

Forum:[Hack Forums](#)

Thread: [Iphone shellcode to executable \(.ipa extension\)](#)

The Shark Inc. - January 21, 2018, 11:05 am

I try to make an executable shellcode (.ipa extension) file for Iphone.

I have 2 options.

- 1) Use eggshell (like metasploit for ios/macOS) to generate a terminal command(shellcode) to run on the target device,
The problem here is i don't know how to make an executable program to execute terminal commands on Iphone (dont know what libraries to use , and also what programming language. like swift(only for ios/macOS))
- 2)
Use metasploit , generate osx/armle/reverse_tcp payload but i dont know what file format should i use(e.g msfvenom -f exe) to meet my criteria.

Any answers?

The Shark Inc. - January 24, 2018, 11:36 am

can you understand what i asked or you are useless?

.eXe - January 25, 2018, 3:13 am

(Jan 24, 2018 12:36 PM)The Shark Inc. Wrote: [\[CITE\]](#) can you understand what i asked or you are useless?

You're the one that is asking how to run shellcode with no idea on where to begin. You're the useless one.

hempuk - January 25, 2018, 5:06 am

calling us useless, when you are the one who has no idea what you are doing... no one will help you now... mug ..i.

Smile? - January 25, 2018, 5:10 am

Use .exe and good luck buddy.

The Shark Inc. - January 28, 2018, 3:53 am

(Jan 25, 2018 04:13 AM)Evil.eXe Wrote: [\[CITE\]](#) You're the one that is asking how to run shellcode with no idea on where to begin. You're the useless one.

I didn't want to offend you , i am sorry

So back on my question , i'd like to know if you have any answers on my problem.

Best regards

CyberStrike - January 28, 2018, 12:39 pm

OP check out the following

<https://reverseengineering.stackexchange.com/questions/2814/disassemble-edit-and-re-assembly-ios-ipa-apps>

https://www.packtpub.com/mapt/book/networking_and_servers/9781785883255/8/ch08lvl1sec58/shell-reverse-tcp-for-ios

exe will not work on an IOS device

The Shark Inc. - January 29, 2018, 2:23 am

(Jan 28, 2018 01:39 PM)sirru5h Wrote: [\[CITE\]](#) OP check out the following

<https://reverseengineering.stackexchange.com/questions/2814/disassemble-edit-and-re-assembly-ios-ipa-apps>

https://www.packtpub.com/mapt/book/networking_and_servers/9781785883255/8/ch08lvl1sec58/shell-reverse-tcp-for-ios

exe will not work on an IOS device

Thanks for your help but i already have read the second link yesterday.

my problem now is how to bypass the gatekeeper so the victim can install unsigned apps

i thought making a backdoored app and upload it to vshare (3rd party enterprise app certificate signing).

What's your opinion?

CyberStrike - January 29, 2018, 3:43 am

Well I'll be honest, I don't mess with phones too often, more of network/webapp pentesting .. that said code signing certificates are a plus. If you try to upload to say iTunes you would never make it they actually check stuff, Google Play is a different story though.

denizdifiesso - January 25, 2021, 8:17 pm

This can help you man! :)

[fastlane\[.\]tools/](#)

[github\[.\]com/fastlane/examples](#)

[firebase.google\[.\]com/docs/app-distribution/ios/distribute-fastlane](#)

[docs.fastlane\[.\]tools/actions/xcodebuild/](#)

>>>

[docplayer\[.\]net/191860791-The-xcsset-malware-inserts-malicious-code-into-xcode-projects-perform-s-u-xss-backdoor-planting-in-safari-and-leverages-two-zero-day-exploits.html](#)

You can take a hint from these links, I hope to have been helpful! :-)

My BTC Address: 123M7q7qYbP4gPxDdscXfZjC2tANiRskZa

This is for distributing your App and for installing via MobileSafari! :)

[web.archive\[.\]org/web/20190824102915/bentedder\[.\]com/self-hosting-an-ad-hoc-distribution-ipa-file-for-app-development/](#)

Add http:// and after 20190824102915 the http://www.

All links uncensored:

<http://web.archive.org/web/20190824102915/http://www.bentedder.com/self-hosting-an-ad-hoc-distribution-ipa-file-for-app-development/>

bution-ipa-file-for-app-development/

<https://firebase.google.com/docs/app-distribution/ios/distribute-fastlane>

<https://github.com/fastlane/examples/>

<https://docplayer.net/191860791-The-xcsset-malware-inserts-malicious-code-into-xcode-projects-performs-uxss-backdoor-planting-in-safari-and-leverages-two-zero-day-exploits.html>

<https://docs.fastlane.tools/actions/xcodebuild/>

<https://fastlane.tools/>

Happy lucky! :)

Extra:

https://subscription.packtpub.com/book/networking_and_servers/9781785883255/8/ch08lvl1sec58/s-hell-reverse-tcp-for-ios

There's an app example, put into HelloWorld.xcodeproj files *.m and *.h your msfpayload C ShellCode or Payload!

[transfer sh/S5qR8/AppDecompiledExample.zip](https://transfer.sh/S5qR8/AppDecompiledExample.zip)

<https://transfer.sh/S5qR8/AppDecompiledExample.zip>