Damocles

illuvium Security Analysis

2024.07.30

Senna

DAMOCLES LABS

Contents

Summary

As a AAA MMORPG GameFi, the game typically consists of: a client for player interaction, a game server for storing game data, and a proxy server for interacting with on-chain data. However, after analyzing traffic and logic, it was found that Illuvium does not have a GS server to support the Overworld mode. Mining, gathering plants, and combat modules are all conducted through the HTTP protocol. Therefore, after in-depth analysis, it can be concluded that the current game server has very weak control over users. All user attributes on the client-side can be modified at will, such as teleportation and various data modifications. Data can be obtained by simulating packet transmission, and game logic is entirely separate from the client.

Based on the above analysis, Damocles rates Illuvium's security as 1 point.

Security Rating： ★☆☆☆☆

Game Background

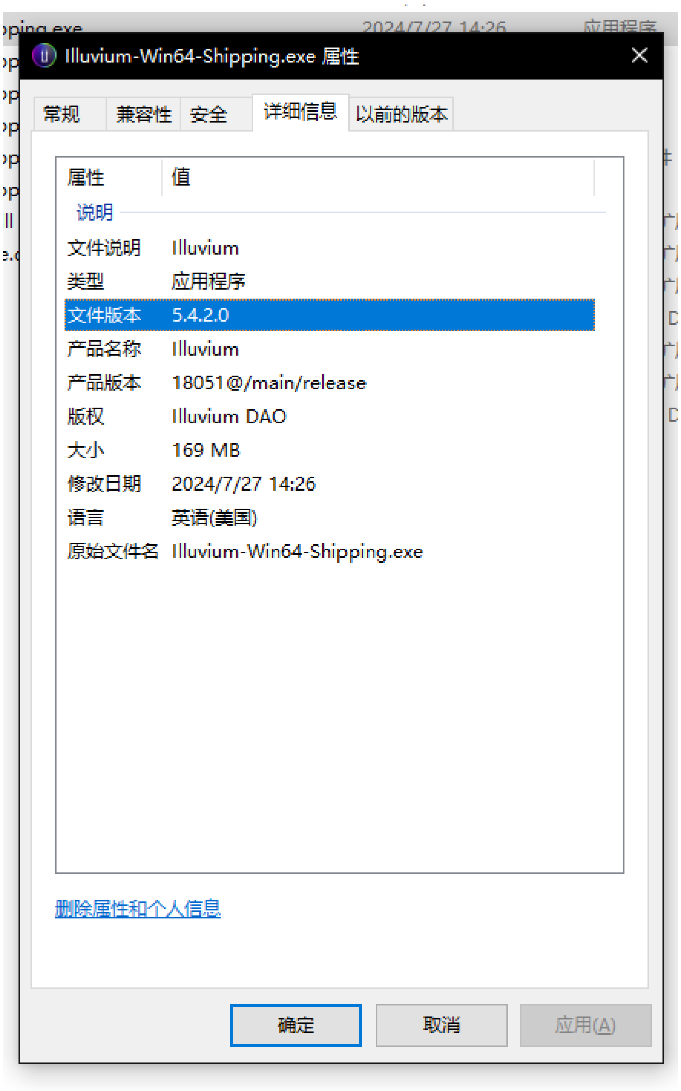
- Game Version Evaluated: illuvium-windows-RC-20958
- Game Type & Engine: MMORPG，UE5
- Potential Gameplay Issues:
    - Arbitrary modification of all local data
    - Automatic mining
    - Offline gameplay

Game Security Analysis

Game Code Protection：

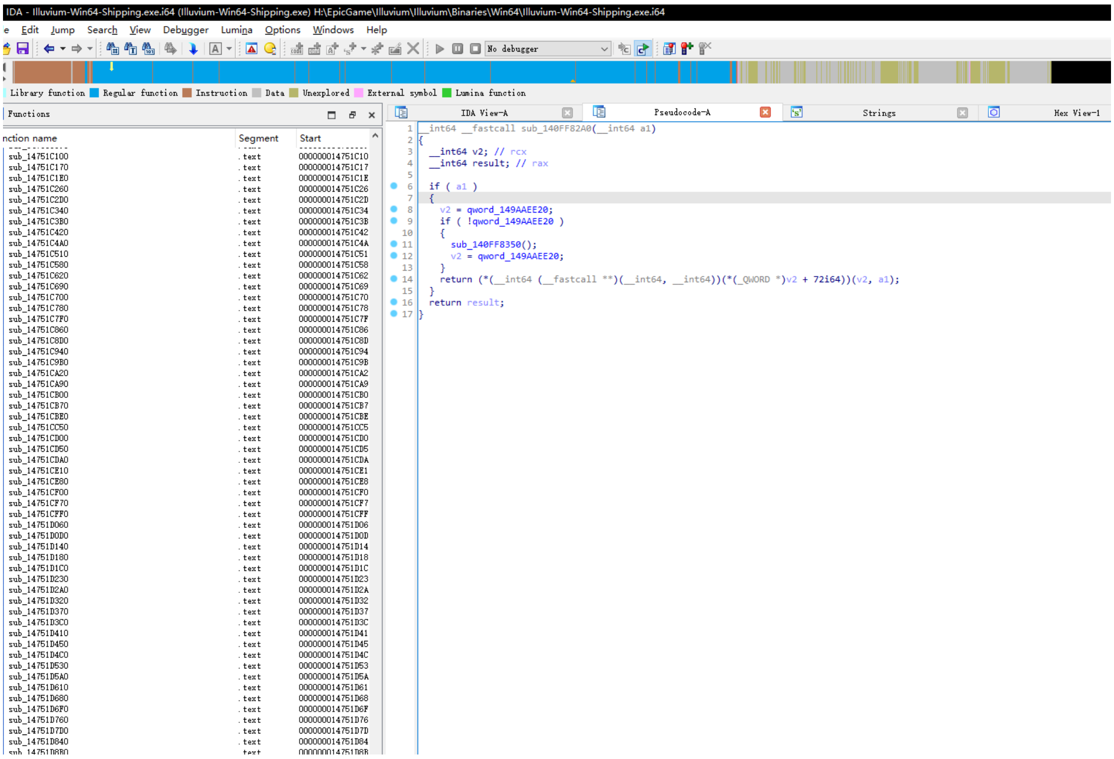
Analysis Process：

1. Determine the game engine by analyzing the game EXE since different engines have different analysis modes. Based on the identification of basic game information, we can confirm that Unity is used for game development.



属性	值
说明	
文件说明	Illuvium
类型	应用程序
文件版本	5.4.2.0
产品名称	Illuvium
产品版本	18051@/main/release
版权	Illuvium DAO
大小	169 MB
修改日期	2024/7/27 14:26
语言	英语(美国)
原始文件名	Illuvium-Win64-Shipping.exe

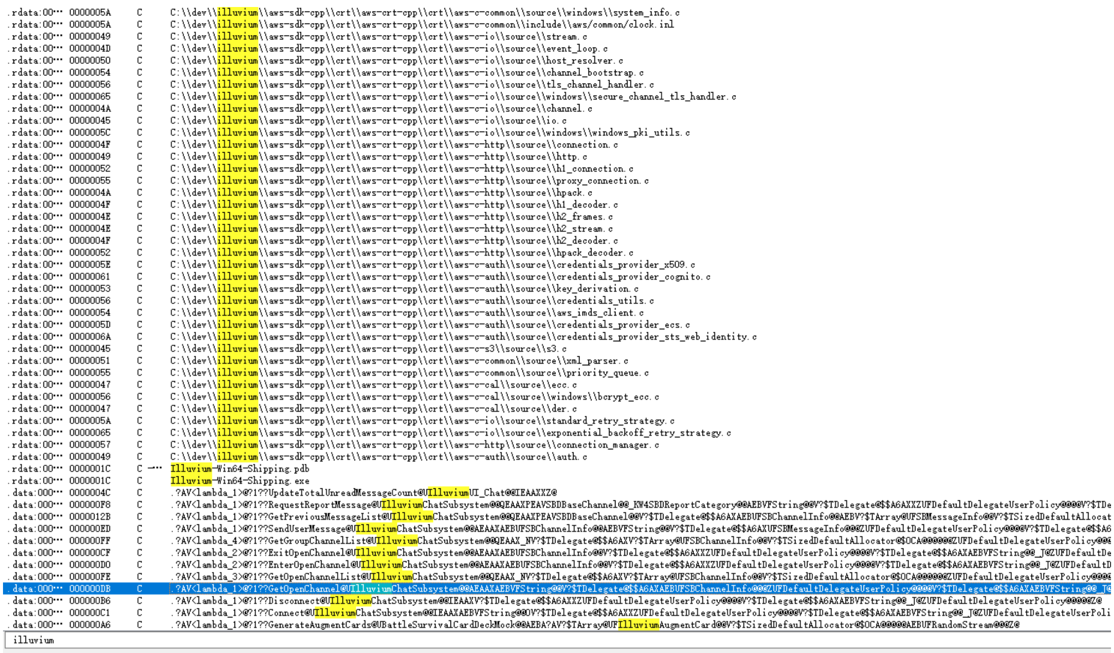
2. Using IDA for decompilation, we found that the code was not encrypted and the strings were not encrypted.


