

勒索软件对科技信息安全的影响研究

丁梅, 柳丹, 彭洋

(湖北省科技信息研究院, 湖北 武汉 430071)

摘要: 在国家促进数据安全产业发展的新环境下, 科技信息在其数字化转型过程中面临勒索软件的威胁。从科技信息管理者角度分析勒索软件攻击科技信息的成因, 以及造成的区别于以往安全威胁的后果。依据数据安全与网络安全的相关理论和技术, 分析被勒索软件 Mallox 攻击过程中产生的 28 597 条相关日志数据和 121 539 个被加密文件, 从而了解 Mallox 的攻击及加密流程, 提出预防勒索软件的方法: 自查向互联网开放的服务和网络安全策略, 评估服务器被入侵的风险; 在日常监测中关注 ID 4625 的日志数量和安全设备日志, 可识别攻击过程; 采用异地存储备份、部署 EDR 服务、使用 VPN 等方式提高科技信息的安全性。

关键词: 数据安全; 勒索软件; 科技信息; 信息安全; 异地备份

DOI: 10.11907/rjdk.231553

中图分类号: TP309

文献标识码: A

开放科学(资源服务)标识码(OSID):

文章编号: 1672-7800(2024)006-0121-07



Research of Ransomware Threats to the Security of Scientific and Technological Information

DING Mei, LIU Dan, PENG Yang

(Hubei Academy of Scientific and Technical Information, Wuhan 430071, China)

Abstract: In the new environment in which the country promotes the development of data security industry, scientific and technological intelligence has to face the threat of ransomware in its process of digital transformation. This paper analyzes the causes of ransomware attacking scientific and technological information from an angle of its administrators. To understand the encryption process, using the theories and technologies of both data security and network security, this paper analyzes 28 597 log data and 121 539 encrypted files which were generated by the ransomware Mallox during its intrusion and brings up methods to avoid Mallox: self-inspection could assess the risk of a server being infected by Mallox through its services and network security strategies. It's suggested to pay attention to the number of ID 4625 logs, and the logs of safety devices in daily monitoring. Administrators can enhance the security of scientific and technological intelligence information by storing backup data in other places, deploying EDR services, and using VPN.

Key Words: data security; ransomware; scientific and technological information; information security; remote backup

1 研究背景

2023年1月13日, 国家工业与信息化部等16部门下发了《关于促进数据安全产业发展的指导意见》中指出: 提升基础软硬件数据安全水平, 推动数据安全产品与基础软硬件的适配发展, 增强数据安全内生能力^[1]。与其他种类的信息不同, 科技信息具有基础性, 是全民科普和信息公

开的基础; 科技信息具有开放性, 是助力产业提升的手段; 科技情报产品具有针对性, 可精细化、专业地面向重点行业领域。杨锐等^[2]以数据驱动环境下的科技信息知识服务研究模式变革为出发点, 提出融合科技数据资源治理大中台与知识服务小前台的敏捷化大数据建设思路和整体框架, 为开展支撑决策的科技信息知识服务提供有效支持, 并为科技信息知识服务创新和迭代赋能提供参考。刘细文^[3]认为, 在数字化、智能化时代, 需要进一步认识科技

收稿日期: 2023-05-26

基金项目: 湖北省软科学研究计划项目(2023EDA006)

作者简介: 丁梅(1983-), 女, 硕士, 湖北省科技信息研究院高级工程师, 研究方向为科技信息管理、网络安全; 柳丹(1980-), 女, 硕士, 湖北省科技信息研究院助理研究员, 研究方向为科技信息管理、科技政策; 彭洋(1983-), 男, 湖北省科技信息研究院助理研究员, 研究方向为科技信息管理、大数据管理。本文通讯作者: 柳丹。

信息资源的重要性,理解科技信息资源的内涵与价值,构建新型学术信息生态,强化学术信息资源的安全治理。

深信服科技发布的《2023年网络安全状况特点及2024年趋势研判》报告称,2023年我国遭受恶意软件攻击总次数达到了281.4亿次,相比2022年的246.3亿次增长了14.3%^[4]。在奇安信行业安全研究中心记录的2023年发生的206起造成重大破坏或严重损失的勒索病毒攻击典型事件中,各类政企机构共有1485台设备感染。由此可见,政府由于数据重要和经济能力较好,已成为勒索团队的重点攻击目标,形成了高级持续性威胁(Advanced Persistent Threat, APT)+勒索软件的复合型攻击。董昱宏等^[5]以WannaCry为样本分析其功能结构与具体工作原理,归纳总结了可行的一般性防范措施,如数据冗余、安全策略、黑白名单策略、动态与静态检测技术等。蔡琴^[6]在分析了WannaCry的传播特点、传播方式和危害性后认为,为避免勒索病毒的侵害,应禁止重要服务器访问外网,并将保存有重要数据的服务器用内网隔离。刘文静等^[7]提出一种基于深度学习的勒索软件早期检测方法,其能够在一个软件运行后数秒内准确判定其是勒索软件还是良性软件。

