勒索病毒盯上了二维码支付

12月4日，信息安全公司火绒在“火绒安全实验室”公众号发布消息称，12月1日爆发的“微信支付”勒索病毒正在快速传播，感染的电脑数量越来越多。腾讯方面4日回应称，微信已第一时间对所涉勒索病毒作者账户进行封禁、收款二维码予以紧急冻结，目前腾讯电脑管家已完成病毒破解。支付宝方面表示，有针对性的防护，目前未收到账户受影响的用户反馈。

腾讯电脑管家技术专家李铁军介绍称，目前上述病毒的全网“中毒”用户近两万人，支付的赎金额为110元/人，尚不清楚病毒作者具体获得的总赎金金额，但由于安全厂商的解密方案是免费的，作者获得的总体赎金应该不高。

全网“中毒”用户近两万人

据腾讯方面介绍，他们从12月1日开始接到用户的“中毒”反馈。这种勒索病毒感染系统后，会加密txt、office文档等有价值数据，并在桌面释放一个“你的电脑文件已被加密，点此解密”的快捷方式。点击后弹出解密教程和收款二维码，强迫受害用户通过手机转账缴付解密酬金。

“这款名为Bcrypt的病毒首先攻击的是软件开发者的电脑，导致开发者使用某工具编程的软件均带毒。用户下载这些‘带毒’软件后电脑就会被感染。病毒能获取键盘记录，这样当用户在各种平台上输入账号、密码时，便会泄露给病毒作者。”支付宝方面在12月4日介绍了该病毒的传播方式。

腾讯电脑管家技术专家李铁军进一步介绍称，上述勒索病毒的传播源是一款叫“账号操作V3.1”的易语言软件（病毒传播者还利用了其他一些类似的黑灰产工具），其声称的主要功能是可以登录多个聊天账户切换管理。该工具为灰色产业开发人群使用的工具，这部分人群使用的工具有许多会被杀毒软件查杀，他们常常会无视杀毒软件的拦截提示。因而，这个勒索病毒针对灰产从业者的定向传播十分奏效。

“火绒安全实验室”在12月1日发布的微信文章中写到，通过勒索病毒的界面信息都是中文可以推测，病毒或为国人制作，并使用不匿名的微信收取赎金，行为十分猖獗。

李铁军向记者表示，目前，上述病毒的全网“中毒”用户近两万人，支付的赎金额为110元/人，尚不清楚病毒作者具体获得的总赎金金额，但由于安全厂商的解密方案是免费的，作者获得的总体赎金应该不高。

微信封禁账户，支付宝称未收用户反馈

上述勒索病毒的扩散逐渐引起关注，微信和支付宝也在昨日披露了相关情况和举措。

腾讯方面介绍称，微信已在第一时间对所涉勒索病毒作者账户进行封禁、收款二维码予以紧急冻结。“微信对任何形式的网络黑产犯罪‘零容忍’，我们一直在持续打击网络黑产，实现了全链条精确打击。微信会通过后台风控策略对高风险交易场景进行提醒和确认，以保护好用户支付和财产安全。”

“我们也提醒广大用户，该勒索病毒可能通过任何形式的支付方式索要转账，若遭遇勒索，不要付款，及时报警。同时，腾讯电脑管家提供解密工具和人工服务，协助用户处理相关情况。”腾讯方面表示。

支付宝是否也受到该勒索病毒的波及？昨日，支付宝安全团队在相关情况介绍中称，目前未收到支付宝账户受影响的用户反馈。“针对此类风险，支付宝风控系统早有针对性的防护，包括二次校验短信校验码、人脸识别等。即便泄露密码，也能最大程度确保账户安全”。

腾讯方面向记者透露，目前腾讯电脑管家已完成病毒破解，并连夜发布本地解密工具测试版，同时结合腾讯电脑管家内置的勒索病毒行为拦截功能、文档守护者功能。腾讯电脑管家现已推出三重安全防御体系，做到事前备份、事中拦截、事后破解，最大限度帮助已中招的网友查杀病毒并修复被加密破坏的文件。腾讯电脑管家还为未安装电脑管家的“中毒”用户，提供了解密工具。

