

Forum:[Hack Forums](#)

Thread: [Downloaders for FUD Malware...What's your take on this?!](#)

Reaper91 - August 23, 2013, 3:16 pm

Hey guys, just wanted to get a second opinion on this matter. I've been noticing more and more what type of things AV's pick up on after messing around with a crypter for a good 2-3 months. So, I have my own advanced codedom based crypter I coded. On first run of it, it was UD 2/35, Ikarus and Asquared. I started to comment out lines til it was FUD. You know what caused the detection? The encryption methods! So, I tossed encryption out the door. I now use compression and data to bmp, due credits to 0xDeadDead for that source I use. Now, it's FUD! So just recently, Ikarus and Asquared came back. And, I'm thinking, WTF?! This time, I'm thinking, dammit, it's my bytes to bmp or compression but more than likely the data/bmp conversion since it is public. So, my idea would be to upload our encryptions, compressions, or data conversions to pastebin and then download on runtime. I know that using this for storage method is a bad idea but what about our data hiding methods?! Would that be all that bad?! Yes, no, maybe so?!

pow3rful_UP - August 24, 2013, 1:28 am

well, downloading is not a bad idea at all, that way you shorten the code you need in the actual stub and have less code that could get detected

Still, one thing you need to remember is that

- A) The connection itself could be detected, that means a av firewall could flag the connection as malicious and stop your file from working.
- B) The downloaded bytes itself are detected > that means you did not encrypt the file on the host > the av will trigger a detection.
- C) Someone could remove the file from your host, or the host could be down

Those are all reasons why downloaders are sometimes not the best ideas for crypters, you infact have a less chance of execution.

My advice for you would be >

Take the encrypted file, and all its functions (runpe, startup etc) put it into a dll, encrypt the dll then add the dll as resource to your stub.

Then decrypt the dll and load it into memory with assembly load

That leaves you behind with 2 methods to fud, the encryption method and the invoking method, that is the LEAST possible code you can generate for a crypter, even with your download method you need a encryption(well, rather a decryption method) and a load into memory method, same as my method..

Reaper91 - August 24, 2013, 10:47 am

Hey pow3r, I already use your method of the dll. It's still flagged by Ikarus and Asquared. The only functions in my stub is invoke, resource reader, decompress, and bmp to bytes. I thinks it's bmp to bytes or resource reading because my compression is not very public. It is gzip though so who knows?!

pow3rful_UP - August 24, 2013, 11:01 am

(Aug 24, 2013 10:47 AM)Reaper91 Wrote: [\[CITE\]](#) Hey pow3r, I already use your method of the dll. It's still flagged by Ikarus and Asquared. The only functions in my stub is invoke, resource reader, decompress, and bmp to bytes. I think it's bmp to bytes or resource reading because my compression is not very public. It is gzip though so who knows?!

Hey, if i could recommend you something then it would be to put the compression into the dll, because the big part that needs the compression is the file you encrypt, not your runpe/startup codes (those codes shouldnt be larger then 50-100 kb)

Also, whats the matter with that bmp to bytes method? What do you use it for? As a storage method? You store the files as bmp file and then read the filebytes from that file with that method?

Also, one thing you should note is that av's flag your stub as detected if it has hardly any code, most people say "junk code is rubbish and is stupid" but that is untrue! Avs do flag your stub if it doesnt contain alot of code (for example, if you have a application with no codes and use the resources your chance of getting a detection caused by the resources is wayyy higher as for a programm with more codes that uses resources)

I have personally experienced that with my own crypter..

So just test it out a bit, really.. You will figure a way out to fud it, and if you dont, well then you should not do crypters, the hard was is to find a fud method, making the crypter work is easy..

Reaper91 - August 24, 2013, 1:00 pm

Alrite, thanks for the idea on the compression. And yes, turning my server bytes into a bmp is my storage method.

Foreground - October 4, 2013, 7:23 am

@Reaper91,

If this is the source from the PM's we had, this pass a lot av's and their corresponding firewalls. I tested and passed Avira, Eset, Norton etc, but some settings from these firewalls did block on occation. I don't know which ones. I tested "live" and saw one firewall from Av "A" pass and on another pc from Av "A" block at the same time. Maybe versions and updates of the Av's?