

Forum:[Hack Forums](#)

Thread: [Silent exploit](#)

Cmartinz - May 31, 2018, 5:32 am

Hi can anyone direct me to were i can get good silent exploit ?

Sp1gg5 - May 31, 2018, 7:13 am

I think you are going to need to give us a bit more details as to what your are trying to do?? If you are just looking for exploits, then exploit-db is a good start !!

Nomad.Null - May 31, 2018, 12:31 pm

Anytime I hear someone say "Silent Exploit" it makes me want to bash my head against a wall. If you're talking about macros or embedded malicious code, call it what it is and do some research. You'll quickly find that it's a very simple thing to do in theory but difficult to get past antivirus or spam filters, assuming you're talking about phishing, which we can't go into detail here.

If you're talking about newer, zero-day exploits for embedding malicious code silently into documents, you'll have no luck finding them. Nobody will sell that information to a newbie for starters because you'll end up over-using the method and it will lose its effectiveness. Second, it's expensive as fuck, and the researchers and malware developers who figure out new ways to do it don't just hand over their code to people because they ask nicely.

hampros2 - June 1, 2018, 8:50 am

for avoiding AV's you can check veil evasion

Astraviruzz - June 1, 2018, 8:56 am

(May 31, 2018 12:31 PM)True Demon Wrote: [\[CITE\]](#) Anytime I hear someone say "Silent Exploit" it makes me want to bash my head against a wall. If you're talking about macros or embedded malicious code, call it what it is and do some research. You'll quickly find that it's a very simple thing to do in theory but difficult to get past antivirus or spam filters, assuming you're talking about phishing, which we can't go into detail here.

If you're talking about newer, zero-day exploits for embedding malicious code silently into documents, you'll have no luck finding them. Nobody will sell that information to a newbie for starters because you'll end up over-using the method and it will lose its effectiveness. Second, it's expensive as fuck, and the researchers and malware developers who figure out new ways to do it don't just hand over their code to people because they ask nicely.

Agree with you %100 ? ? ? ??? ???

nkz66 - July 20, 2018, 4:55 pm

so meaning no one can get access to these silent exploit

Nyx - July 21, 2018, 7:39 pm

(Jul 20, 2018 04:55 PM)nkz66 Wrote: [\[CITE\]](#) so meaning no one can get access to these silent exploit

The reason they are called silent exploits is because no one knows they exist.

Zero-day exploits are exploits that have not been fixed or disclosed outside of the person and or group that is using set exploit.

YourRage - July 21, 2018, 7:42 pm

How to find 0-day exploits? I tried alot

kaibapara5 - July 22, 2018, 1:35 am

Oday(dot)today?

Oday exploits aren't free nor cheap. Just try to find people who doesn't update their PC and use old exploits on Exploit-db.

PerfectStorm - July 22, 2018, 1:38 am

(May 31, 2018 12:31 PM)True Demon Wrote: [\[CITE\]](#) Anytime I hear someone say "Silent Exploit" it makes me want to bash my head against a wall. If you're talking about macros or embedded malicious code, call it what it is and do some research. You'll quickly find that it's a very simple thing to do in theory but difficult to get past antivirus or spam filters, assuming you're talking about phishing, which we can't go into detail here.

If you're talking about newer, zero-day exploits for embedding malicious code silently into documents, you'll have no luck finding them. Nobody will sell that information to a newbie for starters because you'll end up over-using the method and it will lose its effectiveness. Second, it's expensive as fuck, and the researchers and malware developers who figure out new ways to do it don't just hand over their code to people because they ask nicely.

I love this post thank you

(Jul 21, 2018 07:42 PM)YourRage Wrote: [\[CITE\]](#) How to find 0-day exploits? I tried alot ya dont find it ?

HangMansheart - July 22, 2018, 3:07 pm

Oh jesus christ...

I wouldn't ever trust you with anything as powerful as a S I L E N T E X P L O I T.
Especially considering you have no idea what you're talking about.

Gee4rce - July 26, 2018, 6:06 pm

(Jul 21, 2018 07:39 PM)?itch Wrote: [\[CITE\]](#) The reason they are called silent exploits is because no one knows they exist.

Not sure if you was just trolling, but incase not i'd like to point out that a "silent exploit" defines a fully function exploit, which can be caried out remotely to execute code on the targeted system. The term silent describes that from exploit to final execution, there is no user interaction required, nor does the user see anything happen visually on the screen.

