

摧毁黑客攻击网站的“终极武器”

徐汇警方侦破一起破坏计算机信息系统案

10:30 上午首发

首席记者 潘高峰

网络游戏平台黄金时段无法登录,黑客超大流量攻击只为打击同行竞争者。今天上午记者从徐汇警方获悉:一个控制大量“肉鸡”(被木马软件控制的傀儡计算机)和“黑量”(被黑客控制的带宽流量)的网络攻击犯罪团伙被摧毁。

经查,2012年以来,以屠某为首的网络犯罪团伙为牟取不法利益和排挤同业竞争,从黑客处收购“黑量”后,组织网络攻击小组,连续不断地对其他网站开展DDoS(Distributed Denial of Service)攻击,实施敲诈勒索或攻击网站平台后为对方介绍高收费高防机房牟利。目前,3人被刑事拘留,1人被取保候审。

攻击源头来自“肉鸡”

DDoS对于普通网友可能有点

■ 本案中的犯罪嫌疑人控制的黑色流量,大多来自一些缺少管理和维护的政府、学校、大型企事业单位网站。建议有关部门全面开展互联网安全大检查。

■ 现在一些商业类、游戏类网络公司,遇到竞争

往往习惯于通过非正规甚至违法手段打击竞争对手,一次委托攻击费用甚至超过百万元,由此养活了一个收量、维护和网络攻击的黑色产业。警方提醒,这种竞争手段不仅不合法,而且是搬起石头砸自己的脚。

【警方提醒】

陌生,但对于网络攻击犯罪分子来说,通过控制“肉鸡”“黑量”,发动攻击就能成为劫持网站的“终极武器”。DDoS即分布式拒绝服务攻击,其原理就是利用大量无意义的服务请求来占用目标网站的服务资源,从而使正常用户无法得到服务的响应,以达到瘫痪网络的目的。拒绝服务攻击的源头大多来自多个受黑客控制的“肉鸡”,他们接受主控指令同时对一个或多个目标发动攻击,几秒钟内,“肉鸡”上的代理程序被运行,目标网络因为不堪承受流量压力,顷刻崩塌。

今年1月,有用户先后向某公司反映,其旗下的多款网络游戏均无法顺利登录服务器。公司技术人

员排查发现访问流量始终占满,但有效访问几乎没有,公司马上意识到遭到了黑客的DDoS攻击。公司集中技术员努力几天,仍然无法应对这种攻击,1350万注册用户大量流失,造成近千万元的损失。徐汇公安分局接到报案后,在市局网安总队的指导下,迅速成立专案组开展工作,从成千上万的攻击源头中梳理线索。

训练人员广收“黑量”

经过缜密侦查,攻击流量提供者吴某首先进入了民警的视线。几经辛苦周折,转战江西、四川两地,专案组在除夕夜前将吴某从四川抓捕归案。

到案后,吴某交代收购“黑量”并实施攻击的上家另有其人,这伙人盘踞在河南郑州,以经营互联网公司为契机,训练人员在网上广收“黑量”,组织实施网络攻击、敲诈等犯罪行为。

因为正值马年春节,原本吴某每天与上家进行的结算恰好告停,约定正月十五后重启联系。吴某称其河南上家行事小心,一旦失去联系就很有可能察觉,并销毁犯罪证据。这就意味着专案组必须乘胜追击、务必要赶在正月十五前将这个真正实施攻击行为的上家抓捕归案。于是,专案组再次启程,终于赶在元宵之夜将本案主犯屠某及3名副手抓获。

操纵流量达几十个G

经查,以屠某为首的某网络公司,表面上经营网络游戏、视频聊天等业务,但暗中却从事网络色情、域名劫持、垃圾广告以及网络攻击,可以说从事着各种网络违法活动。但其中最为得心应手的还是网络攻击。

