2021年7月9日 星期五
责编 华卫 E—mail:aqwbss@126.com
安庆晚报

勒索软件威胁有何新特点

更多地针对高价值目标、逐渐形成网络犯罪“产业链”等

新华社北京7月8日电 近日美国软件企业卡西亚公司遭勒索软件攻击，其客户企业中有800家至1500家受波及。今年以来，全球勒索软件攻击有愈演愈烈之势，给经济和社会生活造成严重损失，已成为网络安全主流威胁之一。

勒索软件攻击自20世纪80年代末出现，其攻击模式不断发展演化，呈现新的特点和趋势，包括更多地针对高价值目标、负面影响扩大、逐渐形成网络犯罪“产业链”、越来越多地采用双重勒索策略等。

锁定高价目标

近几个月来，全球发生多起重大勒索软件攻击事件。这些勒索软件攻击案有一定相似性，它们都锁定高价值的关键资产并有针对性地发起攻击，索要的赎金数额巨大，造成广泛负面影响。

5月初，美国科洛尼尔管道运输公司遭勒索软件攻击，一条输油干线被迫关停数日，导致美国多个州和地区一度面临燃油供应危机。美国联邦调查局称，一个名为“黑暗面”的网络犯罪团伙是幕后黑手。为尽快恢复系统，科洛尼尔公司以比特币方式向黑客支付价值近500万美元赎金。部分赎金后来由美国司法部追回。

5月中旬，爱尔兰卫生服务执行局网络系统遭黑客攻击，造成全国多家医院的电子信息系统无法进入。爱尔兰公共支出与改革部负责政府电子政务的国务部长奥西安·史密斯表示，对卫生服务执行局网络系统的攻击也许是该国迄今遭受的最严重网络攻击。攻击者是来自国外的网络犯罪团伙，其目的是为了钱。

5月底，世界肉类加工巨头JBS公司受到黑客攻击，其北美和澳大利亚的信息系统被“黑”，部分工厂瘫痪。一个名为“邪恶”的黑客团伙被指认为幕后黑手。该公司美国分部发布声明证实，已向黑客支付相当于1100万美元的赎金，以结束对公司业务的攻击。

最新遭到攻击的卡西亚公司是一家向IT外包公司提供软件的企业。该公司首席执行官弗雷德·沃科拉对媒体表示，最多有1500家客户企业受波及，而这些客户企业的下游用户所受影响还难以确切估计。英国牛津大学网络安全教授夏兰·马丁认为，这种“供应链袭击”以服务数千家下游企业的公司为目标，受害企业总数可能巨大。

美国媒体称，这起攻击同样与“邪恶”黑客团伙有关，该团伙在其暗网网站上提出，卡西亚公司可以用7000万美元加密货币赎金换取解除故障的通用解密器。目前该公司拒绝透露是否打算与黑客谈判或支付赎金等事项。

对高价值目标的定向攻击是随着实体经济的信息化程度不断提升而出现的。据中国安天科技集团首席技术架构师肖新光介绍，较早的勒索软件主要是非定向传播的、带有数据加密和删除功能的蠕虫病毒，依靠网络或U盘大面积感染计算机，勒索赎金额度较低。此后，勒索攻击与高级持续性威胁攻击相结合，演化出针对高价值目标的定向勒索。

勒索模式进化

网络勒索高发、威胁升级的一个重要原因是网络犯罪生态系统的形成发展。美国媒体报道，勒索软件攻击如今演化为“高度分工合作的行业”，由勒索软件供应商、赎金谈判人员、攻击执行人员及话务员等组成。肖新光介绍，在网络勒索“产业链”上，一般上游团伙编写勒索软件并提供攻击设施，下游团伙负责实施攻击，上下游“分享”赎金。

据媒体报道，“邪恶”和“黑暗面”均采取名为“勒索软件即服务”的作案模式。它们向其附属团伙提供勒索软件和相关设施，并从附属团伙所获的赎金中抽成。加密追踪企业英国埃利普蒂克公司联合创始人汤姆·鲁宾逊说，从美国政府缴获的比特币可以看出“黑暗面”与其合作伙伴的分赃比例。

在攻击模式上，上述两个黑客团伙都使用渐成主流趋势的“双重勒索”策略：黑客首先窃取存储在受害者系统内的敏感信息，然后对这些敏感数据加密，并要求以赎金换取密钥；勒索者还会发出额外威胁：如果勒索目标拒绝支付赎金，他们就在网上公布窃取的数据。这意味着无论受害者是否预先备份了数据，都可能被迫支付赎金。