在以上研究的基础上,本文从科技信息向公众服务的特点出发,针对近年持续流行的Mallox勒索软件对科技信息安全造成的影响进行定量分析,对Mallox针对政企目标、多渠道的入侵机制、混合加解密算法等方面进行研究,最后结合软硬件发展情况提出可行的事前预防措施,也探讨了解密的可行性。

2 科技信息安全现状

科技信息种类繁多,数据结构复杂,关联性强。以湖北省科技信息共享服务平台的数据为例,PDF类型的文件占94.38%,其次是CAJ文件占4.72%,其他类型文件还包括JPG、PNG等图片和XML数据。从信息管理的角度看,科技信息可分为科技信息元数据和文件本身^[8]。从数据库管理的角度看,科技信息本身是一对一的关系,但是当各类科技信息相互关联时,可能形成一对多的关系,例如一份科技项目档案中可能包含多个专利技术、科技成果和期刊论文。科技情报信息资源数据库的底层数据由多个专题、多个供应商的数据资源组成,为用户提供较为统一、简便、全面的检索界面^[9]。

2.1 科技信息持续开放与共享

科技信息向社会开放共享,即在互联网上提供文献检索与下载、论文与图书传递、科技项目档案查询借阅等服务。自2006年建成以来,湖北省科技基础条件平台坚持开放共享原则,通过互联网向企业、高校、科研院所等创新主体提供智力支持服务,也不可避免地需要向互联网开放Web和数据库服务^[10]。

科技信息不论以论文、报告或成果等哪种形式为用户

服务,从信息系统管理的角度看,数据库存储和管理的对象都是数据文件。除科技信息文件本身外,还有操作系统中管理数据库的文件、数据库运行所需文件以及数据库里存储的数据文件,这些文件全部都是勒索软件影响的对象。样本中被加密的文件有121539个,其中科技信息文件有114908个,占94.54%。科技信息资源整合平台有大量的Web服务、数据库服务、微服务以及中间件服务器在背后作为支撑,所以维护较为复杂,管理员容易忽视其中的一些环节,一项不安全的配置或漏洞都可能导致科技信息数据的安全问题。

2.2 数据安全法律法规完善

TCP/IP协议簇使人们在不可靠的底层上建立了可靠的网络,在数据可靠性的需求之上是安全性需求。2017年《中华人民共和国网络安全法》施行,2021年《中华人民共和国数据安全法》施行,对数据的机密性、完整性、可用性提出了要求。在建设数字中国的过程中,数据安全越来越重要,尤其在部分数据会对个人安全、社会安全乃至国家安全产生威胁的时候^[11]。

《信息安全等级保护管理办法》将信息系统的安全保护等级分为5级,科技信息系统大部分处于1~2级,如果系统受到破坏,会对公民、法人和其他组织的合法权益或者社会秩序与公共利益造成损害,但不损害国家安全;少数处于3级,如果系统受到破坏,会对国家安全、社会秩序和公共利益造成损害。

2.3 科技信息安全的新风险点

经过“十三五”时期的不断努力,我国的数字经济发展取得了举世瞩目的成就,《国家“十四五”规划纲要》要求在“十四五”时期继续建设数字中国。当个人和社会生活普遍数字化时,会累积前所未有的海量数据。以湖北省为例,在“十三五”期间升级改造了科技信息共享服务平台、大型科学仪器协作共用网,将以前未实现数字化、网络化的科技情报资源,如科技报告、行业报告、科技项目档案等纸质文件转化成便于用户获取的电子文件,推进大型科学仪器信息上网,并进行网络预约和共享^[12]。但这些海量数据在作为资源被采集、清洗、存储、管理、挖掘和利用的过程中,可能成为黑客不当牟利的来源。

首先是破坏性强的勒索软件。根据奇安信安服团队发布的《2023年中国企业勒索病毒攻击态势分析报告》中对勒索软件入侵方式的统计,其中最多的是暴力破解,占52.6%。在勒索攻击造成较为严重后果的重大事件中,49.5%明确与弱口令有关^[13]。2023年遭受过勒索病毒攻击的行业主要集中在制造业、互联网以及医疗卫生行业。此外,能源、服务业、建筑以及教育等行业也逐渐成了勒索攻击团伙的目标。

