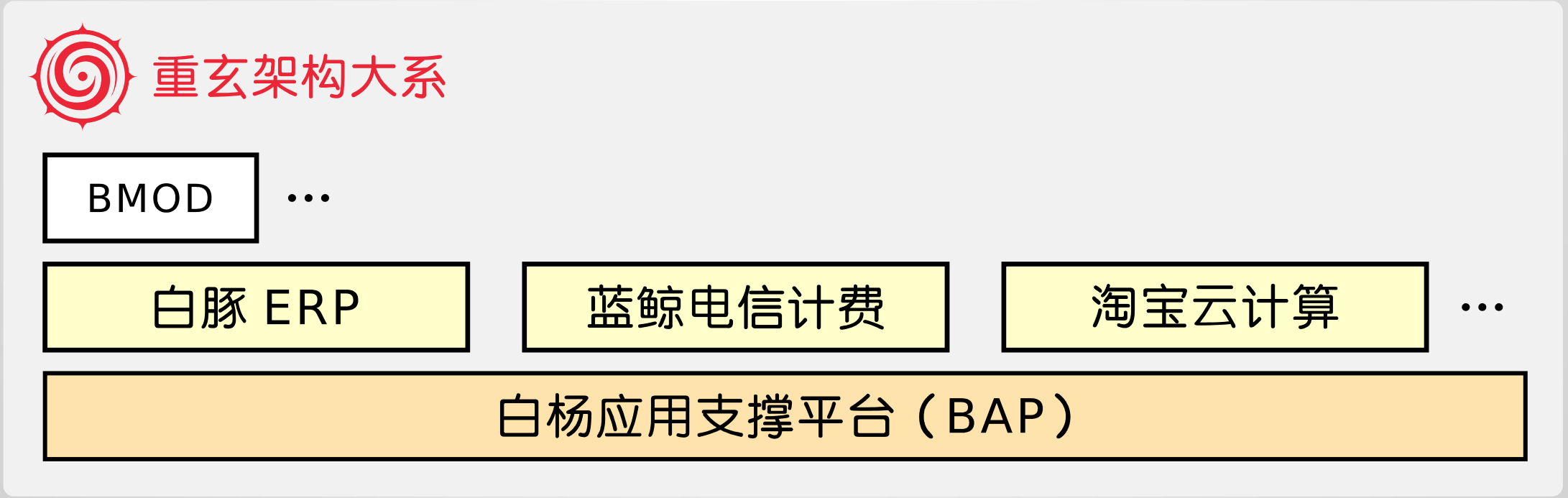
技术优势

简介

- 上海重玄掌握跨平台高效软件开发的领先科技。多年来，我们完成了白杨应用支撑平台（BaiY Application Platform）、蓝鲸电信计费系统、白豚 ERP 平台，以及BYCDN、BYST等多个拥有自主知识产权的自有产品。同时还承接和参与了淘宝/银基云计算平台（阿里云前身）、上海地铁改建工程、SIP 软交换系统、职业精人才平台、智能IoT仓储等多项重大项目的建设。



底层应用支撑平台 - 1

- 白杨应用支撑平台使用汇编、C/C++ 构建，包含数百万行代码和上千个成熟的通用组件。支撑平台经过多家 500 强企业实际生产环境以及多个高负载电信、互联网和分布式计算环境十多年验证。
- 支持 Windows、Linux、BSD、IBM AIX、HP-UX、Solaris、MAC OS X、vxWorks、QNX、DOS, WinCE (Windows Mobile), NanoGUI、eCos、RTEMS 以及 Android、iOS 等绝大多数主流操作系统。
- 支持 x86/x64、ARM、RISC-V、IA64、MIPS、POWER、SPARC 等主流硬件平台。

底层应用支撑平台 - 2

我方拥有由多项国家和国际发明专利保护的强一致多活 IDC 高可用、高可靠和高性能分布式集群组件，支持实时强加密和数据压缩的分布式文件系统等核心技术。可提供超越支付宝、Google GCE、微信等关键服务的高可用性、可靠性和安全性保证。

基于支撑平台的产品可使用由我方自主研发的分布式数据库平台和数据查询分析引擎来实现数据的存储和管理工作。其跨 IDC 的强一致 6 副本技术保证了极高的数据可靠性。

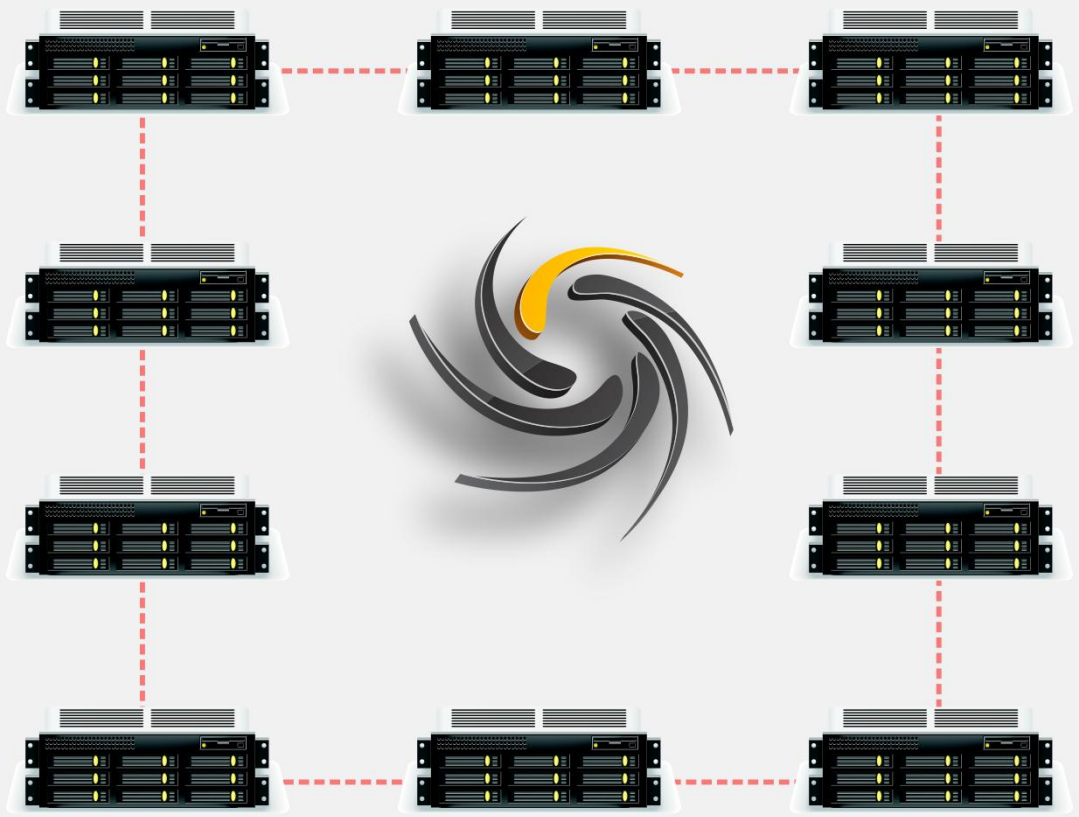
底层应用支撑平台 - 3

超高并发网络服务器组件使用汇编和异步 IO 进行了优化，通过 DMA + 硬件中断实现内存零拷贝的高效异步网络服务。性能、可靠性和可伸缩性都很强。

在 2011 年出厂的，当时售价不足 2 万元人民币的单台至强 5600 系入门级 1U PC Server 上**单台**支撑上千万 TCP/HTTP 并发连接（参考白皮书：3.2.1、3.3.1 以及 3.3.2 小节）。相对应地，一般由 Java / .NET 开发的服务器端，在相同配置的机器上，单点最高可支撑 3000 到 5000 并发，PHP 则更低。

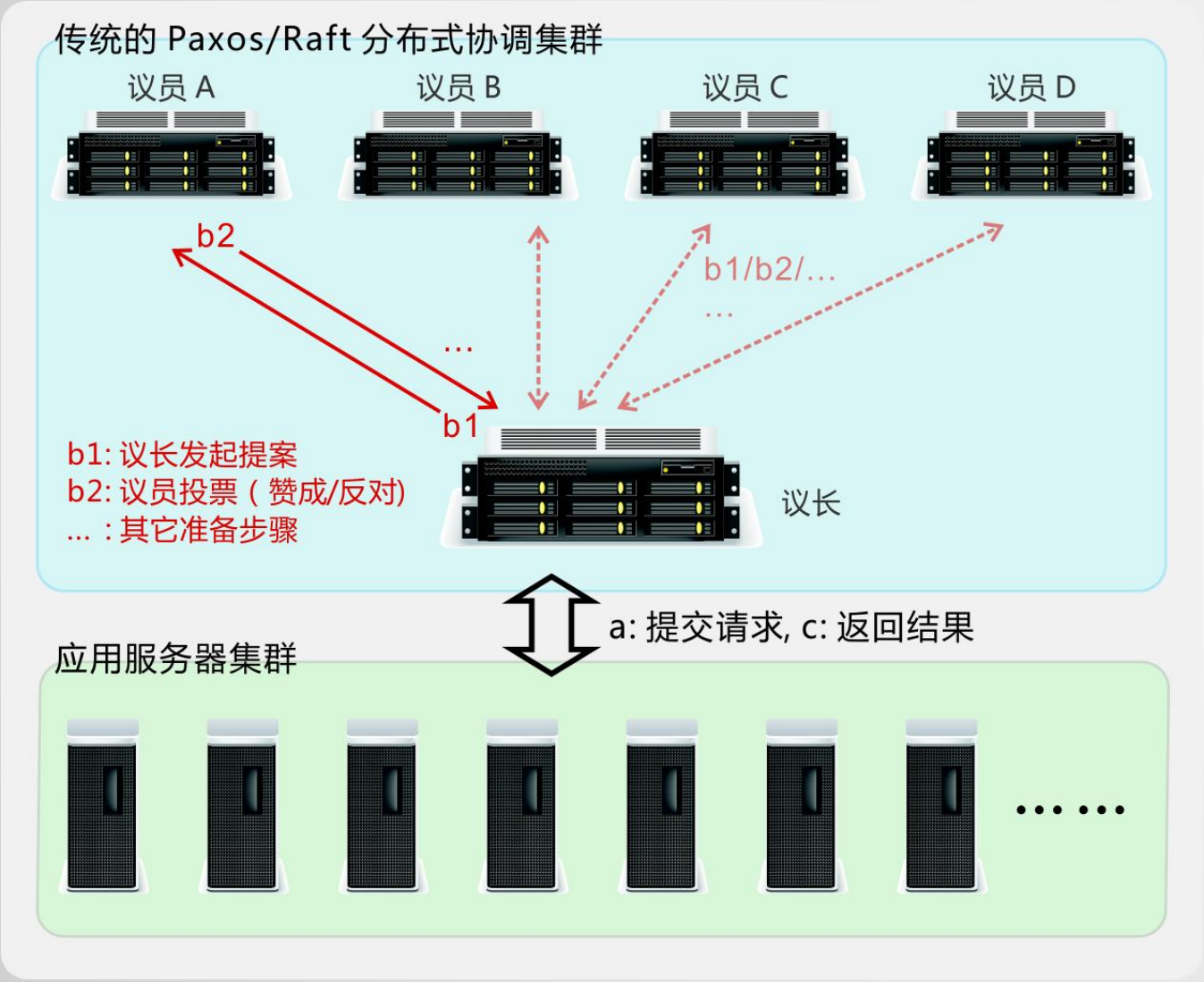
得益于极高的单点性能，以及可大规模横向扩展的分布式高性能集群架构。因此基于应用支撑平台构建的产品系统容量在事实近乎没有上限。

