为报复诈骗平台,他自学黑客技术却在“报仇”中寻到“商机”

景宁警方破获全国首例新型DDoS黑客案

本报记者 陈佳妮 通讯员 梅婷

他们20岁左右,利用最新型的DDoS攻击模式,做了很多“惊天动地”的事情。他们通过攻击境内外服务器,造成政府问政通道无法正常访问,学校网页无法下发通知,购物网页“离奇”丢失,棋牌网游无法登录……

近日,景宁警方破获了全国首例新型DDoS黑客网络犯罪案。昨天,警方公布该案案情。


抓获嫌疑人


缴获的作案工具

明码标价攻击网站

2018年1月初,景宁县公安局网警大队,接到阿里巴巴团队提供的线索:景宁本地,有人使用最新型的DDoS攻击模式,攻击境内外服务器。

DDoS(Distributed Denial of Service)攻击,即分布式拒绝服务。黑客通过对目标网站的攻击,消耗目标网站主机资源,让它无法正常服务。

景宁县公安局网警大队民警陈勇涛说,这种攻击方式十分“简单粗暴”,它就好比叫上一大帮人跑进一家饭店,占据了所有的桌子,却不吃饭,而真想吃饭的客人又进不来。游戏、博彩、互联网金融等行业很容易遭受DDoS攻击。由于这类攻击成本很低,黑客们往往明码标价,形成了相关产业链。用大流量DDoS攻击服务器1小时,网上报价只需50元。

疯狂的“复仇计划”

1月29日,景宁县公安局成立专案组,对此案进行立案侦查,公安部将该案列为2018年第一批打击黑客“净网专项”快侦快破督办案件。经过2个多月缜密侦查,在阿里巴巴团队的协助下,专案组摸清了这一神秘组织的底细。

这个团伙的成员分布在全国各地,其中不乏只有初高中文化程度的青少年,他们通过QQ联系,互相交流技术。

他们搭建各自的DDoS攻击平台,通过刷百度排名,推广DDoS服务。他们提供一对一服务,同时客户也可以在平台上购买不同价格的“攻击套餐”。客户付钱后,只要输入需要攻击的网站网址,平台便会发起自动攻击。

1994年出生的景宁人“落寞”(网名),便是这个团伙的成员之一。

“落寞”高中辍学后,一直在当地打工,2016年,他想通过淘宝刷单获利,没想到遇到了网络诈骗平台,被骗走了几千元积蓄。

当时,“落寞”很气愤,想让这个诈骗平台消失。他疯狂在网上搜索,学习黑客知识,并在论坛上接触到了DDoS攻击。很快,他便加入到一个QQ群中,学习了很多新知识,也小试牛刀攻击了几个博彩网站,大获成功。

这让他信心倍增,开始了他的“报仇”计划——攻击网络诈骗平台。在此过程中,他发现竟有“金主”找上门,希望“落寞”帮忙攻击其他网站,这让“落寞”看到了其中的“商机”。

很快,他搭建起自己的DDoS攻击平台,并开始接待“金主”。让他印象最深的一次,是有“金主”出650元钱1小时,让他攻击比特币挖矿机(用于赚取比特币的电脑),“攻击了整整10小时,赚了6500元钱。”唾手可得的金钱,让“落寞”觉得发财在即。

3月8日早上,“落寞”熬了一个通宵后,准备睡到大中午,再找些朋友喝酒吃饭,度过自己的24岁生日。就在他刚进入梦乡没多久后,景宁警方找上了门,将他带走。

警方的收网行动

“落寞”落网后,这个团伙的其他线索,也逐渐浮出水面。景宁警方随后找到了团伙的另一名成员“二佬”(网名)。

“二佬”是福建人,“落寞”被抓后没几天,“二佬”的女朋友要他陪着一起到浙江,说是女友的姐姐因为涉嫌诈骗,要去金华办理取保候审。

拗不过女朋友,“二佬”陪着女友来到金华。3月16日,“二佬”在金华入住旅馆后,就被景宁警方锁定,得知他已进入浙江境内。当晚民警赶到金华,第二天早上6点,民警敲响了“二佬”的房门,扣住了睡眼朦胧的他。

