勒索软件之所以猖獗，一个重要原因就是制作者经常使用&quot匿名&quot比特币支付逃避警方追踪的功能。

文/八九零

这事发生在一个月前。我们公司被黑客攻击了。黑客留下了一个&quot勒索信&quot如下：

总结一下，我们遇到了一个勒索软件，文档被锁定。对方要求先交0.05比特币再解密。

01。事件[XY002][XY001]的经过和直接影响2021年12月13日星期一&quot网络管理器&quot老沈。10点左右来公司上班&#039；像往常一样打卡。早上，公司的员工少了，老沈&#039；的工作压力比较轻。这种事件史无前例，第一次！一开始老沈只是觉得一个程序不对。当他看到勒索信时，他意识到这是一种勒索病毒。此时此刻袭击已经过去12个多小时了。

8点&#039；12月11日周六晚上打卡，黑客开始入侵我们的服务器，服务器开始报错，频繁登录，有未知访问.所有这些都被留下了。那天是周末。而且是双12的购物节，几乎没人值班。7个小时后，12月12日凌晨3点，服务器被攻破。我们的数据库是加密的。Word和Txt后缀都变了，打不开。

很快，这件事开始直接影响到我们的办公效率。10点35分，公司里一个姓曹的同事发来消息：&quotOA多久能准备好."我们的报销、支付、审批等事项都将在OA(办公系统)上进行。

虽然这句话没有&#039；不指名道姓，大家都知道，是写给行政部的老沈的。是否网页卡住，忘记密码，电脑坏了，或者打印机不工作.问老沈。

老沈经常关心这个，但是他能&#039；我不在乎那个，所以他可以&#039；不要反应太快。。但这一次的反应显然要快得多，但却是坏消息。十分钟后，行政部的一条消息在公司群里引起了轰动：

今天OA服务器可以&#039；不能正常使用。具体原因老沈还在调查。请耐心等待。如果有任何恢复，我们会及时在群里通知你。

&quot；韩元&#039；它今天恢复了吗？急件今天就要盖章。"一个女同事问，带着含泪的表情包。刹那间，屏幕上充满了&quot恨铁不成钢&quot。

02。初步处理失败及原因

老沈，他一直是&quot网络管理器&quot16年来，没有办法做到这一点。我们的应对策略都失败了。

网络断开，但黑客加密已完成。

尽可能备份。，但财务等核心信息已经加密。

找网警报案，虽然已经立案，但是破案时间不定，实在是受不了。

借助现有的安全软件工具，我们查找是否有公开解密工具，但没有结果。

我们也想成全黑客&#039；的愿望。0.05比特币，按照12月13日5万美元的价格，我们需要花费2500美元(折合人民币约1.5万元)。相对于OA系统故障可能造成的损失，这笔钱不算多。

但是老沈觉得对方可能会反悔，甚至在解密邮件上大做文章。

最近也有类似的新闻：去年12月下旬，温州某超市储值卡系统瘫痪，数据库信息被加密。黑客消息24小时内支付0.042比特币(当时相当于1789.2美元)，提供解密工具。超市老板做了，但黑客没有&#039；不要表演。

在这种情况下，表示这件事很可能无法解决。早在2017年，俄罗斯知名杀毒软件供应商卡巴斯基实验室就表示，勒索软件使用的加密算法无解，重装后的系统可以继续使用。，但是加密的文件将会丢失。

现在呢？值得一提的是，在&quotNet2020&quot专项行动，国内首个比特币勒索软件制作者居某(涉案金额500余万元)被抓获。。引用专案组成员、启东市公安局网安支队民警黄晓婷的话说：

一般来说，没有病毒制造者的解密工具，别人可以&#039；无法完成解密。勒索软件入侵计算机并加密文件或系统。每个解密器是根据加密计算机的特征新生成的。

根据2020年360安全大脑的报告，确认受到勒索病毒攻击的案例超过3700起，最终帮助解密文件的案例超过260起。也就是成功率只有7%。形势进一步恶化。12月13日下午2:50，行政部进一步宣布OA服务器本周不能使用。

03。什么&#039；有什么问题吗？勒索病毒又回来了！

回顾勒索软件的历史，2017年，勒索软件&quot想哭&quot横扫全球150个国家的30万台电脑。一般需要支付价值300-600美元的比特币才能解密。

此后，勒索软件不断进化出各种版本和类型。比如：加密文档、锁屏、锁硬盘、加密数据库等等。

国内企业的巅峰在2019年。据亚信安全《2019威胁态势分析》统计，2019年中国勒索病毒感染数量全球第一，占比20%。

老沈记得当时(防护)措施都做好了，所以没被抓到。。但在2021年12月，勒索软件的影响力似乎在下降的时候，我们上当了。

据他猜测，出现这个问题的原因可能是安全服务软件过期了。12月初，我们的安全服务软件服务到期。该费用将在一月份服务器迁移后重新收取。但这半个月，由于防火墙特征库到期，给了黑客可乘之机。

