观星
Data Star Observatory

数字资产暴露面
风险报告

深圳数字观星科技有限公司
2020年12月

目 录

一. 免责声明

本报告中的数据来源于深圳数字观星科技有限公司（简称“观星”）安全运营中心，由于数据样本收集范围所限，未必能够反映行业安全状况的全貌，不能保证所分析数据的完整性和全面性，报告信息具有一定概括性。我们已力求报告内容的客观、事实，文中的观点、建议等仅供参考，特此说明。

二. 报告概述

关键信息基础设施（简称“关基设施”）事关国家安全、社会稳定和经济运行，是关系国计民生的重要战略设施和资源，是支撑运营单位关键业务的重要资产。近几年来，《中华人民共和国网络安全法》颁布实施后，与关基设施相关的《关键信息基础设施安全保护条例》、《网络安全审查办法》、《关键信息基础设施网络安全保护基本要求》等法律法规、规范也相继出台，深刻反映了国家层面对关基设施安全高度重视，标志着我国正在全面加强关键设施保护。

在 2020 全球疫情冲击、新技术深化应用、新基建项目等数字经济转型的大环境下，关基设施对数字化转型升级的支撑作用越来越突显。与此同时，数字资产暴露面不断扩大，风险扩增，伴随 HW 大背景下，数字资产暴露面监测已成为更多运营单位所关注的焦点。

本报告主要以统计图表和描述的方式对银行业、证券业、基金业、保险业、教育、能源、邮政、航空、医疗、运营商、制造业等行业的数字资产暴露面进行

分析，为读者呈现观星实战下的 2020 数字资产暴露面风险，并提出降低数字转型下资产暴露面安全风险的建议措施。

数字资产暴露面风险：指运营单位拥有或控制的域名、IP、网站、公众号、小程序、源代码、数据等资产，被互联网或暗网披露的这些资产所存在的漏洞、弱口令、敏感端口、数据泄露等安全隐患信息所形成的风险。

三. 关键发现

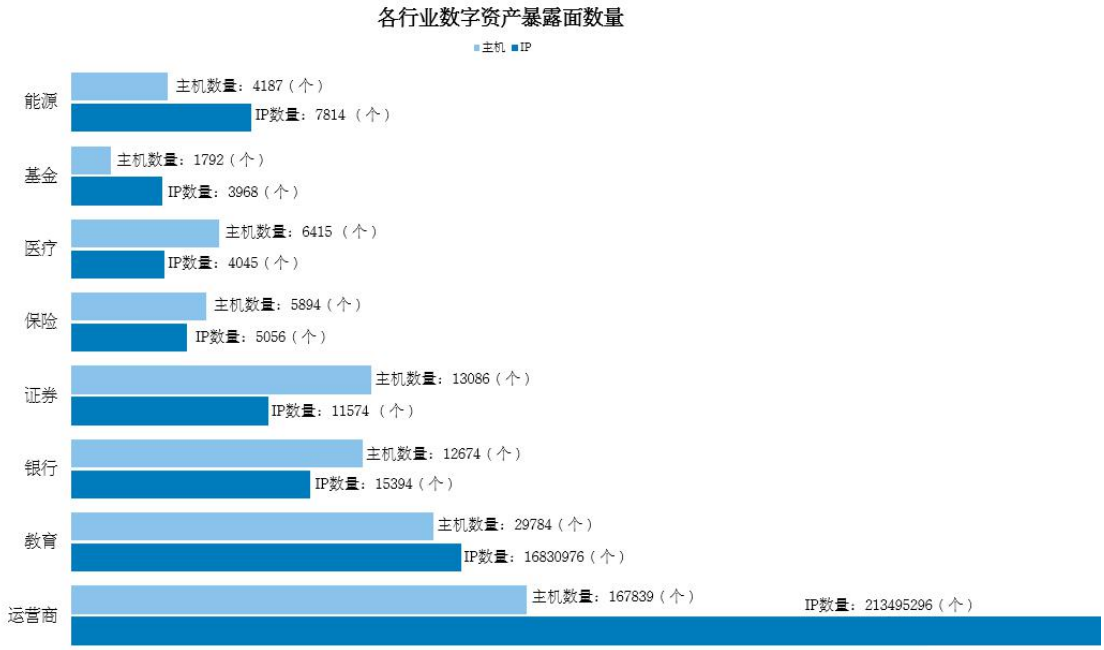
1）业务数字化转型加速，系统迭代加快，系统源代码、密码密钥、技术方案等数据泄露已是企业常态化面临的安全隐患；