分析

互联网勒索病毒攻击特定人群，水平不高但影响大

在此次勒索病毒Bcrypt出现之前，比特币勒索病毒“WannaCry”也曾引起广泛的关注。2017年5月12日晚间，全球近100个国家的微软系统计算机同时遭到名为WannaCry（想哭吗）或Wanna Decryptor（想解锁吗）的电脑病毒袭击。想要被感染病毒的计算机解除锁定，只能向对方支付所要求的比特币，否则硬盘将被彻底清空。该勒索病毒的前身，是之前泄露的NSA黑客武器库中的“永恒之蓝”攻击程序。

火绒安全实验室曾表示，Bcrypt病毒为新型勒索病毒，入侵电脑运行后，会加密用户文件，但不收取比特币，而是要求受害者扫描弹出的微信二维码支付110元赎金，获得解密钥匙，这也是国内首次出现要求微信支付赎金的勒索病毒。

“互联网领域，这几年勒索病毒的数量增长比较快，很多勒索病毒的水平不是很高，但是影响会比较大”，李铁军对新京报记者称。但他表示，病毒攻击特定人群，应该不会大规模扩散，这个病毒没有自扩散能力。

本报综合消息

200元就可买陌陌2600万条信息？
数据安全需各方“协同联动”

2600万条陌陌数据库出售，售价仅200元人民币？近日有爆料显示，在网上有约2600万陌陌数据出售，包括用户的手机号和密码，来源是3年前撞库。不过经验证，这组数据中的密码并不正确，一些手机号不存在。

事件

3年前撞库数据再度被出售

据微博博主lxghost透露，陌陌的约3000万条数据在暗网出售，有多个卖家都有相关资源，价格仅为200元，但不保证数据的有效性。

一个约2600万条的在售数据包括手机号和密码。据卖家介绍，这批数据的来源是3年前撞库而来。数据规模总共3161万行，包括手机号加密码或者仅手机号，其中含密码的数据是2592万行。

卖家还特别警告称，“本人未有大批测试能力，故无法确保数据能登录陌陌或者可搜索到陌陌账号的概率，这一点敬请谅解。”

截图显示，这些陌陌账号和密码被整理成一个GVIM文档，在截图的20个手机号码中，仅有3条无对应密码，其余在手机号后都标有密码。

另一个3000万条数据库的介绍显示，这批数据是2015年7月17日被写入的，总条数3161万条，包含的字段有手机号和密码。卖家介绍称，“数据中密码有空白项，但这部分所占比例不到1%，就算去掉100万条，还有3000万条。”并申明：“本数据不保障现时有效性，只适合撞库等用”。

验证

密码不正确或陌陌号不存在

不过据验证，这些数据的有效性存在很大问题，记者随机验证了几个账号发现，多个账号显示“该陌陌号不存在”，还有的显示“账号或密码错误”。

例如数据中的136xxxx9535，在登录时显示“用户名或密码错误，是否找回密码？”在找回密码时则需要通过手机号码进行验证，他人无法直接进行登录；而152xxxx0634则显示“该陌陌号不存在”，说明数据库数据存伪。

为何会有密码错误或账号不存在的问题？据猜测，一种可能是因为数据库本身有问题，由于暗网是一个匿名网站，上面的数据可能存在捏造等情况，而这些数据是用于出售的，因此很可能是有人捏造数据库而骗取钱财；另一种可能是，三年前存在类似数据库，但陌陌方面已经进行一些措施，提示用户修改密码或在此期间部分用户注销等，目前来看这批数据的利用价值已经不大。

追访

数据库泄露事件缘何时有发生

在信息化、数据化的今天，数据泄露事件并非个案。11月30日，万豪酒店集团披露，旗下喜达屋酒店的一个顾客预订数据库遭到入侵，有约5亿顾客的信息可能遭到泄露。被泄露的信息包括姓名、生日、电话号码、护照号码甚至包括支付卡号码及有效日期。

据业内人士介绍，万豪事件是被“拖库”了，在黑客术语里面，“拖库”是指黑客入侵有价值的网站，把注册用户的资料数据库全部盗走的行为。而陌陌事件中提到的“撞库”，是黑客将一个网站的数据库尝试在其他网站进行登录，由于很多用户喜欢使用相同的用户名和密码，黑客就可以用之前的数据库登录新的网站，盗取用户在新网站的财产和资料。

