我们拥有多年的区块链服务经验，为用户提供专业的服务信息。以下是撕币和撕币的最新消息。选择可以随时随地解决玩币遇到的各种问题，让你不再为职称评定的繁琐业务而烦恼。

专家教你清除rootkit整篇文章

首先大家一定要明白什么是Rootkit？

rootkit基本上是由几个独立的程序组成的。典型的rootkit包括：以太网嗅探器程序。，用于获取网络上传输的用户名、密码等信息。特洛伊木马程序，为攻击者提供了后门。隐藏攻击者目录和进程的程序。它还包括一些日志清理工具。攻击者利用它删除wtmp、utmp、lastlog等日志文件中的上述文章，这些日志文件是自己行踪的条目。复杂的rootkit还可以向攻击者提供telnet、shell和finger等服务。。它还包括一些脚本来清理/var/log和/var/adm目录中的其他文件。

最近最让IT管理员头疼的是什么？毫无疑问是rootkit。这个可恶的程序是工具的集合。黑客用它来掩盖对计算机网络的入侵，获得管理员权限。黑客一旦获得管理员权限，就会利用已知漏洞或破解密码安装rootkit。然后rootkit会在网络上收集用户ID和密码。，使黑客拥有高级访问权限。

rootkit还具有监控网络数据和密钥的功能；打开一个&quot后门&quot黑客系统研究；修改日志文件；攻击网络上的其他计算机；修改系统上的现有工具，以防止它们被检测到。。那么如何找到rootkit呢？让&#039；让我们看看三位Windows安全专家为用户提供了什么解决方案&#039；srootkit问题。//本文来自计算机软硬件应用网

用户&#039；问：我是一家大型非营利组织的IT管理员。由于我们缺乏资金和人力，我们的许多用户需要管理员权限来完成他们的工作。最近，越来越多的用户抱怨他们的管理员应用程序崩溃。。他们的一些管理软件不再工作，例如，一些系统上的防病毒软件神秘地失败了。有的尝试使用应用时蓝屏死机，有的电脑莫名其妙重启或发出错误信息。普通间谍软件和木马扫描工具没有发现问题。。什么&#039；在工作吗？我们需要重新安装所有有问题的电脑吗？

专家教你清除rootkit的诊断：

KurtDillard:细节缺失，但有一些关键信息。。之前一直很可靠的各种计算机系统频繁出现操作系统崩溃，意味着被感染的计算机中的某些东西被改变了。另一个重要线索是防病毒软件会自动关闭。最后一条线索是标准安全工具可以&#039；没有发现任何恶意软件，这表明如果这些电脑中有新软件，这个软件正在秘密运行。这种

文件是隐藏的，但它仍然在运行。如果唯一奇怪的事情是无数的系统崩溃我怀疑操作系统的最新补丁、设备驱动程序或某个安全应用程序有问题。这些症状结合在一起表明有恶意的东西在起作用。然而，它可能不是一个rootkit。你必须做额外的研究来发现正在发生的事情。。

劳伦斯艾布拉姆斯：当你的电脑开始出现异常时，我首先想到的是你的电脑被间谍软件、病毒、木马、蠕虫或其他形式的恶意软件感染了。。如果在使用防病毒软件和/或反间谍软件扫描后问题仍然存在，那么是时候使用一些工具进行深入分析了。需要检查的是电脑的启动程序，看是否有当前杀毒软件中没有定义的新的恶意软件。。一些故障检测的软件程序有：

HijackThis:这是一个通用的主页劫持检测和清除工具，可以持续更新。

WinPFind:这个工具软件可以扫描硬盘上常见的位置。查找与已知恶意软件的使用方式相匹配的文件。

SilentRunners:这个软件工具检查Windows是如何启动的，并创建一个文本文件用于研究或存储作为基准。。如果未检测到任何内容，请尝试在安全模式下运行此程序和您的防病毒/反间谍软件。许多常见的rootkit发布蠕虫可以&#039；不要在安全模式下运行。因此，故障排除软件可以在安全模式下看到这些恶意软件。

如果在安全模式下发现新的记录和文件，计算机可能会被常见的rootkit感染，该rootkit可以&#039；在Windows正式模式下不可见。另一方面，如果你在安全模式下运行相同的工具软件，但仍然没有&#039；我没有发现任何可疑的现象。但是，这种恶意软件的行为仍在继续，您可以猜测您正在处理更高级的rootkit。KevinBeaver:考虑到已安装应用程序的奇怪行为，您可能正在处理某种恶意软件。，很可能是rootkit或远程访问特洛伊木马。这些恶意软件可以让黑客从外部潜入未受保护的计算机。了解这一点的唯一方法是运行其他扫描软件，这些软件可以扫描或监控异常行为和rootkit的存在。。这个工具可以是&quot主要回应&quotSana安全公司的，或者Finjan软件公司和&quotRootkitRevealer&quotSysinternals公司的。

我还建议同时运行至少两三个反间谍工具。也许会有一些你没有的工具和软件&#039；t二手。。除了常见的解决方案，如Spybot-SearchDestroy和LavasoftAd-Aware安全软件，还有一些工具。。我很幸运地使用了管群国际的PestPatrol和微软的AntiSpyware等工具。。监视旧系统活动的另外两个工具是监视和阻止出站通信的个人防火墙(不是Windows防火墙),以及可以监视进出可疑系统的网络通信的网络分析器。当然，只有当您的系统连接到网络时，后一个选项才可用。

专家教你立即采取行动清除rootkit:

KurtDillard:首先，断开受影响系统与网络的连接是个好主意。接下来，你需要决定你愿意投入多少时间。。你愿意收集可能被用于刑事指控的证据吗？收集证据是非常耗时的，你必须仔细遵循适当的证据收集程序。您是否希望确定此事件的根本原因，以便采取具体措施来堵塞任何已被利用的安全漏洞？这也需要很多时间。。或者像我们大多数人一样，你没有&#039；t没那么多时间，只想尽快排除故障，让系统恢复正常？不管你选择什么方式，我希望你能在事件发生之前，制定出具体的事件应对方案。如果你不&#039；我没有这个计划你应该确保写一份适合你的组织的商业需求的书面计划。

收集可以在法庭信息系统中使用的证据需要严格的程序，将发生的一切归档并保护原始数据。我建议你应该与你的组织的法定代表人和一些业内专家合作，在事件发生前制定一个计划。。你应该使用逐字节复制的工具和其他软件(即制导软件公司的EnCase、AccessData公司的FTK成像仪或X-Way软件技术公司的WinHex)。将受影响的系统存储在安全的地方，并将这些工具和软件创建的数据整理出来供法庭使用。