底层应用支撑平台 - 4



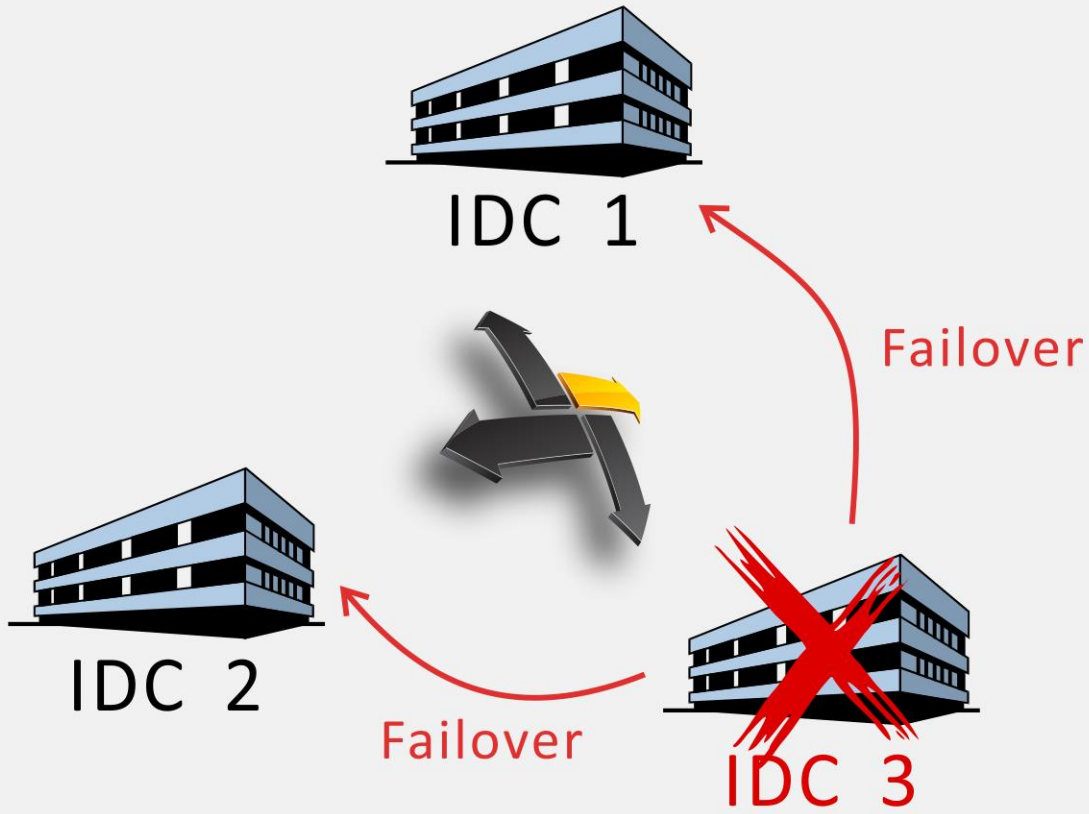
- 分布式协调服务为集群提供服务发现、服务选举、故障检测、故障转移、故障恢复、分布式锁、任务调度，以及消息路由和消息分发等功能。
- 分布式协调服务是分布式集群的大脑，负责指挥集群中的所有协同工作。将分布式集群协调为一个有机整体，使其有效且一致地运转。实现可线性横向扩展的高性能（HPC）和高可用（HAC）分布式集群系统。

底层应用支撑平台 - 5



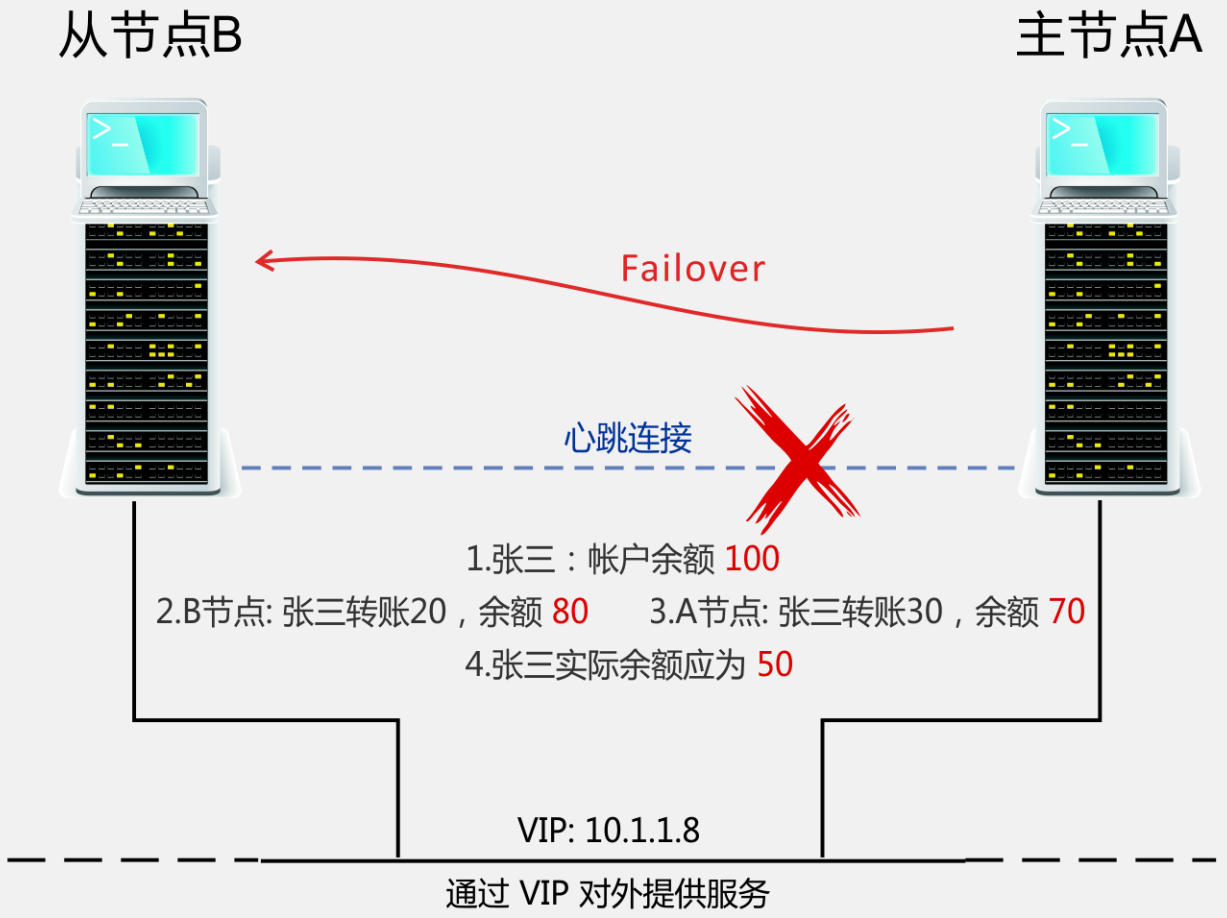
- 传统的 Paxos/Raft 分布式协调算法为每个请求发起投票，产生至少2到4次网络广播和多次磁盘IO。使其对网络吞吐和通信时延要求很高，无法部署在跨 IDC（城域网或广域网）环境。我们的 BYPSS 国际专利算法则完全消除了此类开销。
- 因此大大降低了网络负载，显著提升整体效率。并使得集群跨 IDC 部署（多活 IDC）变得简单可行。

底层应用支撑平台 - 6



- 基于重玄独有的分布式协调技术，可实现高性能、强一致的多活 IDC 机制。
- 可在毫秒级完成故障检测和故障转移，即使整座 IDC 机房下线，也不会导致系统不可用。
- 强一致性保证：即使发生了网络分区也不会出现脑裂（Split Brain）等数据不一致的情形。

底层应用支撑平台 - 7



- 传统的双机容错方案中，从节点在丢失主节点心跳信号后，自动将自身提升为主节点，并继续对外提供服务，以实现高可用。

- 当主从节点均正常，但心跳连接意外断开时（网络分区），就会发生脑裂（Split Brain）问题：此时 A、B 均认为对方已下线，故将自己提升为主节点并分别对外提供服务，产生难以恢复的数据不一致。

底层应用支撑平台 - 8

我方 BYPSS 服务可在跨 IDC 的尺度上提供提供与传统 Paxos/Raft 分布式算法相同水平的强一致性保证，从根本上杜绝脑裂等不一致现象的发生。

类似地：工行、支付宝等服务也有异地容灾方案（支付宝：杭州 -> 深圳、工行：上海 -> 北京）。但在其异地容灾方案中，两座 IDC 之间并无 Paxos 等分布式协调算法保护，因此无法实现强一致，也无法避免脑裂。

举例来说，一个在支付宝成功完成的转账交易，可能要数分钟甚至数小时后才会从杭州主 IDC 被异步地同步到深圳的灾备中心。杭州主 IDC 发生故障后，若切换到灾备中心，意味着这些未同步的交易全部丢失，并伴随大量的不一致。比如：商家明明收到支付宝已收款提示，并且在淘宝交易系统看到买家已付款，并因此发货。但由于灾备中心切换带来的支付宝交易记录丢失，导致在支付宝中丢失了相应的收入，但淘宝仍然提示买家已付款。因此，工行、支付宝等机构在主 IDC 发生重大事故时，宁可停止服务几个小时甚至更久，也不愿意将服务切换到灾备中心。只有在主 IDC 发生大火等毁灭级事故后，运营商才会考虑将业务切换到灾备中心（这也是灾备中心建立的意义所在）。

因此，异地容灾与我方的强一致、高可用、抗脑裂多活 IDC 方案具有本质区别。

底层应用支撑平台 - 9

由于消除了 Paxos/Raft 算法中的大量广播和分布式磁盘 IO 等高开销环节，配合支撑平台中的高并发网络服务器、以及并发散列表等组件。使得 BYPSS 分布式协调组件除了上述优势外，还提供了更多优秀特性：

- **批量操作**：允许在每个网络包中，同时包含大量分布式协调请求。网络利用率极大提高，从之前的不足 5% 提升到超过 99%。类似于一趟高铁每次只运送一位乘客，与每班次均做满乘客之间的区别。实际测试中，在单千兆网卡上，可实现 400 万次请求每秒的性能。在当前 IDC 主流的双口万兆网卡配置上，可实现 8000 万次请求每秒的吞吐。比起受到大量磁盘 IO 和网络广播限制，性能通常不到 200 次请求每秒的 Paxos/Raft 集群，有巨大提升。

- **超大容量**：通常每 10GB 内存可支持至少 1 亿端口。在一台插满 64 根 DIMM 槽的 1U 尺寸入门级 PC Server 上（8TB），可同时支撑至少 800 亿对象的协调工作；在一台 32U 大型 PC Server 上（96TB），可同时支撑约 1 万亿对象的分布式协调工作。相对地，传统 Paxos/Raft 算法由于其各方面限制，通常只能有效管理和调度数十万对象。

底层应用支撑平台 - 10

此外，Paxos / Raft 在经历过半节点同时故障下线并维修恢复的过程中，无法保证数据的强一致性，可能产生幻读等不一致问题。

例如：在一个三节点集群中，节点 A 因为电力故障下线，一小时后节点 B 和 C 则因为磁盘故障下线。此时节点 A 恢复电力供应重新上线，紧接着管理员更换了节点 B 和 C 的磁盘并让它们分别恢复上线。此时整个集群 1 小时内的修改将全部丢失，集群退回到了 1 小时前 A 节点下线时的状态。

而 BYPSS 则从根本上避免了此类问题的发生，因此 BYPSS 拥有比 Paxos / Raft 更强的一致性保证。

底层应用支撑平台 - 11

示例 - BYPSS 与 Redis + MySQL 等现有分布式缓存 + DB 的优势对比：

1. BYPSS 集群**保证强一致性**。而 Redis 等分布式缓存，即使加入了 Revision 字段并利用其实现原子（CAS）操作，仍然无法保证其与 DB 之间的强一致性，只能通过加入失效超时（TTL）等机制来缓解数据不一致所带来的危害（但此举同时也引入了缓存击穿、缓存雪崩等其它问题）。
2. BYPSS 集群可提供**数万倍量级的网络和 CPU 性能提升**。BYPSS 集群以纳秒级的内存直接访问替代了毫秒级的网络查询，性能提升几个数量级。同时避免了每次缓存访问时频繁的数据序列化和反序列化过程，显著降低了 CPU 和网络开销。
3. BYPSS 集群可**完全避免缓存击穿**（失效）问题。由于 BYPSS 集群中的每个对象均仅缓存在其属主节点上，仅该对象的属主节点有权向 DB 发送访问请求（没有并发访问），因此不可能发生缓存击穿。
4. BYPSS 集群可**轻易避免缓存穿透**（无效）问题。由于 BYPSS 集群中的每个对象均有其唯一属主节点，因此很容易在属主节点上对无效（不存在等）的对象进行标记和过滤（例如：高性能 ID 并发散列集合、布隆过滤器等）。因此可以轻易避免缓存穿透问题。
5. BYPSS 集群可**完全避免缓存雪崩**（大面积失效）问题。首先，由于 BYPSS 集群中缓存与 DB 数据间是强一致的，因此无需设置一个缓存过期时间来缓和缓存数据不一致的危害。因此缓存雪崩的一大前提：大量缓存同时到期就不复存在了。其次，由于消除了专门的缓存集群，所有缓存数据均内嵌在 App 服务器内，自然也就不存在“缓存节点宕机”这种问题了。与此同时，BYPSS 提供的强一致多活 IDC 高可用集群能力可保证 App Server 集群不会出现大规模宕机事故（不可抗力除外）。

底层应用支撑平台 - 12

高效、高强度的密码编码学组件：包含公钥算法、对称加密算法、数据编解码、散列和消息验证算法、数据压缩算法等基础功能组件。

除此之外，支撑平台还针对多种不同的常用情形，提供了多个抽象层次更高、可开箱即用的高级密码编码学功能组件，例如：

支持实时压缩和强加密的虚拟文件系统（VFS），VFS支持包括AES（128/256）、SM4、TwoFish 等在内的数十种强加密算法，使用 AES-NI、SSE4、AVX 等汇编指令集优化，效率高。在蓝鲸、白豚、职业精等全线产品中，我们均使用该组件为产品的数据库和配置类数据提供整库级的实时压缩和强加密保护。另外还包括基于公钥体系架构（PKI）的强加密通信保护组件等。