IDA - Illuvium-Win64-Shipping.exe.i64 (Illuvium-Win64-Shipping.exe) H:\EpicGame\Illuvium\Illuvium\Binaries\Win64\Illuvium-Win64-Shipping.exe.i64
e Edit Jump Search View Debugger Lumina Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
IDA View-A
Pseudocode-A
Strings
Hex View-1

```
nction name                         Segment   Start
sub_14751C100                       .text     000000014751C10
sub_14751C170                       .text     000000014751C17
sub_14751C1E0                       .text     000000014751C1E
sub_14751C260                       .text     000000014751C26
sub_14751C2D0                       .text     000000014751C2D
sub_14751C340                       .text     000000014751C34
sub_14751C3B0                       .text     000000014751C3B
sub_14751C420                       .text     000000014751C42
sub_14751C4A0                       .text     000000014751C4A
sub_14751C510                       .text     000000014751C51
sub_14751C580                       .text     000000014751C58
sub_14751C620                       .text     000000014751C62
sub_14751C690                       .text     000000014751C69
sub_14751C700                       .text     000000014751C70
sub_14751C780                       .text     000000014751C78
sub_14751C7F0                       .text     000000014751C7F
sub_14751C860                       .text     000000014751C86
sub_14751C8D0                       .text     000000014751C8D
sub_14751C940                       .text     000000014751C94
sub_14751C9B0                       .text     000000014751C9B
sub_14751CA20                       .text     000000014751CA2
sub_14751CA90                       .text     000000014751CA9
sub_14751CB00                       .text     000000014751CB0
sub_14751CB70                       .text     000000014751CB7
sub_14751CBE0                       .text     000000014751CBE
sub_14751CC50                       .text     000000014751CC5
sub_14751CD00                       .text     000000014751CD0
sub_14751CD50                       .text     000000014751CD5
sub_14751CDA0                       .text     000000014751CDA
sub_14751CE10                       .text     000000014751CE1
sub_14751CE80                       .text     000000014751CE8
sub_14751CF00                       .text     000000014751CF0
sub_14751CF70                       .text     000000014751CF7
sub_14751CFF0                       .text     000000014751CFF
sub_14751D060                       .text     000000014751D06
sub_14751D0D0                       .text     000000014751D0D
sub_14751D140                       .text     000000014751D14
sub_14751D180                       .text     000000014751D18
sub_14751D1C0                       .text     000000014751D1C
sub_14751D230                       .text     000000014751D23
sub_14751D2A0                       .text     000000014751D2A
sub_14751D320                       .text     000000014751D32
sub_14751D370                       .text     000000014751D37
sub_14751D3C0                       .text     000000014751D3C
sub_14751D410                       .text     000000014751D41
sub_14751D450                       .text     000000014751D45
sub_14751D4C0                       .text     000000014751D4C
sub_14751D530                       .text     000000014751D53
sub_14751D5A0                       .text     000000014751D5A
sub_14751D610                       .text     000000014751D61
sub_14751D680                       .text     000000014751D68
sub_14751D6F0                       .text     000000014751D6F
sub_14751D760                       .text     000000014751D76
sub_14751D7D0                       .text     000000014751D7D
sub_14751D840                       .text     000000014751D84
sub_14751D8B0                       .text     000000014751D8B
```

