安全事件周报

安全事件周报 (06.07-06.13)

360CERT
北京奇虎科技有限公司

报告信息

报告名称	安全事件周报 (06.07-06.13)		
报告类型	安全事件周报	报告编号	
报告版本	v1.0	报告日期	2021-06-15
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
v1.0	2021-06-15	360CERT	360CERT	更新报告

目录

1 事件导览 4
2 恶意程序 4
新的 Kubernetes 恶意程序通过 Windows 容器部署后门 6
勒索软件警告：针对学校和大学的攻击又一次激增 6
深入调查 Nefilim 勒索软件集团 7
涉及漏洞 7
计算机内存制造商 ADATA 受到 Ragnar Locker 勒索软件的攻击 8
据报道，中国 APT 集团开发定制后门 8
涉及漏洞 9
新型勒索软件针对全球数十家企业 9
涉及漏洞 10
餐饮服务供应商 Edward Don 遭遇勒索软件攻击 10
** 相关安全建议 ** 10
3 数据安全 11
奥迪、大众 330 万客户遭遇数据泄露 11
美国卡车和军用车辆制造商 Navistar 数据泄露 12
未知的恶意软件收集了数十亿的被盗数据 12
黑客入侵游戏巨头并窃取游戏源代码 13
麦当劳客户及员工信息遭遇数据泄露 13
** 相关安全建议 ** 14
4 网络攻击 14
中国黑客涉嫌攻击俄罗斯政府机构 15
IOC 15

西班牙劳动和社会经济部遭网络攻击 15
** 相关安全建议 ** 16
5 其它事件 16
一次大规模的 CDN 故障使大部分互联网服务离线 16
谷歌修补了 Android RCE 的关键漏洞 17
涉及漏洞 18
JBS 承认支付了 1100 万美元的赎金 18
Avaddon 勒索软件停止运营并公开解密密钥 19
** 相关安全建议 ** 20
6 时间线 20
附录 21
A 产品侧解决方案 21
360 城市级网络安全监测服务 21
360 安全分析响应平台 21
360 安全卫士 22

1 事件导览

本周收录安全热点18项，话题集中在数据安全、勒索软件方面，涉及的组织有：奥迪、大众汽车、麦当劳、EA等。多个龙头企业遭遇数据泄露，数据防护不可忽视。对此，360CERT 建议使用360安全卫士进行病毒检测、使用360安全分析响应平台进行威胁流量检测，使用360城市级网络安全监测服务QUAKE进行资产测绘，做好资产自查以及预防工作，以免遭受黑客攻击。

恶意程序
新的 Kubernetes 恶意程序通过 Windows 容器部署后门
勒索软件警告：针对学校和大学的攻击又一次激增
深入调查 Nefilim 勒索软件集团
计算机内存制造商 ADATA 受到 Ragnar Locker 勒索软件的攻击
据报道，中国 APT 集团开发定制后门
新型勒索软件针对全球数十家企业
餐饮服务供应商 Edward Don 遭遇勒索软件攻击

2 恶意程序

数据安全
奥迪、大众 330 万客户遭遇数据泄露
美国卡车和军用车辆制造商 Navistar 数据泄露
未知的恶意软件收集了数十亿的被盗数据
黑客入侵游戏巨头并窃取游戏源代码
麦当劳客户及员工信息遭遇数据泄露

网络攻击
中国黑客涉嫌攻击俄罗斯政府机构
西班牙劳动和社会经济部遭网络攻击

其它事件
一次大规模的 CDN 故障使大部分互联网服务离线
谷歌修补了 Android RCE 的关键漏洞
JBS 承认支付了 1100 万美元的赎金
Avaddon 勒索软件停止运营并公开解密密钥

2.1 新的 Kubernetes 恶意程序通过 Windows 容器部署后门

1 日期：2021 年 06 月 07 日
2 等级：高
3 作者：Sergiu Gatlan
4 标签：Kubernetes, Windows
5 行业：信息传输、软件和信息技术服务业

活跃了一年多的新恶意软件正在破坏 Windows 容器，从而破坏 Kubernetes 集群，最终目标是对它们进行后门攻击，并为攻击者在其他恶意活动中使用它们铺平道路。Kubernetes 最初由 Google 开发，目前由云原生计算基金会（cloudnativeComputingFoundation）维护。Kubernetes 是一个开源系统，它帮助在主机集群上自动化容器化工作负载、服务和应用的部署、扩展和管理。

