SUMMARY

[0004] The present disclosure describes one or more systems, methods, routines and/or techniques for detection of infected network devices via analysis of responseless outgoing network traffic. The systems, methods, routines and/or techniques of the present disclosure may be designed and/or adapted to detect various techniques used by attackers. One or more embodiments of the present disclosure may describe analyzing outgoing network packets that receive no response packet or no packet with a substantive response (i.e., responseless packets) to detect malware on a device and/or network.

[0004a] In one aspect, there is provided a computer implemented method, comprising: executing, on one or more computers, a routine that receives as input a plurality of pieces of packet information from outgoing network traffic, the outgoing network traffic being transmitted from one or more network devices of an internal network and intended for one or more external network devices outside the internal network; executing, on the one or more computers, a routine that analyzes the pieces of packet information to identify outgoing network packets that receive no response packet during a period of time, wherein an outgoing network packet comprises a network packet sent from an internal network device to initiate a network connection with an external network device, the external network device comprising a computing device configured to take control of the internal network device that sent the outgoing network packet; executing, on the one or more computers, a routine that causes storage and/or tracking, in a tracked connection list, of packet information related to the outgoing network packets that have received no response packet, the packet information comprising packet headers that have been normalized such that identical packet headers that are received within a period of time are grouped together; iteratively determining whether an entry exists in the tracked connection list that comprises normalized header information that is reversed compared to header information of an immediate packet, wherein normalized header information that is reversed represents a destination Internet Protocol (IP) address to a source IP address connection; determining that the immediate packet is a response packet for a connection that was previously stored in the tracked connection list in response to header information of the immediate packet and header information of a stored packet matching in a reversed

manner; and removing the packet or header information associated with the response packet from the tracked connection list in response to the response packet comprising data indicating that the response packet contains a substantive response; and wherein the steps of receiving, analyzing, causing, determining, and removing are performed by one or more processors operably coupled to a memory of the one or more computers.

[0004b] In another aspect, there is provided a data processing system, comprising: one or more communications units that are in communication with one or more networks; one or more memory units that store computer code; and one or more processor units coupled to the one or more communications units and the one or more memory units, wherein the one or more processor units execute the computer code stored in the one or more memory units to adapt the data processing system to: receive as input a plurality of pieces of packet information from outgoing network traffic, the outgoing network traffic being transmitted from one or more network devices of an internal network and intended for one or more external network devices outside the internal network; analyze the pieces of packet information to identify outgoing network packets that receive no response packet during a period of time, wherein an outgoing network packet is identified in response to the outgoing network packet comprising an initial communication network packet sent from an internal network device to establish a network connection with an external network device, the external network device comprising an attacker-controlled server configured to take control of the internal network device that sent the outgoing network packet and instruct the internal network device to perform an action for the attacker; cause storage and/or tracking, in a tracked connection list, of packet information related to the outgoing network packets that have received no response packet, the packet information comprising packet headers that have been normalized such that identical packet headers that are received within a period of time are grouped together; iteratively determine whether an entry exists in the tracked connection list that comprises normalized header information that is reversed compared to header information of an immediate packet, wherein normalized header information that is reversed represents a destination Internet Protocol (IP) address to a source IP address connection; determine that the immediate packet is a response packet for a connection that was previously stored in the tracked connection list in response to header information of the immediate packet and header

information of a stored packet matching in a reversed manner; and remove the packet or header information associated with the response packet from the tracked connection list in response to the response packet comprising data indicating that the response packet contains a substantive response.

[0005] One or more embodiments of the present disclosure describe a computer implemented method for network and/or device security. The method may execute on one or more computers (e.g., one or more firewalls) and may include a number of routines that are executed on one or more of the computers. The method may include a routine that receives as input first packet information. The method may include a routine that analyzes the first packet information to determine whether the first packet information identifies an outgoing network packet that is associated with the initiation of a network communication. The method may include a routine that causes storage and/or tracking, in one or more data stores, of the first packet information if the first packet information identifies an outgoing network packet that is associated with the initiation of a network communication, and if the first packet information is determined to be a potential responseless packet. The method may include a routine that receives as input second packet information. The method may include a routine that analyzes the second packet information to determine whether the second packet information identifies an incoming network packet that is in response to the outgoing network packet. The method may include a routine that causes removal and/or ends tracking, in the one or more data stores, of the first packet information if the second packet information identifies an incoming network packet that is in response to the outgoing network packet, and if the first packet information is determined to not be a responseless packet based on the second packet information.

