

Forum:[Hack Forums](#)

Thread: [Analysis of a VAC module](#)

JPieky - November 27, 2015, 2:40 am

Analysis of a vac module

FileSize: 58,880 Bytes

.text hash: 0x59DC680

Number of scans: 4

TimeStamp: 0x564B49A8h Tue Nov 17 15:37:12 2015

This is a vac module that was created a week and a half ago.
So far it seems to be an updated version of a module that I reversed months ago.

For anyone interested, I run lionsneck.com and use my knowledge of vac to keep my builds undetected.

This is the analysis of the first scan.

To begin, the function 0x1000361C is called passing the current object, the target process id, and a third paramter.

The scan begins by opening a handle to the target process with OpenProcess using the parameters PROCESS_QUERY_INFORMATION and PROCESS_VM_READ.

If it fails to open a handle it calls GetLastError and returns error code 61.

The scan then stores the process id into the current object and calls GetProcessTimes to get and then store the creation timestamp.

Next it gets a handle to Kernel32.dll and gets the proc address of IsWow64Process.

If successful, it calls IsWow64Process on the current process using GetCurrentProcess.

It checks if the current process is 32 bit and if the target process is 64 bit.

If the target process is 64 bit, it does the following actions using the undocumented 64 bit APIs:

Code NtWow64ReadVirtualMemory64

NtWow64QueryInformationProcess64

Once past that, it calls NtQueryInformationProcess on the target process querying ProcessBasicInformation.

Then it stores the parent process id.

It checks if the PebBaseAddress is NULL.

If NULL, it queries NtQueryInformationProcess with the option ProcessImageFileName.

It then copies the image file name using widetochar_s and returns code 66.

If the PebBaseAddress is not NULL.

It uses ReadProcessMemory to read the PROCESS_EXECUTABLE_BLOCK structure from the target process.

Using the PEB it then uses ReadProcessMemory to read the ProcessParameters from the target process as well.

Using ReadProcessMemory it copies the Working Directory, Executable Path, and the Command Line from the target process.

After it finishes copying all the strings above, it reads the LoaderData using the PEB.

An interesting part is how they read the modules.

The undocumented version of the PEB_LDR_DATA contains three LIST_ENTRY structures while the MSDN version of the structure only contains one.

MSDN

```
Code typedef struct _PEB_LDR_DATA {
    BYTE    Reserved1[8];
    PVOID    Reserved2[3];
    LIST_ENTRY InMemoryOrderModuleList;
} PEB_LDR_DATA, *PPEB_LDR_DATA;
```

Undocumented:

```
Code typedef struct _PEB_LDR_DATA_EXTENDED{
    DWORD dwLength;
    DWORD dwInitialized;
    DWORD SsHandle;
    LIST_ENTRY InLoadOrderModuleList;
    LIST_ENTRY InMemoryOrderModuleList;
    LIST_ENTRY InInitializationOrderModuleList;
} PEB_LDR_DATA_EXTENDED;
```

The developers of this module are indirectly accessing the InLoadOrderModuleList by passing a negative index to the InMemoryOrderLinks array.

Code &LdrDataTableEntry.InMemoryOrderLinks.Flink[-1]

You can tell they are using the MSDN version of the structure since they pass 72 bytes to ReadProcessMemory rather than the actual size which is 80 bytes.

The InLoadOrderModuleList pointers happen to exist right above InMemoryOrderModuleList in memory, but InInitializationOrderModuleList does not exist after InMemoryOrderModuleList.

Continuing on.

They read up to a maximum of 1,000 modules in the format.

Code // (sizeof=0x224)

```
typedef struct _VAC_MODULE_ENTRY {
    char field_0[20],
    DWORD dwDllBase,
    DWORD dwSomeSize,
    DWORD dwDllBase2,
    char szImageName[256],
    char szFullDllName[260]
} VAC_MODULE_ENTRY;
```

It copies FullDllName, DllBase, and even assigns the target process id into what seems like the string buffer.

It uses HeapAlloc and HeapReAlloc to increase the size of the VAC_MODULE_ENTRY array with

every loop.