详情

New Kubernetes malware backdoors clusters via Windows containers

2.2 勒索软件警告：针对学校和大学的攻击又一次激增

1 日期：2021 年 06 月 07 日
2 等级：高
3 作者：Danny Palmer
4 标签：NCSC, School
5 行业：教育
6 涉及组织：

英国国家网络安全中心（NCSC）警告称，针对学校、学院和大学的勒索软件攻击数量再次上升。世界各地接连发生勒索软件攻击事件，其中包括对 ColonialPipeline

、爱尔兰卫生服务和肉类供应商 JBS 的网络攻击事件。NCSC 此前曾警告过针对教育部门注意勒索软件攻击，但 5 月下旬和 6 月上旬此类事件又有所增加。

详情

Ransomware warning: There's been another spike in attacks on schools and universities

2.3 深入调查 Nefilim 勒索软件集团

```
日期：2021 年 06 月 08 日
等级：高
作者：Charlie Osborne
标签：Nefilim, Cobalt Strike, Ransomware
行业：跨行业事件
```

研究人员对 Nefilim 进行了案例研究，Nefilim 是一家勒索软件运营商，使用"双重勒索"策略来确保受害者组织的付款。Nefilim 起源于 2020 年 3 月，经常利用公开的远程桌面服务（RDP）服务和公开的 PoC 代码进行攻击，例如：CVE-2019-19781 和 CVE-2019-11634。攻击成功后，Nefilim 首先下载 CobaltStrikebeacon、ProcessHacker (用于终止端点安全代理)、Mimikatz 凭据转储程序和其他工具，然后将部署 Nefilim 勒索软件主程序并开始加密内容。

2.3.1 涉及漏洞

- CVE-2019-11634
- CVE-2017-0213
- CVE-2019-19781

详情

A deep dive into Nefilim, a ransomware group with an eye for $1bn+ revenue companies

2.4 计算机内存制造商 ADATA 受到 Ragnar Locker 勒索软件的攻击

1 日期：2021 年 06 月 08 日
2 等级：高
3 作者：Sergiu Gatlan
4 标签：ADATA, SSD
5 行业：制造业
6 涉及组织：ADATA

总部位于台湾的内存和存储制造商 ADATA 称，一次勒索软件攻击迫使其系统在 5 月下旬离线。ADATA 生产高性能 DRAM 内存模块、NAND 闪存卡和其他产品，包括移动配件、游戏产品、电力系统和工业解决方案。2018 年，该公司被评为第二大 DRAM 内存和固态驱动器（SSD）制造商。ADATA 在侦测到攻击后，将所有受影响的系统关闭，并将此次事件通知所有相关国际当局，协助追查攻击者。

详情

Computer memory maker ADATA hit by Ragnar Locker ransomware

2.5 据报道，中国 APT 集团开发定制后门

1 日期：2021 年 06 月 09 日
2 等级：高

作者：Prajeet Nair
标签：Chinese, Southeast Asia
行业：信息传输、软件和信息技术服务业

CheckPoint 的研究人员发现了一个中国先进的持续威胁组织正在进行的活动，该组织在过去三年里一直在测试和改进其军火库中的一个定制后门，以针对东南亚各国政府开展间谍活动。

2.5.1 涉及漏洞

- CVE-2017-11882

详情

Chinese APT Group Reportedly Develops Custom Backdoor

2.6 新型勒索软件针对全球数十家企业

日期：2021 年 06 月 10 日
等级：高
作者：The Hacker News
标签：Prometheus , Thanos
行业：跨行业事件

一种新型勒索软件变种声称，在其投入运营后的短短 4 个月内，依靠一个臭名昭著的勒索软件集团的帮助，已经突破了 30 个组织。"普罗米修斯"于 2021 年 2 月首次被观测到，它是另一个著名的勒索软件塔诺斯（Thanos）的一个分支，该变种曾在去年针对中东和北非的国营组织进行攻击。

2.6.1 涉及漏洞

- CVE-2019-7481

详情

Emerging Ransomware Targets Dozens of Businesses Worldwide

2.7 餐饮服务供应商 Edward Don 遭遇勒索软件攻击

```
日期：2021 年 06 月 10 日
等级：高
作者：Lawrence Abrams
标签：Edward Don, Qbot
行业：住宿和餐饮业
```

Edward Don & Company 是最大的食品服务设备和用品分销商之一，如厨房用品、酒吧用品和餐具。Edward Don & Company 遭受勒索软件攻击，导致该公司关闭部分网络以防止攻击扩散。