2）伴随着国家和行业的《个人信息保护法》、《个人信息安全规范》、《个人金融信息保护技术规范》等法律法规发布，暗网数据泄露所造成的负面影响将变得更加严重；

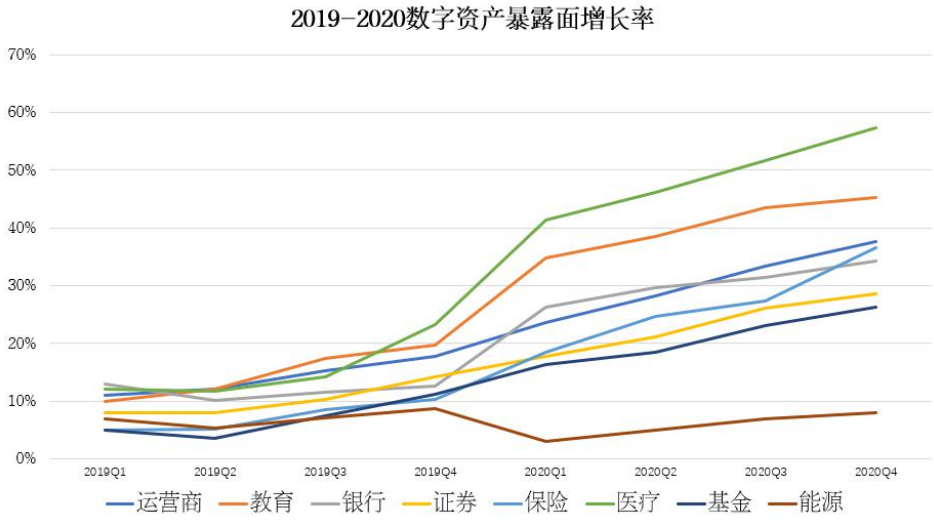
3）微信公众号/小程序持续赋能业务转型升级，微信公众号/小程序资产数量扩增，其安全风险不可忽视；

4）数字资产暴露面正在持续拓宽，暴露面风险增大。

四. 行业数字资产变化趋势



数字化浪潮风起云涌，传统产业与云、大、物、移等新技术开启了前所未有的大融合，数字资产也愈发庞大，已形成对运营单位营收至关重要的生产要素。截止到 2020 年 12 月，根据观星情报数据分析，运营商数字资产数量占首位，其中 IP 数量 213,495,296 个，主机数量 167,839 个，教育资产数量位居第二，IP 数量 16,830,976 个，主机数量 29784 个，其他行业总体相差不大。

