信息泄露：2018年企业信息安全头号威胁

腾讯安全

目录

一、 概述

2017 年 6 月 1 日《网络安全法》正式实施，从法律层面积极推进了网络安全工作，是保障网民个人信息安全的法律武器。同时对企业而言，数据资产的重要性不仅仅体现在经济层面，还要对关键信息基础设施及其重要数据担负一定的法律责任。然而在暗处总有一些人在利益的驱使下伺机而动，窃取数据，谋取私利。

过去的一年，以比特币、门罗币、以太坊币为代表的虚拟数字加密币日益普及，这些虚拟加密币对网络安全生态产生极大影响：各种非法交易使用虚拟加密币完成，一方面使得交易更加直接简单，减少变现中间环节，使非法交易更加隐蔽。另一方面也使执法部门的查处难度大大增强，一定程度上对非法数据买卖、病毒制造传播等黑色产业起到助推器的作用。

回看 2018 年，数据泄露事件频发，某平价连锁酒店集团 5 亿条信息数据、快递订单数据、某高端星级酒店数据、学生信息、大量银行卡身份证等个人敏感数据泄露或直接暗网黑市上公开贩卖。而这些个人信息泄露历来都是各类网络诈骗，尤其是精准诈骗实施的源头。

随着网络技术的发展，暴露在互联网的注册域名、线上主机、IP 网络、业务系统等互联网（外网）资产越来越多，相关的业务也越来越复杂，随之而来的网络安全威胁也越来越多，越来越复杂。互联网资产存在的安全漏洞、安全弱点等安全问题，已经逐渐成为网络安全威胁的重要因素。

本报告以企业暴露在外部的互联网资产角度，评估安全风险，同时通过在互联网、暗网等网络空间“插眼”从而以攻击者视角感知外部存在的风险情

况，并结合腾讯安全大数据及第三方授权或公开的信息和数据为基础，结合抽样分析/调查报告等方法，经综合整理、分析得出。其主要选取了信息化程度高，管理水平强的大中型企业指标数据作为参考对象，涵盖上千家企业网站和线上服务平台。

从报告阐述的问题来看，国内企业互联网资产仍然存在比较严重的已知安全问题，黑客入侵、信息泄露等安全问题对关键信息基础设施及其企业/个人的敏感信息的威胁不容忽视：

- 网络空间资产端口开放较多，隐患大，如开放高危端口的资产比例高达 36%；
- 服务器漏洞风险较大，仍有部分企业使用的服务软件/组件未升级到最新版本，如未及时修复基存在的漏洞，则极易遭受外部不法分子的攻击;
- 数据泄露风险事件频发，帐号/邮箱类信息等老数据以及网购/物流类数据等与个人息息相关的数据备受暗网等黑市交易平台青睐。

二、 企业互联网资产面临严峻安全考验

企业互联网外网资产的安全会影响到内网安全，黑客通过攻击外网服务器，获得成功之后，会以这些服务器为跳板，实现对企业内网的攻击和数据窃取。这也是黑客入侵企业内网最常用的套路。

另外一方面，通过钓鱼、挂马等传统攻击方式，实现对办公电脑的控制或数据洗劫，从而获取进入内网的入口信息（帐号、密码等），或者直接对有价值的办公网系统实施勒索等破坏性攻击。

