

# 哈哈哈哈哈，這個勒索軟件笑死我了！

程序員的那點事 今天

以下文章來源於編程技術宇宙



**編程技術宇宙**

一個專注用故事講解技術的公眾號



來自公眾號：

## 又見勒索軟件

一個讀者微信上緊急聯繫我說，自己的電腦中了勒索病毒！

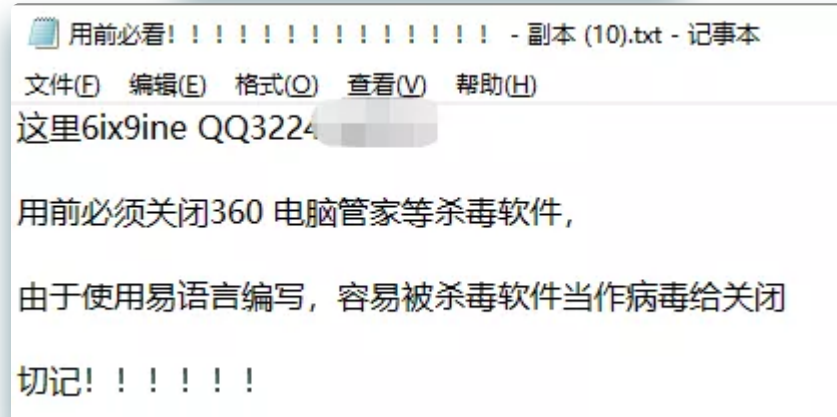
自從之前寫過一篇挖礦病毒的文章後，就收到過不少朋友的消息讓我幫忙處理，不過平時上班太忙，很難抽出功夫分析。這次剛好是假期，就收了魚竿回去分析起來（其實是蹲了一下午，魚兒不給面子）。