找出问题的细节可能要花很多时间。然而，这部作品很吸引人，也很有教育意义。。有一些rootkit检测工具：

rootkitrevealer(由著名且受人尊敬的安全专家MarkRussinovich和BryceCogswell制作)

。

Blacklight(知名安全软件厂商F-Secure出品)

Klist(卑鄙内核模式rootkitFU作者出品——你需要决定是否让你的网络信任这个程序员)。

这些工具都有自己独特的功能和缺陷。我喜欢用RootkitRevealer。然而，恶意软件作者不断更新他们的工具，以避免最新的检测应用程序，所以我最喜欢的工具可能无法检测所有恶意软件。您可能需要手动执行白皮书&quot捉鬼敢死队&quot，微软研究院2004年发布的工具软件。总之您应该在系统启动时拍摄系统快照，并收集每个硬盘的目录列表等信息。然后，您使用备用操作系统启动计算机，并将您在干净的操作系统中看到的内容与操作系统中损坏的内容进行比较。

如果你不&#039；如果没有时间，您可以在断开受影响的计算机系统与网络的连接后，直接进入恢复阶段。

LawrenceAbrams:如果你发现的rootkit看起来像是捆绑了各种恶意软件的普通rootkit，那么把这台电脑断网应该足够作为你的第一个措施了。。这将防止其传播，并可能下载和安装更多的恶意软件。

另一方面，如果你确定是目标rootkit，专门闯入这台电脑，由一个人安装，那么你应该听从你的组织&#039；美国对付侵略的政策。不幸的是，大多数公司对此类事件没有政策。如果你可能采取法律行动，至少你应该立即制作一个可以在法庭上使用的硬盘镜像。保存原电脑作为法庭证据使用。如果你不&#039；如果你不打算采取法律行动，你可以直接进入恢复阶段。凯文比弗：我的第一个建议是把电脑从网络上断开，但是这只有在你能承担损失的情况下(即不影响主营业务经营的情况下)才能做到。这样做有助于防止任何恶意软件传播或影响其他网络计算机。第二，安装/运行我在诊断阶段提到的应用。。您可能需要运行这些程序来监控系统的操作。然而，一旦系统被感染，检测程序很难(如果不是不可能的话)发现异常或正常的行为。这个主要看具体工具的工作情况。

专家教你清除rootkit的恢复系统：

KurtDillard:不幸的是，&quot通过核打击将网站送入轨道&quot是最强有力的恢复方法。一旦黑客闯入你的电脑，您永远无法确定已经找到并清除了所有被修改的内容。

如果您有最新的备份，请按照下列步骤操作：

1。从受感染的计算机上移除硬盘，并将其安装在另一台干净的计算机上；

2。从干净的系统备份数据；

3。删除受影响计算机的操作系统，并使用已知良好的介质为受影响计算机重新安装操作系统；

4。采取预防措施阶段介绍的步骤，尽最大努力确保系统的安全；

5。将数据恢复到重建的计算机上；

6。使用最新的杀毒软件和反间谍软件对恢复的数据进行全面扫描。

7。不要存储任何可执行文件。最好的方法是故意删除任何可执行文件，如二进制文件、脚本和ActiveX控件。

劳伦斯艾布拉姆斯：很难从rootkit的影响中恢复过来。。如果rootkit是普通的、无针对性的恶意软件安装的，那么清除这种侵害你电脑的恶意软件应该比恢复你的电脑更难。另一方面，如果你面对的是黑客卫士、HE4Hook、Vanquish或FU等rootkit，那么就是黑客故意在目标电脑上安装了这些rootkit。记住这个问题。你&#039；你永远也猜不到这些rootkit在你的电脑上安装或修改了什么。黑客可以通过注册表修改安全设置，用被黑的文件替换系统中的重要文件，或者控制受害者&#039；的计算机或网络。在这种情况下我总是建议备份数据并重新安装操作系统。将数据复制到新安装的计算机之前，请扫描数据以查看它是否被感染。

如果无法重新安装计算机，您可以使用rootkit检测器来查找属于rootkit的文件。这类工具软件有Blacklight、RootkitRevealer、Flister等。因为这些文件在rootkit程序之外可能是不可见的您可以使用可引导的Linux分发软件，如KNOPPIX、启动盘，或者通过网络共享清除这些文件(不推荐)。

最后，如果你有资源重装电脑，可能是你最好的选择。

凯文比弗：如果你不。检测不到任何rootkit，但异常行为继续出现，你最好的和最安全的选择是重新格式化和重新安装系统。在此之前，您应该确保备份所有必要的文件。。因为目前大多数恶意软件(尤其是rootkit)不会感染二进制或文本文件，所以这样做是非常安全的。恶意软件主要感染操作系统和应用程序使用的可执行文件和支持库文件。。如果可以清理系统(如果发现rootkit就很难了)，就需要经常扫描系统，监控其他可疑行为。再次强调，一定要使用我在诊断阶段提到的工具。

专家教你清除rootkit的预防措施：

KurtDillard:可以采取很多对策。以下是五个最有效的措施：

1。避免使用具有管理员权限的帐户登录。。您可以通过使用Windows内置的RunAs或MakeMeAdmin等工具来实现这一点。

2。为整个网络运行防火墙集，并为每个端口分配防火墙软件。，如Windows防火墙(包括WindowsXPSP2)；

3。让您的Windows和其他软件使用最新的补丁程序和服务包。如果您只有几个系统您可以使用诸如&quot自动更新&quot。如果您有许多系统，您可以使用Windows服务器来更新服务。

4。使用流行的防病毒软件和最新的特征码库。。要了解有关防病毒软件供应商的更多信息，请参考Microsoft防病毒合作伙伴网站；

5。使用最新的间谍软件防护工具，如Microsoft&#039的Windows反间谍软件。

要了解更多关于降低被该恶意软件攻击的风险的想法，请参考我最近发布的技术指南。

LawrenceAbrams:安全中最重要的一步是尽一切努力防止用户以管理员身份登录网络&#039；的权威。可以理解的是，在当前的Windows体系结构中，这并不总是能够实现的。当恶意软件感染计算机时该恶意软件将以与登录用户相同的安全级别运行。所以，如果用户有管理员权限，这个恶意软件也会有管理员权限。该权限使恶意软件可以完全访问您的计算机。