Once it reaches 1,000 modules, hits a null Flink, or the Flink points to the first entry. It stops copying the modules and the scan is finished.

I hope this was helpful to anyone else that is reversing VAC.

YesHax - November 27, 2015, 2:51 am

the same guy who was selling PEB removal and Server side encryption builds for 100\$/month, go and rip people off at reddit not here.

Almost forgot about you, thanks for reminding.

JPlekly - November 27, 2015, 3:27 am

(Nov 27, 2015 03:51 AM)mekelek Wrote: [\[CITE\]](#) the same guy who was selling PEB removal and Server side encryption builds for 100\$/month, go and rip people off at reddit not here.

Almost forgot about you, thanks for reminding.

Hello mekelek,

I don't believe I've had the pleasure of speaking with you.

However I did receive one of your previous messages:

Quote:On a scale of 1 to cypypaste, how cypypaste is this garbage?

[..]

It was a bit rude, especially since I have no animosity towards you since we have never spoken.

So I'd like to start a dialogue.

Hello, I'm James Plekly.

I did not offer PEB removal on my website.

I assume you're referring to unlinking my module from the PEB_LDR_DATA chain.

Erasing a PEB_LDR_DATA entry from from the module chain does not provide security.

In fact Valve Anti-Cheat can determine if your module has been unlinked by finding the file handle of your executable space with NT APIs.

The first feature that was listed was Portable Executable header removal.

Its not necessarily removal since it is not erased after the fact, but only used as a guideline for generating the payload that is loaded into the game's memory.

I was not offering PE Removal for \$100 USD, but rather 3 dozen features including metamorphic code.

I am not sure if you are aware of the difficulty of metamorphism.

It is not as simple as a packer or some other public solution.

Metamorphing a module requires a 100% analytical disassembly of your module so that when the opcodes are replaced with hundreds of combinations. The module can be reassembled in working order. It requires a thorough understanding of not only assembly, but of how the Microsoft Visual Run-Time Libraries initializes exception handlers, function pointer arrays, pointer jump tables, embedded data, and so much more.

Instead I dissolved the \$100 dollar features into the two existing packages so that they are both undetected from any existing tactics that Valve Anti-Cheat currently uses.

This is beneficial for all my existing customers and anyone interested in experiencing my products. Additionally I removed the listing of all the features since it was unsightly to have a long page of features above the purchase button.

If you have any questions about my builds, just let me know and I would be more than happy to discuss them here in this open forum.

YesHax - November 27, 2015, 3:47 am

(Nov 27, 2015 04:27 AM)JPlekly Wrote: [\[CITE\]](#) Hello mekelek,
I don't believe I've had the pleasure of speaking with you.
However I did receive one of your previous messages:

It was a bit rude, especially since I have no animosity towards you since we have never spoken.
So I'd like to start a dialogue.
Hello, I'm James Plekly.

I did not offer PEB removal on my website.
I assume you're referring to unlinking my module from the PEB_LDR_DATA chain.
Erasing a PEB_LDR_DATA entry from the module chain does not provide security.
In fact Valve Anti-Cheat can determine if your module has been unlinked by finding the file handle of your executable space with NT APIs.

The first feature that was listed was Portable Executable header removal.
Its not necessarily removal since it is not erased after the fact, but only used as a guideline for generating the payload that is loaded into the game's memory.

I was not offering PE Removal for \$100 USD, but rather 3 dozen features including metamorphic code.

I am not sure if you are aware of the difficulty of metamorphism.
It is not as simple as a packer or some other public solution.
Metamorphing a module requires a 100% analytical disassembly of your module so that when the opcodes are replaced with hundreds of combinations. The module can be reassembled in working order. It requires a thorough understanding of not only assembly, but of how the Microsoft Visual Run-Time Libraries initializes exception handlers, function pointer arrays, pointer jump tables, embedded data, and so much more.

