专注APT攻击与防御

https://micropoor.blogspot.com/

程序的主要function，与 procedure

注：Delphi把操作数据的方法分成了两种，一种是function，另一种是procedure，大致理解为“函数”和“过程”。

Procedure类似C语言中的无返回值函数，即VOID。而Function就是c语言中的有返回值函

数，即没有Void。

程序分为2种连接数据库模式：

无论是本地模式，还是联网模式，都是读取，当前路径的config.ini配置文件：

（导致敏感信息暴漏，可直连服务器）

继续跟数据库连接：配合SQL Server数据库，直接带入，可以判断出为明文存储。

config.ini配置如下：

基于TCP通信，SQL Server通信构架大致如下：（可导致通信过程中抓取明文执行）

代入执行：

（导致可拼接sql语句，查询任意语句或者执行命令）

部分语句其中如下：

select distinct memberid,receivecompany from weigh where receivecompany is not null and receivecompany like ''%'+xxxxxx+'%''

软件呈现如下：

对应 收货单位编号，以及收货单位名称。分别为：memberid,receivecompany闭合语句为：

2' ; select loginid as memberid , password as receivecompany from sysuser --

抓取返回如图：

得到admin 账号以及密码。

构造读取远程桌面端口号：

得到远程服务器端口号

2' ; EXEC master..xp\_regread 'HKEY\_LOCAL\_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp','PortNumber' --

copy 获取缓冲区内容：

（导致可从服务器端构造代码）

copy 用法如下：copy（a,b,c);

a：就是copy源，就是一个字符串，表示你将要从a里copy一些东西，

b：从a中的第b位开始copy（包含第11位），

c：copy从第b位开始后的c个字符，

exp： m:=‘the test fuck'

s：=copy（m,2,2）； //s值为‘he’

当超出范围，会发生异常错误。实例中，从服务器数据库获取数据后进行copy。

软件登陆部分代码如下：

（导致可自动化跑 loginid。）

多次尝试错误处理如下：退出软件，并且重新开始计算。

Micropoor