This also refers to "silent drive-by downloads" which are mostly carried out via Browser, where as the silent term describes the fact that these exploits do not need any clicking of link, button, popup and no installing of flash plugin, etc. to get the code execution going.

Cheers, Gee.

Nyx - July 26, 2018, 6:52 pm

(Jul 26, 2018 06:06 PM)Gee4rce Wrote: [\[CITE\]](#) Not sure if you was just trolling, but incase not i'd like to point out that a "silent exploit"

defines a fully function exploit, which can be caried out remotely to execute code on the targeted system. The term silent describes that from exploit to final execution, there is no user interaction required, nor does the user see anything happen visually on the screen.

This also refers to "silent drive-by downloads" which are mostly carried out via Browser,

where as the silent term describes the fact that these exploits do not need any clicking of link, button, popup and no installing of flash plugin, etc. to get the code execution going.

Cheers, Gee.

The OP did not mean the actual operation of the malware was silent, IE, silent malware is malware that the victim is not aware of what is happening like you mentioned above.

The OP wanted an exploit that was a zero-day, IE, an exploit that has not been found.

He used the the term "Silent" with a literal meaning.

Gee4rce - July 27, 2018, 1:34 am

(Jul 26, 2018 06:52 PM)?itch Wrote: [\[CITE\]](#) The OP wanted an exploit that was a zero-day, IE, an exploit that has not been found.

He used the the term "Silent" with a literal meaning.

Ah is see now, i didn't catch that at first read. Thanks for clarifying!

Cheers, Gee.

HiddenEye - August 7, 2018, 7:10 am

(Jul 21, 2018 07:42 PM)YourRage Wrote: [\[CITE\]](#) How to find 0-day exploits? I tried alot actually i should believe that you did not "tried alot" as you did write.

anyway zero day exploit are not for people who don't understand how bugs occur and how to manipulate the bug to get code execution etc.

Overdosed - August 7, 2018, 9:24 pm

(Jul 21, 2018 07:42 PM)YourRage Wrote: [\[CITE\]](#) How to find 0-day exploits? I tried alot

I usually dont get on people for not trying or whatever you want to call it but today ill will shed some info.

The fact youre asking for "0days" on this forum is your first issue. No one just gives "0days" away as there are plenty of people, companies and bounties offering cash rewards for such things so the liklihood youll find some free ones is slim.

The second part here is that you have looked and havent found anything. 0days shared on this forum are far from a zero day and quite frankly youd be wasting your time. Now to direct you in the correct place lets first start off by saying what im about to share will go right over your head and your quest for zero days will be short lived. If youre actually interested in malware and creating your own id suggest you learn some machine code/assembly and get on some more malware oriented websites.

<https://github.com/REal0day/MaliciousPark>

This is a honeypot database that gets updated once in awhile and has some serious exploits that can be reversed and used to your liking. Take a look at that pack of collected malware and get to learning!

HiddenEye - August 11, 2018, 5:21 am

(Aug 7, 2018 09:24 PM)Overdosed Wrote: [\[CITE\]](#) I usually dont get on people for not trying or whatever you want to call it but today ill will shed some info.

The fact youre asking for "0days" on this forum is your first issue. No one just gives "0days" away as there are plenty of people, companies and bounties offering cash rewards for such things so the liklihood youll find some free ones is slim.

The second part here is that you have looked and havent found anything. 0days shared on this

forum are far from a zero day and quite frankly youd be wasting your time. Now to direct you in the correct place lets first start off by saying what im about to share will go right over your head and your quest for zero days will be short lived. If youre actually interested in malware and creating your own id suggest you learn some machine code/assembly and get on some more malware oriented websites.

<https://github.com/REal0day/MaliciousPark>

This is a honeypot database that gets updated once in awhile and has some serious exploits that can be reversed and used to your liking. Take a look at that pack of collected malware and get to learning!

HQ post mate. just HQ for reversers

cthulhu1337 - *August 11, 2018, 6:23 pm*

if anyone has a market pm me too, thanks

daniterrer - *September 4, 2018, 12:03 pm*

(May 31, 2018 05:32 AM)Cmartinz Wrote: [\[CITE\]](#) Hi can anyone direct me to were i can get good silent exploit ?exploitdb, securityfocus, rapid7 are a few websites where you can find out