中国改革报 CHINA REFORM DAILY
2021.06.11 星期五
本版编辑：孟佳惠 Email：crd_xyzhg@163.com 热线：(010)56805187

数字时代 应对“勒索软件”攻击长路漫漫

没人愿意接到收税员的电话。

作为时任美国国防部长，唐纳德·拉姆斯菲尔德(Donald Rumsfeld)监管的预算比一个典型国家的经济规模还要大。尽管如此，他还是觉得这些规定太让人困惑了，以至于他每年都会写信给美国国税局，抱怨自己“不知道”自己的税收申报是否正确。因此，当电话铃响起，一个官方声音说你少缴了税款，要求您支付余款时，普通百姓无不心惊胆战。

然而，这往往是骗局。

新技术“外衣”使老式犯罪更容易实施

事实上，税务机关很少会向个人致电询问他们的纳税情况。他们顶多会在一年后寄给你一封信，通知你税款缴纳不足。而且他们也绝对不会像虚假电话中那样威胁你，“如果你不马上补缴就会被逮捕”。

近年来，类似的骗局已经变得非常普遍。据英国银行业协会(uk Finance)的数据显示，2020年冒充税务人员进行电信诈骗的案件数量比2019年同期翻了一倍。与此同时，其他国家的增长率也同样惊人。

尽管发达国家的犯罪率仍然处于较低水平，但电信诈骗案件的增长率却格外引人注目。根据英格兰和威尔士犯罪调查(the Crime Survey of England and Wales)显示，2019年，英国共发生了380万起欺诈事件，其中，电信诈骗案件占1/3，15%的受害者损失超过1000英镑。据悉，自2017年英国政府开始收集数据以来，这一数字每年都在增长。在美国，2020年电信诈骗案件数量同比增长了69%，损失(不包括银行或信用卡欺诈)高达42亿美元，是2017年的3倍。

其他类型的互联网犯罪也在逐年增长。据悉，犯罪分子每年通过垃圾邮件和短信实施诈骗，可以获利数十亿美元。

新技术使得许多老式犯罪更易实施。毒品贩子使用比特币来接受支付和转移资金，同时，他们还依靠专门的犯罪加密通信软件来组织犯罪。英国国家犯罪局(NCA)的奈杰尔·利里(Nigel Leary)表示，“没有什么严重的有组织的犯罪是没有互联网成分的。”

黑客攻击成网络安全最大威胁

在过去的一年里，“勒索软件”的增长显著。“勒索软件”是一种野蛮的黑客攻击，受害者的个人文件会被锁起来，直到付款为止。过去，“勒索软件”往往出现在垃圾邮件中，目标则是普通人群，为了鼓励人们付款，勒索的金额通常很小。

现如今，黑客们把注意力集中在大型组织上，并索要巨额赎金。恶意软件侵入特定的计算机系统，在锁定数据之前先窃取数据。随后，黑客会索要赎金用于解锁文件，甚至提高赎金数额以防止文件泄露。

黑客勒索的赎金几乎都是用比特币进行支付。网络安全公司Chain analysis表示，与2019年相比，2020年用比特币支付的赎金增加了311%，达到3.5亿美元。受害者以企业为主，也包括政府部门、甚至警察系统。4月27日，华盛顿特区的一名警察透露，他们的系统遭到了黑客的攻击，黑客表示，如果当局不支付赎金，他们将把警方的线人暴露给犯罪团伙。

欧洲刑警组织顾问、苏塞克斯大学(University of Sussex)计算机科学家艾伦·伍德沃德(Alan Woodward)表示，“勒索软件”是网络安全的最大威胁。美国国土安全部部长亚历杭德罗·马约卡斯(Alejandro Mayorkas)也将其描述为“对国家安全的威胁”。

据悉，全球航运公司马士基(Maersk)在2017年的一次“勒索软件”攻击中支付了3亿美元的高额赎金。英国外汇交易商通济纳(Travelex)去年陷入财务危机，裁员1300人。该公司将大部分原因归咎于2019年的一次黑客袭击。2019年底，该公司在“勒索软件”攻击下系统瘫痪，支付了285个比特币(当时价值约230万美元)作为赎金，这直接导致了通济纳在该季度损失了约2500万英镑。

有时，赎金甚至会高得难以想象。今年3月，佛罗里达州布劳沃德县(Broward County)的学校系统遭到“勒索软件”攻击，要求支付4000万美元的比特币。该地区的一名谈判代表对黑客的要求表示不可置信，“你怎么会认为我们支付得起如此高昂的赎金?”