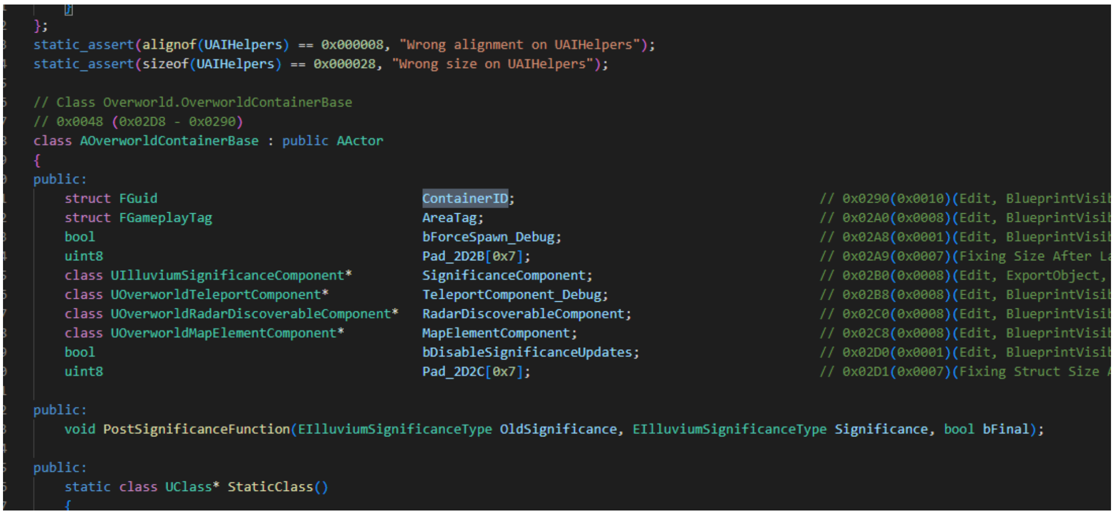
```
__int64 __fastcall sub_140FF82A0(__int64 a1)
{
  __int64 v2; // rcx
  __int64 result; // rax

  if ( a1 )
  {
    v2 = qword_149AAEE20;
    if ( !qword_149AAEE20 )
    {
      sub_140FF8350();
      v2 = qword_149AAEE20;
    }
    return (*(__int64 (__fastcall **)(__int64, __int64))(*(_QWORD *)v2 + 72i64))(v2, a1);
  }
  return result;
}
```



```
.rdata:00···  0000005A  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-common\\source\\windows\\system_info.c
.rdata:00···  0000005A  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-common\\include\\aws/common/clock.inl
.rdata:00···  00000049  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-io\\source\\stream.c
.rdata:00···  0000004D  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-io\\source\\event_loop.c
.rdata:00···  00000050  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-io\\source\\host_resolver.c
.rdata:00···  00000054  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-io\\source\\channel_bootstrap.c
.rdata:00···  00000056  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-io\\source\\tls_channel_handler.c
.rdata:00···  00000065  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-io\\source\\windows\\secure_channel_tls_handler.c
.rdata:00···  0000004A  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-io\\source\\channel.c
.rdata:00···  00000045  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-io\\source\\io.c
.rdata:00···  0000005C  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-io\\source\\windows\\windows_pki_utils.c
.rdata:00···  0000004F  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-http\\source\\connection.c
.rdata:00···  00000049  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-http\\source\\http.c
.rdata:00···  00000052  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-http\\source\\h1_connection.c
.rdata:00···  00000055  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-http\\source\\proxy_connection.c
.rdata:00···  0000004A  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-http\\source\\hpack.c
.rdata:00···  0000004F  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-http\\source\\h1_decoder.c
.rdata:00···  0000004E  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-http\\source\\h2_frames.c
.rdata:00···  0000004E  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-http\\source\\h2_stream.c
.rdata:00···  0000004F  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-http\\source\\h2_decoder.c
.rdata:00···  00000052  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-http\\source\\hpack_decoder.c
.rdata:00···  0000005E  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-auth\\source\\credentials_provider_x509.c
.rdata:00···  00000061  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-auth\\source\\credentials_provider_cognito.c
.rdata:00···  00000053  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-auth\\source\\key_derivation.c
.rdata:00···  00000056  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-auth\\source\\credentials_utils.c
.rdata:00···  00000054  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-auth\\source\\aws_imds_client.c
.rdata:00···  0000005D  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-auth\\source\\credentials_provider_ecs.c
.rdata:00···  0000006A  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-auth\\source\\credentials_provider_sts_web_identity.c
.rdata:00···  00000045  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-s3\\source\\s3.c
.rdata:00···  00000051  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-common\\source\\xml_parser.c
.rdata:00···  00000055  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-common\\source\\priority_queue.c
.rdata:00···  00000047  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-cal\\source\\ecc.c
.rdata:00···  00000056  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-cal\\source\\windows\\bcrypt_ecc.c
.rdata:00···  00000047  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-cal\\source\\der.c
.rdata:00···  0000005A  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-io\\source\\standard_retry_strategy.c
.rdata:00···  00000065  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-io\\source\\exponential_backoff_retry_strategy.c
.rdata:00···  00000057  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-http\\source\\connection_manager.c
.rdata:00···  00000049  C     C:\\dev\\illuvium\\aws-sdk-cpp\\crt\\aws-crt-cpp\\crt\\aws-c-auth\\source\\auth.c
.rdata:00···  0000001C  C ─··· Illuvium-Win64-Shipping.pdb
.rdata:00···  0000001C  C     Illuvium-Win64-Shipping.exe
.data:000···  0000004C  C     .?AV<lambda_1>@?1??UpdateTotalUnreadMessageCount@UIlluviumUI_Chat@@IEAAXXZ@
.data:000···  000000F8  C     .?AV<lambda_1>@?1??RequestReportMessage@UIlluviumChatSubsystem@@QEAAXPEAVSBDBaseChannel@@_KW4SBDReportCategory@@AEBVFString@@V?$TDelegate@$$A6AXXZUFDefaultDelegateUserPolicy@@@@V?$TDe
.data:000···  0000012B  C     .?AV<lambda_1>@?1??GetPreviousMessageList@UIlluviumChatSubsystem@@QEAAXPEAVSBDBaseChannel@@V?$TDelegate@$$A6AXAEBUFSBChannelInfo@@AEBV?$TArray@UFSBMessageInfo@@V?$TSizedDefaultAllocat
.data:000···  000000ED  C     .?AV<lambda_1>@?1??SendUserMessage@UIlluviumChatSubsystem@@AEAAXAEBUFSBChannelInfo@@AEBVFString@@V?$TDelegate@$$A6AXUFSBMessageInfo@@@ZUFDefaultDelegateUserPolicy@@@@V?$TDelegate@$$A6
.data:000···  000000FF  C     .?AV<lambda_4>@?1??GetGroupChannelList@UIlluviumChatSubsystem@@QEAAX_NV?$TDelegate@$$A6AXV?$TArray@UFSBChannelInfo@@V?$TSizedDefaultAllocator@$0CA@@@@@@ZUFDefaultDelegateUserPolicy@@@
.data:000···  000000CF  C     .?AV<lambda_2>@?1??ExitOpenChannel@UIlluviumChatSubsystem@@AEAAXAEBUFSBChannelInfo@@V?$TDelegate@$$A6AXXZUFDefaultDelegateUserPolicy@@@@V?$TDelegate@$$A6AXAEBVFString@@_J@ZUFDefaultDe
.data:000···  000000D0  C     .?AV<lambda_2>@?1??EnterOpenChannel@UIlluviumChatSubsystem@@AEAAXAEBUFSBChannelInfo@@V?$TDelegate@$$A6AXXZUFDefaultDelegateUserPolicy@@@@V?$TDelegate@$$A6AXAEBVFString@@_J@ZUFDefaultD
.data:000···  000000FE  C     .?AV<lambda_3>@?1??GetOpenChannelList@UIlluviumChatSubsystem@@QEAAX_NV?$TDelegate@$$A6AXV?$TArray@UFSBChannelInfo@@V?$TSizedDefaultAllocator@$0CA@@@@@@ZUFDefaultDelegateUserPolicy@@@@
.data:000···  000000DB  C     .?AV<lambda_1>@?1??GetOpenChannel@UIlluviumChatSubsystem@@AEAAXAEBVFString@@V?$TDelegate@$$A6AXAEBUFSBChannelInfo@@@ZUFDefaultDelegateUserPolicy@@@@V?$TDelegate@$$A6AXAEBVFString@@_J@
.data:000···  000000B6  C     .?AV<lambda_1>@?1??Disconnect@UIlluviumChatSubsystem@@IEAAXV?$TDelegate@$$A6AXXZUFDefaultDelegateUserPolicy@@@@V?$TDelegate@$$A6AXAEBVFString@@_J@ZUFDefaultDelegateUserPolicy@@@@@Z@
.data:000···  000000C1  C     .?AV<lambda_1>@?1??Connect@UIlluviumChatSubsystem@@IEAAXAEBVFString@@0V?$TDelegate@$$A6AXXZUFDefaultDelegateUserPolicy@@@@V?$TDelegate@$$A6AXAEBVFString@@_J@ZUFDefaultDelegateUserPoli
.data:000···  000000A6  C     .?AV<lambda_1>@?1??GenerateAugmentCards@UBattleSurvivalCardDeckMock@@AEBA?AV?$TArray@UFIlluviumAugmentCard@@V?$TSizedDefaultAllocator@$0CA@@@@@AEBUFRandomStream@@@Z@
illuvium
```

We can also use UE Dumper to dump data structures for quick analysis understanding of the game logic.



```
    }
};
static_assert(alignof(UAIHelpers) == 0x000008, "Wrong alignment on UAIHelpers");
static_assert(sizeof(UAIHelpers) == 0x000028, "Wrong size on UAIHelpers");

// Class Overworld.OverworldContainerBase
// 0x0048 (0x02D8 - 0x0290)
class AOverworldContainerBase : public AActor
{
public:
    struct FGuid                                  ContainerID;                                       // 0x0290(0x0010)(Edit, BlueprintVisib
    struct FGameplayTag                           AreaTag;                                           // 0x02A0(0x0008)(Edit, BlueprintVisib
    bool                                          bForceSpawn_Debug;                                 // 0x02A8(0x0001)(Edit, BlueprintVisib
    uint8                                         Pad_2D2B[0x7];                                     // 0x02A9(0x0007)(Fixing Size After La
    class UIlluviumSignificanceComponent*         SignificanceComponent;                             // 0x02B0(0x0008)(Edit, ExportObject,
    class UOverworldTeleportComponent*            TeleportComponent_Debug;                           // 0x02B8(0x0008)(Edit, BlueprintVisib
    class UOverworldRadarDiscoverableComponent*   RadarDiscoverableComponent;                        // 0x02C0(0x0008)(Edit, BlueprintVisib
    class UOverworldMapElementComponent*          MapElementComponent;                               // 0x02C8(0x0008)(Edit, BlueprintVisib
    bool                                          bDisableSignificanceUpdates;                       // 0x02D0(0x0001)(Edit, BlueprintVisib
    uint8                                         Pad_2D2C[0x7];                                     // 0x02D1(0x0007)(Fixing Struct Size A

public:
    void PostSignificanceFunction(EIlluviumSignificanceType OldSignificance, EIlluviumSignificanceType Significance, bool bFinal);

public:
    static class UClass* StaticClass()
    {
```

Therefore, the game's logic can be quickly understood through data structures and code

Analysis Conclusion：

Conclusion: Illuvium scores 0 in game code protection. Its client code is not encrypted, and strings are not encrypted, allowing users to easily dump the game's data structure for quick analysis.

