-wireless-iot-maker/

BlackKingdom 勒索软件扫描 Exchange 服务器

日期: 2021-03-22

等级: 高

来源: Lawrence Abrams

标签: ['BlackKingdom', 'ProxyLogon', 'Exchange']

安全研究人员 Marcus Hutchins（又名 MalwareTechBlog）在 tweet 上发布消息称，黑客组织正在通过 ProxyLogon 漏洞危害微软 Exchange 服务器，以部署 BlackKingdom 勒索软件。根据他的蜜罐记录。攻击者利用该漏洞执行 PowerShell 脚本，该脚本从“yuuuuuuu44[.]com”下载勒索软件可执行文件，然后将其推送到网络上的其他计算机。

详情

Microsoft Exchange servers now targeted by BlackKingdom ransomware

https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-now-targeted-by-blackkingdom-ransomware/

Purple Fox 恶意蠕虫针对 Windows 系统

日期: 2021-03-23

等级: 高

来源: Sergiu Gatlan

标签: ['Purple Fox', 'Worms', 'SMB', 'Brute Force']

Purple Fox 是一种恶意软件，主要通过漏洞工具包和网络钓鱼电子邮件传播，现在它添加了一个蠕虫模块，在扫描到可通过网络访问的 Windows 系统后，Purple Fox 将使用 SMB 密码爆破来尝试感染。如果身份验证成功，恶意软件将创建一个服务从众多已感染 HTTP 服务器之中下载 MSI 安装包，从而完成感染。

详情

Purple Fox malware worms its way into exposed Windows systems

https://www.bleepingcomputer.com/news/security/purple-fox-malware-worms-its-way-into-exposed-windows-systems/

REvil 勒索软件现在可以重新启动受感染的设备

日期: 2021-03-24

等级: 高

来源: Akshaya Asokan

标签: ['REvil', 'Safe Mode']

REvil 勒索软件团伙增加了一种新的恶意软件功能，使攻击者能够在加密后重新启动受感染的设备。REvil 勒索软件添加了两个新的命令行，分别称为"AstraZeneca"和"Fanceisshit"，用于访问 Windows 设备的启动设置屏幕，这些功能可能是为了使攻击者能够在 Windows 安全模式下加密文件，以帮助逃避检测。

详情

REvil Ransomware Can Now Reboot Infected Devices

https://www.databreachtoday.com/revil-ransomware-now-reboot-infected-devices-a-16259

Evil Corp 网络犯罪组织转用 Hades 勒索软件逃避制裁

日期: 2021-03-25

等级: 高

来源: Sergiu Gatlan

标签: ['Evil Corp', 'OFAC', 'Hades']

Hades 勒索软件已经与 Evil Corp 网络犯罪团伙绑定在一起，该团伙利用它来逃避财政部外国资产控制办公室（OFAC）施加的制裁。Evil Corp（又名 Dridex gang 或 INDRIK SPIDER）至少从 2007 年就开始活跃，它以散布 Dridex 恶意软件而闻名。他们后来转向勒索软件业务，先是使用 Locky 勒索软件，然后使用勒索软件变种 BitPaymer。从 2020 年 6 月开始，Evil Corp 重新调整了规避制裁的策略，在针对企业组织的攻击中部署了新的 WastedLocker 勒索软件。而 Hades 勒索软件是 WastedLocker 的一个 64 位编译变种，升级了补充代码混淆和一些小的特性更改。

详情

Evil Corp switches to Hades ransomware to evade sanctions

https://www.bleepingcomputer.com/news/security/evil-corp-switches-to-hades-ransomware-to-evade-sanctions/

Black Kingdom 勒索团伙入侵 1500 台 Exchange 服务器

日期: 2021-03-26

等级：高

来源：Sergiu Gatlan

标签：['Microsoft', 'Black Kingdom', 'Exchange', 'ProxyLogon', 'Web Shell']

在大约 1500 台易受 ProxyLogon 攻击的 Exchange 服务器上，微软发现了 Black Kingdom 勒索团伙部署的 web shell。
许多被破坏的系统还没有被二次攻击，如人为操作的勒索软件攻击或数据外泄，这表明攻击者可能正在建立并保持其访问权限，以备之后的攻击行动。

详情

Microsoft: Black Kingdom ransomware group hacked 1.5K Exchange servers

https://www.bleepingcomputer.com/news/security/microsoft-black-kingdom-ransomware-group-hacked-15k-exchange-servers/