其次是以盗取敏感数据为目的的恶意软件和恶意网站。中国信息安全测评中心在《2023年国家网络安全总体态势分析与趋势研判》中将“敏感数据被窃被泄”列为第3

个网络安全风险点,并认为随之产生的受害者范围扩大、非法跨境传输数据、暗网数据交易是其中的突出风险^[14]。科技信息系统也面临伪造网址、通过跳转引导用户进入钓鱼网站、被植入非法链接等安全威胁。

最后是以网络爬虫为主要代表的自动化数据收集技术。网络爬虫技术最早应用于搜索引擎领域,是搜索引擎获取数据来源的支撑性技术之一。随着数据资源自身以及大数据处理技术对数据需求的爆炸式增长,网络爬虫的应用场景变得更多。对部分网络爬虫的不当使用,不但会导致信息泄露,而且过于频繁地抓取内容会影响网站和系统正常提供服务。网络爬虫与恶意网站相结合即形成钓鱼网站。科技信息虽然有开放和共享的属性,但应尽力避

免恶意抓取数据的行为。

3 勒索软件目标特征

勒索软件起源于国外,黑客根据勒索信里的私有密钥区分被勒索的对象,从而知道付款人赎回的具体数据,并要求用数字加密货币支付赎金。数字加密货币的无手续费、低成本、交易快等特点满足了黑客匿名的需求^[15]。勒索软件的攻击行为目的是“勒索”,即得到钱财,所以黑客在选择攻击目标时,首先考虑能够支付较多赎金的数据所有者。

以 mallox 结尾的被加密文件及勒索信如图 1 所示。

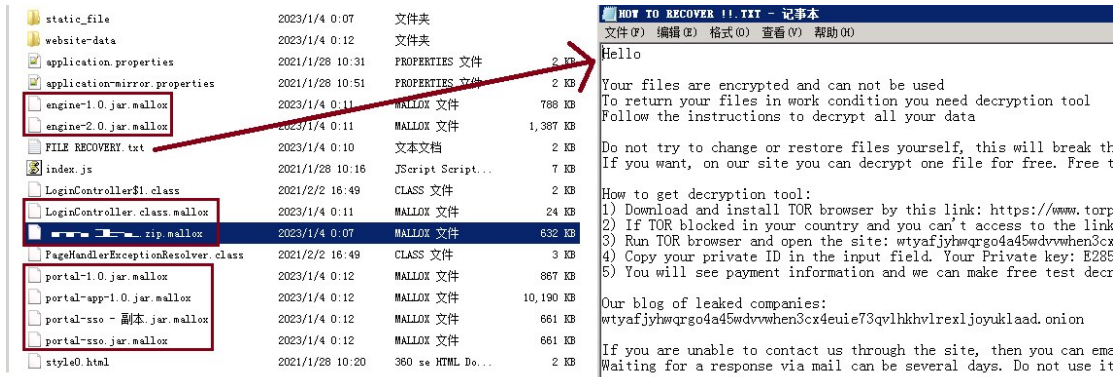


Fig. 1 Encrypted files ending in mallox and ransom letter

图 1 以 mallox 结尾的被加密文件及勒索信

3.1 数据所有者有支付能力

科技信息系统和网站一般归政府的科技主管部门所有,系统的建设、运行、维护由科技系统内承担,科技数据的收集、整理和加工等由不同职能的部门协作完成,数据质量高且应用广泛。因此,科技数据归政府所有。

黑客选择政府单位作为勒索对象,是认为政府资金来源稳定,较可能支付的起赎金^[16]。然而,我国政府及下属机构不可能支付赎金的原因如下:①《关于进一步防范和处置虚拟货币交易炒作风险的通知》要求金融机构和非银行支付机构不得为虚拟货币相关业务活动提供服务,而勒索信要求将赎金付给匿名的境外账户,这是不受法律保护的行为^[17];②财政性资金的申请和使用需遵从《中华人民共和国采购法实施条例》,未在上一财政年度申报的本年度预算内的费用,即使是非常紧急的情况也要经过审批流程,不可能在勒索信要求时限(一般为 72h)内支付;③《关于防范比特币风险的通知》明确我国禁止比特币,因此财政性资金不可能用于购买比特币^[18]。

3.2 数据向互联网开放

科技信息系统向互联网开放数据库服务。被攻陷的系统开放了默认的 1433 端口对互联网上其他用户或其他系统提供 SQL Server 数据库服务。部分数据库管理员为了方便登录,采用 Windows 认证模式。因此,数据库管理工具存储了系统用户名和密码或票据,使黑客可以通过 SQL

Server 数据库获得对系统的全部控制权。此外,SQL Server 数据库开启了默认用户,包括管理员权限的 SA、普通游客权限的 SQL Debugger。如果采用 Windows 认证模式,操作系统中已存在的用户都可以登录到数据库,比如 Guest。可总结为:服务器中存在维护目的或使用人不明确,且具有远程连接权限的账号,容易成为勒索软件攻击的目标。

