INTEZER

INTEZER ANALYZE

Automate Threat Hunting with Code-based Vaccines

Technical Guide

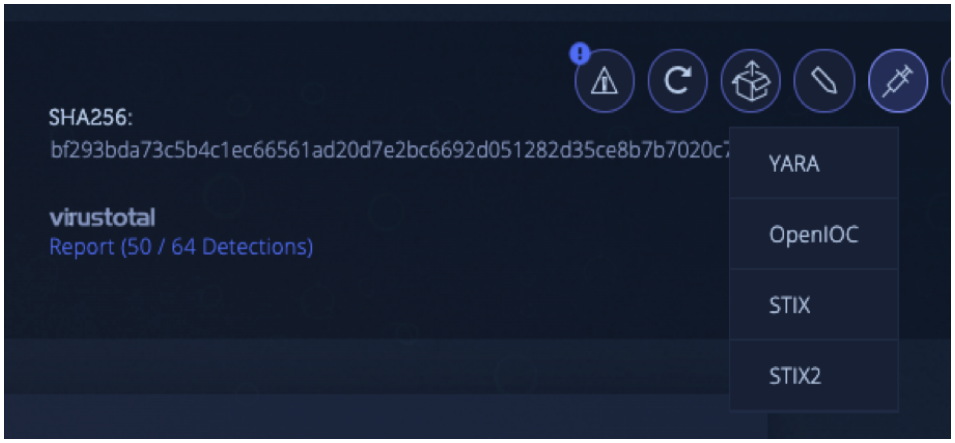
Vaccine

In Intezer Analyze a **vaccine** is an automatically generated YARA signature based on the malicious and unique **genes** (aka **binary code**) of a malware sample.

YARA signatures **that** are based on weak indicators such as strings, command-and-control servers, and domain names, can be easily manipulated, replaced, or encrypted by adversaries to avoid detection. Intezer's YARA signatures are based only on a sample's malicious and unique code, rather than trusted code from a shared or embedded library, to reduce false positives and generate more accurate hits.

How to Produce the YARA Signature

In Intezer Analyze, users have the ability to generate a YARA signature for any specific file simply by clicking on the vaccine icon in the upper right corner of the analysis report **(see Figure 1).**



Vaccine Icon (Figure 1)

Once the vaccine icon is clicked, the YARA signature will be generated immediately and downloaded directly onto your computer. If you open this file, you will see Intezer Analyze searches for specific byte values which represent the genes (see Figure 2). The signature is flexible, as the system searches only for a specific percentage of genes, in order to match other samples from the same malware family.

```
rule Intezer_Vaccine_bf293bda73c5b4c1ec66561ad20d7e2bc6692d051282d35ce8b7b7020c753467
{
    meta:
        copyright = "Intezer Labs"
        description = "Automatic YARA vaccination rule created based on the file's genes"
        author = "Intezer Labs"
        reference = "https://analyze.intezer.com"
        date = "2019-01-06"
        sha256 = "bf293bda73c5b4c1ec66561ad20d7e2bc6692d051282d35ce8b7b7020c753467"
    strings:
        $4237064_289 = { 33 ?? 83 ?? ?? 8A ?? 33 ?? 8A ?? ?? ?? 8B ?? ?? ?? ?? ?? ?? 8B ?
        $4243338_214 = { 8A ?? ?? ?? ?? ?? 5? 5? 88 ?? ?? ?? B9 ?? ?? ?? ?? 33 ?? 8D ?? ?
        $4236863_189 = { 8B ?? ?? ?? 33 ?? 33 ?? 5? 8A ?? 8A ?? ?? C1 ?? ?? 4? 8B ?? ?? C
        $4212672_146 = { 5? 8B ?? 6A ?? 68 ?? ?? ?? ?? 68 ?? ?? ?? ?? 64 ?? ?? ?? ?? ?? 5
        $4199537_113 = { 5? 6A ?? 8D ?? ?? ?? ?? ?? ?? 68 ?? ?? ?? ?? 5? FF D? 5? FF 1? ?
        $4201584_105 = { 81 E? ?? ?? ?? ?? 5? 5? 5? 5? B9 ?? ?? ?? ?? BE ?? ?? ?? ?? 8D ?
        $4244720_98 = { 64 ?? ?? ?? ?? ?? 6A ?? 68 ?? ?? ?? ?? 5? B8 ?? ?? ?? ?? 64 ?? ??
        $4227264_96 = { 81 E? ?? ?? ?? ?? 5? 5? 5? 8B ?? 5? B9 ?? ?? ?? ?? 33 ?? 8D ?? ??
        $4200408_88 = { B9 ?? ?? ?? ?? 33 ?? 8D ?? ?? ?? 88 ?? ?? ?? F3 ?? 66 ?? AA B9 ??
        $4213168_85 = { 5? 8B ?? 6A ?? 68 ?? ?? ?? ?? 68 ?? ?? ?? ?? 64 ?? ?? ?? ?? ?? 5?
        $4241472_84 = { 81 E? ?? ?? ?? ?? A0 ?? ?? ?? ?? 5? 5? 88 ?? ?? ?? B9 ?? ?? ?? ??
        $4241641_81 = { A0 ?? ?? ?? ?? B9 ?? ?? ?? ?? 88 ?? ?? ?? ?? ?? ?? 33 ?? 8D ?? ??
```

YARA Signature (Figure 2)

The vaccines can be used in a variety of cases where YARA is supported, namely with containment and hunting.

INTEZER ANALYZE

Here are Two Ways to Leverage the YARA Signatures

1. Proactive Threat Hunting

The signature will be effective for detecting additional and new hashes of the threat, in addition to similar variants since you can choose how flexible you want the signature to be; based on the number of code strings in the rule (the default value is 70%).

Once the signature has been generated you can deploy it in your feeds. For example, it's possible to integrate the rule within VirusTotal Hunting rules. For every sample that is uploaded to VirusTotal, or if an existing sample is rescanned, it will be executed across the YARA rule and you will receive hits once there is a relevant match.

You can also integrate the rule with any of your own systems that support the YARA format and allow you to deploy YARA rules in them.

2. Scan for Infected Endpoints

When an infection occurs, one of the first steps involved in the response is to understand if the threat has spread throughout the organization. Use the YARA signature to search for matches on other potentially infected endpoints within the organization. Scan other endpoint disks with the signature to ensure that no other computers are infected with the threat. Technically, it needs to be shipped with YARA.exe by executing this command:

yara RULES_FILE TARGET

To scan the memory of your endpoints, we recommend executing our agentless endpoint analysis scanner located in Intezer Analyze. The scanner collects only executable code, not documents or any other data that is not binary code.

The research team at Intezer uses these code-based vaccines to proactively hunt for new threats. Visit intezer.com/blog to read about some of the previously undetected threats they have identified using these signatures.

HiddenWasp

EvilGnome

APT34

APT34