

Forum:[Hack Forums](#)

Thread: [Digital Certification Singer v1.5](#)

Tee Plow - December 19, 2016, 6:21 am

hello

today i release to you this tool a coded longtime ago

it will sign any file you want with a Digital Certification you grab from a signed file like : google chrome,skype, any signed product

this will make your file bypass some AV's

Screenshot :

download : <https://mega.nz/#!/UB1XTDQ!3JgjMJ42WfwFNNZ7K5RMa0kYnz3gvLoXHwrMH-r0cN4>

pass : teeplow

Twistd - December 19, 2016, 6:59 am

May I ask which AV's?

Because i have some serious problems understanding how signing a file with an invalid certificate is going to bypass anything runtime when antiviruses are checking the legitimacy of the certificates. I'd rather think it'd do more harm than good.

Tee Plow - December 19, 2016, 7:52 am

(Dec 19, 2016 07:59 AM)Twistd Wrote: [\[CITE\]](#) May I ask which AV's?

Because i have some serious problems understanding how signing a file with an invalid certificate is going to bypass anything runtime when antiviruses are checking the legitimacy of the certificates. I'd rather think it'd do more harm than good. just try it and u will see

xHeaven - December 19, 2016, 9:11 am

Interesting.

Before: <https://www.pscan.xyz/results.php?id=kOmdMCyjABBJLIFm>

After: <https://www.pscan.xyz/results.php?id=kqYRZmeNDINsOCkK>

LanMan - December 19, 2016, 9:20 am

(Dec 19, 2016 07:59 AM)Twistd Wrote: [\[CITE\]](#) May I ask which AV's?

Because i have some serious problems understanding how signing a file with an invalid certificate is going to bypass anything runtime when antiviruses are checking the legitimacy of the certificates. I'd rather think it'd do more harm than good.

Yea, that actually did bypass 3-4 unknown shitty AVs on virustotal when i tested it.

But thats for extremely detected stub (tested with a DC stub), otherwise you are right and it may cause more trouble than good ..

Edit: Yea, xHeaven post.

Tee Plow - December 19, 2016, 9:55 am

(Dec 19, 2016 10:20 AM)LanMan Wrote: [\[CITE\]](#) Yea, that actually did bypass 3-4 unknown shitty AVs on virustotal when i tested it.

But thats for extremely detected stub (tested with a DC stub), otherwise you are right and it may cause more trouble than good ..

Edit: Yea, xHeaven post.

in the past i was using it to bypass Total Security 360 runtime

LanMan - December 19, 2016, 9:59 am

(Dec 19, 2016 10:55 AM)Tee Plow Wrote: [\[CITE\]](#) in the past i was using it to bypass Total Security 360 runtime

Oh really ?

Anyway that's a free release, that's cool, it will maybe be useful for someone. ?

Twistd - December 19, 2016, 12:43 pm

(Dec 19, 2016 10:20 AM)LanMan Wrote: [\[CITE\]](#) Yea, that actually did bypass 3-4 unknown shitty AVs on virustotal when i tested it.

But thats for extremely detected stub (tested with a DC stub), otherwise you are right and it may cause more trouble than good ..

Edit: Yea, xHeaven post.

Why would you think bypass means scantime? :(

(Dec 19, 2016 10:55 AM)Tee Plow Wrote: [\[CITE\]](#) in the past i was using it to bypass Total Security 360 runtime

Will never work. Try to activate startup and youll get wrecked with or without a signed stub.

sobolek - December 19, 2016, 3:32 pm

(Dec 19, 2016 10:11 AM)xHeaven Wrote: [\[CITE\]](#) Interesting.

Before: <https://www.pscan.xyz/results.php?id=kOmdMCyjABBJLIFm>

After: <https://www.pscan.xyz/results.php?id=kqYRZmeNDINsOCkK>

What about that??

xHeaven - December 19, 2016, 4:34 pm

(Dec 19, 2016 04:32 PM)sobolek Wrote: [\[CITE\]](#) What about that??