不分析不知道，一分析把我裂開了，這是我見過最菜的勒索軟件了。

這位讀者把勒索程序發給了我，這是一個用

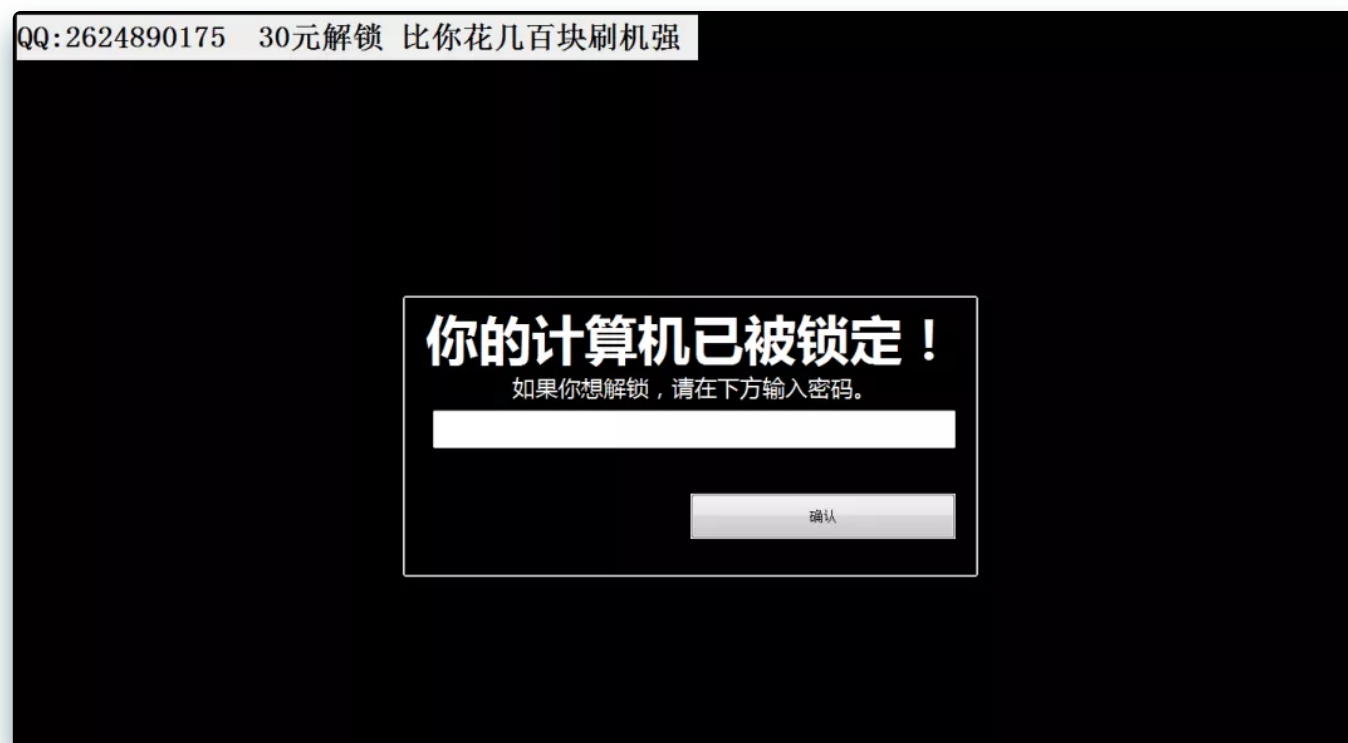
qq开户.exe

用前必看!!!!!!!!!!!!!!!!!!!!



好家伙，居然還騙使用者把安全軟件關掉，理由是容易被當病毒給關閉，這一波偽裝666。

好啦，咱們在



一執行屏幕就黑了，全屏出現了上面這個界面。

引導語還很氣人：

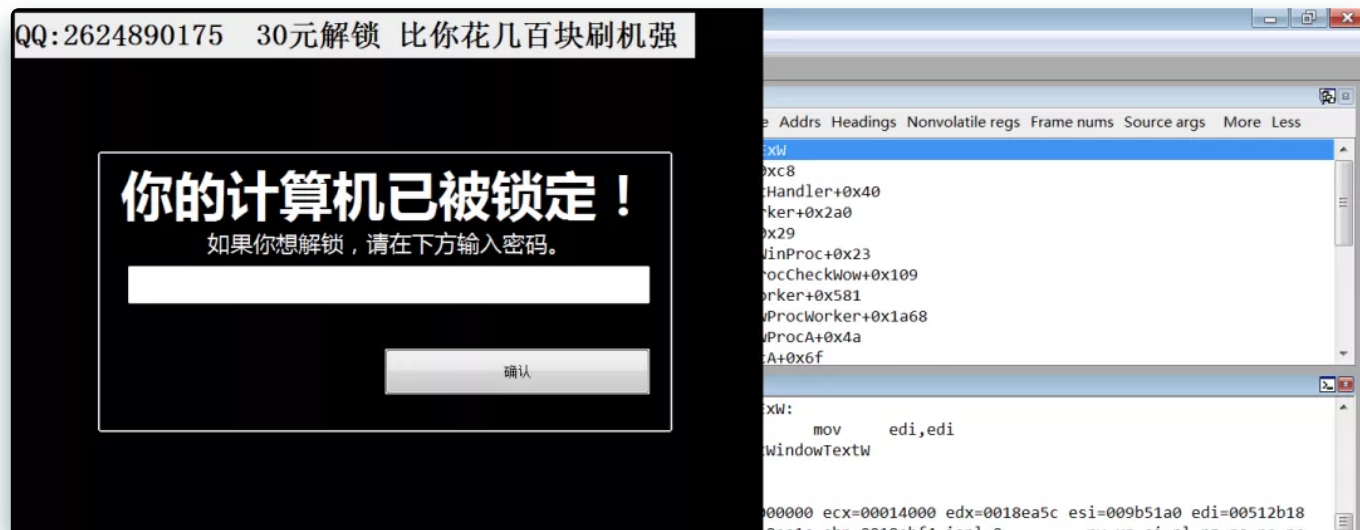
最神奇的是居然還留下了QQ聯繫方式，這病毒製作者看來也是新手，就憑這QQ號，網警分分鐘就能找上門。

