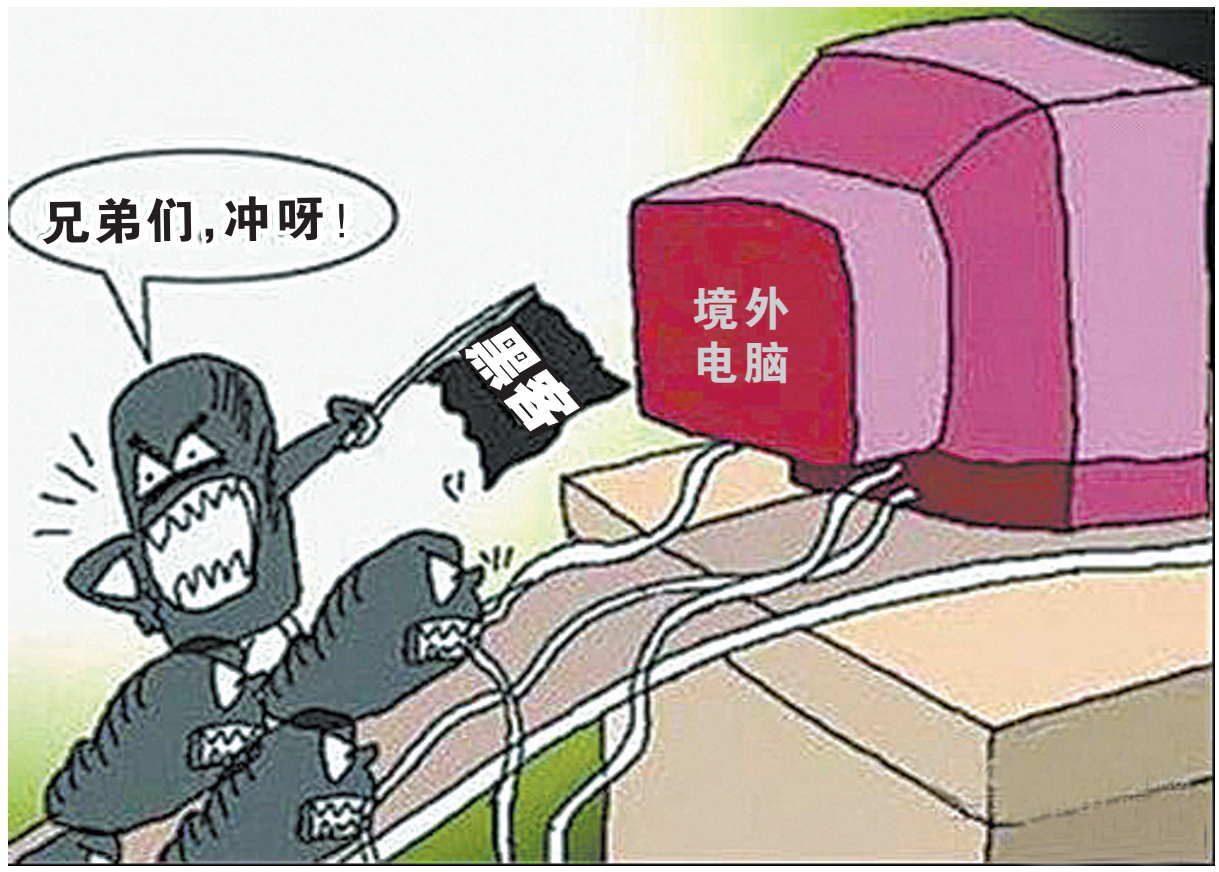
黑客公司“黑”2.5亿台境外电脑 非法获利近8000万元



阅读提示

北京一家科技公司开发名为“FIREBALL(火球)”的恶意软件,捆绑正常软件传染境外互联网,一年内感染全球2.5亿台电脑,并利用植入广告牟利近8000万元人民币。

新京报记者7月24日从海淀警方获悉,目前,这起跨境“黑客”破坏计算机系统案已被侦破,9人因涉嫌破坏计算机系统罪,已被海淀区检察院批准逮捕。

A “海淀网友”发现:黑客在境外推广“有毒”免费软件

2017年6月3日,北京市公安局海淀分局网安大队接到一名热心“海淀网友”张明(化名)举报:他在网上浏览网页时,发现国外某知名安全实验室报道了一起代号为“FIREBALL(火球)”的病毒。

“这个境外报道大致是说,中国一家网络公司在国外推广的免费软件中,镶嵌了恶意代码,用来劫持用户流量,并以此达到流量变现的目的。”张明介绍,根据报道,该病毒感染了境外2.5亿台用户电脑。

