NSFOCUS

2024 上半年

全球云上数据泄露风险分析报告

关于绿盟科技

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日起在深圳证券交易所创业板 上市，证券代码：300369。绿盟科技在国内设有 40 多个分支机构，为政 府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国 硅谷、日本东京、英国伦敦、新加坡设立海外子公司，深入开展全球业务，打造全球网络安全行业的中国品牌。

关于星云实验室

绿盟科技星云实验室专注于云计算安全、云原生安全、解决方案研究与虚拟化网络安全问题研究。基于 IaaS 环境的安全防护，利用 SDN/NFV 等新技术和新理念，提出了软件定义安全的云安全防护体系。承担并完成多个国家、省、市以及行业重点单位创新研究课题，已成功孵化落地绿盟科技云安全解决方案、绿盟科技云原生安全解决方案。

版权声明

NSFOCUS

CONTENTS

执行摘要

近年来，随着云计算技术的迅猛发展，企业在公有云和混合云环境中的业务部署显著增加，随之而来的云租户及云环境安全风险也大幅提升，尤其是云上数据泄露风险持续攀升，许多企业因配置错误等问题发生了严重的数据泄露事件，引发了广泛关注。

绿盟科技创新研究院在云上风险发现和数据泄露领域已有多年深入研究，目前已发布了多篇报告，包括《2021 绿盟科技网络空间测绘年报》[1]、《2022 绿盟科技网络空间测绘年报云上风险测绘篇》[2] 和《2023 公有云安全风险分析报告》[3]。2023 年，全球发生了多起云上数据泄露事件，例如，2023 年 2 月，由于配置错误，Digital Ocean 的对象存储公开可访问，导致印度跨国银行的数百万条数据泄露 [4]，2023 年 5 月，Toyota Connected 因云配置错误发生大规模数据泄露，泄露持续了多年 [5]。

今年我们持续关注全球云上数据泄露风险态势，本报告首先对 2024 上半年发生的云上数据泄露事件分类和映射的 ATT&CK 攻击技术进行了具体说明，以便读者易于理解后续内容。

其次，我们对 2024 上半年全球发生的较大规模云上数据泄露风险和事件进行了详细分析，据绿盟科技创新研究院的统计，2024 年上半年全球发生了 16 起云上数据泄露事件，泄露总量约为 12 亿公民隐私数据。在 16 起事件中，发生云上数据泄露事件最多的国家是美国，共发生 8 起，涉及泄露数据高达 10 亿。行业方面，零售业泄露数据量最多，约 9.4 亿条。事件原因方面，11 起事件是由杂项错误引起，造成约 2567 万数据泄露；1 起事件是由 Web 应用攻击引起，造成约 1.25 亿数据泄露；4 起事件是由系统入侵引起，造成约 10.5 亿数据泄露。本报告主要聚焦于事件成因分析。由于大多数事件成因相似，限于篇幅，我们选取了十起典型行业案例进行详细说明，以展示云上数据泄露的整体态势。

最后，根据事件背后的成因分析，我们针对性地提出了相应的安全建议。本报告旨在提升公众对云上数据泄露的关注，并深入了解其背后成因，以便及时采取有效措施降低云上数据泄露风险，保护资产安全。

专业名词解释

云上数据：泛指公有云、自建云、混合云、多云服务上运行的业务数据。

ATT&CK：MITRE 在 2013 年推出了 ATT&CK™ 模型，全称为 Adversarial Tactics, Techniques,and Common Knowledge(ATT&CK)，它是一个站在攻击者的视角来描述攻击中各阶段用到的技术的模型 [6]。将已知攻击者行为转换为结构化列表，将这些已知的行为汇总成战术和技术，并通过几个矩阵以及结构化威胁信息表达式 (STIX)、指标信息的可信自动化交换 (TAXII) 来表示。

事件分类：在云上数据泄露事件的视角下，事件分类可以帮助企业识别、分析和应对不同类型的数据泄露风险，典型的事件分类如基础 Web 应用攻击、拒绝服务攻击、丢失或被窃取的资产等。

01

云上数据泄露事件分类说明

在对 2024 年上半年的云上数据泄露事件进行深入分析之前，我们首先归纳云上数据泄露事件的主要攻击路径和手法，并梳理云上数据泄露事件分类，有助于读者在后续的具体事件分析章节中更好地理解事件成因与事件分类之间的对应关系。

关于事件分类，我们参考了 VERIZON 数据泄露报告 [7] 中的事件分类模式（Incident Classification Patterns），其中包括以下八种模式：

- Basic Web Application Attacks：基础 Web 应用攻击，攻击主要针对 Web 应用程序，攻击范围为边界攻击，未侵入系统内部进行额外操作。
- Denial of Service：拒绝服务攻击，此类攻击旨在破坏网络和系统的可用性，包括网络层和应用层攻击。
- Lost and Stolen Assets：遗失和被盗窃的资产，包括由于误放置或恶意行为而丢失的资产。
- Miscellaneous Errors：杂项类错误，涵盖因无意行为直接危及信息资产安全性的事件。但不包括丢失设备，这类行为应归类为盗窃。
- Privilege Misuse：特权滥用，此类攻击主要指未经授权或恶意使用合法权限所导致的行为。
- Social Engineering：社会工程学，此类攻击涉及对人的心里操控，诱使受害者采取某种行为违反保密性。
- System Intrusion：系统入侵，指相对复杂的攻击，如利用恶意软件和黑客技术实现目标。
- Everything Else：其他项，泛指不符合以上 7 种分类模式范围的事件类型。

关于云上攻击路径及其涉及的具体技术，我们引用了 MITRE ATT&CK 矩阵 [1]，在接下来的章节中，我们将从多个维度对具体事件进行深入解读，包括：事件时间、泄露规模、事件回顾、事件分析、VERIZON 事件分类以及所使用的 MITRE ATT&CK 技术，这些维度将帮助我们更全面地理解云上攻击的特征与趋势。

1 https://attack.mitre.org/

02

2024 上半年全球云上数据泄露典型事件解读

2.1 西班牙房屋租赁公司 Escapada Rural 泄露 300 万客户信息

事件时间：2024 年 1 月 8 日

泄露规模：约 290 万客户的个人信息，包含姓名、电子邮件地址、电话号码等

事件回顾：

2024 年 1 月 8 日，Cybernews 研究团队发现一个允许任意用户访问的 Amazon S3 对象存储服务，并定位到该服务归属于西班牙一家提供房屋租赁服务的公司——Escapada Rural。该对象存储服务中的一个 CSV 文件中有约 290 万客户信息，包含姓名、电子邮件地址、性别、出生日期和电话号码等。另外，该 S3 对象存储中还包含一个数据库备份文件，但其中信息并不太敏感，多是一些来自 booking 和其他平台的房产列表信息。

Cybernews 研究团队进一步研究发现，他们并不是第一个发现该暴露服务的。2023 年 7 月，不法分子 louhunter 已将该数据集发布在 BreachForums 论坛[1] 进行售卖。而 Escapada Rural 在这六个月期间并未发现数据泄露问题。