Are you blind?

OP wrote

(Dec 19, 2016 07:21 AM)Tee Plow Wrote: [\[CITE\]](#) this will make your file bypass some AV's
My scans

(Dec 19, 2016 10:11 AM)xHeaven Wrote: [\[CITE\]](#) Before:

<https://www.pscan.xyz/results.php?id=kOmdMCyjABBJLIFm>

After: <https://www.pscan.xyz/results.php?id=kqYRZmeNDINsOCkK>

Before signing with a certificate (which always invalid btw), I got 12/35.

After signing, I got 15/35.

So this method isn't bypass any AV's, but trigger some AV's. Not a bad share btw, but a little useless, I think. [This is my opinion.]

Tee Plow - December 19, 2016, 4:51 pm

(Dec 19, 2016 05:34 PM)xHeaven Wrote: [\[CITE\]](#) Are you blind?

OP wrote

My scans

Before signing with a certificate (which always invalid btw), I got 12/35.

After signing, I got 15/35.

So this method isn't bypass any AV's, but trigger some AV's. Not a bad share btw, but a little useless, I think. [This is my opinion.]

u are wrong actually

just try it with another file

i won't share something that is useless

before : <https://scan.majyx.net/scans/result/32d6dded2aecb92403aa7e5a581a750f070c845c>

after : <https://scan.majyx.net/scans/result/2e0872880d1041ebbae0fe0992e98acb4be994d0>

xHeaven - December 19, 2016, 5:04 pm

(Dec 19, 2016 05:51 PM)Tee Plow Wrote: [\[CITE\]](#) u are wrong actually

just try it with another file

i won't share something that is useless

before : <https://scan.majyx.net/scans/result/32d6dded2aecb92403aa7e5a581a750f070c845c>

after : <https://scan.majyx.net/scans/result/2e0872880d1041ebbae0fe0992e98acb4be994d0>

Okay, and what's wrong with my file? Why I get more detections with the signed file? Maybe I'll try with some other files later.

Tee Plow - December 19, 2016, 5:07 pm

(Dec 19, 2016 06:04 PM)xHeaven Wrote: [\[CITE\]](#) Okay, and what's wrong with my file? Why I get more detections with the signed file? Maybe I'll try with some other files later.

maybe the file you grabbed the certification from

try with google chrome,skype,or even an AV like in my example i'm using Total Scurity 360 certification

LanMan - December 19, 2016, 5:15 pm

(Dec 19, 2016 01:43 PM)Twistd Wrote: [\[CITE\]](#) Why would you think bypass means scantime? :(

I don't, we were just talking about scantime and emulation results, well if you have a 45/56 stub at scantime, runtime isn't your priority haha ?

xHeaven - December 19, 2016, 5:20 pm

(Dec 19, 2016 06:07 PM)Tee Plow Wrote: [\[CITE\]](#) maybe the file you grabbed the certification from try with google chrome,skype,or even an AV like in my example i'm using Total Scurity 360 certification

The original file is a Quasar RAT stub, I tried to sign with a Google Chrome certification. I'm totally confused, lol.

I tried with an another file, same results.. [Google Chrome cert.]

Before: <https://www.pscan.xyz/results.php?id=KGENeMYNyRGZcpKh>

After: <https://www.pscan.xyz/results.php?id=ncdfoccOXVfeCCAP>

And with the same file, with an another certification [Avast]

Before: <https://www.pscan.xyz/results.php?id=KGENeMYNyRGZcpKh>

After: <https://www.pscan.xyz/results.php?id=xdKwxYBTiXASiFPD>

Lol, interesting.. O.o IDK, thanks for the share, I'm going to sleep.

Tee Plow - December 19, 2016, 5:29 pm

(Dec 19, 2016 06:20 PM)xHeaven Wrote: [\[CITE\]](#) The original file is a Quasar RAT stub, I tried to sign with a Google Chrome certification. I'm totally confused, lol.