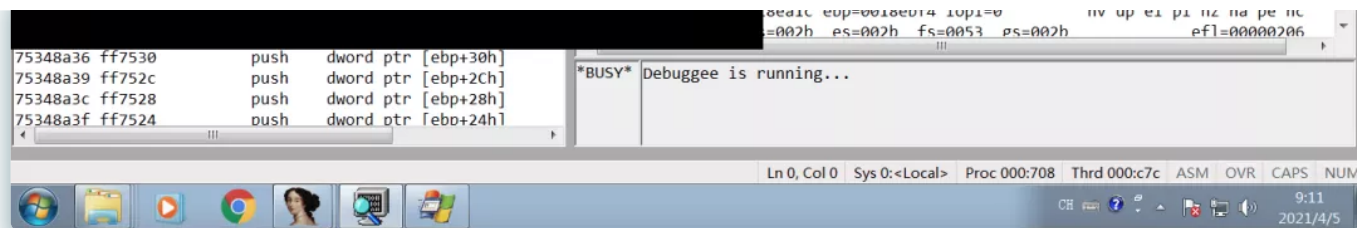
我沒有給這個QQ號打碼，因為我在QQ上搜了這個號碼，已經搜索不到了，不知是已經被端了，還是自己害怕了設置了不允許被搜索到。

接下来，我发现了一个很有意思的现象：我的虚拟机是在macpro上的vmware fusion上面，当我从虚拟机切到Mac系统的屏幕再切回去时发现，虚拟机中Windows的分辨率自动给我重置了。