1 https://breachforums.st/

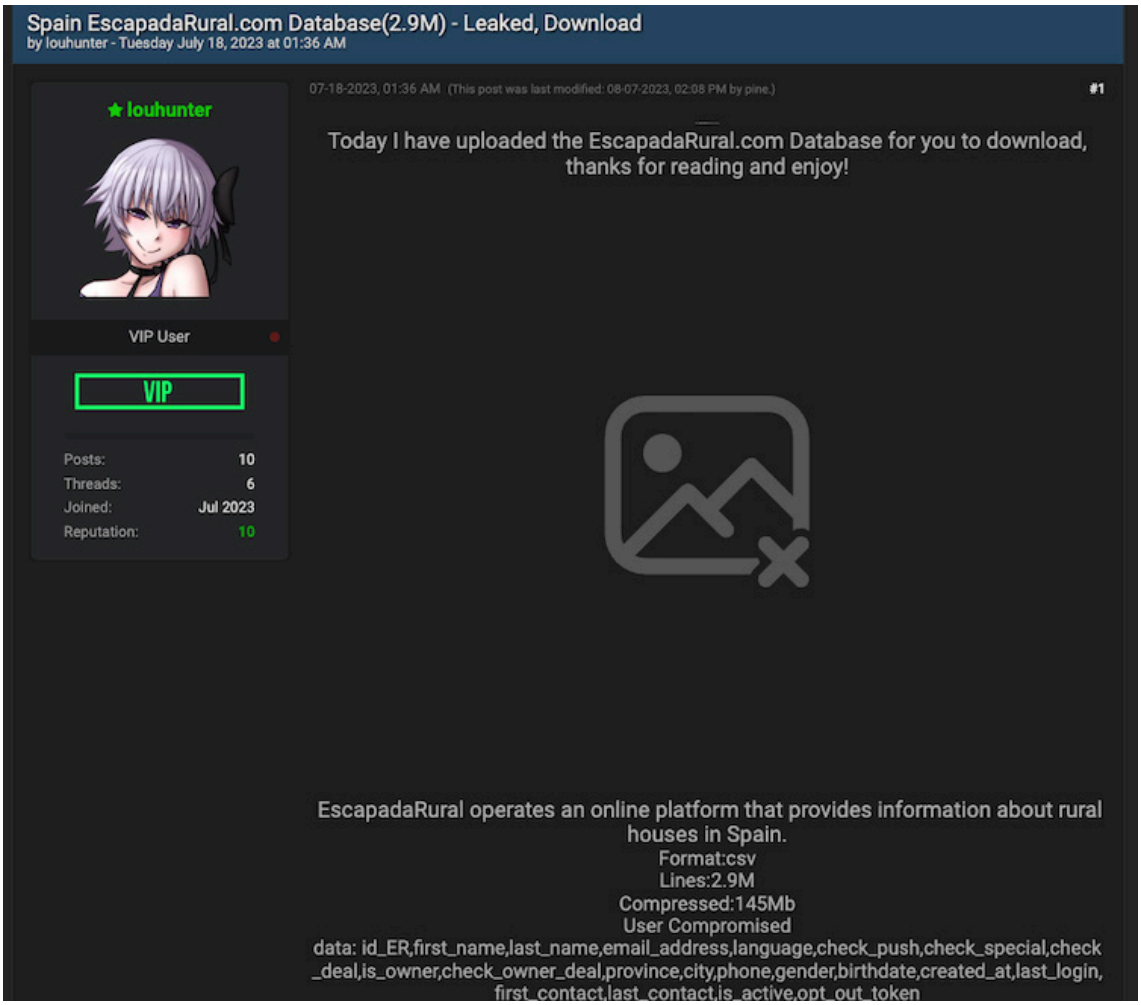

图 1 S3 对象存储中的敏感信息

事件分析：

Amazon S3 是亚马逊云提供的一项对象存储服务，它提供了可配置的安全性、数据保护、合规性和访问控制功能保护用户的数据安全 [8]。但是对于对象存储服务的访问，Amazon 并未强制要求配置访问控制策略，用户仍可以配置对象存储服务的公开访问。

导致此次数据泄露事件的主要原因是服务配置错误。Escapada Rural 公司未对其使用的 Amazon S3 对象存储服务配置安全的访问控制策略，可能导致任何人均可公开访问该对象存储服务，包含恶意攻击者。

VERIZON 事件分类：Miscellaneous Errors（杂项错误）

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1593 搜索开放网站 / 域	.002 搜索引擎	攻击者可能利用网络空间搜索引擎进行情报收集。
T1133 外部远程服务	N/A	攻击者识别暴露服务中的 Amazon S3 对象存储服务。
T1587 开发功能	.004 利用工具	攻击者开发对暴露服务进行安全测试的工具。
T1530 云存储中的数据	N/A	攻击者访问 Amazon S3 对象存储服务的数据。
T1567 通过 Web 服务外泄	N/A	攻击者可能利用 Web 服务进行数据窃取。

参考链接：https://cybernews.com/security/data-leak-escapada-rural/

2.2 在线词典 Glosbe 泄露近 700 万用户数据

事件时间：2024 年 3 月 7 日

泄露规模：700 万用户个人数据、加密密码、社交媒体账号及其他信息

事件回顾：

2023 年 12 月，Cybernews 研究团队发现一个互联网中能够公开访问的 MongoDB 数据库服务，该服务中包含近 700 万用户的个人数据、加密密码、社交媒体标识符和其他详细信息。通过分析，Cybernews 研究团队定位到该服务归属于 Glosbe 在线词典，它号称支持世界上所有语言。

Cybernews 研究团队于当月联系了 Glosbe 官方人员通报此次事件。虽然 Glosbe 并未对此进行正面回复，但涉事 MongoDB 服务已被关闭。2024 年 3 月，Cybernews 研究团队在官方 Blog 中发布了该事件说明。

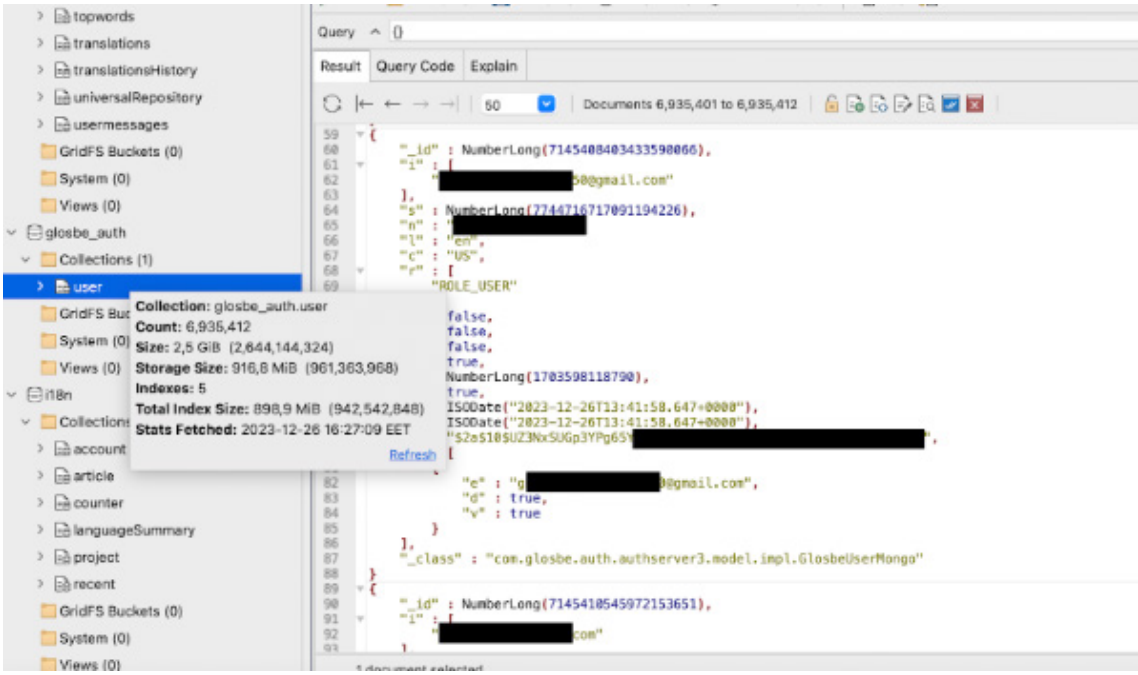

图 2 Mongo 数据实例截图

事件分析：

MongoDB 是一种面向文档的数据库系统，广泛用于处理非结构化数据 [9]。MongoDB 社

区版的默认配置不会启用访问控制和身份验证机制，这意味着数据库在安装后，如果没有进一步进行安全配置，数据库里的数据将公开给所有可以访问的人。

导致此次数据泄露事件的主要原因是服务配置错误，包含以下两点：

1. 未设置访问控制列表（ACL），使得任何人可以通过公开的 IP 地址访问。

2. 未启用认证机制，使得任何可以访问数据库的人可以操作数据库中的数据。

这些配置错误让攻击者能够轻松使用扫描工具发现并访问未保护的数据库实例，从而窃取其中的敏感信息。

VERIZON 事件分类：Miscellaneous Errors（杂项错误）

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1593 搜索开放网站 / 域	.002 搜索引擎	攻击者可能利用网络空间搜索引擎进行情报收集。
T1133 外部远程服务	N/A	攻击者识别暴露服务中的 MongoDB 服务。
T1587 开发功能	.004 利用工具	攻击者开发对 MongoDB 服务进行安全测试的工具。
T1530 云存储中的数据	N/A	攻击者访问 MongoDB 服务的数据。
T1567 通过 Web 服务外泄	N/A	攻击者可能利用 Web 服务进行数据窃取。

