安全事件周报

安全事件周报 (05.10-05.16)

360CERT
北京奇虎科技有限公司 | 2021-05-17

报告信息

报告名称	安全事件周报（05.10-05.16）		
报告类型	安全事件周报	报告编号	B6-2021-051701
报告版本	1.0	报告日期	2021-05-17
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	2021-05-17	360CERT	360CERT	撰写报告

目录

一、 事件概览 1
二、 事件档案 2
三、 事件详情 3
(一) 恶意程序 3
(二) 数据安全 5
(三) 网络攻击 6
(四) 其他事件 8
四、 产品侧解决方案 10
(一) 360 网络空间测绘系统 10
(二) 360 安全分析响应平台 10
(三) 360 安全卫士 11
附录 A 事件等级说明 12
附录 B 事件类型说明 14

一、 事件概览

本周收录安全事件 14 项

话题集中在`勒索软件`、`网络攻击`方面，涉及的组织有：`Colonial Pipeline`、`Microsoft`、`Apple`、`QNAP`等。勒索软件攻击严重破坏国家基础服务正常运行，基础设施防护是重中之重。

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**
美国和澳大利亚发布 Avaddon 勒索软件攻击警告	★★★★
TeaBot: 新的安卓恶意软件	★★★★
Colonial 在勒索软件攻击后重新开始运营	★★★★
保险巨头 CNA 在勒索软件攻击后完成所有系统恢复	★★★★
化学品分销商向 DarkSide 勒索软件支付 440 万美元	★★★★
爱尔兰医疗服务遭到 2000 万美元勒索	★★★★
安盛保险公司遭遇勒索软件攻击	★★★★
数据安全	**等级**
勒索软件泄露大都会警察局数据	★★★★
谈判失败，Babuk 勒索软件帮泄露更多警察局的数据	★★★★
网络攻击	**等级**
微软：新的恶意软件瞄准航空组织	★★★★
法国东芝公司遭 DarkSide 勒索软件组织袭击	★★★★
QNAP 警告称 eCh0raix 勒索软件攻击和 Roon 服务器 0day	★★★★
其他事件	**等级**
美国调用紧急运输规则以保持燃料传输	★★★★★
苹果对受到 XcodeGhost 攻击的用户保持沉默	★★★★

三、 事件详情

(一) 恶意程序

美国和澳大利亚发布 Avaddon 勒索软件攻击警告

日期: 2021-05-10

等级: 高

来源: Sergiu Gatlan

标签: ['FBI', 'ACSC']

联邦调查局（FBI）和澳大利亚网络安全中心（ACSC）警告称，正在进行的 Avaddon 勒索软件活动的目标是美国和世界各地的组织。美国联邦调查局（FBI）发布警报称，Avaddon 勒索软件分支机构正试图破坏全球制造业、医疗保健和其他私营部门组织的网络。

详情

US and Australia warn of escalating Avaddon ransomware attacks

https://www.bleepingcomputer.com/news/security/us-and-australia-warn-of-escalating-avaddon-ransomware-attacks/

TeaBot: 新的安卓恶意软件

日期: 2021-05-10

等级: 高

来源: Waqas

标签: ['Europe', 'Android', 'TeaBot']

意大利米兰在线欺诈预防公司 Cleafy's 的威胁情报和事件响应（TIR）团队发现了一种新的 Android 恶意软件`TeaBot`，恶意软件还处于开发的早期阶段，到目前为止，它已经瞄准了全欧洲的 60 家银行，主要分布国家为意大利、西班牙、德国、比利时和荷兰等欧洲国家。一旦感染该软件，其会控制目标设备、窃取登录凭据、发送和截获短信，并盗窃银行数据。

详情

New Android malware TeaBot found stealing data, intercepting SMS

https://www.cleafy.com/documents/teabot

Colonial 在勒索软件攻击后重新开始运营

日期: 2021-05-12

等级: 高

来源: Scott Ferguson

标签: ['Colonial Pipeline', 'DarkSide']

燃油供应公司 Colonial Pipeline 宣布，在发生 DarkSide 勒索软件攻击事件后，该公司重新开始运营。在 Colonial 宣布这一消息后，美国总统拜登签署了一项行政命令，旨在帮助政府加强对此类攻击的防护以及涉及 SolarWinds 和 Microsoft Exchange 服务器的攻击的对应措施。Colonial 确实指出，要完全恢复供应链运作正常，还需要几天时间。

详情

Colonial Restarts Operations Following Ransomware Attack

https://www.databreachtoday.com/colonial-restarts-operations-following-ransomware-attack-a-16576