部分科技信息系统存在远程维护服务。黑客在夜里 23 点到次日 1 点之间对系统的用户名和密码进行暴力破解。将黑客尝试的用户名按时间排序(见图 2),得知黑客尝试列表的优先级由高到低为:①操作系统默认的权限高的用户名;②常见应用自带的权限高的用户名;③操作系统默认的权限低的用户名;④常见的人名。

3.3 系统存在可互访漏洞

网络的互访策略往往以防火墙为边界,划分为完全信任的内网、完全不信任的外网以及部分信任的隔离区(Demilitarized Zone, DMZ)等逻辑区域,其之间的区别在于安全级别的高低。DMZ 的安全级别位于内、外网之间,其对内网完全开放,对互联网部分开放,如果被黑客占有,内网对 DMZ 的宽松策略便有利于勒索病毒在内网的扩散^[19],此行为符合高级持续性威胁(Advanced Persistent Threat, APT)的潜伏性攻击特征^[20]。Mallox 在内网扩散的特点如下:①方式多样,不仅限于 445 端口;②有潜伏时间,但很短暂;③文件的修改时间差距小,可见加密速度快。

	尝试的用户名 (按时间顺序→)			
T1	Administrator			
T2	Administrator			
T3	Administrator			
T4	Owner		User	
T5	k3admin	kingdeek3net		kingdee
T6	aspnet	root	admins	Guest
T7	Guest ✓		Administrator ✓	

Fig. 2 Hacker's username attempt order

图2 黑客的用户名尝试顺序

值得注意的是,在可互访的多个系统之间,勒索软件扩散过程不会被任何安全设备察觉或触发告警,因为使用正确用户名和密码的远程登录行为是合规的。

4 勒索软件行为分析

4.1 攻击流程

因为勒索软件的加密算法复杂、密钥较长,从时间代价考虑,加密的文件没有用工具自行解密的可能,那么尽早识别勒索软件的攻击行为尤其重要^[21]。从样本来看,Mallox的攻击过程持续了至少20天,期间的规律性行为可作为管理员判断服务器可能被攻击的客观依据。

如图3所示,主要攻击流程如下:Mallox是以勒索软件即服务(RaaS, Ransomware as a Service)方式部署的,分发威胁的基础设施或机构自动地进行大范围扫描,确定运行特定服务且开启的系统为攻击目标。在Mallox样本中,黑客利用SQL Server服务向系统植入名为Lumigent的数据库管理软件,查看并修改了SQL Server数据库的管理员用户名及其密码。随后登录Windows的远程桌面或连接Linux/CentOS的SSH服务,是黑客完全控制系统的必经步骤。黑客在登录系统A后对系统进行遍历,筛选拟加密的文件夹和文件,并以当前系统为据点,默默展开对内网其他关联系统的探测。Mallox受害者系统A首先发动攻击的对象是其通过远程桌面连接过的系统B,系统之间的密码并不相同,黑客在短时间内占领系统B的原因是:受害者系统A对B的远程桌面连接使用了票据,所以黑客可以在不知道B的管理员用户名和密码的情况下,直接从A登录到B,并获得对B的完全控制权,跳过了长达20多天的暴力破解。从被加密文件的修改时间看,各种格式的文件(无论大小)加密完成时间、勒索信的创建时间差在1min以内。

4.2 加密与解密过程

如图4所示,勒索软件常见的加密算法包括4种:对称密钥算法、非对称密钥算法、散列算法、其他混合算法,其中采用最多的是对称密钥算法中的AES(Advanced Encryption Standard, 高级加密标准)算法^[22]。Mallox混合采用