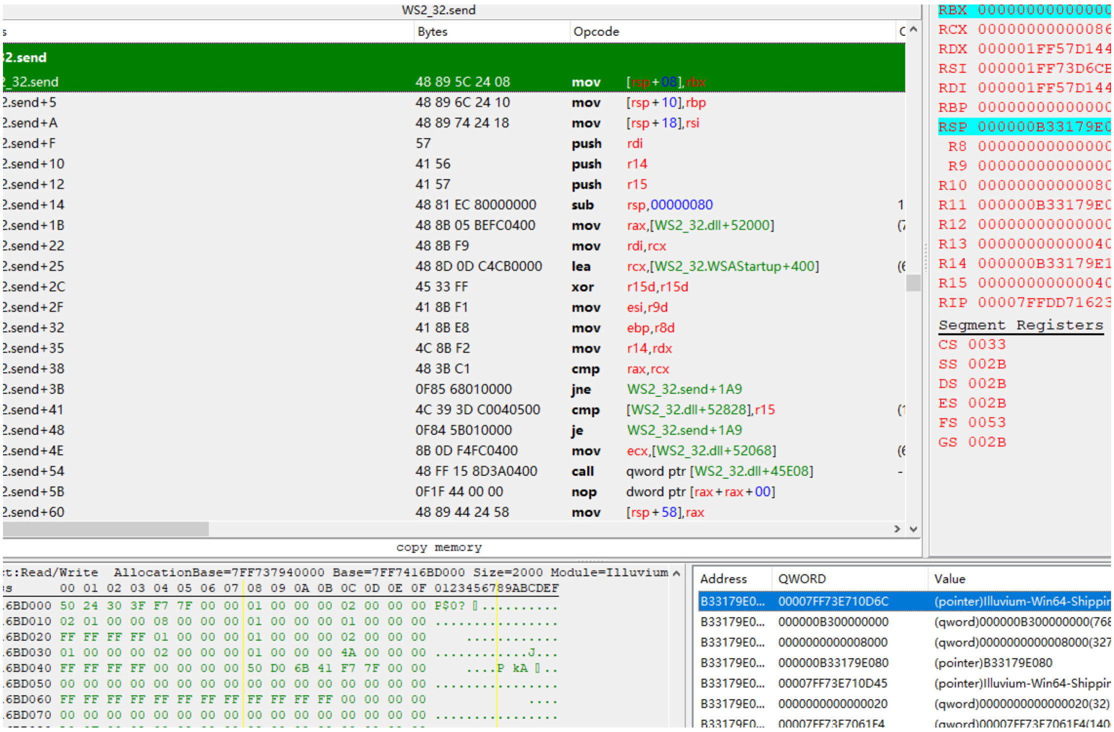
Fix Recommendations: Add local encryption for code and local protection for strings.

Game Basic Anti-Cheat：

Analysis Process：

1. In terms of basic anti-cheat detection, we primarily determine whether the game loads and executes external logic by replacing Lua files.

2. While attaching with Cheat Engine (CE) in the game's open state and setting breakpoints on common functions, it was observed that the game did not exit or provide any prompts.



```
WS2_32.send
s                         Bytes              Opcode
2.send
_32.send                  48 89 5C 24 08     mov    [rsp+08],rbx
2.send+5                  48 89 6C 24 10     mov    [rsp+10],rbp
2.send+A                  48 89 74 24 18     mov    [rsp+18],rsi
2.send+F                  57                 push   rdi
2.send+10                 41 56              push   r14
2.send+12                 41 57              push   r15
2.send+14                 48 81 EC 80000000  sub    rsp,00000080                 1
2.send+1B                 48 8B 05 BEFC0400  mov    rax,[WS2_32.dll+52000]       (7
2.send+22                 48 8B F9           mov    rdi,rcx
2.send+25                 48 8D 0D C4CB0000  lea    rcx,[WS2_32.WSAStartup+400]  (6
2.send+2C                 45 33 FF           xor    r15d,r15d
2.send+2F                 41 8B F1           mov    esi,r9d
2.send+32                 41 8B E8           mov    ebp,r8d
2.send+35                 4C 8B F2           mov    r14,rdx
2.send+38                 48 3B C1           cmp    rax,rcx
2.send+3B                 0F85 68010000      jne    WS2_32.send+1A9
2.send+41                 4C 39 3D C0040500  cmp    [WS2_32.dll+52828],r15       (1
2.send+48                 0F84 5B010000      je     WS2_32.send+1A9
2.send+4E                 8B 0D F4FC0400     mov    ecx,[WS2_32.dll+52068]       (6
2.send+54                 48 FF 15 8D3A0400  call   qword ptr [WS2_32.dll+45E08] -
2.send+5B                 0F1F 44 00 00      nop    dword ptr [rax+rax+00]
2.send+60                 48 89 44 24 58     mov    [rsp+58],rax
```

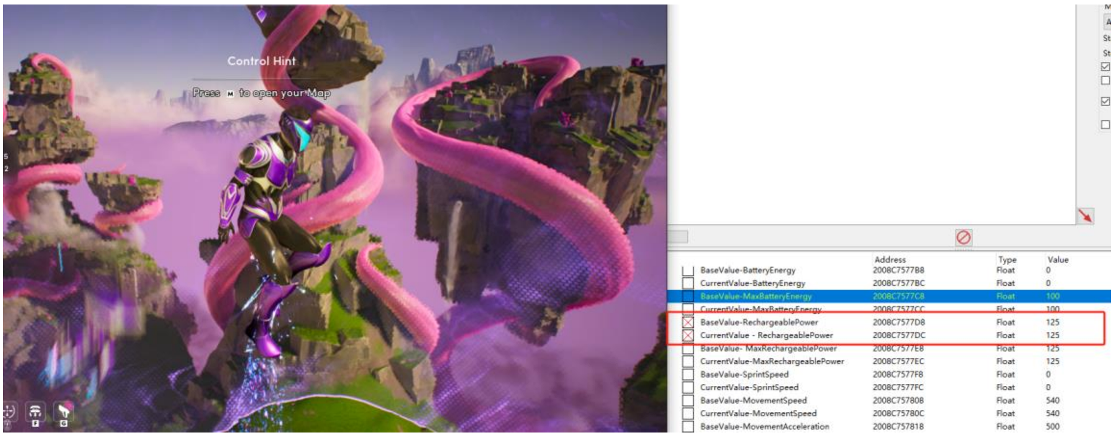
```
RBX 00000000000000
RCX 00000000000086
RDX 000001FF57D144
RSI 000001FF73D6CE
RDI 000001FF57D144
RBP 00000000000000
RSP 000000B33179E0
 R8 00000000000000
 R9 00000000000000
R10 00000000000080
R11 000000B33179E0
R12 00000000000000
R13 00000000000040
R14 000000B33179E1
R15 00000000000040
RIP 00007FFDD71623
Segment Registers
CS 0033
SS 002B
DS 002B
ES 002B
FS 0053
GS 002B
```