参考链接：https://cybernews.com/security/glosbe-dictionary-leaks-user-data/

2.3 谷歌云服务 Google Firebase 泄露 1.25 亿条用户记录

事件时间：2024 年 3 月 18 日

泄露规模：数百个网站暴露了总计约 1.25 亿条用户记录

事件回顾：

2024 年 3 月 18 日，三位独立安全研究员发表了一篇帖子，称他们扫描了 5.5 万个网站中的 JavaScript 代码，发现超 900 个 Google Firebase 凭证信息，可能导致近 1.25 亿条用户信息泄露，包括明文密码、账单等敏感信息。

之后，三位安全研究员在 13 天内共计给受影响的网站运营者发送了 842 封电子邮件。其中，85% 电子邮件已送达，9% 电子邮件被退回。不久之后，约 24% 的网站修复了该问题。其中，约 1% 的网站运营者进行了邮件回复，0.2% 网站运营者给三位安全研究员提供了漏洞赏金。

事件分析：

Google Firebase[1] 是一项由 Google 提供的云服务，通过提供实时数据库、认证、云存储、云函数、推送通知等一系列工具和服务，帮助开发者构建高质量的应用程序 [10]。虽然 Google Firebase 提供了完善、可扩展安全规则，用于保护用户在 Cloud Firestore、Firebase Realtime Database 和 Cloud Storage 中存储的数据，但它并不会对用户配置的不安全规则进行告警，如“允许所有人访问”。

导致此次数据泄露事件的一个原因是由于开发者在网站开发过程中硬编码了明文 Google Firebase 凭证，且未安全、合理地设置凭证的访问策略，导致攻击者能够轻易使用这些凭证达到目的。除此之外，这些开发者也并未对其网站设置健全的反爬虫机制，容易遭受爬虫程序的分析。

VERIZON 事件分类：Basic Web Application Attacks（基础 Web 应用攻击）

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1593 搜索开放网站 / 域	.002 搜索引擎	攻击者可能利用网络空间搜索引擎进行情报收集。
T1587 开发功能	.004 利用工具	攻击者开发用于收集 Google Firebase 凭证的工具。
T1133 外部远程服务	N/A	攻击者利用工具扫描网站、js 中的凭证。
T1588 获得能力	.002 工具	攻击者使用已有工具对凭证进行安全测试。
T1078 有效账户	.004 云账户	攻击者利用云账户进行服务访问。
T1530 云存储中的数据	N/A	攻击者访问 Google Firebase 中的数据。
T1567 通过 Web 服务外泄	N/A	攻击者可能利用 Web 服务进行数据窃取。

参考链接：https://env.fail/posts/firewreck-1/

1 https://firebase.google.com/?hl=zh-cn

2.4 中国某公证处 1.9 万公民信息、公正材料存在泄露风险

事件时间：2024 年 3 月 28 日

泄露规模：1.9 万公民信息、公正材料

事件回顾：

2023 年 3 月，绿盟科技创新研究院发现一个部署在阿里云上的 Gogs 源代码仓库，且未存在任何访问控制策略和身份认证机制。该源代码仓库的所有源代码项目可被任意访问和下载。部分源代码中包含数据库、对象存储服务凭证，导致超 1.9 万敏感信息存在泄露风险，包含公民信息（身份证、姓名、地址等）、公正委托书、询问笔录等存在泄露风险。

研究员通过技术手段定位到该镜像仓库的归属组织机构为国内公证机构后，第一时间将此情报通报给该公司属地监管单位，并协助监管单位对涉事公司存在的数据泄露风险进行治理。

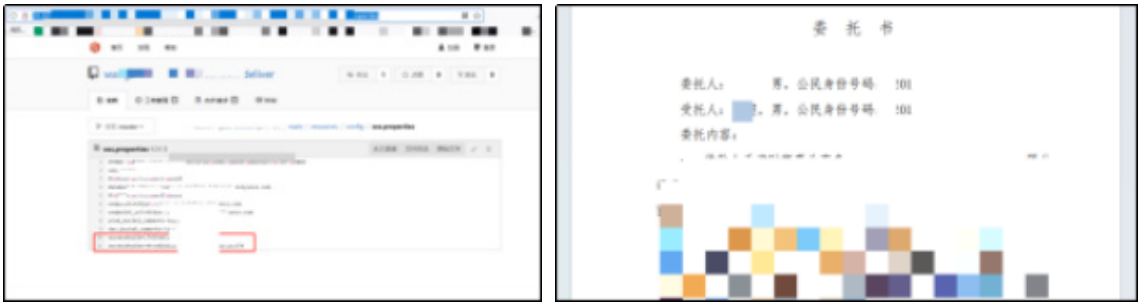

图 3 Gogs 泄露敏感数据截图

事件分析：

Gogs 是一款极易搭建的自助 Git 服务。Gogs 旨在打造一个以最简便的方式搭建简单、稳定和可扩展的自助 Git 服务 [11]。Gogs 支持多种授权认证方式：LDAP-BindDN、LDAP-simple auth、PAM、SMTP 及 Freeipa。但若未在 Gogs 启动时配置相关授权认证文件，则 Gogs 是存在未授权访问的。只要互联网可达，任何人都可以对 Gogs 进行访问，查看其中的源代码项目。

导致此次事件的原因主要有三点，第一，所使用搭建代码仓库的云服务器未设置网络相关的访问控制策略；第二，未开启 Gogs 代码仓库的授权认证机制；第三，源代码项目配置文件中硬编码了明文重要凭证。最终，导致该公证处多个后端系统源代码、公民信息、公正

材料存在泄露风险。

VERIZON 事件分类：Miscellaneous Errors（杂项错误）

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1593 搜索开放网站 / 域	.002 搜索引擎	攻击者可能利用网络空间搜索引擎进行情报收集。
T1133 外部远程服务	N/A	攻击者识别暴露服务中的 Gogs 源代码服务。
T1587 开发功能	.004 利用工具	攻击者开发对暴露服务进行安全测试的工具，以及凭证识别工具。
T1552 不安全凭证	.001 文件中的凭证	攻击者识别源代码中的硬编码的凭证信息。
T1078 有效账户	.004 云账户	攻击者利用云账户进行服务访问。
T1530 云存储中的数据	N/A	攻击者访问数据库、对象存储服务的数据。
T1567 通过 Web 服务外泄	N/A	攻击者可能利用 Web 服务进行数据窃取。

2.5 爱尔兰出租车软件公司 iCabbi 泄露近 30 万乘客信息

事件时间：2024 年 4 月 11 日

泄露规模：30 万名出租车乘客的个人信息，包括姓名、电话号码、电子邮件地址和用户 ID

事件回顾：

2024 年 4 月，VPNMentor[1] 的安全研究员 Jeremiah Fowler 发现一个未设置密码的数据库，其中包括乘客的姓名、电子邮件和电话号码等个人详细信息。经 Fowler 分析确认，该数据库属于爱尔兰出租车软件公司 iCabbi[2]。值得关注的是，被泄露的乘客涉及高级 BBC 主管、记者、英国政府官员及欧盟大使等重要人员。