底层应用支撑平台 - 13

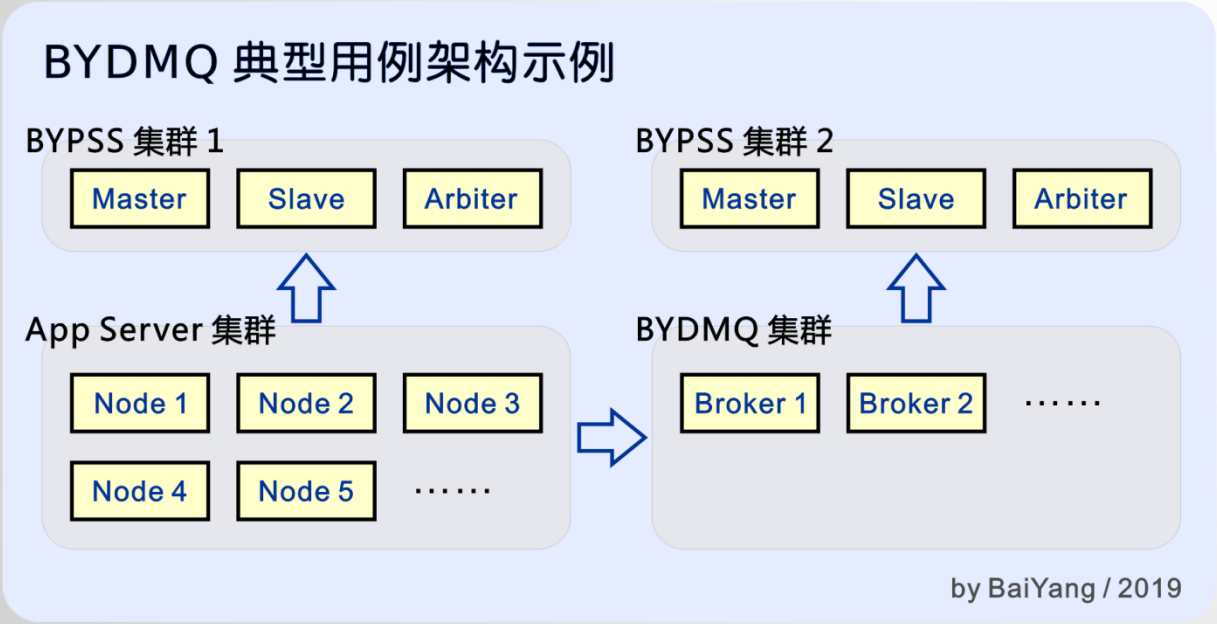
自有查询分析引擎除了可以摆脱对特定 DBMS 的依赖，使我们的产品可以自由地在MySQL、MS SQL Server、Oracle、DB2、SQLite 等传统关系型数据库，Clutrix、Greenplum、TiDB、PostgreSQL-XL 等 NewSQL 数据库，以及MongoDB、SequoiaDB、Cassandra 等 NoSQL 数据库间灵活切换以外。更增加了基于 UNICODE 字符集的 ARE 高级正则查询、表中套表的关联查询、复杂虚拟字段等传统 SQL 查询无法实现的高级特性，为用户提供了更强大灵活的数据分析平台。

因此，自有查询分析引擎在为用户提供了强大的数据智能分析和报表生成功能的同时，也带来了优秀的跨数据库产品支持能力。

查询引擎通过汇编优化的 C/C++ 代码实现词法分析、语法分析、语义分析/中间代码生成、优化等步骤，并可在 2010 出厂的 Thinkpad W510 笔记本上（4核8线程），仅用其中一核一线程实现每秒1300万次以上的表达式求值效率。

底层应用支撑平台 - 14

分布式消息组件 BYDMQ 是一种强一致、高可用、高性能、高吞度、低延迟、可线性横向扩展的分布式消息队列服务。可支持单点千万量级的并发连接以及单点每秒千万量级的消息转发性能，并支持集群的线性横向扩展。



BYDMQ 专注于高吞吐、低延迟的大量业务类消息投递等工作。通过使用成熟的高效网络 IO 组件，以及消息自动批量打包、pipelining 等机制，显著降低了命令处理延迟、提高了网络吞吐、有效增加了网络利用率。同时还支持为每条消息分别指定 TTL、最大重试次数，以及自动分散投递等高级功能。

底层应用支撑平台 - 15

BYST 组件为用户提供了一种端到端的安全隧道服务。BYST 支持数十种强加密和数据校验算法，可为用户提供安全、可靠和一致的数据通信隧道服务。

与此同时，得益于我方成熟的高性能网络 IO 组件、基于自研非线性神经元的 AI 包预测和补偿算法、消息批量打包及拆包、专利的分布式 N:M:N 连接池动态加速、以及高性能数据实时压缩等算法，BYST 显著提升了网络利用率（高载荷比）和网络吞吐量。在典型的日常办公场景（email、OA、文件服务、在线会议）中，BYST 最高可为用户节省超过 50% 的网络流量，显著低了昂贵专线网络的租用成本。

不同于各现有 VPN 方案，受上述强加密、批量 IO 打包和拆包、连接池随机重映射以及数据压缩等算法的影响，BYST 可做到完全无特征（既无可分析的明文字段，亦无任何流量特征）。因此不必担心被防火墙误伤。
同时，BYST 可透明兼容 OpenVPN、CISCO VPN、v2ray、ss 等各类现有方案，无需 IT 部门大动干戈，重新部署。

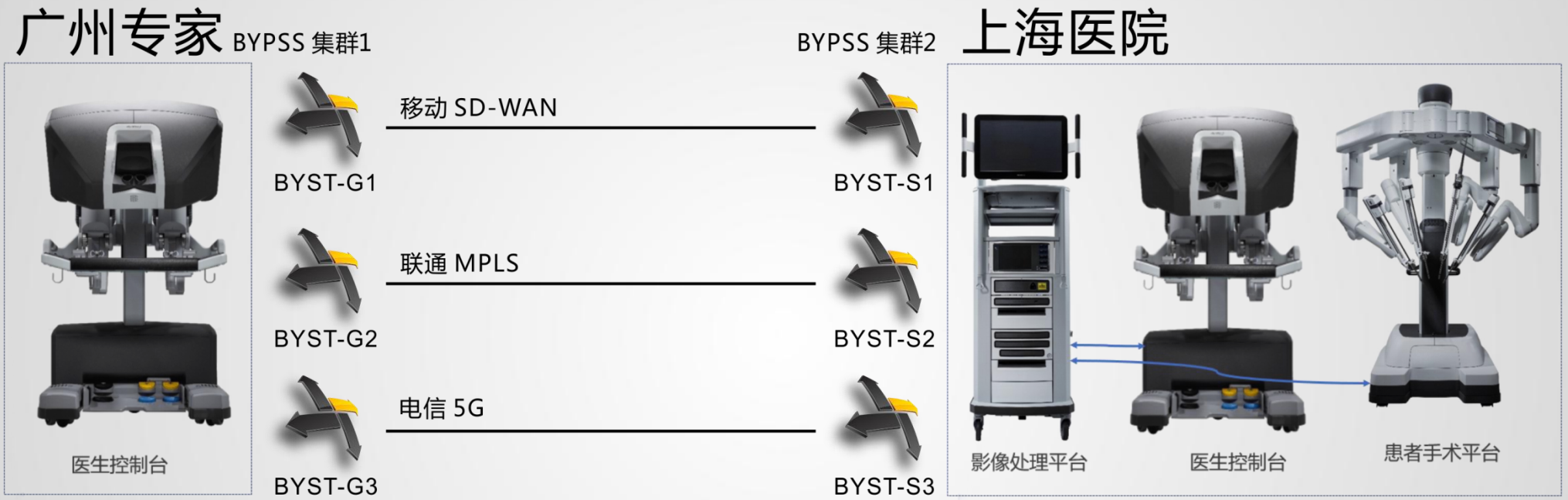
底层应用支撑平台 - 16

BYCDN 服务能节省 95% 流量费用并且避免卡顿。无需客户端或硬件盒子支持，对接只需一行代码，同时无需改变应用和 CDN 等原有架构。

依托于上述 BYPSS 组件，BYCDN 为 P2P CDN 环境量身定制了一整套专利的分布式、超细粒度（数据块级）海量资源实时跟踪和调度算法。该算法可在超大规模并发用户的场景下，以极细的粒度同时对海量在线资源进行强一致的实时跟踪、匹配、分析统计和调度等管理工作。可极大地提高 P2P CDN 共享实时性和成功率，并显著增强 P2P CDN 整体系统对变换莫测的 P2P CDN 网络节点以及密集缓存变化的适应能力。

配合我方自主研发的我方自主研发的“大区/国家 -> ISP -> 州省/地市”三级五层智能组网、网络 QoS 适配、以及数据强加密保护等技术，可以为音视频直播和点播、文件分享、在线办公等业务提供安全强大的数据分发能力。同时节省 95% 的流量和费用，并且避免卡顿问题（看得人越多越流畅）。

底层应用支撑平台 - 17



- BYHAL 高可靠通信平台 POC 案例：广州专家远程为上海病患实施手术，广州和上海各自通过三个 BYST 节点组成 BYPSS 强一致 HAC 集群。每个 BYST 节点通过不同运营商提供的不同线路与上海配对节点建立连接。
- SLA 保证：移动联通电信三线中，同时两路发生故障仍可零抖动正常工作（0ms切换线路）；BYPSS 集群 1 和 BYPSS 集群 2 中，各自可容忍最高一个节点故障下线，此时保证最大抖动小于 50ms（最高 50ms 内完成节点故障检测和切换）；系统保证数据强一致（不丢包、不乱序、不重复）。

底层应用支撑平台 - 18

我们并不依靠“商业秘密”来保护核心竞争力。相反，我们使用更公开透明的商标、认证、版权、专利和公证保管等手段来保护自己的合法权益。因此，我们的技术细节均公开于相应的文档中，详情可见《白杨应用支撑平台技术白皮书》：

http://baiy.cn/doc/asp_whitepaper.pdf
或者：http://baiy.cn/doc/asp_whitepaper_en.pdf（英文版）。

等文档，包括 Hacker News（全球最大的计算机科学新闻网站）、Google Blogger、CSDN 以及博客园在内的多家国内外媒体均转载或报道了这些论文。相较于“严守秘密”，我们相信公开透明下的大量同行审评，加上实际生产环境中的严酷考验，更有利于产品品质的提升。

底层应用支撑平台 - 19

证书号第4249374号

证书号第2776194号

(12) United States Patent
Bai
(54) PORT SWITCH SERVICE SYSTEM

澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
經濟局
Direcção dos Serviços de Economia
發明專利之延伸註冊證
Título de Extensão de Patente de Inve
編號 N.º: J/003824
頁Pág.: 1 / 2
延伸申請日期 Data do pedido de extensão : 2019/09/04
延伸批給日期 Data da concessão de extensão : 2019/10/23
專利權利人 Titular : 白楊

证书号第5635365号
发明专利证书
发明名称：基于N:M连接动态映射的网络连接加速转发方法

证书号第3400663号
发明专利
发明名称：消息端口交换服务系统
发明人：白杨
专利号：ZL 2016 1 0323880.5
专利申请日：2016年05月16日
专利权人：白杨
地址：200092 上海市杨浦区控江路2202号
授权公告日：2019年06月04日
局长
申长雨
第1页(共2页)

Europäisches Patentamt
European Patent Office
Office européen des brevets
URKUNDE
Europäisches Patent
Es wird hiermit bescheinigt, dass für die in der Patentschrift beschriebene Erfindung ein europäisches Patent für die in der Patentschrift bezeichneten Vertragstaaten erteilt worden ist.
CERTIFICATE
European patent
It is hereby certified that a European patent has been granted in respect of the invention described in the patent specification for the Contracting States designated in the specification.
CERTIFICAT
Brevet européen
Il est certifié qu'un européen a été dél l'invention décrite fascicule de brevet Etats contractants dans le fascicule d
Europäisches Patent Nr. European patent No. Brevet européen n°
3422668
Patentinhaber Proprietor(s) of the patent Titulaire(s) du brevet
Bai, Yang
München, den Munich, Munich, le
17.03.21
António Campino
Président des Europ President of the Eur Président de l'Office

US010700948B2
(12) United States Patent
Bai
(10) Patent No.: US 10,700,948 B2
(45) Date of Patent: Jun. 30, 2020
(54) SERVICE-ORIENTED MODULAR SYSTEM ARCHITECTURE
(71) Applicant: Yang Bai, Shanghai (CN)
(58) Field of Classification Search
CPC H04L 41/5048; H04L 41/5051; H04L 41/5054; H04L 9/32; G06F 9/18; G06F 9/44; G06F 9/44526
See application file for complete search history.

