腾讯安全20年“破茧”之路

转载

techweb 于 2020-01-14 12:50:00 发布 880 收藏 1

消费互联网时代，BAT三家称雄。产业互联网时代，BAT无一缺席，但格局已悄然改变。阿里最先跑出来，BT紧随其后，华为等实体企业纷纷介入，原本的三国杀变得扑朔迷离。其中，最大的变量无疑是腾讯，无论是从资本还是体量上来看，腾讯均有打破原本格局的实力。消费互联网时代，腾讯除了手握QQ、微信两大利器，掌握海量用户优势，同时还构建了领先的信息安全技术实力；进入产业互联网，最懂用户的腾讯能否复制过去的发展效率？

（一）守护QQ：被“逼出”安全能力

中国消费互联网的诞生，追根溯源可以到上世纪90年代，但每家公司的命运各不相同，有胜利者也有失落者——最早位于中关村的“瀛海威”，由于找不到清晰的盈利模式而轰然倒下。其后，百度、阿里巴巴等“新生代”互联网公司幸运突围，大都是因为“仿效”海外互联网企业的商业模式而成功，百度对标谷歌、阿里有点像亚马逊，在三巨头中唯一不同的或许是腾讯。

腾讯起身于即时通讯工具，但也是苦于找不到盈利模式。2000年，马化腾每个月都在发愁，用户增长太猛了，服务器费用hold不住，怎么都赚不到钱。因此，小马哥还一度滋生了干脆卖掉算了的念头。如果，当时有个土豪真的“撒币”买下来，还会有现在的QQ吗？这种假设很多人都曾YY过，但历史没有如果。

2003年，QQ秀的出现令马化腾松了一口气，终于有人愿意为QQ付费了。此后，等级加速、背景音乐、空间装扮等新开发的功能犹如一台台钞票机，向腾讯源源不断地输送钞票。但随即，腾讯就尝到了“成长的烦恼”。

的确，当QQ从一个单纯的社交账号升级为个人身份标识时，用户是不吝花钱的。然而，彼时的消费者尚未有明确的网络安全防范意识，从而给一些不法黑产者钻了空子。而用户是不会承认自己的过失，只能将怨气撒到腾讯这个产品的研发者身上。

比如，在QQ的规则中，有一条是通过累计时长可以从星星、月亮升至太阳。而在那个年代，顶着一轮太阳就像是幼儿园朋友得了大红花，倍儿有面。很快，市场上就流行一种“代挂太阳”服务（类似后来的游戏代练），而一些不法代挂者就会利用你的账号密码去干“坏事”，也就是所谓的“盗号”。当然，还有一种更粗暴的方式，就是专门利用针对QQ的病毒木马，直接盗取用户账号。

（还记得那段比拼QQ等级的岁月吗？）

在此基础上，还催生了名为“QQ信封”的黑色产业链条，通过分工合作的模式将用户账号里的q币低价出售，或者帮助某些商家进行投票、打广告或者是诈骗，以此来牟取不法利益。

“盗号”、黑产的破坏，导致用户资产的流失，严重影响用户使用体验，使刚刚盈利的腾讯大为恼火。于是，从2005年开始，腾讯就开始对每一位用户加装密码锁，相继在密码、文件传输、链接等功能上研发了各种安全保护技术，火速上线QQ医生。

不过，QQ医生的推广也并非一帆风顺。用户对于这个新生的软件不太信任，腾讯安全团队的人曾打电话给一位被盗号者，询问其为何不使用QQ医生，得到的回复是“谁知道安全软件是不是在盗取我们的信息？”此后，安全团队的工作人员就不得不化身为“接线员”，与众多QQ用户沟通，反复确认他们的痛点，进而对QQ医生进行升级。

（颇有年代感的“QQ医生”界面）

可以说，腾讯安全的出发点，是先造一个“轮子”守护QQ的安全，保证用户的使用体验，促使用户与盈利的双双增长。但谁也不曾想到，安全这种能力一经发芽，会伴随着腾讯的业务茁壮成长，成为腾讯业务中一条不可或缺的“暗线”。

