

CLAIMS

1. A client system comprising:

a memory, and

at least one hardware processor connected to the memory and configured to execute an anti-malware engine configured to monitor a target process for malicious activity, wherein the target process executes on the client system, wherein the target process comprises an instance of a main executable module and an instance of a shared library, and wherein the at least one hardware processor is further configured to:

receive from a server a first module reputation indicator of the main executable module and a second module reputation indicator of the shared library, the first module reputation indicator determined according to a behavior of another instance of the main executable module, wherein the server is configured to perform anti-malware transactions with a plurality of client systems including the client system, wherein the first module reputation indicator comprises an indicator of a first set of monitoring rules, and wherein the second module reputation indicator comprises an indicator of a second set of monitoring rules;

in response to receiving the first and second module reputation indicators, determine whether the target process is likely to be malicious according to the first and second module reputation indicators; and

in response to determining whether the target process is likely to be malicious, when the target process is not likely to be malicious,

combine the first and second sets of monitoring rules into a combined set of monitoring rules, and

configure the anti-malware engine to monitor the target process according to the combined set of monitoring rules.

2. The client system of claim 1, wherein the at least one hardware processor is configured to determine the combined set of monitoring rules according to a union of the first and second sets of monitoring rules.

3. The client system of claim 1, wherein the at least one hardware processor is configured to determine the combined set of monitoring rules according to an intersection of the first and second sets of monitoring rules.

4. The client system of claim 1, wherein a selected rule of the first set of monitoring rules includes a selected heuristic employed to determine whether the target process is malicious.

5. The client system of claim 1, wherein a selected rule of the first set of monitoring rules instructs the anti-malware engine to determine whether the target process performs a selected action.

6. The client system of claim 1, wherein the another instance of the main executable module executes on a second client system of the plurality of client systems.

7. The client system of claim 1, wherein the at least one hardware processor is further configured, in response to configuring the anti-malware engine, to:

detect an action performed by the target process, the action comprising loading another executable module into the target process, the another executable module distinct from the main executable module and the shared library;

in response to detecting the action, re-evaluate the target process to determine whether the target process is likely to be malicious according to a third module reputation indicator of the another executable module, the third module reputation indicator received from the server; and

in response, re-configure the anti-malware engine according to a third set of monitoring rules indicated by the third module reputation indicator.

8. The client system of claim 1, wherein determining whether the target process is likely to be malicious comprises:

identifying all executable modules loaded by the target process;

determining whether each module of the all executable modules is likely to be malicious according to a module reputation indicator determined for an instance of the each module; and

in response, when each module of the all executable modules is not likely to be malicious, determining that the target process is not likely to be malicious.

9. The client system of claim 8, wherein determining whether the target process is likely to be malicious further comprises, in response to determining whether each module is likely to be malicious, when at least one module of the all executable modules is likely to be malicious, determining that the target process is likely to be malicious.

10. The client system of claim 1, wherein the at least one hardware processor is configured, in response to configuring the anti-malware engine, to:

determine whether the target process performs a malware-indicative action; and

when the target process performs the malware-indicative action,

identify a suspect module of the target process, the suspect module performing the malware-indicative action;

update a module reputation indicator of the suspect module to indicate that the suspect module is likely to be malicious; and

in response to updating the module reputation indicator of the suspect module,

re-configure the anti-malware engine to monitor the target process according to a strict security protocol, wherein the strict security protocol is more computationally expensive than the combined set of monitoring rules.

11. The client system of claim 10, wherein the at least one hardware processor is further configured, in response to updating the module reputation indicator of the suspect module, to transmit the updated module reputation indicator of the suspect module to the server.

12. The client system of claim 10, wherein the at least one hardware processor is further configured, in response to updating the module reputation indicator of the suspect module, to:

identify a second process executing on the client system, the second process comprising an instance of the suspect module; and

in response to identifying the second process, configure the anti-malware engine to monitor the second process according to the strict security protocol.

13. The client system of claim 1, wherein the at least one hardware processor is further configured, in response to configuring the anti-malware engine to:

determine whether the target process performs a malware-indicative action; and

when the target process performs the malware-indicative action, configure the anti-malware engine to employ a strict security protocol to monitor a second process executing on the client system, regardless of whether the second process is likely to be malicious.

14. A server comprising:

a memory, and

at least one hardware processor connected to the memory and configured to:

determine a first module reputation indicator of a main executable module and a second module reputation indicator of a shared library, the first module reputation indicator determined according to a behavior of an instance of the main executable module, wherein the first module reputation indicator comprises an indicator of a first set of monitoring rules, and wherein the second module reputation indicator comprises a second set of monitoring rules; and

in response to determining the first and second module reputation indicators, transmit the first and second module reputation indicators to a client system of a plurality of client systems configured to perform anti-malware transactions with the server,

wherein the client system is configured to execute an anti-malware engine configured to monitor a target process for malicious activity, wherein the target process comprises another instance of the main executable module and an instance of the shared library, and wherein the client system is further configured to:

determine whether the target process is likely to be malicious according to the first and second module reputation indicators;

in response to determining whether the target process is likely to be malicious, when the target process is not likely to be malicious,

combine the first and second sets of monitoring rules into a combined set of monitoring rules, and

configure the anti-malware engine to monitor the target process according to the combined set of monitoring rules.