I tried with an another file, same results.. [Google Chrome cert.]

Before: <https://www.pscan.xyz/results.php?id=KGENeMYNyRGZcpKh>

After: <https://www.pscan.xyz/results.php?id=ncdfoccOXVfeCCAP>

And with the same file, with an another certification [Avast]

Before: <https://www.pscan.xyz/results.php?id=KGENeMYNyRGZcpKh>

After: <https://www.pscan.xyz/results.php?id=xdKwxYBTiXASiFPD>

Lol, interesting.. O.o IDK, thanks for the share, I'm going to sleep.
you are wlc my friend ?

Twistd - December 19, 2016, 11:58 pm

(Dec 19, 2016 06:15 PM)LanMan Wrote: [\[CITE\]](#) I don't, we were just talking about scantime and emulation results, well if you have a 45/56 stub at scantime, runtime isn't your priority haha ?

Fake signature != anti emulation

Why would you not fud your detections properly? Adding a fake signature would probably create more runtime detections than it already has as it cannot be validated.

Tee Plow - December 20, 2016, 3:54 am

(Dec 20, 2016 12:58 AM)Twistd Wrote: [\[CITE\]](#) Fake signature != anti emulation

Why would you not fud your detections properly? Adding a fake signature would probably create more runtime detections than it already has as it cannot be validated.

bla bla bla

Codefuser - December 20, 2016, 4:31 am

(Dec 20, 2016 04:54 AM)Tee Plow Wrote: [\[CITE\]](#) bla bla blaHe is right lol

This is not a reliable way of removing detections.

Tee Plow - December 20, 2016, 4:35 am

(Dec 20, 2016 05:31 AM)Codefuser Wrote: [\[CITE\]](#) He is right lol

This is not a reliable way of removing detections.

(Dec 19, 2016 06:20 PM)xHeaven Wrote: [\[CITE\]](#) And with the same file, with an another certification [Avast]

Before: <https://www.pscan.xyz/results.php?id=KGENeMYNyRGZcpKh>

After: <https://www.pscan.xyz/results.php?id=xdKwxYBTiXASiFPD>

Lol, interesting.. O.o IDK, thanks for the share, I'm going to sleep.

Codefuser - December 20, 2016, 4:58 am

Doesn't make it reliable. Sometimes it works sometimes it doesn't. Sometimes it even adds detection.

Tee Plow - December 20, 2016, 5:07 am

(Dec 20, 2016 05:58 AM)Codefuser Wrote: [\[CITE\]](#) Doesn't make it reliable. Sometimes it works sometimes it doesn't. Sometimes it even adds detection.

no , it's reliable you just have to choose the right certification

LanMan - December 20, 2016, 9:54 am

(Dec 20, 2016 12:58 AM)Twistd Wrote: [\[CITE\]](#) Fake signature != anti emulation

Why would you not fud your detections properly? Adding a fake signature would probably create more runtime detections than it already has as it cannot be validated.

Obviously, that's not what i said.

What if for X reason someone can't ?

It will not create more detections if your stub is already detected by all AVs

And it will only triggers while checking the signature sha1 at scantime.

I agree with you if your base stub is UD or it is crypted, no reason to do a sketchy spoof then, but if you don't have anything it's still better than nothing.

And there is a little typo in the title OP, "Certification SINGER v1.5" haha ?

Twistd - December 20, 2016, 10:13 am

(Dec 20, 2016 10:54 AM)LanMan Wrote: [\[CITE\]](#) Obviously, that's not what i said.

What if for X reason someone can't ?

It will not create more detections if your stub is already detected by all AVs

And it will only triggers while checking the signature sha1 at scantime.

I agree with you if your base stub is UD or it is crypted, no reason to do a sketchy spoof then, but if you don't have anything it's still better than nothing.

And there is a little typo in the title OP, "Certification SINGER v1.5" haha ?

If you don't know programming then sure i agree with you :)