这是什么意思？比如黑客就是偷我们公司东西的小偷。我们大门的管理以前很谨慎，锁会经常换。小偷来我们公司门口找机会下手，但是锁往往两天之内就换了，很难快速匹配到合适的钥匙。渐渐地，小偷失去了兴趣。但直到锁十几二十天不换，小偷才有足够的时间配钥匙。

所以勒索软件是怎么针对我们的？老沈怀疑有人利用了公司&#039；或者有人无意中把病毒带到了公司外面，或者这是黑客的结果&#039；"撒网&quot.总之，各种可能性都存在，很难确定。一般来说，远程桌面、网页挂起、激活/破解、僵尸网络、数据库弱密码、漏洞、钓鱼邮件等。都是勒索软件攻击的常见方式。

不得不提的是，诸多信号提醒我们，勒索病毒很有可能卷土重来。在过去的一年里，巨型企业和重要国家机构出现了多起勒索病毒的案例，非常轰动。

比如2021年5月。美国最大的石油管道运营商ColonialPipeline遭到勒索病毒攻击，其向美国东海岸主要城市输送油气的管道系统离线，甚至引起了美国总统的关注

。

此外，2021年，华盛顿大都会警察局、石油巨头皇家壳牌、全球IT咨询巨头埃森哲、台湾省&#039；美国存储组件制造商ADATA，以及厄瓜多尔国有电信运营商CNT遭到勒索软件攻击。，大量文件泄露被盗。

据360安全大脑《2021年勒索病毒疫情分析报告》统计，2021年超4000用户被勒索病毒攻击，高于2020年超3700用户，高峰期在10-12月。

其中，值得注意的是，根据美国国土安全部部长去年5月的讲话，50-70%的勒索软件攻击是针对中小企业的，2020年共造成3.5亿美元的损失。而思科去年10月发布的一项调查显示，中国有42%的中小企业在过去一年遭受过网络攻击，41%的企业损失超过50万美元。

45万元的教训和经验

12月15日，我们被迫找到杭州某保安服务商，对方全权负责解决此事。要5万元。

这5万元可以支付三次以上的勒索病毒攻击，相当于一套安全软件的费用，一个可以用三到五年的防火墙特征库也差不多这个价格。

3天后，问题基本解决。。12月20日上午10点，OA恢复使用。

至于这家公司是怎么解决问题的，老沈没有&#039；我不知道。"也许我付了赎金，也许我没有&#039；t，可能我搞清楚了勒索软件的版本，找到了解密工具。"老沈说。

关键在于未来的保障。老沈强调，除了保证安全服务软件全天候运行外，还将&quot加强备份&quot。比如财务数据，以前是财务部门管理，只做本地备份。现在是老沈自己管理，做了几次备份。据彭博新闻报道，值得一提的是。上面说的殖民管道虽然交了赎金，但是黑客解密太慢，最后还是靠备份数据恢复系统。

另外，8月份，埃森哲遭遇勒索病毒后，黑客声称&quot埃森哲的6TB数据被盗。并要求支付5000万美元赎金，但埃森哲回应称：&quot事件发生后，受影响的服务器立即被控制和隔离，受影响的系统从备份中完全恢复。"换句话说，备份数据可以在很大程度上避免损失。

综上所述，勒索软件之所以猖獗，其中一个重要原因就是制作者经常使用&quot匿名&quot比特币支付逃避警方追踪的功能。

但一个好的开始是：目前国内有很多数据解密和恢复公司与病毒制造者同流合污，他们承担着渠道商的角色，比如为病毒制造者分发病毒，占国内企业的便宜&#039；不便购买比特币代替交易。

更多人参与其中。犯错的机会会更多。在上述&quotNet2020&quot专项行动，警方破案的关键是借助与病毒制作者有直接合作的数据恢复公司的线索，抓住背后的病毒制作者。在过去的一个月里，比特币崩盘，一度跌至33000美元，为半年来最低价。这也将是对&quot勒索病毒产业链&quot。

最后，我们不&#039；不建议支付赎金。如果有必要，我们可以试着&quot议价&quot。

至少有一个例子可以说明这种可能性：据媒体报道，2017年5月14日，台湾省网友陈子聪感染了勒索病毒，于是他给黑客发了一封邮件&quot恳求&quot:&quot我的月收入是400美元。你想这样对我吗？？结果对方回应：&quot我们显然高估了你的收入。所以你不&#039；我不需要付任何钱。系统稍后将解锁您的计算机。"

作者|林博|责任编辑|李梦晴

责任编辑|何|主编|郑|来源|VCG

——吴晓波领衔50本商业书籍，一起敲开商业之门，欢迎选购——