扬子晚报
报料热线:8530000

“勒索病毒”来了 这次瞄准微信

近日，一种新型的勒索病毒在国内开始传播，该勒索病毒要求受害者使用“微信支付”支付赎金。病毒制作者利用github、CSDN、豆瓣、简书、QQ空间等网站页面作为下发指令的C&C服务器，加密受害者文件并勒索赎金，同时窃取支付宝等软件密码。

据互联网安全专家介绍，该勒索病毒在感染用户计算机后不会勒索比特币，而是弹出微信支付二维码，要求受感染用户使用微信支付110元，从而获得解密密钥，这也是国内首次出现要求使用微信支付的勒索病毒。目前，微信运营商判定该支付二维码存在违规行为，并表示已无法通过扫描二维码支付赎金解密。

截止到12月3日，已有超两万用户感染该病毒，被感染电脑数量还在增长。除了感染电脑中的软件，这次勒索病毒还盯上了包括路由器、智能摄像头在内的智能硬件。

网络安全专家王亮介绍，感染这种勒索病毒之后，用户第一个感觉就是突然自己的桌面背景被人换了，比如说Word文档照片打不开，文件扩展名被修改。

该病毒还窃取用户的各类账户密码，包括淘宝、天猫、阿里旺旺、支付宝、163邮箱、百度云盘、京东、QQ账号。

“不同于其他勒索病毒，此次勒索病毒没有修改文件后缀名。”腾讯电脑管家安全专家称，一经感染，该勒索病毒对用户电脑加密txt、office文档等有价值数据，并在桌面释放一个“你的电脑文件已被加密，点此解密”的快捷方式后，弹出解密教程和收款二维码，最后强迫受害用户通过手机转账缴付解密酬金。

腾讯电脑管家安全专家表示，从多个用户机器提取和后台数据追溯看，该勒索病毒的传播源是一款叫“账号操作 V3.1”的易语言软件，可以直接登录多个QQ账号实现切换管理。

病毒作者首先攻击软件开发者的电脑，感染其用以编程的“易语言”中的一个模块，导致开发者所有使用“易语言”编程的软件均携带该“勒索病毒”。广大用户下载这些“带毒”软件后，就会感染该“勒索病毒”。

12月4日，腾讯方面回应称，已第一时间对所涉勒索病毒作者账户进行封禁、收款二维码予以紧急冻结，微信用户财产和账户安全不受威胁。支付宝安全中心表示，早有针对性的防护，已第一时间跟进，目前没有一例支付宝账户受到影响。

据了解，此勒索病毒已被成功破解，已有相关的安全产品可拦截、查杀。 针对这种新型勒索病毒的攻击，安全专家在此提醒广大用户及时采取五种措施进行防范：

一、安装并及时更新杀毒软件，目前市场主流反病毒软件都已支持针对该勒索病毒的防护与查杀。

二、不要轻易打开来源不明的软件，该勒索病毒通过易语言编写的程序传播，减少使用来源不明的软件可有效预防。

三、如已经感染勒索病毒，可使用相关解密工具尝试解密。目前，许多公司已经针对该勒索病毒开发了解密工具，包括火绒Bcrypt专用解密工具、腾讯电脑管家“文档守护者”、360安全卫士“360解密大师”等。

四、已感染勒索病毒的用户，在清除病毒后，尽快修改淘宝、天猫、支付宝、QQ等敏感平台的密码。

五、定期在不同的存储介质上备份计算机中的重要文件。

（综合新华社、《北京晚报》消息）

至少填埋近8000吨！

化工危险废料如何偷偷“下乡”？

为套取复垦项目资金，村干部默许企业进村掩埋，导致至少近8000吨化工危险废料偷偷“下乡”。“新华视点”记者近期调查发现，江苏泰兴一化工企业将单氯胺废渣偷埋在当地多个村庄，使农地受到严重污染。目前，泰兴市公安局以涉嫌污染环境罪将涉案的30个犯罪嫌疑人移送检察机关审查起诉。

“偷排”。（新华社记者 商海春 制）

“黑土”倒入池塘致鱼死亡，污染土地种树失败

近日，记者来到位于泰兴市张桥镇薛庄村一处危废填埋点。其面积为10亩，上方有塑料布覆盖，四周用铁栏杆圈住。记者看到，当地土壤一般呈现黄色，而这块地的表层土壤呈黑色，用铁锹开挖50厘米深后依然可见“黑土”。

泰兴市公安局一位办案民警介绍，2017年12月份接到群众举报，反映有人借农地复垦的名义偷埋化工废料。经侦查发现，在2017年4月25至7月7日、12月5日至7日两个时间段，泰兴市友联精细化工有限公司委托他人处理该公司的化工废料单氰氨废渣，后者组织人员运输至张桥镇薛庄村五组沟塘内，累计填埋了7997.6吨。

张桥镇郭桥村一王姓村民说，村边高速公路两侧有多个沟塘，2016年以来，村里对其中部分沟塘复垦。当时，他家10亩鱼塘里的鱼还没抓完，就有卡车拉着“黑土”偷偷填入鱼塘里。这些“黑土”刚刚倒入，鱼塘就像煮沸了一样冒气泡，鱼都死了。一些村民怀疑这些“黑土”是从周边化工厂里拉过来的废料。

