安全事件周报

安全事件周报 (08.23-08.29)

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 (08.23-08.29)		
报告类型	安全事件周报	报告编号	B6-2021-083001
报告版本	1	报告日期	2021-08-30
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-08-30	360CERT	360CERT	撰写报告

目录

1 事件导览

本周收录安全热点18项，话题集中在恶意软件、网络攻击方面，涉及的组织有：Realtek、Android、HUAWEI、Cloudflare等。多个信息技术供应商遭遇网络袭击。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。

2 事件目录

数据安全
3800 万条记录因 Microsoft 配置错误而暴露
地下黑客论坛出售 7000 万 AT&T 用户的私人信息
Raven Hengelsport 数据泄露暴露了 18GB 的客户数据

网络攻击
诺基亚分公司 SAC Wireless 在 Conti 勒索软件事件后遭受数据泄露
cloudflare 遭 DDoS - 每秒收到 1720 万次 http 请求
新的 SideWalk 后门瞄准了美国的计算机零售业务
未打补丁的 Microsoft Exchange 服务器遭到 ProxyShell 攻击
21 岁的年轻人是 T-Mobile 黑客攻击的幕后黑手

网络攻击
黑客出售超过 130 万俄罗斯人的护照
Cosmos 数据库严重漏洞影响了数以千计的 Microsoft Azure 客户

其它事件
Razer Synapse 漏洞：简单鼠标插入，即可获得 Windows 系统权限

3 恶意程序

3.1 Ursnif 银行木马

1 日期：2021 年 08 月 23 日
2 等级：高
3 来源：revelock
4 标签：ursnif, banking trojan, Cerberus
5 行业：金融业
6 涉及组织：github

ursnif 是 2007 年发现的用于 Windows 的银行木马，经过多年的发展，仍然活跃，是最普遍的木马之一。

它影响了来自世界各地的许多不同的受害者。以至于 2021 年早些时候，德国银行用户受到其恶意活动的影响，并且在 3 月左右发现了针对意大利银行的新变种。

这些变化和演变的特征可能是由于多种原因造成的，其中包括在 2015 年左右，该恶意软件的源代码被泄露并发布在 github 版本控制平台上。

详情

Ursnif and Cerberus: A Combined Attack

3.2 LockFile 勒索软件通过 ProxyShell 危害 Microsoft Exchange

1 日期：2021 年 08 月 23 日
2 等级：高
3 来源：heimdalsecurity
4 标签：Microsoft Exchange, proxyshell, lockfile, conti, lockbit

5 行业：信息传输、软件和信息技术服务业
6 涉及组织：microsoft

安全研究人员发现了一种针对 MicrosoftExchange 服务器并执行 Windows 域加密的新恶意软件。
名为 lockfile 的勒索软件利用了最近检测到的 proxyshell 漏洞，该勒索软件不仅与 conti 相似，而且与 lockbit 勒索软件相似。
详情
LockFile Ransomware Compromises Microsoft Exchange via ProxyShell

3.3 数十万台设备使用 Mirai 僵尸网络针对的 Realtek SDK

---

1 日期：2021 年 08 月 24 日
2 等级：高
3 来源：heimdalsecurity
4 标签：mirai, realtek, sdk, Botnet
5 行业：制造业

在数十万台基于 realtek 的设备使用的软件 sdk 中发现的严重漏洞正被基于 mirai 的僵尸网络滥用。
研究人员确定了大约 65 个不同的受影响供应商和制造商，其中包含近 200 种受影响的设备。

3.3.1 涉及漏洞

3.3.2 cve-2021-35395

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-35395

3.3.3 cve-2021-20090

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-20090

详情

Hundreds of Thousands of Devices Using Realtek SDK Targeted by Mirai Botnet

3.4 Konni RAT 变体针对俄罗斯

```
日期：2021 年 08 月 24 日
等级：高
作者：Waqas
标签：Cyber Attack, Konni, Malware, Malwarebytes, North Korea, RAT,
↪  security, Windows 10
行业：国际组织
```