屠某通过各种网络群组寻觅提供“黑量”的来源,组织手下对收购来的“黑量”进行测试和维护,保证手头始终有能将任何一个网络攻塌的巨大能量。最高峰时屠某操纵的流量可轻易达到几十个G,而这样就已超过一般的商业网络公司网络带宽,也就是说,屠某手中掌握着一个在网上威力惊人并可以为所欲为的“终极武器”。本案中被攻击的网游公司因与屠某的公司争夺游戏玩家资源而遭屠某报复。屠某还培训堂弟,让他掌握网络攻击的流程和技术,企图把自己的公司作为网络攻击手的培训基地。

江苏靖江长江取水口异味消失 上海两大水库今将恢复取水

本报讯(记者 张欣平)在取水口关闭了3天后,上海以长江原水为水源的青草沙、陈行两大水库预计最快今天下午将恢复取水。目前两大水库取水点的监测数据显示,水质中各项有毒有害物质的关键性指标远远低于标准值,市民完全可以放心饮用。

5月9日,江苏靖江的长江取水口发现异味停止取水之后,江苏环保部门对靖江市饮用水源地取水口及上游50公里、下游30公里布点62个断面,持续32个小时取样监测,目前异味已经消失,但污染原

因还在调查之中。昨天中午起,靖江关闭了备用水源,恢复正常供水。目前,靖江下游的城市张家港、常熟、南通、太仓以及昆山等地也均为检出水质异常。

出于安全考虑,为防止上游原水有污染源,青草沙、陈行两大取水口5月9日下午关闭,暂停取水。经过两天时间,江苏靖江段长江水已流经上海,青草沙、陈行两大水库取水口各项水质指标并未出现异常。市水务部门人士认为,近期长江上游来水较为丰富,有助于稀释长江靖江段水体中可能存在的污染物。

部分老小区水箱弃用 间隔性断水居民闹心

近期,本市月浦、宝钢、永清、杨泰、宝林等老式居民小区的部分居民致电本报,反映小区经常会出现“间隔性断水”现象,日常生活受到影响。记者在采访中了解到,这些受到“间隔性断水”影响的小区,有的原本没有泵房,有的是部分泵房长期弃用,另有部分则属于私自改变原有供水方式,取消泵房或水箱供水改为地面直接供水。

在上海供水历史上,利用水箱供水方式的历史久远,那些一百多年前建造的大楼都采取这种方式。但上海大面积采用水箱供水的方式,则始于上世纪八十年代中期,经过多方比较,社会各界认为水箱供水是比较贴近上海实际的供水方式。目前上海约有十四万只水箱。

一般来说,上海的居民住宅小区都建有供水泵房和屋顶水箱,但有些被人为废除,留下了隐患。大约在2002年前后,社会上出现过一股“废除水箱,直接供水”的时尚,一些地区物业部门以居民要求

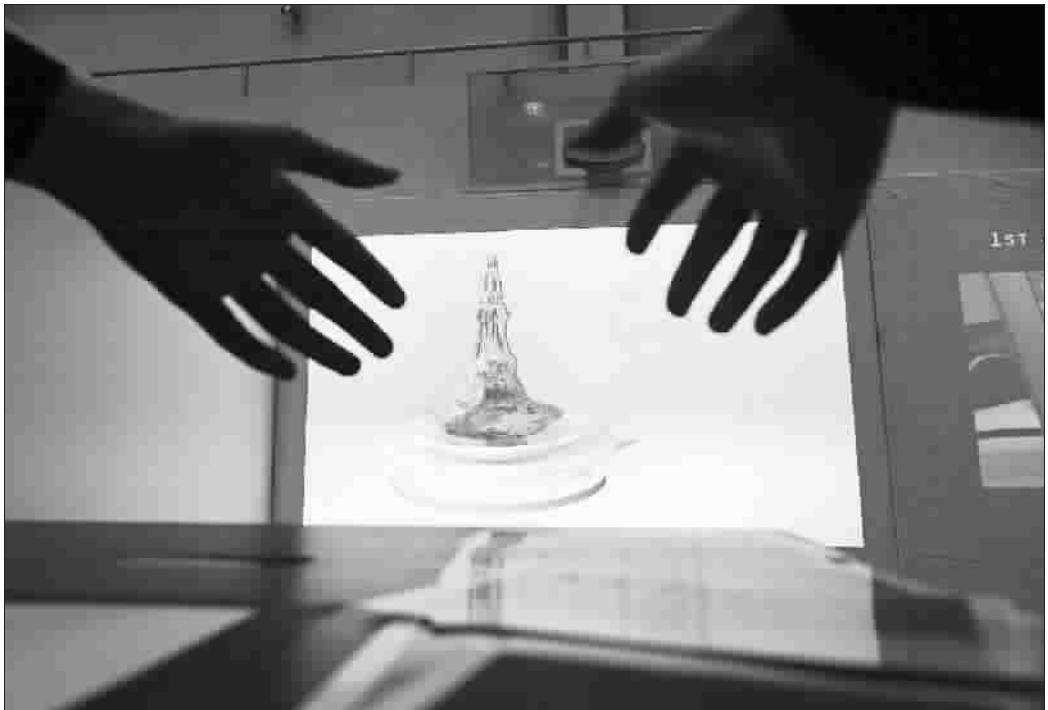
“不喝二次污染的水箱水”之名,自行弃用屋顶水箱。月浦、宝钢、永清、杨泰、宝林等老式居民小区的情况就是如此。