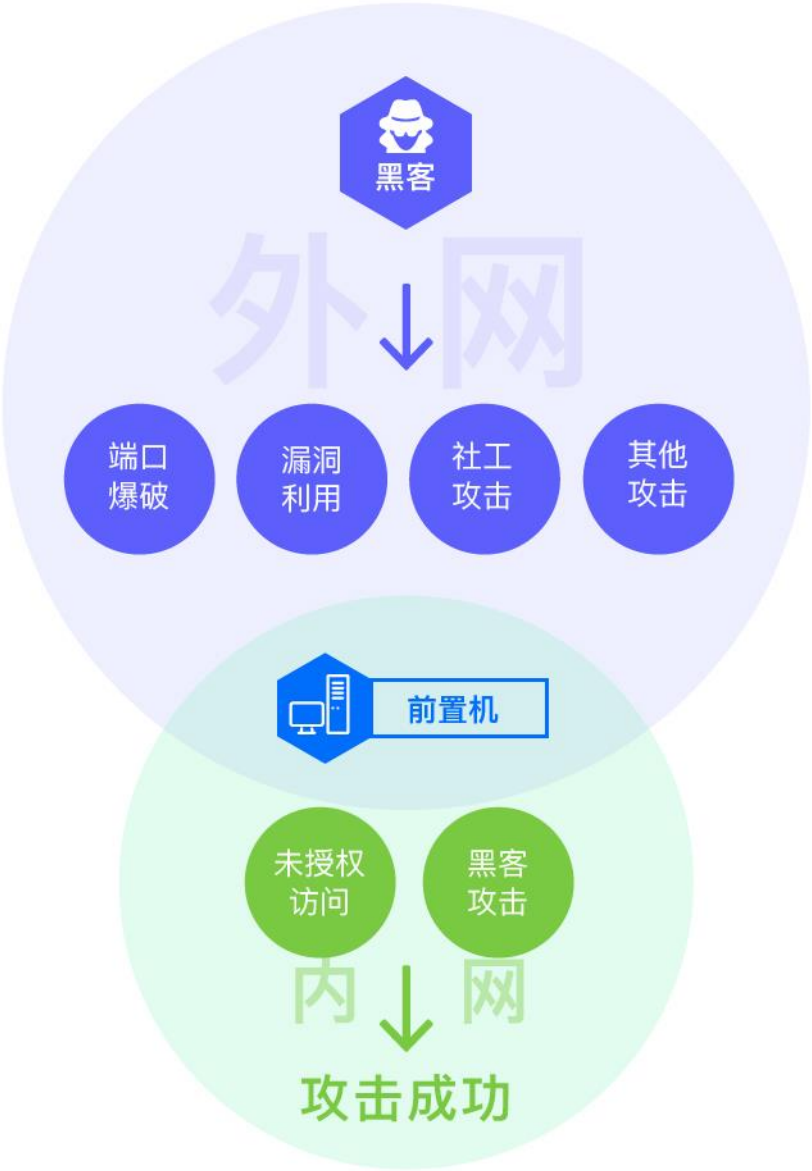


图 2_1：黑客攻击/入侵内网示意图

（一）网络空间资产端口开放较多，隐患较大

1. 端口开放情况

网络空间的基础设施包含网站的服务器以及运行在服务器上的各种服务。网络空间的基础设施承载了包括网站、电子邮件、文件传输等各种网络通信功

能。他们在互联网上的机器语言表现形式是以基于 TCP 和 UDP 的各种端口的网络通信。

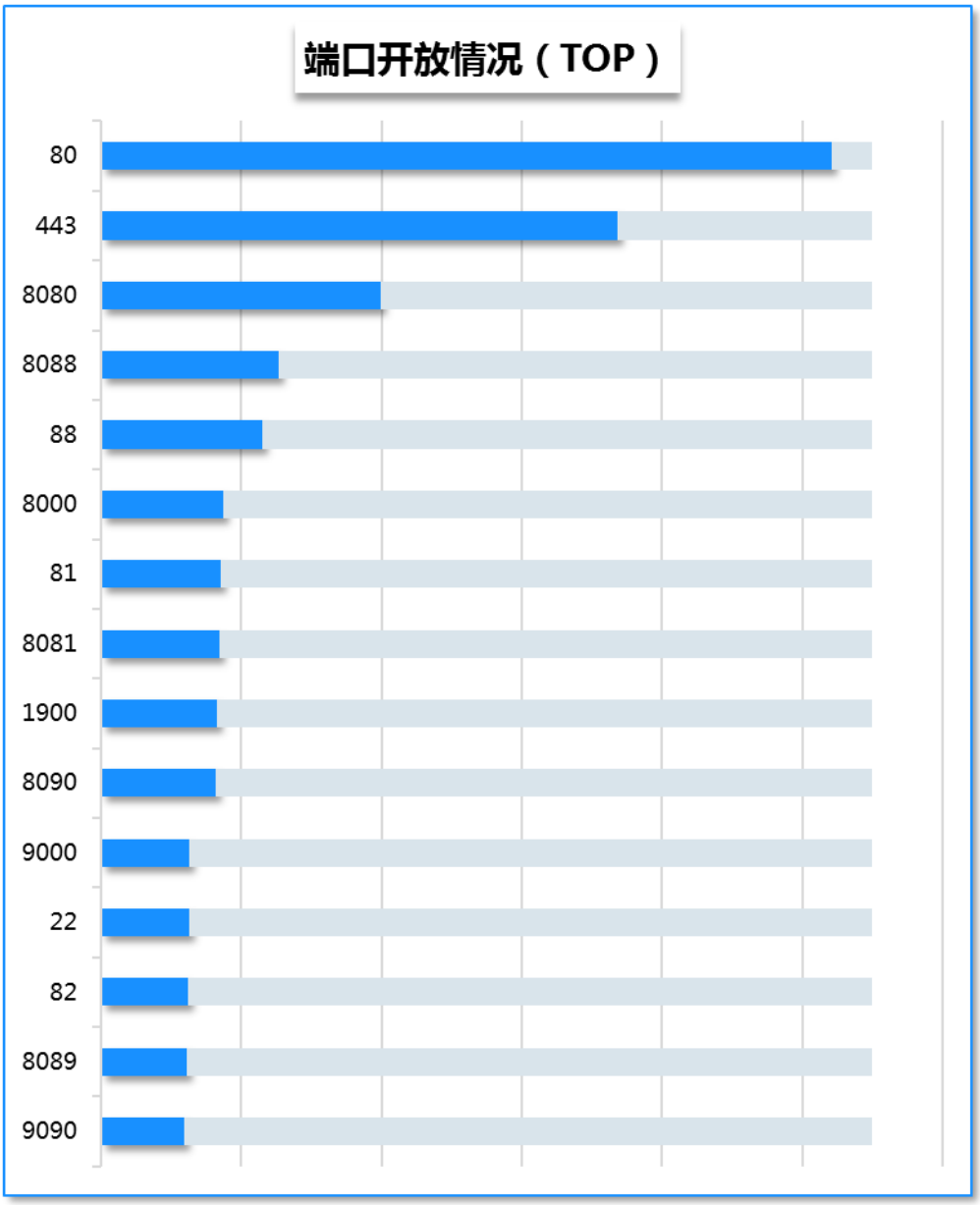


图 2_2：端口开放情况

由上图可以看到，80 端口的开放数量是排名第一位的，这与行业惯例会将 Web 服务(网站)开放在 80 端口是一致的。另外，我们看到 443 端口开放量也比较高，由于 443 端口常用于加密的 https 网站通信，说明相关的企事业单位在保护网络通信方面已经有了一定的成就。

2. 高危端口开放情况

我们将最近几年黑客攻击事件中出现频率较高的端口划为高危端口，并对 3000 多个抽样 WEB 服务器等互联网空间资产做了空间测绘，发现仍有 36%的资产开放着这些高危端口，存在较高的安全隐患。

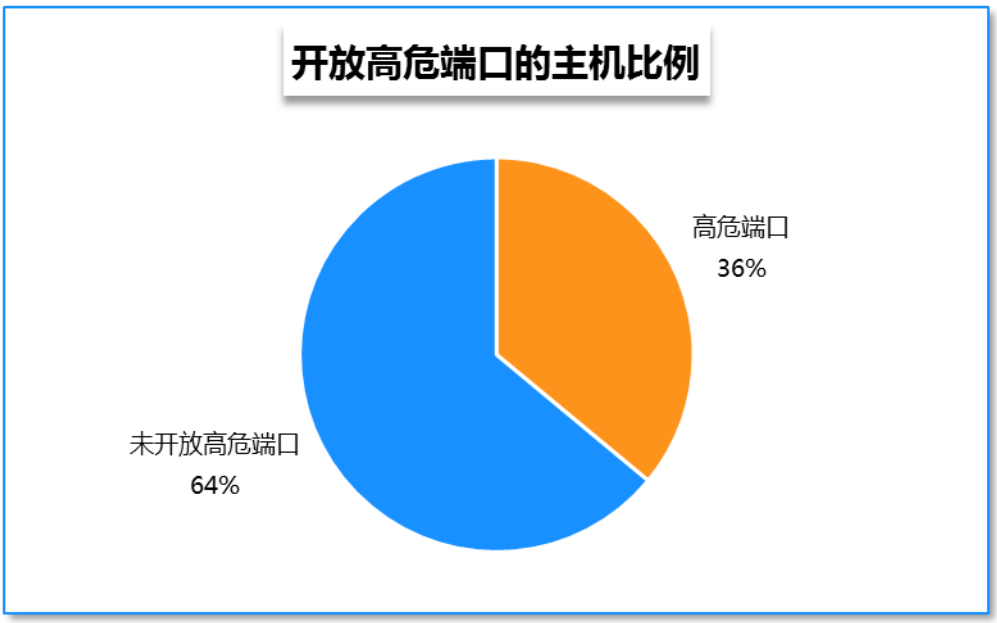


图 2_3：开放高危端口的主机比例

除了 22、1900 等端口之外，还有较大比重的邮件服务、数据库服务等端口暴露在公网上。

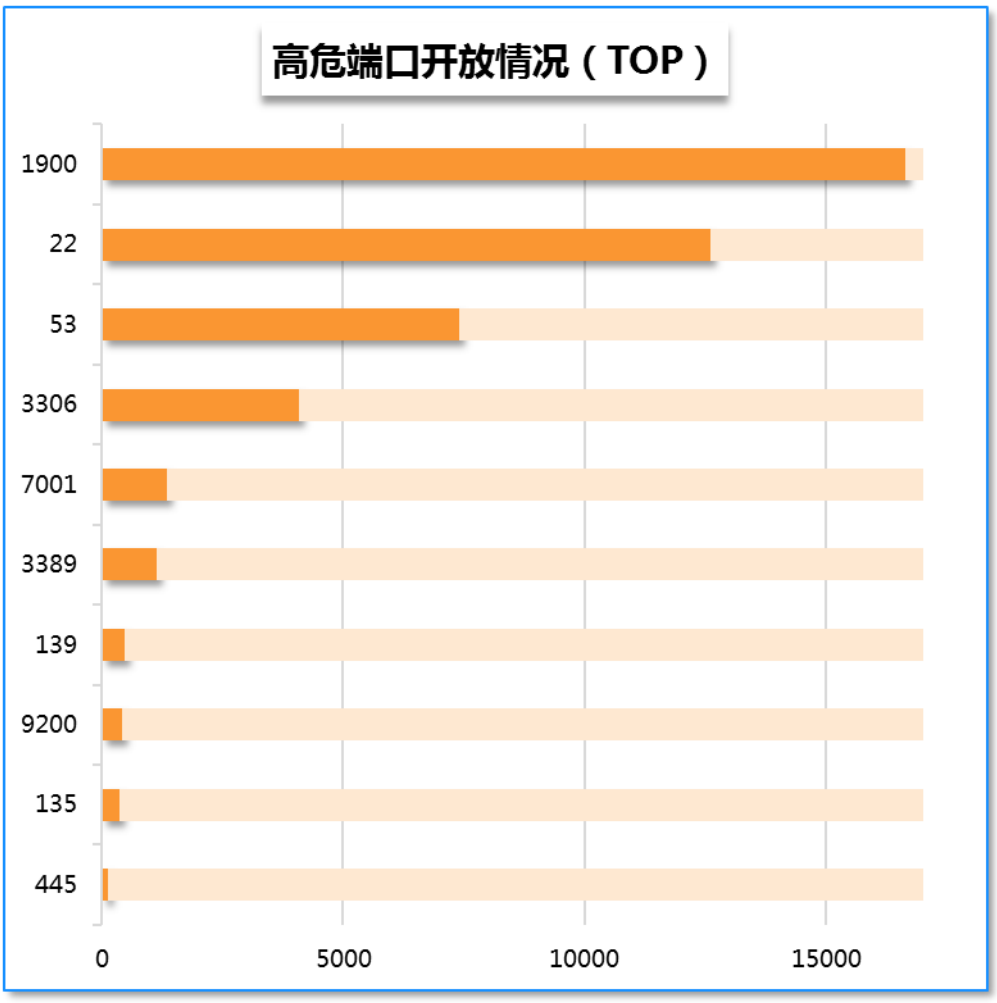


图 2_4：高危端口开放情况

22 端口常用于 Linux 平台的 SSH 远程连接服务，3389 端口常用于 Windows 系统的远程桌面连接。如果管理员使用的密码强度不够，黑客可以轻松的通过暴力破解直接登录网站服务器。

