

CLAIMS

1. A host system comprising a memory unit storing instructions which, when executed by at least one hardware processor of the host system, cause the host system to form an entity management module, an entity evaluator, and a scoring engine, wherein:

the entity management module is configured to manage a collection of evaluated software entities, wherein managing the collection comprises:

identifying a set of descendant entities of a first entity of the collection;
determining whether the first entity is terminated;

in response, when the first entity is terminated, determining whether all members of the set of descendant entities are terminated; and

in response, when all members of the set of descendant entities are terminated, removing the first entity from the collection;

the entity evaluator is configured to:

evaluate the first entity according to an evaluation criterion; and

in response, when the first entity satisfies the evaluation criterion, transmit an evaluation indicator to the scoring engine; and

the scoring engine is configured to:

record a first score determined for the first entity and a second score determined for a second entity of the collection, the first and second scores determined according to the evaluation criterion;

in response to recording the first and second scores, and in response to receiving the evaluation indicator, update the second score according to the evaluation indicator;

in response, determine whether the second entity is malicious according to the updated second score;

in response to receiving the evaluation indicator, update the first score according to the evaluation indicator; and

in response, determine whether the first entity is malicious according to the updated first score.

- 5 2. The host system of claim 1, wherein the first entity is a child of the second entity.
3. The host system of claim 1, wherein the second entity is a child of the first entity.
4. The host system of claim 1, wherein the first entity comprises a section of code injected by the second entity.
- 10 5. The host system of claim 1, wherein the second entity comprises a section of code injected by the first entity.
6. The host system of claim 1, wherein updating the second score comprises changing the second score by an amount determined according to $w \cdot S$, wherein S is the first score, and wherein w is a numerical weight.
7. The host system of claim 1, wherein managing the collection of evaluated software entities further comprises:
- 15

intercepting a launch of a new software entity; and

in response, adding the new software entity to the collection.

8. A non-transitory computer-readable medium storing instructions, which, when executed, configure at least one processor of a host system to:
- 20 manage a collection of evaluated software entities, wherein managing the collection comprises:

identifying a set of descendant entities of a first entity of the collection; determining whether the first entity is terminated;

- 25 in response, when the first entity is terminated, determining whether all members of the set of descendant entities are terminated; and

in response, when all members of the set of descendant entities are terminated, removing the first entity from the collection;

record a first score determined for the first entity and a second score determined for a second entity of the collection, the first and second scores determined according to an evaluation criterion;

in response to recording the first and second scores, evaluate the first entity according to the evaluation criterion;

in response to evaluating the first entity, when the first entity satisfies the evaluation criterion, update the second score;

in response to updating the second score, determine whether the second entity is malicious according to the updated second score;

in response to evaluating the first entity, when the first entity satisfies the evaluation criterion, update the first score; and

in response, determine whether the first entity is malicious according to the updated first score.

9. The computer-readable medium of claim 8, wherein the first entity is a child of the second entity.

10. The computer-readable medium of claim 8, wherein the second entity is a child of the first entity.

11. The computer-readable medium of claim 8, wherein the first entity comprises a section of code injected by the second entity.

12. The computer-readable medium of claim 8, wherein the second entity comprises a section of code injected by the first entity.

13. The computer-readable medium of claim 8, wherein updating the second score comprises changing the second score by an amount determined according to $w \cdot S$, wherein S is the first score, and wherein w is a numerical weight.

14. The computer-readable medium of claim 8, wherein managing the collection of evaluated software entities further comprises:

intercepting a launch of a new software entity; and

in response, adding the new software entity to the collection.

- 5 15. A method comprising employing at least one processor of a host system to:

manage a collection of evaluated software entities, wherein managing the collection comprises:

identifying a set of descendant entities of a first entity of the collection;
determining whether the first entity is terminated;

10 in response, when the first entity is terminated, determining whether all members of the set of descendant entities are terminated; and

in response, when all members of the set of descendant entities are terminated, removing the first entity from the collection;

15 record a first score determined for the first entity and a second score determined for a second entity of the collection, the first and second scores determined according to an evaluation criterion;

in response to recording the first and second scores, evaluate the first entity according to the evaluation criterion;

20 in response to evaluating the first entity, when the first entity satisfies the evaluation criterion, update the second score;

in response to updating the second score, determine whether the second entity is malicious according to the updated second score;

in response to evaluating the first entity, when the first entity satisfies the evaluation criterion, update the first score; and

25 in response, determine whether the first executable entity is malicious according to the updated first score.