Instead I dissolved the \$100 dollar features into the two existing packages so that they are both undetected from any existing tactics that Valve Anti-Cheat currently uses.
This is beneficial for all my existing customers and anyone interested in experiencing my products.
Additionally I removed the listing of all the features since it was unsightly to have a long page of features above the purchase button.

If you have any questions about my builds, just let me know and I would be more than happy to discuss them here in this open forum.
you forgot to post the other funny part about Mr. Thing cutiepie.
talk shit get hit.

J0ntE - November 27, 2015, 3:47 am

I dont understand anything of this but its interesting :D

Freak1234 - November 27, 2015, 5:21 am

Got a dump of input packet? too lazy to fire it up

iamvexatious - November 27, 2015, 5:23 am

Fairly sure this is a VGnosis, Fadedcoder or that tier0 shit, No one has had shitty GUI style and all his websites lookalike and push features in the same way, Regardless you payed for it to be

advertised on reddit, That's just silly.

lurkeryuri - November 27, 2015, 5:32 am

(Nov 27, 2015 06:23 AM)iamvexatious Wrote: [\[CITE\]](#) Fairly sure this is a VGnosis, Fadedcoder or that tier0 shit, No one has had shitty GUI style and all his websites lookalike and push features in the same way, Regardless you payed for it to be advertised on reddit, That's just silly.
top secret: segnosis runs both of those two, and has a sexy voice.

I don't think it's him.

iamvexatious - November 27, 2015, 5:39 am

(Nov 27, 2015 06:32 AM)lurkeryuri Wrote: [\[CITE\]](#) top secret: segnosis runs both of those two, and has a sexy voice.

I don't think it's him.

They both seem to have a hardon for glow esp and metamorphic Code as features, Tier0 and lionsneck both have a pretty similar feature list, Let's not forget that tier0 and lions neck have an nearly identical advertising for crosshair, RCS and both have features under a "Physics" tab (which is silly regardless) So either segnosis is a personal hero of James's or they're pretty tight ;)

Edit: I was well aware it was the same guy behind Faded, Tier0 just didn't know his name outside this forum.

NumbaN1ne - November 27, 2015, 8:42 am

Don't know what any of this means, but I got erect from it.

HOLEON - November 27, 2015, 8:43 am

(Nov 27, 2015 09:42 AM)NumbaN1ne Wrote: [\[CITE\]](#) Don't know what any of this means, but I got erect from it.

Now slap your monitor with it while singing this song:

[Video: https://www.youtube.com/watch?v=O3rpmctmC_M]

LordTristan - November 27, 2015, 3:08 pm

(Nov 27, 2015 04:27 AM)JPlekly Wrote: [\[CITE\]](#) Hello mekelek,
I don't believe I've had the pleasure of speaking with you.
However I did receive one of your previous messages:

It was a bit rude, especially since I have no animosity towards you since we have never spoken.
So I'd like to start a dialogue.
Hello, I'm James Plekly.

I did not offer PEB removal on my website.

I assume you're referring to unlinking my module from the PEB_LDR_DATA chain.

Erasing a PEB_LDR_DATA entry from from the module chain does not provide security.

In fact Valve Anti-Cheat can determine if your module has been unlinked by finding the file handle of your executable space with NT APIs.

The first feature that was listed was Portable Executable header removal.

Its not necessarily removal since it is not erased after the fact, but only used as a guideline for generating the payload that is loaded into the game's memory.

I was not offering PE Removal for \$100 USD, but rather 3 dozen features including metamorphic

code.

I am not sure if you are aware of the difficulty of metamorphism.

It is not as simple as a packer or some other public solution.

Metamorphing a module requires a 100% analytical disassembly of your module so that when the opcodes are replaced with hundreds of combinations. The module can be reassembled in working order. It requires a thorough understanding of not only assembly, but of how the Microsoft Visual Run-Time Libraries initializes exception handlers, function pointer arrays, pointer jump tables, embedded data, and so much more.

Instead I dissolved the \$100 dollar features into the two existing packages so that they are both undetected from any existing tactics that Valve Anti-Cheat currently uses.

This is beneficial for all my existing customers and anyone interested in experiencing my products. Additionally I removed the listing of all the features since it was unsightly to have a long page of features above the purchase button.