这一重置不要紧，刚刚这个勒索软件一下子只有半截了，露出了本来面目：**原来就是一个全局置顶的窗口**，还没有跟随系统分辨率的变化自动调整窗口大小，也是太菜了。

现在这问题就简单了，直接调出任务管理器，把这货的进程杀掉就行了！



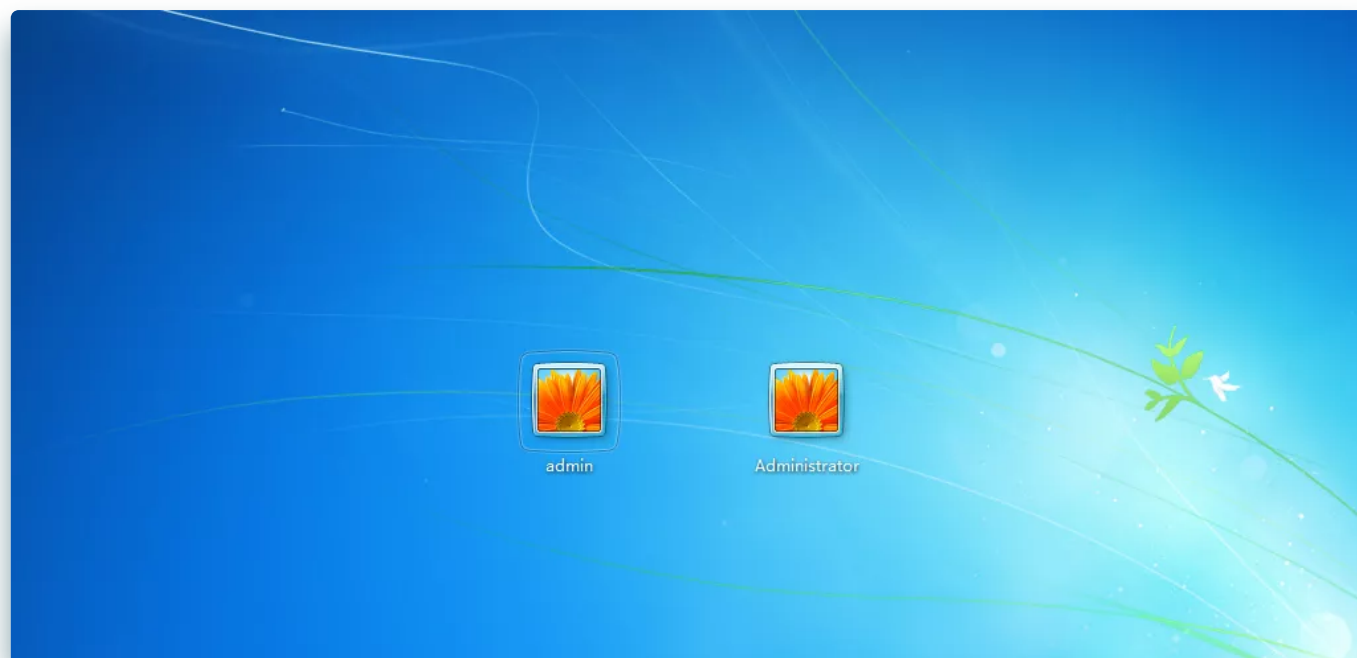


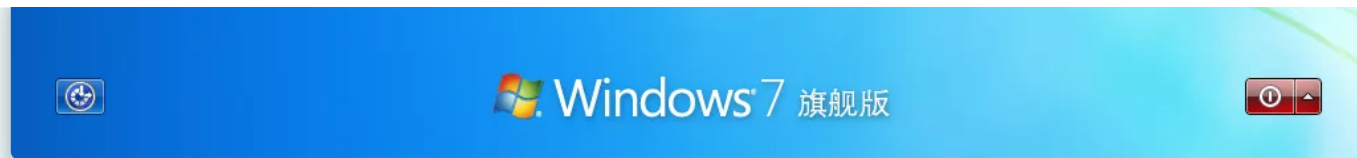
不过考虑到我这是在vmware fusion虚拟机中，才自动调整分辨率，在真实的电脑上，中招的电脑上没有机会调整分辨率，也没法操作把任务管理器给调出来，所以还得看看有没有其他破解之道。

我打算重启后看看这家伙有没有加入开机自启动。

我重启了虚拟机，发现这货居然给我添加了1个admin用户进去，还给我原来的默认用户Administrator添加了密码！！！！

这下好了，真进不去了！






好了，接下来开始启动分析，摸摸这勒索软件的斤两。

## 分析过程

我先把目标锁定在了添加用户这部分，因为得先能进入系统才好调试分析。虽说这软件是用易语言编写，但实际上最终都是会调用Win32的一堆API，所以我开始搜索程序的导入表中与用户添加相关的API：

### User Functions

05/31/2018 • 2 minutes to read • 

The network management user functions control a user's account in the security database, which is the security accounts manager (SAM) database or, in the case of domain controllers, the Active Directory. The user functions are listed following.

Function	Description
<a href="#">NetUserAdd</a>	Adds a user account and assigns a password and privilege level.
<a href="#">NetUserChangePassword</a>	Changes a user's password for a specified network server or domain.
<a href="#">NetUserDel</a>	Deletes a user account from the server.
<a href="#">NetUserEnum</a>	Lists all user accounts on a server.
<a href="#">NetUserGetGroups</a>	Returns a list of global group names to which a user belongs.
<a href="#">NetUserGetInfo</a>	Returns information about a particular user account on a server.
<a href="#">NetUserGetLocalGroups</a>	Returns a list of local group names to which a user belongs.
<a href="#">NetUserSetGroups</a>	Sets global group memberships for a specified user account.
<a href="#">NetUserSetInfo</a>	Sets the password and other elements of a user account.

搜寻了一圈发现这软件并没有是用上面的任何函数，那它是咋添加的用户？

我改变了策略，它不是要添加用户吗，用户不是叫admin嘛，那我搜索程序中有**admin**相关的字符串。这一搜惊掉了我的下巴：

```
.data:0040913F aNetUserAdminis db 'net user Administrator 69',0  
.data:00409159 aNetUserAdminAs db 'net user admin asdfghjkl /add',0  
.data:00409177 aNetLocalgroupA db 'net localgroup administrators admin /add',0
```