MalwarebytesLabs 的 IT 安全研究人员报告了一项新的和正在进行的恶意软件活动，其中主要目标是俄罗斯。

攻击者在这次攻击中投放的有效载荷是 KonniRAT，它于 2014 年首次被发现，被称为 Thallium 和 APT37 的朝鲜黑帽黑客组织使用。

到目前为止，KonniRAT 已经成功避开了检测，因为 VirusTotal 上只有 3 个安全解决方案能够检测到恶意软件。

详情

Konni RAT variant targeting Russia in ongoing attack campaign

3.5 SideWalk 恶意软件分析

```
日期：2021 年 08 月 24 日
等级：高
作者：Thibaut Passilly , Mathieu Tartare
标签：SideWalk, SparklingGoblin
行业：批发和零售业
```

ESET 研究人员最近发现了一个新的未公开的模块化后门 SideWalk，APT 组织 SparklingGoblin 最近针对一家位于美国的计算机零售公司的活动中使用了这个后门。这个后门与该组织使用的另一个后门 CROSSWALK 有很多相似之处。

详情

The SideWalk may be as dangerous as the CROSSWALK

3.6 新加坡一家眼科诊所遭勒索软件攻击，73,500 名患者数据被泄露

```
日期：2021 年 08 月 27 日
等级：高
来源：ehackingnews
标签：Cyber Attacks, Exposed Patient Records, IT system, MOH,
↪ Ransomware attack, Singapore
行业：卫生和社会工作
```

8 月初，一家私人眼科诊所的约 7.35 万名患者的个人信息和诊疗信息遭到勒索软件攻击，这是一个月内第三次发生此类事件。

据眼科和视网膜外科医生说，数据包括姓名、地址、身份证号码、联系信息和临床信息。

详情

73,500 Patients Data was Compromised in a Ransomware Attack on a Singapore Eye Clinic

3.7 Mozi 僵尸网络针对 Netgear、华为、中兴网关

```
日期：2021 年 08 月 24 日
等级：中
作者：Doug Olenick
标签：Mozi, Botnet, Netgear, Huawei, ZTE
行业：制造业
涉及组织：microsoft, huawei, ibm, ZTE
```

微软安全研究人员表示，成熟的 moziiot 僵尸网络的运营商已经对恶意软件进行了升级，使其能够在 Netgear、华为和中兴通讯制造的网关上实现持久化。

Mozi 是一种点对点僵尸网络，它使用类似 BitTorrent 的网络来感染从网关到 DVR 的连接设备。恶意软件通过利用弱 telnet 密码或未修补的 IoT 漏洞获得访问权限。Mozi 主要用于进行分布式拒绝服务攻击，但也可用于支持数据泄露和有效载荷执行。

3.7.1 涉及漏洞

3.7.2 cve-2014-2321

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-2321

详情

Mozi Botnet Targeting Netgear, Huawei, ZTE Gateways

3.8 ** 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

4 数据安全

4.1 3800 万条记录因 Microsoft 配置错误而暴露

1 日期：2021 年 08 月 24 日
2 等级：高
3 来源：ehackingnews
4 标签：API，COVID-19，Data Breach，Microsoft，Social Security Number，
↪ User Privacy，User Security
5 行业：卫生和社会工作
6 涉及组织：microsoft

据专家称，使用微软 PowerApps 门户平台的 1000 多个 Web 应用程序中的大约 3800 万条数据可以在线访问。
数据来自 covid-19 接触者追踪操作、疫苗注册和员工数据库的数据，包括家庭住址、电话号码、社会安全号码和疫苗接种状态。
详情
38 Million Records Exposed Due to Microsoft Misconfiguration

4.2 地下黑客论坛出售 7000 万 AT&T 用户的私人信息

1 日期：2021 年 08 月 23 日
2 等级：高
3 来源：ehackingnews
4 标签：Data Breach，Personal Information，Shiny Hunters，User Data，
↪ User Security