If you have any questions about my builds, just let me know and I would be more than happy to discuss them here in this open forum.

Don't waste your time responding to him, Mekelek is not a developer, he's just a forum troll. Nice share though.

Vuno - November 27, 2015, 3:10 pm

Mekelek is annoying. Should develop a task force like they did Osama Bin Laden and eliminate this nigga.

LordTristan - November 27, 2015, 3:12 pm

(Nov 27, 2015 04:10 PM)Vuno Wrote: [\[CITE\]](#) Mekelek is annoying. Should develop a task force like they did Osama Bin Laden and eliminate this nigga.

It would make sense if he was a developer and his opinion, even if insane, was backed up by knowledge but it's not, he's like Finale, if Finale wasn't a developer. That is awful, regardless, he's already on thin ice and he'll be gone from HF soon if he keeps up with his usual bullshit.

Vuno - November 27, 2015, 3:13 pm

Lmao I tried to report his post, and it was already reported. Task force started!

LordTristan - November 27, 2015, 3:15 pm

(Nov 27, 2015 04:13 PM)Vuno Wrote: [\[CITE\]](#) Lmao I tried to report his post, and it was already reported. Task force started!

You're welcome. ?

Illusionisten - November 27, 2015, 3:24 pm

(Nov 27, 2015 04:12 PM)LordTristan Wrote: [\[CITE\]](#) It would make sense if he was a developer and his opinion, even if insane, was backed up by knowledge but it's not, he's like Finale, if Finale wasn't a developer. That is awful, regardless, he's already on thin ice and he'll be gone from HF soon if he keeps up with his usual bullshit.

Finale best developer, he works as support in a tele company. Typical minimum wage immigrant.

i n v a l i d - November 27, 2015, 3:31 pm

Thanks for posting information that has been known for years now, you must of forgot about other garbage vac does, but who cares since you kids don't do anything different anyway.

Leave vac analyst to cra0 since you all have no clue what you're spewing

LordTristan - November 27, 2015, 8:03 pm

(Nov 27, 2015 04:31 PM)j n v a l i d Wrote: [\[CITE\]](#) Thanks for posting information that has been known for years now, you must have forgotten about other garbage vac does, but who cares since you kids don't do anything different anyway.

Leave vac analyst to cra0 since you all have no clue what you're spewing@ 13th November 2015, 11:49 PM

About a week later, it took me... about four hours to find, develop, test and complete a method to bypass ESEA so is that the same cra0 who's dick you're riding like a cheap AIDS infected whore? Because the moment all my ESEA bans lifted, I had ESEA bypassed again within hours. I guess your obsession needed my help.

The OP was kind enough to share information about the VAC modules, maybe just say thank you next time, asshole?

PS: cra0 is chill, nobody should take my comment as an attack on cra0.

Jidvei - November 28, 2015, 1:36 am

I find Tristan quite sympathetic :-)

YesHax - November 28, 2015, 2:46 am

(Nov 27, 2015 04:12 PM)LordTristan Wrote: [\[CITE\]](#) It would make sense if he was a developer and his opinion, even if insane, was backed up by knowledge but it's not, he's like Finale, if Finale wasn't a developer. That is awful, regardless, he's already on thin ice and he'll be gone from HF soon if he keeps up with his usual bullshit. Soon i won't even need to bother responding to you cause you will be put out of business.

In Pyro we trust.

I should make an account on the sites you're begging for help and troll you there, would be even more hilarious, if i would give a shit ofcourse.

swag1337 - November 28, 2015, 9:20 am

(Nov 28, 2015 03:46 AM)mekelek Wrote: [\[CITE\]](#) Soon i won't even need to bother responding to you cause you will be put out of business.

In Pyro we trust.

I should make an account on the sites you're begging for help and troll you there, would be even more hilarious, if i would give a shit ofcourse.

Obviously he(Tristan) Can't Understand Normal Thinking.