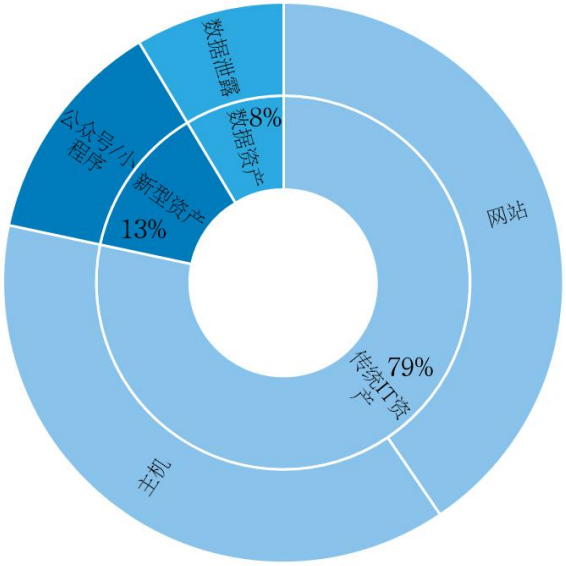


从 2019 年至 2020 年，各行业数字资产暴露面数量向上增长趋势大致相同，

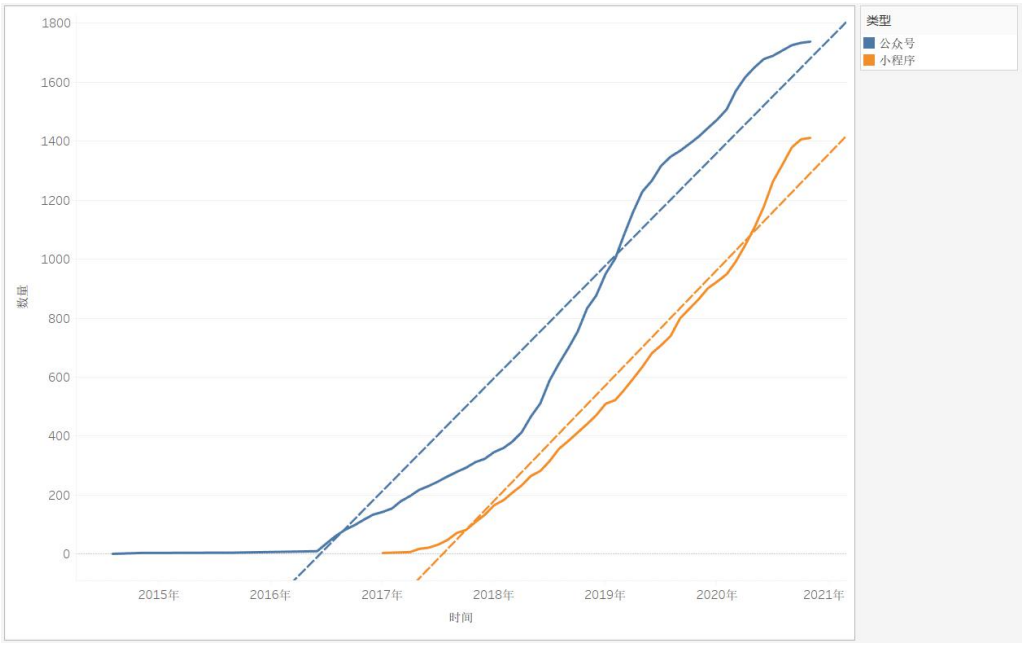
其中因 2020 年疫情影响，数字资产呈现暴增趋势，其中医疗、教育增速尤其明显，医疗增速高达 57%，能源增速放缓，仅有 1%-5%的增长率。

