CLAIMS:

1. A method for disrupting an information security attack on a computing device in a computer network, the method comprising:

receiving a first alert and a second alert from a monitoring device linked to the computing device, wherein the first alert and the second alert both include an Internet Protocol address of a source that initiated the information security attack on the computing device and only an identity of an intermediate upstream gateway of the computer network through which the attack passed, whereby the attack on the computing device passed through the intermediate upstream gateway and at least one other gateway in the computer network;

determining if the Internet Protocol address of the source that initiated the information security attack on the computing device is to be disrupted;

if the Internet Protocol address of the source that initiated the information security attack on the computing device is to be disrupted, generating a first set of instructions and transmitting the first set of instructions to the intermediate upstream gateway, wherein the first set of instructions instruct the intermediate upstream gateway to add the IP address of the source that initiated the information security attack to an access control list of the intermediate upstream gateway;

generating a second set of instructions and transmitting the second set of instructions to the intermediate upstream gateway after a first period of time has lapsed, wherein the second set of instructions instruct the intermediate upstream gateway to remove the IP address of the source that initiated the information security attack from the access control list of the intermediate upstream gateway;

determining, during the first period of time, if a new mitigation action is to be created to address the first alert and the second alert based on a security alert database; and

if the new mitigation action is to be created to address the first alert and the second alert, transmitting the first alert and the second alert to a command centre.

2. The method of claim 1 wherein the transmitting of the first set of instructions to the intermediate upstream gateway of the computer network comprises:

determining if the first set of instructions can be transmitted to the intermediate upstream gateway of the computer network using a telecommunication network; and

if it is determined that the first set of instructions cannot be transmitted using the telecommunication network, transmitting the first set of instructions to the intermediate upstream gateway of the computer network using an out-of-band network.

3. The method of claim 1 wherein the generating of the first set of instructions comprises:

using the identity of the intermediate upstream gateway to select an associated instruction set from a intermediate upstream gateway brand and model database; and

compiling the first set of instructions using the selected instruction set.

4. The method of claim 1 wherein the transmitting of the second set of instructions to the intermediate upstream gateway of the computer network comprises:

determining if the second set of instructions can be transmitted to the intermediate upstream gateway of the computer network using a telecommunication network; and

if it is determined that the second set of instructions cannot be transmitted using the telecommunication network, transmitting the second set of instructions to the intermediate upstream gateway of the computer network using an out-of-band network.

5. The method of claim 1 wherein the generating of the second set of instructions comprises:

using the identity of the intermediate upstream gateway to select an associated instruction set from a intermediate upstream gateway brand and model database; and

compiling the second set of instructions using the selected instruction set.

6. The method of claim 1 wherein the intermediate upstream gateway comprises a network node on the computer network that is located upstream of the monitoring device and the at least one other gateway in the computer network.

7. The method of claim 1 wherein the intermediate upstream gateway comprises:

a first network node on the computer network and a second network node on the computer network wherein the second network node is located upstream of the first network node, and the first network node is located upstream of the monitoring device.

8. The method of claim 1 wherein the transmitting the first alert and the second alert to the command centre comprises:

determining if the first alert and the second alert can be transmitted to the command centre directly using a telecommunication network; and

if it is determined that the first alert and the second alert cannot be transmitted directly using the telecommunication network, transmitting the first alert and the second

alert to the intermediate upstream gateway of the computer network using an out-of-band network, wherein the first alert and second alert is then transmitted from the intermediate upstream gateway to the command centre using the telecommunication network.

9. The method of claim 1 wherein the determining if the Internet Protocol address of the source that initiated the information security attack on the computing device is to be disrupted comprises:

determining if the first alert correlates with the second alert; and

if the first alert correlates with the second alert, confirming that the Internet Protocol address of the source that initiated the information security attack is to be disrupted.