详情

Foodservice supplier Edward Don hit by a ransomware attack

2.8 ** 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

3 数据安全

3.1 奥迪、大众 330 万客户遭遇数据泄露

```
日期：2021 年 06 月 12 日
等级：高
作者：Lawrence Abrams
标签：Audi, Volkswagen
行业：制造业
```

奥迪和大众汽车遭遇数据泄露，影响了 330 万客户。泄露的数据包括姓名、个人或公司邮寄地址、电子邮件地址或电话号码。在某些情况下，数据还包括有关购买、租赁或查询的车辆的信息，如车辆识别号（VIN）、品牌、型号、年份、颜色和装饰。还有极少数的出生日期、社会保障或社会保险号码、账户或贷款号码以及税务识别号码。

详情

Audi, Volkswagen data breach affects 3.3 million customers

3.2 美国卡车和军用车辆制造商 Navistar 数据泄露

日期：2021 年 06 月 07 日
等级：高
作者：Sergiu Gatlan
标签：Navistar, SEC
行业：制造业
涉及组织：Navistar

总部位于美国的卡车和军用车辆制造商 Navistar 国际公司（NavistarInternational-Corporation）表示，在 2021 年 5 月 20 日发现网络安全事件后，不明身份的攻击者窃取了其网络上的数据。该公司在提交给美国证券交易委员会（SEC）的一份报告中披露了此次攻击。Navistar 表示，尽管其 IT 系统已全面运行，但其运营并未受到安全漏洞的影响。该公司还采取了一系列措施，旨在减轻 5 月安全漏洞的潜在影响。

详情

US truck and military vehicle maker Navistar discloses data breach

3.3 未知的恶意软件收集了数十亿的被盗数据

日期：2021 年 06 月 09 日
等级：高
作者：Tara Seals
标签：NordLocker, Windows, Cookie
行业：信息传输、软件和信息技术服务业

研究人员发现了一个 1.2 兆字节的被盗数据数据库，该数据库是由一个未知的恶意软件在两年内从 320 万台基于 Windows 的计算机上盗取的。被盗信息包括 660 万个文

件和 2600 万个凭证，以及 20 亿个网络登录 cookies，其中 4 亿个 cookies 在数据库被发现时仍然有效。NordLocker 的研究人员称，罪魁祸首是一种隐秘的、不知名的恶意软件，在 2018 年至 2020 年间通过木马化的 AdobePhotoshop 版本、盗版游戏和 Windows 破解工具传播。

详情

Mysterious Custom Malware Collects Billions of Stolen Data Points

3.4 黑客入侵游戏巨头并窃取游戏源代码

```
日期：2021 年 06 月 10 日
等级：高
作者：Sergiu Gatlan
标签：EA, BleepingComputer
行业：信息传输、软件和信息技术服务业
```

黑客入侵了游戏巨头艺电（ElectronicArts，EA）的网络，声称窃取了大约 750gb 的数据，包括游戏源代码和调试工具。EA 在发给 BleepingComputer 的一份声明中证实了这一数据泄露事件。攻击者声称可以访问 EA 的所有服务，告诉愿意为被盗数据支付 2800 万美元的客户，他们还将获得“使用所有 EA 服务的能力”。

详情

Hackers breach gaming giant Electronic Arts, steal game source code

3.5 麦当劳客户及员工信息遭遇数据泄露

```
日期：2021 年 06 月 11 日
等级：高
```

作者：Sergiu Gatlan

标签：McDonald's, XSS

行业：住宿和餐饮业

全球最大的快餐连锁店麦当劳（McDonald's）披露了一起数据泄露事件，黑客入侵了麦当劳的系统，窃取了来自美国、韩国和台湾的顾客和员工的信息。作为全球食品服务零售商，麦当劳每天在 100 多个国家的 39000 多个地点为几亿顾客提供服务，其中仅在美国就有约 14000 家餐厅。

详情

McDonald's discloses data breach after theft of customer, employee info

3.6 ** 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

4 网络攻击

4.1 中国黑客涉嫌攻击俄罗斯政府机构

1 日期：2021 年 06 月 08 日
2 等级：高
3 作者：JUAN ANDRÉS GUERRERO-SAADE
4 标签：TA428，APT
5 行业：政府机关、社会保障和社会组织

sentinelone 分析人员发现利用"Mail-O"恶意软件针对俄罗斯联邦安全局和其他政府机构发起攻击的幕后黑手疑似是中国组织：TA428，sentinelone 将攻击活动命名为"ThunderCats"，并对此进行了追踪与分析。

