安全事件周报

安全事件周报 (03.15-03.21)

360CERT
北京奇虎科技有限公司 | 2021-03-22

报告信息

报告名称	安全事件周报（03.15-03.21）		
报告类型	安全事件周报	报告编号	
报告版本	1.0	报告日期	2021-03-22
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	2021-03-22	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`勒索软件`、`网络攻击`方面，涉及的组织有：`宏碁`、`Microsoft`、`Apple`等。近期黑客利用 Exchange 和 F5 漏洞进行大批量扫描，各单位要及时进行漏洞修补。

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**
电脑巨头宏碁遭 5000 万美元勒索软件攻击	★★★★★
微软 Exchange 服务器 0day 攻击：在英国 2300 台机器上发现恶意软件	★★★★
针对 Exchange 漏洞的 DearCry 勒索软件	★★★★
新的 Mirai 变种和 ZHtrap 僵尸网络恶意软件出现	★★★★
苹果开发者成为新恶意软件 EggShell 的目标	★★★★
联邦调查局：网络钓鱼邮件正在传播 Trickbot 恶意软件	★★★★
Android 特洛伊木马冒充 Clubhouse 应用	★★★★
数据安全	**等级**
以色列汽车融资公司遭受数据泄露	★★★★
网络攻击	**等级**
2020 年美国公立学校遭受超过 400 起网络攻击	★★★★
SolarWinds 攻击者窃取了 Mimecast 源代码	★★★★
Office 365 网络钓鱼攻击的目标是财务主管	★★★★

三、 事件详情

(一) 恶意程序

电脑巨头宏碁遭 5000 万美元勒索软件攻击

日期: 2021-03-19

等级: 高

来源: Lawrence Abrams

标签: ['Acer', 'REvil', 'Ransomware']

电子业巨头宏碁（Acer）遭到了一次 REvil 勒索软件攻击，攻击者要求获得迄今为止已知的最大赎金 5000 万美元。这个勒索软件团伙在他们的数据泄露网站上宣布，他们进入了宏碁的系统，并分享了一些据称被盗文件的图片作为证据。这些泄露的图像是用于包括财务电子表格、银行余额和银行通信的文档。

详情

Computer giant Acer hit by $50 million ransomware attack

https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/

微软 Exchange 服务器 0day 攻击：在英国 2300 台机器上发现恶意软件

日期: 2021-03-15

等级: 高

来源: Danny Palmer

标签: ['Exchange', 'NCSC']

英国国家网络安全中心（NCSC）的警告说，所有使用受影响版本的 Microsoft Exchange Server 的组织应紧急应用最新更新，以保护其网络免受包括勒索软件在内的网络攻击。NCSC 官员说，他们已经帮助检测并删除了英国 2300 多家企业机器上与攻击有关的恶意软件。同时，英国仍然有 3000 多家机构使用的 Microsoft Exchange 电子邮件服务器尚未安装最新的安全补丁，因此仍然面临着风险。

详情

Microsoft Exchange Server zero-day attacks: Malicious software found on 2,300 machines in the UK

https://www.zdnet.com/article/microsoft-exchange-server-zero-day-attacks-malicious-software-found-on-2300-machines-in-uk/

针对 Exchange 漏洞的 DearCry 勒索软件

日期: 2021-03-16

等级: 高

来源: Mathew J. Schwartz

标签: ['Exchange', 'Sophos', 'DearCry', 'Ransomware']

针对尚未部署的本地 Exchange 服务器的最新勒索软件似乎已被推向市场。
3 月 9 日 DearCry 首次在野外被发现，其目标是 Microsoft Exchange 电子邮件服务器中的一个严重的 proxylogon 漏洞，这是 Microsoft 通过 3 月 2 日发布的软件更新修补的四个 0day 之一，当时已经警告说该漏洞已经在野外被利用。

详情

Rushed to Market: DearCry Ransomware Targeting Exchange Bug

https://www.databreachtoday.com/rushed-to-market-dearcry-ransomware-targeting-exchange-bug-a-16189

新的 Mirai 变种和 ZHtrap 僵尸网络恶意软件出现

日期: 2021-03-16

等级: 高

来源: The Hacker News

标签: ['Mirai', 'ZHtrap', 'Botnet', 'Shell', 'Malware']

网络安全研究人员 3 月 14 日披露了新一轮持续的攻击，这些攻击利用多个漏洞在受感染的系统上部署 Mirai 变体。
在成功利用后，攻击者试图下载恶意的 shell 脚本，其中包含进一步的感染行为，例如下载和执行 Mirai 变体和暴力破解程序。

详情

New Mirai Variant and ZHtrap Botnet Malware Emerge in the Wild

https://thehackernews.com/2021/03/new-mirai-variant-and-zhtrap-botnet.html

苹果开发者成为新恶意软件 EggShell 的目标

日期: 2021-03-18

等级: 高

来源: Charlie Osborne

标签: ['Xcode', 'EggShell', 'Backdoor', 'XcodeSpy']

Xcode 是一个用于 macOS 开发苹果软件和应用程序的集成开发环境（IDE），项目正被用来劫持开发人员系统和散布 EggShell 后门。根据 SentinelLabs 发表的研究，IDE 中的 Run 脚本功能正被利用，攻击者通过在网上免费共享的木马化 Xcode 项目，对 iOS 开发者进行有针对性的攻击。

详情

Apple developers targeted by new malware, EggShell backdoor

https://www.zdnet.com/article/apple-developers-targeted-by-new-malware-eggshell-backdoor/