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. 各主机安装 EDR 产品，及时检测威胁
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. 注重内部员工安全培训

(二) 数据安全

能源巨头 Shell 遭遇数据泄露

日期：2021-03-22

等级：高

来源：Sergiu Gatlan

标签：['Shell', 'FTA', 'Accellion']

能源巨头壳牌公司（Shell）披露了一起数据泄露事件，此前攻击者入侵了该公司的安全文件共享系统。壳牌（Royal Dutch Shell plc）是一家由石油化工和能源公司组成的跨国集团，在 70 多个国家拥有 86000 多名员工。壳牌在其网站上发表的一份公开声明中披露了这起攻击事件，并表示这起事件只影响了用于安全传输大型数据文件的 Accellion FTA 设备，因此对壳牌的核心 IT 系统没有任何影响。

详情

Energy giant Shell discloses data breach after Accellion hack

https://www.bleepingcomputer.com/news/security/energy-giant-shell-discloses-data-breach-after-accellion-hack/

在线交易经纪商 FBS 曝光 20TB 数据，160 亿条记录

日期: 2021-03-24

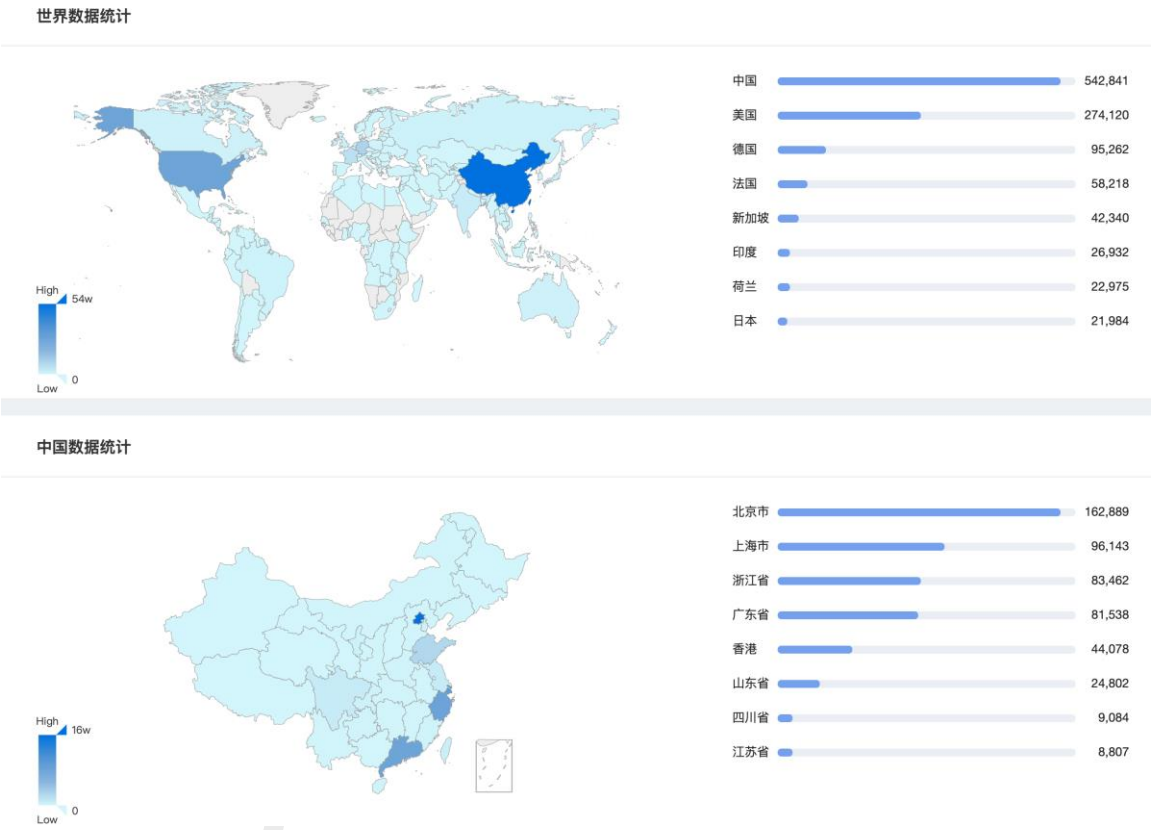
等级: 高

来源: Waqas

标签: ['FBS', 'Elasticsearch']