10. A method for disrupting an information security attack on a computing device in a computer network, the method comprising:

receiving an alert from a monitoring device linked to the computing device, wherein the alert includes an Internet Protocol address of a source that initiated the information security attack on the computing device and only an identity of an intermediate upstream gateway of the computer network through which the attack passed, whereby the attack on the computing device passed through the intermediate upstream gateway and at least one other gateway in the computer network;

generating a first set of instructions and transmitting the first set of instructions to the intermediate upstream gateway, wherein the first set of instructions instruct the intermediate upstream gateway to add the IP address of the source that initiated the information security attack to an access control list of the intermediate upstream gateway;

generating a second set of instructions and transmitting the second set of instructions to the intermediate upstream gateway after a first period of time has lapsed, wherein the second set of instructions instruct the intermediate upstream gateway to remove the IP address of the source that initiated the information security attack from the access control list of the intermediate upstream gateway;

determining, during the first period of time, if a new mitigation action is to be created to address the alert based on a security alert database; and

if the new mitigation action is to be created to address the alert, transmitting the alert to a command centre.

11. A system for disrupting an information security attack on a computing device in a computer network comprising:

a processing unit; and

a non-transitory media readable by the processing unit, the media storing instructions that when executed by the processing unit, cause the processing unit to:

receive a first alert and a second alert from a monitoring device linked to the computing device, wherein the first alert and the second alert both include an Internet Protocol address of a source that initiated the information security attack on the computing device and only an identity of an intermediate upstream gateway of the computer network through which the attack passed, whereby the attack on the computing device passed through the intermediate upstream gateway and at least one other gateway in the computer network;

determine if the Internet Protocol address of the source that initiated the information security attack on the computing device is to be disrupted;

if the Internet Protocol address of the source that initiated the information security attack on the computing device is to be disrupted, to generate a first set of instructions and to transmit the first set of instructions to the intermediate upstream gateway, wherein the first set of instructions instruct the intermediate upstream gateway to add the IP address of the source that initiated the information security attack to an access control list of the intermediate upstream gateway;

generate a second set of instructions and to transmit the second set of instructions to the intermediate upstream gateway after a first period of time has lapsed, wherein the second set of instructions instruct the intermediate upstream gateway to remove the IP address of the source that initiated the information security attack from the access control list of the intermediate upstream gateway;

determine, during the first period of time, if a new mitigation action is to be created to address the first alert and the second alert based on a security alert database; and

if the new mitigation action is to be created to address the first alert and the second alert, to transmit the first alert and the second alert to a command centre.

12. The system of claim 11 wherein the instruction to transmit the first set of instructions to the intermediate upstream gateway of the computer network comprises:

instructions for directing the processing unit to:

determine if the first set of instructions can be transmitted to the intermediate upstream gateway of the computer network using a telecommunication network; and

if it is determined that the first set of instructions cannot be transmitted using the telecommunication network, to transmit the first set of instructions to the intermediate upstream gateway of the computer network using an out-of-band network.

13. The system of claim 11 wherein the instructions to generate the first set of instructions comprises:

instructions for directing the processing unit to:

use the identity of the intermediate upstream gateway to select an associated instruction set from a intermediate upstream gateway brand and model database; and

compile the first set of instructions using the selected instruction set.

14. The system of claim 11 wherein the instructions to transmit the second set of instructions to the intermediate upstream gateway of the computer network comprises:

instructions for directing the processing unit to:

determine if the second set of instructions can be transmitted to the intermediate upstream gateway of the computer network using a telecommunication network; and

if it is determined that the second set of instructions cannot be transmitted using the telecommunication network, to transmit the second set of instructions to the intermediate upstream gateway of the computer network using an out-of-band network.

15. The system of claim 11 wherein the instructions to generate the second set of instructions comprises:

instructions for directing the processing unit to:

use the identity of the intermediate upstream gateway to select an associated instruction set from a intermediate upstream gateway brand and model database; and

compile the second set of instructions using the selected instruction set.

