

Claims

1. An agent comprising:

a monitor module, executing on a computing device, configured to monitor ~~a the~~ computing device for an instruction to execute a legitimate application on the computing device, the legitimate application comprising a non-malware application;

an application identification module configured to identify one or more attributes of the legitimate application;

a vulnerability module configured to retrieve risk information based on the one or more attributes of the legitimate application, the risk information determined from known vulnerabilities of the legitimate application, the risk information including a risk value associated with the legitimate application;

a rules database for storing a rule associated with the risk information; and

a rule module configured to retrieve the rule from the ~~rule~~ rules database based on the risk information and to control the legitimate application based on a comparison of the risk value and a predetermined threshold risk value defined by the rule.

2. The agent of claim 1, wherein the rule module configured to control the legitimate application ~~based on the rule~~ comprises blocking the legitimate application from executing ~~based on the rule~~.

3. The agent of claim 1, wherein the rule module configured to control the legitimate application ~~based on the rule~~ comprises allowing the legitimate application to execute ~~based on the rule~~.

4. The agent of claim 1, wherein the rule module configured to control the legitimate application ~~based on the rule~~ comprises allowing the legitimate application to execute ~~based on the rule~~ but blocking some functionality of the legitimate application from executing ~~based on the rule~~.

5. The agent of claim 1, wherein the monitor module configured to monitor the computing device for an instruction to execute the legitimate application comprises the monitor module intercepting instructions being provided to or from an operating system of the computing device.

6. The agent of claim 1, wherein ~~the attribute~~ one of the one or more attributes is an application identifier.
7. The agent of claim 1, wherein ~~the attribute~~ one of the one or more attributes is an application version identifier.
8. The agent of claim 1, wherein the rule comprises an instruction to block all or part of ~~the~~ execution of the legitimate application if the risk information indicates, at least in part, that a vulnerability associated with the legitimate application was publicly disclosed before a predetermined date.
9. The agent of claim 8, wherein the predetermined date is calculated as occurring at a period of time before a current date.
10. The agent of claim 1, wherein the rule comprises an instruction to block all or part of ~~the~~ execution of the legitimate application if the risk information indicates, at least in part, that a public exploit of a vulnerability associated with the legitimate application exists.
11. The agent of claim 1, wherein the rule comprises an instruction to block all or part of ~~the~~ execution of the legitimate application if the risk information indicates, at least in part, that a vulnerability associated with the legitimate application was identified before a predetermined period of time.
12. The agent of claim 1, wherein the rule is applicable to multiple different legitimate applications on the computing device.
13. The agent of claim 1, wherein the rule module is configured to retrieve a plurality of rules from the rule database, each of the plurality of rules associated with the risk information.
14. The agent of claim 13, wherein the rule module configured to control the legitimate application based on the comparison of the risk value and the predetermined threshold risk value defined by the rule comprises controlling the legitimate application based on the comparison of the risk value and the predetermined threshold risk value defined by a strictest rule of the plurality of rules.
15. The agent of claim 1, wherein the risk information comprises a risk value and the rule comprises instructions regarding control of the legitimate application based on the risk value.

16. A method comprising:
- monitoring, via a processor, a computing device for an instruction to execute a legitimate application on the computing device, the legitimate application comprising a non-malware application;
 - identifying one or more attributes of the legitimate application;
 - retrieving risk information based on the one or more attributes of the legitimate application, the risk information determined from known vulnerabilities of the legitimate application, the risk information including a risk value associated with the legitimate application;
 - storing a rule associated with the risk information;
 - retrieving the rule from the rule database based on the risk information; and
 - controlling the legitimate application based on a comparison of the risk value and a predetermined threshold risk value defined by the rule.
17. The method of claim 16, wherein controlling the legitimate application ~~based on the rule~~ comprises blocking the legitimate application from executing ~~based on the rule~~.
18. The method of claim 16, wherein the controlling the legitimate ~~the legitimate~~ application ~~based on the rule~~ comprises allowing the legitimate application to execute ~~based on the rule~~.
19. The method of claim 16, wherein the controlling the legitimate ~~the legitimate~~ application ~~based on the rule~~ comprises allowing the legitimate application to execute ~~based on the rule~~ but blocking some functionality of the legitimate application from executing ~~based on the rule~~.
20. The method of claim 16, wherein the monitoring the computing device for an instruction to execute the legitimate application comprises intercepting instructions being provided to or from an operating system of the computing device.
21. The method of claim 16, wherein ~~the attribute~~ one of the one or more attributes is an application identifier.
22. The method of claim 16, wherein ~~the attribute~~ one of the one or more attributes is an application version identifier.
23. The method of claim 16, wherein the rule comprises an instruction to block all or part of ~~the~~ execution of the legitimate application if the risk information indicates, at least in part, that

a vulnerability associated with the legitimate application was publicly disclosed before a predetermined date.

24. The method of claim 23, wherein the predetermined date is calculated as occurring at a period of time before a current date.

25. The method of claim 16, wherein the rule comprises an instruction to block all or part of ~~the~~ execution of the legitimate application if the risk information indicates, at least in part, that a public exploit of a vulnerability associated with the legitimate application exists.

26. The method of claim 16, wherein the rule comprises an instruction to block all or part of ~~the~~ execution of the legitimate application if the risk information indicates, at least in part, that a vulnerability associated with the legitimate application was identified before a predetermined period of time.

27. The method of claim 16, wherein the rule is applicable to multiple different legitimate applications on the computing device.

28. The method of claim 16, wherein retrieving the rule comprises retrieving a plurality of rules from the rule database, each of the plurality of rules associated with the risk information.

29. The method of claim 28, wherein controlling the legitimate application based on the comparison of the risk value and the predetermined threshold risk value defined by the rule comprises controlling the legitimate application based on the comparison of the risk value and the predetermined threshold risk value defined by a strictest rule of the plurality of rules.

30. The method of claim 16, wherein the risk information comprises a risk value and the rule comprises instructions regarding control of the legitimate application based on the risk value.

31. A non-transitory computer readable medium comprising instructions executable by a processor to perform a method, the method comprising:

monitoring a computing device for an instruction to execute a legitimate application on the computing device, the legitimate application comprising a non-malware application;

identifying one or more attributes of the legitimate application;

retrieving risk information based on the one or more attributes of the legitimate application, the risk information determined from known vulnerabilities of the legitimate

application, the risk information including a risk value associated with the legitimate application;

storing a rule associated with the risk information;

retrieving the rule from the rule database based on the risk information; and

_____controlling the legitimate application based on a comparison of the risk value and a predetermined threshold risk value defined by the rule.