当年这些地区的住宅小区,还可以依靠水厂直接加压解决供水问题。但随着城市规模日益扩大,这种无泵房、无水箱小区直接依靠水厂加压供水的弊端就日益显现。

其实,那些被废除的水箱就在居民楼屋顶,恢复它的功能只需接上进水管即可,难度并不大,但为何一直无法恢复呢?这主要是物业单位“多一事不如少一事”,恢复水箱、泵房需要人力、财力,费用谁来承担?其次,部分居民对物业管理缺乏信心,坚决反对恢复,这也在客观上阻碍了水箱供水方式的恢复。

应该说,水箱容易造成二次污染,但可以靠有效管理来解决。一些业内人士指出,水箱、泵房的恢复,不能就事论事,应该与本市推进二次供水改造的大背景相结合。

本报记者 张欣平 通讯员 喻晓



多媒体还原古代制陶工艺

在上海工程技术大学中韩多媒体设计学院2014年毕业作品展上,林宇丰和邱成凯两名大四学生用多媒体技术完美还原了中国古代制陶工艺的过程。

这项多媒体作品取名“律动青花”:用手轻按触摸屏,眼前的大屏幕上,青花瓷拉坯塑形、烤制、花纹贴图等制作环节一一展现出来。

中韩多媒体设计学院院长唐幼纯表示:本次作品展以“千态万想”为主题,每一幅作品洋溢着千般新意,万种创想。从作品看人才,相信这些学生能成为新媒体时代创新的生力军。

本报记者 张炯强 孙中钦 摄影报道

上海自贸区全面推行预检验制度 进口货物出区“零等待”

本报讯(记者 陈杰)5月1日起,上海出入境检验检疫局在中国(上海)自由贸易试验区范围内全面推行进口货物预检验制度,企业可在货物入境进区或在区仓储时申请预检验,对预检合格的货物实施核销放行,免于检验。该项制度实行后,货物进境通关时间普遍缩短50%以上。

进口货物预检验及核销,是指根据企业申请,检验检疫部门

对区内货物实施集中检验,分批核销出区的工作模式。企业在货物入境进区或在区仓储时申请预检验,即可以由检验检疫机构一次完成检验检疫工作,货物一经检验合格,检验检疫机构将登记预检验合格信息,并签发核销凭证。凭此凭证,预检验合格货物可以免于检验,随时分批出区,直接核销放行。通过预检验及核销制度的实施,可以在自贸区“二线”

严密防范质量安全风险的同时,有效地将刚性的进口现场检验和实验室检测时间前置到货物的在区仓储期间,实现了货物出区时“零等待”和预检验后,货物进境到进口通关的整个流程时间至少缩短50%。进口工业品从7到8个工作日缩短至3到4个工作日,进口化妆品从12个工作日缩短到5个工作日。

上海市经济管理学校
社校联建 和谐发展
www.sems.cn