随后，Fowler 就风险情况通知了 iCabbi，该公司承认此次事件，并表示已采取措施并通知了受影响的出租车公司，但未透露是否有实际损失发生。

Fowler 提醒用户警惕来自出租车服务提供商的网络钓鱼攻击和可疑邮件，尤其是当攻击者掌握了敏感的联系信息和电话时，可能会利用这些信息进行更加针对性的攻击。

事件分析：

由于事件披露的信息中并未提及关于数据库的更多信息，我们无法做更多的分析。但其原因和事件 2 在线词典 Glosbe 泄露近 700 万用户数据事件相似，均是由于未限制数据库访问范围，从而使资产公开暴露于互联网，导致敏感数据被泄露，此处不再赘述。

VERIZON 事件分类：Miscellaneous Errors（杂项错误）

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1593 搜索开放网站 / 域	.002 搜索引擎	攻击者可能利用网络空间搜索引擎进行情报收集。
T1133 外部远程服务	N/A	攻击者识别暴露服务中的数据库服务。
T1587 开发功能	.004 利用工具	攻击者开发对数据库服务进行安全测试的工具。
T1530 云存储中的数据	N/A	攻击者访问数据库服务的数据。
T1567 通过 Web 服务外泄	N/A	攻击者可能利用 Web 服务进行数据窃取。

参 考 链 接：https://www.independent.ie/business/technology/personal-information-of-287000-taxi-passengers-exposed-in-data-breach/a355367209.html

1 https://www.vpnmentor.com/
2 https://icabbi.com/about-us/

2.6 巴西游戏开发公司 Asantee Games 泄露数百万玩家信息

事件时间：2024 年 4 月 21 日

泄露规模：超过 1400 万名玩家的个人数据，包括用户名、电子邮件、设备数据、游戏统计信息及加密的管理员凭证

事件回顾：

Asantee Games[1] 是一家成立于 2012 年的小型游戏开发工作室。该公司的《Magic Rampage》游戏在 Android 和 iOS 平台上的下载量超过 1000 万次。Cybernews 研究团队发现，该公司发生了一次严重的数据泄露事件，该事件影响了超过 1400 万名《Magic Rampage》游戏玩家。泄露的数据包括玩家的用户名、电子邮件、设备数据、游戏统计信息和管理员凭证等敏感信息。

随后，Cybernews 研究团队将该事件通知了 Asantee Games，虽然该公司反馈已立即采取措施保护数据库，但已泄露的数据可能对用户产生较大影响。

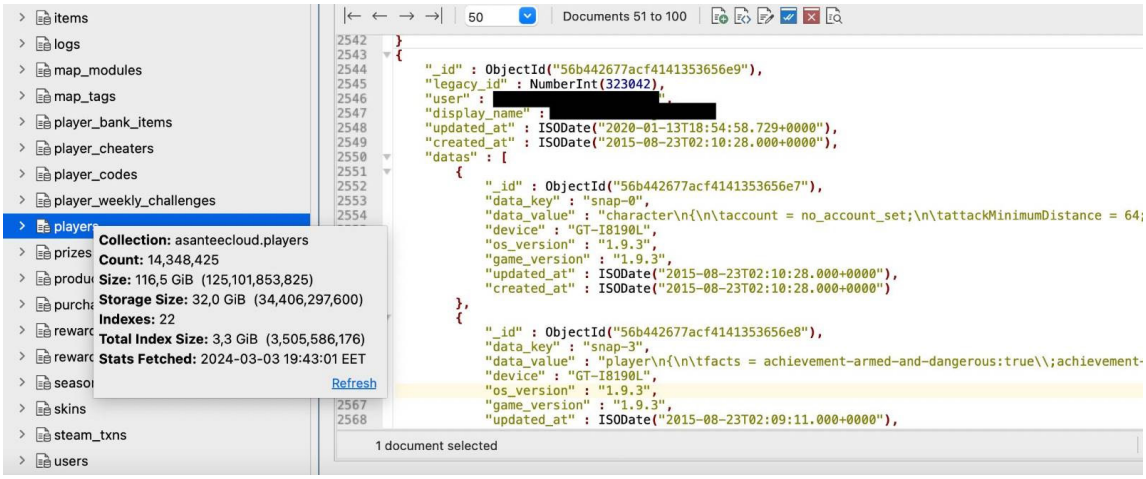

图 4 泄露的数据样本

事件分析：

MongoDB 是一种面向文档的数据库系统，广泛用于处理非结构化数据。MongoDB 社区版的默认配置不会启用访问控制和身份验证机制，这意味着数据库在安装后，如果没有进一步进行安全配置，数据库里的数据将公开给所有可以访问的人。

1 https://asanteegames.com.br/

本次 Asantee Games 的泄露事件中，同样是由于配置错误所导致，由于未配置合理的访问控制策略，因而导致攻击者能够轻松使用扫描工具发现并访问未保护的数据库实例，从而窃取包含玩家用户名、电子邮件、设备数据、游戏统计信息及管理员凭证在内的大量敏感信息。

VERIZON 事件分类：Miscellaneous Errors（杂项错误）

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1593 搜索开放网站 / 域	.002 搜索引擎	攻击者可能利用网络空间搜索引擎进行情报收集。
T1133 外部远程服务	N/A	攻击者识别暴露服务中的 MongoDB 服务。
T1587 开发功能	.004 利用工具	攻击者开发对 MongoDB 服务进行安全测试的工具。
T1530 云存储中的数据	N/A	攻击者访问 MongoDB 服务的数据。
T1567 通过 Web 服务外泄	N/A	攻击者可能利用 Web 服务进行数据窃取。

参考链接：https://cybernews.com/security/magic-rampage-asantee-games-data-leak/

2.7 全球票务公司 Ticketmaster 泄露约 5.6 亿用户信息

事件时间：2024 年 5 月 28 日

泄露规模：约 5.6 亿用户个人信息，包括姓名、电子邮件地址、付款信息和购票历史记录

事件回顾：

2024 年 5 月 28 日，Hackread[1] 报道了一起涉及 Ticketmaster[2] 的严重数据泄露事件，如图 5 所示，Ticketmaster 约 5.6 亿用户的身份信息被黑客组织 ShinyHunters[3] 在 BreachForum 上以 50 万美元的价格一次性出售。这些被出售的信息主要涉及大量用户敏感信息（姓名、地址、邮件地址、电话）、门票、活动详情、订单信息（姓名、卡号后四位数字、有效期）等。