REPUBLIC OF SINGAPORE
THE PATENT ACT (CHAPTER 221)
CERTIFICATE ISSUED UNDER SECTION 35
I HEREBY CERTIFY that under the provisions of the Patent Act, a patent has been granted in respect of an invention having the following particulars:

TITLE	:	PORT SWITCH SERVICE
APPLICATION NUMBER/ PATENT NUMBER	:	11201808659V
DATE OF FILING	:	8 AUGUST 2016
PRIORITY DATA	:	16 MAY 2016 - PATENT APPLICATION NO. 201610323880.5 (CHINA)
NAME OF INVENTOR(S)	:	BAI, YANG
NAME(S) AND ADDRESS(ES) OF PROPRIETOR(S) OF PATENT	:	BAI, YANG
DATE OF GRANT	:	19 July 2021

DATED THIS 19th DAY OF JULY 2021
Mrs. Rena Lee
Registrar of Patents
Singapore

REPUBLIC OF SINGAPORE
THE PATENTS ACT 1994
CERTIFICATE ISSUED UNDER SECTION 35
ERTIFY that under the provisions of the Patents Act, a patent has been granted in nvention having the following particulars:
: SERVICE-ORIENTED MODULAR SYSTEM ARCHITECTURE

知識產權署專利註冊處
Patents Registry
Intellectual Property Department
香港特別行政區政府
The Government of the Hong Kong Special Administrative Region

批予轉錄標準專利證明書
《專利條例》(第 514 章)
CERTIFICATE OF GRANT OF STANDARD PATENT
BY RE-REGISTRATION
Patents Ordinance (Chapter 514)
茲證明下述轉錄標準專利根據《專利條例》第 2 部在今日批予:
I hereby certify that a standard patent by re-registration with the following particulars has been granted under Part 2 of the Patents Ordinance today:
專利編號 Patent No.: HK1259712
申請編號 Application No.: 19119473.7
專利所有人姓名或名稱及地址 Name and Address of Proprietor:
Bai, Yang

WO 2016/169529
PCT/CN2016/093880

安全性和可靠性

- 基于支撑平台的产品可通过强一致在线复制（分布式文件系统）、多版本控制系统、磁盘快照、自动备份和自动恢复、数据强加密、CHAP 鉴权、BYST 双端鉴权安全传输、TLS（HTTPS） 安全传输、以及高可用集群（HAC）等多种手段，从数据存储、网络传输、节点容错等各个方面来保证服务的安全性、可靠性、稳定性和健壮性。

安全性和可靠性 - 数据可靠性

- 跨 IDC 的强一致分布式 6 副本技术，在保证强一致的前提下，确保包括业务数据、配置数据、附件数据在内的所有用户数据可靠性均高达 17个9（99.99999999999999%）。即使整座 IDC 被灾难性地完全摧毁，也不会丢失任何数据。

- 可每日自动完成快照备份，并保留指定时间范围内的磁盘快照。快照数据能够基于可靠的多副本技术或多重EC算法，可有效找回由用户误操作或恶意操作引起的数据丢失。备份快照可交错储存于不同的 IDC 机房中，以进一步提升其可靠性。配合无限多版本控制技术，可从容审计和回顾系统的历史状态。

- 数据可集中存放在由我方自主研发的，带有实时（on-the-fly）压缩和强加密保护的虚拟文件系统（VFS）中。每次发生变更时，都可以对数据进行自动备份。每次数据访问前，都会进行完整性检查，若发生错误，则自动恢复。

安全性和可靠性 - 服务可用性

- 由我方自主研发，基于多数派算法的强一致抗脑裂（Split Brain）多活 IDC 高可用集群（HAC）专利架构，服务整体可用性可达 6个9（99.9999%）。确保即使整座 IDC 由于市政施工、自然灾害、人为失误等原因下线，也可在秒级完成故障转移，自动切换到其它可用 IDC 不间断提供服务。

- 精心设计的故障检测、服务发现、服务选举、分布式锁以及消息路由等分布式协调和数据同步算法提供的强一致性保证确保了跨 IDC 的故障转移也不会导致数据一致性问题。

注：我方高可用（HAC）、高性能（HPC）分布式架构和算法受到多项国家和国际发明专利保护。

安全性和可靠性 - 可靠性补充说明

- 带强一致保证的多活 IDC 技术是现代高性能和高可用集群的关键技术，也是业界公认的主要难点。作为实例：2018 年 9 月 4 日微软美国中南区某数据中心空调故障导致 Office、Active Directory、Visual Studio 等服务下线近 14 小时不可用； 2015 年 8 月 20 日 Google GCE 服务中断 12 小时并永久丢失数据；2015 年 5 月 27 日、2016 年 7 月 22 日及 2019 年12 月 5 日支付宝多次中断数小时；以及 2013 年 7 月 22 日、2023 年 3 月 29 日微信服务中断数小时等重大事故均属于产品未实现多活 IDC 架构，单个 IDC 故障导致服务全面下线的惨痛案例。

- 在上述方面，我方拥有超过十年的积累，受多项国家和国际发明专利保护的分布式架构和算法。得益于领先的强一致、高可用、高性能分布式集群算法和架构，我们在蓝鲸、白豚、职业精等全系列产品上，均实现了真正的强一致多活 IDC 架构，为客户提供了无以伦比的数据可靠性和服务可用性保证。

安全性和可靠性 - 高可用性反例

- 微信未实现多活 IDC, 导致瘫痪数小时

微信全面瘫痪：服务器故障 国内外均无法连接

中国网 www.china.com.cn 2013-07-22 10:02 打印 | 转发 | 评论

中国网7月22日讯(记者 乔红康)7月22日早间，有大量用户反映腾讯微信发生故障，包括微信信息无法发出、无法刷新朋友圈、无法登陆公众账号平台、无法连接微信网页版等。

从网友反馈的结果来看，包括北京、广东、浙江、山东、黑龙江、河南等地区在内，微信均发生全面故障。有用户表示，目前他人在美国，但也连不上微信。

腾讯微信官方微博对此发布回应称，由于服务器基础网络故障导致出现收发问题，并表示正在恢复中。截至22日上午10:00整，该故障仍未修复。

近期，微信多次出现相关故障，仅在上个月就连续出现多次登录、公众平台、连接服务器等方面的故障。

安全性和可靠性 - 高可用性反例

- 微信和QQ未实现多活 IDC，单IDC空调故障导致微信和QQ瘫痪数小时

工业和信息化部信息通信管理局指导重要业务系统安全稳定运行

间：2023-04-14 16:57　来源：信息通信管理

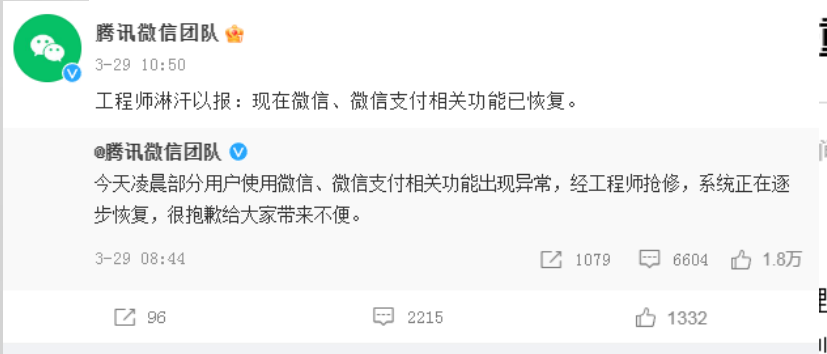
局听取腾讯公司关于“3·29”微信业务异常情况汇报，要求腾讯公司进一步健全安
坚决避免发生重大安全生产事故，切实提升公众业务安全稳定运行水平。
局将深入贯彻落实党的二十大报告关于提高公共安全治理水平的决策部署，统筹发展
管力度，指导电信业务经营者严格落实主体责任、完善保障措施、强化事故应急处置
行业高质量发展。

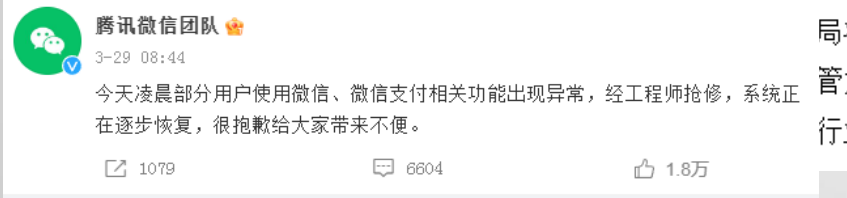
工信部听取“3•29”微信业务异常情况汇报，腾讯：已处罚相关负责人

红星新闻　2023-04-14 21:28

红星资本局4月14日消息，据工信部官网，工信部信息通信管理局听取腾讯公司关于“3·29”微信业务异常情况汇报，要求腾讯公司进一步健全安全生产管理制度、落实网络运行保障措施，坚决避免发生重大安全生产事故，切实提升公众业务安全稳定运行水平。

对此，腾讯方面的相关负责人向红星资本局表示，3月29日凌晨，由于机房配套设施故障，部分用户使用微信相关功能时出现异常。事故发生后，微信内部快速拉起了专项团队，对问题予以解决，并进行全链条梳理、优化产品保障机制。



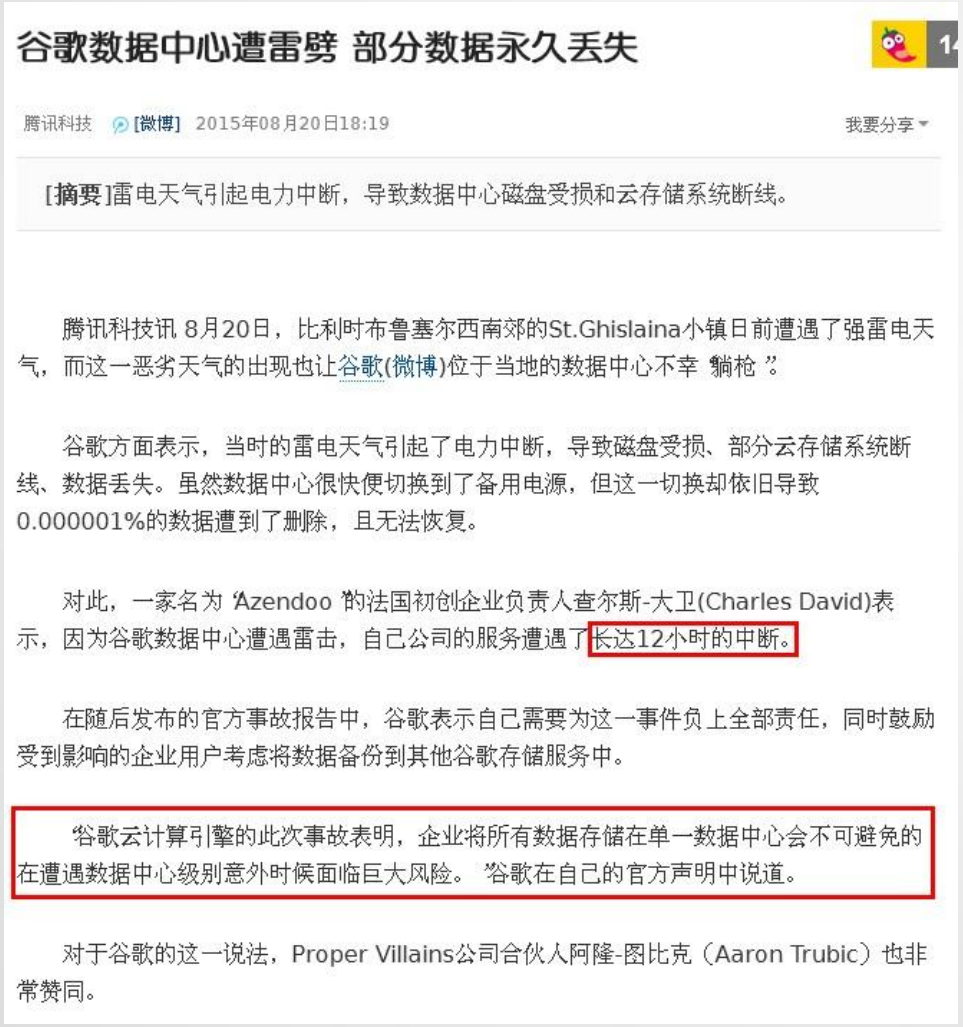


安全性和可靠性 - 高可用性反例

- 支付宝未实现多活IDC, 导致多次瘫痪数小时

安全性和可靠性 - 高可用性反例

- 谷歌云计算服务瘫痪 12 小时并永久丢失数据



谷歌数据中心遭雷劈 部分数据永久丢失

腾讯科技 [微博] 2015年08月20日18:19 我要分享

[摘要]雷电天气引起电力中断，导致数据中心磁盘受损和云存储系统断线。

腾讯科技讯 8月20日，比利时布鲁塞尔西南郊的St.Ghislaina小镇日前遭遇了强雷电天气，而这一恶劣天气的出现也让谷歌(微博)位于当地的数据中心不幸“躺枪”。

谷歌方面表示，当时的雷电天气引起了电力中断，导致磁盘受损、部分云存储系统断线、数据丢失。虽然数据中心很快便切换到了备用电源，但这一切换却依旧导致0.000001%的数据遭到了删除，且无法恢复。

对此，一家名为“Azendoo”的法国初创企业负责人查尔斯-大卫(Charles David)表示，因为谷歌数据中心遭遇雷击，自己公司的服务遭遇了长达12小时的中断。