“用户要避免在不同的网站使用相同的用户名和密码，以避免被撞库”，一位安全专家表示，“当然，贩卖和购买公民信息是违法的，这些售卖和购买数据库的网友也将承担相应的法律责任。”大安全时代，数据泄露事件并不是单一厂商的密码泄露，而是一直以来或明或暗的安全事件——个人、信息安全行业、公司实体都无法置身事外，需要建立一个协同联动的机制和体系。

一份汇总分析了84个国家的《2017年的数据泄露调查报告》显示，数据泄露原因方面，62%的数据泄露与黑客攻击有关；81%的数据泄露涉及到撞库或弱口令。导致数据泄露的主要手段分为技术手段（黑客入侵、软件漏洞、恶意木马）、非技术手段（内部人员泄密、非有意识泄密）。

最新消息

陌陌回应：他人无法仅凭手机号和密码登录用户账号

近日，陌陌公开回应了关于用户数据安全一事。

陌陌称本着对用户数据和隐私安全负责的态度，现就此事说明如下：第一，这个所谓的三年多前通过撞库得来的数据，跟陌陌用户的匹配度极低。多家媒体测试验证的情况显示，返回的也都是错误信息。第二，陌陌采用高强度单向散列算法（用户密码被单向加密成密文，但不能通过密文还原为明文）加密存储用户密码，因此任何人无法直接从陌陌数据库中直接获取用户明文密码。

陌陌最后表示，“请陌陌用户放心，陌陌采用包括密码验证、设备验证等多重校验机制，以保护用户信息安全，任何人在其他设备上仅用手机号和密码试图登录陌陌账号，都会触发短信验证码等多种信息验证措施，他人根本无法仅凭手机号和密码就登录用户陌陌账号。”

本报综合消息

11部门大战“僵尸企业”
以去产能化解债务

新华社北京12月5日电（记者 王璐）国家发展改革委、工业和信息化部、财政部等11个部门4日联合发布《关于进一步做好“僵尸企业”及去产能企业债务处置工作的通知》，要求尚未确定过“僵尸企业”和去产能企业债务处置名单的地方各级人民政府、各级相关国有资产管理部门，应在本通知发布后三个月内确定首批名单。要合理安排确定后续处置企业名单，原则上应在2020年底前完成全部处置工作。

通知明确，分类处置“僵尸企业”和去产能企业的直接债务，提出要完善政策与制度环境，加大对兼并重组的金融支持，鼓励金融机构在依法合规和风险可控的前提下提供发放并购贷款，支持符合条件的企业发行并购票据和引入并购基金。

自2016年供给侧结构性改革大幕开启至今，大部分行业去产能进程已经接近尾声。新时代证券首席经济学家潘向东认为，剩下的无效产能多集中在“僵尸企业”，由于目前的制度安排，有一些“僵尸企业”没有得到很好的处置。记者也了解到，去产能企业负债水平处于高位，偿债压力较大，而且债务构成复杂，处置成为棘手问题，进展较慢。

根据通知要求，要积极稳妥处置“僵尸企业”和去产能企业债务，加快“僵尸企业”出清，有效防范化解企业债务风险，助推经济提质增效。其中，由“僵尸企业”和去产能企业法人单位作为借贷主体、债权债务关系清晰的债务被归为直接债务，处置方式是依据营业价值、债务清偿能力、资产负债状况等因素，按照相关法规，分别采取破产清算、破产重整、债务重组、兼并重组等方式分类处置。

针对由企业集团作为借贷主体统借统还实际用于“僵尸企业”和退出的合法合规在籍产能项目债务，通知要求，允许相关企业和债权人自主协商一致后清分“僵尸企业”和去产能企业统借债务并纳入直接债务处置。此外，自主协商处置“僵尸企业”和去产能企业的担保债务，可按照产能占比等因素予以部分解除。

此外，一些制度梗阻也将被打破。通知明确，可积极利用产权交易所、租赁、资产证券化等多方式充分盘活“僵尸企业”及去产能企业有效资产，用于清偿债务。