

CLAIMS

1. A host system comprising at least one hardware processor and a memory unit, the at least one hardware processor configured to execute an entity manager and a heuristic engine, wherein:

the entity manager is configured to organize a collection of monitored executable software entities into a plurality of entity groups, wherein organizing the collection comprises:

in response to detecting that a first entity of the collection has spawned a child entity, determining whether the first entity belongs to a group creator category of entities;

in response to determining whether the first entity belongs to the group creator category, when the first entity belongs to the group creator category:

adding a new entity group to the plurality of entity groups, and assigning the child entity to the new entity group; and

in response to determining whether the first entity belongs to the group creator category, when the first entity does not belong to the group creator category:

selecting a first entity group from the plurality of entity groups so that the first entity is a member of the first entity group, and

assigning the child entity to the first entity group; and the heuristic engine is configured, in response to a first action performed by the child entity, to:

select a second entity group from the plurality of entity groups so that the child entity is a member of the second entity group, wherein the child entity is a member of the second entity group while also being a member of the first entity group or of the new entity group; and

in response to selecting the second entity group, determine whether the first action is indicative of a malware attack according to a second action performed by another member of the second entity group, wherein the at least one hardware processor is further configured, in response to the heuristic engine determining whether the first action is indicative of a malware attack, when the first action is indicative of the malware attack, to take an anti-malware action.

2. The host system of claim 1, wherein organizing the collection further comprises, in response to determining whether the first entity belongs to the group creator category, when the first entity does not belong to the group creator category: selecting a third entity group from the plurality of entity groups so that the first entity is a member of the third entity group, and assigning the child entity to the third entity group.

3. The host system of claim 1, wherein organizing the collection further comprises, in response to detecting that the child entity has injected code into a third entity of the collection:

selecting a third entity group from the plurality of entity groups so that the child entity is a member of the third entity group; and

in response, assigning the third entity to the third entity group.

4. The host system of claim 1, wherein organizing the collection further comprises, in response to detecting that the first entity has spawned the child entity:

determining whether the child entity belongs to the group creator category; and

in response, when the child entity belongs to the group creator category, remove the child entity from the group creator category.

5. The host system of claim 1, wherein determining whether the first entity belongs to the group creator category comprises determining whether the first entity is a component of a web browser executing on the host system.

6. The host system of claim 1, wherein determining whether the first entity belongs to the group creator category comprises determining whether the first entity is a component of an operating system executing on the host system.

7. The host system of claim 1, wherein determining whether the first action is indicative of the malware attack comprises determining whether the first action has occurred before the second action.

8. The host system of claim 1, wherein the heuristic engine is configured to determine whether the first action is indicative of the malware attack further according to a third action performed by a third entity of the second entity group.

9. The host system of claim 1, wherein determining whether the first action is indicative of the malware attack comprises determining whether the first action is part of a malware-indicative set of actions, wherein all actions of the malware-indicative set of actions are performed by members of the second entity group.

10. The host system of claim 9, wherein determining whether the first action is part of the malware-indicative set of actions comprises determining whether a subset of the malware-indicative set of actions occurred in a specific order.

11. The host system of claim 1, wherein the anti-malware action comprises terminating a plurality of members of the second entity group.

12. The host system of claim 11, wherein the plurality of members comprises all members of the second entity group.

13. The host system of claim 1, wherein the anti-malware action comprises undoing a set of changes caused to the host system by execution of members of the second entity group.

14. A method comprising:

employing at least one hardware processor of a host system to organize a collection of monitored executable software entities into a plurality of entity groups, wherein organizing the collection comprises:

in response to detecting that a first entity of the collection has spawned a child entity, determining whether the first entity belongs to a group creator category of entities;

in response to determining whether the first entity belongs to the group creator category, when the first entity belongs to the group creator category:

adding a new entity group to the plurality of entity groups, and assigning the child entity to the new entity group; and

in response to determining whether the first entity belongs to the group creator category, when the first entity does not belong to the group creator category:

selecting a first entity group from the plurality of entity groups so that the first entity is a member of the first entity group, and assigning the child entity to the first entity group;

in response to a first action performed by the child entity, employing at least one hardware processor of the host system to select a second entity group from the plurality of entity groups so that the child entity is a member of the second entity group, wherein the child entity is a member of the second entity group while also being a member of the first entity group or of the new entity group;

in response to selecting the second entity group, employing at least one hardware processor of the host system to determine whether the first action is indicative of a malware attack according to a second action performed by another member of the second entity group; and

in response to determining whether the first action is indicative of a malware attack, when the first action is indicative of the malware attack, employing at least one hardware processor of the host system to take an anti-malware action.