1900 UDP 端口 源于 SSDP Discovery Service 服务。通过使用 SSDP 协议对端口 1900 进行扫描可以发现 UPnP（即插即用协议）设备，攻击者可以利用这些设备发动 DDos 攻击，制造出大量流量，导致目标企业的网站和网络瘫痪。

7001 端口是 WebLogic 的默认端口，WebLogic 今年被爆出多个可被远程攻击的高危漏洞，如果漏洞未能及时修复，则不排除有远程攻击的可能。

3306 是 MySQL 数据库的默认端口，而数据库是几乎所有黑客都觊觎的东西，所以数据库系统直接暴露在外网是非常危险的行为，而使用默认端口的数据库暴露在外网会极大减低黑客攻击的难度，增加被攻击的风险。

数据库攻击者，除了窃取数据信息（拖库）之外，还可能针对数据库的数据实施经济勒索攻击。攻击者先将数据库进行备份，然后利用远程命令删除数据库从而实施勒索。最典型的勒索攻击莫过于 2017 年 5 月份爆发的 WannaCry，该病毒会对公网随机 IP 地址的 445 端口进行扫描感染。

根据测绘结果分析，仍有部分服务器资产开放了 445 端口。如果这些服务器没有打上相应的补丁，那么仍然存在被勒索病毒攻击的风险。即便是打上了补丁，也仍然需要面对勒索病毒变种的攻击。

（二）企业服务器需警惕安全漏洞威胁

基于 2018 年几个高危漏洞对应的服务软件/组件产品和影响版本号，我们比对了抽样企业服务器的相应的服务软件/组件产品和版本号，仍然有部分服务器使用的服务软件/组件的版本在几个高危漏洞受影响的范围内，如果这些漏洞未能及时修复，则不排除有远程攻击的可能。

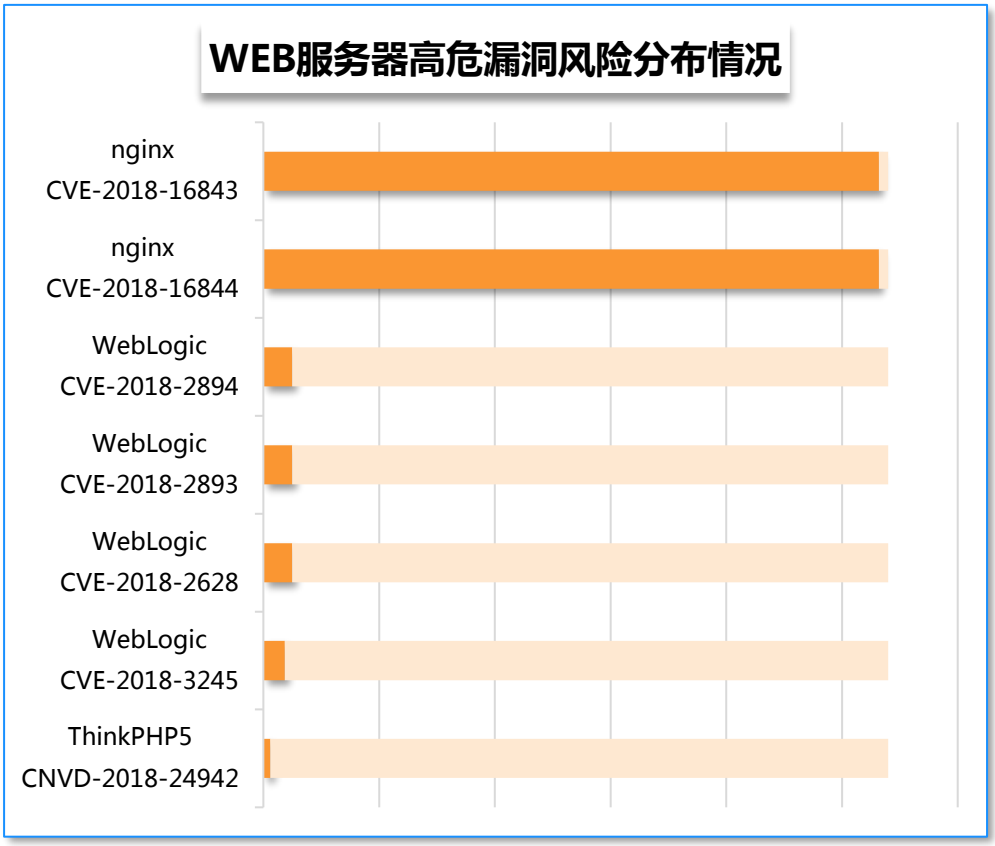


图 2_5：WEB 服务器高危漏洞风险分布情况

1. Nginx 漏洞（CVE-2018-16843，CVE-2018-16844）

2018 年 11 月 nginx 被爆出存在安全问题，有可能会致使 1400 多万台服务器易遭受 Dos 攻击。而导致安全问题的漏洞存在于 HTTP/2 和 MP4 模块中。

nginx Web 服务器于 11 月 6 日 发布了新版本 ，用于修复影响 1.15.6, 1.14.1 之前版本的多个安全问题，被发现的安全问题有一种这样的情况 ——允许潜在的攻击者触发拒绝服务（DoS）状态并访问敏感的信息。

2. WebLogic 反序列化漏洞

WebLogic 今年被爆出多个可被远程攻击的高危漏洞，如果漏洞未能及时修复，则不排除有远程攻击的可能。

- CVE-2018-2628

Oracle 官方发布的 4 月份的关键补丁更新 CPU（Critical Patch Update）中包含了一个 Weblogic 反序列化漏洞，可导致远程代码执行漏洞。漏洞威胁等级为高危，对应的 CVE 编号为 CVE-2018-2628。

漏洞影响版本：10.3.6.0， 12.2.1.2， 12.2.1.3， 12.1.3.0

- CVE-2018-2893

Oracle 官方在 2018 年 7 月发布的关键补丁更新中包含了 Oracle WebLogic Server 的一个高危的 WebLogic 反序列化漏洞 CVE-2018-2893 ,通过该漏洞，攻击者可以在未授权的情况下远程执行代码。

此漏洞产生于 WebLogic T3 服务，当开放 WebLogic 控制台端口（默认为 7001 端口）时，T3 服务会默认开启，因此会造成较大影响。结合曾经爆出的 WebLogic WLS 组件漏洞，不排除会有攻击者利用漏洞挖矿的可能，因此，建议受影响企业用户尽快部署防护措施。

漏洞影响版本：10.3.6.0， 12.2.1.2， 12.2.1.3， 12.1.3.0

- CVE-2018-3245

攻击者可利用这些漏洞在未授权的情况下发送攻击数据，通过 T3 协议在 WebLogic Server 中执行反序列化操作,最终实现远程代码执行。

漏洞影响版本：10.3.6.0, 12.2.1.3，12.1.3.0

- WebLogic 任意文件上传漏洞(CVE-2018-2894)

基于 JavaEE 结构的中间件 WebLogic 产品存在一个远程上传漏洞，攻击者利用这个漏洞，可上传恶意脚本文件，在被攻击 Weblogic 服务器上执行任意代码。

漏洞影响版本：10.3.6.0, 12.1.3.0, 12.2.1.2, 12.2.1.3

- ThinkPHP5 远程代码执行高危漏洞(CNVD-2018-24942)