5 行业：信息传输、软件和信息技术服务业

据报道，一个臭名昭著的黑客组织 Shinyhunters，正在出售一个包含 7000 万 at&t 客户私人详细信息的数据库。然而，美国电信供应商 at&t 否认遭受数据泄露。Shinyhunters 共享了被盗数据、姓名、联系电话、实际地址、社会安全号码 (ssn) 和出生日期的样本子集。

一位匿名安全专家称样本中的四人中有两人是 at&t 数据库中的用户。

详情

Private Details of 70M AT&T Users Offered For Sale on Underground Hacking Forum

4.3 Raven Hengelsport 数据泄露暴露了 18GB 的客户数据

1 日期：2021 年 08 月 29 日
2 等级：高
3 来源：ehackingnews
4 标签：Microsoft Azure, Raven Hengelsport
5 行业：农、林、牧、渔业
6 涉及组织：microsoft, Raven Hengelsport

RavenHengelsport 总部位于荷兰德隆滕，从事渔具和设备业务。网络安全研究人员发现了一个与 RavenHengelsport 相关联的未加密的 microsoftazureblob 存储服务器。服务器上泄露大量客户信息，共计 42.5 万条，泄露的信息包括客户用户名、送货信息、回单、运费、交易和货件跟踪号码。客户 pii[个人识别信息]、姓名、居住地、电话号码、电子邮件，甚至公司客户的职位也被暴露。

详情

Raven Hengelsport Data Breach Exposes 18GB of Customer Data

4.4 ** 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

5 网络攻击

5.1 诺基亚分公司 SAC Wireless 在 Conti 勒索软件事件后遭受数据泄露

1 日期：2021 年 08 月 24 日
2 等级：高
3 来源：heimdalsecurity
4 标签：sac wireless，Nokia Branch，Ransomware，Conti，Data Breach
5 行业：制造业
6 涉及组织：experian，Nokia，sac wireless

在诺基亚子公司 sacwireless 的系统被加密且数据在 contiransomware 集团进行的网络攻击中被盗后，该公司披露其遭受了数据泄露。

该公司发现，conti 勒索软件开发人员已获得对其系统的访问权限，将文件上传到其云存储，然后于 6 月 16 日部署勒索软件以加密 sac 无线系统上的文件。

详情

Nokia Branch SAC Wireless Had Suffered a Data Breach Following a Conti Ransomware Incident

5.2 cloudflare 遭 DDoS - 每秒收到 1720 万次 http 请求

1 日期：2021 年 08 月 24 日
2 等级：高
3 作者：Comenta primero!
4 标签：cloudflare，botnet，ddos

行业：金融业
涉及组织：cloudflare

cloudflare 报告称，它面临有史以来最大的分布式拒绝服务 (ddos) 攻击。在这次攻击中，cloudflare 声称它每秒收到不少于 1720 万个 http 请求 (rps)。
此攻击由强大的僵尸网络发起，目标是金融行业的 Cloudflare 客户。几秒钟内，僵尸网络就以超过 3.3 亿个攻击请求轰炸了 cloudflare 边缘。

详情

Reportado ataque DDoS de más de 17.2M rps (el más grande hasta ahora)

5.3 新的 SideWalk 后门瞄准了美国的计算机零售业务

日期：2021 年 08 月 25 日
等级：高
作者：Ravie Lakshmanan
标签：SideWalk, Backdoor, Computer Retail Business
行业：批发和零售业
涉及组织：google

一家位于美国的计算机零售公司成为 SideWalk 后门目标，这是中国高级持续威胁组织最近开展的一项活动的一部分，该组织主要针对东亚和东南亚的实体。

详情

New SideWalk Backdoor Targets U.S.-based Computer Retail Business

5.4 未打补丁的 Microsoft Exchange 服务器遭到 ProxyShell 攻击

1 日期：2021 年 08 月 26 日
2 等级：高
3 作者：Waqas
4 标签：CISA, Cyber Attack, Exchange Server, Microsoft, ProxyShell,
↪ Vulnerability
5 行业：信息传输、软件和信息技术服务业
6 涉及组织：microsoft