大多数政府机构都不会向黑客支付赎金，但随之而来的后果可能同样昂贵。去年，在马里兰州巴尔的摩县(Baltimore County)，由于系统遭到“勒索软件”攻击，学校不得不停止在线教学一周。2019年，邻近的巴尔的摩市(City of Baltimore)市政系统遭遇袭击，纳税人为此损失了1800万美元。在新冠肺炎疫情期间，医院系统也受到了黑客攻击。法国去年报道了27起针对医院系统的黑客攻击事件，在德国和美国，也由于黑客攻击，导致医疗一度被推迟。

加密货币为“洗钱”提供“捷径”

从事黑客攻击的犯罪分子鱼龙混杂，很难彻查。许多犯罪团伙似乎位于俄罗斯、中东欧等地区。据报道，一些黑客组织与国家安全部门有隐秘的联系。

但从事黑客攻击的犯罪团伙似乎并不像贩毒集团或黑手党那样是组织严密的犯罪集团。他们的力量分散且隐蔽，每次案件的个别要素都是作为一种服务提供给组织者，有人负责编写和销售“勒索软件”，有人负责将其侵入目标的计算机中，还有一部分人负责收集赎金并参与“洗钱”，一些重要人物可能会资助并组织整个行动。然而，他们彼此之间可能永远不知道对方的名字或地点。

奈杰尔·利里说，像银行抢劫这样的犯罪已经是过去式了。1983年的Brink’s Mat劫案，6名劫匪从伦敦希思罗机场的仓库里偷走价值260万英镑(约合380万美元)的黄金、钻石和黄金，像这样的大型劫案需要作案团伙成员之间相互认识并彼此信任。目前，大规模犯罪正被科技“工业化”。奈杰尔·利里表示，“进入门槛真的非常低。”

事实上，加密货币的诞生在很大程度上为犯罪分子“洗钱”提供了“捷径”。微软数字犯罪部门律师肯巴·瓦尔登(Kemba Walden)表示，“勒索软件”犯罪分子喜欢使用比特币，因为比特币流动性和匿名性较好。犯罪分子可以在匿名的情况下进行比特币交易。

犯罪分子将收益变现存在一定风险，因为在大多数发达国家，比特币交易所实行严格的“客户识别”制度，但这也并非完全不可能。一些监管较少的国家的比特币交易所采用的标准相对宽松，犯罪分子可以进行比特币“大幅”交换，以隐藏其来源，然后在监管良好的交易所进行出售。

除加密货币之外，其他技术创新也为网络电信诈骗提供了滋长的温床。例如，可隐藏电话来源的simbox主要用于市场营销，但在犯罪分子别有用心地利用之下，它成为发送垃圾邮件或短信的工具；Tor是一款通过在世界各地收集数据来匿名化互联网连接的软件，它让“暗网”蓬勃发展，并为犯罪分子提供了论坛，让他们可以在上面匿名交易他们的产品；“防弹托管”服务器具有高度的安全性和私密性，就像“虚拟安全屋”一样运作，在那里，犯罪信息总是能够在警察到达之前被瞬间转移。

随着“勒索软件”的蔓延，各行业都在积极防范，发挥技术优势，遏制电信诈骗犯罪。卡迪夫大学(Cardiff University)的迈克尔·列维(Michael Levi)说，由于马士基公司(Maersk)遭遇的袭击，这种犯罪行为“变得更加引人注目”，各组织正试图加强防御。然而，一些公司不愿公开其被黑客欺诈的事实，原因是数据泄露对公司的信誉也会造成不可估量的损失。

警方担心更多的传统犯罪转向网络犯罪。奈杰尔·利里表示，“现在，‘暗网’常被用于赃物交易、毒品交易和枪支交易。”在3月份的一次突袭中，比利时警方缴获了28吨可卡因，以及现金、枪支、警服和一个集装箱中的凶器。据报道，犯罪分子一直在使用Skyecc进行联络，这是一家加拿大公司出售的加密电话设备。这些设备似乎是专门为了隐藏犯罪活动而设计的，端口的加密、匿名的信息且无GPS定位。在欧洲警察设法将监视软件注入设备前，这些设备给犯罪团伙带来了极大的匿名保护。