copy memory

```
t:Read/Write  AllocationBase=7FF737940000 Base=7FF7416BD000 Size=2000 Module=Illuvium
s        00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
.6BD000  50 24 30 3F F7 7F 00 00 01 00 00 00 02 00 00 00 P$0? ▯..........
.6BD010  02 01 00 00 08 00 00 00 01 00 00 00 01 00 00 00 ................
.6BD020  FF FF FF FF 01 00 00 00 01 00 00 00 02 00 00 00     ............
.6BD030  01 00 00 00 02 00 00 00 01 00 00 00 4A 00 00 00 ............J...
.6BD040  FF FF FF FF 00 00 00 00 50 D0 6B 41 F7 7F 00 00     ....P kA ▯..
.6BD050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
.6BD060  FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00 00             ....
.6BD070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

Address	QWORD	Value
B33179E0...	00007FF73E710D6C	(pointer)Illuvium-Win64-Shippir
B33179E0...	000000B300000000	(qword)000000B300000000(768
B33179E0...	0000000000008000	(qword)0000000000008000(327
B33179E0...	000000B33179E080	(pointer)B33179E080
B33179E0...	00007FF73E710D45	(pointer)Illuvium-Win64-Shippir
B33179E0...	0000000000000020	(qword)0000000000000020(32)
B33179E0...	00007FF73E7061F4	(qword)00007FF73E7061F4(140

3. Combined with the dumped data structure, data can be quickly located and modified. The figure shows unlimited energy.



		Address	Type	Value
□	BaseValue-BatteryEnergy	2008C7577B8	Float	0
□	CurrentValue-BatteryEnergy	2008C7577BC	Float	0
□	BaseValue-MaxBatteryEnergy	2008C7577C8	Float	100
□	CurrentValue-MaxBatteryEnergy	2008C7577CC	Float	100
☒	BaseValue-RechargeablePower	2008C7577D8	Float	125
☒	CurrentValue - RechargeablePower	2008C7577DC	Float	125
□	BaseValue- MaxRechargeablePower	2008C7577E8	Float	125
□	CurrentValue-MaxRechargeablePower	2008C7577EC	Float	125
□	BaseValue-SprintSpeed	2008C7577F8	Float	0
□	CurrentValue-SprintSpeed	2008C7577FC	Float	0
□	BaseValue-MovementSpeed	2008C757808	Float	540
□	CurrentValue-MovementSpeed	2008C75780C	Float	540
□	BaseValue-MovementAcceleration	2008C757818	Float	500

Analysis Conclusion：

1. 1. Illuvium offers virtually no basic protection against cheating, lacking countermeasures against dynamic debugging and analysis. This makes it very easy for malicious players to cheat, as there is no detection for already cheating players.
2. 2. The reason for only testing anti-debugging and read-write protection is that, for most cheats, finding data and implementing functionality can be achieved through debugging and read-write operations. If these basic protections are missing, more advanced injection and hook detection are meaningless.

Fix Recommendations: Increase data synchronization for player characters and add server-side validation of player character attributes.

Game Protocol & Logic Security Analysis

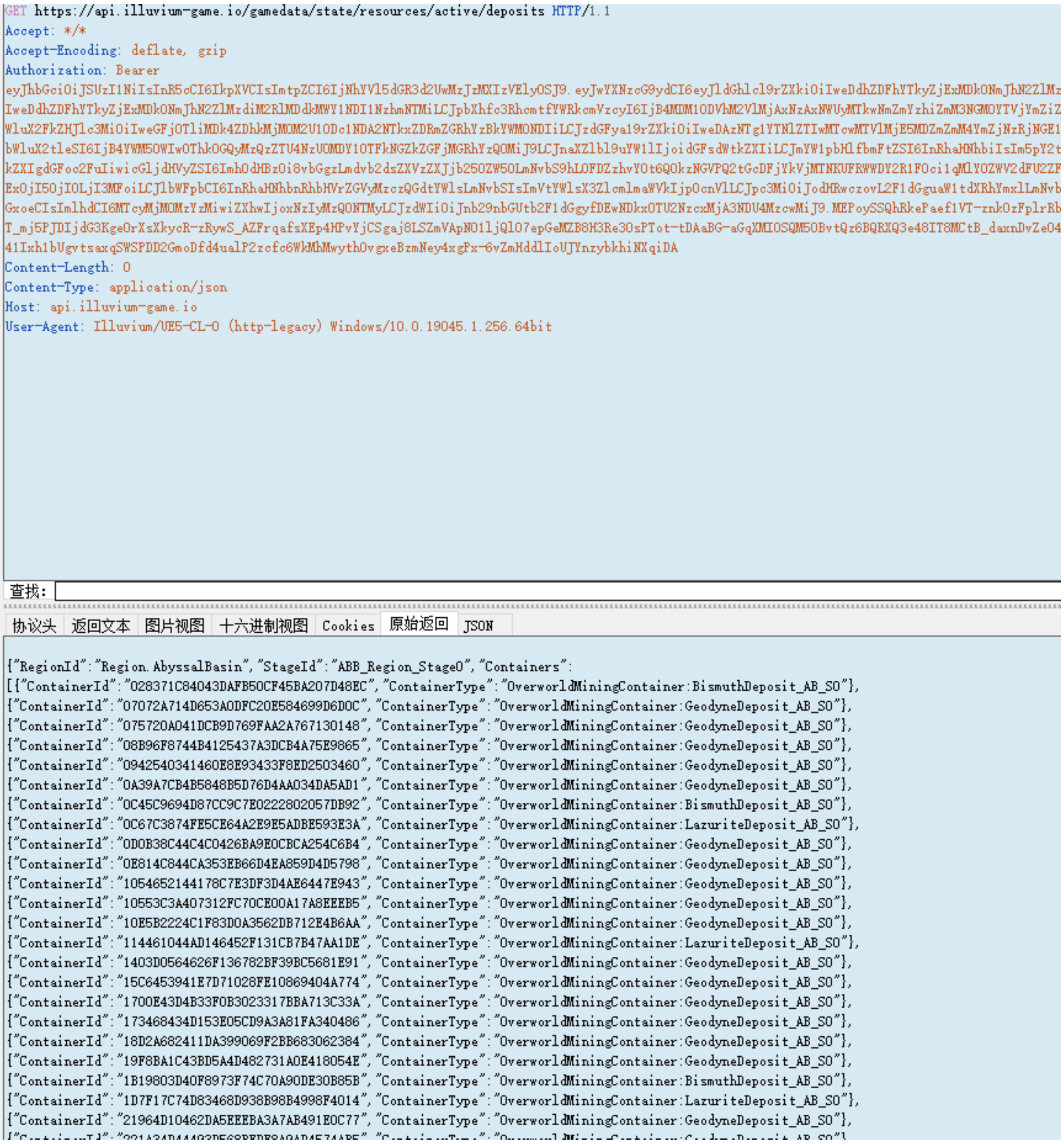
Analysis Process：

In the Overworld mode of Illuvium, the main interaction or earning logic involves mining and capturing Illuvials. Since most data changes are not tied to the local client, we combined protocol and logic security analysis.

1. Using packet capture tools on the game client, it was found that all client demonstrations, including mining and gathering plant resources, are reported to the server via HTTPS, where the server makes the final determination.

2. During map generation, the server communicates with the client to inform the

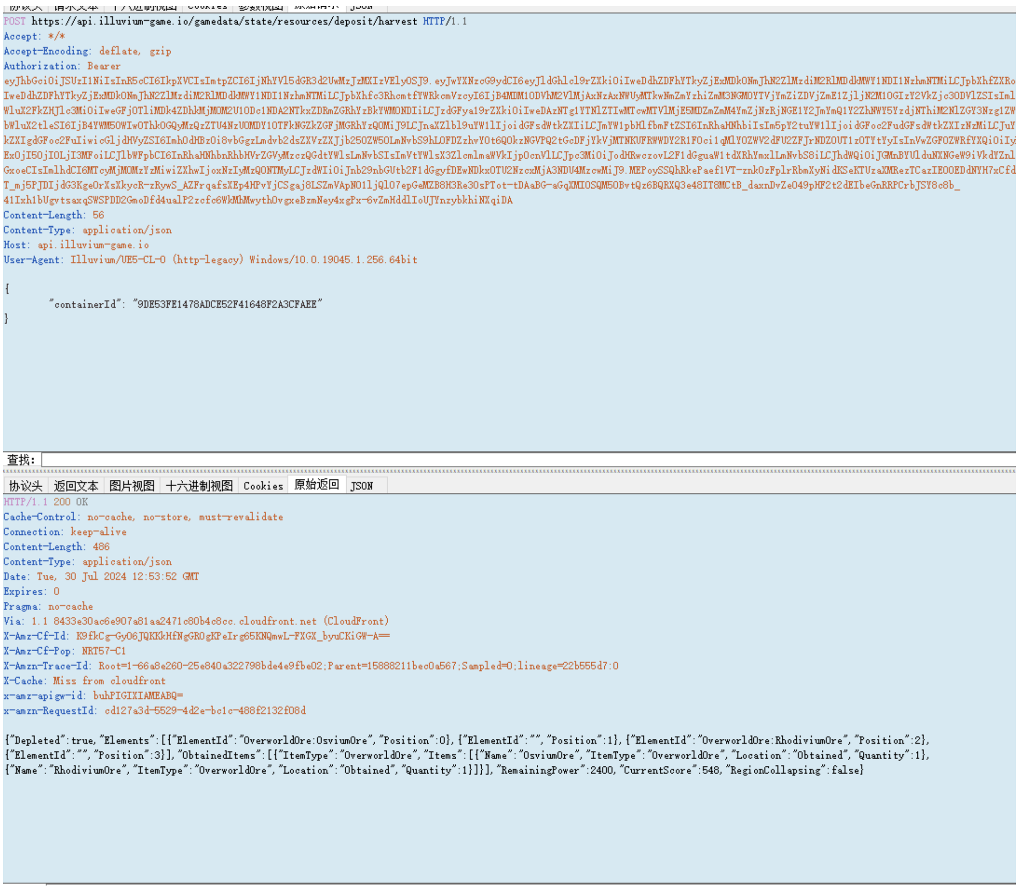
client of all resource container IDs on the current map.



