1. Virus encoder:

A virus encoder is used to encode a virus in a way so that it can not be read and not be detected by anti-malware software and network intrusion detection.

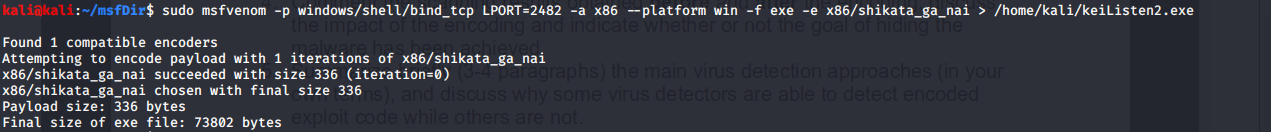
“Shikata\_ga\_nai,” on msfvenom, which is Japanese and it means, “nothing can be done.” It is a polymorphic XOR additive feedback encoder.

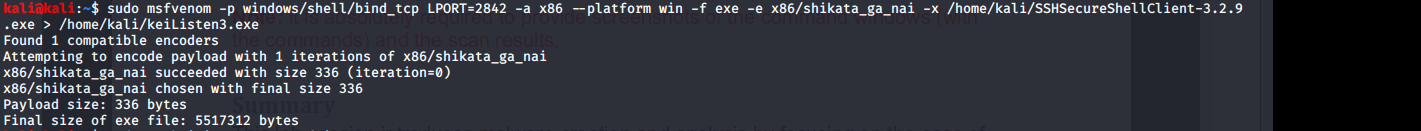
It is polymorphic because each shellcode created is different from the last. It does this in such ways such as:

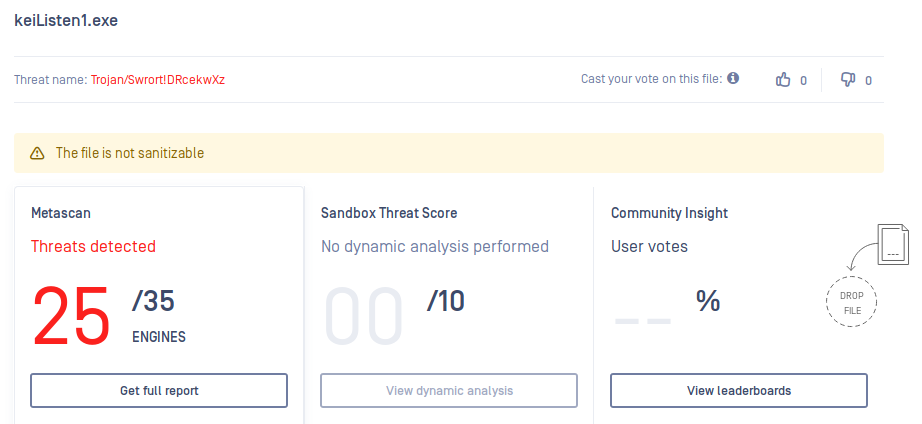
* Dynamic instruction substitution
* Dynamic block ordering
* Randomly interchanging registers
* Randomizing instruction ordering
* Inserting junk code
* Random keys
* Randomization of instruction spacing between other instructions.

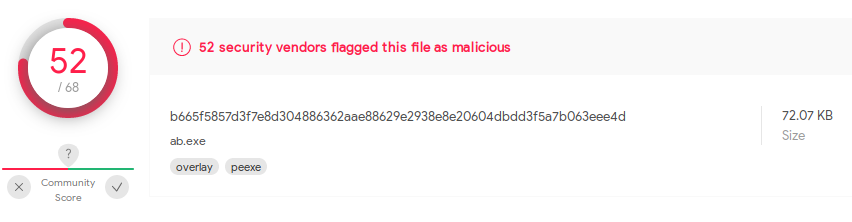
The XOR additive feedback means the algorithm is XORing future instructions by a random key and then adding that instruction to the key to be used again to encode the next instruction.