使用最佳实践来防止其他恶意软件也可以防止rootkit(无论是由目标蠕虫还是病毒蠕虫携带)。

1。使用防火墙来阻止经常被黑客破坏的WindowsTCP端口。例如端口20、21、23、80、135、139、443和445。从源头堵住这些端口，你首先会降低被黑的风险。最佳实践是阻塞每个端口，只将一个端口映射到需要打开该端口的机器。。这些端口是最近蠕虫利用的程序中的安全漏洞。如果某台计算机需要使用上述端口，防火墙应该确定哪台计算机可以通过该端口远程访问该计算机，而不是让该端口完全开放；

2。和每台计算机都应该有最新的安全更新，并运行每天更新的防病毒软件。病毒软件的新定义经常发布，因此拥有这些最新定义非常重要。

3。除了反病毒软件之外，还需要至少两个反间谍工具，比如在电脑上安装Spybot-Search和Destroy，Webroot软件公司的SpySweeper或者Lavasoft公司的Ad-Aware。。使用最新更新每天或每周扫描一次可以自动利用最新的病毒定义；

4。最后一个，但不是最不重要的。应该教育用户采用良好的实践。。用户应该知道不要点击互联网广告、陌生人从即时消息中发送的链接或陌生人发送的附件。如果新的蠕虫开始传播，IT人员应立即向所有用户发送电子邮件，解释附件、配置或措辞。

有了现成的防火墙、反恶意软件工具、最新的安全更新和良好的互联网用户指南，您应该能够避免被这些类型的恶意软件感染。

凯文比弗：只要计算机是人类操作的，或者是联网的，就没有办法保证绝对的安全。但可以安装反间谍软件、rootkit检测工具和监控异常情况的软件，保证系统的安全性。理想情况下，如果你被袭击了一次，不要&#039；我不想再被攻击了，你&

#039；最好安装上面提到的三种安全软件。另外，这句话可能是老生常谈，但要强调。您应该确保严格执行所有操作系统和应用程序都使用最新安全补丁的规则。

木马病毒是不是与

病毒有很大区别的主要数据破坏？破坏软硬件的目的主要是

木马程序窃取数据，篡改数据木马

的目的可能是失去对账号、各种密码、用户名的访问。，你的电脑&#039；s远程控制，打开外围设备远程控制你的机器

木马程序是目前比较流行的病毒文件，它并不&#039；t复制自己，它不会&#039；t&quot故意&quot感染其他文件。它通过伪装吸引用户下载并执行一个木马，这个木马就是门户网站。提供开放种子程序的计算机可以破坏任何类型的设施，根据品种窃取这些文件，甚至远程控制谁是计算机类型。。木马有点类似于计算机网络中经常使用的远程控制软件，但由于远程控制软件是善意控制的，所以通常不会隐藏。木马则相反，应该认识到。"盗窃&quot的遥控器，如果没有很强的隐蔽性。，是&quot一文不值&quot。

一个完整的特洛伊木马程序由两部分组成：&quot服务器&quot在&quot控制&quot而植入物被植入所谓的&quot黑客&quot。&quot服务器&quot零件用途&quot控制器&quot到&quot服务器&quot运行计算机。。特洛伊木马运行&quot服务器&quot，任何一个是计算机的人都必须打开一个或多个端口，这样黑客就可以利用这些打开的端口进入计算机系统，安全和个人隐私将得不到保障！病毒附着在一段计算机代码上。可以在计算机之间传输的程序或文件。和被感染的电脑，当它传播的时候。病毒可能会损坏您的软件、硬件和文件。

病毒(名词):明确自我复制代码编写的目的。病毒附着在宿主程序上。然后试着从一台电脑传到另一台电脑。否则，可能会损坏硬件、软件和信息。

按照严重程度分类，像人类病毒(埃博拉病毒来源于常见的流感病毒)，计算机病毒分为轻型和重型，重型只造成部分干扰，重型设备完全被破坏。。幸运的是，真正的病毒没有人员是不会传播的。您必须共享文件，并通过一个人发送电子邮件来一起移动它。

的全称&quot特洛伊木马&quot是&quot特洛伊木马&quot。古希腊士兵藏在木马里变成敌人的故事&#039；占领这座城市，所以敌人&#039；s市。在互联网上，&quot特洛伊木马&quot指的是一些程序员(或者恶意马夫)，他们可以从网络应

用或者游戏，或者网页上(下载)插件。包含用户的计算机系统可以控制或下载用户的信息，这可能导致用户&#039；系统被破坏、丢失甚至导致系统崩溃。

一个木马功能

服务器型号/木马。它分为两部分。，在客户端和服务器端。它的原理是一台主机服务(服务端)，另一台主机接收服务(客户端)。作为服务器，主机通常会打开一个默认端口进行监控。如果您有客户端连接请求。，相应的程序会自动运行在承诺的服务器到客户端请求的服务器的端口上。这个过程叫过程。

一般发现后门木马，窃取密码的基础。统计显示，现在木马病毒超过了四分之一。近年来，病毒、木马和病毒统治阶级的汹涌浪潮将在未来几年内增加。特洛伊木马是一种特殊的病毒。如果你不小心把它当成一个软件，电脑上的木马就会&quot善良&quot。互联网之后，电脑已经完全把控制权交给了黑客。他将能够通过跟踪键盘输入来窃取密码、信用卡号和其他机密信息，他还可以跟踪计算机监控、控制、查看和数据操作。

二、木马攻击特征

在使用电脑的过程中，如果你发现电脑&#039；的反应速度变了，硬盘在不停地读写，鼠标没有&#039；t工作，键盘无效，他们的一些窗口关闭，新窗口莫名其妙打开，网络传输指示灯不停闪烁，系统越来越慢。，占用大量系统资源，站内，或者运行一个没有体现的程序(这类程序一般比较小，从十几元到几百KK不等)，或者当你关闭一个程序的时候，有防火墙检测到发送的消息.这些异常表明你的电脑中了木马病毒。

三、木马项目及手动查杀介绍

因为大部分玩家对安全问题了解很多，所以不&#039；我不知道如何删除&quot特洛伊木马&quot在他们的电脑上。所以，最重要的是要知道木马的工作原理，这样才会很容易发现木马。。相信看完这篇文章，你会成为一个杀人高手&quot特洛伊木马&quot。(如果可以&#039；不要以客为尊，建议你用橡皮筋打竹楼玻璃，呵呵)