ThinkPHP 官方 12 月安全更新中公告了一个远程命令执行的高危漏洞(CNVD-2018-24942)，该漏洞主要因为 php 代码中 route/dispatch 模块没有对 URL 中的恶意命令进行过滤导致，在没有开启强制路由的情况下，能够造成远程命令执行，包括执行 shell 命令，调用 php 函数，写入 webshell 等。

漏洞影响版本：5.x < 5.1.31， 5.x <= 5.0.23

三、 现实案例：脆弱的外网资产或致敏感数据泄露

暴露在外网中的互联网资产存在的业务漏洞、敏感端口开放等安全问题，会给未授权访问和黑客入侵渗透带来极大的便利，从而增加数据泄露的风险。

眼观全球，黑客攻击造成的的信息泄露事件仍然频发。过去的 2018 年，单次泄露数据大于 500 条的数据泄露事件就发生了数百起，几乎每个月都会发生数起重大数据泄露事件，涉及互联网、酒店、物流等多个行业企业。

（一）某快递企业数据泄露

6 月 19 日，一用户在暗网上开始兜售某快递公司的 10 亿条快递数据，该用户表示售卖的数据为 2014 年下旬的数据，数据信息包括寄(收)件人姓名，电话，地址等信息，10 亿条数据已经经过去重处理，数据重复率低于 20%，并以 1 比特币打包出售。

并且该用户还支持用户对数据真实性进行验货，但验货费用为 0.01 比特币(约合 431.98 元)，验货数据量为 100 万条。此验货数据是从 10 亿条数据里随机抽选的，每条数据完全不同，也就是说用户只要花 430 元人民币即可购买到 100 万条某快递公司的个人用户信息，而 10 亿条数据则需要 43197 元人民币。

（二）某平价连锁酒店信息泄露

某平价连锁酒店开房信息数据正在暗网出售，受到影响的酒店，包括HT酒店、MJ、XY、MX、NFT、MJ、CG、JZ、QJ、XC、YBS、YL、HY等等10余个连锁子品牌，泄露数据总数更是近 5亿!

从网络上流传的截图可以看出，黑客目前正在数据信息如下，有几大数字值得我们注意：

1. 该平价连锁酒店官网注册资料，包括姓名、手机号、邮箱、身份证号、登录密码等，共 53 G，大约1.23 亿条记录;

2. 酒店入住登记身份信息，包括姓名、身份证号、家庭住址、生日、内部 ID 号，共 22.3 G，约 1.3 亿人身份证信息;

3. 酒店开房记录，包括内部ID账号，同房间关联号、姓名、卡号、手机

号、邮箱、入住时间、离开时间、酒店ID账号、房间号、消费金额等，共66.2 G，约 2.4 亿条记录;

数据之齐全，令人咋舌。

发帖人声称，所有数据脱库时间是 8 月 14 日，每部分数据都提供 10000 条测试数据。所有数据打包售卖 8 比特币，按照当天汇率约约合 37 万人民币。而经过媒体报道之后，该发帖人称要减价至 1 比特币出售……

据研究人员表示，此次泄露的原因是华住公司程序员将数据库连接方式及密码上传到 GitHub 导致的。而数据库信息是20天前传到了Github上，而黑客拖库是在14天前，黑客很可能是利用此信息实施攻击并拖库.

信息化时代的今天，面对数据泄露事件的层出不穷，国家，企事业单位，个人都应提高对数据安全的重视，加强对自身数据的保护措施。

（三）某知名招聘网站信息被出售

2018 年 6 月 16 日，有人在暗网叫卖某招聘网站的用户信息，其中涉及 195 万用户的求职简历，随后官方强调，确认了部分用户帐号密码泄露源于被撞库而非拖库，而其中的大部分数据均在 2013 年以前注册，且来自于一些邮箱泄露的帐号密码。

（四）Facebook

2018 年 3 月，一家名为 Cambridge Analytica 的数据分析公司通过一个应用程序收集了 5000 万 Facebook 用户的个人信息，该应用程序详细描述了用户的个性、社交网络以及在平台上的参与度。尽管 Cambridge Analytica 公

司声称它只拥有 3000 万用户的信息，但经过 Facebook 的确认，最初的估计实际上很低。4 月，该公司通知了在其平台上的 8700 万名用户，他们的数据已经遭到泄露。

不幸的是，随着对 Facebook 应用程序更深入的审查，看起来 Cambridge Analytica 丑闻可能只是冰山一角。6 月 27 日，安全研究员 Inti DeCeukelaire 透露了另一个名为 Nametests.com 的应用程序，它已经暴露了超过 1.2 亿用户的信息。

（五）美国社交问答网站 Quora

当地时间 11 月 3 号，美国社交问答网站 Quora CEO 周一发表题为《Quora 安全更新》的博文称，其用户数据遭第三方未经授权恶意访问，包括用户帐户信息(姓名、电子邮件地址、加密后的密码等等)和其他私人信息（非匿名评论、回答等数据）等大约 1 亿 Quora 用户的信息可能已被泄露。

（六）某高端星级酒店集团数据泄露

某高端星级酒店集团 11 月 30 号天公布公告，称其旗下某子品牌酒店一个客房预订数据库遭黑客入侵，可能有约 5 亿顾客信息遭泄露，包括客户的姓名、地址、电话、邮箱、护照等，甚至还可能包括部分客户的支付卡号码和有效日期。万豪集团称，此次用户数据泄露事件仅与旗下四家子品牌酒店有关，而其他不使用同一系统的酒店未受影响。

四、 “暗流涌动”的黑市交易侵蚀数据安全

黑产从业者往往会利用一些平台泄露的帐号密码等信息通过撞库等手段，获取更多的用户信息从而实施变现。除了盗号、发广告、刷量（刷量、刷赞、刷粉、刷榜……）等直接变现之外，黑产从业者还会利用撞库攻击得到一些新的用户数据，然后通过大数据分析等技术手段，获得更丰富的用户信息，从而放到暗网等黑产平台继续售卖，不法分子通过购买得到数据，并利用这些数据进行精准诈骗、敲诈勒索等犯罪活动，或利用大量非法获取的个人信息去注册大量帐号方便进一步从事网络犯罪活动。

（一）暗网为个人信息贩卖的主要渠道

暗网，即“洋葱暗网”，简单理解就是一个互联网的“地下黑市”，它是美国军方出于政治目而进行研发和支持的一种隐蔽的网络，暗网论坛等一些暗网网站通过谷歌、百度等普通的搜索引擎是无法搜索到的，仅对于知道怎么打开它的人可见。

洋葱暗网在数据传输时会经过层层的洋葱路由，每个路由之间输出的信息都会进行一层加密，数据经由的每个节点恰似一层层的洋葱皮，故名洋葱网络（Tor），同时洋葱网络的数据会通过层层的“洋葱皮”进行“接力”传输，数据接收者只能看到上一层“洋葱皮”的“接力”传输者，而不能看到首位发送者，从而实现了互联网的匿名交流和沟通。