15. The method of claim 14, wherein organizing the collection further comprises, in response to determining whether the first entity belongs to the group creator category, when the first entity does not belong to the group creator category: selecting a third entity group from the plurality of entity groups so that the first entity is a member of the third entity group, and assigning the child entity to the third entity group.

16. The method of claim 14, wherein organizing the collection further comprises, in response to detecting that the child entity has injected code into a third entity of the collection: selecting a third entity group from the plurality of entity groups so that the child entity is a member of the third entity group; and in response, assigning the third entity to the third entity group.

17. The method of claim 14, wherein organizing the collection further comprises, in response to detecting that the first entity has spawned the child entity: determining whether the child entity belongs to the group creator category; and in response, when the child entity belongs to the group creator category, remove the child entity from the group creator category.

18. The method of claim 14, wherein determining whether the first entity belongs to the group creator category comprises determining whether the first entity is a component of a web browser executing on the host system.

19. The method of claim 14, wherein determining whether the first entity belongs to the group creator category comprises determining whether the first entity is a component of an operating system executing on the host system.

20. The method of claim 14, wherein determining whether the first action is indicative of the malware attack comprises determining whether the first action has occurred before the second action.

21. The method of claim 14, further comprising determining whether the first action is indicative of the malware attack according to a third action performed by a third entity of the second entity group.

22. The method of claim 14, wherein determining whether the first action is indicative of the malware attack comprises determining whether the first action is part of a malware-indicative set of actions, wherein all actions of the malware-indicative set of actions are performed by members of the second entity group.

23. The method of claim 22, wherein determining whether the first action is part of the malware-indicative set of actions comprises determining whether a subset of the malware-indicative set of actions occur in a specific order.

24. The method of claim 14, wherein the anti-malware action comprises terminating a plurality of members of the second entity group.

25. The method of claim 24, wherein the plurality of members comprises all members of the second entity group.

26. The method of claim 14, wherein the anti-malware action comprises undoing a set of changes caused to the host system by execution of members of the second entity group.

27. A non-transitory computer-readable medium storing instructions which, when executed by at least one hardware processor of a host system, cause the host system to form an entity manager and a heuristic engine, wherein:

the entity manager is configured to organize a collection of monitored executable software entities into a plurality of entity groups, wherein organizing the collection comprises:

in response to detecting that a first entity of the collection has spawned a child entity, determining whether the first entity belongs to a group creator category of entities;

in response to determining whether the first entity belongs to the group creator category, when the first entity belongs to the group creator category: adding a new entity group to the plurality of entity groups, and assigning the child entity to the new entity group; and

in response to determining whether the first entity belongs to the group creator category, when the first entity does not belong to the group creator category:

selecting a first entity group from the plurality of entity groups so that the first entity is a member of the first entity group, and

assigning the child entity to the first entity group; and

the heuristic engine is configured, in response to a first action performed by the child entity, to:

select a second entity group from the plurality of entity groups so that the child entity is a member of the second entity group, wherein the child entity is a member of the second entity group while also being a member of the first entity group or of the new entity group; and

in response to selecting the second entity group, determine whether the first action is indicative of a malware attack according to a second action performed by another member of the second entity group,

wherein the instructions further cause the host system, in response to determining whether the first action is indicative of a malware attack, when the first action is indicative of the malware attack, to take an anti-malware action.

28. The host system of claim 1, wherein the heuristic engine is further configured, in response to the entity manager assigning the child entity to the first group, and in response to the first action, to determine whether the first action is indicative of the malware attack according to a third action performed by yet another member of the first entity group.

29. The method of claim 14, further comprising, in response to assigning the child entity to the first group, and in response to the first action, employing at least one hardware processor of the host system to determine whether the first action is indicative of the malware attack according to a third action performed by yet another member of the first entity group.

30. The host system of claim 1, wherein organizing the collection further comprises, in response to assigning the child entity to the first entity group, and in response to detecting that the child entity has injected code into a third entity of the collection, assigning the third entity to the first entity group.

31. The method of claim 14, further comprising, in response to assigning the child entity to the first entity group, and in response to detecting that the child entity has injected code into a third entity of the collection, assigning the third entity to the first entity group.