Vuno - November 28, 2015, 9:32 am

(Nov 28, 2015 03:46 AM)mekelek Wrote: [\[CITE\]](#) Soon i won't even need to bother responding to you cause you will be put out of business.

In Pyro we trust.

I should make an account on the sites you're begging for help and troll you there, would be even more hilarious, if i would give a shit ofcourse.

Don't steal my shit.

In Vuno we trust.

It's better to ask for help than scam users of a private hack, and get them banned. With only a 20 user base...Go pay someone to develop you a proper hack.

JPIekly - November 28, 2015, 9:35 am

(Nov 27, 2015 04:08 PM)LordTristan Wrote: [\[CITE\]](#) Don't waste your time responding to him,

Mekelek is not a developer, he's just a forum troll. Nice share though.

My mistake then.

I should have known better than to engage a forum troublemaker with content to use.

Later today I will be working on the additional scans and append my findings for everyone interested in this subject.

(Nov 27, 2015 06:21 AM)Freak1234 Wrote: [\[CITE\]](#) Got a dump of input packet? too lazy to fire it up I had not logged the runfunc parameters for this module.

It was cold disassembly in IDA Pro without any debugging.

If I encounter this module again I'll be sure to log the parameters.

Freak1234 - November 28, 2015, 9:42 am

(Nov 28, 2015 10:35 AM)JPlekly Wrote: [\[CITE\]](#) My mistake then.

I should have known better than to engage a forum troublemaker with content to use.

Later today I will be working on the additional scans and append my findings for everyone interested in this subject.

I had not logged the runfunc parameters for this module.

It was cold disassembly in IDA Pro without any debugging.

If I encounter this module again I'll be sure to log the parameters.

Roger that. I always appreciate if someone dumps them too cause it reveals much stuff in there / about the deployment

LordTristan - November 28, 2015, 9:56 am

(Nov 28, 2015 03:46 AM)mekelek Wrote: [\[CITE\]](#) Soon i won't even need to bother responding to you cause you will be put out of business.

In Pyro we trust.

I should make an account on the sites you're begging for help and troll you there, would be even more hilarious, if i would give a shit ofcourse.

If I have to choose between bruising my ego by asking for help or getting users VAC banned or league banned, I choose asking for help. I like to learn and understand.

swag1337 - November 28, 2015, 10:02 am

(Nov 28, 2015 10:56 AM)LordTristan Wrote: [\[CITE\]](#) If I have to choose between bruising my ego by asking for help or getting users VAC banned or league banned, I choose asking for help. I like to learn and understand.

but you still don't so.....

how02 - November 28, 2015, 10:32 am

You're all a bunch of amateurs it's funny to read :)

swag1337 - November 28, 2015, 12:58 pm

(Nov 28, 2015 11:32 AM)how02 Wrote: [\[CITE\]](#) You're all a bunch of amateurs it's funny to read :)

It is quite humorous ?

But I don't think you should be talking much either, you did get detected by h1z1's anticheat which is arguably worse than vac is.. not that vac is any good either.

how02 - November 28, 2015, 1:15 pm

(Nov 28, 2015 01:58 PM)swag1337 Wrote: [\[CITE\]](#) It is quite humorous ?

But I don't think you should be talking much either, you did get detected by h1z1's anticheat which is arguably worse than vac is.. not that vac is any good either.

On an early version that didn't include any security, big deal ?

swag1337 - November 28, 2015, 2:04 pm

(Nov 28, 2015 02:15 PM)how02 Wrote: [\[CITE\]](#) On an early version that didn't include any security, big deal ?

Well software being secure or not is a property of quality; so releasing a cheat that takes no regards to prevent itself from being detected would be "amateurish" as you stated. Ergo it's hypocritical.

KREAM_ - November 28, 2015, 4:22 pm

(Nov 28, 2015 03:46 AM)mekelek Wrote: [\[CITE\]](#) Soon i won't even need to bother responding to you cause you will be put out of business.

In Pyro we trust.

I should make an account on the sites you're begging for help and troll you there, would be even more hilarious, if i would give a shit ofcourse.

Fuck you are so gay it's not even funny.