中国改革报 CHINA REFORM DAILY
2021.12.10 星期五
本版编辑：孟佳惠 Email：crd_xyzhg@163.com 热线：(010)56805187

勒索病毒猖獗 以色列应对有妙招

勒索病毒往往利用一些操作系统漏洞实施攻击，对抗勒索病毒，需要网络安全技术上的创新。目前，以色列在该领域已经做出了有意义的探索。

□ 胡定坤 于紫月

某个周一的早上，一家金融投资公司的首席执行官正为最近的行情欣喜，准备在新的一周大干一场。突然，秘书告诉他公司遭受网络攻击，电脑全部瘫痪，数据都被加密，黑客只留下一封电子信：要想恢复数据，请交巨额赎金，否则公布贵司所有商业机密……这是勒索病毒攻击的典型场景，既能获取敏感信息，又能勒索巨额钱财，不法黑客对其“爱不释手”。

由于特殊的地缘政治环境，以色列是各种网络攻击的重要目标。那么，作为著名的网络技术强国，以色列在应对勒索病毒方面有哪些特殊的妙招呢？

做好备份很重要

今年10月中旬，位于以色列北部城市哈代拉的希勒尔·亚菲医疗中心遭遇勒索病毒袭击，计算机系统瘫痪，几乎所有医疗数据全部丢失，其被迫暂停非紧急就医服务，并向附近医院转移部分患者。然而，也许是未雨绸缪、早有准备，该中心急救、分娩、重要手术等紧急医疗领域预先准备了备份系统，并在一线系统瘫痪后迅速启动，正是这些平时坐“冷板凳”的“替补队员”在关键时刻确保了对紧急就医患者的正常治疗。

网络攻击发生后，以色列卫生部迅速下发通知，要求各医疗机构迅速纸质化打印医疗数据，预防更大规模的新一轮攻击。希勒尔·亚菲中心甚至恢复了纸质处方和人力传递检查影像，一天之内倒退到数十年前。

这次事件是以色列关键基础设施首次被黑客攻陷，给该国敲响了警钟。目前，以色列卫生部已经与美国数据保护软件公司Commvault开展合作，更换和升级卫生机构的备份系统，防止在下一次勒索病毒攻击中再次遭到严重损失。据说，Commvault采用人工智能等技术检测网络攻击，可有效防御勒索病毒、保障数据安全。

防御技术需创新

勒索病毒往往利用一些操作系统漏洞实施攻击，这也是其重要的特征之一。大部分安全软件通过代码扫描方式判断目标程序是否为钻漏洞的恶意程序。不过，这就出现了问题，一旦勒索软件使用了一种刚刚发现的、安全软件未覆盖的新漏洞，则其几乎可以畅通无阻地攻入目标系统。换句话说，常规安全软件可以防御已经出现过的勒索病毒，但很难防御使用新漏洞的新型勒索病毒。

因此，对抗勒索病毒，需要网络安全技术上的创新。目前，以色列在该领域已经做出了有意义的探索。11月17日，2021年以色列国土安全创新科技展会在特拉维夫召开，以色列网络安全企业“密涅瓦实验室”向《科技日报》记者介绍了他们的解决方案。

“密涅瓦”研究人员称，勒索病毒在攻击一个目标前会判断其是否适合自身生存。“密涅瓦”开发的反勒索病毒软件并不检测病毒代码，而是模拟对勒索病毒的不利环境，使其主动放弃攻击。例如，有的勒索病毒会检测目标是否有某些安全工具，如果没有再启动攻击程序，“密涅瓦”软件即可模拟这些病毒不愿看到的东西。

“我们非常了解勒索病毒的运行方式，知道它们不会在哪些环境下攻击，因此可以研制出这种技术。”该研究人员说，“密涅瓦”软件可防御新型、未知的勒索病毒，曾经成功抵挡了著名的永恒之蓝、太阳风等网络攻击。

专业谈判或有益

计算机系统被勒索病毒感染了，到底要不要交赎金？

就像各国警方均反对人质家属向绑匪付赎金一样，以色列、美国等国政府也反对向黑客付钱。原因有二：一是会助长不法分子的嚣张气焰，鼓励其采取进一步攻击行动；二是即使付了赎金，黑客也可能不为你解锁数据，就像绑匪收了钱但“撕票”一样。

但是，很多企业在遭遇勒索病毒攻击时还是会选择破财免灾。例如，今年5月，美国科洛尼尔管道公司就曾向黑客支付了500万美元的赎金。

那么，赎金可以还价吗？答案是可以，而且折扣可能还不小。

以色列NEST谈判公司首席执行官克里斯托透露，该公司承接过不少与黑客谈判的订单，他们既要与黑客玩心理战讨价还价，又要评估这些黑客的口碑和人品如何，是否会出尔反尔，最后给雇主提供解决方案。