（二）从造“发动机”到构建“安全云库”

QQ医生是专门针对QQ安全问题而产生的一款软件，但仅靠QQ医生能守护用户的QQ安全吗？答案显然是：NO！毕竟，一些不法黑客的门道太多了，他们可以在电脑端、浏览器以及其他应用上植入木马病毒，进而侵入QQ的账号体系。

而当时，国内众多安全厂商基本上都没有自己的杀毒技术，基本上都是采用OEM的方式。其中，自然也包括腾讯。而这就造成了两个方面的不利后果：其一，核心杀毒引擎受制于人，很容易被别人卡住脖子，导致出现类似于后来中兴事件的危机；其二，产品与杀毒引擎匹配度不高，用户体验不好，不仅无法适应日益增长的用户规模，也不能真正守护用户安全。

尤其是突如其来的3Q大战，彻底坚定了腾讯在安全核心技术建设方面投入的决心。

腾讯意识到，“我们不仅应该只造轮子，更应该造发动机”，开始下大力气自研杀毒引擎。2011年，以马劲松为首的安全团队用了半年时间，摸索出一款TAV杀毒引擎。产品出来一测评，对病毒的检出率指标虽然不错，但是，它对电脑的内存占用甚至超过了OEM，本来那点儿值得骄傲的资本瞬间没有了。

怎么办？重新做呗。经过对文件筛选过滤，根据细分场景进行文件检查，精简病毒库，改进算法引擎，等等，又折腾了一年多，2012年中期，杀毒引擎达到了理想状态，装了该杀毒引擎的电脑管家在第三方软件测评中跻身第一梯队，PC终端的防护终于有了保障。

（2015年，马劲松和同事在办公室等待测评结果）

并且，在腾讯自研第二代“鹰眼”引擎、QQ全景防卫等技术创新基础上，腾讯电脑管家还将其运营的全球最大风险网址数据库命名为“安全云库”，并进一步推进腾讯电脑管家互联网安全开放平台建设，面向“搜索引擎、社交工具、论坛、网购”等网民主流上网入口服务商免费输出网址云安全数据与服务。这就意味着，腾讯并不满足于为用户提供一款安静好用的杀毒软件，而是极力打造全球最大风险网址数据库平台，将安全能力辐射到整个互联网环境中。

（三）积蓄人才，开放生态

移动互联网时代，腾讯继续以QQ、微信等社交优势构建IM“入口”来圈占用户。而在构建人与人连接后，腾讯意识到如果想要开拓更多的商业应用、更好地将用户变现，只有让更多的合作伙伴参与进来，开辟更多应用场景，才能为用户提供更多有价值的服务。于是，京东、58、大众点评、美团、猫眼等相继加入腾讯生态阵营，腾讯由此延伸到人们生活的各个层面。

然而，移动互联网红利的爆发，也使得安全能力的重要性更加突出，如移动支付、信息诈骗、垃圾短信等都成为了新型的、攻击性更强的黑产模式。一招不慎，用户就会“羊入虎口”。因此，腾讯不惜投入重金网罗安全人才，加强对安全技术的研发，极力构建一张涵盖安全攻防、威胁情报等多个领域的安全网。

业内人士指出，国内安全行业的现状是——缺乏权威人才培训和认证标准，缺乏培养机制和体系。因此，一方面，腾讯宣布成立七大安全实验室，将TK、吴石、yuange等安全行业Top级白帽黑客吸纳进来，专注安全技术研究及安全攻防体系搭建。另一方面，还面向全球范围内的在校学生、安全从业者等，发起TCTF、极棒等安全专业赛事；并积极参加强网杯、DEF CON CTF等国内外顶级比赛，选拔出最具潜力的年轻安全人才，并通过后续持续培养，建立集人才挖掘、人才培养、价值转化为一体的链式网络安全人才培养体系，打造互联网安全领域未来领军人才。

