

Forum:[Hack Forums](#)

Thread: [Make Landing Page undetectable to AV](#)

Ancap - May 3, 2023, 2:51 am

Hey guys, I have a landing page that is being detectable to AV, mainly AVAST. When I enter the website it detects it as malicious.

Do you know how can I make it undetectable?

murado - May 3, 2023, 3:34 am

What exactly is a landing page? I read it very often. Is it some kind of website tricking people into clicking something or is it some kind of phishing page?

bronzegods - May 3, 2023, 3:39 am

If it is NSFW then you can add a warning before entering. If it doesn't work then you can request avast to remove your website from their blacklist.

Ph4n70M Phr34K - May 3, 2023, 3:43 am

(May 3, 2023 03:34 AM)murado Wrote: [\[CITE\]](#) What exactly is a landing page? I read it very often. Is it some kind of website tricking people into clicking something

Yes this is exactly, some kind of decoy website to make someone do something(for example download and run a file).

Phishing website is a website set up to steal your identity, or at least part of it. It does this by trying to convince you that it is a legitimate website, which needs those details to perform an action from which you will benefit.

OP. you didnt post any relevant info that would be needed to help you. At this moment we could only guess.

Ancap - May 4, 2023, 1:21 am

(May 3, 2023 03:34 AM)murado Wrote: [\[CITE\]](#) What exactly is a landing page? I read it very often. Is it some kind of website tricking people into clicking something or is it some kind of phishing page?

Its a page where I send my traffic to convert into something (buying something in this case). No phishing.

(May 3, 2023 03:39 AM)bronzegods Wrote: [\[CITE\]](#) If it is NSFW then you can add a warning before entering. If it doesn't work then you can request avast to remove your website from their blacklist. Not adult and they don't remove.

(May 3, 2023 03:43 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) Yes this is exactly, some kind of decoy website to make someone do something(for example download and run a file).

Phishing website is a website set up to steal your identity, or at least part of it. It does this by trying to convince you that it is a legitimate website, which needs those details to perform an action from which you will benefit.

OP. you didnt post any relevant info that would be needed to help you. At this moment we could only guess.

Its not pishing, In the landing there are some alerts like "you have a virus" "scan your PC" and Avast detect it as TechScam Website. I tried to obfuscate the code but not working. Is there anyway to "hide" the code or create new code automatly to trigger the AV?

Dread.Reaper - May 4, 2023, 6:07 am

(May 4, 2023 01:21 AM)Ancap Wrote: [\[CITE\]](#) Its a page where I send my traffic to convert into something (buying something in this case). No phishing.

Not adult and they don't remove.

Its not pishing, In the landing there are some alerts like "you have a virus" "scan your PC" and Avast detect it as TechScam Website. I tried to obfuscate the code but not working. Is there anyway to "hide" the code or create new code automatly to trigger the AV?

Well obfuscating the codes not going to help much, scanners will flag that even more.

Theres a few likely reasons why this could be happening but my best guess is the host you are using has a previous track record with the company for hosting or having hosted malicious content. and they are preforming a blanket approach to address the problem.

B3hindY0u - May 4, 2023, 6:43 am

In case if you are trying to get it fixed on the same server/domain, it will never work, since those itself will be blacklisted.

In my experience easiest way to get the page undetected is to write the source code from scratch, that way there will not be any already known "signatures", and avoid using sketchy keywords. Also disabling indexing and robots can help.

Ancap - May 4, 2023, 9:27 am

(May 4, 2023 06:07 AM)Dread.Reaper Wrote: [\[CITE\]](#) Well obfuscating the codes not going to help much, scanners will flag that even more.

Theres a few likely reasons why this could be happening but my best guess is the host you are using has a previous track record with the company for hosting or having hosted malicious content. and they are preforming a blanket approach to address the problem.

The hosting is not the problem I think because I open in locally and still getting the avast alert.

(May 4, 2023 06:43 AM)B3hindY0u Wrote: [\[CITE\]](#) In case if you are trying to get it fixed on the same server/domain, it will never work, since those itself will be blacklisted.

In my experience easiest way to get the page undetected is to write the source code from scratch, that way there will not be any already known "signatures", and avoid using sketchy keywords. Also disabling indexing and robots can help.

Is there any automation tool for this? Or is anyone that can do it paying? It's very very long and I don't know that much code.

Dread.Reaper - May 4, 2023, 9:31 am

(May 4, 2023 09:27 AM)Ancap Wrote: [\[CITE\]](#) The hosting is not the problem I think because I open in locally and still getting the avast alert.

Is there any automation tool for this? Or is anyone that can do it paying? It's very very long and I don't know that much code.

Well if what you are saying is accurate and there is nothing malicious on the website it would likely point to the host being the issue and not the sites scripting.

