安全事件周报

安全事件周报 (05.17-05.23)

360CERT
北京奇虎科技有限公司 | 2021-05-24

报告信息

报告名称	安全事件周报（05.17-05.23）		
报告类型	安全事件周报	报告编号	B6-2021-052401
报告版本	1.0	报告日期	2021-05-24
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	2021-05-24	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 14 项

话题集中在`恶意软件`、`数据泄露`方面，涉及的组织有：`CNA Financial`、`Codecov`、`Guard.me`、`爱尔兰卫生部`等。勒索赎金再创新高，恶意软件肆虐医疗和金融保险行业。

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**
美国保险业巨头 CNA Financial 支付 4000 万美元赎金	★★★★★
Bizarro 银行木马在欧洲激增	★★★★
2021 年 290 多家企业遭 6 个勒索团伙袭击	★★★★
Qlocker 勒索软件勒索数百名 QNAP 用户后关闭	★★★★
澳大利亚，新西兰遭受恶意软件攻击	★★★★
Conti 勒索软件提供免费解密程序	★★★★
WastedLocker 新变体利用 Internet Explorer 漏洞	★★★★
研究人员发现 DarkSide 勒索软件变种	★★★★
阿拉斯加卫生部服务受到恶意软件攻击的影响	★★★★
数据安全	**等级**
Codecov 黑客获得了 Monday.com 源代码的访问权限	★★★★★
学生健康保险公司 Guard.me 遭受数据泄露	★★★★
电子商务巨头在 Codecov 事件中遭受重大数据泄露	★★★★
网络攻击	**等级**
联邦调查局：Conti 勒索软件攻击了 16 个美国医疗保健和急救机构	★★★★
其他事件	**等级**
针对 Windows HTTP 漏洞的利用程序已发布	★★★★

三、 事件详情

(一) 恶意程序

美国保险业巨头 CNA Financial 支付 4000 万美元赎金

日期: 2021-05-21

等级: 高

来源: Charlie Osborne

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

美国最大的保险公司之一 CNA Financial 同意支付 4000 万美元，以便在勒索软件攻击后恢复对其系统的访问。在网络攻击期间，该公司员工无法访问公司系统，该公司业务停滞，机密数据被盗。CNA 发言人在一份声明中表示，不会对赎金置评，也不会公开哪些信息被盗。

详情

US insurance giant CNA Financial paid $40 million ransom to regain control of systems: report

https://www.zdnet.com/article/us-insurance-giant-cna-financial-paid-40-million-ransom-to-wrestle-back-control-of-systems/

Bizarro 银行木马在欧洲激增

日期: 2021-05-19

等级: 高

来源: Charlie Osborne

标签: ['Bizarro', 'Trojan']

研究人员称：Bizarro banking 特洛伊木马正从巴西基地转移到欧洲，并已经锁定了至少 70 家银行的客户。木马通过社工手段入侵受害者，一旦启动，程序将从已沦陷网站或服务器下载.ZIP 副本。副本文件包含一个用 Delphi 编写的恶意.DLL、一个自动运行的可执行文件和一个从.DLL 调用导出函数的脚本。此函数经过模糊处理，会触发银行特洛伊木马程序所需的恶意代码。在启动时，Bizarro 将关闭现有的浏览器进程，包括任何与网上银行服务的活动会话。一旦受害者重新启动会话，恶意软件就会悄悄地捕获银行凭据，并将其发送到攻击者的命令和控制（C2）服务器。

详情

Bizarro banking Trojan surges across Europe

https://www.zdnet.com/article/bizarro-banking-trojan-surges-across-europe/

2021 年 290 多家企业遭 6 个勒索团伙袭击

日期: 2021-05-19

等级: 高

来源: Jonathan Greig

标签: ['Ransomware']

根据研究报告表明，每周都有一个新的组织面临勒索软件攻击，仅在 2021 年，6 个勒索软件集团就在 1 月 1 日至 4 月 31 日期间危害了 292 个组织。该报告估计，这些组织设法从这些袭击中至少获利 4500 万美元，并详述了未公开的多起事件。报告详情如下方链接。

详情

More than 290 enterprises hit by 6 ransomware groups in 2021

https://www.esentire.com/resources/library/six-ransomware-gangs-claim-290-new-victims-in-2021-potentially-reaping-45-million-for-the-hackers