16. The system of claim 11 wherein the intermediate upstream gateway comprises a network node on the computer network that is located upstream of the monitoring device and the at least one other gateway in the computer network.

17. The system of claim 11 wherein the intermediate upstream gateway comprises:

a first network node on the computer network and a second network node on the computer network wherein the second network node is located upstream of the first network node, and the first network node is located upstream of the monitoring device.

18. The system of claim 11 wherein the instructions to transmit the first alert and the second alert to the command centre comprises:

instructions for directing the processing unit to:

determine if the first alert and the second alert can be transmitted to the command centre directly using a telecommunication network; and

if it is determined that the first alert and the second alert cannot be transmitted directly using the telecommunication network, to transmit the first alert and the second alert to the intermediate upstream gateway of the computer network using an out-of-band network, wherein the first alert and second alert is then transmitted from the intermediate upstream gateway to the command centre using the telecommunication network.

19. The system of claim 11 wherein the instructions to determine if the Internet Protocol address of the source that initiated the information security attack on the computing device is to be disrupted comprises:

instructions for directing the processing unit to:

determine if the first alert correlates with the second alert; and

if the first alert correlates with the second alert, to confirm that the Internet Protocol address of the source that initiated the information security attack is to be disrupted.

20. A system for disrupting an information security attack on a computing device in a computer network comprising:

a processing unit; and

a non-transitory media readable by the processing unit, the media storing instructions that when executed by the processing unit, cause the processing unit to:

receive an alert from a monitoring device linked to the computing device, wherein the alert includes an Internet Protocol address of a source that initiated the information security attack on the computing device and only an identity of an intermediate upstream gateway of the computer network through which the attack passed, whereby the attack on the computing device passed through the

intermediate upstream gateway and at least one other gateway in the computer network;

generate a first set of instructions and transmit the first set of instructions to the intermediate upstream gateway, wherein the first set of instructions instruct the intermediate upstream gateway to add the IP address of the source that initiated the information security attack to an access control list of the intermediate upstream gateway;

generate a second set of instructions and transmit the second set of instructions to the intermediate upstream gateway after a first period of time has lapsed, wherein the second set of instructions instruct the intermediate upstream gateway to remove the IP address of the source that initiated the information security attack from the access control list of the intermediate upstream gateway;

determine, during the first period of time, if a new mitigation action is to be created to address the alert based on a security alert database; and

if the new mitigation action is to be created to address the alert, to transmit the alert to a command centre.

21. A system for disrupting an information security attack on a computing device in a computer network comprising:

circuitry configured to receive a first alert and a second alert from a monitoring device linked to the computing device, wherein the first alert and the second alert both include an Internet Protocol address of a source that initiated the information security attack on the computing device and only an identity of an intermediate upstream gateway of the computer network through which the attack passed, whereby the attack on the computing device passed through the intermediate upstream gateway and at least one other gateway in the computer network;

circuitry configured to determine if the Internet Protocol address of the source that initiated the information security attack on the computing device is to be disrupted;

circuitry configured to generate a first set of instructions and to transmit the first set of instructions to the intermediate upstream gateway, if it is determined that the Internet Protocol address of the source that initiated the information security attack on the computing device is to be disrupted, wherein the first set of instructions instruct the intermediate upstream gateway to add the IP address of the source that initiated the information security attack to an access control list of the intermediate upstream gateway;

circuitry configured to generate a second set of instructions and to transmit the second set of instructions to the intermediate upstream gateway after a first period of time has lapsed, wherein the second set of instructions instruct the intermediate

upstream gateway to remove the IP address of the source that initiated the information security attack from the access control list of the intermediate upstream gateway;

circuitry configured to determine, during the first period of time, if a new mitigation action is to be created to address the first alert and the second alert based on a security alert database; and

circuitry configured to transmit the first alert and the second alert to a command centre, if it is determined that the new mitigation action is to be created to address the first alert and the second alert.