五. 数字资产暴露面和风险分析

5.1 数字资产暴露面整体分布



传统 IT 资产占比 79%，数据资产占比 8%，新型资产占比 13%，随着数字化业务应用窗口不断增加，新型资产数量呈现不断扩增趋势，如下图所示：



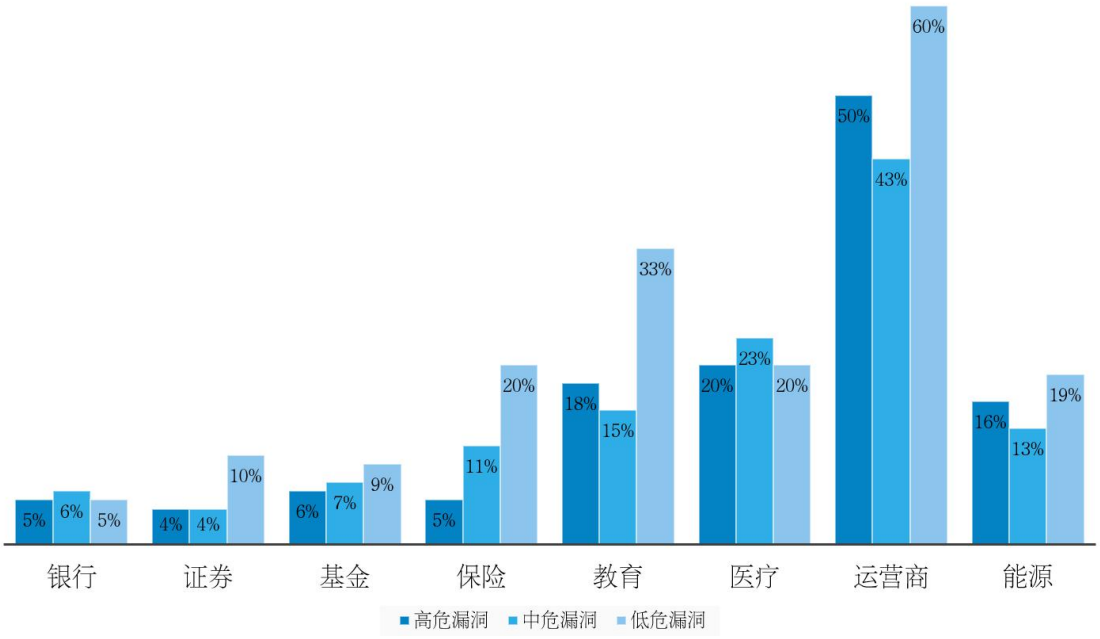
从公众号、小程序增长趋势可见，2016 年 6 月份起，公众号资产呈明显增

长趋势，小程序发布时间稍微晚一些，在 2017 年 1 月开始，5 月份开始增长。

我们研究发现公众号、小程序只是数字化转型的一面，在数字资产日益增长，伴随着暴露面扩大，运营单位所面临的风险也在不断增加，对于运营单位的网络安全也带来了挑战。

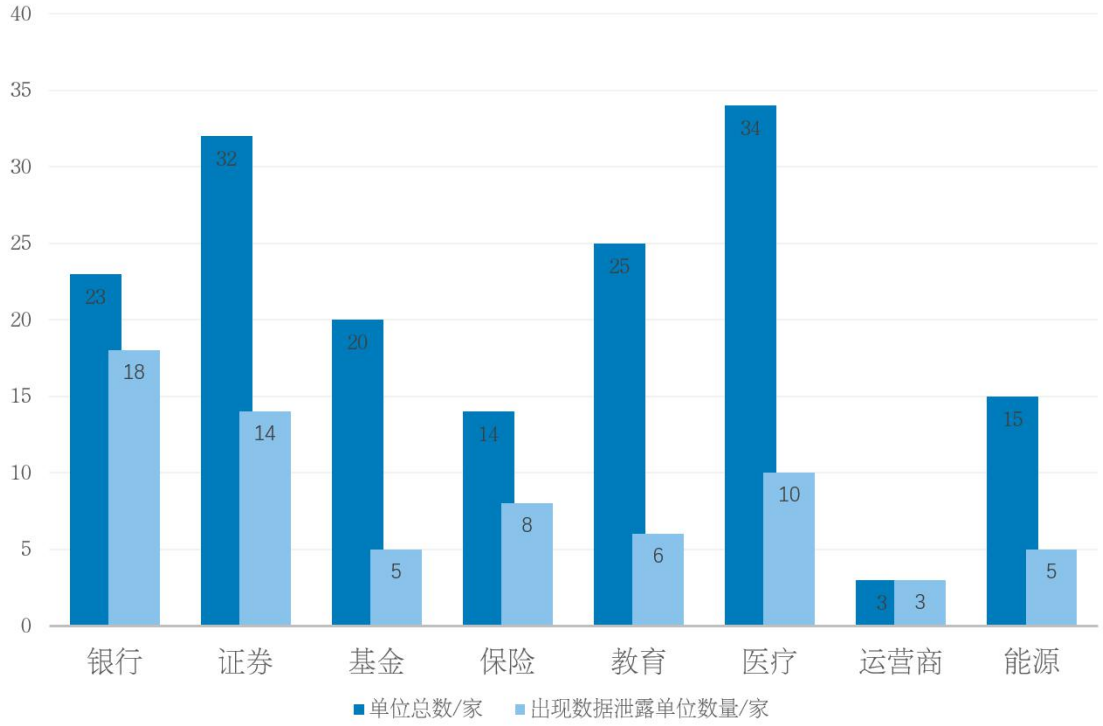
5.2 行业数字资产暴露面风险分布

5.2.1 从数字资产暴露面漏洞看行业网安建设水平



从行业用户出现的高中危漏洞占比分析，金融行业数字资产暴露面漏洞较少，网安建设水平远高于其他行业，虽然整体数字资产暴露面及动态变化有着不可预期的风险，但从监测、响应、应急、处置等方面金融行业表现得更加敏捷和健全。数字资产暴露面漏洞风险最高为运营商行业，其次是医疗、教育和能源行业。