[0006] In some embodiments, the first packet information and the second packet information may each be packet header information. In some embodiments, the first packet information and the second packet information may each be normalized packet

CLAIMS

1. A computer implemented method for network and/or device security, comprising:

executing, on one or more computers, a routine that receives as input a plurality of pieces of packet information from network traffic;

executing, on the one or more computers, a routine that analyzes the pieces of packet information to identify outgoing network packets that receive no response packet during a period of time; and

executing, on the one or more computers, a routine that causes storage and/or tracking, in one or more data stores, of packet information related to the outgoing network packets that have received no response packet.

2. The computer implemented method of claim 1, wherein the step of analyzing the pieces of packet information to identify outgoing network packets that receive no response packet during a period of time includes analyzes the pieces of packet information to identify outgoing network packets that are Dead-SYN packets.

3. The computer implemented method of claim 1, further comprising:

executing, on the one or more computers, a routine that analyzes packet information, from the one or more data stores, to determine whether anomalies exist in the network traffic; and

generating one or more events based on the determination of whether anomalies exist in the network traffic, the one or more events indicating that malware may exist in a network or on a device.

4. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a particular source device has generated multiple outgoing network packets that received no response packet.

5. The computer implemented method of claim 3, further comprising:

executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,

wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication, and

wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:

analyzing the group of packet information to determine a number of pieces of packet information in the group with the same source and destination; and

determining whether the number of pieces of packet information with the same source and destination exceeds a threshold.

6. The computer implemented method of claim 5, wherein the number of pieces of packet information included in the group is determined by comparing a time period configuration to the time indication of each piece of packet information such that a number of pieces of packet information are received over determined a period of time.

7. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether multiple source devices have been infected with the same malware.

8. The computer implemented method of claim 3, further comprising:

executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,

wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication, and

wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:

analyzing the group of packet information to determine, for each destination, a number of pieces of packet information in the group for each unique source; and

determining whether the number of pieces of packet information with each unique source, for a single destination, exceeds a threshold.

9. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a source device is attempting to communicate with multiple destinations.

10. The computer implemented method of claim 3, further comprising:

executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,

wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication, and

wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:

analyzing the group of packet information to determine, for each source, a number of pieces of packet information in the group for each unique destination; and

determining whether the number of pieces of packet information with each unique destination, for a single source, exceeds a threshold.

11. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a particular

source device is attempting to communicate with a particular destination on a reoccurring basis.

12. The computer implemented method of claim 3, further comprising:

executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,

wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication,

wherein each of the pieces of packet information in the group has the same source and destination, and

wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:

analyzing the group of packet information to determine, for each destination, a number of pieces of packet information in the group; and

determining whether the number of pieces of packet information, for a single destination, exceeds a threshold.

13. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a particular source device is attempting to communicate with a particular destination an average number of times over a time period that is about the same as averages over previous time periods.

14. The computer implemented method of claim 12, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic further includes:

determining, for the single destination, an average number of pieces of packet information in the group with the single destination per source;

comparing the average number to a previous average number of a previous group of packet information; and

determining whether the average number and the previous average number are about the same.

15. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a particular source device is generated repeating clusters of outgoing network packets that received no response packet.

16. The computer implemented method of claim 3, further comprising:

executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,

wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication;

wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:

analyzing the group of packet information and, for each source, forming packet clusters for pieces of packet information having time indications that are relatively close to each other; and

determining whether the time between the packet clusters is repeating.

17. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a particular source device is attempting to communicate with a particular destination in repeating clusters.

