

谨慎防范网络隐患以此来保护Oracle数据 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/253/2021_2022__E8_B0_A8_E6_85_8E_E9_98_B2_E8_c102_253886.htm Oracle在线数据经常遭到威胁，一些数据窃取者编写“Hoovers”（一种数据收集工具）来模拟在线数据库处理来获取有价值的信息。eBay（电子商务网站公司）等一些Oracle的联机主要客户不得不阻止“Hoovers”来防止数据窃取者，但是骗子却在不断变化，费尽心思来窃取你的一些有价值网上信息。我们同样可以看到一些内部数据安全事件，如万豪国际酒店集团数据丢失的重大损失。对那些关注内部安全的公司，专家们建议可以采取监控、必要时修改其内部处理和数据存取控制的方法。Oltsik说，“偷取磁带是不值得称道，但却是最有效的攻击方法，很多公司会想到防范那些直接进入其内部服务器的黑客行为，但是如果他们公司内部安全防范很弱的话，数据窃取者可以直接带走一箱子的磁带。但是知识产权保护力度的缺乏已经改变了信息分配情况。专属性质的原万维网不见了，免费的带宽模式已经取代西方联盟来传递大量的有价值的信息。网上小偷可以数字化畅销书籍，以及瞬间从网上任何地方下载并盗印出版。更糟的是，网上黑客正在攻击数据库并窃取数据。盗窃知识产权已经成为一种流行病，作家Steven King因为其畅销书被数字化并免费发布到网上而损失了几百万美元。即使最慎重的出版商也在冒着盗版的风险。我自己的一本书，Oracle 10g 应用服务器管理手册也曾被盗窃并仅以6.5美元的价格在eBay上出售。发行人并不能将盗窃者逮捕或起诉。但是对那些敢于使其网上Oracle数据很容易获取的人来说

，他们的处境就更加危险了，其中就有一些公司的全部数据被外国人所窃取。推动对知识产权盗窃者的逮捕行动需要花费数十万美元，而骗子们知道那些小公司并没有这样的财力来对付他们，除非是一家拥有上亿美元的公司。一般的美国出版商很少对全球性的Oracle数据窃取者诉诸于法律。因此，窃贼们窃取Oracle数据时不会担心被拘捕，甚至入狱。迟早，这个问题或许会更严重，传统出版商可能遭遇破产，他们其高质量的文章正在变成厚厚的垃圾或者杂乱的博客。只有世界范围的对知识产权的强有力的保护，才可以保护我们的信息不会被大规模的盗窃。与以往相比，Oracle数据库管理员必须知道更多的公司数据可能被窃取的方式。在我作为Oracle数据库管理者时，我发现存在各种个样的数据窃取方式，之后我便出版了针对所有远程数据库存取操作的《数据安全指导方针》：内部工作有很多的国外远程数据库管理员已经窃取了全部的数据，并且还利用病毒来吸收新数据，Email到海外。其他的还有H-1b签证工作人员可能窃取Oracle数据，并大量的送到海外法律上不追究的地方。外部威胁即使Oracle本身具有安全防护功能，某些人仍可能申请一个合法数据库账户，并通过木马之类的病毒程序来监测并获取数据。已经证明外包趋势给公司数据带来了风险，而且那些合同上的远程Oracle数据库管理员提供商有时候实际上数据窃取行动的幌子。一起Oracle数据盗窃之后，很多公司都不好意思或担心对偷窃负面宣传报道，这就使得很难准确的统计Oracle数据失窃问题 聪明地使用Oracle远程数据库管理员已经成为绝对的需要，同时应保证选择本国的提供商，这样就可以用法律来保护自己的数据，而不会再出现跨司法的问题