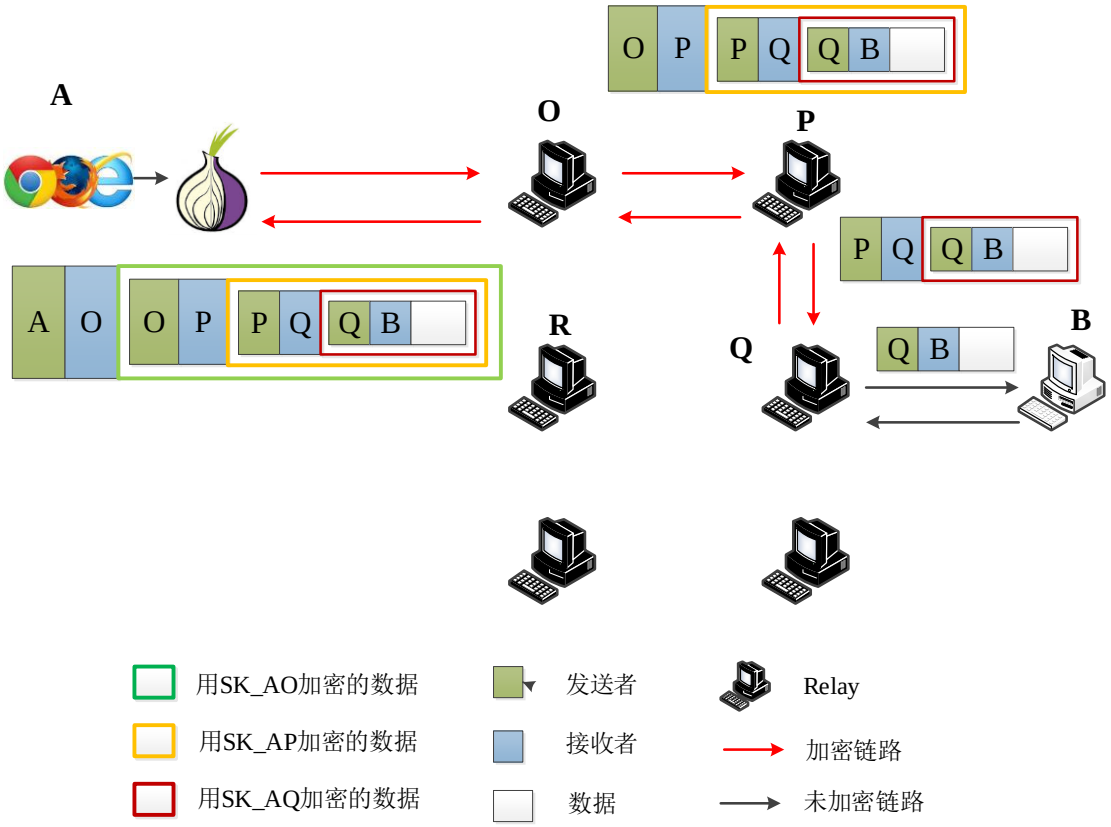


图 4_1：Tor 网络访问网络示意图

1. 暗网的数据交易情况

然而暗网带来更多的却是违法犯罪行为的传播,人性的丑陋和罪恶尽在其中，暗网网络中充满了犯罪、黄暴血腥画面。同时比特币的发明，又助推了暗网的发展，几乎所有的黑市都使用比特币进行匿名交易，这也导致了用于网络诈骗、定向攻击的个人隐私数据也越来越多的被“明码标价”挂售。

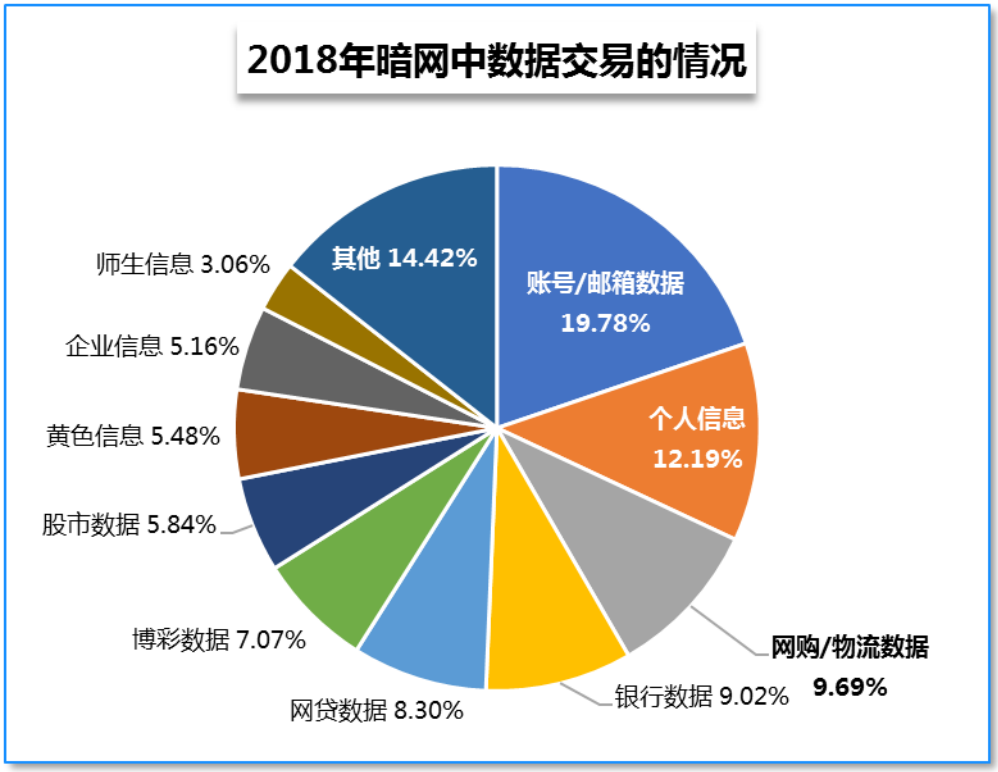


图 4_2：2018 年暗网中数据交易的情况

从 2018 年暗网数据交易的情况（抽样数据）来看帐号/邮箱类数据、个人信息（身份证、通信/通讯类信息）、网购/物流数据是主要是数据卖点，撞库、拖库等手段对个人信息进行裂变式扩散以及精准电信诈骗等活动的需求推动了数据交易的需求，另外这也与今年酒店、物流等行业暴露的数据泄露信息有一定的关联。

除此之外，银行数据和网贷数据等金融数据在今年下半年开始增多，可能与今年爆雷的 P2P 等金融平台相关。

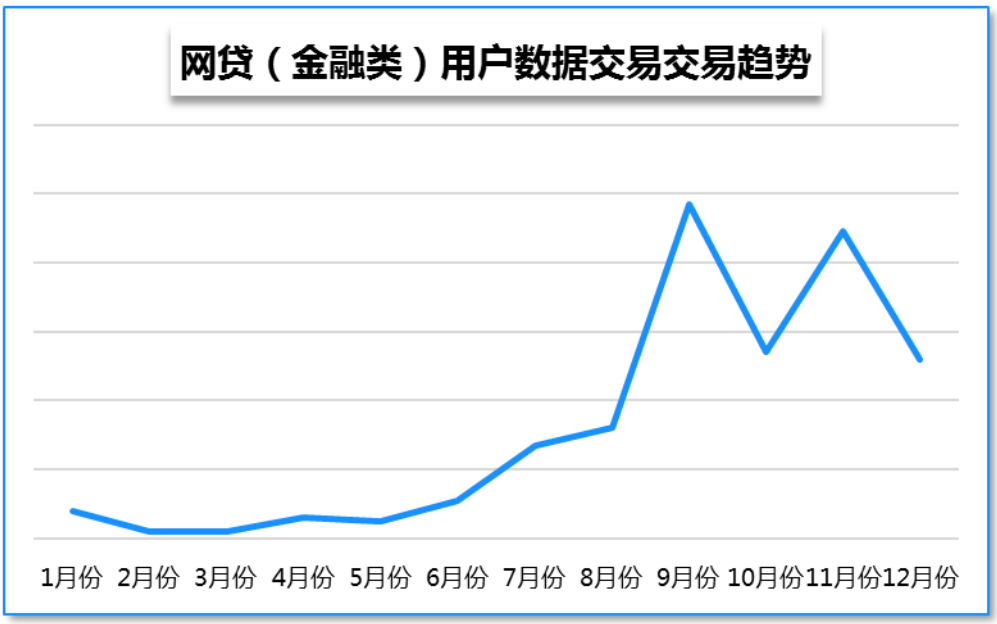


图 4_3：网贷（金融类）用户数据交易交易趋势

2. 典型的数据交易案例

某平价连锁酒店集团 5 亿条信息数据、浙江学生学籍、母婴数据信息、快递订单数据等等公民个人信息交易帖层出不穷。黑产从业者除了利用技术攻击、钓鱼攻击和勾结内鬼等手段获取这些一手信息资料之外，撞库攻击也是其获得用户隐私数据的主要方式。暗网中兜售的帐号密码类信息，为撞库攻击提供了第一手资料。