（2016年，腾讯七大安全实验室掌门人）

这种切入上下游，实现高校、实验室等共同联动的安全人才培养机制，可谓是一记妙招，从人才梯队建设上对其他安全厂商形成“截胡”。无怪乎，近年来腾讯在安全攻防领域成绩骄人：2018年四大国赛包揽三项冠军，并夺得堪称国内最严苛的云安全挑战赛——贵阳大数据及网络安全攻防演练中攻与防的双料冠军。2019年某国家级重保行动中，阻断TCP攻击近20亿次，阻断WEB攻击近300万次，封禁IP6.8万，实现0事件通报、0失分。

（2016年DE FCON CTF 2016，腾讯-0ops和blue-lotus组成的b1o0p战队斩获第二名，创造该项赛事中国战队新的排名纪录）

腾讯的另一记妙手是“开放”，奉众人之力以供安全，与合作伙伴联手共建云安全生态。比如，借鉴微软、谷歌、Facebook、苹果等公司的做法，开展了“漏洞奖励计划”并推出了“安全问题反馈平台”，邀请广大安全专家帮助腾讯发现安全问题。2015年10月，腾讯更是将“漏洞奖励计划”正式升级为“威胁情报奖励计划”。再比如，腾讯还联合国内安全上市公司发起P17安全领袖俱乐部，以及聚合国内主流安全新锐力量的FP50俱乐部，希望通过“能力开放、服务开放、生态共建”三大举措，全面开放腾讯产业生态资源。

（P17安全领袖俱乐部在CSS 2019上合影）

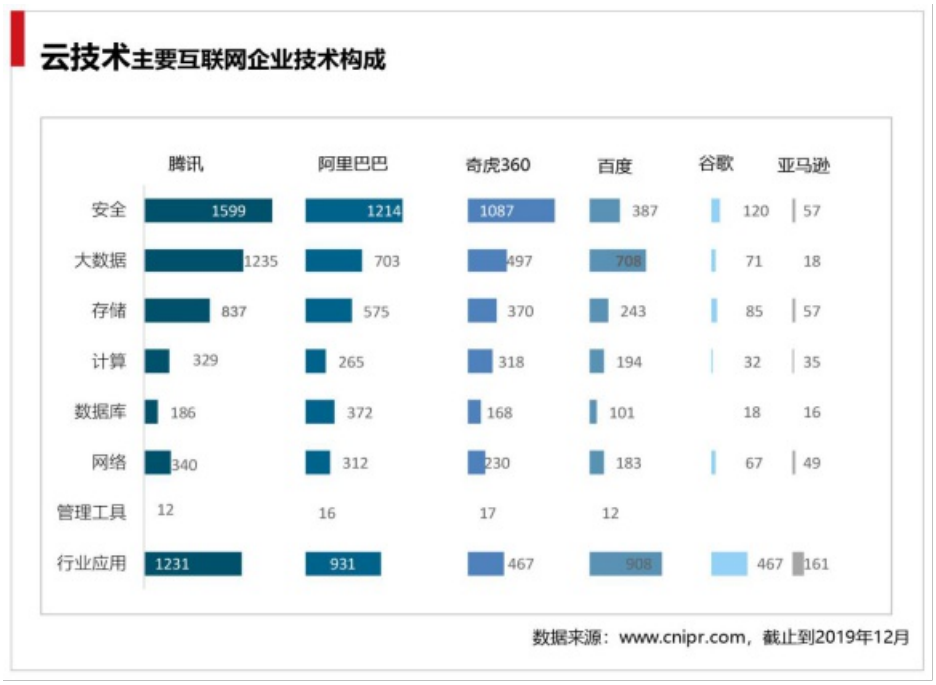
“安全为人人，人人为安全”。凭此，腾讯的业务迅速渗入到消费者互联网的各个场景中，增强了用户粘性，也夯实了腾讯在安全大数据、安全攻防、威胁情报等方面的实力，更让众多不法黑产者陷入人民群众的“群体智慧”汪洋大海之中。

（四）护航产业互联网，打造云上安全竞争力

互联网下半场，AI、5G、云计算等数字技术加速产业互联网发展，服务稳定、信息安全已经成为各大互联网公司发力云计算市场争夺的核心竞争力，也是客户在选择云计算服务厂商的核心考量要素之一。