4.1.1 IOC

Hash

- 603881f4c80e9910ab22f39717e8b296910bff08cd0f25f78d5bff1ae0dce5d7
- b7c1ec9484c4c2dcd01f861eeaa3b915c3e3312e
- d58b95f8413f784552d7fdadbb621243

详情

中国黑客涉嫌攻击俄罗斯政府机构

4.2 西班牙劳动和社会经济部遭网络攻击

1 日期：2021 年 06 月 09 日
2 等级：高
3 作者：Sergiu Gatlan

4 标签：MITES, Spain

5 行业：政府机关、社会保障和社会组织

西班牙劳动和社会经济部（MITES）负责协调和监督西班牙的就业、社会经济和企业社会责任政策。MITES 遭到网络攻击后，正致力于恢复服务。MITES 的媒体办公室说："劳动和社会经济部受到了网络攻击的影响，工信部和国家密码中心的技术管理人员正在共同努力，确定出处，尽快恢复正常。"

详情

Spain's Ministry of Labor and Social Economy hit by cyberattack

4.3 ** 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

5 其它事件

5.1 一次大规模的 CDN 故障使大部分互联网服务离线

---

1 日期：2021 年 06 月 08 日

2 等级：高

作者：Danny Palmer
标签：CDN，Outage
行业：跨行业事件

2021 年 6 月 8 日，互联网上的大部分网站都无法访问。包括《卫报》、《金融时报》、《纽约时报》和 ZDNet 在内的媒体出版物，以及 Reddit、Twitch、亚马逊、PayPal 和英国政府网站 gov.UK 在内的网站因设备故障而瘫痪。访问这些网站的访问者会收到一条错误消息："错误 503 服务不可用"。这个问题可能与云平台和内容交付网络（CDN）的故障有关。

详情

A massive outage just took large sections of the internet offline

5.2 谷歌修补了 Android RCE 的关键漏洞

日期：2021 年 06 月 08 日
等级：高
作者：Tara Seals
标签：Google，Android，Pixel
行业：信息传输、软件和信息技术服务业
涉及组织：google

谷歌修补了影响设备和第三方安卓手机操作系统中的 90 多个安全漏洞，其中包括一个严重的远程代码执行漏洞，该漏洞可让攻击者攻陷易受攻击的 Android 移动设备。该漏洞（CVE-2021-0507）存在于 Android 操作系统的系统组件中，可能使远程攻击者能够使用特制的传输在特权进程的上下文中执行任意代码。

5.2.1 涉及漏洞

- CVE-2021-0512
- CVE-2021-0608
- CVE-2020-14305
- CVE-2021-0521
- CVE-2020-1971
- CVE-2021-0508
- CVE-2021-0565
- CVE-2021-0571
- CVE-2021-0516
- CVE-2021-0557
- CVE-2021-0511
- CVE-2021-0520
- CVE-2021-0607
- CVE-2021-0555
- CVE-2021-0510
- CVE-2021-0507
- CVE-2021-0509

详情

Google Patches Critical Android RCE Bug

5.3 JBS 承认支付了 1100 万美元的赎金

1 日期：2021 年 06 月 10 日
2 等级：高
3 作者：Simon Sharwood

4 标签：USA，JBS
5 行业：制造业
6 涉及组织：JBS

全球最大的肉类生产商之一 JBSFoods 日前透露，公司已交出相当于 1100 万美元的赎金，以解决导致澳大利亚、美国和加拿大业务中断的勒索软件感染问题。该公司的一份声明说，支付这笔费用的决定是与内部 IT 专业人士和第三方网络安全专家协商后作出的，目的是减轻与攻击有关的任何不可预见的问题，并确保没有数据被泄露。

详情

Ransomware

5.4 Avaddon 勒索软件停止运营并公开解密密钥

---

1 日期：2021 年 06 月 11 日
2 等级：高
3 作者：Lawrence Abrams
4 标签：Avaddon
5 行业：跨行业事件

Avaddon 勒索软件团伙已经停止了行动，并将 2934 个受害者的解密密钥公开。Avaddon 的所有 Tor 网站都无法访问，目前尚不清楚 Avaddon 关闭的原因，但很可能是由于最近针对关键基础设施的攻击之后，全球执法部门和政府加大了压力和审查。

详情

Avaddon ransomware shuts down and releases decryption keys

5.5 ** 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

6 时间线

2021-06-15 360CERT 发布安全事件周报

A 产品侧解决方案

A.1 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台 (quake.360.cn)，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。

A.2 360 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，对网络攻击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。

A.3 360 安全卫士

针对以上安全事件，360cert 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。