。互联网中有很多可疑的Oracle远程数据库管理员支持提供商，他们的业务主要针对那些法律上对数据盗窃不能强制执行的国家。已经有一些警告，说Oracle远程数据库管理员支持提供商正是一些数据盗窃的假面具。他们没有公开他们公司远程数据库管理员的姓名和简历 他们没有提及他们的国家背景 Oracle数据管理人员使用Oracle远程数据库管理员的服务是他们自己的危险。如果你居住在美国，那么使用一个美国的远程数据库管理员是绝对关键的，因为在这儿数据隐私可以受法律保护，同时，在数据窃取案中你拥有追索权。你还必须小心维持本国的Oracle支持，避免国外远程数据库管理员支持。这篇名为“海外外包带来隐私风险”的计算机方面的文章仅仅揭露了在委托Oracle数据库给国外公司过程中很少部分的危险 隐私和安全专业人员于上周表示，工作外包给境外地点,大大提高了数据隐私的风险和进行管理的复杂性 这个问题不仅是媒体夸张，而是相当的真实，另外，很多公司已经丢失了对窃贼的关键评论Oracle数据。2004年公司收到一个客户的电话，他一直在抱怨他们的网上数据库的执行问题，这个数据库运行在一个标准的Linux服务器上。这家公司的业务是给第三方公司提供信用信息，用来评估个人财政危机的概率。在访问他们的服务器上很显然存在一些严重的问题。即使是空闲的时候，数据库也在不停的执行输入/输出操作，而处理器也是激活状态。在咨询一位Linux专家之后，我们发现了真正的问题。一个定时炸弹被国外远程提供商激活，一个隐藏的进程在不断地j监测Oracle数据库，吸收新的数据并Email到海外邮箱 恶意的外籍雇员已取代了标准Linux命令，它是一种在互联网上很容易用到的进攻方法。Linux命令被

一个掩盖数据窃取机制的存在的别名取代。数据窃取是如此充满破坏性以至于把公司逼至破产，这些都是因为国外Oracle支持廉价的诱惑。公司发现太晚以至于不可能对窃取Oracle数据起诉。由于骗子们知道他们有了一道坚不可摧的纠葛矛盾的法律和司法管辖的保障。Oracle数据库管理员对其管理有着诚信的责任，应该采取一切可能的安全措施防范Oracle数据盗窃,另外还有一些新的Oracle数据库存取控制标准：监控终端用户威胁--很多Oracle数据盗窃的案件是我们的“合法”系统用户，他们不停地重复交易以窃取数据。大多数公司运用先进的工具来审计和切断可疑的Oracle数据库交易模式。避免国外Oracle支--一次又一次地，国外Oracle开发商和数据库管理员提供商正在偷窃Oracle数据，并知道他们很少有机会被绳之以法。谨慎的Oracle用户会仔细的审核所有远程提供商而只会雇佣他们本国的远程支持提供商。你应该只和一个公开其姓名、背景以及其职员的条件等信息的可信任的供应商。但是并不都是坏消息，因为经济实力比较强的大公司正在寻求正义的审判。保护Oracle数据是一件有意义的事，但是我们在保护知识产权方面已经有了一些进展。以Hew Raymond Griffiths的案子为例，他被从澳大利亚引渡到回美国接受盗版行为的审判，应该指出的是，受害人(微软)大概在花费了巨额的钱财在复杂的证据收集过程和跨司法管理问题上。助理检察长说，“Alice Fisher Griffiths声称超出了美国法律范围之外，而今天，我们证明了另一种方式的存在，这个引渡代表了律政司的对那些其他国家公民违反本国知识产权保护法律也要追究的承诺”，美国律师Chuck Rosenberg也说：“我们代理商和检察官都在不知疲倦地工作,捉住知识产权小偷,即使

其罪行跨越国际边界。”在时间上我们期待看到越来越孤立Oracle数据库作为一个防火墙,不受外来威胁,我们也越来越清楚,所有Oracle数据库管理员必须加大力度履行作为公司数据的管理人的职责。100Test 下载频道开通,各类考试题目直接下载。详细请访问 www.100test.com