图 4-4 暗网贩卖快递实时订单的帖子截图

2018 年-12 月-30 日 凌晨 01:55，暗网中文论坛出现一个帖子，声称售卖 30 万某酒店的数据，内含身份证、住址、电话等用户敏感信息，叫价 0.00268 比特币，约合人民币 69 元，从数据的时间来看，疑似一份 2012 年的老数据。该酒店成立于 2010 年，旗下拥有 3400 多家分店，会员数据超 4400 万，主要分布在二三线城市。

图 4_5：某酒店数据在暗网中贩卖截图

另外暗网“数据-情报类”版块中，有很多邮箱帐号类信息被挂出来贩卖。暗网一交易帖子号称所贩卖的数据包含了 16 亿邮箱+密码数据，涵盖了国内各大互联网平台。从成交量来看，已经成交了 38 单，另外从商品单价来看售价 0.0005 比特币，价值 3.25 美元（约合人民币 22 元），低廉的售价不难看出这份数据应该是一份老数据。

图 4-6 暗网中贩卖 16 亿邮件帐号数据的帖子截图

一贩卖某邮箱帐号数据的帖子号称包括了该平台 52G 的帐号+密码数据，该批帐号信息泄露的时间最早可以追溯到 2015 年。

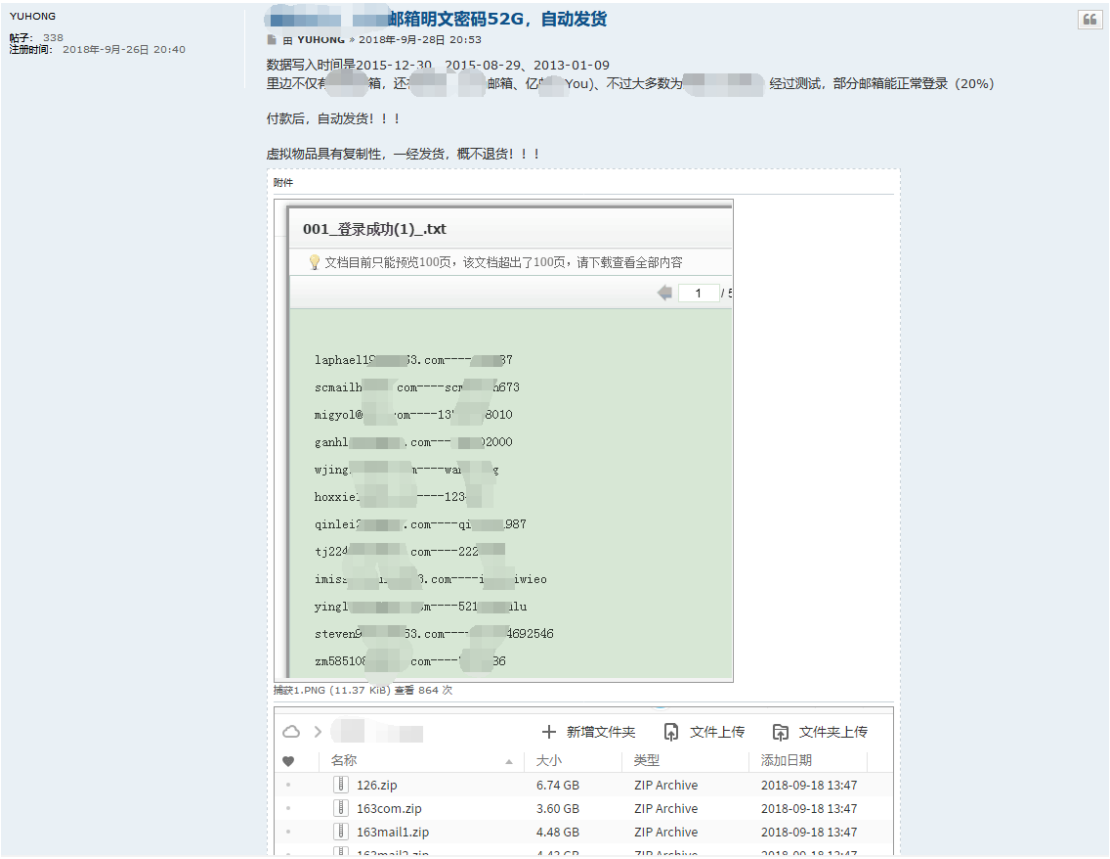


图 4-7 暗网中贩卖某邮件帐号数据的帖子截图

（二）详细的个人信息催生精准诈骗

通过大数据分析等技术，黑产从业者可以将不平台获得的用户信息进行关联分析，从而精准的做出用户画像，比如用户住哪里、去过哪里旅游、住过哪些酒店、购买过什么物品等等。然后再通过暗网等交易平台贩卖给电信诈骗者。

诈骗者通过暗网等黑产平台获得用户的个人详细信息后，就会通过手机、电脑等终端对受害者实施针对性的电信诈骗。“购物退款”、冒充“公检法”、“发放助学金”、“航班取消”、“二胎生育退费”、“交通违章提醒”、“积分兑换现金”等等精准诈骗，均是诈骗者基于个人信息特点精心设计的具有针对性的诈骗剧本。

1.“购物退款”诈骗

购物者在网购平台购物完成之后，会收到热心“客服”的电话，“客服”会以质量问题、物流问题等事由，通过核对购买物品的信息和受害者个人信息，并强调要退款给受害者等话术，从而骗取受害者的信任，然后实施诈骗。

一般情况下，“客服”会发送给受害者一个所谓的退款网页链接或二维码，受害者进去之后按照提示操作，就会收到高于购物款的退款或退款保证金，之后“客服”会进一步引导受害者将多收到的退款或退款保证金通过扫描指定二维码的方式退还给网店。

在这个过程中，受害者收到的款项其实是一些正规的贷款平台的快速贷款，诈骗者利用网银或第三方支付平台上快速授信贷款等服务，误导受害者从贷款平台贷款，然后将“多余”的款项打回（骗回）诈骗者的网络帐户。

“购物退款”诈骗作案流程示意图

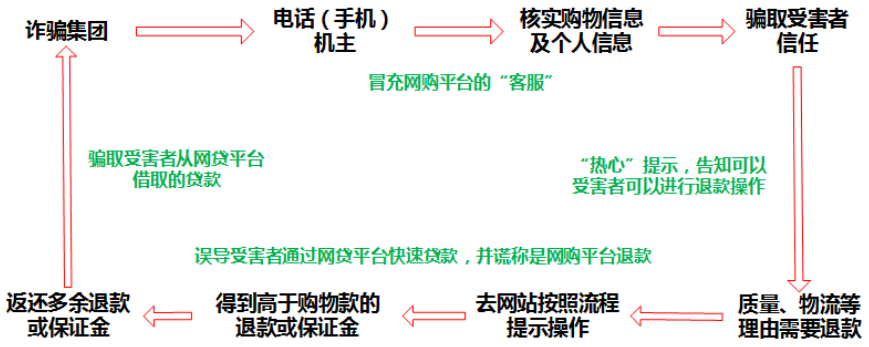


图 4-8 “购物退款”诈骗作案流程示意图

2. 冒充“公检法”诈骗

一般情况下诈骗者会告知受害者涉嫌洗黑钱或快递包裹被查禁等违法犯罪行为，同时会引导受害者登录一个假的《中华人民共和国最高人民检察院》的网站对自己的“犯罪记录”进行查询和澄清登记，继而骗取用户的银行卡以及个人敏感信息，并“好心”引导受害者下载一款名为《检察院安全控件》的软