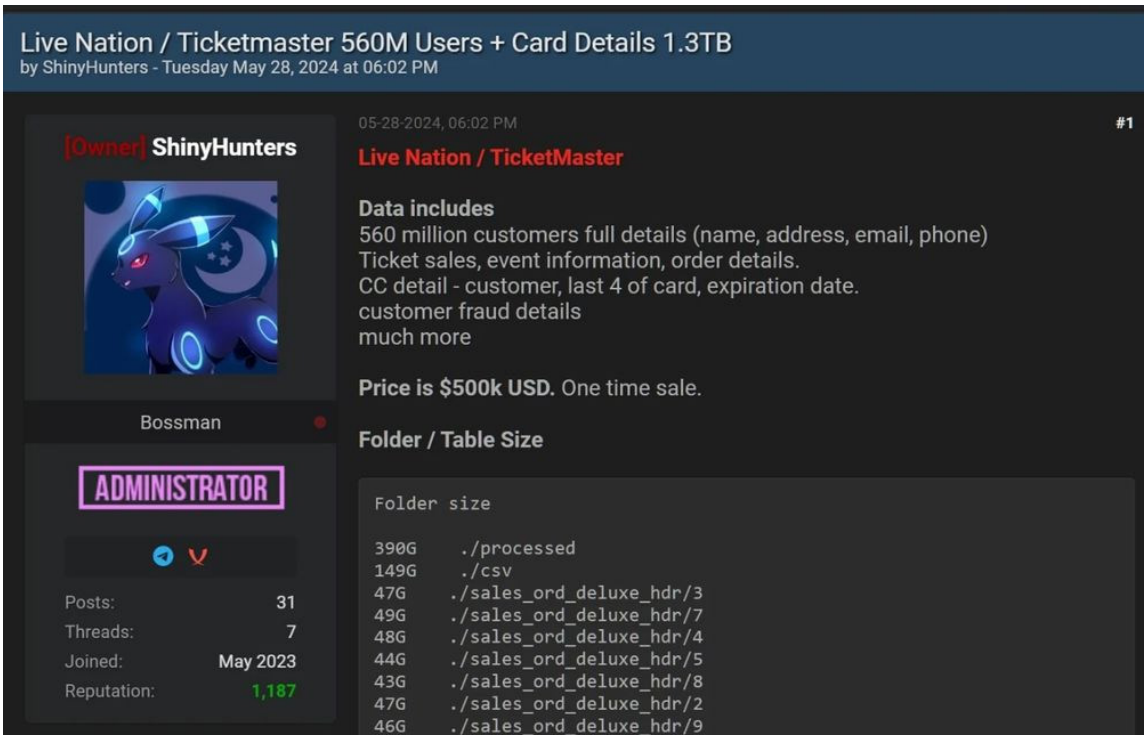

图 5 在暗网上售卖的 Ticketmaster 相关信息

2023 年 5 月 31 日，Ticketmaster 的母公司 Live Nation Entertainment 在向美国证券交易委员会（SEC）提交的一份文件中确认 [12]，其第三方云上数据库环境于 5 月 20 日遭遇了

1 https://hackread.com/
2 https://en.wikipedia.org/wiki/Ticketmaster
3 https://en.wikipedia.org/wiki/ShinyHunters

大量未授权访问。这一事件主要涉及 Ticketmaster LLC 的公司数据。尽管该事件的潜在影响被认为对公司业务不大，但 Live Nation 仍表示将持续评估相关风险并采取补救措施。

Ticketmaster 在其官方网站上发表了声明，重申用户的 Ticketmaster 账户是安全的，并强调此次数据泄露源自第三方数据服务供应商。泄露的数据库包含北美（包括美国、加拿大和墨西哥）活动门票购买者的客户信息 [13]。Ticketmaster 表示，他们正在通过电子邮件或书面形式通知受影响的客户，并与执法部门及银行合作进行调查。此外，为了保护客户数据安全，Ticketmaster 承诺为相关客户提供 12 个月的免费身份监控服务。

Ticketmaster 声称他们正在邮件或者书面通知受影响的客户，并与执法部门、银行进行合作调查。同时，Ticketmaster 承诺将为相关客户免费提供 12 个月的身份监控服务，以保护客户数据安全。

虽然 Live Nation 和 Ticketmaster 在回应中没有明确指出具体的第三方公司，但据 Hackread 的跟踪报道，涉及的公司可能是 Snowflake Inc.[14]。Snowflake 是一家提供 SaaS 化数据库服务的公司，为超过 1 万家公司提供服务 [1]。Snowflake 随后在官方网站上发表了声明，澄清此次数据泄露与其产品本身无关，并持续进行更新 [15]。

事件分析：

根据 Mandiant 分享的 Snowflake 攻击调查文章，数据泄露事件的根本原因被认定为凭证泄露 [16]。报告显示，在这次数据泄露中，超过 79.7% 的 Snowflake 客户凭证曾被各种信息窃取软件盗取，涉及的恶意软件包括 VIDAR、RISEPRO、REDLINE、RACOON STEALER、LUMMA 和 METASTEALER 等。

Mandiant 的调查还发现，一名 Snowflake 前雇员的个人凭证被窃取，攻击者利用该凭证访问了 Snowflake。然而，Snowflake 声明该账户用于测试，且不含敏感数据，与此次数据泄露事件无关联。这些被植入恶意软件的设备通常来自 Snowflake 的客户或外包公司的服务系统。

如图 6 所示，如果 Snowflake 未启用多因素身份验证，攻击者（UNC5537）可以通过被盗的凭证直接登录到 Snowflake，对数据实施盗窃。一般而言，攻击者在获取 Snowflake 凭证后，可以通过匿名 VPS 上的 SnowSight（可视化界面）或 SnowSQL（命令行工具）连接客户的 Snowflake 实例。此外，他们甚至可以分析和收集数据中的其他认证口令，以获取更多敏感

1 https://www.snowflake.com/en/company/overview/about-snowflake/

信息或实施更进一步的攻击。

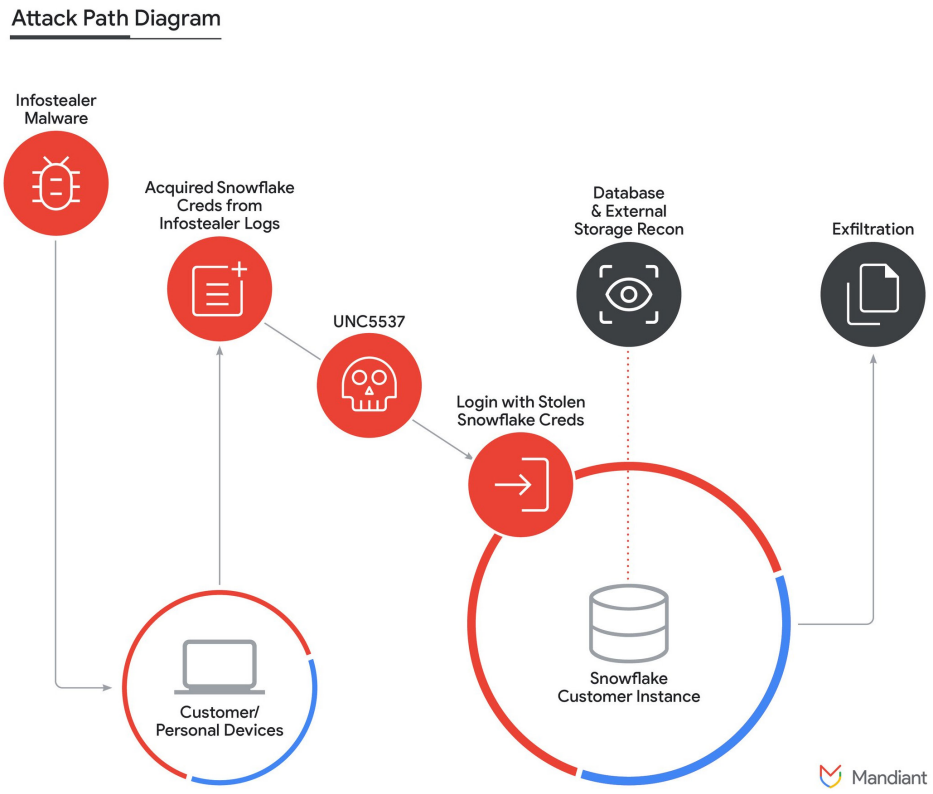

图 6 Snowflake 攻击路径示意图

VERIZON 事件分类：System Intrusion(系统入侵)