保险巨头 CNA 在勒索软件攻击后完成所有系统恢复

日期: 2021-05-13

等级: 高

来源: Sergiu Gatlan

标签: ['Phoenix CryptoLocker', 'CNA Financial']

总部位于美国的领先保险公司 CNA Financial 在 2021 年 3 月下旬遭到 Phoenix CryptoLocker 勒索软件攻击并中断在线服务和业务运营后，已全面恢复系统。攻击者在 3 月 21 日在 CNA 网络上部署勒索软件有效载荷后，对超过 15000 台设备进行了加密。。根据保险信息研究所提供的统计数据，CNA 提供包括网络保险单在内的多种保险产品，是美国第六大商业保险公司。

详情

Insurance giant CNA fully restores systems after ransomware attack

https://www.bleepingcomputer.com/news/security/insurance-giant-cna-fully-restores-systems-after-ransomware-attack/

化学品分销商向 DarkSide 勒索软件支付 440 万美元

日期: 2021-05-13

等级: 高

来源: Lawrence Abrams

标签: ['Brenntag', 'Bitcoin', 'DarkSide']

化学品分销公司 Brenntag 以比特币形式向黑暗勒索软件团伙支付了 440 万美元的赎金，以获得加密文件的解密器，并防止攻击者公开泄露的被盗数据。Brenntag 是一家全球领先的化学品分销公司，总部位于德国，在全球 670 多个工厂拥有 17000 多名员工。

详情

Chemical distributor pays $4.4 million to DarkSide ransomware

https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/

爱尔兰医疗服务遭到 2000 万美元勒索

日期: 2021-05-15

等级: 高

来源: Lawrence Abrams

标签: ['Ireland', 'HSE', 'Conti']

爱尔兰公共资助的医疗保健系统健康服务执行局（HSE）在遭遇 Conti 勒索软件攻击后，关闭了所有的 IT 系统。爱尔兰国家卫生局说：“我们已经采取预防措施，关闭了我们所有

的 IT 系统，以保护它们免受这次攻击，并让我们与自己的安全伙伴有充分事件评估局势。同时，我们拒绝向 Conti 勒索软件团伙支付 2000 万美元的赎金”

详情

Ireland’s Health Services hit with $20 million ransomware demand

https://www.bleepingcomputer.com/news/security/ireland-s-health-services-hit-with-20-million-ransomware-demand/

安盛保险公司遭遇勒索软件攻击

日期: 2021-05-16

等级: 高

来源: Ax Sharma

标签: ['AXA', 'Avaddon']

保险巨头 AXA 总部设在泰国、马来西亚、香港和菲律宾的分支机构遭受 Avaddon 勒索网络攻击。Avaddon 勒索软件集团在他们的泄密网站上声称，他们从 AXA 的亚洲业务中窃取了 3TB 的敏感数据。该组织称，Avaddon 获得的泄露数据包括客户医疗报告（暴露其性健康诊断）、身份证复印件、银行账户对账单、索赔表、付款记录、合同等。

详情

Insurer AXA hit by ransomware after dropping support for ransom payments

https://www.bleepingcomputer.com/news/security/insurer-axa-hit-by-ransomware-after-dropping-support-for-ransom-payments/

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) 数据安全

勒索软件泄露大都会警察局数据

日期: 2021-05-11

等级: 高

来源: Sergiu Gatlan

标签: ['Babuk Locker', 'MPD', 'DC Police']

Babuk Locker 泄露了属于大都会警察局（也称为 MPD 或 DC 警察）的数据，公布的文件包括来自华盛顿特区警察个人档案的 150MB 数据。勒索软件团伙声称，这些数据被泄露是因为华盛顿警方愿意支付的金额与 Babuk Locker 的勒索要求不符。勒索团队说，如果华盛顿警方不愿意满足他们的要求，所有数据都将被泄露。

详情

Ransomware gang leaks data from Metropolitan Police Department

https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-from-metropolitan-police-department/

谈判失败，Babuk 勒索软件帮泄露更多警察局的数据

日期: 2021-05-12

等级: 高

来源: Deeba Ahmed

标签: ['Babuk', 'Columbia's Metropolitan Police Department']

在谈判失败后，Babuk 勒索软件帮派泄露了 DC 警察更多的数据，最新泄露的数据包含价值 26GB 的记录。黑客发布警告说，如果再不支付赎金，他们将公布整个 250GB 的数据库。数据库包括情报简报、调查报告、纪律处分和逮捕数据。

详情

Babuk ransomware gang leaks DC police data as negotiations fail

https://www.hackread.com/babuk-ransomware-gang-leaks-dc-police-data/

相关安全建议

1. 及时备份数据并确保数据安全
2. 合理设置服务器端各种文件的访问权限
3. 严格控制数据访问权限
4. 及时检查并删除外泄敏感数据
5. 发生数据泄漏事件后，及时进行密码更改等相关安全措施
6. 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

