

Forum:[Hack Forums](#)

Thread: [IonCube Decoding](#)

eddie_1600 - September 11, 2024, 10:25 pm

We all know of the indian scam websites claiming that they can decode PHP scripts encoded with IonCube in exchange for your money, but has there been any real progress made toward reverse-engineering modern versions of IonCube? If so, can anyone link any interesting research to read up on? I couldn't find anything myself. Thanks (:

kolaz - September 14, 2024, 1:11 am

You can check this site <https://phpdecode.xyz/?s=ioncube>

bl4cklak3 - September 18, 2024, 7:22 am

Is PHP encryption/obfuscation still a thing in 2024?

Years ago, there were multiple softwares that were capable of reverse engineering the ioncube encrypted code, so I can only assume this is still available somewhere on the internet.

notagh0st - September 18, 2024, 12:47 pm

(Sep 18, 2024 07:22 AM)bl4cklak3 Wrote: [\[CITE\]](#) Is PHP encryption/obfuscation still a thing in 2024?

Years ago, there were multiple softwares that were capable of reverse engineering the ioncube encrypted code, so I can only assume this is still available somewhere on the internet.

Ioncube is a little different than your normal PHP obfuscation, mainly because it uses a custom bytecode interpreter that runs in a VM, loading an encrypted AES bytecode and decrypting in memory. I still think it's probably possible, but like with many other things on this website, without an example of what OP is working with, can't really do much.

bl4cklak3 - September 18, 2024, 3:06 pm

(Sep 18, 2024 12:47 PM)notagh0st Wrote: [\[CITE\]](#) Ioncube is a little different than your normal PHP obfuscation, mainly because it uses a custom bytecode interpreter that runs in a VM, loading an encrypted AES bytecode and decrypting in memory. I still think it's probably possible, but like with many other things on this website, without an example of what OP is working with, can't really do much.

A rule of thumb is - if the program runs on your machine, you can reverse it.

I am not familiar on how Ioncube works. What I am saying is that there were multiple softwares that were able to reverse the files to their "near" original form years ago.

eddie_1600 - September 18, 2024, 6:10 pm

(Sep 18, 2024 12:47 PM)notagh0st Wrote: [\[CITE\]](#) Ioncube is a little different than your normal PHP obfuscation, mainly because it uses a custom bytecode interpreter that runs in a VM, loading an encrypted AES bytecode and decrypting in memory. I still think it's probably possible, but like with many other things on this website, without an example of what OP is working with, can't really do much.

While any encoding scheme can in-theory be decoded, there is no widely-known formula for decoding arbitrary IonCube PHP scripts (current latest version). My guess is that this will remain the case at least until after current versions are already replaced with something better

notagh0st - September 19, 2024, 6:49 am

(Sep 18, 2024 03:06 PM)bl4cklak3 Wrote: [\[CITE\]](#) A rule of thumb is - if the program runs on your machine, you can reverse it.

I am not familiar on how Ioncube works. What I am saying is that there were multiple softwares that were able to reverse the files to their "near" original form years ago.

Agreed, but it's similar to how VMProtect virtualization works (at least to my understanding, especially the newer version). Sure, it can be reversed, but it's extremely difficult, more so than your average run-of-the-mill PHP obfuscation. Without more information from OP, there's not really a whole lot of help that anyone can give.

eddie_1600 - September 19, 2024, 6:57 pm

(Sep 19, 2024 06:49 AM)notagh0st Wrote: [\[CITE\]](#) Agreed, but it's similar to how VMProtect virtualization works (at least to my understanding, especially the newer version). Sure, it can be reversed, but it's extremely difficult, more so than your average run-of-the-mill PHP obfuscation. Without more information from OP, there's not really a whole lot of help that anyone can give.

You don't have anything valuable to contribute regardless, so don't mind

notagh0st - September 19, 2024, 7:59 pm

(Sep 19, 2024 06:57 PM)eddie_1600 Wrote: [\[CITE\]](#) You don't have anything valuable to contribute regardless, so don't mind

Except for describing how ioncube works, as far as I know. But we still don't know what sample you're working with, what environment it's in (is it running in an environment you have access to, or was it a sample you found online that belonged to someone else), what the ioncube interpreter startup code/configuration looks like (if you have it), etc.