CLAIMS

1. A malware monitoring method, comprising:

obtaining a malware sample;

extracting operational parameters corresponding to the malware sample;

configuring an emulator application corresponding to the malware sample using the operational parameters;

selecting a plurality of client attribute sets from a preconfigured list of client attributes, each of the selected plurality of client attribute sets including at least a geographic region;

executing a plurality of instances of the configured emulator application, each of the plurality of instances having a respective one of the selected plurality of client attribute sets;

collecting output data from each of the plurality of instances;

generating indicators of compromise (IOCs) based on the collected output data output;

periodically detecting that a first subset of the plurality of instances are not generating output; and

terminating the first subset of the plurality of instances, while continuing execution of a second subset of the plurality of instances.

2. The method of claim 1, wherein obtaining the malware sample includes retrieving the malware sample from at least one preconfigured source.

3. The method of claim 1, wherein extracting the operational parameters includes:

executing the malware sample in a plurality of sandbox environments to generate respective sets of sample output; and

extracting the operational parameters from the sets of sample output at an extraction module external to the plurality of sandbox environments.

4. The method of claim 3, wherein the respective sets of sample output include at least one of memory dumps, files, and network traffic.

5. The method of claim 1, wherein the operational parameters include at least a network address of a control server corresponding to the malware sample.

6. The method of claim 5, wherein periodically detecting that the first subset of the plurality of instances are not generating output includes:

determining whether any of the plurality of instances have not received data from the control server for a predetermined period of time.

7. The method of claim 1, wherein each of the selected plurality of client attribute sets further includes at least one of a client operating system, and a client computing architecture.

8. The method of claim 1, wherein executing the plurality of instances includes routing requests to a control server through a proxy interface corresponding to the geographic region.

9. The method of claim 1, further comprising:

determining whether the output data indicates an update requirement for the plurality of instances; and

when the determination is affirmative, repeating the extraction of operational parameters.

10. A computing device, comprising:

a communications interface;

a memory; and

a processor configured to:

obtain a malware sample;

extract operational parameters corresponding to the malware sample;

configure an emulator application corresponding to the malware sample using the operational parameters;

select a plurality of client attribute sets from a preconfigured list of client attributes, each of the selected plurality of client attribute sets including at least a geographic region;

execute a plurality of instances of the configured emulator application, each instance of the plurality of instances having a respective one of the selected plurality of client attribute sets;

collect output data from each of the plurality of instances;

generate indicators of compromise (IOCs) based on the collected output data;

periodically detect that a first subset of the plurality of instances are not generating output; and

terminate the first subset of the plurality of instances, while continuing execution of a second subset of the plurality of instances.

11. The computing device of claim 10, wherein the processor is configured, in order to obtain the malware sample, to retrieve the malware sample from at least one preconfigured source.

12. The computing device of claim 10, wherein the processor is configured, in order to extract the operational parameters, to:

execute the malware sample in a plurality of sandbox environments to generate respective sets of sample output; and

extract the operational parameters from the sets of sample output at an extraction module external to the plurality of sandbox environments.

13. The computing device of claim 12, wherein the respective sets of sample output include at least one of memory dumps, files, and network traffic.

14. The computing device of claim 10, wherein the operational parameters include at least a network address of a control server corresponding to the malware sample.

15. The computing device of claim 14, wherein the processor is further configured, to periodically detect that the first subset of the plurality of instances are not generating output to:

determine whether any of the plurality of instances have not received data from the control server for a predetermined period of time.

16. The computing device of claim 10, wherein each of the selected plurality of client attribute sets further includes at least one of a client operating system, and a client computing architecture.

17. The computing device of claim 10, wherein the processor is configured, in order to execute the plurality of instances, to route requests to a control server through a proxy interface corresponding to the geographic region.

18. The computing device of claim 10, wherein the processor is further configured to:

determine whether the output data indicates an update requirement for the plurality of instances; and

when the determination is affirmative, repeat the extraction of operational parameters.