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1589 收集受害者身份信息	.002 电子邮件地址	攻击者可能利用社交媒体或网络引擎引擎收集受害者电子网邮件地址。
T1566 网络钓鱼	.001 鱼叉式网络钓鱼 - 附件 .002 鱼叉式网络钓鱼 - 链接	攻击者定向发送伪装的恶意附件或者执行恶意程序的连接。
T1204 用户执行	.001 恶意连接 .002 恶意文件	诱使受害者执行恶意文件或者点击恶意链接。
T1087 账号发现	.004 云账户	通过恶意程序获取受害者本地信息，发现 Snowflake 凭证
T1078 有效账户	.004 云账户	通过恶意程序窃取 Snowflake 凭证，使用 Snowflake 凭证登录 Snowflake 服务。
T1041 通过 C2 通道进行数据外泄	N/A	攻击者可能通过现有的命令和控制通道窃取数据。

参考链接：https://hackread.com/hackers-ticketmaster-data-breach-560m-users-sale/

2.8 中国某信息技术公司自建镜像仓库存在泄露风险

事件时间：2024 年 5 月 23 日

泄露规模：18 万公民信息，包含姓名、身份证、电话、工作单位等。

事件回顾：

2023 年 5 月 23 日，绿盟科技创新研究院发现一个部署在阿里云上的 Harbor 镜像仓库存在未授权访问的镜像。能够访问的镜像文件中包含数据库、对象存储服务凭证，导致超 18 万公民敏感信息存在泄露风险，包含姓名、身份证、电话、工作单位等。

研究员通过技术手段定位到该镜像仓库的归属组织机构为国内某信息技术公司后，第一时间将此情报通报给该公司属地监管单位，并协助监管单位对涉事公司存在的数据泄露风险进行治理。

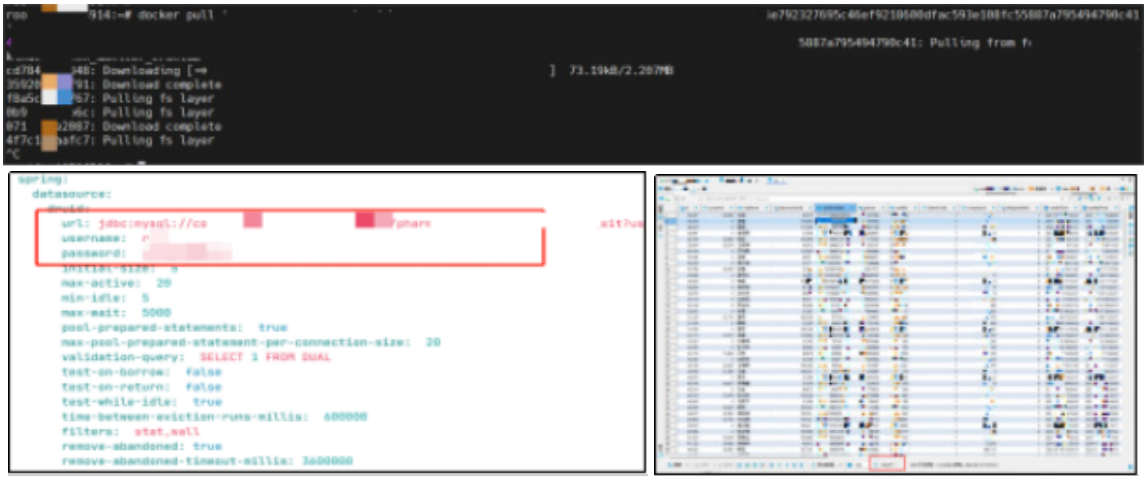

图 7 仓库泄露的泄露敏感数据截图

事件分析：

Harbor 是一个开源的企业级 Docker Registry 管理项目，由 VMware 公司开源 [17]。Harbor 提供了集中式的镜像管理、安全性控制、镜像复制等功能，帮助用户更好地管理和存储 Docker 镜像。虽然 Harbor 有完整的访问控制机制，但若使用者将镜像项目设置为公开，则任意用户可以对其进行访问和拉取。这是 Harbor 官方承认的特性之一，许多安全意识不足的开发者容易导致镜像泄露风险。

导致此次事件的原因主要有三方面：

首先，所使用搭建镜像仓库的云服务器未设置网络相关的访问控制策略；

其次，该镜像仓库中存在被设置为公开的镜像项目；

最后，该镜像文件系统中的配置文件中硬编码了明文数据库的配置信息，从而导致该信息技术公司多个后端系统源代码、数据库配置信息、公民信息存在泄露风险。

VERIZON 事件分类：Miscellaneous Errors（杂项错误）

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1593 搜索开放网站 / 域	.002 搜索引擎	攻击者可能利用网络空间搜索引擎进行情报收集。
T1133 外部远程服务	N/A	攻击者识别暴露服务中的 Harbor 镜像服务。
T1587 开发功能	.004 利用工具	攻击者开发对暴露服务进行安全测试的工具，以及凭证识别工具。
T1552 不安全凭证	.001 文件中的凭证	攻击者识别镜像中的硬编码的凭证信息。
T1078 有效账户	.004 云账户	攻击者利用账户进行数据库服务访问。
T1530 云存储中的数据	N/A	攻击者访问数据库存储服务的数据。
T1567 通过 Web 服务外泄	N/A	攻击者可能利用 Web 服务进行数据窃取。

2.9 美国电信巨头 AT&T 泄露约 1.1 亿用户电话记录

事件时间：2024 年 7 月 12 日

泄露规模：约 1.1 亿用户的电话记录，包括通话记录、短信记录及位置数据。

事件回顾：

2024 年 7 月 12 日，TechCrunch[1] 发表文章称美国电话公司 AT&T[2] 发生严重数据泄露事件，攻击者几乎窃取了 2022 年 5 月 1 日至 2022 年 10 月 31 日以及 2023 年 1 月 2 日所有 AT&T 客户的电话记录。泄露的数据包括双方的电话号码、通话时长、基站 ID 等敏感信息，但不含通话内容和短信内容。

AT&T 表示，其已于 4 月 19 日发现了此次数据泄露事件，随即聘请网络安全专家展开调查并上报了监管机构。AT&T 表示本次事件与 3 月份的数据泄露事件 [18] 无关，发言人 Huguely 向 TechCrunch 透露，此次泄露的数据是从 Snowflake 上窃取的。

AT&T 就此次数据泄露事件在其官网上进行了公示 [19]，文中表示，泄露的客户数据来源于第三方云平台的非法下载，目前这些被盗的数据尚未公开，他们正在与执法部门合作以逮捕涉案罪犯。AT&T 特别表明，当前抓捕行动已经取得进展，至少一名罪犯已经被捕。

事件分析：

由于对国家安全或公共安全存在潜在风险，此次数据泄露事件 AT&T 没有披露更多细节。但这是继事件七 全球票务公司 Ticketmaster 泄露约 5.6 亿用户信息和美国汽车售后零部件供应商 Advance Auto Parts 在 Snowflake 内存储的数据被盗事件 [20]、QuoteWizard 在 Snowflake 中存储的数据被窃取事件 [21] 之后又一起由于 Snowflake 凭证泄露导致的数据泄露事件，特别是 Advance Auto Parts 事件泄露了 3.8 亿份客户资料，影响范围之广泛，令人担忧。由此看来，Snowflake 数据被盗似乎已屡见不鲜。

攻击者利用先前购买或窃取的凭证，直接登录了未开启多因素认证的 Snowflake 账号，并窃取了其中的用户数据。值得欣慰的是，Snowflake 在最近的申明中表示，其正在制定一项计划，强制客户实施高级安全控制，如多因素身份验证 (MFA) 或网络策略等 [15]。

VERIZON 事件分类：System Intrusion(系统入侵）

所用 MITRE ATT&CK 技术：

1 https://en.wikipedia.org/wiki/TechCrunch
2 https://www.att.com/

技术	子技术	利用方式
T1589 收集受害者身份信息	.002 电子邮件地址	攻击者可能利用社交媒体或网络引擎收集受害者电子网邮件地址。
T1566 网络钓鱼	.001 鱼叉式网络钓鱼 - 附件 .002 鱼叉式网络钓鱼 - 链接	攻击者定向发送伪装的恶意附件或者执行恶意程序的连接。
T1204 用户执行	.001 恶意连接 .002 恶意文件	诱使受害者执行恶意文件或者点击恶意链接。
T1087 账号发现	.004 云账户	通过恶意程序获取受害者本地信息，发现 Snowflake 凭证
T1078 有效账户	.004 云账户	通过恶意程序窃取 Snowflake 凭证，使用 Snowflake 凭证登录 Snowflake 服务。
T1041 通过 C2 通道进行数据外泄	N/A	攻击者可能通过现有的命令和控制通道窃取数据。