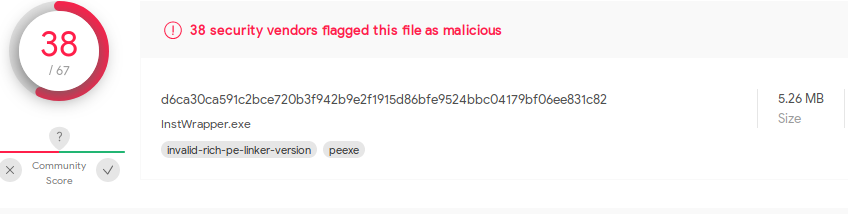
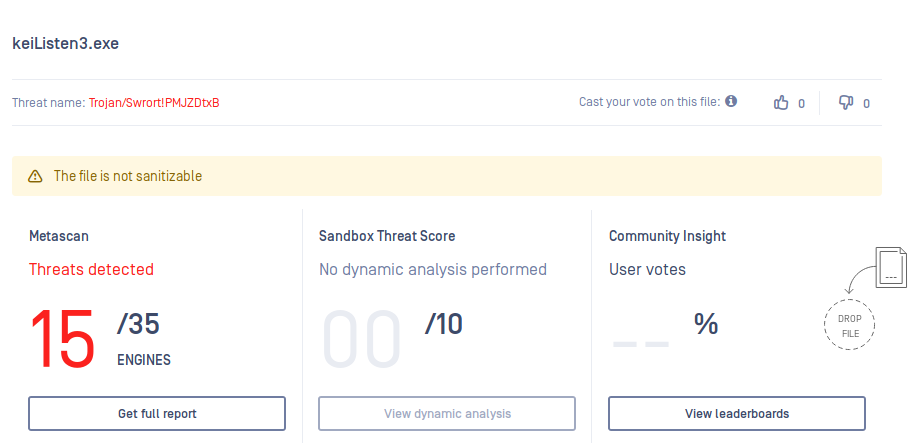
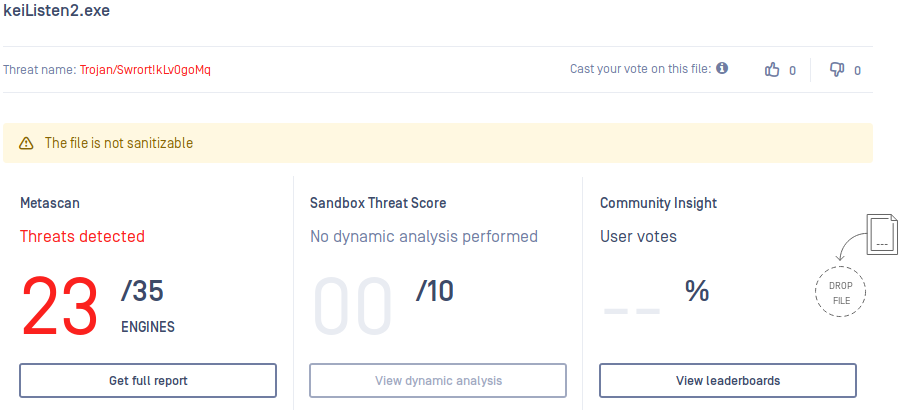












Before the process of encoding, the malware was detected by a large majority of the malware detection programs. After the encoding, there were less detections which means that the encoding helped to get the malware past the detection of the programs. This means that encoding the malware can be the difference between success and failure when attacking. As long as they have an anti-malware program that it can bypass, encoding will allow the attack to be successful.



There are many virus detectors out there on the internet in this day and age. The anti-virus software scans incoming files or codes passing through the network. The company responsible for the particular anti-virus software will have a database composed of all known viruses and similarly encoded viruses. This extensively composed database is used to compare the incoming files and will detect any similarities that are viruses.

In a sense, it is similar to the password dictionaries that attackers use. The dictionary that the attacker creates is a database that searches for similarities by comparing the passwords. The anti-virus software does it in nearly the same way which comes with the same pros and cons.

The software is able to detect viruses but only those that are recorded in their database. THis means that companies that do not update their database will fall behind in the ever evolving race between the growth and development of exploit codes and the protection against it. The softwares that are not updated will not be able to detect some exploit codes and definitely not be able to detect it if it has been encoded.