木马会想尽一切办法隐藏自己。主要方式有：把自己藏在任务栏里。这是最基本的形式。Visible属性为False。SHOWINTASKBAR设置为False，因此程序运行时不会出现在任务栏中。在任务管理器中不可见：此程序被设置为&quot系统服务&quot很容易伪装自己。

A、启动一组类(即机器启动时文件组运行)

当然木马会悄悄启动，你当然不&#039；t不希望用户单击&quot特洛伊&quot图标来运行服务器。(没有人会这么傻吧？之后)。木马会在用户每次启动服务器时自动加载，应用程序也会自动加载。启动时会在Windows系统中使用木马，比如：startupgroup，win.ini，system.ini。、注册表等等都是&quot特洛伊人&quot藏身的好地方。Win.ini和system.ini用于加载木马。在Windows系统上，win.ini和system.ini都存储在C:Windows目录中。可以用记事本打开。你可以用“quotload=file.exe程序，Run=file.exe&#039s&quot在win.ini文件窗口中实现自动加载木马的目的。此外根据&quotshell=Explorer.exe&#039s&quot(Windows系统界面的图形命令解释程序)在系统的启动部分。INI一般情况下。让&#039；让我们具体谈谈木马是如何自动加载的。

1。在win.ini文件中的[WINDOWS]下，&quotRun=&quot和&quotLOAD=&quot可能的装货路线。木马一定要密切关注。一般情况下，它们后面没有等号。如果你发现后面的路径和文件名不是你熟悉的启动文件，你的电脑可能是木马。当然，你必须观看它，因为许多&quot特洛伊人&quot，如&quotAOLTrojan特洛伊木马&quot，把自己伪装成COMMAND.EXE的档案。如果你不&#039；不注意，你可能不会发现它不是一个真正的系统启动文件。

使用c:windowswininit.ini文件。很多木马在这里做一些手脚，这种方法经常用在安装文件中。，文件将在安装后立即执行，原始文件将被删除。同时会进行干净的Windows安装，所以隐蔽性很强，比如，当名字为abschnittswininit.inidiefolgendeninhalte:NUL=C:windowspicture.exe，陈述C:windowspicture.exe发送至空，这意味着原始文件pictrue.exe已经被删除，所以运行它是特别微妙的。

2，在system.ini文件中，有一个&quotshell=文件名&quot在[靴]下。。正确的文件名应该是&quotexplorer.exe&#039s&quot。如果不是&quotexplorer.exe&#039s&quot但是&quotshell=explorer.exe&#039的程序名&quot，那么它后面的程序就是一个&quot特洛伊木马&quot程序。，你一定是在&quot特洛伊木马&quot。请参阅&quot中

的win.ini文件运行&quot，并通过&quot开始&quotsystem.ini文件中的。只需键入&quotmsconfig&quot然后单击&quot好的&quot在&quot运行&quot对话框。。这里应该注意的是，如果你不&#039；don’你对计算机了解不多。不要输入这个命令或删除里面的文件，否则你将承受一切后果并失去自我。画报，我不&#039；我不承担任何责任。)

3。以下文件一定要节制检查，木马可能隐藏

。

c:windowsinstart.bat和c:windowsinit.ini，自动执行。Bat

B，注册表(注册表就是注册表，懂电脑的人看一个)

1，从菜单加载。如果文件是自动加载的，直接在Windows菜单中添加。通常&quot开始程序开始&quot在主菜单上。Win98的资源管理器那里是位置&quotC:Windows开始菜单程序开始&quot位于。就这样，就这样当文件通常存储在注册表的以下四个位置时，会自动加载：

HKEY_Current_UserSoftwareMICROSOFTWINDOWSCurrentVersionBrowserShellFolder

BR/HKEYcurrentusersoftwareMICROSOFTWINDOWScurrentversionbrowseruser!hellFolders

HKEY_LOCAL_MACHINEsoftwareMICROSOFTWINDOWScurrentversionadventureusershellfolder

HKEY_LOCAL_MACHINEsoftwareMICROSOFTWINDOWScurrentversionadventureshellfolder

2，在最复杂的情况下，注册表，点击到：&quotHKEY-本地-机器软件微软视窗当前版本运行&quot目录。，检查键值中是否有不熟悉的EXE扩展名的自动启动文件。记住这里：有些文件类似于文件系统本身由&quot特洛伊木马&quot程序必须通过伪装来愚弄，例如&quotAcidBatteryv1.0特洛伊木马&quot。Itsregistry"ThecurrentversionofWindowsinHKEYlocalmachinesoftwareMicrosoftCruns"Changebrowserunder=browseritem"WINDOWSexpiorer.exe"木马只有I和L与真正的进程资源管理器的区别。当然，有很多地方&quot特洛伊&quot程序可以隐藏在注册表中。,suchas:"HKEY-ThecurrentversionofMICROSOFTWINDOWS,thecurrentusersoftware,runs","HKEY-user***softwareMicrosoft"directoryispossible.,thebestwayisin"ThecurrentversionofWINDOWSrunsTrojanhorse"ThefilenameoftheprogramHKEY-thecurrentversionoflocalmachinesoftwareMICROSOFTWINDOWSruns"Find"，然后搜索整个注册表。

3。同时，在HKEY_class_ROOTEXFILEshell打开的地方command=

&quot；1&quot和&quot*&quot在注册表中，如果&quot1&quot在它被拒绝，

特洛伊木马，所以每次启动木马，比如著名的Ice木马可执行文件，Notepad.exetxt文件都会被更改！它自己的启动文件，每次都会自动打开记事本启动ice木马的时候，已经很隐蔽了。

注册表在“运行”对话框中，选中并键入&quotREGEDIT&quot。需要指出的是，系统注册表的操作一定要删除注册表备份和注册表操作，因为有一定的风险，之前发现错误可能会有一些错误。您可以备份注册表文件，并将其导入系统进行恢复。子命令同样危险，比如计算机。请不要&#039；不要试图去理解他们。记住)

C，port(端口，实际上是网络数据通过操作系统输入电脑)

1，最后。特洛伊木马有启动方式，它只在特定情况下启动。所以平时多注意你的端口。一般木马默认端口有

BO31337、YAL1999、Deep2140、Throat3150和Glacier7636。，Sub71243

那么怎么打开机器看看有哪些端口呢？

在dos下输入命令：netstat-one，可以看到他们的嘴。常见的网络端口有：21、23、25、53、80、110、139。如果你有其他端口，就要注意了，因为有很多木马可以自己设置端口。(以上端口之前都是木马，由于时间原因。现在我不&#039；很多新的安全木马端口我都不知道，也不敢尝试，因为技术更新太快，我跟不上。55555555555555)