参考链接：https://techcrunch.com/2024/07/12/att-phone-records-stolen-data-breach/?guccounter=1

2.10 丰田公司泄露 240GB 员工和客户信息

事件时间：2024 年 8 月 16 日

泄露规模：240GB 的文件，包含丰田员工和客户的信息以及合同和财务信息

事件回顾：

2024 年 8 月 16 日，黑客组织 ZeroSevenGroup 表示侵入了一家美国机构，窃取到了 240GB 文件，其中包含丰田员工和客户的信息及合同和财务信息。另外，他们还声称会提供带有密码的所有目标网络的 ADRecon[1]。虽然丰田没有透露泄露的日期，但 BleepingComputer 发现这些文件可能已于 2022 年 12 月 25 日被盗。

8 月 17 日，丰田汽车北美公司承认了此次数据泄露事件影响到了部分丰田员工和客户，表示他们正在与可能受影响的员工和客户对接，并在需要时提供帮助。最后，他们声称这些数据是从一个三方机构泄露的，他们自身的系统不存在漏洞，也没有遭到任何攻击。

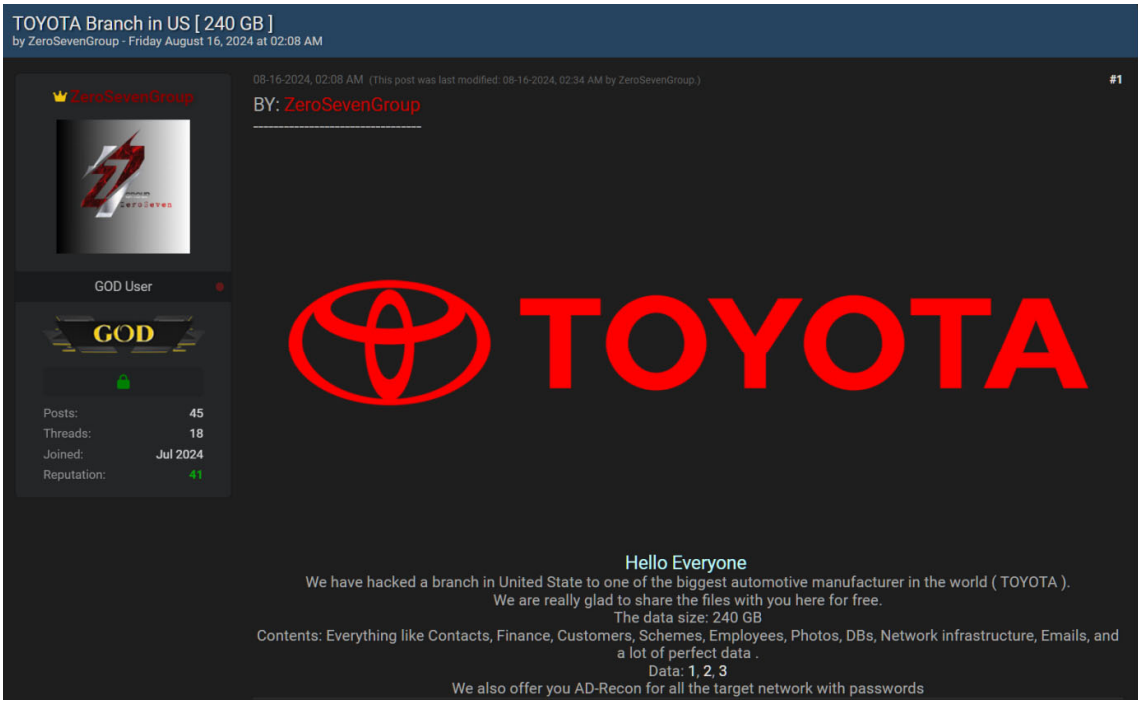

图 8 黑客组织 ZeroSevenGroup 发布的事件截图

1 ADRecon 是一种从 AD 域环境中进行信息收集的工具，包括 Domain、Trusts、Subnets 等。ADRecon 可以从能够连接到环境的任何服务器中运行，甚至包含不是域成员的主机。

事件分析：

AD 域（Active Directory Domain）是微软 Windows 网络环境中的一个核心概念，它是微软提供的一种目录服务，存储了网络中各类资源信息，如用户账户、组、计算机、共享资源等，允许网络管理员和用户通过图形界面或命令行工具来管理这些信息。

黑客组织 ZeroSevenGroup 可能通过某种攻击方式拿到目标主机权限，并使用 ADRecon 工具在主机中进行信息收集。最终，ZeroSevenGroup 发现并窃取了 240GB 的文件，涉及丰田北美公司。泄露文件内容包含：联系人、财务、客户、计划、员工、照片、数据库、网络基础设施、电子邮件等。

VERIZON 事件分类：System Intrusion（系统入侵）

所用 MITRE ATT&CK 技术：

技术	子技术	利用方式
T1588 获得能力	.002 工具	攻击者使用 ADRecon 工具。
T1059 命令行和脚本解释器	.001 PowerShell	使用命令行执行 ADRecon 工具。
T1552 不安全凭证	.001 文件中的凭证	攻击者识别 AD 域中的凭证信息。
T1530 云存储中的数据	N/A	攻击者访问 AD 域中的数据。
T1567 通过 Web 服务外泄	N/A	攻击者可能利用 Web 服务进行数据窃取。

参考链接：https://www.bleepingcomputer.com/news/security/toyota-confirms-third-party-data-breach-impacting-customers/

03

安全建议

前文我们对全球上半年云上数据泄露事件进行了详细解读，如图 9 所示，从事件分类模式上看，杂项错误是导致数据泄露的主要原因，占比高达 60%。其次为系统入侵和基础 Web 应用攻击，分别占 30% 和 10%。

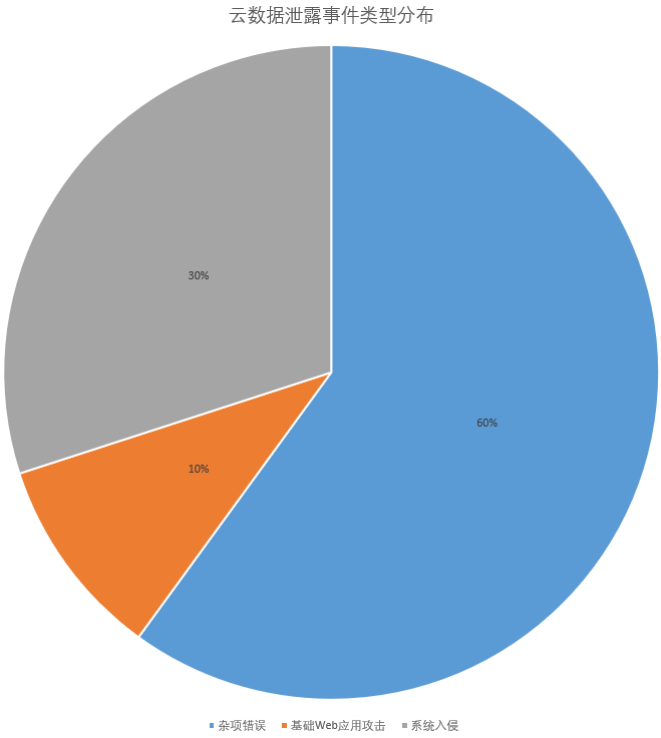

图 9 2024 上半年云上数据泄露事件类型分布

其中，杂项错误主要是错误配置导致的未授权访问，系统入侵则是通过社工、扫描攻击或者恶意软件窃取受害者账号口令，再通过这些账号口令窃取敏感信息，基础 Web 应用攻击主要是通过爬虫等技术获取凭证或未授权的服务访问路径。下面我们将针对上述事件分类模式提出相应安全建议，希望能给企业提供一些安全防护思路。