不过，这种谈判有时会有“意料之外、情理之中”的结果。克里斯托说：“有一次，经过艰苦磋商，赎金被压到500万，我和雇主说，再给我一天时间，我们可以将赎金谈到400万。但雇主说，早一天结束，他能多赚1000万，所以最后结果是立即付款、停止谈判。”

纽约市要求所有私企员工接种疫苗

美国纽约市长德布拉西奥12月6日宣布，所有私营企业员工须12月27日前接种新冠疫苗，5岁及以上儿童也须在规定日期前接种疫苗，具体细则将于下周发布。图为12月7日，在美国纽约，一名男子走向新冠疫苗接种车。

新华社记者 王 迎 摄

国际观察

陷入“杰利蝾螈”怪圈 “美式”民主引发信任危机

□ 张梦旭

美国近期举行的多场地方选举，被视为明年中期选举的风向标。在这些选举中，美国的“杰利蝾螈”怪象再次被置于媒体聚光灯下。

1812年，美国马萨诸塞州州长杰利为谋求本党利益，签署法案将州内一个选区划成类似蝾螈的极不规则形状。这种做法后被称为“杰利蝾螈”，即通过不公平的选区划分，帮助本党在选举中获得优势，赢得尽可能多的议席。《人民日报》记者了解到，美国宪法和法律规定，各州立法机构有权划分选区，这为州议会多数党搞“杰利蝾螈”提供了操作空间。“杰利蝾螈”主要靠两种操作：一是“集中”，即尽可能将反对党选民集中划入少数特定选区，牺牲这些选区以换取其他选区绝对安全；二是“打散”，即将反对党选民相对集中的地区拆分划入周边不同选区，从而稀释反对党选票。

200多年来，“杰利蝾螈”这一美国特有的政治操作愈演愈烈。无论是民主党还是共和党，在本党控制的州都习惯于利用“杰利蝾螈”操弄选举。今年9月，民主党控制的俄勒冈州在全美率先完成选区重新划分。根据最新人口普查结果，该州可增加1个国会选区，将总选区数增至6个。民主党将这个新增选区设在波特兰市南部，而波特兰恰是该州最大、民主党选民最多的城市。此次重划后，民主党牢牢控制的选区由原来的2个增至4个，“摇摆选区”由2个减至1个，这意味着该党可凭借57%的实际选民占比，控制该州83%的国会选区。

近日，共和党控制的北卡罗来纳州议会敲定该州国会选区划分图，通过将城市中的民主党选民分开，使得该州倾向于共和党的选区数量从8个增加到10个。今年10月，共和党控制的得克萨斯州划分新选区，“巧妙地”将倾向于民主党的少数族裔新增选民划分到白人占主导地位的选区，最终共和党牢牢控制的选区由原来的22个增至24个，“摇摆选区”由原来的6个减为1个，共和党可凭借52.1%的实际选民占比，占据该州65%的国会众议院席位。

“杰利蝾螈”被视为美式民主肌体上的“恶性肿瘤”。美国《纽约时报》指出，几乎每个州都在进行类似的政治把戏，这种扭曲地域和种族属性的选区划分，使得少数族裔的政治影响力日益被淹没。美联社今年3月发布的民调显示，67%的受访民众认为“杰利蝾螈”是美国选举制度中的严重问题。威斯康星州前参议员戴尔·舒尔茨说，“杰利蝾螈”事实上造成议员挑选选民，而不是选民挑选议员。

美国政治极化日益加剧，两党均竭力谋求自身利益最大化，“杰利蝾螈”现象更是积重难返。2019年，民主党控制的众议院曾通过一项法案，要求禁止“杰利蝾螈”，但该法案未在共和党控制的参议院通过。2019年6月，美国最高法院认定“杰利蝾螈”属于政治问题，必须由民选政府部门解决，拒绝再受理此类案件。此后，由于无须担心本州的选区地图会被最高法院推翻，两党操弄“杰利蝾螈”更加肆无忌惮。

“杰利蝾螈”怪象是美式民主痼疾的缩影。“金钱政治”大行其道，权力制衡变成“否决政治”，规则缺陷损害公平正义，制度失灵引发信任危机……“杰利蝾螈”侵蚀美式民主，导致其日益异化、变味、变质。

海外传真

加密货币又曝巨额窃案 黑客盗取近两亿美元

本报讯 据美国消费者新闻与商业频道网站报道，一家网络安全公司日前表示，黑客从加密货币交易平台Bitmart盗取了1.96亿美元。据全球化数字货币交易平台币虎提供的数据显示，Bitmart是提供即期交易、杠杆期货交易以及贷款等服务的交易平台，按交易量计算是顶级集中加密交易平台之一。

报道称，Bitmart于12月4日晚间发表官方声明证实了黑客入侵事件，称这是“一次大规模安全攻击事件”，黑客提取了价值约1.5亿美元的资产。然而，区块链安全和数据分析公司派盾公司估计损失接近2亿美元。