看来我太高估这个程序了，不用什么Win32 API，直接调用cmd执行命令就行了。

而且，命令啥的这么重要的信息完全明文暴露，密码也就真相大白了：

- admin: asdfghjkl
- Administrator: 69

admin的密码我好理解，就是键盘上A键开头的那一排英文字母嘛，可这个Administrator的密码为什么是69，69是什么意思？我到现在都没想明白。

持着怀疑的态度，输入上面的密码，还真给进去了，这也太菜了X2~~

不过一进去，马上又弹出了那个黑色的勒索界面，看来还真是加入了开机启动项。

我随意输入了一些密码，都是提示密码错误，看来还得再琢磨一下它的密码是如何校验的。

QQ:2624890175 30元解锁 比你花几百块刷机强



这种情况，一般都是先定位到执行密码校验的部分，然后分析判断逻辑。

定位的方法在这里可以给GetWindowText和SetWindowText下断点，这两函数分别是获取密码输入框的内容和设置“密码错误”的提示。

通过两个函数的调用堆栈，往前倒推，执行密码校验的部分很快就能圈定。



不过还没等我用上面的方法来分析，这个勒索软件真正让我裂开的地方出现了，我在“密码错误！”的提示字符串旁边，看到了另外一串字符，跟Administrator的密码一样，也是**asdfghjkl**。

```

00409130 00 00 00 3F 01 00 00 00 00 00 00 00 00 00 00 6E ...?.....n
00409140 65 74 20 75 73 65 72 20 41 64 6D 69 6E 69 73 74 et·user·Administ
00409150 72 61 74 6F 72 20 36 39 00 6E 65 74 20 75 73 65 rator·69.net·use
00409160 72 20 61 64 6D 69 6E 20 61 73 64 66 67 68 6A 6B r·admin·asdfghjk
00409170 6C 20 2F 61 64 64 00 6E 65 74 20 6C 6F 63 61 6C l·/add.net·local
00409180 67 72 6F 75 70 20 61 64 6D 69 6E 69 73 74 72 61 group·administra
00409190 74 6F 72 73 20 61 64 6D 69 6E 20 2F 61 64 64 00 tors·admin·/add.
004091A0 5C 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 \.....@.....
004091B0 00 73 40 00 00 00 00 00 00 63 40 61 73 64 66 67 .s@.....c@asdfg
004091C0 68 6A 6B 6C 00 C3 DC C2 EB B4 ED CE F3 A3 A1 00 hkl.密·码·错·误·! ..
004091D0 C4 E3 B5 C4 BC C6 CB E3 BB FA D2 D1 B1 BB CB F8 你·的·计·算·机·已·被·锁·
004091E0 B6 A8 A3 A1 00 38 00 00 00 EE 08 00 00 01 00 00 定·! ..8.....
004091F0 00 66 6F 72 6D 00 00 00 00 00 00 00 00 00 00 .form.....