件，该软件是款定制版的远程控制终端，骗子通过该终端并利用已经骗取的银行卡等信息远程操控受害者的电脑上，将受害者网上银行能够转走的钱洗劫一空。

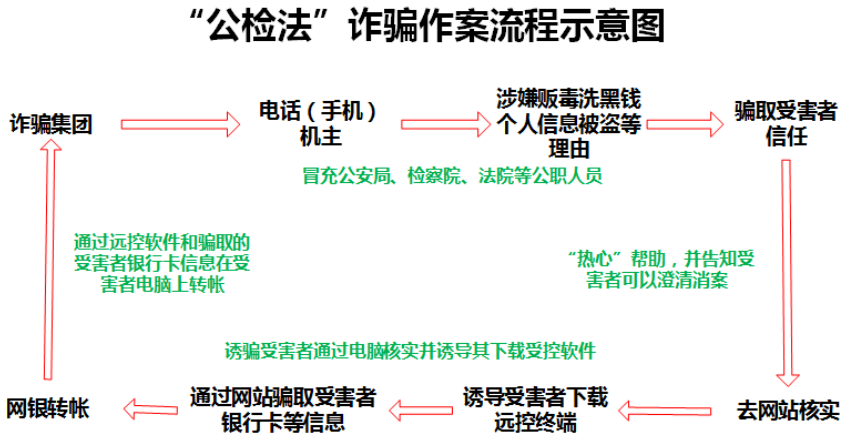


图 4-9 冒充“公检法”诈骗作案流程示意图

上述的诈骗流程和主要方法多年来没有太大的变化。与以往不同的是，随着反诈骗宣传力度的不断增强、反诈骗意识的不断提升，诈骗对象从普撒网式的人群转变为了特定、精准人群诈骗，用户的详细信息一旦被泄露，落入诈骗者手中，就很容易被诈骗“瞄准打击”从而实施精准诈骗。诈骗者不但知道受害者的基本信息，还能知道受害者的职业、爱好以及最近关注的事物、当前的状态等等信息，甚至在有些方面的信息，诈骗者比受害者还了解其自身的情况。

（三）撞库攻击催化信息泄露裂变式增长

全球恶意登录的次数在不断增加，情况不容乐观。据国外某安全研究团队撰写的《2018 年互联网安全状况报告：撞库攻击》，仅在 2016 年 11 月到 2017 年 6 月末期间，全球恶意登录尝试就超过 300 亿次。而恶意登录尝试多

数是撞库攻击，撞库攻击简单理解就是拿 A 网站的帐号密码，去 B 网站上尝试登陆。

由于很多用户喜欢在不同的平台使用统一的帐号密码，导致了以撞库攻击造成的数据泄露可以像裂变原子一样呈指数级增长。

从近三个月的蜜罐流量可以看到，恶意攻击的流量稳中有长，而这些恶意攻击流量当中更多是一些撞库和扫号攻击。

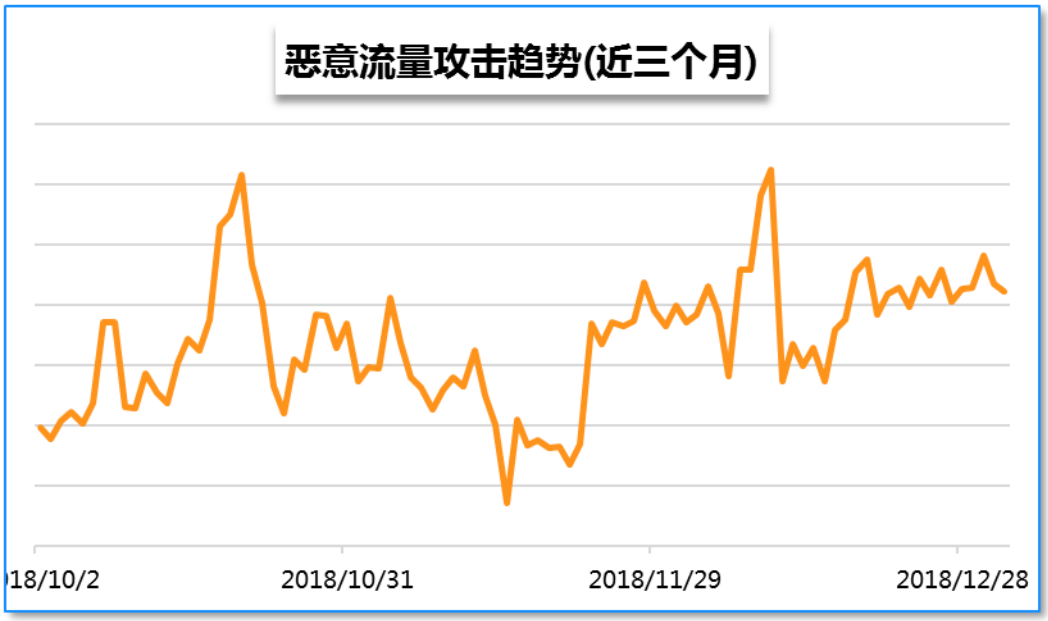


图 4-10 恶意流量攻击趋势(近三个月)

