很多网友对近两个月前一次网络大面积瘫痪事情记忆犹新:5月19日21:50开始,江苏、安徽、广西、海南、甘肃、浙江六省(区)用户访问网站速度变慢或干脆断网。截至20日凌晨1时20分,受影响地区的互联网服务才基本恢复正常。

7月6日,这起受到全国普遍关注的"5·19"网络瘫痪案,其4名犯罪嫌疑人被常州市天宁区检察院以涉嫌破坏计算机信息系统罪批准逮捕。

昨天,办案的检察官在接受快报记者采访时道出这起案件缘起:"5·19"六省(区)的网络瘫痪案,起因竟是几个经营私服的"小混混"和竞争对手相互掐架。其掐架犹如推倒的多米诺骨牌,引发了连锁反应。值得深思的是,这种相互采取黑客攻击式的掐架,在目前的网络私服行业相当普遍。

■通讯员 殷茹 快报记者 刘国庆

网络私服"掐架"引发多省断网

"5·19"六省区网络瘫痪事件犯罪嫌疑人被常州检方批捕

回放

六省区断网两个多小时

5月19日下午,在常州市区一家写字楼内上班的小陈感觉网速越来越慢,随后,新浪、搜狐、网易等各大门户网站均不能访问。一开始,他以为是自己电脑中毒了,于是不断地杀毒、优化、清除电脑垃圾,可是一点效果也没有。随后,他发现单位同事的电脑也出现同样的情况。于是,同事们又不断地将单位的路由器重启,可是,一点效果也没有。让小陈和他的同事们没有想到的是,他们正在经历着一次影响到全国六省区的大面积断网事件。

5月21日,工信部发布消息称,5月19日21:50开始,江苏、安徽、广西、海南、甘肃、浙江六省区用户访问网站速度变慢或干脆断网。截至20日凌晨1时20分,受影响地区的互联网服务基本恢复正常。

对于事件的原因,当时众说纷纭。工信部正式发表通报,初步解释此次事故的原因:由于暴风影音(影音播放软件)网站的域名解析系统受到网络攻击,导致电信DNS服务器访问量突增,网络处理性能下降。

公安机关接报后,立即组织江苏、浙江等地公安机关开展调查。一时间,此案受到全国媒体普遍关注。

由于此次"私服"攻击的那台服务器设在常州,公安部将此案交由常州警方办理。

常州警方通过网络技术监控发现,在广东佛山一台服务器有异常情况,经布控,将这台服务器主人抓获,并一举控制其他3名同伙。目前,4名犯罪嫌疑人已被常州市天宁区检察院以涉嫌破坏计算机信息系统罪批准逮捕。

这种引发大面积网络瘫痪的案件,近10年来都十分罕见。这起案件是怎样引发的?幕后又隐藏了些什么?