3.1 针对杂项错误的安全建议

2024 年上半年云上数据泄露事件中，其中绝大多数事件是由于服务访问控制策略配置不当导致的。这些云服务包含公有云提供的服务也包括自建类服务，如 MongoDB、Google Cloud Storage 和 Amazon S3 对象存储等均是因为配置了公开访问才进一步导致数据泄露。因此，我们提供以下安全建议：

1. 通过配置防火墙、访问控制列表（ACL）、角色访问控制（RBAC）或者服务监听策

略等方式缩小服务暴露范围。例如通过配置 bindIp 参数，限制 MongoDB 只监听特定的私有网络地址。如图 10 所示，在 mongod.conf 中设置：

```
net:
  bindIp: 127.0.0.1, 192.168.0.1  # 仅允许本地和指定IP访问
```

图 10 MongoDB 监听配置

2. 禁止服务匿名访问策略，如修改 mongod.conf 文件的“authorization" 为 "enabled”，禁止 MongoDB 匿名访问；

3. 监控和记录所有访问请求，并配置异常活动告警。如公有云服务可直接开启云审计和告警服务。例如，使用 aws cloudtrail create-trail 配置跟踪访问日志，并设置告警以监测异常活动 [22]。

3.2 针对系统入侵的安全建议

1. 设置网络隔离策略，如根据资产或业务设置多个微分段网络，针对每个微分段设置白名单放行规则等；

2. 启用多因素身份验证（MFA），增强高敏感系统和数据的访问控制；

3. 定期轮换服务账户的访问密钥和 API 密钥，并及时撤销不再使用的密钥。可利用云厂商的密钥管理服务（Key Management Service KMS）；

4. 实施集中凭证管理，防止凭证泄露。如使用 AWS Secrets Manager 或 Azure Key Vault；

5. 定期为员工提供云安全培训，内容涵盖配置管理、数据保护、凭证管理、安全监控和应急响应，提升开发人员的安全意识，确保运维人员能够快速应对泄露事件；

6. 自动撤销离职员工对系统的访问权限，包括云服务平台、内部系统、邮件账户和第三方服务等，并停用和删除相关的账户和认证口令；

7. 对所有敏感数据进行加密处理，无论是静态存储还是传输过程中的数据，确保即使数据泄露，攻击者也无法读取。

3.3 针对基础 Web 应用攻击的安全建议

1. 建立 Web 应用反爬机制，如针对频繁请求使用验证码、通过 IP 地址限制请求频率、使用 AJAX 加载部分内容等；

2. 建议强制启用多因素身份验证（MFA），即使攻击者获取了用户名和密码，也无法轻易登录系统；

3. 服务设置登录失败次数限制，防止密码暴破；

4. 服务定期提醒用户修改密码，若未及时修改，则自动重置为高强度密码。

3.4 其他建议

除以上针对性建议外，用户还可以参考通用类缓解措施以降低数据泄露风险 :

1. 使用外部攻击面管理平台（EASM）方案，扫描和监控网络资产，识别公网暴露资产、漏洞和配置错误，结合真实攻击路径评估可能存在泄露风险的资产和数据。借助这些自动化的技术方案，企业可以更全面、精确地管理外部威胁，降低泄露风险；

2. 实施供应商访问控制管理，限制第三方对内部系统和数据的访问权限，如云厂商提供的访问控制机制 AWS IAM。

04

总结

本篇报告分析了2024年上半年全球云上数据泄露的风险与事件，系统性探讨了事件成因，包括主流云攻击手法和配置错误等人为因素。为了更清晰地描述云上数据泄露的攻击路径，我们引用了 MITRE ATT&CK 模型中的攻击手法并进行了说明，有助于读者更好地理解这些攻击机制。

绿盟科技创新研究院在云上风险发现和数据泄露领域已经开展了多年的研究。借助 Fusion 数据泄露侦察平台，我们已监测到数万个云端暴露资产存在未授权访问的情况，包括但不限于自建仓库、公有云对象存储、云盘、OLAP/OLTP 数据库，以及各类存储中间件等，具体研究内容可参考《2023 公有云安全风险分析报告》[3]。

Fusion 是由绿盟科技创新研究院研发的一款面向数据泄露测绘的创新产品，集探测、识别、泄露数据侦察于一体，针对互联网中暴露的泛云组件进行测绘，识别组件关联的组织机构和组件风险的影响面，实现自动化的资产探测、风险发现、泄露数据分析、责任主体识别、数据泄露侦察全生命周期流程。

图 11 Fusion 能力全景图

Fusion 的云上风险事件发现组件具有如下主要特色能力：

资产扫描探测：通过多个分布式节点对目标网段 / 资产进行分布式扫描探测，同时获取外部平台相关资产进行融合，利用本地指纹知识库标记，实现目标区域云上资产探测与指纹标记；

资产风险发现：通过分布式任务管理机制对目标资产进行静态版本匹配和动态 PoC 验证的方式，实现快速获取目标资产的脆弱性暴露情况；

风险资产组织定位：利用网络资产信息定位其所属地区、行业以及责任主体，进而挖掘

主体间存在的隐藏供应链关系及相关风险。

资产泄露数据分析：针对不同组件资产的泄露文件，结合大模型相关技术对泄露数据进行分析与挖掘，实现目标资产的敏感信息获取；

当今数字化迅速发展的时代，数据安全问题越来越受到广泛关注。与此同时，随着云计算技术的普及和应用，企业也不可避免面临着云上数据泄露事件的频繁发生，为了提供公众和相关行业对数据安全的认知，我们计划持续发布关于云上数据泄露的分析报告，内容涵盖最新的案例解读、核心攻击技术分析、趋势洞察、安全防护最佳实践及专家建议等。

如果读者对本报告有任何意见或疑问，欢迎批评指正。如有合作意向请联系我们（邮箱chenfozhong@nsfocus.com）。

05

参考文献

[1]https://www.nsfocus.com.cn/html/2022/92_0126/171.html

[2]https://www.nsfocus.com.cn/index.php?m=content&c=index&a=show&catid=92&id=202

[3] https://www.nsfocus.com.cn/html/2024/92_0313/212.html

[4]https://cybernews.com/security/icici-bank-leaked-passports-credit-card-numbers/

[5]https://global.toyota/jp/newsroom/corporate/39174380.html

[6]https://attack.mitre.org/matrices/enterprise/

[7]https://www.verizon.com/business/resources/reports/dbir/

[8]https://aws.amazon.com/cn/pm/serv-s3/

[9]https://www.mongodb.com/zh-cn

[10]https://firebase.google.com

[11]https://gogs.io/

[12]https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm

[13]Ticketmaster Data Security Incident – Ticketmaster Help

[14] https://hackread.com/live-nation-confirms-ticketmaster-data-breach/

[15] https://snowflake.discourse.group/t/detecting-and-preventing-unauthorized-user-access/8967

[16] https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

[17] https://goharbor.io/

[18]https://techcrunch.com/2024/03/30/att-reset-account-passcodes-customer-data/

[19]https://www.att.com/support/article/my-account/000102979

[20] Snowflake-linked attack on Advance Auto Parts exposes 2.3 million people | Cybersecurity Dive

[21] https://cybernews.com/news/quotewizard-snowflake-confirms-breach/

[22]Amazon S3 中的日志记录和监控 - Amazon Simple Storage Service

NSFOCUS

扫码可在手机端直接观看

巨人背后的专家