CLAIMS:

1. A method comprising:

analyzing network traffic information;

identifying a domain name system (DNS) amplification attack based on the network traffic information;

in response to identifying the DNS amplification attack, invoking a threat mitigation action;

receiving a domain name system (DNS) query from a source address;

determining, by a DNS server, that a payload size of a response to the DNS query exceeds a threshold payload size; and

dropping the response to the DNS query based on the threat mitigation action.

2. The method of claim 1, wherein the detecting of the DNS amplification attack includes:

identifying a rate of traffic from the source address for a certain period of time; and

determining that the rate of the traffic exceeds a threshold rate.

3. The method of claim 1 or 2, wherein the detecting of the DNS amplification attack includes:

examining payloads of a plurality of first responses generated by the DNS server for a certain period of time; and

determining that one or more payloads of the plurality of first responses exceeds the threshold payload size.

4. The method of any preceding claim, wherein the detecting of the DNS amplification attack includes:

determining a historical ratio based on one or more historical DNS queries and one or more historical responses;

determining a current ratio based on recent DNS queries and their associated DNS responses during a particular time period; and

determining that a difference between the current ratio and the historical ratio exceeds a threshold value.

5. The method of any preceding claim, wherein the threat mitigation action includes deploying a filtering rule to filter the response to the DNS query.

6. The method of claim 5, wherein the filtering rule is deployed on a router for filtering the response to the DNS query.

7. The method of claim 5 or 6, wherein the filtering rule is deployed on the DNS server for filtering the response to the DNS query.

8. The method of any one of claims 5 to 7, wherein the filtering rule includes the source address and the threshold payload size.

9. The method of any preceding claim, further comprising determining the threshold payload size dynamically based on a machine learning model and previous responses to DNS queries within a specified time period.

10. The method of any preceding claim, wherein the DNS server calculates an anticipated payload size of the response prior to generating the response and wherein dropping the response to the DNS query comprises not generating the response.

11. A system, comprising:

at least one processor; and

memory, storing instructions that, when executed by the at least one processor, cause the system to perform a method, the method comprising:

analyzing network traffic information;

identifying a domain name system (DNS) amplification attack based on the network traffic information;

in response to identifying the DNS amplification attack, invoking a threat mitigation action;

receiving a domain name system (DNS) query from a source address;

determining, by a DNS server, that a payload size of a response to the DNS query exceeds a threshold payload size; and

dropping the response to the DNS query based on the threat mitigation action.

12. The system of claim 11, wherein the detecting of the DNS amplification attack includes:

identifying a rate of traffic from the source address for a certain period of time; and

determining that the rate of the traffic exceeds a threshold rate.

13. The system of claim 11 or 12, wherein the detecting of the DNS amplification attack includes:

examining payloads of a plurality of first responses generated by the DNS server for a certain period of time; and

determining that one or more payloads of the plurality of first responses exceeds the threshold payload size.

14. The system of any one of claims 11 to 13, wherein the detecting of the DNS amplification attack includes:

determining a historical ratio based on one or more historical DNS queries and one or more historical responses;

determining a current ratio based on recent DNS queries and their associated DNS responses during a particular time period; and

determining that a difference between the current ratio and the historical ratio exceeds a threshold value.

15. The system of any one of claims 11 to 14, wherein the threat mitigation action includes deploying a filtering rule to filter the response to the DNS query.

16. The system of claim 15, wherein the filtering rule is deployed on a router for filtering the response to the DNS query.

17. The system of claim 15 or 16, wherein the filtering rule is deployed on the DNS server for filtering the response to the DNS query.

18. The system of any one of claims 15 to 17, wherein the filtering rule includes the source address and the threshold payload size.

19. The system of any one of claims 11 to 18, wherein the method further comprises determining the threshold payload size dynamically based on a machine learning model and previous responses to DNS queries within a specified time period.

20. A system, comprising:

at least one processor; and

memory, storing instructions that, when executed by the at least one processor, cause the system to perform a method, the method comprising:

analyzing network traffic information;

identifying a domain name system (DNS) amplification attack based on the network traffic information;

determining a threshold payload size dynamically based on a machine learning model and the network traffic information received within a specified first period;

in response to identifying the DNS amplification attack, invoking a threat mitigation action, including distributing a filtering announcement to at least one network device, wherein the filtering announcement includes instructions to cause the at least one network device to:

receive a current DNS query from a source address;

receive a response to the current DNS query;

determine that a payload size of the response to the current DNS query exceeds the threshold payload size; and

drop the response to the DNS query based on determining that the payload size of the response to the current DNS query exceeds the threshold payload size;

determining an updated threshold payload size dynamically based on the machine learning model and the network traffic information received within a specified second period; and

distributing an updated filtering announcement with the updated threshold payload size to the at least one network device.