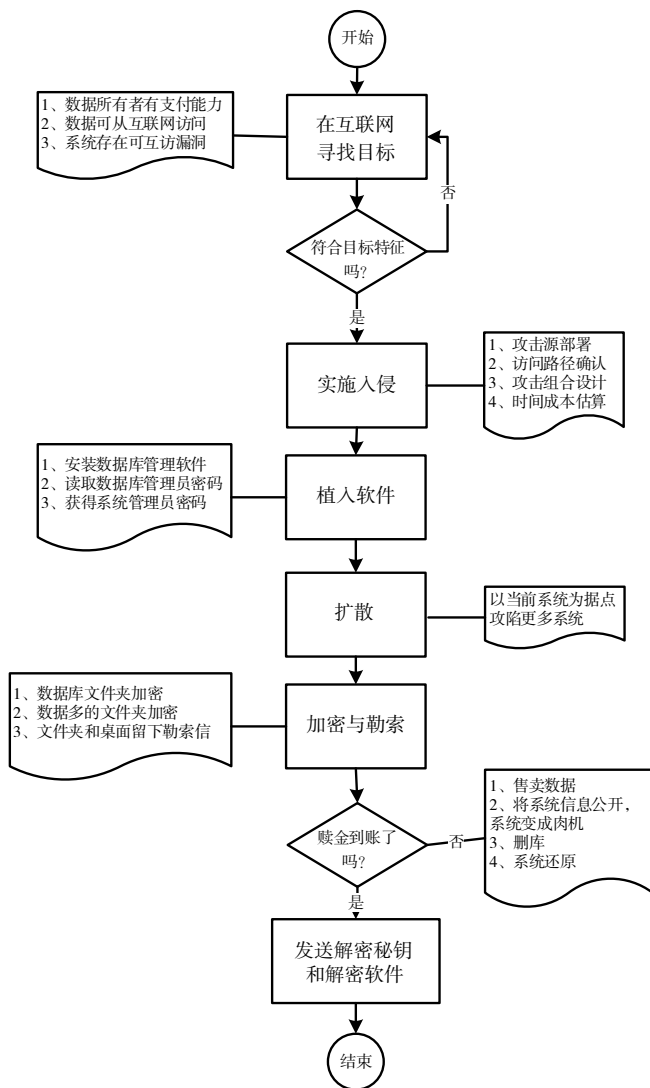


Fig. 3 Flow of Mallox intrusion

图3 Mallox攻击流程

ECDH (Elliptic Curve Diffie - Hellman Key Exchange, 椭圆曲线迪菲-赫尔曼密钥交换)算法和Chacha20算法,其中非对称的ECDH负责密钥交换和传输,对称的Chacha20负责对系统内的文件进行加密^[23-24]。Chacha系列流密码具有很强的抵抗密码分析攻击的特性,名字中的20表示该算法有20轮加密计算。其速度快、节省流量,可以通过互联网快速且不易察觉地进行加密。

4.3 日志分析

服务器自带的管理模块“事件查看器”的安全日志中记录了各种用户以各种登录方式连接服务器的记录。在勒索软件Mallox导致网站崩溃之前的20天以内, ID 4625的事件占有所有记录的99.52%。其是审核失败的记录,且源网络IP各不相同,每次攻击更换一个。在实验环境中,一次成功的远程登录会产生1条审核成功的ID 4624事件,此作为基线。与勒索软件会导致API请求异常^[25]类似,若ID 4625的事件过频,可判断服务器正遭受远程桌面暴力破解的攻击。此处有一点局限:由于ID 4625的事件过多,

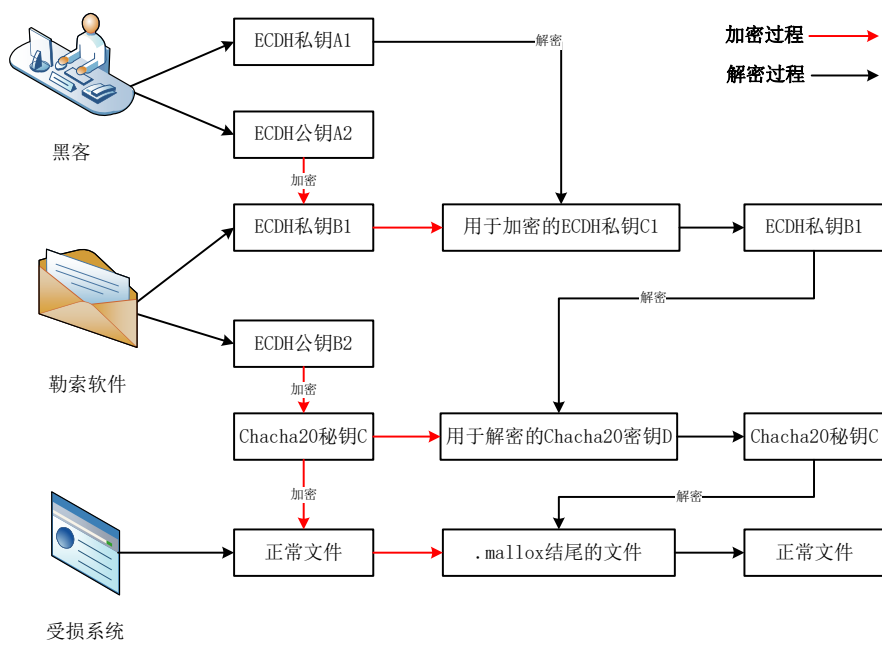


Fig. 4 Encryption and decryption process of Mallox
图 4 Mallox 加密与解密过程

使日志数量满溢,只能追溯到 Mallox 发作的前 20 天,实际攻击的开始时间可能更早。攻击行为在尝试次数上从 48 到 17 839 不等,在时间上集中在节假日和工作日的非工作时间,应该是黑客为了躲避人工监管。