2、由于一个正常的木马通过网络连接的操作。所以如果你发现一个可疑的网络连接，可以推测最简单的检查木马存在的方法就是使用Windows内置的Netstat命令。一般来说，如果没有互联网运营，，使用netstat命令来查看MS-DOS窗口有什么信息，然后可以使用&quotnetstat-a将&quot和&quot-a&quot；显示当前计算机中所有端口的选项。如果未知端口正在侦听现在他们不&#039；不能对网络服务做任何事情，所以监听端口很可能是特洛伊木马。

3、对于系统进程：

XP/press&quot；CTLALTDEL&quot进入任务管理器。，可以看到所有正在运行的系统进程，11盘点活动，可以发现木马进程。

在Win98下，在搜索过程中不是那么容易访问，但是在发现过程中也有一些工具。。通过检查系统进程来检测木马是非常简单的，但是你必须熟悉系统，因为系统正在运行一个大家都不是很熟悉的运行进程，所以这个时候要小心，木马还是可以通

过这个方法检测出来的。

4。木马查杀软件介绍

上面说的木马程序会被手动检测或者删除，但是一般没那么容易发现木马，而且木马很隐蔽，哦。还好有很多反木马软件。下面是几个软件，

1。瑞星杀毒软件。

2、天网防火墙个人版。根据这个原则，即使你对别人&#039；的木马，木马客户端无法连接，因为防火墙将您的计算机与外界隔离。防火墙启动后一旦出现可疑的网络连接或特洛伊木马&#039；发现对方对电脑的控制，防火墙会报警，而对方显示的IP地址和接入端口可以手动设置，其他都不会被攻击。但是对于一些个别机器来说，天网会影响机器的运行速度。

3、木马克星。据我所知，只有查杀木马软件才能查杀一样多的木马软件。顾名思义，不是立法，尤其是针对各类木马。呵呵，不过这&#039；这不是绝对的。因为如果&quot灰鸽子&quot可以屏蔽木马克星。哦，我&#039；我听说过。它没有&#039；没试过。"灰鸽子&quot是一种特洛伊木马，类似冰川。)(木马克星现在大多都是未注册版本，可以去查查木马克星。如果发现木马，只有注册用户才能清除。这是一个小手段。其实他的意思是，如果我们发现一个木马，只有注册用户才能看懂。如果你真的发现了木马，木马软件会告诉你具体位置和名字是什么，我们不&#039；我不知道其他的软件和工具是什么第四章.绿鹰电脑万能精灵他会监控你的电脑，观看心理安慰&quot系统安全&quot实时地。

有了这些类似的防护软件，你的电脑基本上是安全的。但是请记住。最近在伪装的木马程序中有一个转折点(我不&#039；t不知道是哪个高手做的，很厉害)，这是基于生物产生多种排列组合，带杀毒软件的木马只能杀了它们的妈妈。那么，木马就不会被发现并生成。所以我们还是有一些办法可以通过人工来清除木马的。

其他的杀毒软件都是木马，也是相当成功有效的，但是也不完全清楚是不是理想的，因为按照木马的正常时间，电脑每次启动都会自动加载。杀毒软件无法完全清除木马文件。一般情况下，杀毒软件作为木马入侵防御更为有效。

五种木马防御

随着网络设备和可以兑换人民币的网络游戏的普及，木马的传播速度越来越快。而另一种新的变种，虽然我们检测到并去除了，但更应该注意采取措施预防。以下是木马的几种防范方法。(大家&#039；的意见，我借用一下)

1、不要下载、接收、执行来自未知的

许多木马通过其他软件或文件相互通信。软件或文件一旦运行，就会被感染绑定。所以在下载的时候要特别注意相对高的，信誉好的网站。安装软件前必须用杀毒软件检查。特别建议检查一下查杀木马的软件，确保无毒无马。

2。唐&#039；不要打开电子邮件附件，也不要&#039；不要点击可疑邮件的图片。(这里&#039；这是描述信息的另一个例子。请注意。)

3，资源管理器被配置为总是显示扩展名。Windows资源管理器配置为总是显示扩展名，一些带有文件扩展名的VBS、SHS、PIF文件多为木马病毒特征码文件，需要注意。如果你遇到这些可疑的文件扩展名。

4。尽可能少使用共享文件夹。如果因为工作或者其他原因不得不设置共享电脑，最好单独开一个共享文字！在文件夹中，所有需要的文件共享都放在共享文件夹中，而不管系统目录是否设置为共享。

5、反木马运行实时监控程序。木马卫士重要的一点是，上网时最好运行反木马程序实时监控，PC软件，如通用向导。，可以实时显示和详细描述当前所有程序的运行情况。另外，用一些专业的最新杀毒软件，个人防火墙等基本监控也可以放心。

6、定期升级系统。很多木马都是通过系统漏洞进行攻击的，而这些漏洞被发现后，微软会在第一时间发布补丁，有很多时候打补丁后系统本身就是防止木马的最好方法之一。

特洛伊木马传播的六个独立示例(介绍邮件类)

1从网络上越来越多的二手软件或操作系统平台的攻击来看，一些恶意木马页面通过小程序和javascript脚本语言程序的安全漏洞，嵌入到网页的HTMLHTMLJavaApplet等等。，ActiveX软件组件支持程序交互，自动执行代码，强制用户&#039；的操作系统&#039；的注册表和系统配置实用程序，并实现非法控制系统资源、数据破坏、硬盘格式化、木马感染等用途。

来自当前网页的攻击

分为两种：一种是编辑脚本到IE浏览器，一种是直接破坏Windows系统。前者通常是IE浏览器的标题栏、默认主页或者直接到木马&quot种植&quot在你的机器上。，以此类推；后者直接锁定你的键盘、鼠标等输入设备，然后破坏系统。

(作者插话):还好，盗取当前千年木马功能的用户名和密码只是盗窃，并没有发展成破坏行为。不，是偷来的，否则硬盘格式化的方式。我第一次觉得我再也拿不回我的密码了。我希望这不会发生。这些是问题，让我们&#039；让我们仔细阅读它们！如果您收到电子邮件附件，好像有这么一个文件(或者好像上面文章的内容是一个文件。简而言之，这是一个特别有吸引力的文件，但格式仍然是安全的。):QQ昵称跑路。Txt，你当然不会&#039；不认为这是一个纯文本文件？我想告诉你，不一定。！它的实际文件名可以运行QQ昵称。TXT.{3050f4d8-98b5-11CF-BB82-00aa00BDce0b}.注册表