毕竟，在企业纷纷上云的情况下，在云管端等每一个节点出现故障都有可能引发企业震荡。2018年，全球最大的连锁酒店万豪国际酒店旗下的喜达屋因被黑客入侵，造成约5亿用户信息泄露，不仅在美国遭遇全体诉讼，索赔125亿美元。消息公布后，万豪国际美股盘前跌逾5%。而与前些年的广撒网式勒索攻击相比，2019年针对性勒索逐渐增多，黑客通过人工主动渗透确认高价值服务器后，加密数据并勒索高额赎□……在企业安全方面，永远没有后来者。

腾讯在信息安全方面的20余年技术积累和经验沉淀，恰好成为其核心优势。从QQ开始，腾讯经历了软件安全、终端安全、业务安全、云安全、内部安全能力工程化输出等几个阶段，其本身就是产业互联网时代的系统性安全实践样板。因此，在涉及主机安全、账号安全、数据安全等安全技术以及大数据领域等方面，腾讯都储备了大量专利。据i智库发布的《中国互联网云技术专利分析报告》显示，腾讯在以上两个技术分支的专利申请量均排名第一，具有极大的技术优势。



（《中国互联网云技术专利分析报告》）

基于以往自研安全产品和原生安全等理念，腾讯对云进行了全栈基础设施建设的规划，确立“一个基础底座、两个中台、一个中心”。其中，一个基础底座指的是腾讯云的全栈基础设施，两个中台指“云数据安全中台”和“租户安全运营中台”，一个中心是指“云安全管理中心”。

（企业“开箱即用”的云数据安全中台）

与此同时，腾讯还专门成立了云全栈安全研究组，集结内部七大安全实验室和安全平台部超过300人的顶尖研究力量，对云平台的合规管理、基础设施、系统安全、数据安全、应用安全、网络访问固件自身的安全展开全面、前瞻性的研究，构建一套基于云的原生安全体系，不仅保障云平台的安全性和稳定性，同时也将安全服务内置到云中。

其次，在消费互联网时代，腾讯拥有超过500个业务场景，积累了海量针对C端用户安全的经验。那么，在产业互联网时代，腾讯就能够通过每天数百P的数据运算能力，利用其强大的中台能力，将这些安全经验沉淀成产品和服务提供给B端用户，向企业输出定制化的安全服务。

（灵鲲平台可视化数据呈现）

比如，在2019年6月中标的智慧绿道项目中，腾讯云就开放了公有云平台系统服务、网络安全系统服务、大数据平台系统服务等能力，与东华软件提供的智慧产业应用相互融合，从文化、体育、旅游、商业、农业五个方面，为市民游客、企业商家及政府提供更加智能、高效的数字化服务。

而在20年与黑产者激烈“拼杀”的过程中，通过用户举报、情报分析等，腾讯在安全领域积累了大量黑产数据。依托这些海量安全数据，腾讯能够利用人工智能技术，通过态势感知等手段帮助企业做到主动安全防御。

比如，零售企业是众多羊毛党紧盯的目标，因为只靠薅企业做营销的羊毛，他们就能够获得一笔不错的收入。很多传统企业对此感到很是无奈，2000万的营销费用，有可能四分之一都到了羊毛党的手里。众多企业也一致表示，这种“人为刀俎，我为鱼肉”的感觉着实不好受。在这方面，腾讯有蒙牛、东鹏特饮等大量的客户服务案例和实践，帮助他们杜绝了近千万资金流入到羊毛党的口袋中。

从QQ圈占用户、再到如今服务企业级用户，安全能力始终是腾讯最底层的核心实力。那么，凭借腾讯的原生安全理念，以及在人才、技术、生态等方面的协同“组合拳”，在高速发展的云计算市场，会催化怎样的变量？或许，只有时间才能告诉我们最后的答案。

— 【 THE END 】 —

往期精彩文章回顾：

| 支付宝集五福活动火爆，微信坐不住了，下手真快！

| “日本王思聪”在线征集女友，要求20岁以上爱好世界和平，将一起环月旅行

| 支付宝“集五福”正式上线，已有超30万人集齐福卡，终极大奖48888元！