据悉，派盾公司是最早注意到黑客攻击事件的机构。该公司指出，Bitmart提供的一个地址显示，数千万美元源源不断地流向一个被以太坊浏览器标记为“Bitmart黑客”的地址。据派盾公司估计，Bitmart在以太坊区块链上的各种加密货币损失了约1亿美元，在币安智能链上的加密货币损失了9600万美元。黑客盗取了20多种加密货币，包括币安币、“安全月亮”数字货币和柴犬币。

Bitmart方面表示，受影响的以太币和币安币“热钱包”只是该交易平台资产的“一小部分”，其他所有钱包都“安然无恙”。据了解，加密货币的持有者可以用“热”“冷”或两者兼有的方式将其储存起来。热钱包与互联网相连，客户可以相对容易地获取并使用加密货币，但方便的代价是风险较高。

Bitmart说，目前尚不清楚黑客使用了哪些方法，但据派盾公司表示，在入侵之后发生的事情简单明了：这是一起“提取、交换、清洗”的典型案例。网络威胁情报公司“数字影子”首席信息安全官里克·霍兰说，网络犯罪分子往往针对提供混合服务的平台。在这种平台上，用户可以将非法资金与干净的加密货币相结合，创造出一种新的加密货币，然后进行加密货币交换。尽管区块链是公开的，但黑客仍有办法让调查人员难以追踪到交易的最终去向。 （许 参）

秘鲁卫生部将开发应用程序 以核实疫苗接种卡真伪

本报讯 据秘鲁《公言报》12月6日报道，秘鲁卫生部报告说，正在开发一个应用程序，以验证民众出示的新冠疫苗接种卡的真伪，该程序会在未来几天内投入使用。

由于秘鲁政府将从12月10日开始要求18岁以上民众，出示“疫苗接种卡”才能进入封闭的公共场所，首都利马近来出现了一些出售伪造疫苗接种卡的团体。为此，卫生部已经推出了一款应用程序“疫苗接种卡”，民众可以在安卓或苹果手机的应用商店下载该程序，并用身份证登录，程序将生成一个二维码，以证明疫苗接种卡的真伪。

据报道，“疫苗接种卡”的验证工作将通过二维码或查看数字身份证上的照片来完成，这个工具将使核查过程更快。卫生部强调，该应用程序将对每个人的数据进行保密，对于了解相关人员是否接种了两剂疫苗至关重要。同时，只有在员工证明他们已经完全接种了新冠疫苗的情况下，公司才能允许他们回公司上班。另外，所有公共交通服务的司机和收款员，以及提供送货服务的人，只有在能够证明他们已经完全接种疫苗的情况下，才会被允许工作。

截至当地时间12月6日，秘鲁有超过573万人尚未接种任何剂量的新冠疫苗，这一数字约占目标人口的20%。未接种疫苗人数最多的年龄组分别为，12岁~16岁、20岁~29岁以及30岁~39岁。

秘鲁卫生部长塞瓦略斯表示，相信政府能够实现年底前，为免疫目标人口的80%接种新冠疫苗的目标。他还强调，接种新冠疫苗能够预防重症和死亡，是最好的保护，并呼吁继续遵守预防措施，如勤戴口罩，保持社交安全距离，避免前往拥挤的场所。 （甘 甜）

或因留学生倒卖免税品 日本拟不再允许留学生免税购物

本报讯 据日本共同社报道，12月5日，针对访日外国人的消费税免税制度，日本政府和执政党决定，外国留学生等长期逗留的人，将不再允许免税购物。

报道称，由于确认留学生是否为可免税对象人群的作业繁琐，且留学生倒卖免税品的行为泛滥，日本将在2022年度税制修改时，调整该制度，以改善这种情况。

具体做法是，将至今外汇法规定的只要是“非居住者”就可免税购物的条件，缩小为在留资格90天以内“短期逗留”的游客等。

据报道，2020年4月，日本国税厅采用了顾客信息电子化机制，发现许多留学生存在可疑的“爆买”现象。其原因可能是留学生大量购买免税品，再以含消费税的价格倒卖，赚取差价。

根据现行制度，长期逗留的留学生除有兼职者之外，允许在入境半年内，免税购物。免税店在销售时，需确认留学生是否在打工，要花费许多人力，因此有意见要求改善。此外，不认真确认的店铺更受欢迎，也有人对这种不公平现象表示不满。

另外，报道称，因新冠新变异病毒奥密克戎变异株的出现，目前无法预测日本何时重新接纳访日游客，但为迎接旅游需求的恢复期，日本将调整制度以助于妥善运用。

（邢晓婧）

社址：北京市西城区月坛南街59号（邮政编码100045） 值班电话(010)56805051 广告发行部(010)56805116 广告经营许可证：京大工商广登字20180001号 零售价2.00元 印刷单位：经济日报印刷厂（地址：北京市西城区白纸坊东街2号）