微软：新的恶意软件瞄准航空组织

日期: 2021-05-12

等级: 高

来源: Sergiu Gatlan

标签: ['Microsoft', 'RAT', 'Aerospace', 'Travel']

微软警告称，针对航空航天和旅游组织的"鱼叉"网络钓鱼活动正在进行中，这些组织使用新的隐蔽恶意软件加载程序部署了多个远程访问特洛伊木马（RAT）。攻击者的最终目的是利用遥控、键盘记录和密码窃取功能从受感染的设备中获取和过滤数据。

详情

Microsoft: Threat actors target aviation orgs with new malware

https://www.bleepingcomputer.com/news/security/microsoft-threat-actors-target-aviation-orgs-with-new-malware/

法国东芝公司遭 DarkSide 勒索软件组织袭击

日期: 2021-05-14

等级: 高

来源: Charlie Osborne

标签: ['French', 'Toshiba', 'DarkSide']

法国东芝公司已经成为 DarkSide 勒索软件攻击的最新受害者。东芝公司表示受到一次网络攻击，该攻击已波及欧洲一些地区。在发现攻击后，东芝公司关闭了日本、欧洲及其子公司之间的网络，以防止损害的蔓延，同时实施恢复协议和数据备份。该公司表示，已经对损害程度展开调查，并已派出第三方网络取证专家协助。

详情

Toshiba unit struck by DarkSide ransomware group

https://www.zdnet.com/article/toshiba-unit-struck-by-darkside-ransomware-group/

QNAP 警告称 eCh0raix 勒索软件攻击和 Roon 服务器 0day

日期: 2021-05-14

等级: 高

来源: Sergiu Gatlan

标签: ['QNAP', 'Roon Server', 'NAS']

QNAP 警告客户，Roon Server 0day 漏洞和 eCh0raix 勒索软件攻击正在被积极利用，目标是他们的网络连接存储（NAS）设备。QNAP 敦促客户立即行动，通过以下方式保护其数据免受潜在的 eCh0raix 攻击：

- 为管理员帐户使用更强大的密码

- 更改 NAS 密码

- 启用 IP 访问保护

- 更改系统端口号。

详情

QNAP warns of eCh0raix ransomware attacks, Roon Server zero-day

https://www.bleepingcomputer.com/news/security/qnap-warns-of-ech0raix-ransomware-attacks-roon-server-zero-day/

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

(四) 其他事件

美国调用紧急运输规则以保持燃料传输

日期: 2021-05-10

等级: 高

来源: Liam Tung

标签: ['FMCSA', 'USDOT', 'Ransomware']

针对 Colonial Pipeline 的勒索软件攻击事件影响美国东海岸 45%的燃料，美国交通部（USDOT）已经动用了紧急权力——涉及限制道路燃料运输的法律的临时豁免，并允许司机工作更长时间。豁免适用于向阿拉巴马州、阿肯色州、哥伦比亚特区、特拉华州、佛罗里达州、乔治亚州、肯塔基州、路易斯安那州、马里兰州、密西西比州、新泽西州、纽约州、北卡罗来纳州、宾夕法尼亚州、南卡罗来纳州、田纳西州、德克萨斯州和弗吉尼亚州运输汽油、柴油、喷气燃料和其他精炼石油产品的车辆，以便更方便地通过公路运输燃料。

详情

Pipeline ransomware attack: US invokes emergency transport rules to keep fuel flowing

https://www.zdnet.com/article/pipeline-ransomware-attack-us-invokes-emergency-transport-rules-to-keep-fuel-flowing/

苹果对受到 XcodeGhost 攻击的用户保持沉默

日期: 2021-05-10

等级: 高

来源: Deeba Ahmed

标签: ['iOS', 'XcodeGhost', 'Apple']

据报道，近 1.28 亿 iOS 用户下载了包含 XcodeGhost 恶意软件的应用程序，但苹果没有告知受害者此次攻击。2021 年 3 月，Hackread.com 报告了一次 supply check 攻击，其中

XcodeSpy 恶意软件被用于针对使用 Xcode 集成开发环境的开发人员，2015 年还使用了类似的恶意软件。它的代号为 XcodeGhost，允许攻击者使用从第三方网站下载的 Xcode 的恶意版本在合法应用程序中插入恶意代码。

详情

Apple kept mum about XcodeGhost malware attack against 128M users
https://www.hackread.com/apple-xcodeghost-malware-attack-against-users/

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