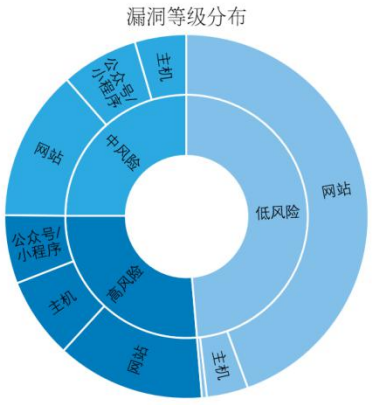
5.2.2 金融行业成数据泄露的重灾区

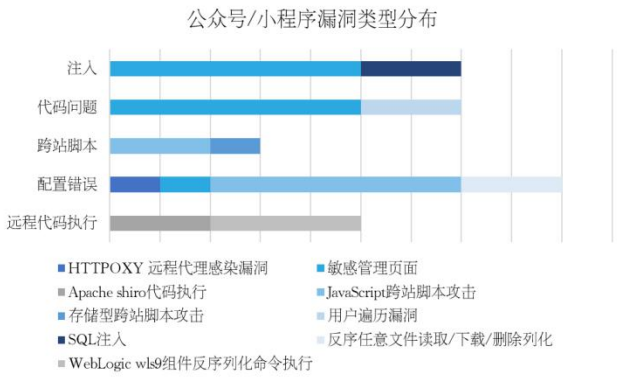


虽然分析行业运营单位数量各不相同，但对比每个行业外部数据泄露可以看出，“银行、证券、基金和保险”外部数据泄露最多，平均每 2 家单位就有 1 家单位出现外部数据泄露问题，每家单位平均每季度泄露数据约 10 起。