近年来，各国政府开始重视网络犯罪。美国司法部已经指派了一个小组来处理“勒索软件”攻击。“五眼”盟友——美国、澳大利亚、英国、加拿大和新西兰——正在分享这方面的情报，但仍任重道远。据《泰晤士报》报道，根据《信息自由法案》(Freedom of Information Act)披露的数据显示，在英国，尽管电信欺诈影响恶劣，但每200名警察中只有1名关注欺诈行为。

在过去的6个月里，全球比特币的价值飙升至1万亿美元以上，流动性的激增使得隐藏犯罪似乎变得更加容易。正如伍德沃德所言，“如果可以选择，你为什么要拿着一把锯掉的猎枪走进一家银行去抢3万英镑，而不是通过暗网发起‘勒索软件’攻击敲诈数百万英镑呢?”

（本文出处：《Tte Economist》2021年5月8日刊 孟佳惠/译）

德国首家华为旗舰店在柏林开业

中国华为公司德国首家旗舰店日前在柏林开业，这是华为在欧洲地区营业的第五家旗舰店。图为在德国首都柏林拍摄的华为旗舰店一角。

新华社记者 单宇琦 摄

评 论

网络袭击频发 企业发展需筑牢安全“防火墙”

□ 郭言

5月，全球范围内接连发生两起影响较大的黑客袭击事件，产生很大的影响。袭击事件频发凸显全球网络安全所面临的严峻挑战。

5月底，全球销售额最大的肉制品加工企业，总部位于巴西的JBS遭遇勒索软件攻击，导致其美国牛肉和猪肉加工厂大部分关停，澳大利亚业务在5月31日关闭，北美和澳大利亚的肉类生产中断，出现消费者抢购现象，肉类供应压力加大。

此前，美国最大的燃料管道公司科洛尼尔遭到黑客攻击，导致美国东南部地区的燃料输送瘫痪数日，一度进入国家紧急状态。

这两起案件只是全球网络攻击案件的冰山一角。据英国一家IT管理公司的统计，仅2021年5月，全球发生的网络数据泄露和网络攻击案件的记录就高达1.16亿条，高于4月份的1亿条，其中40%由勒索软件引发。

美国坦普尔大学发起的“关键基础设施勒索软件攻击”数据库追踪数据显示，近几年全球这一类案件快速增长。2019年~2020年针对关键基础设施的网络勒索案件占过去7年多此类案件报告总数的一半以上，其中政府设施、医疗设施和教育部门遭网络勒索的频次列前三位。

只要仔细梳理就能发现行业巨头被黑客攻击带来的巨大负面影响。科洛尼尔公司运营的燃油管道长达5500英里，主要将汽油和其他燃料从得克萨斯州运往东北部地区，其所提供的燃油约占东海岸燃料消耗总量的45%。黑客攻击造成该公司向美国东部沿海各州供油的关键燃油网络被迫关闭近一周，影响约5000万人。东芝在被勒索软件攻击后，黑客组织声称其窃取的数据超过740GB，内容涉及管理信息、新业务以及个人数据。JBS公司服务器遭黑客攻击，导致其美国和澳大利亚部分工厂暂停作业。因其产品出口到150多个国家和地区，如此大面积停产，或将让刚刚走出疫情阴霾的全球肉类供应链再次遭受严重冲击。

伴随企业智能化、数字化、物联网进程加速，本应防范能力更强、技术水平更高的企业网络安全，为何如此“不堪一击”?

如今，人类已经步入数字化时代，随着关键基础设施的数字化程度不断提高，越来越多的服务通过网络提供，越来越多的企业正在把业务迁移到云中，人类对网络的依赖性正在加大。与此同时，对信息安全的重视却要滞后于数字服务的采用，这种落差造成数字业务系统的脆弱性增加，导致网络攻击和数据泄露事件越来越多。

科学技术水平日益发达的今天，无论是企业还是个人，面临的网络安全环境也愈发复杂。研究表明，软件漏洞是病毒渗透企业防御体系的重要突破口，而传统的防御手段存在防护空窗期，给关乎企业根本利益的核心数据再加一层保险至关重要。如今，网络漏洞和攻击方式层出不穷，光靠“封堵查杀”的传统手段已难以应对。因此，定期进行安全预警，并制定专门的响应策略必不可少。