中国瑞星公司6月发布的《瑞星防勒索指南》认为，这种“复合勒索”使受害企业既面临隐私数据泄露，还面临相关法规、财务和声誉受损等多重风险。

由于网络勒索多为跨国、跨境作案并具有在网络空间难以追踪等特性，取证和执法面临诸多挑战。欧洲刑警组织去年10月发布报告建议，为了更有效应对网络犯罪挑战，应通过公共部门和私人伙伴之间的协调与合作加强信息共享，增强防范意识和防御能力建设，同时让多边协作机制继续在打击网络犯罪领域发挥关键作用。

南非前总统祖马向警方投案

南非警方7月7日说，前总统祖马当天深夜已向警方投案。2018年2月，时任南非总统祖马宣布辞职，时任副总统拉马福萨成为总统。目前，祖马因涉嫌收受贿赂、洗钱等多项罪名接受调查。

这是7月4日，南非前总统祖马的支持者聚集在祖马位于夸祖卢-纳塔尔省恩坎德拉的家附近。

新华社发

美国救援人员停止搜寻楼房倒塌事故幸存者

事故已致54人死亡86人失联

新华社华盛顿7月7日电 美国佛罗里达州迈阿密-戴德县消防局官员7日表示，鉴于无望找到幸存者，救援人员已停止在该县瑟夫赛德镇坍塌住宅楼废墟中搜寻幸存者的工作。目前，该事故已致54人死亡、86人失联。

据多家美国媒体报道，该县消防局助理局长拉伊德·贾达拉当天下午在一场闭门会议上告知相关家属，基于当前事实，救援人员认为已无希望找到幸存者，将不再使用搜救犬和探测设备搜寻生还者，但会继续找寻被废墟掩埋的遇难者遗体。据报道，在场家属闻讯后泪流满面。

迈阿密-戴德县县长丹妮拉·卡瓦在当晚举行的发布会上说，向失联人员家属通告停止搜寻幸存者的消息“令人痛心”。卡瓦说，事故造成的死亡人数已升至54人，其中33人的身份已得到确认，仍有86人失联。

据美国有线电视新闻网报道，7日下午，一批幸免于难的坍塌楼房住户在警方护送下前往事故现场，接受心理咨询服务。其中一名老年女性住户表示，自己很伤心，但还是想回到曾经的家看看。

事故的调查和追责工作已经展开。佛罗里达州律师协会下属不动产、遗嘱认证及信托法科6日发表声明说，该科已组建工作组，审查该州与住宅楼开发相关的监管法律。迈阿密-戴德县检察官凯瑟琳·伦德尔7日发表声明说，已指派一个大陪审团调查塌楼事故原因。

6月24日凌晨，滨海小镇瑟夫赛德的一栋12层住宅楼发生局部坍塌。事故楼房共有136套住房，其中55套在坍塌中损毁。事故救援工作已持续近两周，而自坍塌发生一小时后迄今，救援人员没有找到任何幸存者。

马来西亚执政联盟最大成员党宣布撤回对总理穆希丁的支持

新华社吉隆坡7月8日电 马来西亚总理穆希丁所领导执政联盟中的最大成员党马来西亚民族统一机构（巫统）8日宣布，立即撤回对穆希丁的支持，要求他辞去总理职务。

巫统主席扎希德8日凌晨在巫统最高理事会会议后召开新闻发布会表示，穆希丁政府未能有效应对新冠肺炎疫情，此外还存在其他执政失败之处，巫统决定立即撤回对穆希丁的支持。

扎希德敦促穆希丁辞职，以便产生一名新总理。后者的任务是应对疫情、推动新冠疫苗接种，并在达到群体免疫后立即建议最高元首举行大选，以选出一个稳定的政府。

穆希丁去年3月出任马来西亚总理，接替此前突然辞去总理职务的马哈蒂尔。但穆希丁领导的多党执政联盟在国会下议院所掌握的过半数优势较微弱。

巫统共有38名国会下议院议员，自去年3月以来已多次与穆希丁领导的土著团结党发生摩擦。7日早些时候，穆希丁任命国防部长伊斯梅尔·萨布里为副总理、外交部长希沙姆丁为高级部长，两人均为巫统成员。