5.3 数字资产暴露面风险现状

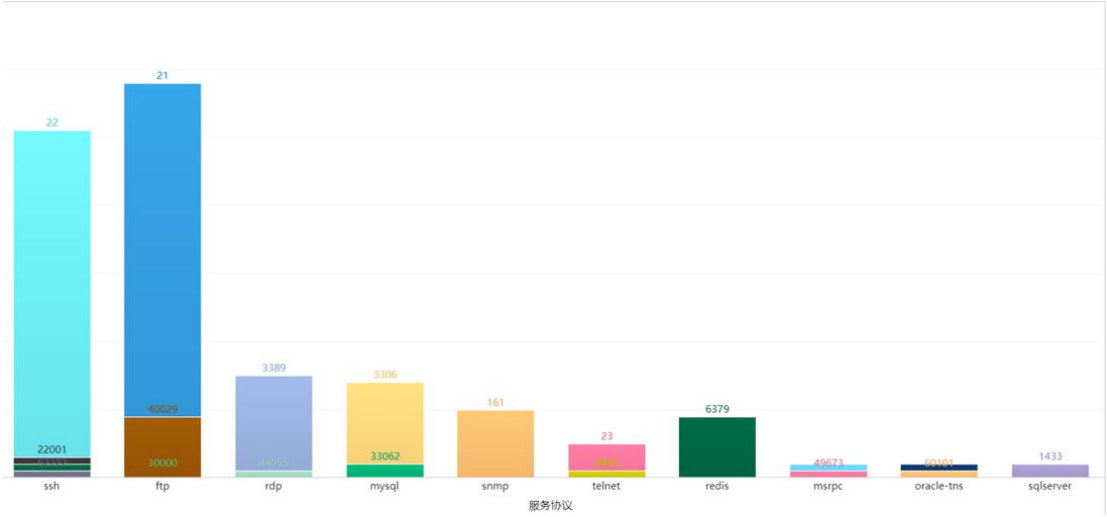
5.3.1 数字资产暴露面漏洞情况





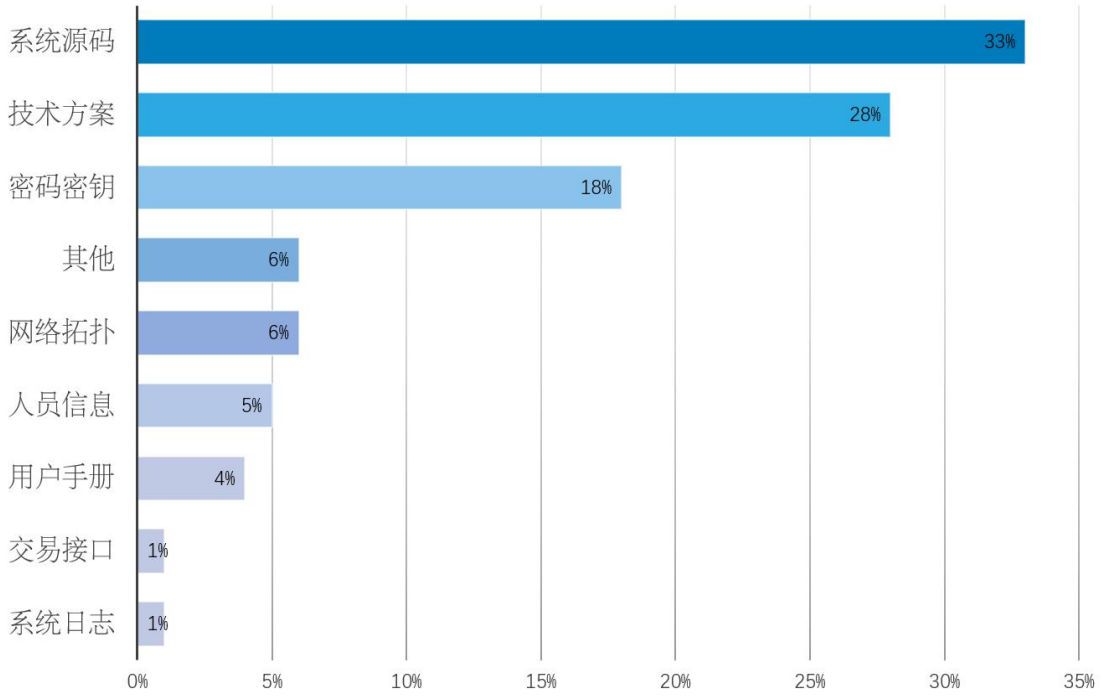
以新型资产暴露面漏洞为例，运营单位使用公众号/小程序开展业务，由于新型资产缺少相应监测手段，容易出现注入、代码问题、跨站脚本、配置错误、远程代码执行等漏洞风险。

5.3.2 数字资产敏感端口风险情况



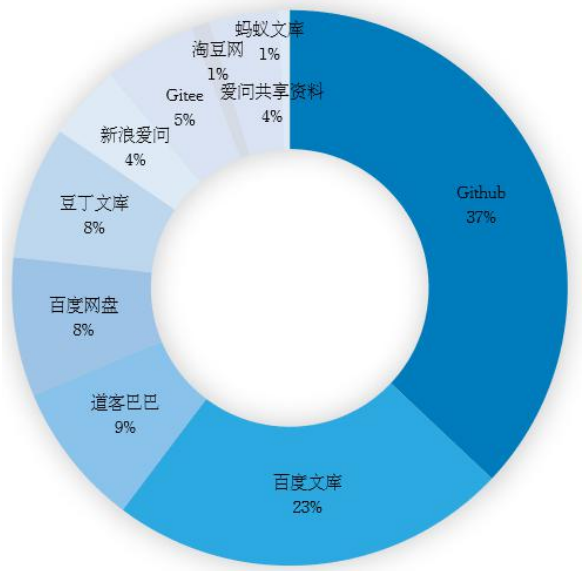
数字资产云化、边界不受控、流程管理问题、安全意识差等是导致敏感端口大门向外部开放的主要原因，敏感端口暴露 Top5 主要有 22、21、3389、3306、23。