中的

{3050f4fd8-98b5-11cf-bb82-00aa00bdce0b}表示HTML文件关联。但是，当您将其保存为文件名时，它将不会显示。你看到的是一个.Txt文件，这几乎是同一个QQ昵称运行。Txt.html.然后直接打开文件。为什么危险？如果你看这个文件的内容如下：

你可能会认为它会调用记事本运行，但是如果你双击它，结果在运行后台和自动启动页面中调用HTML加载木马文件。这个同步显示对话框&quot就是打开文件&quot想愚弄你。可以自由打开附件阅读txt。够危险吗？

欺骗原理：当你双击这个伪装成txt。，因为真正的文件扩展名是{3050f4FD8-98b5-11cf-bb82-00aa00bdce0b}，是html文件，所以。它将采用HTML文件的形式，这是它运行的先决条件。

在一些恶意木马中，&quotWScript&quot会被称为。

wscript的全称是WindowsScriptingHost。，是Win98下新增加的函数，是一个批处理语言/自动执行工具——其对应的程序&quotWScript.exe&#039s&quot是一个脚本语言解释器，位于C:Windows下，它使脚本能够被执行。，作为同一批次执行。在WindowsScriptingHost脚本环境中，预定义了一些对象，通过自己内置的对象，可以实现获取环境变量、创建快捷方式、加载程序、读写注册表等功能。

最近很多玩家反映很多新郎&quot确认你的密码一千年，&quot假装向玩家发送消息，如&quot你建议的千禧数据保护官方网站的名字&quot等等，为了欺骗玩家&#039；信任并运行木马来点击邮件。。希望广大玩家在点击新闻的时候一定要看到来自千年官网的新闻。如果是来自任何其他电子邮件网站或个人，应立即删除。记得删了往右走。唐&#039；不要冒险。

七。在&quot特洛伊木马&quot辩护(纯属个人观点

防止木马在网上到家是一件很简单的事情，但是很多杀毒软件都是及时安装升级的。(同样，新木马只要传播速度快，很快就会成为各种杀毒软件的战利品。除非这个人专门定制了个人木马，加个天网防火墙(很多黑客和安全漏洞都是用密码远程控制，可以防止密码和攻击)基本就能解决问题，除非你很好奇或者不小心打开了木马。这种情况我觉得是有一定比例的！

但是对于网吧来说，再好的防御疏散也是白来的。

据我所知，网上的安全系数差不多是10万美元，是目前最厉害的。我们还应该安装一个&quot它的原始精神&quot但是.我个人认为有用的东西不是很大，就是保护用户&#039；它是一个软件保护系统。现在的木马一般都是邮件发送密码，也就是只要你控制了木马。在输入框输入密码，必须拿到ID和密码(一般不超过三分钟)！对于网吧的朋友来说，通过复制访问被认为是最安全的。很多木马其实就是一个键盘记录工具。如果你不自觉地把自己所有的记录都输入到键盘里，那就把ID和密码通过网络发过来！(哈哈就是这么可怕，不过现在我知道公安部和文化部已经明令禁止网吧安装还原精灵了，谁说为了保存历史之类的。唉，防御意味着

总之，家庭上网者要记得更新自己的病毒库，经常检查电脑程序，查杀和立即发现的过程是未知的，不要浏览一些不知名的网站(我一般是靠域名来分析网站的可靠性。，一般级别的域名不会出现恶意代码和木马)，但是不会给人接收文件和发送邮件的自由！

互联网安全真的很难。每个人都有，而且很复杂。连老板都花钱注册了木马，呵呵。无效的不&#039；我不想做同样会杀了他的坏事。个人认为除了在输入框复制粘贴ID密码外，其他都辞职了

8。用1.1G对酒鬼的描述

用其他人&#039；的软件。。前段时间酒鬼1.1G软件运行后，有人说没有反应。这时关掉软件，一些防护软件注意：这个软件是监控本地键盘的！

其实我&#039；我在hook.dll纸醉金迷的巷子里玩耍。这里我们讨论了我的问题。

什么是钩子

在Windows系统中，钩子是一种特殊的消息处理机制。消息挂钩可以用在各种监视系统或进程中，这些系统或进程发送消息来拦截目标窗口和处理事件消息。。这样我们就可以在你的系统钩子自定义监控系统的特定事件发生时，完成特定功能的安装，比如拦截键盘、鼠标输入、抓图、日志监控等等。可以看出，使用钩子可以实

现许多特殊而有用的功能。因此对于高级程序员来说，主钩子编程方法是必须的。

钩子类型

主线程和系统钩子

(1)监视指定线程的钩子事件消息的线程。

(2)监视所有线程的系统挂钩的系统事件消息。因为系统会影响系统钩子的所有应用，钩子函数必须放在独立的动态链接库(DLL)中。这是系统钩子和线程钩子的一个很大的区别。

在hook.dll，程序

醉翁巷因为方案钩子的特殊性，已经完成了上述功能，所以会有一些软件报告他在记录击键，但是没有报告他是木马。哦，它&#039；这真的很可怕，但即使它记录了击键。它&#039；没有他们就不寄太危险了。

九、一个很大的数字(也就是顶着一大笔钱)

我们知道&quot特洛伊人&quot，杀死它们就变得容易了。如果你发现&quot特洛伊人&quot,最安全有效的方法就是立即断开与电脑的网络连接，通过网络，防止黑客攻击你。然后根据实际情况处理。

这里说的是我的机器防护装备：

。

XFILTER个人防火墙：这是一款没有杀毒功能的防火墙，不仅可以通过我的个人权限监控所有与网络的连接。它将连接到任何网络通知和要求。安装软件，如在&quot首先&quot操作在。，它将提示您连接到C:programfile1000Y的Client.exe网络，是否发布它。这是为了防止这种情况。

瑞星杀毒软件：查杀各类恶意病毒和木马2004版主要致力于游戏防护。

还原向导：记录当前硬盘和系统信息。硬盘和系统，无论什么样的动作，都可以恢复到原来的样子。比如2003年11月1日，我们目前的C硬盘和系统备份被保留，2003年12月1日，我们感染了一个木马程序。2003年11月1日以后一切都会恢复是备份的方式。无论你在c盘上做什么，都会被改回备份。这个软件有个缺点，会影响