```

这会是个啥，我怀着试试的态度，输入到了密码输入框，点击确定，居然奇迹般的解开了锁定！30元的勒索密码就这样明文躺在错误提示的旁边，你敢信？

这勒索软件也太菜了X3！

## 教你几招

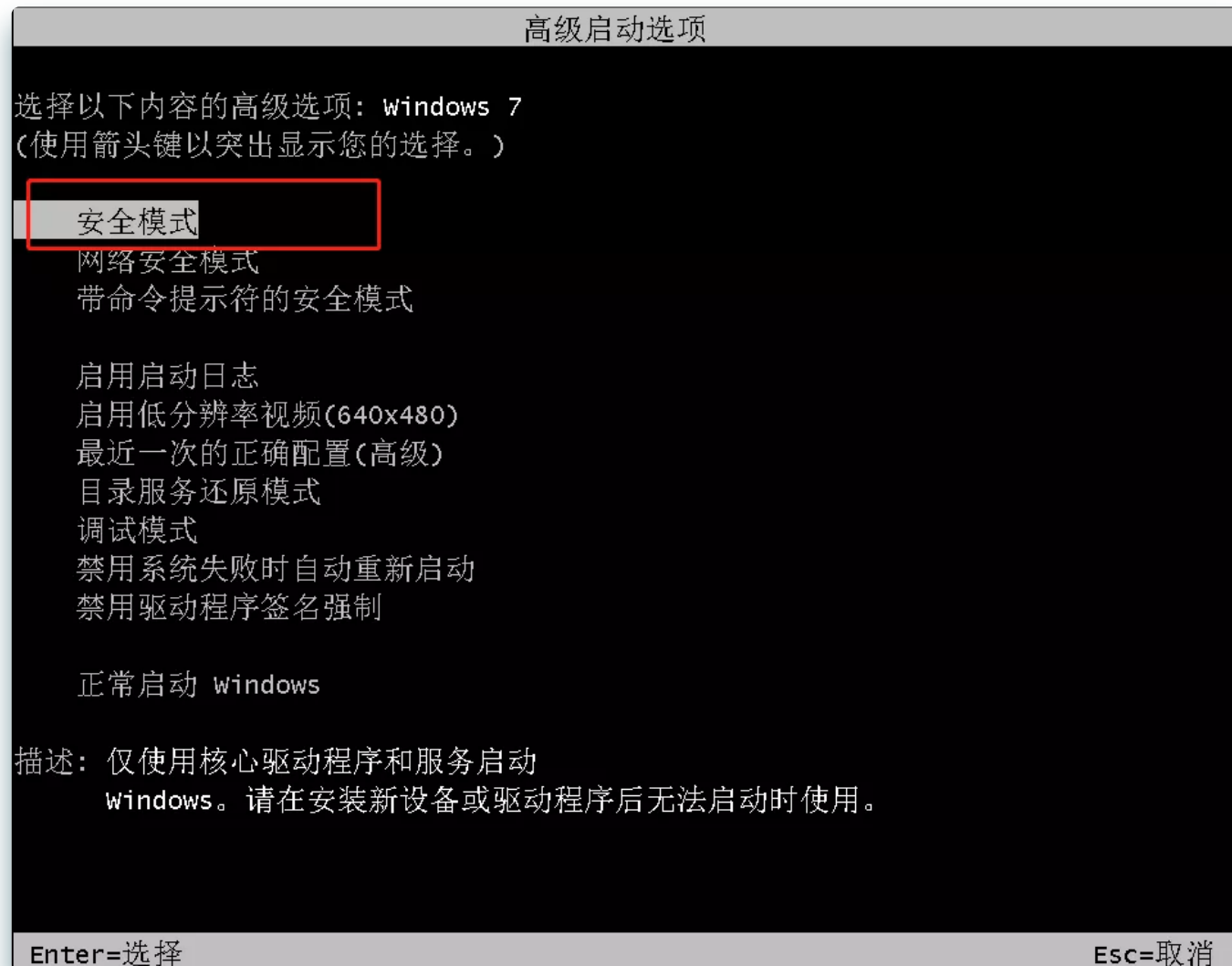
言归正传，懂技术的人能看出，这勒索软件做的确实不入流，技术一般也就罢了，还明目张胆的暴露了自己。不过，这软件菜归菜，如果是普通用户遇到了，还确实是件比较头疼的事情。

接下来轩辕这里介绍几招，遇到了一般的勒索软件不要慌。

## 安全模式



安全模式是Windows提供的一种启动模式，在这种模式下，普通的开机自启动程序都不会执行，很多驱动程序也不会加载，是一个相对干净的环境，你可以进入这个环境下删除病毒程序。