5.3.3 系统源码成数据泄露类型的主角



系统源码和技术方案占据外部数据泄露类型 61%，分析发现泄露系统源码中含有密码密钥风险最高，也是众多运营单位用户最为关注的外部数据泄露风险。

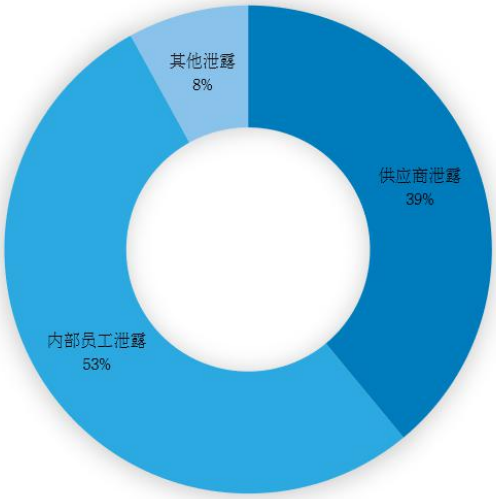
5.3.4 Github 和百度文库成数据泄露渠道最为关注的明星



由于知识共享、知识付费的兴起，越来越多的用户将自己编写的代码、文档作为经验、工具分享至第三方开源社区和知识付费平台。内部数据外泄，容易成

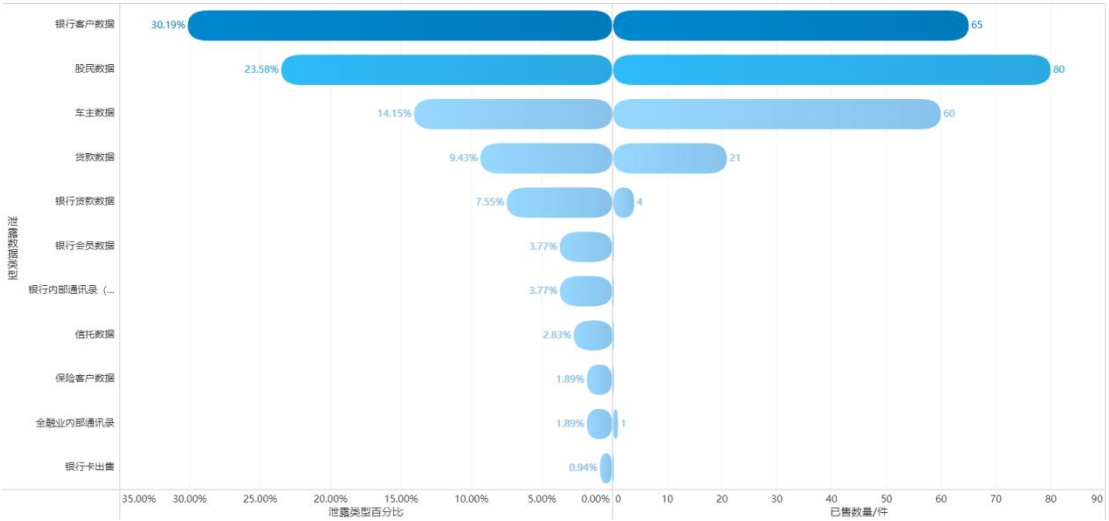
为攻击者和黑客社工利用重要渠道，分析发现在 Github 和百度文库共享导致数据泄露比例高达 60%。

5.3.5 内部员工和供应商依旧是高风险人群



内部员工和供应商引起的外部数据泄露事件占比 92%，普遍由于存在网络安全意识薄弱和安全管理不足导致敏感数据泄露的问题。

5.3.6 冰山下的暗网数据泄露交易活跃



2020 年，观星暗网情报监测共发现 1500+起，交易数量 231+件，交易用户数据高达 780w+条，由于暗网自身具有较强的匿名性和隐蔽性，暗网数据交易也成为金融客户数据泄露贩卖交易的主要渠道。