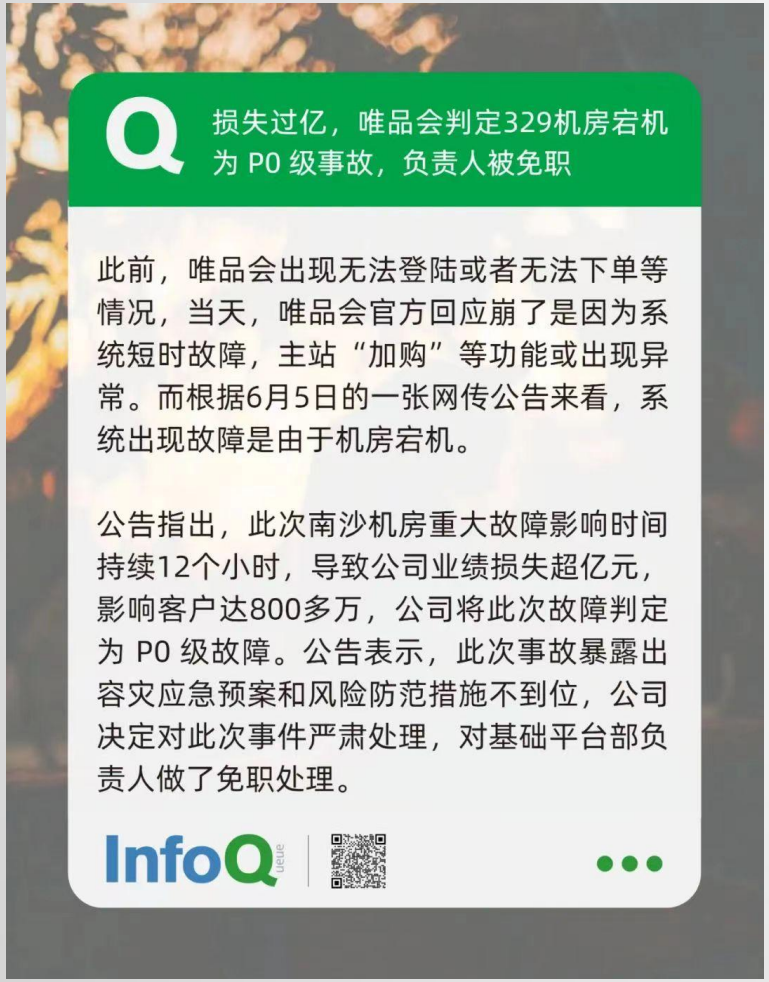
在随后发布的官方事故报告中，谷歌表示自己需要为这一事件负上全部责任，同时鼓励受到影响的企业用户考虑将数据备份到其他谷歌存储服务中。

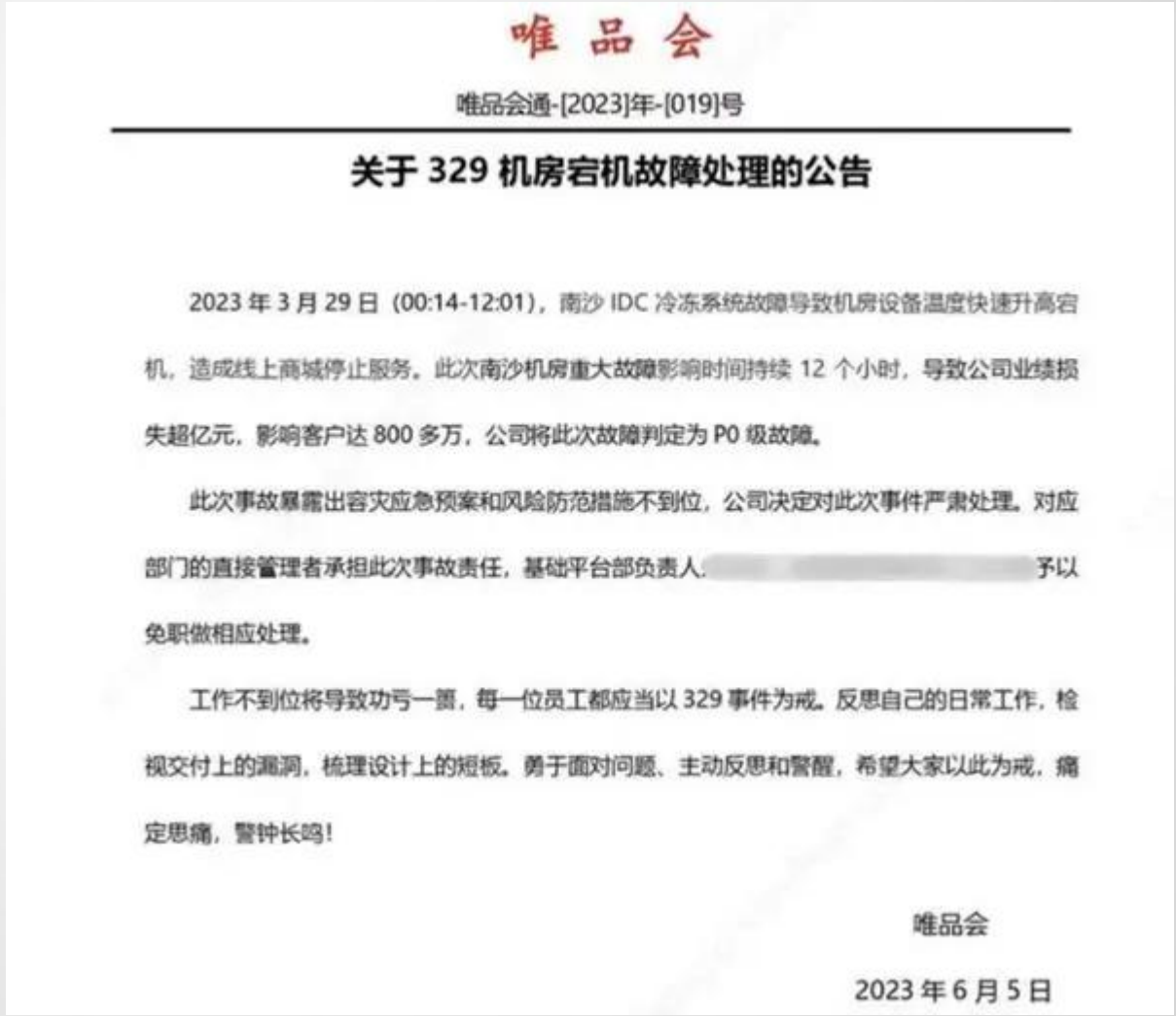
“谷歌云计算引擎的此次事故表明，企业将所有数据存储在单一数据中心会不可避免的在遭遇数据中心级别意外时候面临巨大风险。”谷歌在自己的官方声明中说道。

对于谷歌的这一说法，Proper Villains公司合伙人阿隆-图比克（Aaron Trubic）也非常赞同。

安全性和可靠性 - 高可用性反例

- 唯品会未实现多活 IDC，机房故障下线12小时，损失过亿影响800万用户





唯 品 会

唯品会通-[2023]年-[019]号

关于 329 机房宕机故障处理的公告

2023 年 3 月 29 日（00:14-12:01），南沙 IDC 冷冻系统故障导致机房设备温度快速升高宕机，造成线上商城停止服务。此次南沙机房重大故障影响时间持续 12 个小时，导致公司业绩损失超亿元，影响客户达 800 多万，公司将此次故障判定为 P0 级故障。

此次事故暴露出容灾应急预案和风险防范措施不到位，公司决定对此次事件严肃处理。对应部门的直接管理者承担此次事故责任，基础平台部负责人[redacted]予以免职做相应处理。

工作不到位将导致功亏一篑，每一位员工都应当以 329 事件为戒。反思自己的日常工作，检视交付上的漏洞，梳理设计上的短板。勇于面对问题、主动反思和警醒，希望大家以此为戒，痛定思痛，警钟长鸣！

唯品会

2023 年 6 月 5 日

安全性和可靠性 - 高可用性反例

- QQ 邮箱未实现多活 IDC, 服务大规模瘫痪

就 QQ邮箱等产品大规模瘫痪 作出说明

发布时间：2015-03-20　更新时间：2015-03-31　来源：网络　作者：natty

关键词： 腾讯 公告 网络故障

技术资料　云计算　云服务器ECS　rds　大数据　建站　com域名　软件安装　域名注册

1月21日中午消息，腾讯客服今日发布公告，就 QQ邮箱等产品大规模瘫痪 作出说明。公告指出，由于网络系统故障，QQ空间、QQ邮箱等16款腾讯旗下产品受到影响，目前相关服务正在恢复中。

今日早些时候有消息指出，本次QQ邮箱无法正常登陆的原因是，腾讯第三方登录服务器出现了宕机，但腾讯官方未就此作出回应。

今天上午，多家媒体及微博大号报道了腾讯多款产品无法正常使用的情况，不少网友调侃称 腾讯出事了，出大事了，年终奖发少了，技术把服务器格式化了！”

截至记者发稿，此次网络故障所影响的产品已经基本恢复正常。(木南)

腾讯公告原文：

关于网络故障造成部分业务无法正常使用的通知

尊敬的用户：

您好，非常抱歉，由于网络系统故障，导致您的部分服务使用可能受到影响，目前相关服务正在恢复中，请您稍后再使用，由此给您带来的不便敬请谅解！感谢您的支持。

安全性和可靠性 - 高可用性反例

- 阿里云机房多次故障导致服务中断

尊敬的阿里云用户：

您好，杭州可用区D网络故障确认由于市政施工导致运营商光纤受损 ，现场正在紧急抢修，目前部分链路已经恢复，请您协助我们一起测试观察，详细情况我们稍后给出。

给您
阿里云
2014年

3月3日凌晨，阿里云开始出现大规模故障，位于华北地区的多家互联网公司的 IT 运维人员发现
后一批程序员赶往公司加班。这起宕机事故持续了三个小时左右，事后观察了两个小时。

阿里云

公告

阿里云首页 > 其他 > 【其它】关于华北2地域可用区C部分EC

【其它】关于华北2地域可用区C部分ECS服务器IO HANG通报

北京时间2019年3月3日凌晨，华北2地域可用区C部分
ECS服务器等实例出现IO HANG，经紧急排查处理后
已全部恢复。目前我们已经全面排查其他地域及可用
区，未发现此类情况。
非常抱歉给您带来的影响！如有任何问题，可通过电话
工单随时反馈，感谢您的理解和支持！
针对本次故障，我们将根据SLA协议，尽快处理赔偿事
宜。

阿里云计算有限公司
2019年3月3日

阿里云官方公告

阿里云香港机房为何瘫痪12小时

2015年06月23日 20:53 来源于 财新网

事故发生24小时后，阿里云和运营商对事故原因和细节仍莫衷一是，甚至无辜的消防和电力部门也被拉来躺枪。阿里云作为国内最大的互联网云提供商是否已经准备好

相关报道

【财新周刊】以阿里云击IOE

【大家谈】阿里云：冲看第一而来

阿里云海外扩张提速 借道拜拉进中东北非

中石化牵手阿里云 开启能源大数据

12306春运火车票查询75%由阿里云分流

中国猛虎邮箱将关 阿里云接管

阿里蚂蚁金服60亿建本地生活O2O平台

阿里CEO张勇：做生意的方式将彻底改变

软华联手阿里、中影打造中国电视网络（更新）

阿里挑战CDN玩法

阿里当家 网商银行能飞多高

【财新网】（记者 屈运祖 驻香港记者 王端 见习记者 刘晓景）没有挖断光纤，也不是电力部门问题，更没有所谓的消防警报延误抢修时间，经过财新记者多方调查核实，阿里云在香港中止服务12小时就是一起由硬件故障引发、抢修和恢复严重超时的事故。

这类数据中心的电力事故原本是国内外云服务商普遍面临的一大问题，但用一位业内资深人士的话来说，“12小时才恢复实在太久了。应该几分钟就解决的。”

