

Forum:[Hack Forums](#)

Thread: "[Stegosploit t00lkit V2 \(Exploit Delivery via Steganography\)](#)"

nezha240697 - July 8, 2015, 8:53 am

Thanks to a technique called Stegosploit, a hacker can infect your system by simply making you load an image on the Internet. You don't even have to click or download the image.

What is Stegosploit?

Stegosploit is a technique developed by Security researcher Saumil Shah. The researcher presented it at Hack in the Box Conference recently held in Amsterdam. Using this technique, hackers can embed a malicious code inside the pixels [a pixel is a single point in a graphic image] of an image. And once a user loads this image on their browser, the malware will get downloaded automatically. Pictures that carry such codes do not look any different from other images. This technique works for both JPEG and PNG images.

So what does this mean?

It means that you may download a nasty virus on your system simply by viewing an image on your browser, without even clicking on it or downloading it.

Has Stegosploit been used in the wild?

There have been no reports which can evident the use of Stegosploit in the real world. But this does not mean that it won't. It is also important to note that, using this technique, hackers can accomplish practically anything such as stealing the victim's personal data, modifying files, opening a backdoor for other malware, etc.

and this toolkit?what does it do?

this toolkit lets you encode browser exploits in any picture you like by injecting it in the pixels of the image thus making it almost impossible to detect (you can't stop what you can't see)

features:

exploits hidden in pixels

image "auto runs" upon load

no visible distortion

decoder code bundled with the image

exploit automatically decoded and triggered

all with 1 image

the toolkit contains the following:

[img]http://s1.postimg.org/fo1u0zevz/capture2.png[/img]

[img]http://s7.postimg.org/d6rygm417/capture3.png[/img]

[img]http://s10.postimg.org/hkvaegcg9/capture6.png[/img]

[img]http://s13.postimg.org/d7o44oz5j/capture4.png[/img]

[img]http://s7.postimg.org/86ltu0u97/capture8.png[/img]

[BUY NOW](#)

ps:

read the README file FOR INSTRUCTIONS

works with meterpreter payloads

use at ur own risks

tutorial:

[Video: <https://www.youtube.com/watch?v=O9vSSQIZPII>]

Armada - July 8, 2015, 9:35 am

VERY interesting product.

Would you be interested in offering a vouch copy so I can review for you?

morph - July 8, 2015, 9:40 am

If you could provide me with a copy I'll write a highly detailed review for you.

V?rt - July 11, 2015, 9:50 pm

Wow, that's crazy. I'm never opening pics again.

lxcalthxst - July 11, 2015, 9:56 pm

Very nice... Will buy this soon

spidum - July 11, 2015, 10:01 pm

Wow I saw this years ago watching blackhat. I never thought I would ever have the opportunity to buy it haha. This shit is dangerous.

daymon - July 11, 2015, 10:07 pm

Stegosploit is an obfuscation technique to hide an exploit within images, its not actually an exploit.

xchg - July 11, 2015, 10:07 pm

(Jul 8, 2015 09:35 AM)A?mªDa Wrote: [\[CITE\]](#) VERY interesting product.

Would you be interested in offering a vouch copy so I can review for you?

I agree this is a very interesting product presentation.

Forgive me, but I'm a bit skeptical.

(Jul 11, 2015 10:07 PM)Sin???? Wrote: [\[CITE\]](#) Stegosplit is an obfuscation technique to hide an exploit within images, its not actually an exploit.

Thank you for clearing this up

?

nezha240697 - July 12, 2015, 2:23 pm

hey guys i understand your doubts that s why an awesome HF member is working on an honest review have a Nice day

indicud - July 23, 2015, 10:28 am

Does this work OP? I really want to purchase this...

Fresh Money - July 23, 2015, 10:37 am

Looks great, let me know if you still seek to give out some vouch copies, I will be more than happy to review this one for yu.

jarvis1 - February 9, 2016, 12:25 pm

Hi i know this thread is a bit old but i would like to know if this method is still working on browsers like chrome, firefox or safari.

Plus, i've read that you can also use your own exploit, i just want to know if i generate a python backdoor with veil evasion can i copy and paste the whole source code directly into this stegosplit toolkit or should i write a special "ad hoc" code?

Thanks :)

inferno.c - February 9, 2016, 12:30 pm

LOL! You are selling a free exploit and it's SUPER OLD

n3tw0rksyst2m - February 9, 2016, 8:48 pm

it's fake.

I buy it yesterday
but it's not work.

it can't encoding

I have a question.

then, what is new exploit toolkit?

answer to me. thanks :)

didonadezuk - April 27, 2016, 4:51 am

It's nice

Ready to take ,
Contact me soon
Thank's

Handsome-Jack - September 10, 2016, 10:57 am

This guy is selling free software yo.
Ban a mother fucker.

SKYGEN01 - November 4, 2016, 5:49 am

so u have stegosploit i m looking for

oliver77776 - November 4, 2016, 9:50 am

i tried clicking buy but get a error please pm me the new buying link or update it thanks

nezha240697 - November 5, 2016, 5:35 am

it is free now :

<https://sourceforge.net/projects/t800-mod/>

SKYGEN01 - November 5, 2016, 7:16 pm

This tool have in ur hand ? show me the demo so i can buy. contact me with ur skype id

nezha240697 - November 6, 2016, 5:54 am

(Nov 5, 2016 07:16 PM)SKYGEN01 Wrote: [\[CITE\]](#) This tool have in ur hand ? show me the demo so i can buy. contact me with ur skype id
new link :

google
enjoy

Armada - November 6, 2016, 8:41 am

(Nov 6, 2016 06:54 AM)nezha240697 Wrote: [\[CITE\]](#)
new link :

<https://rocketr.net/buy/360cb670e44e>

enjoy
Your selling stego now?

Its free on a google search dude. ?

BeyondInfinity - November 16, 2016, 6:11 am

This looks like an good thread !

Conscious - November 16, 2016, 6:19 am

I thought everyone knew that this is more or less public information?

I was at a conference where we heard about this among other stuff.
Don't buy this unless he offers something unique in he's "tool"

DocExploitTools - November 16, 2016, 6:45 am

Can you describe the exploit in detail?

vela1987 - March 6, 2017, 8:48 pm

the version in google doesnt allow to encode the payload

vrplayer22 - March 10, 2017, 9:26 pm

That is very interesting tool,I will purchase that someday.Thank you for share that :)