在勒索软件 Mallox 对样本的攻击过程中,网络安全设备无一识别或触发告警。也许是因为安全厂家对勒索软件行为的分析并不能完全识别各家族,尤其是对于新出现的勒索软件^[26]。根据对样本的分析,攻击行为未触发安全设备告警的原因如下:①黑客连接服务器的请求不密集,既没有引起抗分布式拒绝服务攻击(Anti-DDoS Service, ADS)的封锁,也没有让应用防火墙(Application Firewall, AF)认为是异常连接;②黑客不停地更换发动攻击的 IP 地址,在国外 ASN 的归属地中,俄罗斯最多,其次是英国,使得安全设备难以锁定对象(攻击来源的统计结果与 360 安全中心发布的《2022 年勒索软件流行态势报告》^[27]一致);③在安全设备的策略中,对内网连接的审查级别较低,未能识别勒索软件在内网的扩散。

5 解决建议

对勒索软件这类网络攻击无法主动判断,被动的解决办法可分为事前、事后两类。事前做好预防措施,在攻击发生时准确定位、安全自查还要异地存储备份。事后需尽快恢复数据,缩短系统的宕机时间,或使用备份文件恢复,或使用秘钥将被加密的文件解密。文件备份需在事前完成,因此在预防措施中进行叙述。

5.1 预防措施

一是系统减少向互联网开放端口。向互联网开放数

据库服务或支撑 Web 服务,或其他数据库同步数据,支撑 Web 服务的数据库服务器可以只向 Web 服务器开放服务,而非面向整个互联网。如果 Web 和数据库服务器在同一内网,可以在内网传输,避开来自互联网的攻击。不在同一内网的数据库之间可以通过安全的中转服务来相互传递数据。对于对实时性要求不高的同步,也可以定时开启和关闭端口。

二是部署终端安全及防病毒系统(Endpoint Detection and Response, EDR)设备或服务。截止目前,深信服等安全厂家声称可以提供治理已知和未知的勒索软件服务,但是对被保护对象的部署有一定要求,例如对被保护对象的访问路径必须经过深信服的网络。监控需要采样点,这让采购方不得不考虑其数据的安全性。独有但不涉密的数据,如何在接入其他网络时保持独有性,是购买方倾向于购买硬件在本地部署,而非软件在异地部署的原因。

三是优化远程维护手段。使用堡垒机或虚拟专用网络(Virtual Private Network, VPN)设备,关闭远程维护端口,远程维护工程师从互联网进入服务器至少需要经过两层认证。这两种设备都有资源管理的功能,限制了远程维护工程师能操作的服务器,可避免误操作和越权操作。

四是异地备份。科技信息中从各数据供应商处购买的数据及数据库是可恢复的,但是自加工、机构特有的数据只能通过数据备份来恢复。勒索软件 Mallox 不但加密了数据库文件,而且加密了数据本身,导致存放在一起的备份文件不可用,所以要进行异地存储。对于不频发更新的数据,也可采用冷备份。

5.2 文件解密

样本共有 121 539 个被加密的文件和勒索信,在被加

密的文件中,大部分可以从数据供应商处恢复。不可恢复的文件如表1所示。

Table 1 Unrecoverable files
表1 不可恢复的文件

文件类型	受损文件数	文件总数	受损率/%
馆藏特色资源文件	130	366	35.52
操作系统中管理数据库的文件	66	106	62.26
数据库运行所需文件	297	668	44.46
数据库里存储的数据文件	1 470	1 500	98.00

文件解密的方法分为两种:暴力破解和使用密钥。暴力破解即以枚举方式尝试各种组合的符合长度要求的字符串作为密钥来运行解密算法,试图得到加密前的文件,代价是时间和算力。以AES-128算法的密钥破解为例,需要一亿年以上。部分数据恢复公司声称可以解密被勒索软件加密的文件,有以下可能:①部分重复使用的密钥被作者公开;②密钥较短,小于56位的密钥可在有限时间内暴力破解;③能恢复部分文件,但不保证可用。无论能否解密,均不建议向黑客购买密钥。

6 结语

勒索软件造成的恶劣后果只能由数据拥有者和使用者共同承担,这是政府和社会大力建设数字资源道路上的一个阻碍。如果反病毒技术和政策法规能够相互支持,可以更好地遏制勒索软件的流行^[28-29]。但是,不管采用怎样的数据备份方式,需要注意系统之间的逻辑隔离。未来还需对以下内容进行研究:很多单位和个人都使用Wifi网络,类似“Wifi万能钥匙”的APP可以分享Wifi密码。黑客在不知道密码的前提下通过共享的Wifi进入内网,可以访问到不向互联网开放的内部服务及数据,同时避开安全设备的审计。此漏洞是否存在需要进一步求证。

参考文献:

[1] Ministry of Industry and Information Technology. Guideline on promoting the development of data security industry by sixteen departments[EB/OL]. http://www.cac.gov.cn/2023-01/14/c_1675346873856103.htm.
工业和信息化部.十六部门关于促进数据安全产业发展的指导意见[EB/OL]. http://www.cac.gov.cn/2023-01/14/c_1675346873856103.htm.