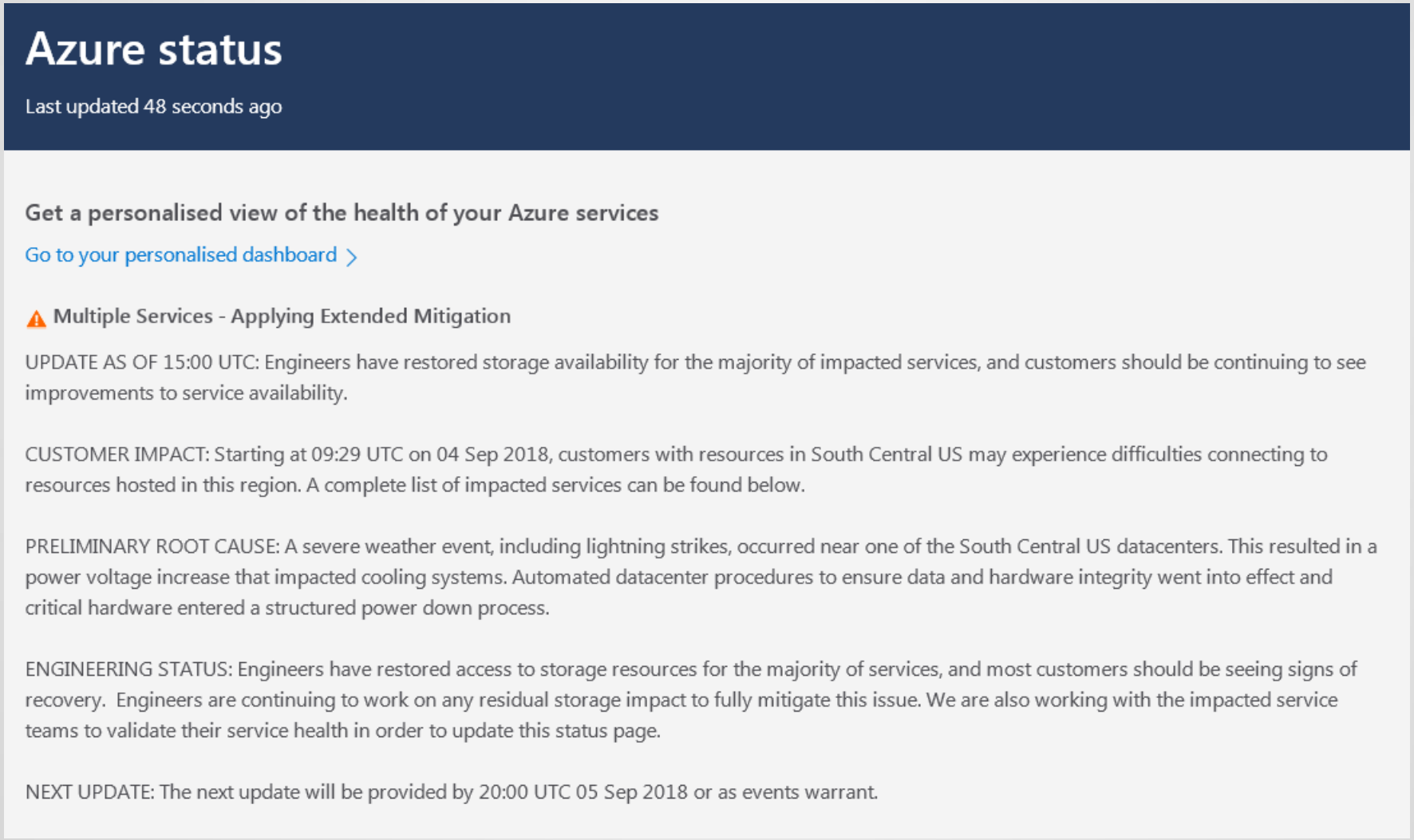
12小时的超长处理时间，以及过程当中阿里云与相关方陆续给出的五花八门甚至自相矛盾的解释引发了用户的不满和业内的质疑，也暴露了阿里云在故障处理和公众沟通中存在的问题。有部分用户甚至反映15个小时业务才恢复。

安全性和可靠性 - 高可用性反例

- 英国航空因机房电力故障导致系统瘫痪数日

安全性和可靠性 - 高可用性反例

- 微软某机房空调故障导致 Office、AD、VS 等服务下线近 14 小时不可用



Azure status

Last updated 48 seconds ago

Get a personalised view of the health of your Azure services

Go to your personalised dashboard ›

⚠ Multiple Services - Applying Extended Mitigation

UPDATE AS OF 15:00 UTC: Engineers have restored storage availability for the majority of impacted services, and customers should be continuing to see improvements to service availability.

CUSTOMER IMPACT: Starting at 09:29 UTC on 04 Sep 2018, customers with resources in South Central US may experience difficulties connecting to resources hosted in this region. A complete list of impacted services can be found below.

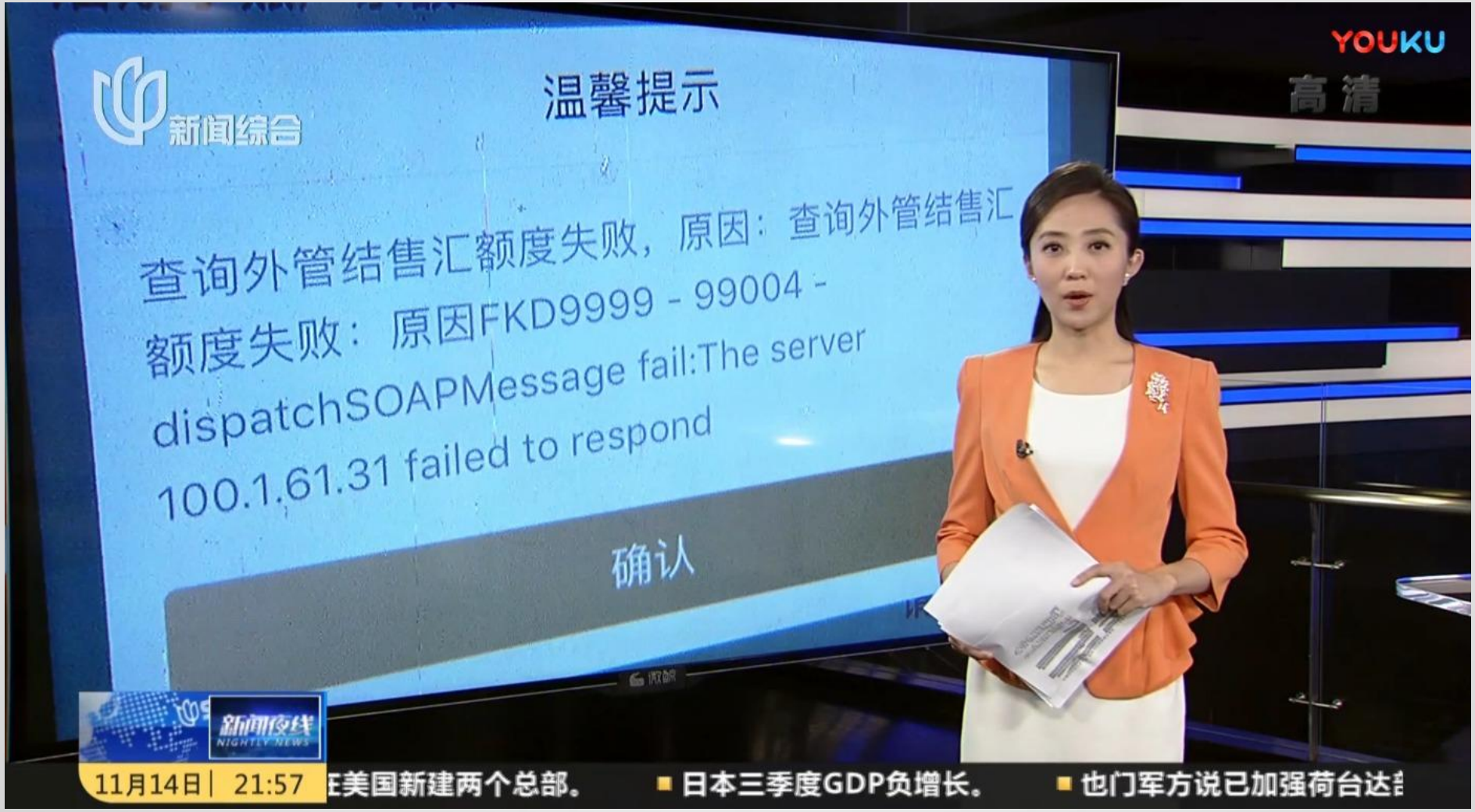
PRELIMINARY ROOT CAUSE: A severe weather event, including lightning strikes, occurred near one of the South Central US datacenters. This resulted in a power voltage increase that impacted cooling systems. Automated datacenter procedures to ensure data and hardware integrity went into effect and critical hardware entered a structured power down process.

ENGINEERING STATUS: Engineers have restored access to storage resources for the majority of services, and most customers should be seeing signs of recovery. Engineers are continuing to work on any residual storage impact to fully mitigate this issue. We are also working with the impacted service teams to validate their service health in order to update this status page.

NEXT UPDATE: The next update will be provided by 20:00 UTC 05 Sep 2018 or as events warrant.

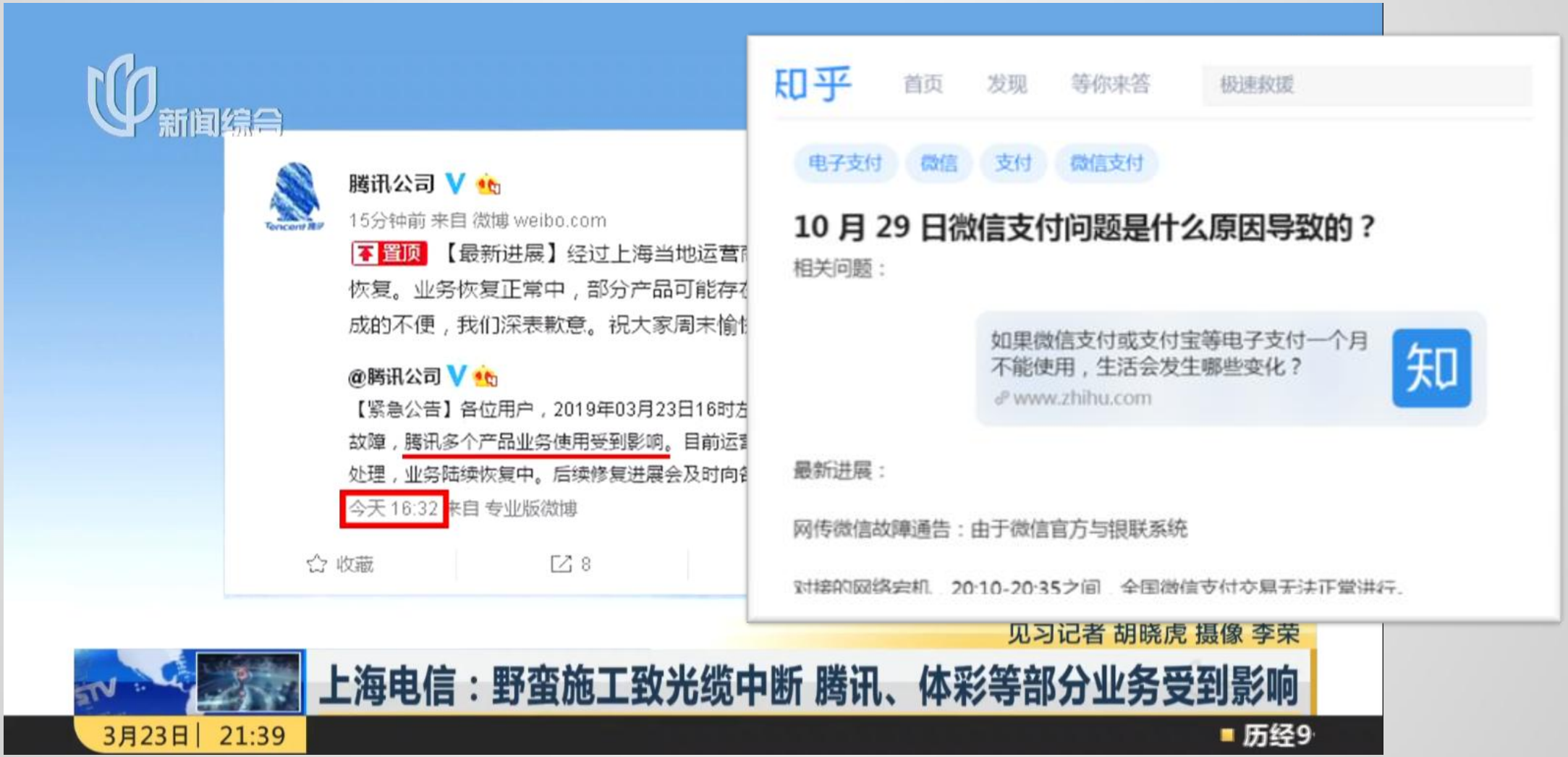
安全性和可靠性 - 高可用性反例

- 国家外汇系统发生故障导致国内所有银行外汇兑换业务停止数小时



安全性和可靠性 - 高可用性反例

- 上海电信光纤被挖断导致腾讯英雄联盟（LoL）等多项业务停止数小时



安全性和可靠性 - 数据安全性 1

- 基于我方自主研发，支持实时（on-the-fly）数据压缩和强加密的虚拟文件系统（VFS），可对包括数据库在内的所有数据提供整库级别的强加密保护，支持包括 AES、 SM4、 BlowFish 在内的数十种业界认可的强加密算法。

注：普通的，以数据库记录为单位的加密通常会将相同的明文转换为同样的密文。

例如：若数据库内的用户表中，有一个名为 Name 的字段用来存放员工姓名，并且明文“张三”被加密后的密文为 “ABCD” ，则对于逐行（逐字段）加密的算法来说，表中每次出现名为“张三”的员工，都将被加密为“ABCD”（类 ECB 模式）。

所有类 ECB 模式对静态分析、差分分析、已知部分明文攻击等破解手段防护能力都很弱，无法确保数据安全。

我方 VFS 使用基于 CTR、CBC 等安全加密模式和 AES 等强加密算法的整库加密技术，提供数学上可证明的强安全性（可靠性、一致性、保密性）保护。即使是相同的明文，也会被变换为不同且完全无关的密文，从而杜绝了上述攻击方式。