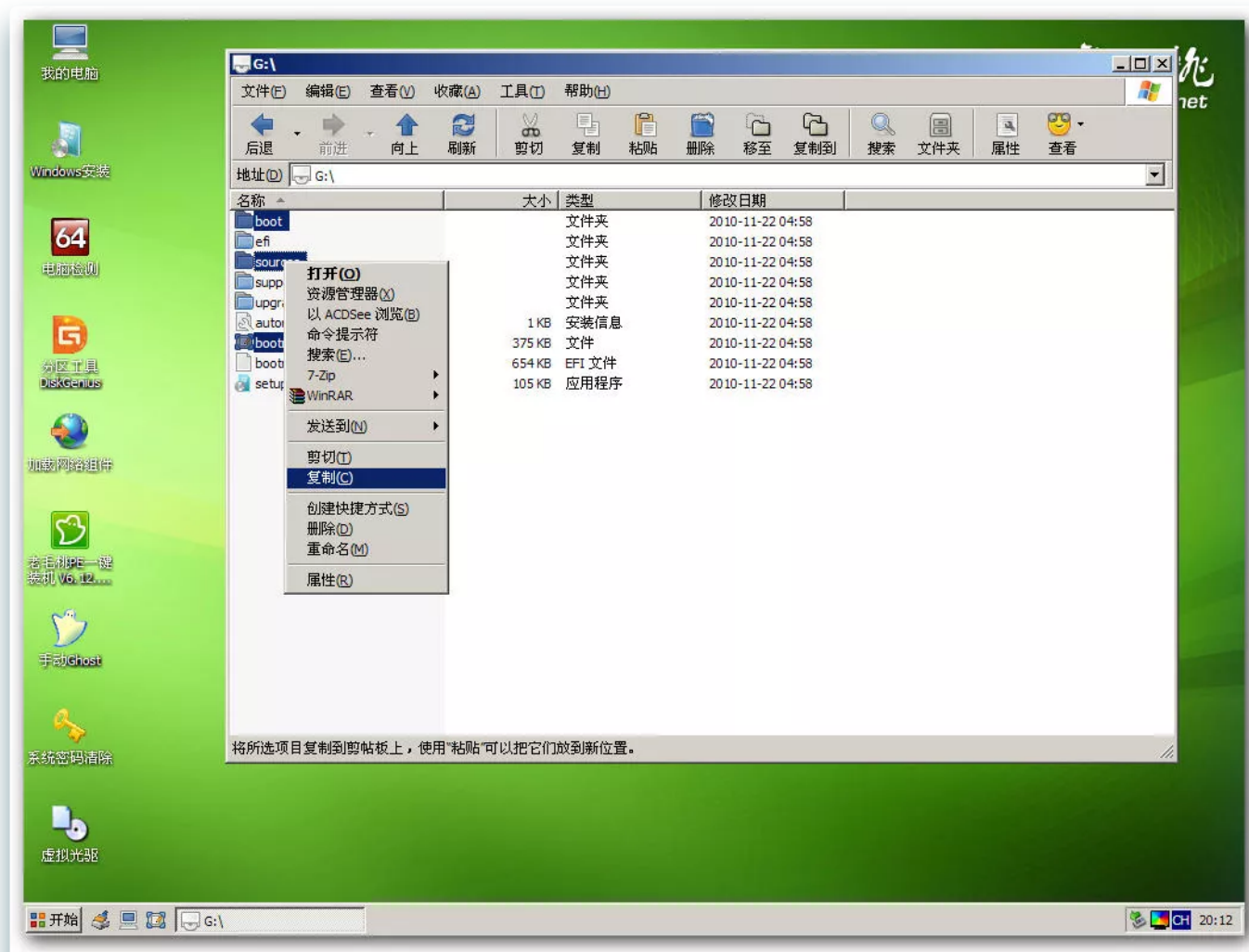


U盘进入

安全模式也不是万能的，有些比较厉害的程序，即使进入安全模式也会运行，这种情况下就得另辟蹊径。

针对这种级别的入侵，可以选择像用U盘安装系统那样，使用U盘制作一个启动盘，修改BIOS中的引导项，使用U盘引导。

开机后，直接进入U盘中的WinPE环境，这是一个用于预安装的小型系统，进入这个环境清除掉硬盘上的勒索软件程序。



最後的最後，還是老生常談了，重要的數據多備份，雲盤、移動硬盤、電腦都存著，狡兔還三窟呢，應對勒索軟件，備份才是王道！

--- EOF ---

推薦↓↓↓



### 程序員求職面試

分享程序員找工作經驗，程序員筆試、面試題



公眾號

喜歡此內容的人還喜歡

如果惡魔給你一億，一年之後必須還兩個億，你會接受嗎？

了不起的程序員



程序員的噩夢之一

程序員的幽默



某985學歷程序員嫌棄女朋友高職畢業學歷低，但女朋友實在太漂亮，好猶豫！

程序員八卦