"5·19"断网事件

5月19日21时50分至次日凌晨1时20分,江苏、安徽、广西、海南、甘肃、浙江等省(区)出现罕见断网故障。

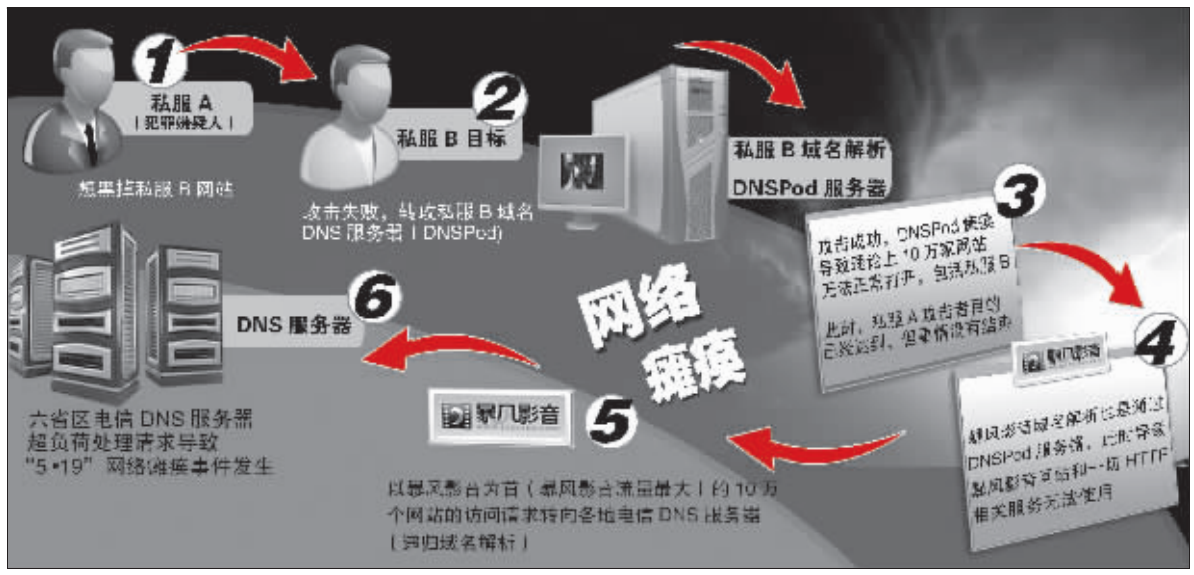
5月20日,中国电信宣布已排除故障,并解释原因在于暴风影音网站。

5月20日,暴风影音发布公告表示,六省(区)断网故障已恢复正常,事故原因是DNS域名解析系统受到攻击。

5月21日,免费域名解析服务商DNSPod站长吴洪声接受专访称源头为黑客私斗。

5月24日,暴风发布关于断网事件向网民和新老用户的公开信,正式就该事件道歉,并称已正式完成报案程序。

6月1日,暴风公司CEO冯鑫宣布将召回1.2亿播放器软件,称正评估断网损失。



制图 俞晓翔

■调查

他租用91台私服去攻击别人

在办案的检察官眼中,这4个犯罪嫌疑人都是年轻的"80后",案件的两个核心人物是小兵(化名)和小青(化名),两人都是1986年出生。

小兵是浙江人,父亲在广东佛山开一家棉花厂。小兵和小青是同学,小兵毕业后到父亲的棉花厂帮忙。不久,小青也来到棉花厂。有一次,小青告诉小兵,说经营私服(私人服务器)赚钱。小兵决定投资私服(私人服务器),专门经营网络游戏和广告。在这个小公司里,小兵是大股东,负责投资,小青负责技术。

私服是未经版权拥有者授权,非法获得服务器端安装程序之后设立的网络服务器,本质上属于网络盗版,而盗版的结果是直接分流了运营商的利润。一些网络游戏等网站商家租用像小兵这样经营的私服,半年或一年一租。

在强手如云的私服业内,像小兵这样经营私服的公司规模小、技术薄弱,他们小打小闹,很难赚到钱。后来,他们发现,他们赚不到钱的主要原因是,在私服业内,各经营私服的对手经常相互攻击,只有将对手击败后,自己才能将对方的客户抢过来。

自己经常被攻击,公司盈利不高,为此,小兵一直头痛不已。后来,小兵认识了一位网友。两人在聊到经营私服被对手攻击的时候,这位网友说,攻击人家的网站,需要一定的流量,否则很难奏效。

流量是什么概念?"办理这个案子后,我从一个电脑盲差不多变成了半个专家了,"办理此案的检察官笑着说,流量好比A手机对B手机发送一条短信,B手机运行正常,但是,如果同一时间有5000只手机对B手机发送短消息,那B手机肯定会爆掉。

那位网友就跟小兵解释这个原理。那要如何才能达到一定的流量呢?这位网友说,要达到一定流量,就要增加攻击的私服数量。

为此,小兵、小青联合两人的亲戚小风、小宝一共投资了28万,请那位网友联系,租用了91台私服,专门用来攻击其他私服。租用的这91台私服,在浙江苍南。

正面强攻不佳,转向攻击"域名解析"

由于几个人对网络技术并不专业,尽管租用了91台服务器,但在直接攻击其他网游私服的过程中,发现对部分私服的攻击效果不是很好。为此,几个人在网上发帖寻求"帮助"。

很快,小兵就认识了一位网友小强(化名)。值得注意的是,直到抓捕归案,两人以前从未谋面。小兵就向小强请教怎么攻击对手私服。小强告诉他,直接攻击私服效果不是很好,如果攻击这些网站的域名解析服务器,致使这些网站无法访问,应该效果不错。小强自己也在浙江东阳经营一家网络公司,也同时经营私服。但是小强自己也对网络技术不够专业。于是他叫自己的手下员工小刚(化名)完成这个任务。小刚接到任务后,连夜赶制了成套网上攻击的方法,写成文本文件,通过邮件发给了小青。

小强在整个过程中,未收取小兵方面一分钱,那么他为什么要这么做呢?据小强自己说,私服行业整个的风气就是相互恶意攻击,谁攻击对方取得成功,谁就能赚钱,他教小兵实施攻击,主要目的,一个是为自己在"网络江湖"上扬名立万,另外就是这样做了以后,他的名声传出去,也没人敢攻击他自己公司的私服,对自己也是一种保护。

5月18日晚攻击正式开始。具有讽刺意味的是,案件的主要人物小兵并没有把这次攻击当回事情。他将整个攻击的工作交给小青,自己则去一家酒吧会女网友去了。

当晚,7点左右,小青用公司的电脑开始发起攻击。他们谁都没料到,这个小刚设计的攻击方法采用的是"擒贼先擒王"的策略,也就是直接攻击私服网站的"首脑"——DNSPod服务器。

