Control Flow Analysis

R5AC is planting control flow enumeration helpers into important game mode.

Just because a module is signed, doesn't mean that R5AC will give it a pass.

It follows a strict whitelist which at the time of this writing, consisted of the following ranges.

r5apex_dx12.exe	(+1000 → +13d2000) ; '.text'
KERNEL32.DLL	(+1000 → +7f4bb) ; '.text'
ntdll.dll	(+1000 → +119f1e) ; '.text'
ntdll.dll	+11a000 → +11a592) ; 'PAGE'
ntdll.dll	(+11b000 → +11b1f9) ; 'RT'
steamnetworkingsockets.dll	(+1000 → +2f63a8) ; '.text
steam_api64.dll	(+1000 → +243de) ; '.text'
EOSSDK-Win64-Shipping.dll	(+1000 → +d8117c) ; '.text

Their whitelist is using a relatively primitive structure for describing what they deem a whitelisted memory range:

> struct WHITELISTED_REGION
>
> {
>
> u64 Begin;
>
> u64 End;
>
> };

> In more recent builds of**Apex Legends**, this list is now more complex to interpret ~~and seems to have switched to using the LDR directly, with some middle steps that i haven't figured out yet..~~ **EDIT**: actually, they still build a list of whitelisted regions. I was just too focused on other things and the hash calculation memes had initially confused me. Check S30 r5apex_dx12.exe+0x1D83E40 for the initializer, which is responsible for looking up the used API's and construct the initial list.

> In 2026, R5AC has switched to manual stack tracing via RtlCaptureContext + RtlLookupFunctionEntry + RtlVirtualUnwind.

> Additionally, respawn seems to have added some old code back, which was basically a broad check for return address spoofing. It first checks if the current retaddr entry that it previously captured using their manual stack unwind. It only proceeds with the actual heuristic if the memory interpreted as uint8 at retaddr-5 is not evaluated to 0xE8. In x64, this is a direct near CALL instruction using a signed, 32-bit displacement for affecting the program counter. So if it reads something that isn't 0xE8, it will proceed to run the following heuristic. It starts by doing a backwards scan, beginning at retaddr - 2. It then continuously keeps interating until a maximum of 6. It checks whether any code bytes during the backwards scan evaluate to 0xFF. If that is positive, it will try to filter out the REG field of the current instruction's MODRM byte, and if it doesn't find patterns resembling a FF/2 or FF/3 type of CALL instruction, it will fall through to the telemetry submission label,

> Additional heads up: If the currently scanned retaddr happens to be of value zero, it will jump directly to the telemetry submission label. I can't say if the telemetry is actually sent because in that label it does a couple further checks first before finally sending it.

An example of this instance of detection can be found in C_ViewRender::GetMostRecentClipTransform.

> ```
> __int64 C_ViewRender::GetMostRecentClipTransform(__int64 a1, char frameIndex)
> {
>   v152 = frameIndex;  // Prime RNG (seems unrelated to stack walker)
>   R5AC::Prime = 214013 * R5AC::Prime + 2531011;  // Early exit: check stack walker enablement
>   if (!R5AC::IsStackWalkerEnabled)
>     return *(_QWORD *)(a1 + 8i64 * v152 + 1155920);  __int64 stackFrames[2] = { 0 };
>   __int128 stackData[2] = { 0 };  unsigned short numFrames = R5AC::Imp::RtlCaptureSBT(1, 5, stackData);
> ```

```
    if (!numFrames)
        return *(_QWORD *)(a1 + 8i64 * v152 + 1155920);    // Compute simple
hash of the captured stack
    int hashA = 5381, hashB = 0;
    char* p = reinterpret_cast<char*>(stackData);
    for (size_t i = 0; i < 8 * numFrames; ++i)
    {
        unsigned char val = *p++;
        hashA = val + 33 * hashA;
        hashB = val + 65599 * hashB;
    }
    int stackHash = hashA ^ hashB;    // Lock to check hash
    MEMORY[0x7FFE8D571760](&R5AC::SoemLock, 0);
    char hasChanged =
R5AC::HashmapHasChangedData((__int64)&R5::HashedCodeExecutionFrames,
&stackHash);
    MEMORY[0x7FFE8D571920](&R5AC::SoemLock);    if (hasChanged != -1)
    {
        // If hash is known, return cached transform
        return *(_QWORD *)(a1 + 8i64 * v152 + 1155920);
    }    // Iterate captured frames
    for (unsigned int i = 0; i < numFrames; ++i)
    {
        __int64 frameAddr = *reinterpret_cast<__int64*>(stackData + i);
        if (!frameAddr)
            break;        // Check if frame is in whitelisted regions
        bool inWhitelist = false;
        for (int j = 0; j < R5AC::WhitelistedSectionCount; ++j)
        {
            _WHITELISTED_SEGMENT_* region = &R5AC::WhitelistedSections[j];
            if (frameAddr >= region->Begin && frameAddr <= region->End)
            {
                inWhitelist = true;
                break;
            }
        }        if (inWhitelist)
            continue;        // If not whitelisted, fetch mapped module and push
violation
        char moduleName[272] = { 0 };
        ((void(__fastcall*)(__int64, __int64*, char*, __int64))0)(-1, frameAddr,
moduleName, 260);        if (moduleName[0])
        {
            R5AC::PushViolation(nullptr, 1, frameAddr,
reinterpret_cast<__int64>(moduleName));
```

```
            return *(_QWORD *)(a1 + 8i64 * v152 + 1155920);
          }
      }    // If no violations, store new hash
      MEMORY[0x7FFE8D5790A0](&R5AC::SoemLock,
R5AC::WhitelistedSectionCount, numFrames, R5AC::WhitelistedSections);
      sub_2345E0(&R5::HashedCodeExecutionFrames, &stackHash);
      MEMORY[0x7FFE8D562C70](&R5AC::SoemLock);    return *(_QWORD *)(a1 +
8i64 * v152 + 1155920);
}
```

A look at the Callers of RtlCaptureSBT

Some cheat developers have actually been using the aforementioned functionality against apex. See, because the API respawn uses for stack walking is resolved into an unchecked pointer in .data, anyone can just swap it out and fake the back trace buffer, or even cheaper: pretend like nothing on the stack was unwindable. As if that wasn't enough, respawn also have decided to making calls by referencing it's value across the game's entire code base.



What makes this much worse is the fact that this vulnerable pointer is referenced by numerous critical game functions. It's literally a backdoor so handy that you don't even need to hook CreateMove anymore, for example. You can just swap this pointer, check if caller (return address) is **C_Input::CreateMove**, and and that's it! Well, you'd also have to reconstruct the arguments passed down to it if your hook cares about that. It definitely will if you are planning to use the sequence number argument to retrieve an usercmd pointer.

> Actually, you could detect this quite trivially by checking where these manually resolved API's point to. You might also be detected indirectly if they actually keep track of writable regions and diff them or something like that. I know that approach might be very effective for catching changes on read-only stuff. Maybe they're doing these or something else already.

Above code was tested on retail apex legends, on both windows and linux. Since the flaw is in R5AC itself, platform mostly does not matter.

Revision #38
Created 2026-02-12 23:12:59 UTC by Admin
Updated 2026-11-02 16:33:51 UTC by Admin