Qlocker 勒索软件勒索数百名 QNAP 用户后关闭

日期: 2021-05-19

等级: 高

来源: Lawrence Abrams

标签: ['Qlocker', 'QNAP NAS']

研究人员发现，在勒索数百名 QNAP 用户后，Qlocker 关闭了运营。2021 年 4 月 19 日开始，全世界的 QNAP NAS 设备所有者突然发现，他们设备的文件被加密。除了加密的文件，QNAP 所有者还发现了一个 `!!!READ_ME.txt`勒索说明，文件内容称需要访问 Tor 网站支付勒索才能取回他们的文件。Tor 网站将攻击者识别为 Qlocker，并要求 0.01 比特币（约合 550 美元）来接收其文件的密码。通过这种方式，Qlocker 勒索软件团伙在一个月内赚了 35 万美元后。

详情

Qlocker ransomware shuts down after extorting hundreds of QNAP users

https://www.bleepingcomputer.com/news/security/qlocker-ransomware-shuts-down-after-extorting-hundreds-of-qnap-users/

澳大利亚，新西兰遭受恶意软件攻击

日期: 2021-05-20

等级: 高

来源: Asha Barbaschow

标签: ['Hospital', 'Phishing']

澳大利亚和新西兰受到了恶意软件的广泛攻击，其中包括澳大利亚数字房地产企业、新西兰 Waikato 卫生局、Waikato 医院、Thames 医院、Te Kūiti 医院、Tokoroa 医院 、Taumarunui 医院。恶意软件通过钓鱼邮件入侵相关系统，并实施勒索攻击。其中部分医院的手术、门诊活动均被被推迟。

详情

Domain Group says phishing attack targeted site users

https://www.zdnet.com/article/domain-group-says-phishing-attack-targeted-site-users/

Conti 勒索软件提供免费解密程序

日期: 2021-05-20

等级: 高

来源: Lawrence Abrams

标签: ['Conti', 'Ireland', 'HSE']

爱尔兰卫生部门遭到了 Conti 勒索软件团伙的袭击，并被迫关闭了 IT 系统。2021 年 5 月下旬，Conti 勒索软件团伙已经为爱尔兰的健康服务机构 HSE 发布了一个免费的解密程序，但警告说如果不支付 2000 万美元的赎金，他们仍将出售或公布被盗的私人数据。

详情

Conti ransomware gives HSE Ireland free decryptor, still selling data

https://www.bleepingcomputer.com/news/security/conti-ransomware-gives-hse-ireland-free-decryptor-still-selling-data/

WastedLocker 新变体利用 Internet Explorer 漏洞

日期: 2021-05-20

等级: 高

来源: Akshaya Asokan

标签: ['WastedLocker', 'WastedLoader', 'Internet Explorer']

一个 WastedLocker 恶意软件新变种，正在利用互联网浏览器中的两个漏洞，将恶意广告插入合法网站，该变种被称为：WastedLoader。研究人员称："攻击始于合法网站发布的恶意广告，恶意广告将重定向到标题为"RIG EK"的登录页。然后该页将利用这两个漏洞执行攻击，如果攻击成功，它将下发恶意软件。"

详情

New WastedLocker Variant Exploits Internet Explorer Flaws

https://www.databreachtoday.com/new-wastedlocker-variant-exploits-internet-explorer-flaws-a-16705

研究人员发现 DarkSide 勒索软件变种

日期: 2021-05-20

等级: 高

来源: Akshaya Asokan

标签: ['DarkSide', 'Ransomware']

FortiGuard 实验室的安全研究人员发现了一种具有破坏性的 DarkSide 勒索软件变体。攻击者能够搜索磁盘分区信息并加密多个磁盘中的文件。FortiGuard 研究人员指出："这种 DarkSide 变体会在多引导系统上寻找分区，以找到要加密的额外文件，从而造成更大的破坏。"

详情

Researchers Uncover Another DarkSide Ransomware Variant

https://www.databreachtoday.com/researchers-uncover-another-darkside-ransomware-variant-a-16704

阿拉斯加卫生部服务受到恶意软件攻击的影响

日期: 2021-05-20

等级: 高

来源: Marianne Kolbasuk McGee

标签: ['Alaska', 'Health Department']