机器的启动速度。但不影响机器的运行。最近游戏新版本有一些朋友。，有冲突。特洛伊木马克星：我可以&#039；不要再说了，这&#039；这是网络游戏玩家的必备。

十六进制编译器：我赢了&#039；具体名字就不说了，感兴趣的朋友很容易找到并使用。主要用于扫描和检测可疑程序的数量。。

以上软件在各大门户网站和各大下载专业网站都可以找到，其中一个小姑娘就可以&#039；不要提供网址，以免不必要的麻烦。

在公链中TRON被称为三大公链之一，新项目官网在非常大的程度上支持TRONDAPP。创&#039；s绿色生态发展趋势也很好，其DAPP活跃客户仅次于ETH。。数据钱包是公链绿色生态中基础设施建设的一大专用工具。它在客户和公链之间起着连接的作用，数据钱包的提升水平损害了公链客户的应用体验。创&#039；有很多钱包，波场钱包TokenPocket的应用体验非常流畅。让&#039；让我们来看看在wavefieldwalletTokenPocket中做了些什么。一、如何获得TRX如果你想买卖TRXToken，，可以按照TokenPocket中的货币交易进行交易。除了货币交易，根据TokenPocket的闪兑功能，还可以用其他代币兑换TRX，比如用USDT和BTC兑换必要的TRX代币。此外，还可以根据TokenPocket发布的TP交易中心(聚合交易中心)买卖TRX代币。二、TRON转账/支付TRON转账/支付是TRON公链客户使用较多的一个功能。，这也是每个TRON钱包必不可少的功能之一。TokenPocket有三种转账方式：即时转账、通讯录转账、扫描二维码转账。即时转账也是一种广泛使用的转账方式。，即输入收款人TRON账户和转账总额，然后按照提示进行实际操作。使用通讯录转账时，首先要建立一个通讯录，类似于手机上的手机通讯录，在通讯录中存储经常和自己有业务往来的TRON账户。那样的话，在转移TRON的时候，可以应用通讯录转移方式，可以在通讯录中选择要转移的TRON地址。扫描二维码转账类似于手机微信扫描二维码转账，扫描TokenPocket中对方TRON账户的二维码进行转账。。除了以上三种转账方式，如果账户之前有转账记录，还可以从最近的转账记录中选择要转账的TRON地址，这样可以防止输入错误。第三，TRON节点投票TRON公链采用DPoS共识机制。撕裂链中的交易由分布在世界各地的撕裂节点确认，TRON节点由TRON令牌持有者选举产生。票数越高，排名越高，节点收入越高。对于TRON令牌持有者，通过投票，可以为生态做贡献，同时可以获得一定的投票收入。在&quot更多工具-投票管理&quot在波场钱包的令牌袋中。在投票管理页面中，选择TRON投票节点和TRX投票数投票节点。类似EOS节点投票(EOS投票前需要抵押)，投TRON节点前TRX要被冻结。，可以冻结指定数量的TRX以获得TRONPower投票权，冻结的TRX不能流通或用于交易转移。第四，体验TRONDAPP。您可以通过wavewalletTokenPocket在TROND生态系统中体验DAPP。。首先，导入TRON帐户，然后单击&quot创&quot在&quot发现&quot来到TRON

DAPP应用区，点击相应的TRONDAPP进行体验。

波场DeFi项目BTRX(波场数字银行)在官网上线2小时完成代币兑换。并在社区宣布即将上线去中心化交易所JustSwap。BTRX是一个基于波场开发的DeFi项目。，致力于Apollo市场生态中代币存储、贷款、保险的应用场景。在BTRX在官网的第一轮交换中，BTRX使用了完全去中心化的交换系统。据官方透露，BTRX未来还将完成一个去中心化的集资平台，帮助优质项目满足其集资需求。

撕裂的数字货币不能交易。《撕裂货币》最新消息报道称，TornadoCash混合货币协议8日被美国财政部列入SDN制裁名单，禁止所有美国人和实体与该协议互动。

将下架。

国内大部分交易平台宣布撕令牌下架。

加密货币交易所，钱&#039；安在其官方推特账户上宣布，将暂停Tron网络上的存款和取款。根据公告，暂停将是暂时的。。TRON现在是分散金融(DeFi)协议的第三大区块链，仅次于以太坊和BSC。

第十三本6_13_幽灵船

厄尼惊呆了。因为他发现学校操场上跑着一艘鬼船，但班上只有他和杰德能看到。他们一起帮助佩格列格船长找到了他的宝藏，最后幽灵船开始渐渐远去，消失了。1艘幽灵船一天，厄尼上学迟到了。他跑上学校的小山，钻过篱笆上的洞。他希望校长没有&#039；我没见过他。

&quot；哇！"厄尼喘着气。

操场上漂浮着一艘幽灵船。它看起来像一艘普通的船，但它是白色透明的。他知道这不可能&#039；这不是真的。幽灵船被绑在一个网球柱上。一束奇怪的光从那里发出。它上下摇摆，仿佛在驾驭一片看不见的大海。一只幽灵海鸥绕着它飞。

&quot；嘿，幽灵船！"厄尼勇敢地喊道。

鬼&#039；她的头伸出窗外。。"谁说的？"鬼魂问。

&quot；我说了！"厄尼说。

&quot；但是你不应该&#039；别见我！"鬼魂喘息着。

然后鬼魂又想。

&quot；你确定你能看见我吗？"鬼魂问道。

&quot；我&#039；我确定。"厄尼说。窗户砰地关上了。

&quot；我&#039；我在和一个鬼魂说话！"厄尼喊道。看门人威金斯先生听到了厄尼&#039；哭吧。她跑向操场。

&quot；我和鬼魂说话。！"厄尼结结巴巴地说。

&quot；嘘！唐&#039；不要告诉任何人。"威尔金斯老师说。

&quot；为什么？"厄尼问道。

&quot；我不&#039；我不想让你让普通的孩子难过。！"威金斯老师说。

&quot；但是这艘幽灵船停在操场上，&quot厄尼说。但是他们休息的时候出来就会看到了。"

&quot；不是每个人都能看到的。"威尔金斯老师说。

&quot；嗯，我看得出来。"厄尼，告诉他。

&quot；然后那个&#039；是我们。"威尔金斯小姐叹了口气。威金斯先生大步走向幽灵船。

&quot；嘿！船！"威金斯小姐喊道。

窗户砰的一声开了，往外看的还是那个鬼。

&quot；啊！威金斯先生。鬼魂礼貌地说。

&quot；皮格莱格船长！"威金斯老师骂了一句&quot你保证除了我没人能看见你。但是一个四班的孩子看到了！不是&#039；对吧，厄尼？"