由 Ata Hakcil 领导的 WizCase 安全研究小组发现了大量属于 FBS 的数据。FBS 是一家著名的在线交易经纪商，在伯利兹和塞浦路斯设有办事处。FBS 拥有来自 190 多个国家的 1600 万名交易员和 40 万名合作伙伴。据研究人员称，FBS 暴露了价值近 20TB 的数据，包括超过 160 亿条记录。因此，数百万 FBS 客户的信用卡和护照可以在网上访问，在没有任何安全认证的情况下，这些数据在 Elasticsearch 服务器上对公众开放。

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



详情

Online trading broker FBS exposes 20TB of data with 16 billion records

https://www.hackread.com/online-trading-broker-fbs-exposes-data/

选举前一天，黑客泄露了数百万以色列选民的详细信息

日期: 2021-03-24

等级: 高

来源: Pierluigi Paganini

标签: ['Israeli', 'Elections', 'Leaked']

在以色列大选前几个小时，黑客泄露了选民登记和 650 多万公民的个人详细信息。
数据来源似乎是由软件公司 Elector Software 为以色列政党 Likud 开发的应用程序 Elector。
公开的数据包括居民住址，电话号码和注册选民的出生日期。

详情

A day before elections, hackers leaked details of millions of Israeli voters
https://securityaffairs.co/wordpress/115918/hacking/israeli-voters-leak.html

相关安全建议

1. 条件允许的情况下，设置主机访问白名单
2. 及时检查并删除外泄敏感数据
3. 及时备份数据并确保数据安全
4. 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

(三) 网络攻击

MangaDex 漫画网站遭遇网络攻击后关闭

日期: 2021-03-22

等级: 高

来源: Lawrence Abrams

标签: ['MangaDex', 'Source Code']

漫画扫描巨头 MangaDex 在遭受网络攻击后，源代码被盗，暂时关闭。MangaDex 是最大的漫画扫描（扫描翻译）网站之一，游客可以免费在线阅读漫画。一个攻击者通过网站漏洞窃取了管理员用户的会话令牌后获得了对该网站的访问权，黑客下载网站的源代码，并使用别名"holo gfx"在 GitHub 上发布了该站点的源代码。

详情

MangaDex manga site temporarily shut down after cyberattack
https://www.bleepingcomputer.com/news/security/mangadex-manga-site-temporarily-shut-down-after-cyberattack/

微软警告绕过电子邮件网关的网络钓鱼攻击

日期: 2021-03-23

等级: 高

来源: Sergiu Gatlan

标签: ['Microsoft', 'Phishing', 'Office 365']

自 2020 年 12 月以来，一个正在进行的网络钓鱼行动窃取了大约 40 万个 OWA 和 Office 365 凭据，目前已经扩展到滥用新的合法服务来绕过安全电子邮件网关（SEG）。这些攻

击是多个网络钓鱼活动的一部分，自 2020 年初以来一直活跃，WMC 全球威胁情报小组首次发现了这些活动。微软的安全专家说："网络钓鱼者继续成功地利用电子邮件营销服务上的泄露账户，从合法的 IP 范围和域发送恶意电子邮件。2021 年 1 月，攻击改为模仿 Office 365 品牌，可能会获取更多员工的凭据。"

详情

Microsoft warns of phishing attacks bypassing email gateways

https://www.bleepingcomputer.com/news/security/microsoft-warns-of-phishing-attacks-bypassing-email-gateways/

针对加州机构的网络钓鱼攻击锁定 9000 名员工

日期: 2021-03-24

等级: 高

来源: Steve Zurier

标签: ['California Agency', 'Phishing']

加利福尼亚州一家机构遭遇了一起网络钓鱼事件，一名员工点击了一个链接，该员工的账户就有了 24 小时的外部访问权限。据 KrebsOnSecurity 的一份报告称，在此期间，攻击者窃取了数千名国家工作人员的社会安全号码和敏感文件，然后向至少 9000 名其他国家工作人员及其联系人发送了有针对性的网络钓鱼信息。这起袭击发生在 3 月 18 日至 3 月 19 日，地点是加利福尼亚州州长办公室（SCO）的财产部门。

详情

9,000 employees targeted in phishing attack against California agency

https://www.scmagazine.com/home/security-news/phishing/9000-employees-targeted-in-phishing-attack-against-california-agency/

相关安全建议

1. 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
2. 积极开展外网渗透测试工作，提前发现系统问题
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

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