张桥镇几个村的村民向当地环保、公安等部门多次反映，后来虽然拉过来的“黑土”少了，但是仍有大批建筑垃圾被拉来填埋，直到2017年底，填埋才结束。

根据危险废物鉴别技术规范和危险废物鉴别标准，单氰胺废渣属于危险废物。永清环保股份有限公司总工程师安洪逸告诉记者，单氰胺属于氰化物系列，属于剧毒性物质，在土壤污染里属于比较严重的污染物。当地村民反映，曾在污染地块上种植树木，但未存活。

张桥镇副镇长朱军介绍，除公安已确定的危废填埋点外，另外还有7处沟塘也疑似填埋了单氰氨废渣，目前已委托专业检测机构抽样检测。泰兴市公安局和环保局办案人员介绍，单氰氨废渣填埋总量有待权威机构进一步确认。

非法处置几无成本，村企勾结逃避监管

非法倾倒危险废物的是一家什么企业？友联化工官网显示，该公司主要生产医药及农药中间体。

据警方调查，友联化工监事黄某为解决本公司废渣胀库问题，经法人代表徐某同意后，找到中间人王某两次分别以每吨11.5元和13.5元的处置费，委托处理单氰胺废渣。

正规与违法处置成本之间巨大的差异，是不法分子不惜铤而走险的原因。一家危废处置企业负责人介绍，一吨单氰胺废渣按正规处置成本需数千元，非法填埋则只需要十几元，非法填埋处置与合规处置的成本相差几百倍。仅以查实的7997.6吨计算，能省去两三千万元。

虽然国家对填埋危废有明确规定，但涉事企业与村干部勾结，绕开了监管。“原薛庄村党总支书记印某跟中间人王某有口头协议，默许对方把‘黑土’拉过来填埋。”泰兴市公安局一办案民警介绍，企业表示只要村里同意填埋危废就可出钱，而复垦异地取土困难、成本越来越高，村干部唯利是图，双方一拍即合。

泰兴市国土局工作人员朱鹏介绍，土地复垦项目要求回填的必须是良土，但由于土地复垦项目多，国土人员很难做到全覆盖核查，即使核查也只是看其是否平整，难以监测深层填埋物性质。

后续安全处置面临多重难题，应进一步加强惩处与问责

近年来，一些地方土地整治项目中将建筑垃圾、生活垃圾甚至化工废料回填的事件频发。今年初，原江苏省国土资源厅已发文，要求土地整治项目所需客土，要有相关部门审查合格的鉴定报告，包括客土来源地、土壤成分及土方量等。但仍难以做到全天候监管。

朱鹏认为，针对工业固废“下乡”问题，应进一步提高基层干部环保意识和监管能力，对违法行为坚决惩处和追责。此外，属地政府、环保及国土部门之间应加强协作，发现疑似利用土地整治项目偷倒工业固废等环境污染情况时，需及时互通信息，打击违法违规行为。

据悉，此次偷埋危废事件的后续安全处置，依然面临多重难题。“本地一家有资质的企业年处理量仅有6000多吨，在有限的时间内消纳不了近8000吨危废。”张桥镇党委书记熊亚平说，他已联系了江苏省内三家有资质企业，但都容量接近饱和没有接收，跨省转运处置更为困难。

熊亚平介绍，根据相关要求，张桥镇政府需在今年年底前将上述危废转移暂存完毕，明年3月底前完成处置工作。该镇一级财政难以承受此次危废处置费用，目前只能先向泰兴市政府申请环保公益基金，等后期诉讼时再向涉事企业追偿。

（新华社视点）

相关新闻

近三分之一水体返黑返臭

安徽芜湖黑臭水体整治敷衍被通报

据新华社电 在整治黑臭水体工作中，安徽省芜湖市对部分整改工作敷衍应付、推进不力，上报已完成整治的46条黑臭水体中有15条返黑返臭，近日被中央环保督察通报。

根据中央环保督察通报，2017年9月，安徽省要求芜湖市针对中央环保督察组反馈的问题制定整改方案，但芜湖市直至2018年1月30日才印发市级整改方案。2017年10月以来，芜湖市环境保护督察问题整改工作领导小组未对督察整改工作进行部署调度。2018年11月4日至9日，中央第三生态环境保护督察组对芜湖市集中式饮用水水源地安全保障、入河排污口排查整治、黑臭水体治理以及边督边改等4个方面整改工作进行了下沉督察，发现当地敷衍整改问题突出。

督察组现场检查发现，芜湖市老城区雨污分流不到位、入河排污口排查不全面、截污不彻底，加上城镇生活污水处理厂处理能力严重不足，导致大量生活污水直排水体。芜湖市控源截污不到位导致黑臭水体整治流于表面，多条黑臭水体出现反弹，上报已完成整治的46条黑臭水体中，15条存在返黑返臭现象，其中有9条是因为大量污水入河所致。

中央环保督察通报显示，针对督察中发现的问题，芜湖市党委、政府作为中央环保督察整改第一责任主体，对督察交办问题整改工作重视不够、调度督办不力，导致部分整改任务敷衍应付，没达到预期效果。同时，芜湖市水利、住建、环保等部门责任落实不到位，水利部门入河排污口排查不全面，大量生活废水直排水体；住建部门控源截污、管网建设工作推进不力，黑臭水体整治成效不佳，返黑返臭多发；环保部门工作标准不高、要求不严，导致集中式饮用水水源地问题解决不彻底。芜湖经济技术开发区管委会对群众信访举报问题调查整改不力，敷衍塞责，表面整改。