今年4月底,各地警方收网,抓捕了一批犯罪嫌疑人。期间,一名叫“玖爱”(网名)的湖南人,将自己的平台刷到了百度排名的第一位。5月5日晚,随着嫌疑人“玖爱”在湖南落网,至此,公安部督办的“129破坏计算机信息系统案”告一段落。警方一共摧毁黑客攻击平台3个,抓获平台主要创办者3人,查获境外发包机15台、攻击日志10万余条。

目前,案件还在进一步侦办中。

车队通过收费站,拉着“鲜鸡蛋”打开蛋箱没鸡蛋,只有零配件

东阳破获冒充农产品逃费系列案

通讯员 徐步文

为了逃避高速缴费,车队的驾驶员打起了鲜活农产品运输绿色通道的主意。这些运输车上明明载着的是机器配件等,他们却用装农产品的箱子包装起来,放进车厢,企图蒙混过关。但“障眼法”并没有逃过收费站工作人员和警方的“火眼金睛”。

近日,东阳警方侦破了冒充运输鲜活农产品逃费系列案,并发布了案件详情。

鸡蛋箱里没有鸡蛋

2017年9月7日傍晚,甬金高速东阳出口,又到车辆的进出高峰期。

一辆带有鲜活农产品运输绿色通道通行证的大型集装箱运输车,驶入收费站的鲜活农产品运输绿色专用通道口。

当天,收费站工作人员对这辆车进行了常规检查。打开车厢,里面放着88个标注整齐的“鲜鸡蛋”箱,但有70个“鲜鸡蛋”箱却是空箱。再仔细一查,工作人员发现,剩下“鲜鸡蛋”箱里放着的全是机器零配件、橡胶等货物。

收费站的这个绿色专用通道,对整车合法运输鲜活农产品车辆给予减免通行费的优惠政策。而这辆悬挂江西牌照、核载50吨的运输车,却伪装成运有农产品的车辆,企图减免通行费。

收费站工作人随即报警。经调查,驾驶员葛某是河南人,2016年初应聘进入福建泉州某车队运输货物。

“老板会把通行费一次性给我们,至于用掉多少,老板不管。我看到其他驾驶员用农产品箱子填充车辆,逃避缴费,我也学到了这个‘省钱窍门’。”葛某说,自己之前曾多次从绿色专用通道下高速,“省”下的通行费,进了自己的口袋。

葛某走的这条运输线路,需要从福建泉州到北京,全程2000多公里。在浙江省境内,葛某从温州上高速,到长兴南下高速,正常来回一趟需要2100元左右的高速通行费。2016年2月到2017年9月,葛某偷逃了6万余元的通行费。

事后,葛某因涉嫌诈骗罪,被东阳市公安局刑事拘留,车辆被扣押。

但案件并没有结束。

辗转千里调查取证

东阳警方根据初步判断,认为该案背后很可能存在一个犯罪团伙。警方随即与甬金高速东阳收费站取得了联系,梳理了近几年在收费站申请绿色通道的车辆。

此后,警方赶赴葛某所属的运输车队所在地——福建省石狮市,开展调查取证。

在当地派出所协助下,东阳民警找到了该车队,车队负责人吴某接待了警方。吴某已知悉葛某被抓,早有心理防备。

但民警还是在车队办公室的角落里,发现了大量散乱的车辆费用结算单,这些单子上均有驾驶员的签名,民警随后将这些单据调走。

对600多张单据进行梳理,并结合相关调查后,警方推测,该车队拥有的12辆大货车、10余名驾驶员,均涉嫌在高速公路上逃费。

由于车队的货车运输途径遍布全国各地,为加快调查取证,警方先后辗转河北、江苏、山东等地,调取了两万多条数据。并基本确定该团伙涉嫌在浙江、江苏、山东、河北等地的高速公路上逃费。

由于葛某落网后,车队其余嫌疑人已逃至各地,警方随后展开抓捕行动。经过近半年的努力,近日,该车队涉嫌逃费的14名犯罪嫌疑人全部到案。

经查实,该团伙作案1673件,其中,浙江省内作案947起,其余省市作案626起,警方追缴了赃款74万余元。目前,14名犯罪嫌疑人全部被移送检察院审查起诉。