&quot；是的，&quot厄尼说。我看到了。"

&quot；嗯，这可能会发生，你知道&quot船长说，听起来有点不安。"不经常，

但有时会发生。"

&quot；如果有人能看到你，那你就不应该在这里航行。"威金斯老师坚定地说。

&quot；我可以&#039；Idon’我不能在这里航行。"船长告诉她。

&quot；为什么？"厄尼问道。

&quot；只有我在船上！"船长说，&quot我可以&#039；Idon’我不能独自驾船，所以我只能随波逐流。"。我只希望它能在这里飘得更远。然后我可以去寻找我的宝藏。船长接着说，“你知道吗？我注定要永远在海上航行，直到失去我的宝藏。我知道&#039；在这里，因为它&#039；它画在我的地图上。"

&quot；你&#039；这次最好找到它，否则！"威尔金斯老师警告说。窗户砰的一声关上了。

&quot；鬼宝！"厄尼说。等等，我&#039；我会把这件事告诉四班！""

2。"我们可以&#039；我没看见！

大家都要等到课间休息才能看到鬼船。他们冲出教室去操场。

&quot；那&#039；就是它！"厄尼指着幽灵船喊道。

大家仔细看了看。他们看到了垃圾箱和栅栏，但是他们看不到。我看不到任何船。

&quot；我们可以&#039；我没看见！"路易斯说

&quot；但是这里有幽灵船！"厄尼说，你看。同时穿过它。幽灵船是透明模糊的。

&quot；这里没有鬼船！"路易斯说。幽灵海鸥飞下来，落在路易斯身上&#039；的头。

&quot；一只幽灵海鸥刚刚落在你头上。"厄尼告诉路易斯。

&quot；哦不不！"路易斯说他不能&#039；我看不到也感觉不到。

&quot；哦，是的，它是！"厄尼喊道。

&quot；哦不不！"其他人都疯狂地喊着。他们嘲笑厄尼&#039；关于幽灵海鸥和船的故事。然后他们就跑去玩了。四班最年轻最聪明的杰德走了过来。。"什么&#039；那艘幽灵船在这里干什么？"她问厄尼。

&quot；你也能看出来！"厄尼喘着气。

&quot；我当然能看到。"杰德说。

&quot；除了我和威金斯先生。没有人能看到它&quot厄尼说。"我是皮格莱格船长。他注定要永远在海上航行，直到他找到他丢失的宝藏。他认为他把它落在这里了。"

&quot；我们可以帮他找到宝藏。"小玉说。

&quot；怎么找？"厄尼问道。

&quot；我的父亲&#039；上面的文章是一本关于寻宝的书。杰德说。"我们可以读读他的书，看看该怎么办。"

&quot；寻找幽灵宝藏现在开始！"厄尼喊道。

&quot；让&#039；让我们从阅读爸爸开始&#039；的书！"玉说

铃响了。

&quot；放学后！"杰德告诉他唐&#039；放学后不要到处闲逛！

3。放学后，他们去了杰德&#039；的房子，得到了她父亲&#039；这是一本关于寻宝的书。

&quot；我们就是这样做的！"杰德说给厄尼看一页书。

&quot；但是我们可以&#039；我从那得不到任何东西。"厄尼指着金属探测器说。

&quot；我父亲有，&quot杰德说。"当他在海滩上寻找硬币和东西时，他就利用他。。那&#039；这就是为什么他有所有以寻宝为内容的书。他们跑回校山，到达了学校。厄尼提着一把铲子，杰德提着一个装有金属探测器的大袋子。

&quot；皮格莱格上尉。！"厄尼喊道。船长在甲板上。"它&#039；又是你！"皮格莱格船长说。你还能看见我吗？"

&quot；是的。"厄尼说。

&quot；我们都知道你可以&#039；不找到你丢失的幽灵宝藏，就不要停止航行。"杰德告诉船长

，&quot我们想帮你找到它。"厄尼补充道。

&quot；但是我们想先看看你的地图。"杰德说。地图被撕成碎片，上面有许多洞。

&quot；幽灵海鸥这样啄它！"皮格莱格说。

&quot；上面写着：X标记了地图上的宝藏，&quot杰德说。"但是我可以&#039；我看不到任何x。

&quot；海鸥幽灵啄掉了我的x。我能&#039；Idon’我记不起它在哪里了。皮格莱格叹了口气说。"我可以&#039；甚至找不到金银岛.但是我&#039；我肯定它以前在这里。"

&quot；是的。！杰德咧着嘴笑着回答说。金银岛就在这里，我们站的地方！"

&quot；你怎么知道的？"厄尼问道。

&quot；看啊！"杰德说，她把它画在船长的背上&#039；的地图。

&quot；这个突然出现的地方就是校山！"她告诉厄尼&quot我们现在房子所在的地方在它下面，很多年前。我父亲告诉我的。"

&quot；我们还是不要&#039；我不知道去哪里找！"厄尼说"我们只能整天挖，找不到宝藏。"

&quot；我们将利用我的父亲&#039；金属探测器。杰德解释道。"当我们接近宝藏时，它会发出&quot砰&quot声音。"

&quot；如果金属探测器能在鬼宝里工作！"厄尼嘀咕道。

&quot；嗯，这可能行得通。杰德说。"至少我们可以试试。"他们寻找宝藏。但是他们没有&#039；我找不到它.他们找啊找啊找.

[XY001].他们看了又看.然后金属探测器发出砰，砰，砰的声音。

It&#039；这是一笔财富！他们挖出了皮格莱格船长。装满黄金的幽灵宝箱。里面有鬼金，所以没有真金重。他们开始把它搬回船上。至少

那&#039；这就是他们开始做的事情。但当他们走回学校时，幽灵宝盒开始褪色。皮格莱格船长也平息了。

&quot；再见，皮格莱格船长。"玉低声说。

&quot；因为我们找到了皮格莱格船长&#039；奇珍异宝，鬼船平息了。"第二天，厄尼告诉四班。

&quot；没有幽灵船。"路易斯说。

&quot；哦，是的，有。"厄尼喊道。

&quot；哦，不，我没有&#039；t.&quot其他人都喊道。在遥远的某个地方，一只幽灵海鸥穿过了小路。但是没有人听到，除了厄尼。杰德和威尔金斯先生。

那&#039；关于撕币的最新消息介绍就够了。感谢您花时间阅读本网站的内容。唐&#039；别忘了在这个网站上搜索更多关于残币的信息和残币的最新消息。