22. The system of claim 21 wherein the circuitry configured to transmit the first set of instructions to the intermediate upstream gateway of the computer network comprises:

circuitry configured to determine if the first set of instructions can be transmitted to the intermediate upstream gateway of the computer network using a telecommunication network; and

circuitry configured to transmit the first set of instructions to the intermediate upstream gateway of the computer network using an out-of-band network, if it is determined that the first set of instructions cannot be transmitted using the telecommunication network.

23. The system of claim 21 wherein the circuitry configured to generate the first set of instructions comprises:

circuitry configured to use the identity of the intermediate upstream gateway to select an associated instruction set from a intermediate upstream gateway brand and model database; and

circuitry configured to compile the first set of instructions using the selected instruction set.

24. The system of claim 21 wherein the circuitry configured to transmit the second set of instructions to the intermediate upstream gateway of the computer network comprises:

circuitry configured to determine if the second set of instructions can be transmitted to the intermediate upstream gateway of the computer network using a telecommunication network; and

circuitry configured to transmit the second set of instructions to the intermediate upstream gateway of the computer network using an out-of-band network, to if it is determined that the second set of instructions cannot be transmitted using the telecommunication network.

25. The system of claim 21 wherein the circuitry configured to generate the second set of instructions comprises:

circuitry configured to use the identity of the intermediate upstream gateway to select an associated instruction set from a intermediate upstream gateway brand and model database; and

circuitry configured to compile the second set of instructions using the selected instruction set.

26. The system of claim 21 wherein the intermediate upstream gateway comprises a network node on the computer network that is located upstream of the monitoring device and the at least one other gateway in the computer network.

27. The system of claim 21 wherein the intermediate upstream gateway comprises:

a first network node on the computer network and a second network node on the computer network wherein the second network node is located upstream of the first network node, and the first network node is located upstream of the monitoring device.

28. The system of claim 21 wherein the circuitry configured to transmit the first alert and the second alert to the command centre comprises:

circuitry configured to determine if the first alert and the second alert can be transmitted to the command centre directly using a telecommunication network; and

circuitry configured to transmit the first alert and the second alert to the intermediate upstream gateway of the computer network using an out-of-band network, wherein the first alert and second alert is then transmitted from the intermediate upstream gateway to the command centre using the telecommunication network, if it is determined that the first alert and the second alert cannot be transmitted directly using the telecommunication network.

29. The system of claim 21 wherein the circuitry configured to determine if the Internet Protocol address of the source that initiated the information security attack on the computing device is to be disrupted comprises:

circuitry configured to determine if the first alert correlates with the second alert; and

circuitry configured to confirm that the Internet Protocol address of the source that initiated the information security attack is to be disrupted, if the first alert correlates with the second alert.

30. A system for disrupting an information security attack on a computing device in a computer network comprising:

circuitry configured to receive an alert from a monitoring device linked to the computing device, wherein the alert includes an Internet Protocol address of a source that initiated the information security attack on the computing device and only an identity of an intermediate upstream gateway of the computer network through which the attack passed, whereby the attack on the computing device passed through the intermediate upstream gateway and at least one other gateway in the computer network;

circuitry configured to generate a first set of instructions and transmit the first set of instructions to the intermediate upstream gateway, wherein the first set of instructions instruct the intermediate upstream gateway to add the IP address of the source that initiated the information security attack to an access control list of the intermediate upstream gateway;

circuitry configured to generate a second set of instructions and transmit the second set of instructions to the intermediate upstream gateway after a first period of time has lapsed, wherein the second set of instructions instruct the intermediate upstream gateway to remove the IP address of the source that initiated the information security attack from the access control list of the intermediate upstream gateway;

circuitry configured to determine, during the first period of time, if a new mitigation action is to be created to address the alert based on a security alert database; and

circuitry configured to transmit the alert to a command centre, if a new mitigation action is to be created to address the alert.