DNSPod是一个免费域名,它的东家是南通万达网络服务公司,负责人是一个叫吴洪声的年轻人,今年才24岁。

吴洪声的个人网站主要为国内众多网站提供域名解析服务。虽然是非公司运营,但他旗下已经拥有16台服务器,分布在全国各地。他服务的网站包括Verycd、雨林木风、4399、小游戏、暴风影音、CNZZ等知名网站。

DNSPod服务器下面管理着很多私服,是众多私人服务器的首脑。一旦DNSPod受攻击瘫痪,其他私服都会受损。

当初小青他们选择攻击对象的时候,表面上他们选择攻击的六七个私服,都是几家游戏网站,他们万万没想到或者说根本没这方面的意识,这几家网站和暴风影音是同一个DNSPod服务器。

攻击仅20多分钟,六省区网络瘫痪

吴洪声的这台DNSPod服务器委托常州电信托管,安放在常州电信勤业机房内。

小青在自己的电脑公司内实施攻击了20多分钟后,就将攻击程序关闭了。然后就在公司内的办公椅上打瞌睡,他丝毫没有意识到他这次20分钟的攻击会引发轩然大波。

小青实施攻击后不久,远在常州的电信勤业机房管理员发现,DNSPod服务器端口流量异常,立即向上级汇报,常州电信接报后又向江苏电信汇报请示。为防止意外发生,江苏电信果断决定,立即关闭DNSPod服务器。

不幸的是,这台被电信关闭的DNS服务器当时恰好在为大约10万家网站提供域名解析服务,其中就包括暴风影音。此外还包括大量地方门户网站、个人网站和企业网站。这导致大量用户随后无法访问这些网站。

也许有人会问,DNSPod关闭后,为何18日晚没有出现网络瘫痪,而一直到19日晚才全面爆发?原来,万达公司与常州电信签订托管协议时,对DNSPod约定有缓冲时间,请求解析一次失败后,DNSPod有24小时的缓存期。但也正是由于缓存期的存在,一直正常的表象并没有让管理方找到DNSPod端口流量异常的真实原因,以致没有采取正确的挽救措施,从而引起大面积瘫痪事故。

19日晚事发后,吴洪声一直忙于解决18日晚的攻击问题,直到20日下午有朋友告诉他,19日晚大面积故障可能与DNSPod有关,他才恍然大悟。此时工信部已召开紧急会议,暴风高层也联系到吴洪声,商量后续备份域名服务器问题。

21日,工信部联合暴风及DNSPod向公安部门报案。

7月6日,小兵等4人因涉嫌破坏计算机信息系统罪被天宁区检察院批准逮捕。

分析

"小混混掐架"引发蝴蝶效应

据办案的检察官介绍,4名犯罪嫌疑人事前一直不认为自己的行为是在犯罪。他们一直认为,国内很多经营私服的网络公司之间,相互攻击,这种行为太多了,甚至大家认为这是一种正常行为。

办案的检察官说,对"黑客"攻击行为,法律上有两条罪名可以追究,一是非法侵入计算机信息系统,另一条是破坏计算机信息系统罪,前者是涉及到国家安全,小兵等人的行为则适用于后者。案中4人不但没有意识到自己是在犯罪,甚至根本没想到自己的攻击行为会引发这么严重的一个后果。

一位专业人士称,"5·19"事件的严重程度就像蝴蝶效应,美洲热带雨林一只蝴蝶震动翅膀,可能引发太平洋上一场猛烈的风暴海啸。"5·19"断网事件的始作俑者,在网络黑客眼里,根本就是江湖的几个小混混在掐架,结果引发的却是网络大面积瘫痪,谁能想得到?他们掐架,推倒的只是第一块多米诺骨牌。

此次断网事件开始于"私服"经营者之间的恶性竞争,他们的目的很简单,就是"扬名谋利"。在目前的网络行业中,这种恶性竞争很普遍。只不过这次由于一些偶然的因素造成了更加恶劣的后果,才让这几家网游私服之间的事暴露出来。此次网络大瘫痪爆发得如此突然,涉及范围如此之广,影响如此之深,令广大网民和业内专家都始料未及。

办案的检察官告诉记者,办理这次案子,发现有很多值得深思的地方,从技术上、法律上、行业上,国家相关部门都应加强监管。

链接

私服

私服是未经版权拥有者授权,非法获得服务器端安装程序之后设立的网络服务器,本质上属于网络盗版,而盗版的结果是直接分流了运营商的利润。私服存在的主要目的同官方服务器是一样的,都是向玩家收费以获利。

域名解析

我们平常所用的网址,在后台服务器上都有一个对应的IP地址。机器间互相只认IP地址,域名与IP地址之间是一一对应的,它们之间的转换工作称为域名解析,域名解析需要由专门的域名解析服务器来自动完成。