研究人员发现，在 1900 个未打补丁的 MicrosoftExchange 服务器上，已经启动了 140 多个 webshell。
ProxyShell 漏洞正被不同的攻击者利用，旨在危害全球的 MSExchange 服务器。
ProxyShell 漏洞在整个 8 月份都被积极利用，而攻击者试图在利用 ProxyShell 代码后安装后门访问。

5.4.1 涉及漏洞

5.4.2 cve-2021-34473

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-34473

5.4.3 cve-2021-34523

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-34523

5.4.4 cve-2021-31207

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-31207

详情

Unpatched Microsoft Exchange servers hit with ProxyShell attack

5.5 21 岁的年轻人是 T-Mobile 黑客攻击的幕后黑手

日期：2021 年 08 月 26 日
等级：高
作者：Jonathan Greig
标签：21-year-old, T-Mobile, turkey
行业：信息传输、软件和信息技术服务业
涉及组织：twitter, fbi

一名居住在土耳其的 21 岁本地人承认，他是大规模 t-mobile 黑客攻击的幕后主力，这次黑客攻击暴露了超过 5000 万人的敏感信息。

他最初是在 7 月份通过未受保护的路由器获得了 t-mobile 网络的访问权限。他一直在通过互联网地址寻找 t-mobile 的漏洞，并进入了华盛顿东韦纳奇附近的一个数据中心，在那里他可以探索该公司的 100 多台服务器。

到 8 月 4 日，他已经窃取了数百万份文件

详情

21-year-old tells WSJ he was behind massive T-Mobile hack

5.6 黑客出售超过 130 万俄罗斯人的护照

1 日期：2021 年 08 月 26 日
2 等级：高
3 来源：ehackingnews
4 标签：Data Breach, Database Leaked, Hackers News
5 行业：批发和零售业

黑客在网络犯罪论坛 raidforums 上发布了一个 809GB 的档案，其中包含超过 130 万份俄罗斯公民护照扫描件，这些文件是在入侵化妆品公司 oriflame 的服务器后被盗的。

7 月 31 日和 8 月 1 日，oriflame 遭受了一系列网络攻击，导致该公司的信息系统被未经授权访问。

oriflame 保证用户的银行帐号、电话号码、密码和商业交易不受攻击影响。

详情

Hackers put up for sale the passports of more than 1.3 million Russians

5.7 Cosmos 数据库严重漏洞影响了数以千计的 Microsoft Azure 客户

1 日期：2021 年 08 月 27 日
2 等级：高
3 作者：Ravie Lakshmanan
4 标签：Cosmos, Microsoft Azure, nosql
5 行业：信息传输、软件和信息技术服务业
6 涉及组织：microsoft, automatic

云基础设施安全公司 wiz 披露了 azurecosmos 数据库漏洞的细节，目前该漏洞已修复。

该漏洞允许任何 azure 用户在未授权的情况下对其他客户的数据库进行完全管理和访问。

该漏洞授予读取、写入和删除权限，被称为“chaosdb”

详情

Critical Cosmos Database Flaw Affected Thousands of Microsoft Azure Customers

5.8 ** 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

6 其它事件

6.1 Razer Synapse 漏洞：简单鼠标插入，即可获得 Windows 系统权限

日期：2021 年 08 月 23 日
等级：高
来源：heimdalsecurity
标签：razer, Windows, Vulnerability
行业：制造业
涉及组织：twitter, razer

漏洞产生于 razersynapse，razer 是金融领域、消费电子、游戏设备和计算机外围设备制造商的服务供应商。
这家科技公司因其生产的游戏键盘和鼠标而最受欢迎。
该漏洞只需将其插入计算机即可。当此类设备连接到 Windows10 或 11 时，razersynapse 会自动下载和安装软件和驱动程序。
详情
Razer Synapse Vulnerability: with a Simple Mouse Plugging in, Windows System Privileges Are Achieved

6.2 ** 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

7 时间线

2021-08-30 360CERT 发布安全事件周报

A 产品侧解决方案

若想了解更多信息或有相关业务需求，可移步至http://360.net

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。