```
GET https://api.illuvium-game.io/gamedata/state/resources/active/deposits HTTP/1.1
Accept: */*
Accept-Encoding: deflate, gzip
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjNhYVl5dGR3d2UwMzJzMXIzVElyOSJ9.eyJwYXNzcG9ydCI6eyJldGhlcl9rZXkiOiIweDdhZDFhYTkyZjExMDk0NmJhN2ZlMz
IweDdhZDFhYTkyZjExMDk0NmJhN2ZlMzdiM2RlMDdkMWY1NDI1NzhmNTMiLCJpbXhfc3RhcmtfYWRkcmVzcyI6IjB4MDM1ODVhM2VlMjAxNzAxNWUyMTkwNmZmYzhiZmM3NGM0YTVjYmZiZ
WluX2FkZHJlc3MiOiIweGFjOTliMDk4ZDhkMjM0M2U1ODc1NDA2NTkxZDRmZGRhYzBkYWM0NDIiLCJzdGFyal9rZXkiOiIweDAzNTg1YTNlZTIwMTcwMTVlMjE5MDZmZmM4YmZjNzRjNGE1
bWluX2tleSI6IjB4YWM5OWIwOThkOGQyMzQzZTU4NzU0MDY1OTFkNGZkZGFjMGRhYzQ0MiJ9LCJnaXZlbl9uYW1lIjoidGFsdWtkZXIiLCJmYW1pbHlfbmFtZSI6InRhaHNhbiIsIm5pY2t
kZXIgdGFoc2FuIiwicGljdHVyZSI6Imh0dHBzOi8vbGgzLmdvb2dsZXVzZXJjb250ZW50LmNvbS9hL0FDZzhvY0t6Q0kzNGVPQ2tGcDFjYkVjMTNKUFRWWDY2R1F0ci1qMlY0ZWV2dFU2ZF
Ex0jI50jI0LjI3MFoiLCJlbWFpbCI6InRhaHNhbnRhbHVrZGVyMzczQGdtYWlsLmNvbSIsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJpc3MiOiJodHRwczovL2F1dGguaW1tdXRhYmxlLmNvb
GxoeCIsImlhdCI6MTcyMjM0MzYzMiwiZXhwIjoxNzIyMzQ0NTMyLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwNDkxOTU2NzcxMjA3NDU4MzcwMiJ9.MEPoySSQhRkePaef1VT-znk0zFplrRb
T_mj5PJDIjdG3KgeOrXsXkycR-zRywS_AZFrqafsXEp4HPvYjCSgaj8LSZmVApN01ljQl07epGeMZB8H3Re30sPTot-tDAaBG-aGqXMIOSQM5OBvtQz6BQRXQ3e48IT8MCtB_daxnDvZe04
41Ixh1bUgvtsaxqSWSPDD2GmoDfd4ualP2zcfc6WkMhMwythOvgxeBzmNey4xgPx-6vZmHddlIoUJYnzybkhiNXqiDA
Content-Length: 0
Content-Type: application/json
Host: api.illuvium-game.io
User-Agent: Illuvium/UE5-CL-0 (http-legacy) Windows/10.0.19045.1.256.64bit
```

```
{"RegionId":"Region.AbyssalBasin","StageId":"ABB_Region_Stage0","Containers":
[{"ContainerId":"028371C84043DAFB50CF45BA207D48EC","ContainerType":"OverworldMiningContainer:BismuthDeposit_AB_S0"},
{"ContainerId":"07072A714D653A0DFC20E584699D6D0C","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"075720A041DCB9D769FAA2A767130148","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"08B96F8744B4125437A3DCB4A75E9865","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"0942540341460E8E93433F8ED2503460","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"0A39A7CB4B5848B5D76D4AA034DA5AD1","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"0C45C9694D87CC9C7E0222802057DB92","ContainerType":"OverworldMiningContainer:BismuthDeposit_AB_S0"},
{"ContainerId":"0C67C3874FE5CE64A2E9E5ADBE593E3A","ContainerType":"OverworldMiningContainer:LazuriteDeposit_AB_S0"},
{"ContainerId":"0D0B38C44C4C0426BA9E0CBCA254C6B4","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"0E814C844CA353EB66D4EA859D4D5798","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"1054652144178C7E3DF3D4AE6447E943","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"10553C3A407312FC70CE00A17A8EEEB5","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"10E5B2224C1F83D0A3562DB712E4B6AA","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"114461044AD146452F131CB7B47AA1DE","ContainerType":"OverworldMiningContainer:LazuriteDeposit_AB_S0"},
{"ContainerId":"1403D0564626F136782BF39BC5681E91","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"15C6453941E7D71028FE10869404A774","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"1700E43D4B33F0B3023317BBA713C33A","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"173468434D153E05CD9A3A81FA340486","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"18D2A682411DA399069F2BB683062384","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"19F8BA1C43BD5A4D482731A0E418054E","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
{"ContainerId":"1B19803D40F8973F74C70A90DE30B85B","ContainerType":"OverworldMiningContainer:BismuthDeposit_AB_S0"},
{"ContainerId":"1D7F17C74D83468D938B98B4998F4014","ContainerType":"OverworldMiningContainer:LazuriteDeposit_AB_S0"},
{"ContainerId":"21964D10462DA5EEEBA3A7AB491E0C77","ContainerType":"OverworldMiningContainer:GeodyneDeposit_AB_S0"},
```

3. Therefore, using Python code locally, resources, plants, and energy storage can be automatically acquired

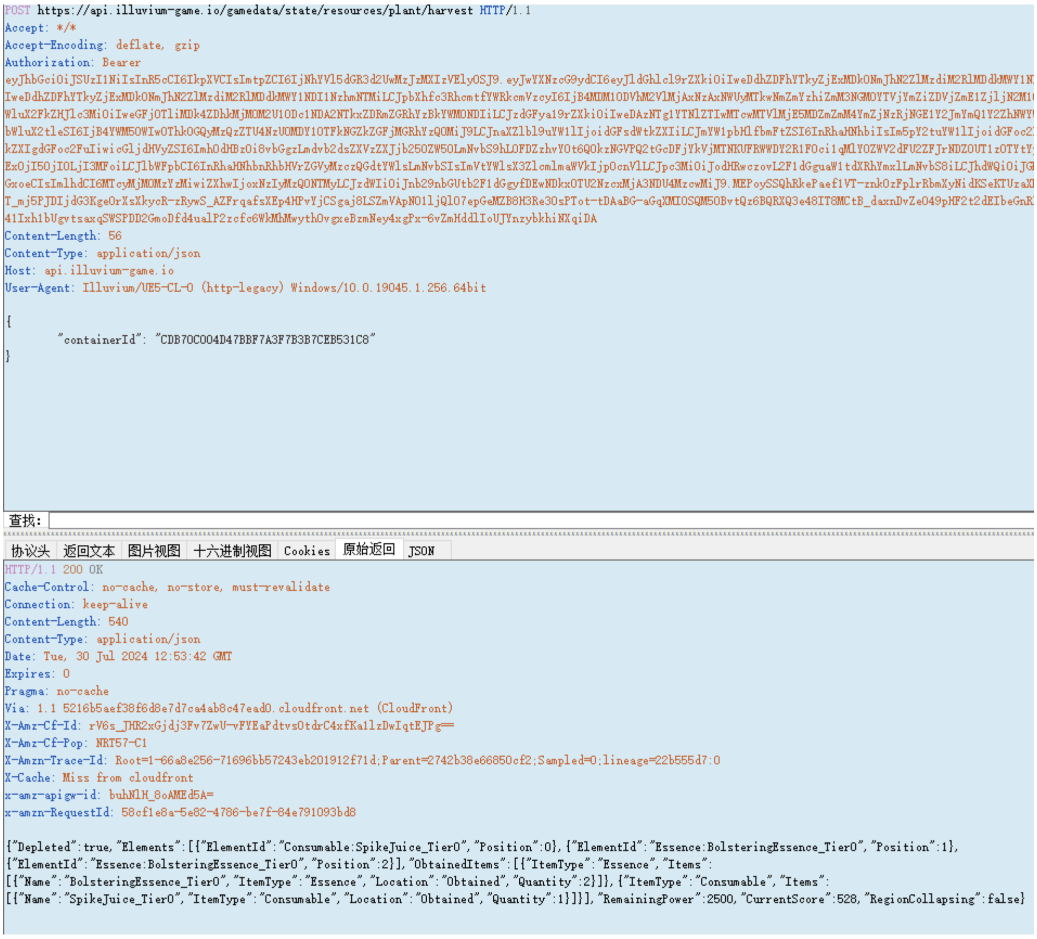