18. The computer implemented method of claim 3, further comprising:

executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,

wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication,

wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:

analyzing the group of packet information and, for each source/destination pair, forming packet clusters for pieces of packet information having time indications that are relatively close to each other; and

determining whether the time between the packet clusters is repeating.

19. A data processing system for network and/or device security, comprising:

one or more communications units that are in communication with one or more networks;

one or more memory units that store computer code; and

one or more processor units coupled to the one or more communications units and the one or more memory units, wherein the one or more processor units execute the computer code stored in the one or more memory units to adapt the data processing system to perform the method of any one of claims 1 to 18.

20. A computer readable medium comprising computer readable instructions, that when executed by one or more processor units of a data processing system, cause the data processing system to perform the method of any one of claims 1 to 18.

CLAIMS

1. A computer implemented method, comprising:

executing, on one or more computers, a routine that receives as input a plurality of pieces of packet information from outgoing network traffic, the outgoing network traffic being transmitted from one or more network devices of an internal network and intended for one or more external network devices outside the internal network;

executing, on the one or more computers, a routine that analyzes the pieces of packet information to identify outgoing network packets that receive no response packet during a period of time, wherein an outgoing network packet comprises a network packet sent from an internal network device to initiate a network connection with an external network device, the external network device comprising a computing device configured to take control of the internal network device that sent the outgoing network packet;

executing, on the one or more computers, a routine that causes storage and/or tracking, in a tracked connection list, of packet information related to the outgoing network packets that have received no response packet, the packet information comprising packet headers that have been normalized such that identical packet headers that are received within a period of time are grouped together;

iteratively determining whether an entry exists in the tracked connection list that comprises normalized header information that is reversed compared to header information of an immediate packet, wherein normalized header information that is reversed represents a destination Internet Protocol (IP) address to a source IP address connection;

determining that the immediate packet is a response packet for a connection that was previously stored in the tracked connection list in response to header information of the immediate packet and header information of a stored packet matching in a reversed manner; and

removing the packet or header information associated with the response packet from the tracked connection list in response to the response packet comprising data indicating that the response packet contains a substantive response; and

wherein the steps of receiving, analyzing, causing, determining, and removing are performed by one or more processors operably coupled to a memory of the one or more computers.

2. The computer implemented method of claim 1, wherein the step of analyzing the pieces of packet information to identify outgoing network packets that receive no response packet during a period of time includes analyzing the pieces of packet information to identify outgoing network packets that are Dead-SYN packets.

3. The computer implemented method of claim 1, further comprising: executing, on the one or more computers, a routine that analyzes packet information, from the one or more data stores, to determine whether anomalies exist in the network traffic; and
generating one or more events based on the determination of whether anomalies exist in the network traffic, the one or more events indicating that malware may exist in a network or on a device.

4. The computer implemented method of claim 3, wherein the step of determining whether anomalies exist in the network traffic includes detecting anomalies that are indicative of Advanced Persistent Threats (APTs).

5. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a particular source device has generated multiple outgoing network packets that received no response packet.

6. The computer implemented method of claim 3, further comprising:
executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,
wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication, and
wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:
analyzing the group of packet information to determine a number of pieces of packet information in the group with the same source and destination; and
determining whether the number of pieces of packet information with the same source and destination exceeds a threshold.

7. The computer implemented method of claim 6, wherein the number of pieces of packet information included in the group is determined by comparing a time period configuration to the time indication of each piece of packet information such that a number of pieces of packet information are received over determined a period of time.

8. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether multiple source devices have been infected with the same malware.

9. The computer implemented method of claim 3, further comprising:

executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,
wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication, and
wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:
analyzing the group of packet information to determine, for each destination, a number of pieces of packet information in the group for each unique source; and
determining whether the number of pieces of packet information with each unique source, for a single destination, exceeds a threshold.

10. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a source device is attempting to communicate with multiple destinations.

11. The computer implemented method of claim 3, further comprising:
executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,
wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication, and
wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:
analyzing the group of packet information to determine, for each source, a number of pieces of packet information in the group for each unique destination; and
determining whether the number of pieces of packet information with each unique destination, for a single source, exceeds a threshold.

12. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a particular source device is attempting to communicate with a particular destination on a reoccurring basis.

13. The computer implemented method of claim 3, further comprising:
executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,

wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication,
wherein each of the pieces of packet information in the group has the same source and destination, and
wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:
analyzing the group of packet information to determine, for each destination, a number of pieces of packet information in the group; and
determining whether the number of pieces of packet information, for a single destination, exceeds a threshold.

14. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a particular source device is attempting to communicate with a particular destination an average number of times over a time period that is about the same as averages over previous time periods.

15. The computer implemented method of claim 13, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic further includes:
determining, for the single destination, an average number of pieces of packet information in the group with the single destination per source;
comparing the average number to a previous average number of a previous group of packet information; and
determining whether the average number and the previous average number are about the same.

16. The computer implemented method of claim 13, wherein the number of pieces of packet information included in the group is determined by comparing a time period configuration to the time indication of each piece of packet information such that a number of pieces of packet information are received over determined a period of time.

17. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a particular source device is generated repeating clusters of outgoing network packets that received no response packet.

18. The computer implemented method of claim 3, further comprising:
executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,

wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication,
wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:
analyzing the group of packet information and, for each source, forming packet clusters for pieces of packet information having time indications that are relatively close to each other; and
determining whether the time between the packet clusters is repeating.

19. The computer implemented method of claim 3, wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes analyzing packet information to determine whether a particular source device is attempting to communicate with a particular destination in repeating clusters.

20. The computer implemented method of claim 3, further comprising:
executing, on the one or more computers, a routine that receives as input, from one or more data stores, a group of packet information that includes multiple pieces of packet information,
wherein each of the pieces of packet information is associated with a network packet and includes a source and a destination of the associated packet and a time indication,
wherein the step of analyzing packet information from the one or more data stores to determine whether anomalies exist in the network traffic includes:
analyzing the group of packet information and, for each source/destination pair, forming packet clusters for pieces of packet information having time indications that are relatively close to each other; and
determining whether the time between the packet clusters is repeating.

21. A data processing system, comprising:
one or more communications units that are in communication with one or more networks;
one or more memory units that store computer code; and
one or more processor units coupled to the one or more communications units and the one or more memory units, wherein the one or more processor units execute the computer code stored in the one or more memory units to adapt the data processing system to:
receive as input a plurality of pieces of packet information from outgoing network traffic, the outgoing network traffic being transmitted from one or more network devices of an internal network and intended for one or more external network devices outside the internal network;
analyze the pieces of packet information to identify outgoing network packets that receive no response packet during a period of time, wherein an outgoing network packet is identified in response to the outgoing network packet comprising an initial communication network packet sent from an internal network device to establish a

network connection with an external network device, the external network device comprising an attacker-controlled server configured to take control of the internal network device that sent the outgoing network packet and instruct the internal network device to perform an action for the attacker;
cause storage and/or tracking, in a tracked connection list, of packet information related to the outgoing network packets that have received no response packet, the packet information comprising packet headers that have been normalized such that identical packet headers that are received within a period of time are grouped together;
iteratively determine whether an entry exists in the tracked connection list that comprises normalized header information that is reversed compared to header information of an immediate packet, wherein normalized header information that is reversed represents a destination Internet Protocol (IP) address to a source IP address connection;
determine that the immediate packet is a response packet for a connection that was previously stored in the tracked connection list in response to header information of the immediate packet and header information of a stored packet matching in a reversed manner; and
remove the packet or header information associated with the response packet from the tracked connection list in response to the response packet comprising data indicating that the response packet contains a substantive response.

22. The data processing system of claim 21, wherein the one or more processor units execute the computer code stored in the one or more memory units to adapt the data processing system to:
analyze packet information, from the one or more data stores, to determine whether anomalies exist in the network traffic; and
generate one or more events based on the determination of whether anomalies exist in the network traffic, the one or more events indicating that malware may exist in a network or on a device.

23. The data processing system of claim 22, wherein the data processing system is a firewall.