CLAIMS

1. A computer system comprising at least one hardware processor configured to operate a reverse address mapper, a registration data filter connected to the reverse address mapper, and a content analyzer connected to the registration data filter, wherein:

the reverse address mapper is configured to identify a set of co-hosted Internet domains according to a known fraudulent Internet domain, wherein the known fraudulent Internet domain is located at a target Internet Protocol (IP) address, and wherein identifying the set of co-hosted Internet domains comprises selecting the set of co-hosted Internet domains so that all members of the set of co-hosted Internet domains are located at the target IP address;

the registration data filter is configured to filter the set of co-hosted Internet domains to produce a subset of fraud candidate domains, wherein filtering the set of cohosted Internet domains comprises:

determining whether a selection condition is satisfied according to domain name registration data characterizing a domain of the set of co-hosted Internet domains, wherein the domain name registration data characterizing the domain comprises an email address, and wherein the registration data filter is configured to determine whether the selection condition is satisfied according to at least one of a length of the email address and/or a randomness of the email address, and

in response, selecting the domain into the subset of fraud candidate domains when the selection condition is satisfied; and

the content analyzer is configured to:

analyze an electronic document distributed by a candidate domain selected from the subset of fraud candidate domains to determine whether the electronic document is fraudulent, and

in response, when the electronic document is fraudulent, determine that the candidate domain is fraudulent;

wherein the computer system is configured to transmit a fraud assessment indicator generated according to the determination that the candidate domain is fraudulent to block access to a resource hosted by the candidate domain.

2. The computer system of claim 1, wherein determining whether the selection condition is satisfied comprises comparing the domain name registration data characterizing the domain with domain name registration data characterizing the known fraudulent Internet domain.

3. The computer system of claim 2, wherein determining whether the selection condition is satisfied comprises comparing a registration timestamp of the domain to a registration timestamp of the known fraudulent Internet domain.

4. The computer system of claim 1, wherein the registration data filter is configured to determine whether the selection condition is satisfied according to the length of the email address.

5. The computer system of claim 1, wherein the registration data filter is configured to determine whether the selection condition is satisfied according to an identity of a mail server handling email sent to the email address.

6. The computer system of claim 1, wherein the registration data filter is configured to determine whether the selection condition is satisfied according to whether a provider of the email address allows anonymous email accounts.

7. The computer system of claim 1, wherein the domain name registration data characterizing the domain comprises a telephone number, and wherein the registration data filter is configured to determine whether the selection condition is satisfied according to the telephone number.

8. The computer system of claim 7, wherein determining whether the selection condition is satisfied comprises performing a reverse telephone number lookup to determine an entity owning to the telephone number, and wherein the registration data filter is configured to determine whether the selection condition is satisfied according to a result of the reverse telephone number lookup.

9. A method of identifying fraudulent Internet domains, the method comprising:

employing at least one hardware processor to identify a set of co-hosted Internet domains according to a known fraudulent Internet domain, wherein the known fraudulent Internet domain is located at a target Internet Protocol (IP) address, and wherein identifying the set of co-hosted Internet domains comprises selecting the set of co-hosted Internet domains so that all members of the set of co-hosted Internet domains are located at the target IP address;

employing the at least one hardware processor to filter the set of co-hosted Internet domains to produce a subset of fraud candidate domains, wherein filtering the set of co-hosted Internet domains comprises:

determining whether a selection condition is satisfied according to domain name registration data characterizing a domain of the set of co-hosted Internet domains, wherein the domain name registration data characterizing the domain comprises an email address, and wherein the registration data filter is configured to determine whether the selection condition is satisfied according to at least one of a length of the email address and/or a randomness of the email address, and

in response, selecting the domain into the subset of fraud candidate domains when the selection condition is satisfied;

employing the at least one hardware processor to analyze an electronic document distributed by a candidate domain selected from the subset of fraud candidate domains, to determine whether the electronic document is fraudulent;

in response to analyzing the electronic document, when the electronic document is fraudulent, determining that the candidate domain is fraudulent; and

transmitting a fraud assessment indicator generated according to the determination that the candidate domain is fraudulent to block access to a resource hosted by the candidate domain.

10. The method of claim 9, wherein determining whether the selection condition is satisfied comprises comparing the domain name registration data characterizing the domain with domain name registration data characterizing the known fraudulent Internet domain.

11. The method of claim 10, wherein determining whether the selection condition is satisfied comprises comparing a registration timestamp of the domain to a registration timestamp of the known fraudulent Internet domain.

12. The method of claim 9, comprising determining whether the selection condition is satisfied according to the length of the email address.

13. The method of claim 9, comprising determining whether the selection condition is satisfied according to an identity of a mail server handling email sent to the email address.

14. The method of claim 9, comprising determining whether the selection condition is satisfied according to whether a provider of the email address allows anonymous email accounts.

15. The method of claim 9, wherein the domain name registration data characterizing the domain comprises a telephone number, and wherein the method comprises determining whether the selection condition is satisfied according to the telephone number.

16. The method of claim 15, wherein determining whether the selection condition is satisfied comprises performing a reverse telephone number lookup to determine an entity owning to the telephone number, and wherein the method comprises determining whether the selection condition is satisfied according to a result of the reverse telephone number lookup.

17. A non-transitory computer-readable medium storing instructions which, when executed by at least one hardware processor, cause the at least one hardware processor to form a reverse address mapper, a registration data filter connected to the reverse address mapper, and a content analyzer connected to the registration data filter, wherein:

the reverse address mapper is configured to identify a set of co-hosted Internet domains according to a known fraudulent Internet domain, wherein the known fraudulent Internet domain is located at a target Internet Protocol (IP) address, and wherein identifying the set of co-hosted Internet domains comprises selecting the set of co-hosted Internet domains so that all members of the set of co-hosted Internet domains are located at the target IP address;

the registration data filter is configured to filter the set of co-hosted Internet domains to produce a subset of fraud candidate domains, wherein 5 filtering the set of cohosted Internet domains comprises:

determining whether a selection condition is satisfied according to domain name registration data characterizing a domain of the set of co-hosted Internet domains, wherein the domain name registration data characterizing the domain comprises an email address, and wherein the registration data filter is configured to determine whether the selection condition is satisfied according to at least one of a length of the email address and/or a randomness of the email address, and

in response, selecting the domain into the subset of fraud candidate domains when the selection condition is satisfied; and

the content analyzer is configured to:

analyze an electronic document distributed by a candidate domain selected from the subset of fraud candidate domains to determine whether the electronic document is fraudulent, and

in response, when the electronic document is fraudulent, determine that the candidate domain is fraudulent;

wherein the instructions further cause the at least one hardware processor to transmit a fraud assessment indicator generated according to the determination that the candidate domain is fraudulent to block access to a resource hosted by the candidate domain.