```
POST https://api.illuvium-game.io/gamedata/state/resources/deposit/harvest HTTP/1.1
Accept: */*
Accept-Encoding: deflate, gzip
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjNhYVl5dGR3d2UwMzJzMXIzVElyOSJ9.eyJwYXNzcG9ydCI6eyJldGhlcl9rZXkiOiIweDdhZDFhYTkyZjExMDk0NmJhN2ZlMzdiM2RlMDdkMWY1NDI1NzhmNTMiLCJpbXhfZXRo
IweDdhZDFhYTkyZjExMDk0NmJhN2ZlMzdiM2RlMDdkMWY1NDI1NzhmNTMiLCJpbXhfc3RhcmtfYWRkcmVzcyI6IjB4MDM1ODVhM2VlMjAxNzAxNWUyMTkwNmZmYzhiZmM3NGM0YTVjYmZiZDVjZmE1ZjljN2M1OGIzY2VkZjc3ODVlZSIsIml
WluX2FkZHJlc3MiOiIweGFjOTliMDk4ZDhkMjM0M2U1ODc1NDA2NTkxZDRmZGRhYzBkYWM0NDIiLCJzdGFya19rZXkiOiIweDAzNTg1YTNlZTIwMTcwMTVlMjE5MDZmZmM4YmZjNzRjNGE1Y2JmYmQ1Y2ZhNWY5YzdjNThiM2NlZGY3Nzg1ZW
bWluX2tleSI6IjB4YWM5OWIwOThkOGQyMzQzZTU4NzU0MDY1OTFkNGZkZGFjMGRhYzQ0MiJ9LCJnaXZlbl9uYW1lIjoidGFsdWtkZXIiLCJmYW1pbHlfbmFtZSI6InRhaHNhbiIsIm5pY2tuYW1lIjoidGFoc2FudGFsdWtkZXIzNzMiLCJuY
kZXIgdGFoc2FuIiwicGljdHVyZSI6Imh0dHBzOi8vbGgzLmdvb2dsZXVzZXJjb250ZW50LmNvbS9hL0FDZzhvY0t6Q0kzNGVPQ2tGcDFjYkVjMTNKUFRWWDY2R1F0ci1qMlY0ZWV2dFU2ZFJrNDZ0UT1zOTYtYyIsInVwZGF0ZWRfYXQiOiIy
Ex0jI50jI0LjI3MFoiLCJlbWFpbCI6InRhaHNhbnRhbHVrZGVyMzczQGdtYWlsLmNvbSIsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJpc3MiOiJodHRwczovL2F1dGguaW1tdXRhYmxlLmNvbS8iLCJhdWQiOiJGMnBYUlduNXNGeW9iVkdYZnl
GxoeCIsImlhdCI6MTcyMjM0MzYzMiwiZXhwIjoxNzIyMzQ0NTMyLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwNDkxOTU2NzcxMjA3NDU4MzcwMiJ9.MEPoySSQhRkePaef1VT-znk0zFplrRbmXyNidKSeKTUzaXMRezTCazIEOOEDdNYH7xCfd
T_mj5PJDIjdG3KgeOrXsXkycR-zRywS_AZFrqafsXEp4HPvYjCSgaj8LSZmVApNO1ljQl07epGeMZB8H3Re3OsPTot-tDAaBG-aGqXMIOSQM5OBvtQz6BQRXQ3e48IT8MCtB_daxnDvZe049pHF2t2dEIbeGnRRPCrbJSY8c8b_
41Ixh1bUgvtsaxqSWSPDD2GmoDfd4ualP2zcfc6WkMhMwyth0vgxeBzmNey4xgPx-6vZmHddlIoUJYnzybkhiNXqiDA
Content-Length: 56
Content-Type: application/json
Host: api.illuvium-game.io
User-Agent: Illuvium/UE5-CL-0 (http-legacy) Windows/10.0.19045.1.256.64bit

{
        "containerId": "9DE53FE1478ADCE52F41648F2A3CFAEE"
}
```

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Connection: keep-alive
Content-Length: 486
Content-Type: application/json
Date: Tue, 30 Jul 2024 12:53:52 GMT
Expires: 0
Pragma: no-cache
Via: 1.1 8433e30ac6e907a81aa2471c80b4c8cc.cloudfront.net (CloudFront)
X-Amz-Cf-Id: K9fkCg-Gy06JQKKkHfNgGR0gKPeIrg65KNQmwL-FXGX_byuCKiGW-A==
X-Amz-Cf-Pop: NRT57-C1
X-Amzn-Trace-Id: Root=1-66a8e260-25e840a322798bde4e9fbe02;Parent=15888211bec0a567;Sampled=0;lineage=22b555d7:0
X-Cache: Miss from cloudfront
x-amz-apigw-id: buhPIGIXIAMEABQ=
x-amzn-RequestId: cd127a3d-5529-4d2e-bc1c-488f2132f08d

{"Depleted":true,"Elements":[{"ElementId":"OverworldOre:OsviumOre","Position":0},{"ElementId":"","Position":1},{"ElementId":"OverworldOre:RhodiviumOre","Position":2},
{"ElementId":"","Position":3}],"ObtainedItems":[{"ItemType":"OverworldOre","Items":[{"Name":"OsviumOre","ItemType":"OverworldOre","Location":"Obtained","Quantity":1},
{"Name":"RhodiviumOre","ItemType":"OverworldOre","Location":"Obtained","Quantity":1}]}],"RemainingPower":2400,"CurrentScore":548,"RegionCollapsing":false}
```