[2] YANG R, CHEN W, ZHANG M, et al. Research and application of science and technology information knowledge service platform from the perspective of big data: a case study of the energy field[J]. Science and Technology Management Research, 2022, 42(9): 168-173.
杨锐,陈伟,张敏,等.大数据视角下科技信息知识服务平台研究应用——以能源领域为例[J].科技管理研究, 2022, 42(9): 168-173.

[3] LIU X W. Strengthening the construction of S&T information resources in the new ages[J]. Digital Library Forum, 2022(6): 10-13.
刘细文.新时期需要强化我国科技信息资源建设[J].数字图书馆论

坛, 2022(6): 10-13.

[4] Sangfor Qianlimu Security Technology Center. Characteristics of network security situation in 2023 and trend analysis for 2024 [R]. Shenzhen: SANGFOR, 2024.
深信服千里目安全技术中心.2023年网络安全状况特点及2024年趋势研判[R].深圳:深信服科技, 2024.

[5] DONG Y H, SONG G J. Review on the technology development of ransomware[J]. Computer Applications and Software, 2023, 40(1): 331-343.
董显宏,宋广佳.勒索病毒技术发展研究综述[J].计算机应用与软件, 2023, 40(1): 331-343.

[6] CAI Q. Computer network security and countermeasures against blackmail virus[J]. Wireless Internet Technology, 2022, 19(12): 29-31.
蔡琴.计算机网络安全与勒索病毒应对策略[J].无线互联科技, 2022, 19(12): 29-31.

[7] LIU W J, GUO C, SHEN G W, et al. Ransomware early detection method based on deep learning[J]. Computer Science, 2023, 50(3): 391-398.
刘文静,郭春,中国伟,等.基于深度学习的勒索软件早期检测方法[J].计算机科学, 2023, 50(3): 391-398.

[8] MAIGIDA A M, ABDULHAMID S M, OLALERE M, et al. Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms [J]. Journal of Reliable Intelligent Environments, 2019(5): 67-89.

[9] CHEN R, LIU Y B, LIU D, et al. Research on the construction of Hubei science and technology resource sharing service platform based on microservice architecture [J]. China Science & Technology Resources Review, 2021, 53(1): 47-53.
陈瑞,刘延滨,柳丹,等.基于微服务架构的湖北省科技资源共享服务平台建设研究[J].中国科技资源导刊, 2021, 53(1): 47-53.

[10] FAN Q T. Investigation and analysis of the status quo of construction of provincial scientific and technical information institute's website [J]. Competitive Intelligence, 2021, 17(6): 24-32.
凡庆涛.我国省级科技情报机构网站建设现状调查与分析[J].竞争情报, 2021, 17(6): 24-32.

[11] QUE T S, WANG Z Y. Global data security governance and action strategies for China's participation in the era of digital economy [J]. Journal of International Security Studies, 2022, 40(1): 130-154, 158.
阙天舒,王子玥.数字经济时代的全球数据安全治理与中国策略[J].国际安全研究, 2022, 40(1): 130-154, 158.

[12] CHEN R, JIANG K. Strategies for improving the service capability of science and technology information sharing platform - taking Hubei as an example [J]. Pioneering With Science & Technology Monthly, 2020, 33(10): 69-71.
陈瑞,姜鲲.科技信息共享平台服务能力提升策略——以湖北为例[J].科技创业月刊, 2020, 33(10): 69-71.

[13] Qi An Xin Security Service Team. Analysis report on the situation of ransom virus attacks in Chinese enterprises in 2023 [R]. Beijing: Qi An Xin Technology Group Inc., 2023.
奇安信安服团队.2023年中国企业勒索病毒攻击态势分析报告[R].北京:奇安信科技集团股份有限公司, 2023.

