CLAIMS

1. A security appliance configured to protect a client device against computer security threats, the security appliance comprising at least one hardware processor configured to:

detect a first wireless communication comprising an availability notification emitted in preparation for establishing a peer-to-peer connection with an administration device;

in response to detecting the first wireless communication, determine whether the first wireless communication fits a notification pattern specific to the client device, the notification pattern comprising a pattern of hopping between a carrier signal frequency bands;

in response, when the first wireless communication does not fit the notification pattern, transmit a second wireless communication configured to mimic a response by the administration device to the first wireless communication; and

in response to transmitting the second wireless communication, perform a security action to protect the client device or the administration device.

2. The security appliance of claim 1, wherein the at least one hardware processor is configured to determine whether the first wireless communication fits the notification pattern according to a time interval separating the first wireless communication from a previously-detected wireless communication comprising another availability notification emitted by the client device.

3. The security appliance of claim 2, wherein the at least one hardware processor is configured to:

compare a difference between a size of the time interval and a reference interval size characteristic of the client device to a pre-determined threshold; and

in response, determine whether the first wireless communication fits the notification pattern according to a result of the comparison.

4. The security appliance of claim 1, wherein the at least one hardware processor is configured to determine whether the first wireless communication fits the notification pattern according to a notification frequency specific to the client device, the notification frequency determined according to a count of availability notifications emitted by the client device within a pre-determined time interval.

5. The security appliance of claim 1, wherein the at least one hardware processor is configured to determine whether the first wireless communication fits the notification pattern according to an indicator of a signal-to-noise ratio of a carrier signal of the first wireless communication.

6. The security appliance of claim 1, wherein the at least one hardware processor is configured to determine whether the first wireless communication fits the pattern of hopping according to a frequency of a carrier signal of the first wireless communication and further according to another frequency of another carrier signal of another availability notification detected by the security appliance.

7. The security appliance of claim 1, wherein the at least one hardware processor is further configured, in preparation for determining whether the first wireless communication fits the notification pattern, to:
detect a plurality of availability notifications emitted by the client device; and
in response, determine the notification pattern according to the plurality of availability notifications.

8. The security appliance of claim 1, wherein mimicking the response by the administration device comprises initiating another peer-to-peer connection with a sender of the first wireless communication while impersonating the administration device.

9. The security appliance of claim 8, wherein the security action comprises maintaining the other peer-to-peer connection active for a pre-determined amount of time.

10. The security appliance of claim 8, wherein the security action comprises transmitting a set of surrogate data to the sender of the first wireless communication over the other peer-to-peer connection.

11. The security appliance of claim 8, wherein impersonating the administration device comprises configuring the second wireless communication to include an identifier of the administration device.

12. A method of protecting a client device against computer security threats, the method comprising employing at least one hardware processor of a security appliance to:
detect a first wireless communication comprising an availability notification emitted in preparation for establishing a peer-to-peer connection with an administration device;
in response to detecting the first wireless communication , determine whether the first wireless communication fits a notification pattern specific to the client device, the notification pattern comprising a pattern of hopping between a carrier signal frequency bands;
in response, when the first wireless communication does not fit the notification pattern, transmit a second wireless communication configured to mimic a response by the administration device to the first wireless communication; and
in response to transmitting the second wireless communication, perform a security action to protect the client device or the administration device.

13. The method of claim 12, comprising employing the at least one hardware processor to determine whether the first wireless communication fits the notification pattern according to a time interval separating the first wireless communication from a previously-detected wireless communication comprising another availability notification emitted by the client device.

14. The method of claim 13, further comprising employing the at least one hardware processor to:
compare a difference between a size of the time interval and a reference interval size characteristic of the client device to a pre-determined threshold; and
in response, determine whether the first wireless communication fits the notification pattern according to a result of the comparison.

15. The method of claim 12, comprising employing the at least one hardware processor to determine whether the first wireless communication fits the notification pattern according to a notification frequency specific to the client device, the notification frequency determined according to a count of availability notifications emitted by the client device during a pre-determined time interval.

16. The method of claim 12, comprising employing the at least one hardware processor to determine whether the first wireless communication fits the notification pattern according to an indicator of a signal-to-noise ratio of a carrier signal of the first wireless communication.

17. The method of claim 12, comprising employing the at least one hardware processor to determine whether the first wireless communication fits the pattern of hopping according to a frequency of a carrier signal of the first wireless communication and further according to another frequency of another carrier signal of another availability notification detected by the security appliance.

18. The method of claim 12, further comprising employing the at least one hardware processor, in preparation for determining whether the first wireless communication fits the notification pattern, to:
detect a plurality of availability notifications emitted by the client device; and
in response, determine the notification pattern according to the plurality of availability notifications.

19. The method of claim 12, wherein mimicking the response by the administration device comprises initiating another peer-to-peer connection with a sender of the first wireless communication while impersonating the administration device.

20. The method of claim 19, wherein the security action comprises maintaining the other peer-to-peer connection active for a pre-determined amount of time.

21. The method of claim 19, wherein the security action comprises transmitting a set of surrogate data to the sender of the first wireless communication over the other peer-to-peer connection.

22. The method of claim 19, wherein impersonating the administration device comprises configuring the second wireless communication to include an identifier of the administration device.

23. A non-transitory computer-readable medium storing instructions which, when executed by at least one hardware processor of a security appliance, cause the security appliance to:

detect a first wireless communication comprising an availability notification emitted in preparation for establishing a peer-to-peer connection with an administration device;

in response to detecting the first wireless communication , determine whether the first wireless communication fits a notification pattern specific to a selected client device, the notification pattern comprising a pattern of hopping between carrier signal frequency bands;

in response, when the first wireless communication does not fit the notification pattern, transmit a second wireless communication configured to mimic a response by the administration device to the first wireless communication; and

in response to transmitting the second wireless communication, perform a security action to protect the client device or the administration device.