15. The server of claim 14, wherein the client system is configured to determine the combined set of monitoring rules according to a union of the first and second sets of monitoring rules.

16. The server of claim 14, wherein the client system is configured to determine the combined set of monitoring rules according to an intersection of the first and second sets of monitoring rules.

17. The server of claim 14, wherein a selected rule of the first set of monitoring rules includes a selected heuristic employed to determine whether the target process is malicious.

18. The server of claim 14, wherein a selected rule of the first set of monitoring rules instructs the client system to determine whether the target process performs a selected action.

19. The server of claim 14, wherein the instance of the main executable module executes on a second client system of the plurality of client systems.

20. The server of claim 14, wherein the client system is further configured, in response to configuring the anti-malware engine, to:

detect an action of the target process, the action comprising loading another executable module into the target process, the another executable module distinct from the main executable module and the shared library;

in response to detecting the action, re-evaluate the target process to determine whether the target process is likely to be malicious according to a third module reputation indicator of the another executable module, the third module reputation indicator received from the server; and

in response, re-configure the anti-malware engine according to a third set of monitoring rules indicated by the third module reputation indicator.

21. The server of claim 14, wherein determining whether the target process is likely to be malicious comprises:

identifying all executable modules loaded by the target process;

determining whether each module of the all executable modules is likely to be malicious according to a module reputation indicator determined for an instance of the each module; and

in response, when each module of the all executable modules is not likely to be malicious, determining that the target process is not likely to be malicious.

22. The server of claim 21, wherein determining whether the target process is likely to be malicious further comprises, in response to determining whether each module is likely to be malicious, when at least one module of the all executable modules is likely to be malicious, determining that the target process is likely to be malicious.

23. The server of claim 14, wherein the client system is further configured, in response to configuring the anti-malware engine, to:

determine whether the target process performs a malware-indicative action; and

when the target process performs the malware-indicative action,

identify a suspect module of the target process, the suspect module performing the malware-indicative action;

update a module reputation indicator of the suspect module to indicate that the suspect module is likely to be malicious; and

in response to updating the module reputation indicator of the suspect module,

re-configure the anti-malware engine to monitor the target process according to a strict security protocol, wherein the strict security protocol is more computationally expensive than the combined set of monitoring rules.

24. The server of claim 23, further configured to receive the updated module reputation indicator of the suspect module from the client system.

25. The server of claim 23, wherein the client system is further configured, in response to updating the module reputation indicator of the suspect module, to:

identify a second process executing on the client system, the second process comprising an instance of the suspect module; and

in response to identifying the second process, configure the anti-malware engine to monitor the second process according to the strict security protocol.

26. The server of claim 14, wherein the client system is further configured, in response to configuring the anti-malware engine, to:

determine whether the target process performs a malware-indicative action; and

when the target process performs the malware-indicative action, configure the anti-malware engine to employ a strict security protocol to monitor a second process executing on the client system, regardless of whether the second process is likely to be malicious.

27. A non-transitory computer readable medium storing instructions which, when executed, configure at least one processor of a client system executing a target process, the target process comprising an instance of a main executable module and an instance of a shared library, to:

receive from a server a first module reputation indicator of the main executable module and a second module reputation indicator of the shared library, the first module reputation indicator determined according to a behavior of another instance of the main executable module, wherein the server is configured to perform anti-malware transactions with a plurality of client systems including the client system, wherein the first module reputation indicator comprises an indicator of a first set of monitoring rules, and wherein the second module reputation indicator comprises an indicator of a second set of monitoring rules;

in response to receiving the first and second module reputation indicators, determine whether the target process is likely to be malicious according to the first and second module reputation indicators; and

in response to determining whether the target process is likely to be malicious, when the target process is not likely to be malicious,

combine the first and second sets of monitoring rules into a combined set of monitoring rules, and

configure the anti-malware engine to monitor the target process according to the combined set of monitoring rules.

28. The client system of claim 1, wherein the at least one hardware processor is further configured, in response to determining whether the target process is likely to be malicious, when the target process is likely to be malicious, to configure the anti-malware engine to monitor the target process according to a strict security protocol, wherein the strict security protocol is more computationally expensive than the combined set of monitoring rules.

29. The server of claim 14, wherein the client system is further configured, in response to determining whether the target process is likely to be malicious, when the target process is likely to be malicious, to configure the anti-malware engine to monitor the target process according to a strict security protocol, wherein the strict security protocol is more computationally expensive than the combined set of monitoring rules.