六. 观星建议与展望

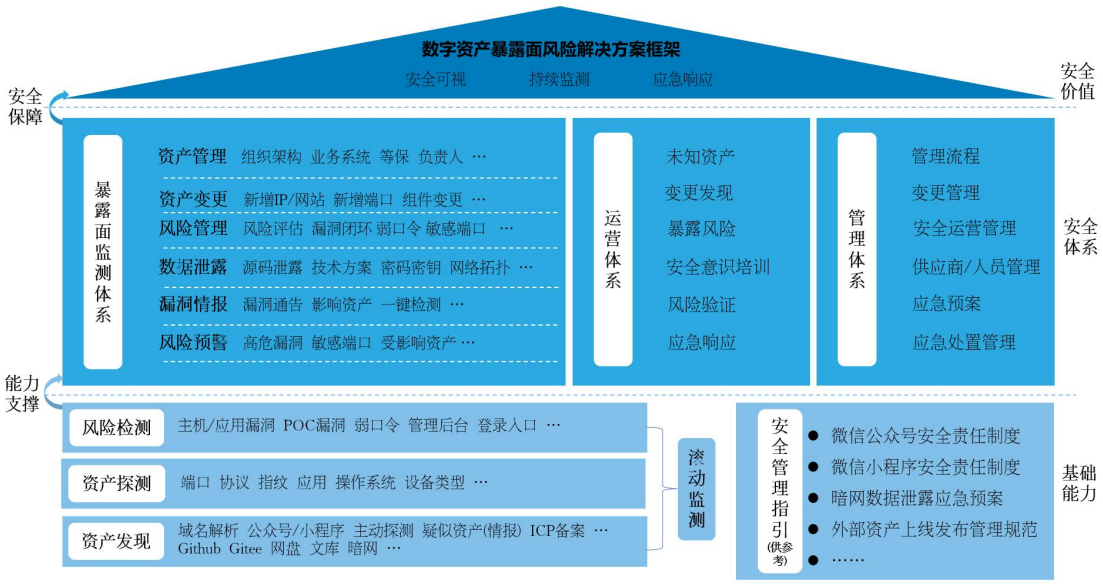
从情报数据分析发现，随着数字化转型的加速，越来越多的数字资产游离于关基设施运营单位检测和管理范围之外，这为关键业务带来了新的暴露风险，而关基设施运营单位往往对这部分风险缺乏足够和及时感知。关基单位需要通过平台或工具手段，持续不断的以黑客视角发现数字资产暴露面存在的风险，同时结合流程化安全管理手段，才能够真正做到“摸清家底”，从而降低暴露面风险。资产暴露面监测是专业性和复杂度极强的工作，必要时可借助外部的专业安全机构实现及时和有效的数字资产暴露面风险监测和预警。

观星根据 2020 数字资产暴露面风险分析和实战运营经验，总结提出以下建议：

1) 加强风险暴露面相关理论和安全案例的学习，充分认识数字资产暴露面风险监控的意义和价值；
2) 加强外部数字资产暴露面发现及威胁检测，同时要更加关注新型资产的暴露面风险，看清、看全数字资产暴露面变化，提升数字资产与数字化业务关联性，从而提高业务视角的安全风险的决策效率；
3) 建立建全暗网情报监测和配套应急机制，防范负面风险信息扩大化，减少因客户数据泄露额外带来的法律或者处罚风险；
4) 加强外部供应商安全管理，配套建立外部动态监测、响应和处置机制，防患于未然。

观星依托于多年的实战经验，已为业内众多用户打造了数字化转型下的数字资产暴露面风险解决方案，并不断探索实践，助力行业用户在数字化浪潮下让资产的安全保障“看得清”和“管得好”，加强资产威胁监测和应急响应能力，为

推动数字化转型战略保驾护航。



观星 2021 数字资产暴露面展望：

1) 随着业务向云上转移，传统 IT 资产呈现云化趋势，越来越多的业务将不存在固定的 IP 地址，通过 IP 共享提供服务；

2) 微信公众号和小程序开展业务将呈持续上升趋势，或许会成为监管部门的关注重点；

3) 国家和监管机构对个人敏感数据保护越来越重视，APP 或许将成为数字资产暴露面的下一个重点；

4) 运营单位安全部门对代码泄露的不断重视，源代码泄露情况会有所好转；

5) 暗网交易持续活跃，随着疫情的不断发展，医疗行业的数据泄露有可能迎来新的高峰。

观星
Data Star Observatory

数字观星® 是国内数字资产威胁管理领域的开拓者。

基于海量安全情报数据，为用户提供数字资产威胁管理运营：数字资产发现与管理、资产威胁监测与分析、暗网溯源。

观星® 以成为世界级数字资产安全运营服务商为奋斗愿景，立志捍卫国家关键基础设施资产安全、保护企业数字资产安全。

4000-365-911
contact@shuziguanxing.com