安全性和可靠性 - 数据安全性 2

- 支撑平台支持以加盐的安全散列值来存储用户密码。这些信息将经过压缩和强加密处理后才保存到配置存储中。

- 支撑平台支持以基于角色的严格授权机制和访问控制列表（ACL）统一管理用户权限。在开启了整库加密功能后，即使网络管理员也无法窥视企业数据。

安全性和可靠性 - 传输安全性

- 基于支撑平台的产品可使用公认权威机构发布的数字证书，提供网银级别的 TLS（HTTPS）网络数据传输保护以及基于 BYST 的端到端安全传输能力。

- 用户密码以加盐安全散列的形式进行存储。使用基于 SHA 和 HMAC 安全算法的 CHAP 鉴权协议完成网络鉴权流程。即使不依赖 TLS 加密保护（全明文传输），也不会发生密钥泄露。

- 可配置同一用户连续 N 次登陆失败后，强制冷却 M 分钟，配合入侵检测和恶意请求过滤技术，防止暴力破解。此外，管理员也可自定义最小长度，大小写字母和数字组合等密码复杂度要求。

- 可使用 EAL5+ 级别专用智能卡实现硬件级别的安全鉴权访问。

安全性和可靠性 - 系统安全性 1

- Java（JRE）、C#（.NET）以及 Tomcat 等环境存在大量严重安全漏洞，有极高安全隐患。通过国际安全组织公开的 CVE 数据库可发现，上述产品几乎每年都会有多个严重等级为“满分”最高级的新漏洞被披露。例如：

- Java：https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-19117/Oracle-JRE.html

- Tomcat：https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-887/Apache-Tomcat.html

- .NET：https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-2002/Microsoft-.net-Framework.html

- 等等。

安全性和可靠性 - 系统安全性 2

- 如左图所示：对 Java、.NET 等动态运行时环境、Tomcat 等容器，以及 Spring 等第三方框架的依赖，导致系统中被引入了大量额外的，不受开发商控制的第三方组件。
- 可以看到，使用 Java、.NET、PHP 等动态语言开发的产品，其应用程序与底层基础设施间包含了第三方框架、Web容器、动态运行时等多个额外层面。这些不受开发商控制的，由第三方软件组成的额外层面包含大量广为人知，可被轻易利用的安全漏洞。

安全性和可靠性 - 系统安全性 3

- 甚至任何稍有常识的普通用户都可以通过搜索引擎简单地找到可成功利用这些漏洞进行攻击的免费开源工具，并以此入侵企业系统，完成数据窃取、数据篡改、数据销毁等非法操作。请尝试百度“漏洞扫描”、“渗透工具”等关键词。

- 由此可见，引入不受控制的额外层面大大增加了系统的受攻击面，严重增加了系统的安全风险。同时大大增加了运维人员的工作负担，提升了系统的总体拥有成本（TCO）。

安全性和可靠性 - 系统安全性 4

- 如上图所示：基于支撑平台的产品使用汇编、C/C++等工具开发。
- 直接构建在底层操作系统和硬件平台之上。

- 基于支撑平台的产品以高效的原生机器码（Native Code）直接运行在裸硬件和操作系统构成的底层基础设施上，为软件产品带来了无与伦比的时空效率和安全性保障。

- 由于无需依赖动态运行时、Web容器等不可控的第三方组件，因此大大减少了软件的受攻击面，极大地降低了系统安全隐患。同时在很大程度上减轻了运维人员的工作负担，降低了客户总体成本。

安全性和可靠性 - 安全性补充说明

- 近年来安全问题频发，亚马逊、沃尔玛、Yahoo、Linkedin（领英）、索尼、OpenAI（ChatGPT）、摩根大通、UPS、eBay、京东、支付宝、协程、12306、网易、CSDN、中国人寿、以及各大酒店集团（锦江、洲际、喜来登、万豪、华住等）等国内外知名企业均频频报出大量用户信息泄露的严重安全事件，安全保障已经刻不容缓。

- 支撑平台支持所有数据库（整库）和本地配置数据均存放在我方自主研发的，支持实时（on-the-fly）数据压缩和强加密的虚拟文件系统（VFS）中，进行全方位保护，支持数十种业界公认的强加密安全算法，即使系统管理员也无法窥视企业数据。

- 基于业界标准的强加密算法保证了即使未来出现了每秒钟可完成一千万亿次密钥破解尝试的超级计算机，也需要平均五千四百万亿年才能破解一个密钥。安全性得到了极大保证。

安全性和可靠性 - 安全性反例

思科：Java 成 91% 恶意攻击的主要原因

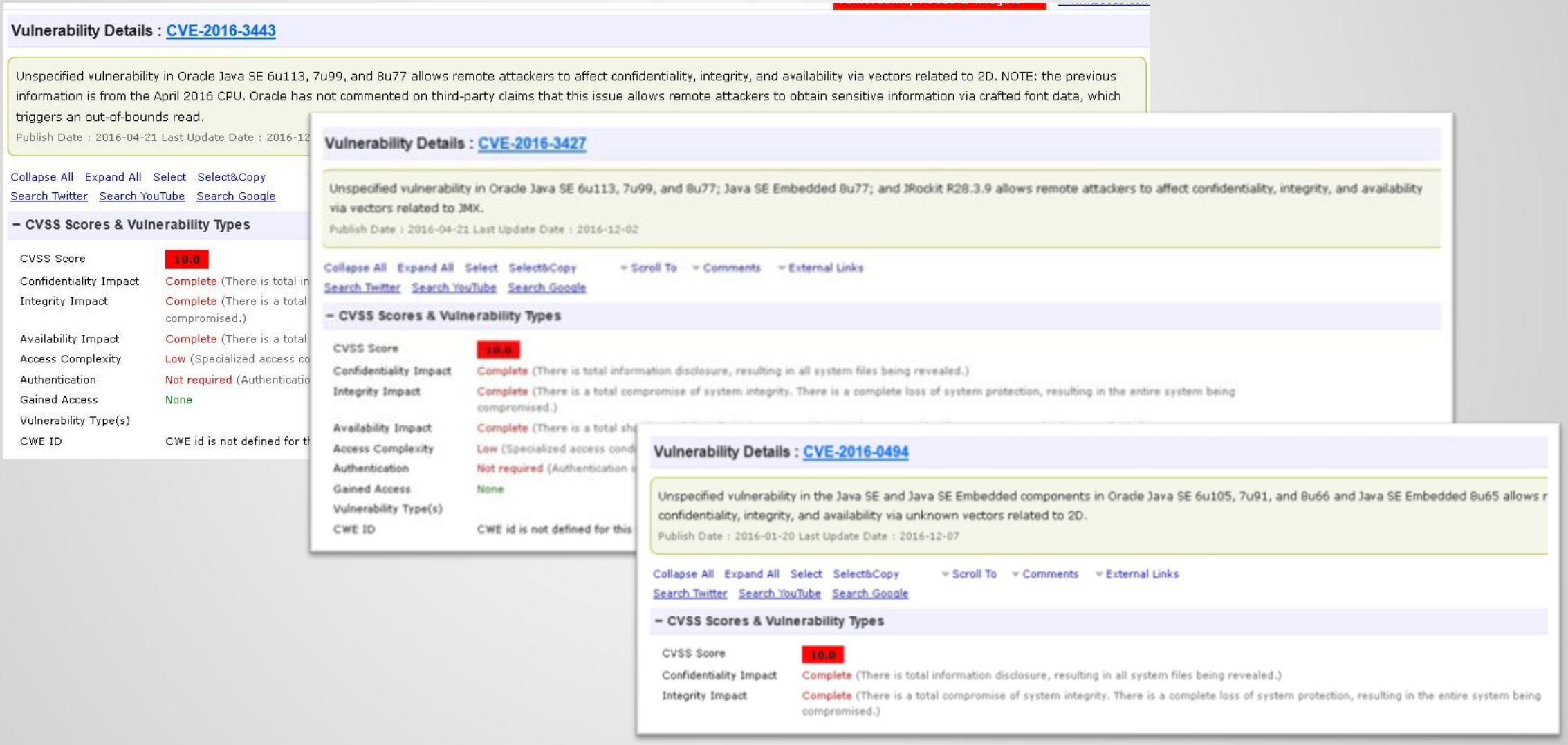
2018开源代码安全报告：每个代码库平均包含64个漏洞

王练　发布于2018年07月06日　收藏 3　评论 2

Synopsys 公司近日发布了"2018 年开源代码安全和风险分析" Black Duck（黑鸭）报告，深入考察了商业软件中开源安全性，许可证合规以及代码质量风险的状况。本次报告讨论的是从 2017 年审计的超过 1,100 个商业代码库中的匿名数据所得出的结果，行业包括汽车、大数据（主要是人工智能和商业智能）、网络安全、企业软件、金融服务、医疗保健、物联网（IoT）、制造业和移动应用市场。

安全性和可靠性 - 安全性反例

- Java 高危漏洞一瞥



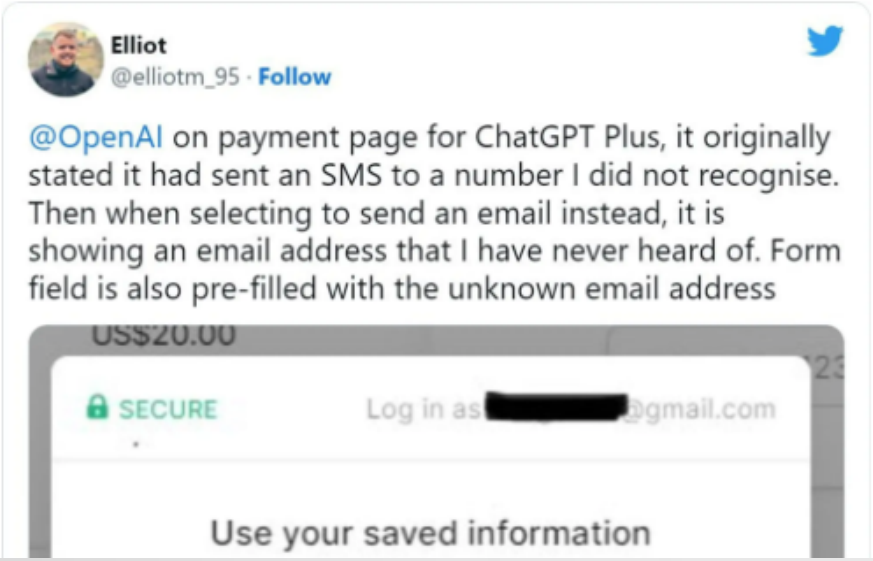
安全性和可靠性 - 安全性反例

- ChatGPT 因 Redis 的安全漏洞泄露用户隐私会话数据

Redis 错误导致 ChatGPT 数据泄露，技术细节一并公布

来源: OSCHINA　编辑: Alias_Travis　2023-03-27 08:52:26　8

在上周一，ChatGPT 遭遇了一次用户数据泄漏事件，许多 ChatGPT 的用户都在自己的历史对话中看到了其他人的对话记录。不光是对话的历史记录，不少 ChatGPT Plus 用户还在 Reddit 和 Twitter 等平台发出了截图，表示在他们的订阅页面上看到了其他人的电子邮件地址。



安全性和可靠性 - 安全性反例

- 安全漏洞导致 Yahoo 泄露超 30 亿用户数据

安全性和可靠性 - 安全性反例

- 网易泄露过亿用户数据

网易邮箱被曝过亿数据泄露

腾讯科技 [微博] 梁辰 2015年10月19日15:39 我要分享

腾讯科技讯（梁辰）10月19日，有用户“路人甲”在国内安全网络反馈平台WooYun（乌云）发布消息称，网易163/126邮箱过亿数据泄漏，涉及邮箱账号、密码、用户密保等。这一漏洞危害等级被标注为“高”。另有消息称，此次泄露规模或达5亿条的规模。同时也有人表示，已向苹果客服咨询，苹果客服称网易服务器被入侵。

不过，截至腾讯科技发稿时，乌云平台已将“网易邮箱”抹掉，改为“某邮箱”。目前的漏洞状态为已交由第三方合作机构(cncert国家互联网应急中心)处理。

导致此次安全事件的原因，疑似网易用户数据库泄露，影响数量总共数亿条。乌云方面称，目前已通过乌云漏洞平台第一时间通知到网易。

乌云平台披露，目前泄露的信息包括用户注名、MD5（一种算法）密码、密码提示问题和答案、注册IP、生日等。据悉，解开后测试大部分邮箱依旧还可登陆。

安全性和可靠性 - 安全性反例

- Java Struts 框架漏洞致京东数千万用户帐户密码和信用卡等敏感数据泄露

安全性和可靠性 - 安全性反例

- 支付宝泄露数千万用户数据

支付宝数据泄露!工信部介入密码泄露调查

字号 大 小

2011年12月30日11:06 来源： 太平洋电脑网 作者：盛夏Veya 欢迎发表评论

将本文转发至：

纠错 | 收藏

12月30日消息，中国互联网正在遭遇一场最大规模的用户信息泄露事件，而此次“泄密门”事件波及的范围也越来越广，从互联网科技公司，到互联网电商企业，都难逃数据泄露的厄运。而如今，就连银行、出入境局登记数据也被传有泄露。目前，工信部已经介入此次大规模的密码泄露事件，强烈谴责窃取和泄露用户信息的行为，责令发生用户信息泄露的网站尽快发出警示，要求互联网站开展全面的安全自查。

不断扩大的互联网用户信息泄露阴影

继CSDN、天涯社区等论坛确认用户资料被泄露之后，一向被用户定义为“安全”的第三方支付平台也被爆料称上千万的用户信息外泄。

漏洞概要 关注数(8)

缺陷编号： WooYun-2011-03871
漏洞标题： 支付宝用户大量泄漏，被用于网络营销
相关厂商： 支付宝
漏洞作者： 路人甲
提交时间： 2011-12-28
漏洞类型： 用户资料大量泄漏
危害等级： 高
自评Rank： 20
漏洞状态： 等待厂商处理
漏洞来源： http://www.wooyun.org
Tags标签： 无
分享漏洞：

漏洞详情

简要描述：

支付宝用户大量泄漏，被用于网络营销 泄漏总量达1500-2500W之多 泄漏时间不明，里面只有支付宝用户的账号，没有密码

漏洞hash：6701ae23372bbea6c1dd74f23d8c584e

支付宝用户信息也被泄露

日前，网络安全问题反馈平台“乌云漏洞”指出，支付宝部分账号信息被泄露，涉及邮箱数量在1500万至2500万。对此，支付宝公关经理朱先生否认支付宝存在漏洞一说，并称相关账号并

安全性和可靠性 - 安全性反例

- 信用巨头 Equifax 因 Java Struts 漏洞泄露 1.43 亿人社保、信用卡等敏感记录

Cybersecurity Incident & Im

Consumer Notice FAQs Potential Impact Enroll Trust

A Progress Update for Consumers

September 13, 2017

1) Updated information on U.S. website application vulnerabi

Equifax has been intensely investigating the scope of the intrusion wit
information was accessed and who has been impacted. We know tha
Apache Struts CVE-2017-5638. We continue to work with law enforce
with law enforcement.