联邦调查局：网络钓鱼邮件正在传播 Trickbot 恶意软件

日期: 2021-03-18

等级: 高

来源: Danny Palmer

标签: ['Trickbot', 'JavaScript', 'Phishing']

美国联邦调查局（FBI）和网络安全与基础设施安全局（CIA）联合发布的一份咨询报告警告称，一项新的鱼叉式网络钓鱼活动正试图用 Trickbot 病毒感染个人电脑，该网站的作者们正在使用一种新的策略，将含有违反交通规则证据的网络钓鱼邮件发送给目标，恶意电子邮件包含一个链接，该链接将用户定向到恶意网站，该网站告诉受害者单击照片查看证据。他们点击照片，实际上下载了一个 JavaScript 文件，打开后连接到一个 C2 服务器，该服务器将 Trickbot 下载到他们的系统中。

详情

FBI: Phishing emails are spreading this sophisticated malware

https://www.zdnet.com/article/fbi-phishing-emails-are-spreading-this-sophisticated-malware/

Android 特洛伊木马冒充 Clubhouse 应用

日期: 2021-03-18

等级: 高

来源: AmerOwaida

标签: ['Clubhouse', 'ESET', 'BlackRock']

ESET 恶意软件研究人员卢卡斯·斯特凡科（Lukas Stefanko）发现，网络犯罪分子正试图利用 Clubhouse 的流行，发布恶意软件，目的是窃取用户的登录信息，用于各种在线服务。该恶意软件包伪装成 Android 版的仅限邀请函的音频聊天应用程序，由一家具有正版会所网站外观的网站提供。该恶意程序可以盗取受害者至少 458 个在线服务的登录数据。目标名单包括知名金融和购物应用程序、加密货币交易所，以及社交媒体和消息平台。

详情

Beware Android trojan posing as Clubhouse app

https://www.welivesecurity.com/2021/03/18/beware-android-trojan-posing-clubhouse-app/

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. 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. 各主机安装 EDR 产品，及时检测威胁
5. 严格做好主机的权限控制
6. 注重内部员工安全培训

(二) 数据安全

以色列汽车融资公司遭受数据泄露

日期: 2021-03-16

等级: 高

来源: Prajeet Nair

标签: ['Israeli', 'K.L.S.Capital Ltd.', 'Black Shadow']

黑影黑客组织声称，他们入侵了以色列汽车金融公司 K.L.S.Capital Ltd.并窃取了客户数据。2020 年 12 月，该组织泄露了数千份包含以色列 Shirbit 保险公司客户个人信息的文件。这个黑客组织声称，因为没有支付赎金，他们毁掉了这家汽车金融公司的服务器。

详情

Israeli Car Financing Company Suffers Data Breach

https://www.databreachtoday.com/hackers-steal-data-from-israeli-car-financing-company-a-16187

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

(三) 网络攻击

2020 年美国公立学校遭受超过 400 起网络攻击

日期: 2021-03-15

等级: 高

来源: Doug Olenick

标签: ['Public Schools', 'COVID-19', 'Virtual Learning']

2020 年，由于疫情，美国公立学校普遍采取在线上课的方式，这导致去年创纪录的网络攻击事件，光报道的就超过 400 起。这影响了 40 个州的 377 个不同的公共机构，其中城市、郊区和富裕地区最常成为袭击目标。同时，许多学区也受到了最近微软 Exchange 问题和物联网摄像机问题的影响。

详情

Over 400 Cyberattacks at US Public Schools in 2020

https://www.databreachtoday.com/over-400-cyberattacks-at-us-public-schools-in-2020-a-16183

SolarWinds 攻击者窃取了 Mimecast 源代码

日期: 2021-03-17

等级: 高

来源: Lindsey O'Donnell

标签: ['Mimecast', 'SolarWinds', 'Source Code']

据 SolarWinds 公司的最新消息，黑客入侵了 Mimecast 网络，并窃取了该安全公司的一些源代码。
该安全公司最初报告说，一月份的证书泄露是 SolarWinds 供应链攻击的一部分，该攻击还袭击了 Microsoft，FireEye 和一些美国政府机构。
最初发现攻击者窃取了 Mimecast 客户的一部分电子邮件地址和其他联系信息，以及某些经过哈希处理的凭据。
但是，在对 SolarWinds 黑客的最新调查中，Mimecast 说，它已经发现证据表明黑客也可以访问"数量有限"的源代码存储库。

详情

Mimecast: SolarWinds Attackers Stole Source Code
https://threatpost.com/mimecast-solarwinds-attackers-stole-source-code/164847/

Office 365 网络钓鱼攻击的目标是财务主管

日期: 2021-03-19

等级: 高

来源: Becky Bracken

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

根据 area1security 的报告，一种新的网络钓鱼骗局正在兴起，目标是保险和金融服务行业的高管获取他们的 microsoft365 证书，并发起商业电子邮件泄露（BEC）攻击。这些新的、复杂的攻击针对 C-suite 高管、他们的助理和财务部门，可以绕过电子邮件安全和 office365 防御。研究人员补充说，他们截获的大多数攻击都试图破坏金融部门，袭击始于 2020 年 12 月，一直持续到 2021 年 2 月。研究人员的报告中说："通过针对这些公司的财务部门，攻击者可能通过发票和账单获取第三方的敏感数据，这通常被称为 BEC（商业电子邮件泄露）攻击。"

详情

Office 365 Phishing Attack Targets Financial Execs
https://www.area1security.com/blog/microsoft-365-spoof-targets-financial-departments/

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. 注重内部员工安全培训

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