基于抽样的蜜罐流量数据，可以看到，黑产从业者仅通过某网络平台的一登录入口就有约 100 万/天的撞库攻击量，其中超过一半的请求被平台主动拦截。

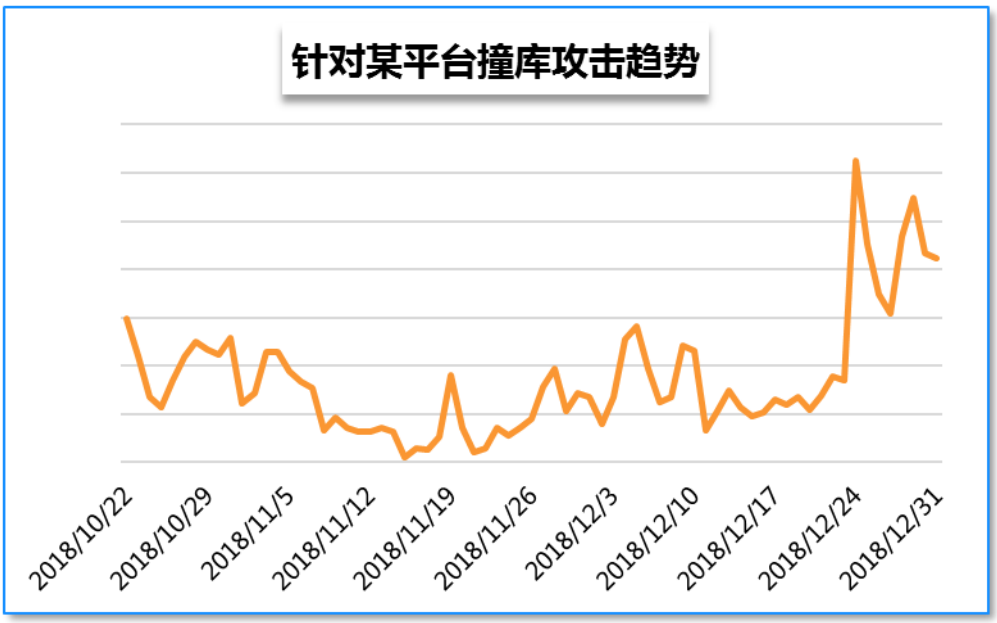


图 4-11 针对某平台撞库攻击趋势

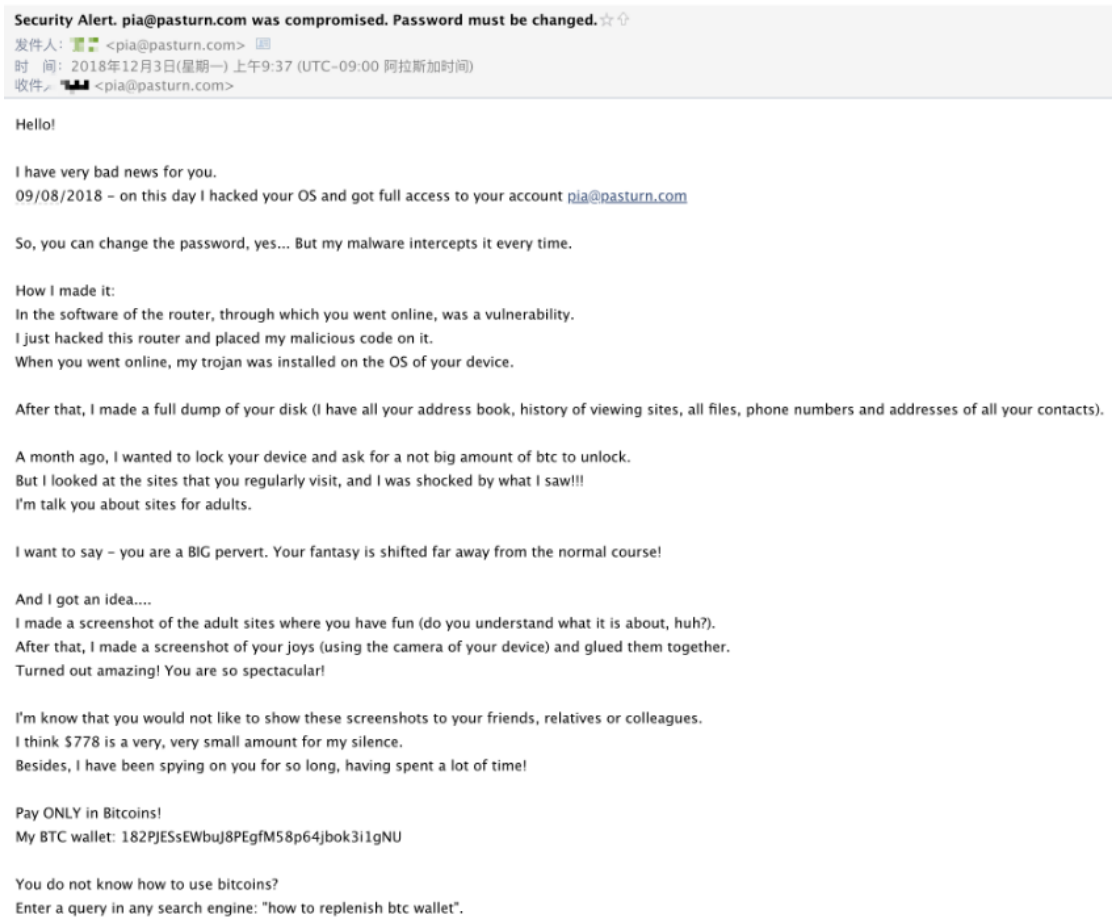
被平台拦截的撞库请求大约占总量的 55%，其中有 52%的请求被认为为异常 IP 被直接封禁了 IP，另外 3%的请求被检测出了登录风险，从而通过验证码进行拦截。

值得关注的是撞库成功的账号约为 23%左右，按照每天 100 万条撞库账号预估，每天约有 23 万账户被撞库成功。

（四）海量的信息泄露滋生了撒网式诈骗

除了用来撞库和精准诈骗之外，这些泄露的数据还被用来做撒网式诈骗。

前一段一些网友纷纷发帖，称自己从“黑客”手里收到了恐吓邮件，邮件里称在其访问成人网站植入了恶意程序，能盗取用户帐号密码，并控制摄像头录制用户观看成人视频的隐私过程，以此要求支付指定赎金，否则向邮箱里的所有联系人发送视频文件。



Security Alert. pia@pasturn.com was compromised. Password must be changed. ☆☆

发件人: [redacted] <pia@pasturn.com>
时　间: 2018年12月3日(星期一) 上午9:37 (UTC-09:00 阿拉斯加时间)
收件人: [redacted] <pia@pasturn.com>

Hello!

I have very bad news for you.
09/08/2018 – on this day I hacked your OS and got full access to your account pia@pasturn.com

So, you can change the password, yes... But my malware intercepts it every time.

How I made it:
In the software of the router, through which you went online, was a vulnerability.
I just hacked this router and placed my malicious code on it.
When you went online, my trojan was installed on the OS of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).

A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock.
But I looked at the sites that you regularly visit, and I was shocked by what I saw!!!
I'm talk you about sites for adults.

I want to say – you are a BIG pervert. Your fantasy is shifted far away from the normal course!

And I got an idea....
I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).
After that, I made a screenshot of your joys (using the camera of your device) and glued them together.
Turned out amazing! You are so spectacular!

I'm know that you would not like to show these screenshots to your friends, relatives or colleagues.
I think $778 is a very, very small amount for my silence.
Besides, I have been spying on you for so long, having spent a lot of time!

Pay ONLY in Bitcoins!
My BTC wallet: 182PJESsEWbuJ8PEgfM58p64jbok3i1gNU

You do not know how to use bitcoins?
Enter a query in any search engine: "how to replenish btc wallet".

图 4-12 慌称掌握用户隐私视频的恐吓邮件截图

另外，近期一些网友也收到了一些帐号异常的钓鱼邮件，“黑客”冒充官方身份向邮箱发送帐号异常提醒，并引导受害者进入一个假冒的网站进行撤销、解冻等操作，，而一旦受害者通过打开假冒网站，就会被假冒网站要求输入正确的帐号密码 ,从而导致用户帐号密码被假冒网站收集窃取 ,造成用户信息二次泄露。

图 4-13 假冒帐号异常的钓鱼邮件截图

五、 总结

大规模的信息泄露在世界各地接连出现，一起大规模信息泄露的影响可能持续很久，影响范围也会扩散到各个行业。不管是企业受害者，还是个人消费者，遭遇信息泄露事件之后，往往难以应付次生风险。只有预防信息泄露，让这些事件不再发生，才是根本的解决办法。

对于普通用户而言，注意保护自己的个人隐私数据。不要在多个平台使用相同的帐号密码，并保持定期更换复杂密码的习惯。安全专家反复建议个人用户宜将所有已提供双重验证功能的互联网服务开通双重验证。开通双重验证后，当自己的帐号因某种原因泄露到攻击者手中，也能及时保障个人信息安全。

对企业来讲，数据安全保护不仅仅是对数据本身的保护，也是对企业经济利益和信任感的维护。企业终端设备被入侵及内部安全管理机制不完善等问题值得关注。虽然一些大型企业都组建有自己的技术团队，但其在安全信息安全

方面可能并没有做好足够的准备，随着大数据、人工智能、云计算等技术的不断深入发展，网络攻击事件防不胜防，数据安全不再局限于防火墙、入侵检测和防病毒等层面，而需要通过构建从内到外、全面的信息安全防护体系，建立可感知、可控、可审计的安全环境，第一时间发现企业暴露在外部的各类安全风险，及时感知、及时处理，才能解决企业在网络安全上的痛点。

另外随着欧盟 GDPR（《一般数据保护条例》）以及国内的《网络安全法》、《公安机关互联网安全监督检查规定》等相关法律法规的生效和实施，企业保护用户数据安全也是一种法律责任。企业履行保护用户数据的责任需要加强在信息安全领域的投入、建立系统化的安全保障体系，包括选择专业的安全解决方案，建立系统化的安全保障体系，定期排查风险隐患、强化防护技术手段、完善安全管理制度、落实网络安全责任等等，从而提升企业业务运营过程风险感知和发现能力，降低安全风险。

腾讯安全不仅在终端推出了针对恶意攻击的有效解决方案，还面向企业推出了腾讯安脉外部风险防控体系，为企业提供有效的业务风险监测和预警 SaaS 服务。

腾讯安脉以互联网、暗网中的开放数据、部署的全球蜜罐节点为基础，借助腾讯多年来积累的大数据处理和安全研究经验，帮助企业第一时间发现各类安全风险，如互联网资产暴露、企业品牌形象监测、高危漏洞预警、互联网业务安全风险。提供行业安全动态，协助企业做出正确的业务风险判断和处置建议。

参考链接：

https://mp.weixin.qq.com/s/vKejiR628Frb_-y9WzTmIQ

https://mp.weixin.qq.com/s/iL8pMJqlhzmEf4hMQyhhzw

https://mp.weixin.qq.com/s/Bo3y51iCEzzyHl9XXWo5mQ

https://mp.weixin.qq.com/s/8JliL07O6mL1vKs4k6QBqg

https://www.freebuf.com/articles/web/169770.html

https://cloud.tencent.com/info/71abe1e1ae97740ce376d8b46f894dbd.html

扫描下方二维码

了解腾讯安全


腾讯安全