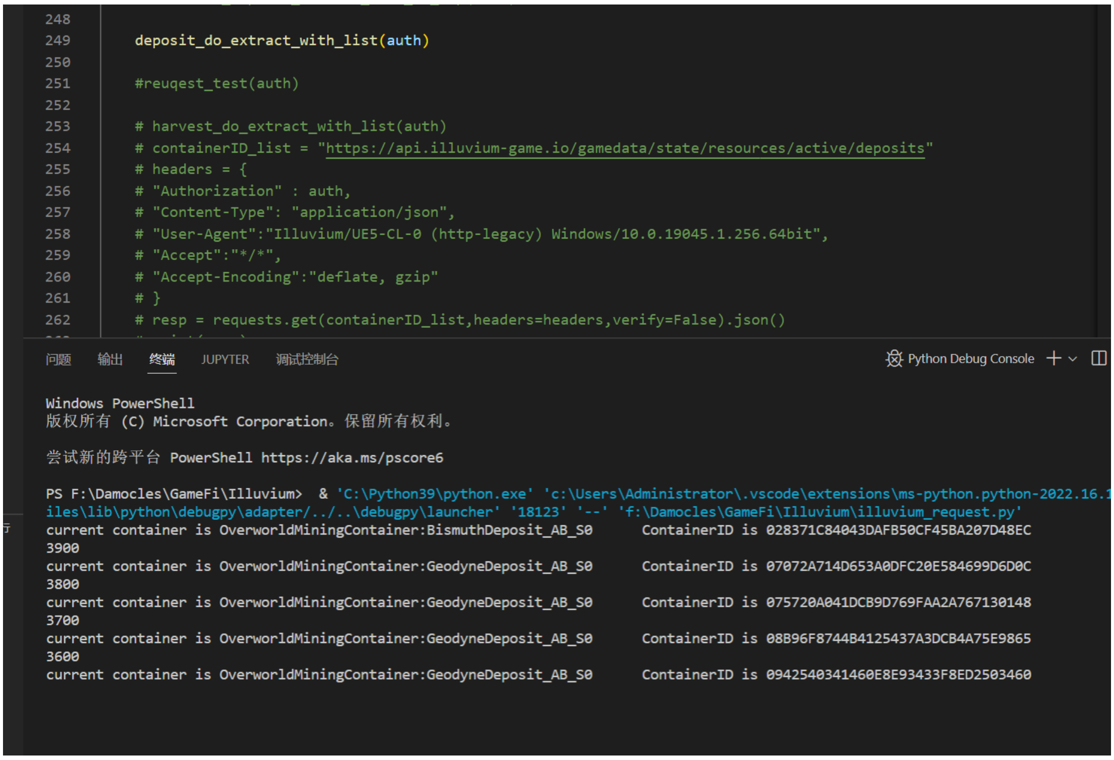


```
POST https://api.illuvium-game.io/gamedata/state/resources/plant/harvest HTTP/1.1
Accept: */*
Accept-Encoding: deflate, gzip
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjNhYVl5dGR3d2UwMzJzMXIzVElyOSJ9.eyJwYXNzcG9ydCI6eyJldGhlcl9rZXkiOiIweDdhZDFhYTkyZjExMDk0NmJhN2ZlMzdiM2RlMDdkMWY1N
IweDdhZDFhYTkyZjExMDk0NmJhN2ZlMzdiM2RlMDdkMWY1NDI1NzhmNTMiLCJpbXhfc3RhcmtfYWRkcmVzcyI6IjB4MDM1ODVhM2VlMjAxNzAxNWUyMTkwNmZmYzhiZmM3NGM0YTVjYmZiZDVjZmE1ZjljN2M1
WluX2FkZHJlc3MiOiIweGFjOTliMDk4ZDhkMjM0M2U1ODc1NDA2NTkxZDRmZGRhYzBkYWM0NDIiLCJzdGFya19rZXkiOiIweDAzNTg1YTNlZTIwMTcwMTVlMjE5MDZmZmM4YmZjNzRjNGE1Y2JmYmQ1Y2ZhNWY
bWluX2tleSI6IjB4YWM5OWIwOThkOGQyMzQzZTU4NzU0MDY1OTFkNGZkZGFjMGRhYzQ0MiJ9LCJnaXZlbl9uYW1lIjoidGFsdWtkZXIiLCJmYW1pbHlfbmFtZSI6InRhaHNhbiIsIm5pY2tuYW1lIjoidGFoc2
kZXIgdGFoc2FuIiwicGljdHVyZSI6Imh0dHBzOi8vbGgzLmdvb2dsZXVzZXJjb250ZW50LmNvbS9hL0FDZzhvY0t6Q0kzNGVPQ2tGcDFjYkVjMTNKUFRWWDY2R1F0ci1qMlY0ZWV2dFU2ZFJrNDZ0UT1zOTYtY
Ex0jI50jI0LjI3MFoiLCJlbWFpbCI6InRhaHNhbnRhbHVrZGVyMzczQGdtYWlsLmNvbSIsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJpc3MiOiJodHRwczovL2F1dGguaW1tdXRhYmxlLmNvbS8iLCJhdWQiOiJG
GxoeCIsImlhdCI6MTcyMjM0MzYzMiwiZXhwIjoxNzIyMzQ0NTMyLCJzdWIiOiJnb29nbGUtb2F1dGgyfDEwNDkxOTU2NzcxMjA3NDU4MzcwMiJ9.MEPoySSQhRkePaef1VT-znk0zFplrRbmXyNidKSeKTUzaX
T_mj5PJDIjdG3KgeOrXsXkycR-zRywS_AZFrqafsXEp4HPvYjCSgaj8LSZmVApNO1ljQl07epGeMZB8H3Re3OsPTot-tDAaBG-aGqXMIOSQM5OBvtQz6BQRXQ3e48IT8MCtB_daxnDvZe049pHF2t2dEIbeGnR
41Ixh1bUgvtsaxqSWSPDD2GmoDfd4ualP2zcfc6WkMhMwyth0vgxeBzmNey4xgPx-6vZmHddlIoUJYnzybkhiNXqiDA
Content-Length: 56
Content-Type: application/json
Host: api.illuvium-game.io
User-Agent: Illuvium/UE5-CL-0 (http-legacy) Windows/10.0.19045.1.256.64bit

{
        "containerId": "CDB70C004D47BBF7A3F7B3B7CEB531C8"
}
```

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Connection: keep-alive
Content-Length: 540
Content-Type: application/json
Date: Tue, 30 Jul 2024 12:53:42 GMT
Expires: 0
Pragma: no-cache
Via: 1.1 5216b5aef38f6d8e7d7ca4ab8c47ead0.cloudfront.net (CloudFront)
X-Amz-Cf-Id: rV6s_JHR2xGjdj3Fv7ZwU-vFYEaPdtvs0tdrC4xfKa1lzDwIqtEJPg==
X-Amz-Cf-Pop: NRT57-C1
X-Amzn-Trace-Id: Root=1-66a8e256-71696bb57243eb201912f71d;Parent=2742b38e66850cf2;Sampled=0;lineage=22b555d7:0
X-Cache: Miss from cloudfront
x-amz-apigw-id: buhNlH_8oAMEd5A=
x-amzn-RequestId: 58cf1e8a-5e82-4786-be7f-84e791093bd8

{"Depleted":true,"Elements":[{"ElementId":"Consumable:SpikeJuice_Tier0","Position":0},{"ElementId":"Essence:BolsteringEssence_Tier0","Position":1},
{"ElementId":"Essence:BolsteringEssence_Tier0","Position":2}],"ObtainedItems":[{"ItemType":"Essence","Items":
[{"Name":"BolsteringEssence_Tier0","ItemType":"Essence","Location":"Obtained","Quantity":2}]},{"ItemType":"Consumable","Items":
[{"Name":"SpikeJuice_Tier0","ItemType":"Consumable","Location":"Obtained","Quantity":1}]}],"RemainingPower":2500,"CurrentScore":528,"RegionCollapsing":false}
```



```
    deposit_do_extract_with_list(auth)

    #reuqest_test(auth)

    # harvest_do_extract_with_list(auth)
    # containerID_list = "https://api.illuvium-game.io/gamedata/state/resources/active/deposits"
    # headers = {
    # "Authorization" : auth,
    # "Content-Type": "application/json",
    # "User-Agent":"Illuvium/UE5-CL-0 (http-legacy) Windows/10.0.19045.1.256.64bit",
    # "Accept":"*/*",
    # "Accept-Encoding":"deflate, gzip"
    # }
    # resp = requests.get(containerID_list,headers=headers,verify=False).json()
```

```
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。

尝试新的跨平台 PowerShell https://aka.ms/pscore6

PS F:\Damocles\GameFi\Illuvium>  & 'C:\Python39\python.exe' 'c:\Users\Administrator\.vscode\extensions\ms-python.python-2022.16.1
iles\lib\python\debugpy\adapter/../..\debugpy\launcher' '18123' '--' 'f:\Damocles\GameFi\Illuvium\illuvium_request.py'
current container is OverworldMiningContainer:BismuthDeposit_AB_S0      ContainerID is 028371C84043DAFB50CF45BA207D48EC
3900
current container is OverworldMiningContainer:GeodyneDeposit_AB_S0      ContainerID is 07072A714D653A0DFC20E584699D6D0C
3800
current container is OverworldMiningContainer:GeodyneDeposit_AB_S0      ContainerID is 075720A041DCB9D769FAA2A767130148
3700
current container is OverworldMiningContainer:GeodyneDeposit_AB_S0      ContainerID is 08B96F8744B4125437A3DCB4A75E9865
3600
current container is OverworldMiningContainer:GeodyneDeposit_AB_S0      ContainerID is 0942540341460E8E93433F8ED2503460
```

4. This allows for malicious resource acquisition through automated resource gathering, enabling rapid scanning and completing levels quickly.

Analysis Conclusion：

1. The current protocol and logic have certain risks. However, it was found that the client reports the current location information during reporting. Thus, collection requests can be partially validated based on location information, although the range is difficult to grasp. The security rating for game protocol and logic is 1 point.

   Fix Recommendations: Increase detection of user behavior and encrypt requests. Add encryption at the blueprint script layer.

WEB3 Security Analysis：

Currently, Illuvium assets are issued on IMX. Given the stateless nature of assets on this chain, the current security of Web3 assets is relatively high.

About Damocles

Damocles Labs is a security team established in 2023, specializing in security for the Web3 industry. Their services include contract code auditing, business code auditing, penetration testing, GameFi code auditing, GameFi vulnerability discovery, GameFi cheat analysis, and GameFi anti-cheat measures. They are committed to making continuous efforts in the Web3 security industry, producing as many analysis reports as possible, raising awareness among project owners and users about GameFi security, and promoting the overall security development of the industry.。

Twitter: https://twitter.com/DamoclesLabs

WebSite：http://damocleslabs.com/

Analysis Report repo：https://github.com/DamoclesLabs/GameFi-Analysis-Report/