“我自己本身就是一名网络安全公司的技术人员,我们公司对于这些会格外关注。”张明称,在看到国外的实验室分析后,他结合专业知识,对“火球”病毒传播途径进行了分析,同时协助民警对该网络公司推广的免费软件进行样本固定和功能性分析,确定在这些推广的免费软件内,存在相同的恶意代码。

B 警方与黑客“斗法”:模拟中毒过程警方锁定证据

在北京市公安局网安总队的领导下,海淀分局网安大队对涉案网络公司进行了调查,发现该公司办公地、注册地均在海淀区。

随后,警方网安部门和刑侦部门成立专案组,对此开展立案调查。

“因为软件上需要数字签名,通过数字签名能确定公司名称,再找到工商注册信息,最后找到该公司的法人。”网友张明称,这是这次协助警方比较顺利的一个原因。

办案民警介绍,接到线索后,警方从病毒程序的运行方式入手,通过模拟系统中毒过程结合实地调查追踪,准确掌握嫌疑人制作病毒自行侵入用户电脑,强行修改系统配置,劫持用户流量,恶意植入广告牟利的犯罪事实。

通过监测,民警固定了整个犯罪行为过程的关键证据,同步摸清了该公司组织架构。

6月15日,警方在该公司所在地将犯罪团伙破获,控制马某、鲍某、莫某等11名嫌疑人,他们已承认犯罪事实,其中9人因涉嫌破坏计算机系统罪,已被海淀区检察院批准逮捕,案件还在进一步审理中。

C 黑客公司也有“准备”:为逃避制裁作案前咨询法律人士

“目前被批捕的9人是公司的骨干人员,都很年轻,有过几年IT行业的从业经验,也有一定的反侦查意识。”办案民警介绍,该网络公司位于北京市海淀区,成立于2015年底,对外名义上是网络科技公司,由马某任公司总裁,鲍某和莫某任公司技术总监和运营总监。公司的规模在100多人左右,分别负责开发正常软件和恶意代码,专门测试恶意代码和正常代码捆绑后的效果等。

民警介绍,根据嫌疑人的供述,他们通过开发恶意软件捆绑正常软件,从而达到植入广告牟利的劫持流量的目的,“通俗地说,也就是通过用户在不知情的情况下,点击他们经过捆绑的网页链接,达到提升广告浏览量的目的,再以此增加推广广告费收入。”

据介绍,在开发出“FIREBALL”恶意软件之后,考虑到国内网络安全监管严厉,为了躲避国内监管,他们就在国外开通账户,然后将该恶意软件捆绑正常的软件投放在国外软件市场进行传播。

“其实他们在作案前,也有过担心,还专门咨询了法律人士,了解违法情况以逃避制裁。”民警称,该公司国外的账户,仅在去年就非法获利近8000万元人民币。

海淀区检察院办案检察官介绍,案件目前还在进一步的侦办审理中,由于主要侵害对象在国外,在进行证据的保全后,对病毒的侵害过程进行了模拟还原,后续也请第三方对开发的恶意软件进行鉴定。

“对嫌疑人的批准罪名是破坏计算机信息系统罪,后续如果出现什么其他犯罪情节和行为,会在补充侦查中追加,但目前还没有发现侵犯公民个人信息的违法犯罪情况。”检察官表示,嫌疑人罪名查实后,面临的可能是5年以上的有期徒刑。

D 新闻链接:恶意代码植入浏览器劫持国内用户流量

海淀警方7月24日介绍,除了破获“火球”病毒劫持境外用户流量案件外,近日警方还破获了北京市首例利用流氓软件劫持国内用户流量的案件。

今年4月28日,海淀分局网安大队接到辖区百度公司报案,称其公司网络流量出现异常,网民访问渠道被更改,当用户从百度旗下的hao123等两个网站下载软件时,会被植入恶意代码。这一事件造成经济损失约2000万元人民币,百度公司清理了相关恶意代码后报案。

警方经初步调查,锁定了一家涉案公司的服务器,该公司根据带入的流量向百度公司索取报酬。后经查实,这些流量是通过篡改网民访问路径得到的。民警通过对百度服务器以及被篡改电脑的访问路径进行数据勘验,发现北京某网络技术公司在hao123浏览器的安装包内植入恶意代码,对安装浏览器网民的电脑进行流量劫持,恶意更改网民访问路径,从而非法获利。

固定证据后,警方准备进行抓捕时,发现涉案公司已被变卖,部分证据也被销毁,主要嫌疑人失联。两个月后,办案民警通过涉案嫌疑人上传恶意代码的账号,查清了3名嫌疑人的落脚点,后在顺义、朝阳等地将3名嫌疑人控制。据百度公司介绍,此次警方抓捕的犯罪嫌疑人系某外包公司前员工。

目前,3名嫌疑人因涉嫌非法破坏计算机信息系统罪,被海淀警方依法采取刑事强制措施,案件仍在进一步审理中。(左燕燕)