[14] China Information Security Evaluation Center. Analysis and trend analysis of the overall situation of national cybersecurity in 2023 [R]. Bei-

- jing: China Information Security Evaluation Center, 2023.
- 中国信息安全测评中心. 2023年国家网络安全总体态势分析与趋势研判[R]. 北京: 中国信息安全测评中心, 2023.
- [15] SUN Q Q. Research on legal regulation of money laundering crime of digital encrypted currency [D]. Nanchang: Jiangxi University of Finance and Economics, 2021.
- 孙倩倩. 数字加密货币洗钱犯罪法律规制研究[D]. 南昌: 江西财经大学, 2021.
- [16] LI R W, HUANG H Y, LUO H. Defense and killing strategies of ransom virus GANDCRAB V5. 2 [J]. Research on Digital Media, 2021, 38(4): 37-40.
- 李荣伟, 黄慧扬, 罗欢. 勒索病毒GANDCRAB V5. 2的防御与查杀策略[J]. 数字传媒研究, 2021, 38(4): 37-40.
- [17] The People's Bank of China. Notice on further preventing and dealing with the risks of speculation in virtual currency transactions [EB/OL]. http://www.gov.cn/zhengce/zhengceku/2021-10/08/content_5641404.htm.
- 中国人民银行. 关于进一步防范和处置虚拟货币交易炒作风险的通知 [EB/OL]. http://www.gov.cn/zhengce/zhengceku/2021-10/08/content_5641404.htm.
- [18] The People's Bank of China. Notice on preventing bitcoin risks [EB/OL]. http://www.gov.cn/gzdt/2013-12/05/content_2542751.htm.
- 中国人民银行. 关于防范比特币风险的通知 [EB/OL]. http://www.gov.cn/gzdt/2013-12/05/content_2542751.htm.
- [19] YUE X D. Security protection of blackmail virus in the internal network of radio management [J]. China Radio, 2020(2): 42-44.
- 岳新东. 浅谈无线电管理内部网络勒索病毒安全防护[J]. 中国无线电, 2020(2): 42-44.
- [20] DONG G, YU W, XUAN G Z. Analysis and detection of attack characteristics in advanced persistent threats [J]. Journal of Jilin University (Science Edition), 2019, 57(2): 339-344.
- 董刚, 余伟, 玄光哲. 高级持续性威胁中攻击特征的分析与检测[J]. 吉林大学学报(理学版), 2019, 57(2): 339-344.
- [21] LI H S, HUANG J. Identification, disposal and defense of extortion virus [J]. Journal of Information Security Research, 2019, 5(4): 346-351.
- 李华生, 黄进. 勒索病毒识别、处置与防御[J]. 信息安全研究, 2019, 5(4): 346-351.
- [22] LU T L, LI G Y, WU J, et al. Review on application and defense methods of cryptographic algorithms in computer virus [J]. Science and Technology Management Research, 2020, 40(2): 207-215.
- 芦天亮, 李国友, 吴警, 等. 计算机病毒中的密码算法应用及防御方法综述[J]. 科技管理研究, 2020, 40(2): 207-215.
- [23] TOPSEC Technologies Group. Ransomware Mallox is coming [EB/OL]. <http://www.topsec.com.cn/newsx/1961>.
- 天融信科技集团. Mallox 勒索病毒来势汹汹 [EB/OL]. <http://www.topsec.com.cn/newsx/1961>.
- [24] 360 Internet Security Center. Sample analysis of ransomware TargetCompany (Mallox) [EB/OL]. <https://bbs.360.cn/thread-16043918-1-1.html>.
- 360 互联网安全中心. TargetCompany (Mallox) 勒索病毒样本分析 [EB/OL]. <https://bbs.360.cn/thread-16043918-1-1.html>.
- [25] HAMPTON N, BAIG Z, ZEADALLY S. Ransomware behavioural analysis on windows platforms [J]. Journal of Information Security and Applications, 2018(40): 44-51.
- [26] MATTHEW A M, CHOWDHURY M M. The growing influence of ransomware [C]//IEEE International Conference on Electro Information Technology (EIT), 2020: 643-647.
- [27] 360 Government Enterprise Security Advanced Threat Research and Analysis Center Antivirus Department. 2022 report of ransomware trend [R]. Beijing: 360 Internet Security Center, 2023.
- 360 政企安全高级威胁研究分析中心反病毒部. 2022年勒索软件流行态势报告[R]. 北京: 360 互联网安全中心, 2023.
- [28] ROMAN R, ELENA B. Urgent problems in the investigation of computer crimes at the modern stage [M]. Berlin: Springer, 2019: 411-417.
- [29] TANG L. Reflections on the dilemmas in the construction of international norms in cyberspace from the perspective of WannaCry ransomware [J]. Journal of Yunnan Nationalities University: Social Sciences, 2019, 36(6): 145-156.
- 唐岚. 从 WannaCry 事件看网络空间国际规则的困境及思考[J]. 云南民族大学学报(哲学社会科学版), 2019, 36(6): 145-156.

(责任编辑: 黄健)