阿拉斯加卫生和社会服务部遭遇恶意软件的网络攻击，该部门表示："我们正在与有关当局合作调查这起事件，并采取相关行动，防止服务器、系统和数据库受到进一步破坏和损害。"阿拉斯加州部门官员说，该部门的网站在遭受攻击之后，于晚上关闭，在该此次事件公布细节之前，公众将无法访问。

详情

Alaska Health Department Services Affected by Malware Attack

https://www.databreachtoday.com/alaska-health-department-services-affected-by-malware-attack-a-16708

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

Codecov 黑客获得了 Monday.com 源代码的访问权限

日期: 2021-05-18

等级: 高

来源: Ax Sharma

标签: ['Monday.com', 'Codecov']

Monday.com 称受到 Codecov 供应链攻击的影响。Monday.com 是一个在线工作流管理平台，供项目经理、销售和 CRM 专业人员、营销团队以及其他各种组织部门使用。该平台的客户包括优步、BBC 工作室、Adobe、环球、Hulu、欧莱雅、可口可乐和联合利华等知名品牌。在对 Codecov 漏洞进行调查后，Monday.com 发现未经授权的攻击者者获得了他们源代码的只读副本。

详情

Codecov hackers gained access to Monday.com source code

https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/

学生健康保险公司 Guard.me 遭受数据泄露

日期: 2021-05-17

等级: 高

来源: Lawrence Abrams

标签: ['guard.me']

学生健康保险运营商 Guard.me 遭遇网络攻击，攻击者可以任意访问保单持有人的个人信息，目前 Guard.me 已将其网站下线。guard.me 是全球最大的保险公司之一，专门为在另一个国家旅行或出国留学的学生提供健康保险。Guard.me 称：此漏洞允许攻击者访问学生的出生日期、性别、电子邮件地址、邮寄地址、电话号码和加密密码。

详情

Student health insurance carrier Guard.me suffers a data breach

https://www.bleepingcomputer.com/news/security/student-health-insurance-carrier-guardme-suffers-a-data-breach/

电子商务巨头在 Codecov 事件中遭受重大数据泄露

日期: 2021-05-21

等级: 高

来源: Ax Sharma

标签: ['Mercari', 'Codecov']

电子商务平台 Mercari 披露了一起因 Codecov 供应链攻击曝光而发生的重大数据泄露事件。Mercari 是一家日本上市公司，也是一家在线市场，最近已将其业务扩展到美国和英国。截至 2017 年，Mercari 应用程序在全球的下载量已超过 1 亿次，该公司是日本第一家达到独角兽地位的公司。

详情

E-commerce giant suffers major data breach in Codecov incident

https://www.bleepingcomputer.com/news/security/e-commerce-giant-suffers-major-data-breach-in-codecov-incident/

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

联邦调查局：Conti 勒索软件攻击了 16 个美国医疗保健和急救机构

日期: 2021-05-21

等级: 高

来源: Sergiu Gatlan

标签: ['FBI', 'Conti']

联邦调查局（FBI）说，Conti 勒索软件团伙试图破坏十多个美国医疗和急救组织的网络。这一信息是通过 TLP:WHITE flash 警报共享的，该警报旨在帮助系统管理员和安全专业人员保护组织的网络免受 Conti 攻击。联邦调查局网络部门说：“联邦调查局在过去一年内确认了至少 16 起针对美国医疗保健和急救网络的连续勒索软件攻击，还包括执法机构、紧急医疗服务、911 调度中心和市政当局。”

详情

FBI: Conti ransomware attacked 16 US healthcare, first responder orgs

https://www.bleepingcomputer.com/news/security/fbi-conti-ransomware-attacked-16-us-healthcare-first-responder-orgs/

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

针对 Windows HTTP 漏洞的利用程序已发布

日期: 2021-05-17

等级: 高

来源: Sergiu Gatlan

标签: ['Windows', 'Http', 'CVE']

漏洞攻击代码已经发布，可用于最新的 Windows 10 和 Windows Server 版本。这个漏洞被追踪为 CVE-2021-31166。该漏洞可允许未经验证的攻击者在大多数情况下远程执行任意代码。

详情

Exploit released for wormable Windows HTTP vulnerability
https://www.bleepingcomputer.com/news/security/exploit-released-for-wormable-windows-http-vulnerability/

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