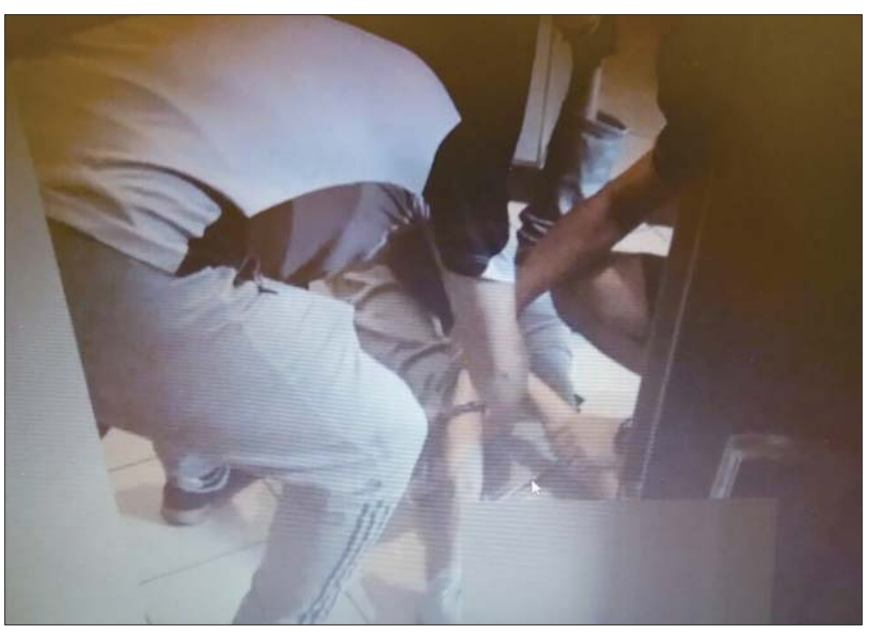
盯上理财网站漏洞,大举攻击2小时

充1元提现20万 黑客划走1800万

广东一男子黄迪(化名)发现山东某公司的理财网站存在漏洞后,就利用黑客技术采取"先充值1元,再修改成20万"的方式,从该公司资金池内提现20万元。为了混淆警方视线,曾有非法入侵计算机系统前科的黄迪还把这一漏洞公之于众。结果导致短短两小时内,山东某公司的理财网站遭众黑客攻击,1800万元资金被疯狂提现。2018年5月2日,记者从历下警方获悉:接警后,他们迅速出击,不仅成功抓获包括黄迪在内的18名嫌犯,还冻结及追回涉案资金987万,打掉了这个公安部督办、涉及全国22个省份的破坏计算机信息的特大网络盗窃团伙。



专案组民警赶赴广东,将黄迪抓获。

网络盗窃流程

理财网站注册,然后充值1元

↓

借助某种软件劫取数据包,篡改数据

↓

实际充值1元,系统默认其账户内有20万元

↓

每次提取20万,因这是系统的提现限额

↓

以8万元将信息卖给另一黑客,并在QQ空间公布了漏洞,导致大量黑客疯狂提现1800万元

文/片 本报记者 尉伟
通讯员 赵杨

理财网站2小时内 大量新用户注册提现

事情还得从2017年9月14日下午说起。当时,山东某公司向历下警方报警称:自己的网站被人攻破,公司在第三方支付公司的账户的钱被转走1800余万元。

"这是一家投资公司,被攻击的是他们的理财网站。"2018年5月2日,历下公安网警大队民警顾威告诉记者:用户在该理财网站注册成功后,就可以实现网上投资、提现,而其资金的转入转出都是通过第三方支付公司的账户来进行的。而这家投资公司为了保持每日的正常运营,在第三方支付公司的账户里都会保有3000万元资金。

可民警调查发现,从2017年9月14日中午12点至下午2点短短两个小时的时间内,该理财网站有大量新用户注册,然后第三方支付公司账户内的大量资金被这些新用户划走、提现。

案发后,历下警方成立专案组,并兵分两路:一路向山东省公安厅、济南市公安局反诈骗中心汇报情况,通过电信诈骗案件侦办平台,成功止付16笔异常划拨资金共计400余万元人民币;另一路则奔赴上海、厦门等地调取相关数据,"上海是第三方支付公司所在地,而该理财网站维护运营的公司在厦门"。

最终,通过对这些涉案账户对比分析,历下警方获取了线索,并成功锁定了首个攻击山东某公司理财网站的嫌犯黄迪。

将漏洞8万元卖出 还在QQ空间公布

很快,专案组民警赶赴广东,将嫌犯黄迪抓获。

"黄迪28岁,来自广东博罗。"民警顾威说。而此前,黄迪就曾因非法侵入计算机系统而被外地警方处理过。

原来,没有正当职业的黄迪整日在网上闲逛,并试图利用自己所学的计算机技术来"发财"。一次偶然的机会,他发现山东某公司的理财网站在第三方支付跳转时存在漏洞。于是,黄迪先在该理财网站注册,然后充值1元,在借助某种软件劫取数据包、篡改数据。"修改数据后,虽然他实际充值1元,但系统认为他的账户内有20万元资金。"民警顾威介绍,黄迪之所以提现是20万,而不是30万或者更多,"是因为系统规定的每次提现最高额度就是20万元"。

得手后,曾有前科的黄迪十分狡猾:他先是把该漏洞以8万多元的价格卖给另一个黑客,然后又在自己的QQ空间内公之于众,致使该漏洞被其他黑客大量传播利用。"最多的一个黑客从资金池里转走了260万元。"民警说,黄迪此举的目的就是为了混淆视听,干扰警方的侦查视线,以便让自己能逃之夭夭。

值得一提的是,在民警抓获黄迪的第二天,另一名黑客谢某自觉事情不妙,还拨打黄迪的电话进行试探。而民警接听了电话后,告知谢某事件的利害,并晓之以理、动之以情。很快,谢某迫于压力到派出所投案自首。

18名嫌犯落网 冻结追回近千万元

5月2日,记者从历下警方获悉:截至目前,民警已抓获嫌犯18名,其中刑事拘留9人、取保候审2人,查获涉案电脑15台,手机27部,银行卡46张,冻结及追回涉案资金987万,打掉了这个公安部督办、涉及全国22个省份的破坏计算机信息的特大网络盗窃团伙。

不过同时,民警也注意到:这些黑客在山东某公司理财网站注册时所用的身份信息等都是他人的、真实的。"这些都是他们专门花钱买来的一整套信息。"民警介绍:这所谓的一整套身份信息包括身份证、电话卡和五张相应的银行卡;其中一张银行卡还是带U盾的,用来在网上操作,"有些偏远地区的人,觉得身份证没用,就200元卖给别人用。收的人就利用这些身份证办理电话卡、银行卡,然后再以1000元的高价卖出去"。而一些理财网站在用户注册时,只注重个人信息是否一致,却不能认证是否本人在注册、操作,这也给了不法分子以可乘之机"。

民警告诉记者,互联网的虚拟性,导致一些人在高额利润的诱惑下,在虚拟世界为非作歹。历下警方也将进一步提高打击网络犯罪的能力,变被动为主动,打团伙、打源头,不断加大打击整治的力度和深度,并同时也提醒广大市民:仔细甄别各类网站、软件的真假,不要对外提供个人的相关信息。