

## CLAIMS

1. A first computer system comprising at least one memory and at least one associated microprocessor configured to perform, externally from a potential domain generation algorithm (DGA) malware host, the following steps:

intercept an original answer to a first external access request, wherein the first external access request is sent by the potential DGA malware host to an external site;

parse at least one of the first external access request and the original answer to the first external access request to determine whether the original answer to the first external access request comprises a real time indicating a present time of the original answer;

send a modified answer to the potential DGA malware host, the modified answer being generated from the original answer by replacing the real time included in the original answer with an accelerated real time subsequent to the original real time;

intercept, in response to a second external access request sent by the potential DGA malware host, an answer indicating that the second access request was not successful, wherein the second external access request is sent after the first external access request is sent; and

in response to intercepting the answer indicating that the second access request was not successful, determine that the potential DGA malware host includes malware executing a domain generation algorithm.

2. The first computer system of claim 1, wherein parsing at least one of the first external access request and the original answer to the first external access request comprises identifying an address of a time server in an address field of the first external access request.

3. The first computer system of claim 1, wherein parsing at least one of the first external access request and the original answer to the first external access request comprises parsing the original answer to the first external access request to identify a real time field from a plurality of fields of the original answer to the first external access request.

4. The first computer system of claim 3, wherein identifying the real time field comprises comparing a content of the real time field to an independent real time value determined by the first computer system.

5. The first computer system of claim 1, wherein the potential DGA malware host is a second computer system physically distinct from the first computer system.

6. The first computer system of claim 1, wherein the potential DGA malware host is a virtual machine hosted by the first computer system.

7. The first computer system of claim 1, wherein the at least one associated microprocessor is further configured to determine a domain name generated by the domain generation algorithm and identify, according to the domain name, a plurality of computer systems suspected of executing the domain generation algorithm.

8. The first computer system of claim 1, wherein the at least one associated microprocessor is further configured, in response to determining that the potential DGA malware host includes malware executing the domain generation algorithm, to add a domain name generated by the domain generation algorithm to a security application blacklist.

9. A first computer system comprising at least one memory and at least one associated microprocessor configured to perform, externally from a potential domain generation algorithm (DGA) malware host, the following steps:

20 parse a first external access request to determine whether the first external access request comprises a real time indicating a present time of the first external access request, wherein the first external access request is sent by the potential DGA malware host to an external site;

25 parse a first original answer to the first external access request to determine whether the first original answer comprises a first information indicating that the real time is not accurate;

send a modified answer to the potential DGA malware host, the modified answer being generated from the first original answer by replacing the first information with a second information indicating that the real time is accurate;

30 intercept, in response to a second external access request sent by the potential DGA malware host to a second external site, a second original answer indicating that the second access request was not successful; and

determine, in response to intercepting the second answer, that the potential DGA malware host includes malware executing a domain generation algorithm.

10. A non-transitory computer readable medium storing instructions that, when executed, configure at least one memory and at least one associated microprocessor of a first computer system to perform, externally from a potential domain generation algorithm (DGA) malware host, the following steps:

5           intercept an original answer to a first external access request, wherein the first external access request is sent by the potential DGA malware host to an external site;

          parse at least one of the first external access request and the original answer to the first external access request to determine whether the original answer to the first external access request comprises a real time indicating a present time of the original answer;

10           send a modified answer to the potential DGA malware host, the modified answer being generated from the original answer by replacing the real time included in the original answer with an accelerated real time subsequent to the original real time;

          intercept, in response to a second external access request sent by the potential DGA malware host, an answer indicating that the second access request was not successful,  
15           wherein the second external access request is sent after the first external access request is sent; and

          in response to intercepting the answer indicating that the second access request was not successful, determine that the potential DGA malware host includes malware executing a domain generation algorithm.

20

11. The non-transitory computer readable medium of claim 10, wherein parsing at least one of the first external access request and the original answer to the first external access request comprises identifying an address of a time server in an address field of the first external access request.

25

12. The non-transitory computer readable medium of claim 10, wherein parsing at least one of the first external access request and the original answer to the first external access request comprises parsing the original answer to the first external access request to identify a real time field from a plurality of fields of the original answer to the first external access  
30           request.

13. The non-transitory computer readable medium of claim 12, wherein identifying the real time field comprises comparing a content of the real time field to an independent real time value determined by the first computer system.

35

14. The non-transitory computer readable medium of claim 10, wherein the potential DGA malware host is a second computer system physically distinct from the first computer system.

5 15. The non-transitory computer readable medium of claim 10, wherein the potential DGA malware host is a virtual machine hosted by the first computer system.

16. The non-transitory computer readable medium of claim 10, wherein the at least one associated microprocessor is further configured to determine a domain name generated by  
10 the domain generation algorithm and identify, according to the domain name, a plurality of computer systems suspected of executing the domain generation algorithm.

17. The non-transitory computer readable medium of claim 10, wherein the at least one associated microprocessor is further configured, in response to determining that the potential  
15 DGA malware host includes malware executing the domain generation algorithm, to add a domain name generated by the domain generation algorithm to a security application blacklist.