CLAIMS

What is claimed is:

1. A method comprising:

determining, in a computer, an area where an undesired computer program will reside; and

providing a data object in the area, so that the data object is an antibody that provides security to the computer and immunity against the undesired program.

2. The method of claim 1, further comprising:

providing a null configuration object in a second area in the computer, wherein the null configuration object is associated with the data object.

3. The method of claim 2, wherein the null configuration object comprises a null registry key.

4. The method of claim 2, wherein the null configuration object comprises a null configuration information.

5. The method of claim 1, further comprising:

preventing the deletion or modification of the data object.

6. The method of claim 5, wherein preventing the deletion or modification of the data object comprises:

setting a security permission for the data object.

7. The method of claim 5, wherein preventing the deletion or modification of the data object comprises:

modifying the data object to an object type that differs from the undesired program.

8. The method of claim 7, wherein preventing the deletion or modification of the data object comprises:

placing a second data object in the data object type.

9. The method of claim 1, further comprising:

generating a security event in response to an access of the data object.

10. The method of claim 2, further comprising:

generating a security event in response to an access of the null configuration object.

11. An apparatus comprising:

an inoculator engine configured to determine, in a computer, an area where an undesired computer program will reside and provide a data object in the area, so that the data object is an antibody that provides security to the computer and immunity against the undesired program.

12. The apparatus of claim 11, wherein the inoculator engine is configured to provide a null configuration object in a second area in the computer, wherein the null configuration object is associated with the data object.

13. The apparatus of claim 12, wherein the null configuration object comprises a null registry key.

14. The apparatus of claim 12, wherein the null configuration object comprises a null configuration information.

15. The apparatus of claim 11, further comprising a security subsystem configured to prevent the deletion or modification of the data object.

16. The apparatus of claim 15, wherein the security subsystem prevents the deletion or modification of the data object by setting a security permission for the data object.

17. The apparatus of claim 15, wherein the security subsystem prevents the deletion or modification of the data object by modifying the data object to an object type that differs from the undesired program.

18. The apparatus of claim 17, wherein the security subsystem prevents the deletion or modification of the data object by placing a second data object in the data object type.

19. The apparatus of claim 11, further comprising:

a security subsystem configured to generate a security event in response to an access of the data object.

20. The apparatus of claim 12, further comprising:

a security subsystem configured to generate a security event in response to an access of the null configuration object.

21. An apparatus comprising:

means for determining, in a computer, an area where an undesired computer program will reside; and

means for providing a data object in the area, so that the data object is an antibody that provides security to the computer and immunity against the undesired program.

22. An article of manufacture, comprising:

a computer-readable medium having stored thereon instructions to:

determine, in a computer, an area where an undesired computer program will reside; and

provide a data object in the area, so that the data object is an antibody that provides security to the computer and immunity against the undesired program.

Claims:

1. An invention not claimed in any divisional application.