2) Temporary interruption to credit freeze sign-up link.

sina 新浪财经 新浪财经 > 美股> 正文

美国1.43亿人个人信息被泄露

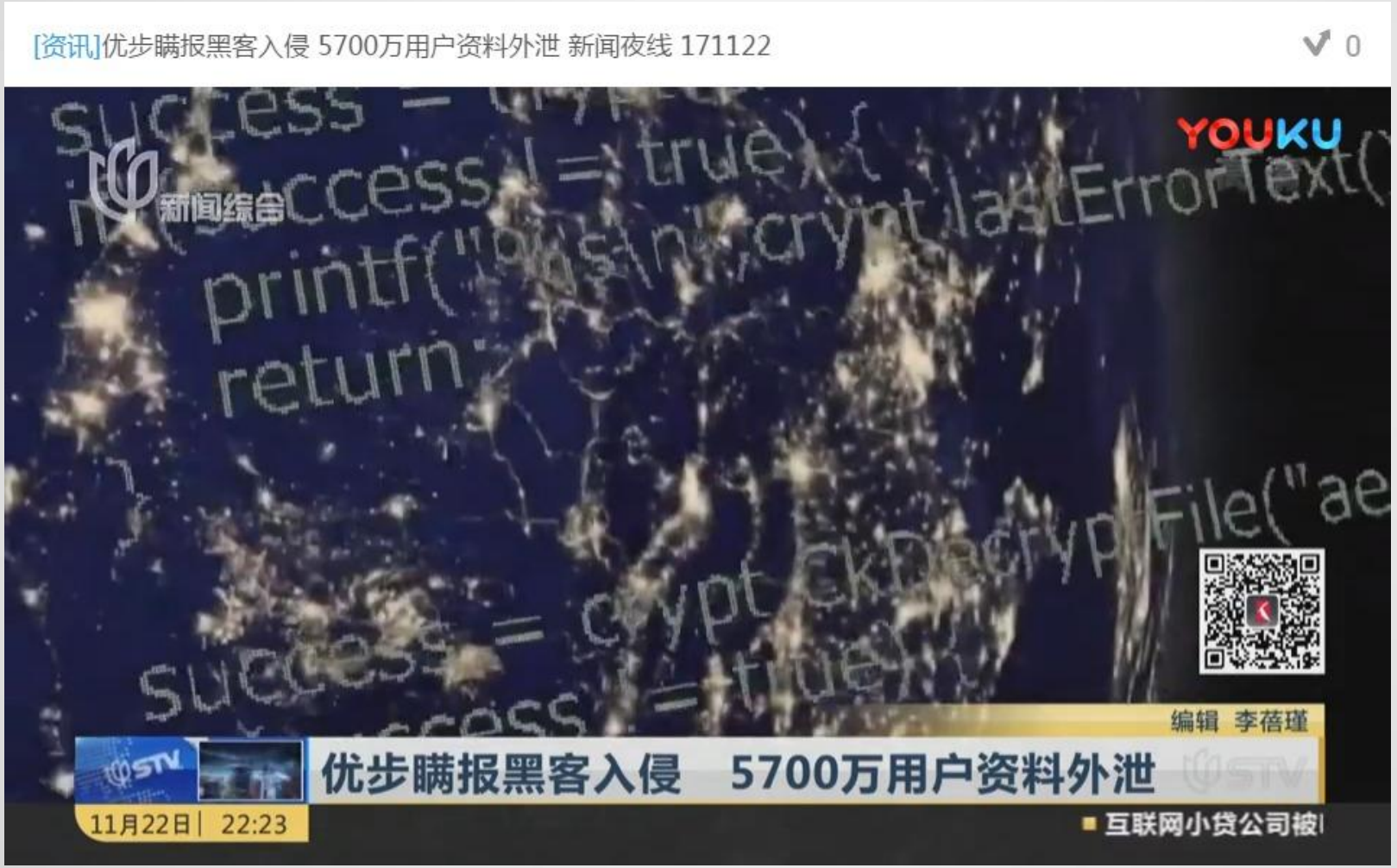
2017年09月08日 08:40 新浪科技 微博 暂无评论(10人参与) 收藏本文

美股行情中心：独家提供全美股行业板块、盘前盘后、ETF、权证实时行情

新浪科技讯 北京时间8日早间消息，美国征信企业Equifax披露称，其网站遭遇黑客攻击，造成1.43亿人的个人信息泄露，包括社会保障号码和驾照信息等。这可能是近年来最大的一起泄露事故。之前雅虎虽然泄露了10亿账户信息，但里面没有包含社会保障号和驾照信息。

安全性和可靠性 - 安全性反例

- 优步 (Uber) 瞒报黑客入侵 5700万用户资料外泄



安全性和可靠性 - 安全性反例

- Java XML 组件 XXE 漏洞导致的微信支付“零元买买买”重大安全事故

www.news.cn 新华网 NEWS www.xinhuanet.com

让新闻离你更近

微信支付曝“0元购”漏洞 安全

2018-07-04 15:04:57 来源：新华

关注新华网

微信

微博

Qzone

0 评论

新华社厦门7月4日电（记者颜之宏）3日，有网络安全机构曝光了一组
技术漏洞，据称攻击者可利用该漏洞将自己伪装成微信支付平台，通过篡改
获得“0元购”特权。记者3日晚间从微信支付官方渠道获悉，该漏洞已修复，
度恐慌。

据网络安全专家谢忱介绍，从当前被公开的漏洞信息来看，网络攻击者
信支付官方SDK（软件工具开发包）存在的漏洞，将自己伪装成“微信支付平
通过微信的漏洞伪造与商户的直接通信，在篡改微信支付的正常通信信息后
换柱”的目的。

谢忱表示，正常的支付流程应该是由用户发起，经由微信支付平台到达
会有一个与微信支付平台确认支付结果的过程，而网络攻击者恰恰是利用了
“骗”过了商户。谢忱认为，一些商家的安全防护水平较低，攻击者还可通过
商户的密钥等信息，再通过这个漏洞就可以实现“将订单设置为0元”等操作，
导致该商户的消费者信息等数据内容泄漏。

网络支付安全专家于迪则认为，接入微信支付的商户不必过度恐慌。于迪表示，该

关于20180704微信支付漏洞的分析

kanmars
一个不懂生活的人，正在补习前半生的失误

+ 关注他

2 人赞了该文章

今天看新闻，说微信官方SDK有漏洞。

微信支付曝漏洞：可发伪造信息使购物无需付费

7月4日消息，近日有网友在国外安全社区发帖称微信支付官方SDK存在的严重漏洞，攻击者可通过此漏洞侵入商家服务器，获得商家关键安全密钥，通过发送伪造信息来欺骗商家而无需付费购买任何东西。

腾讯对此表示，微信支付技术安全团队已第一时间关注及排查，对官方网站上该SDK漏洞进行更新，修复了已知的安全漏洞，并在此提醒商户及时更新。

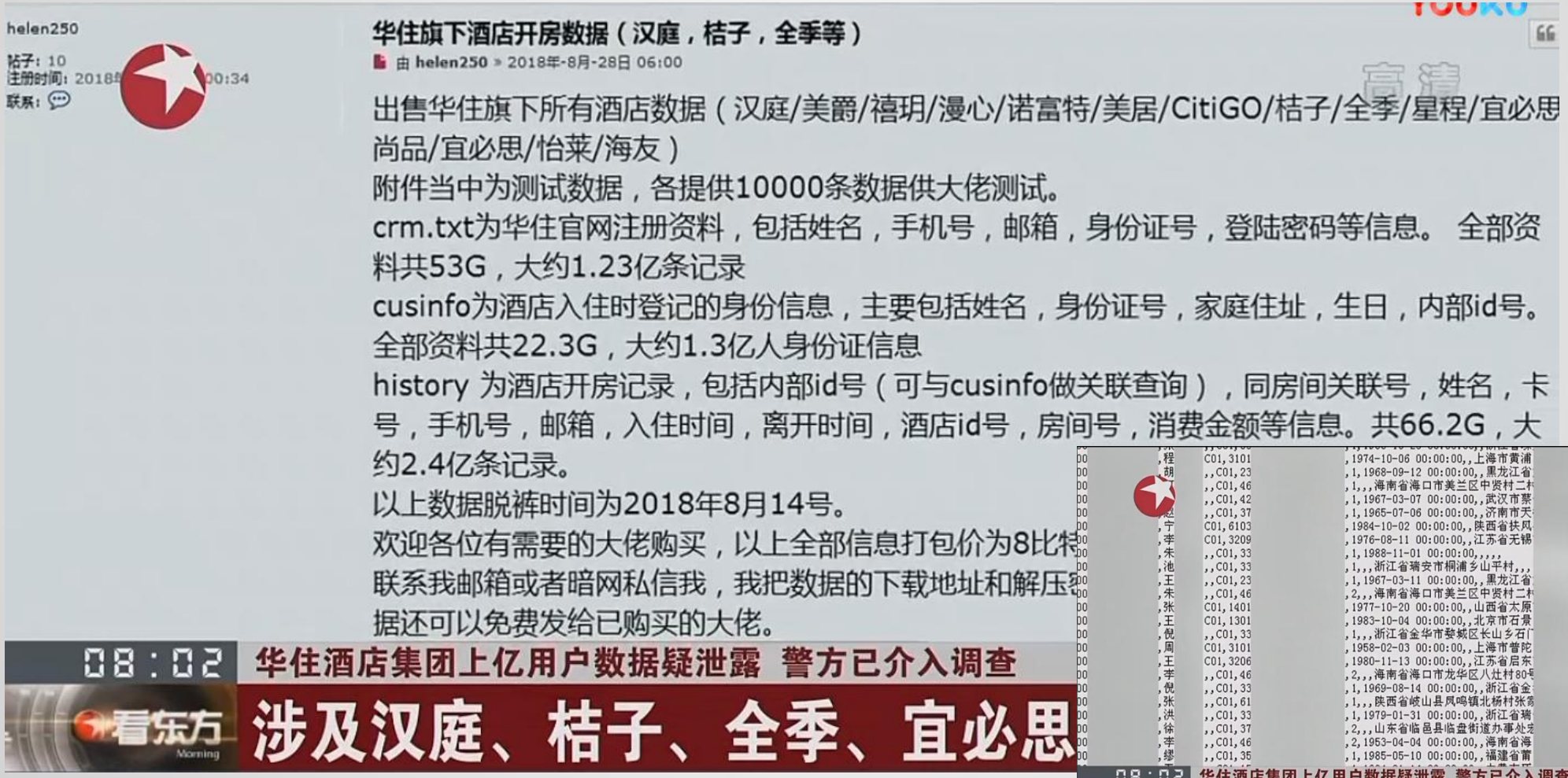
```
Example  vivo :
 attack:
    notify url:   https://pay.vivo.com.cn/webpay/wechat/callback.oo
          cmd: /home/

     result:
        tomcat

attack:
    notify url:   https://pay.vivo.com.cn/webpay/wechat/callback.oo
          cmd: /home/tomcat
    result:
```

安全性和可靠性 - 安全性反例

- 华住集团汉庭、桔子等多家酒店泄露 1.3 亿人敏感信息和 2.4 亿开房记录



安全性和可靠性 - 安全性反例

- 万豪集团喜来登、威斯汀、W等多家酒店泄露 5 亿人敏感信息和开房记录


重玄科技
PHILO-TECH