安全是发展的前提，发展是安全的保障。构建并确保安全的网络环境，不仅需要基础设施、核心技术、社会管理和法律治理等系统“升级”，还需要人才的加持。筑牢安全屏障有了这些整体支撑，发展才能在安全“防火墙”的庇护下行稳致远。

海外传真

滥用广告领域支配地位 谷歌在法国被罚2.2亿欧元

本报讯 据外媒报道，法国竞争事务监管机构日前宣布，因美国谷歌公司滥用在网络广告市场的支配地位，对其开出2.2亿欧元的罚单。分析指出，这意味着该搜索引擎巨头将审视其用以进行数字广告业务的服务平台，法国的这一处罚还可能对全球其他监管机构正在对谷歌进行的相关调查和法律诉讼产生影响。

法国竞争管理局表示，谷歌凭借其市场支配地位，以多种方式在网络广告领域进行不公平竞争，其行为损害了竞争对手以及移动网络和应用开发商的利益。法国竞争管理局的负责人伊莎贝尔·德席尔瓦表示，此次处罚深入考虑了谷歌网络广告业务算法的复杂性。此次处罚以及谷歌调整相关业务的承诺将使为所有市场参与者建立公平竞争环境以及令所有开发商从其广告空间中获取最大利益成为可能。

这一处罚决定是对三家传媒企业所提投诉的处理结果。新闻集团、法国《费加罗报》和比利时罗塞尔集团投诉说，谷歌不正当竞争，令它们出售旗下网站和手机应用程序上广告位的收入蒙受损失。

法新社报道称，这笔罚款对谷歌不过是“小意思”，谷歌今年一季度收入553亿美元，主要就来自网络广告销售。

有法律人士表示，这项处罚可能将为其他正在审视谷歌市场垄断地位的监管机构提供解决方案的样本。据了解，美国司法部以及一些州去年都对谷歌提起了反垄断调查，审视其是否损害了消费者和广告商的利益。德国竞争监管机构上周表示，正在调查谷歌去年秋季推出的广告授权平台是否包含不合理的条款。 （言 阙）

新加坡总统签字批准国家重大建设借贷法令

本报讯 6月7日，新加坡总统哈莉玛签字批准新加坡国家重大建设借贷法令。她表示，政府的借贷将设有足够保障措施，以确保借贷可持续，未来新加坡不会因此承担过重的融资成本。

据了解，新加坡国家重大建设借贷法令将允许新加坡政府发行债券资助该国主要及长期基础设施建设。相关法案上个月初在新加坡国会三读通过。此次，总统签字批准，将使法令正式生效。

在新法令下，新加坡政府借贷设有保障措施，包括发债规模限额为900亿新元，发债所得资金也只能用以资助新加坡长期发展和可持续项目，例如，地铁建设和应对海平面上升的基础设施等。

哈莉玛指出，为国家融资提供这一保障是非常重要的，可以缓解因借贷而动用国家储备金的风险。她表示，这是她批准法令生效最重要的原因。

（孙牧宁）

欧盟委员会提议推出“数字身份钱包”加强数字服务

本报讯 欧盟委员会日前提议为欧盟成员国居民和企业提供“数字身份钱包”，以加强数字服务。

欧盟委员会表示，用户可在“数字身份钱包”中存储和管理个人身份数据，并通过“数字身份钱包”关联驾照、文凭、医疗处方、银行账户等信息。

欧盟委员会说，用户可使用“数字身份钱包”进入网络银行、申请贷款、提交纳税证明以及办理欧盟范围内的高校注册入学等。另外，“数字身份钱包”还可用于办理机场登机手续、租车等服务。

用户可自主决定通过“数字身份钱包”分享哪些个人信息，不必担心与相关在线服务无关的个人信息泄露。

根据欧盟委员会提出的方案，欧盟不会强制要求成员国居民和企业使用“数字身份钱包”，但提供在线服务的私营或公共机构必须接受“数字身份钱包”。

欧盟委员会计划与各成员国进一步商讨这一方案，争取尽快就技术细节达成一致并开始试点。按照欧盟相关规定，方案需获得所有成员国批准。

（邵 莉）

本报社址：北京市亦庄地盛西路6号中改传媒大厦 邮政编码100176 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 本报照排 经济日报印刷厂印刷