Claims

1. A computer-implemented method, comprising:

at a device having one or more processors and memory:

identifying respective uncompressed sub-portions of an application installation package in accordance with a predetermined threshold size established for each uncompressed sub-portion;

decompressing the respective uncompressed sub-portions one sub-portion at a time to acquire corresponding decompressed data for each respective uncompressed sub-portion;

before completing the un-compression of all sub-portions of the application installation package, checking the corresponding decompressed data of a first respective sub-portion of the application installation package according to virus samples in a virus feature library; and

concluding that the application installation package is a virus-infected file or rogue software in accordance with a determination that the corresponding decompressed data of the first respective sub-portion includes respective features of at least one of the virus samples;

wherein each of the virus samples includes an offset address and a virus signature;

wherein checking the corresponding decompressed data of the first respective sub-portion according to the virus samples in the virus feature library comprises:

when the length of data with the offset address as its starting point in the decompressed data is shorter than a length of the virus signature, acquiring, from at least two of the sub-portions, virus checking data having the offset address as its starting point and a length equal to the length of the virus signature, and making a comparison of the virus checking data with the virus signature.

~~2. The method of claim 1, wherein each of the virus samples includes a respective offset address and a respective virus signature.~~

~~3~~2. The method of claim ~~2~~1, wherein checking the corresponding decompressed data of the first respective sub-portion according to the virus samples in the virus feature library further comprises:

acquiring, from the corresponding decompressed data of the first respective sub-portion, respective virus checking data, wherein the respective virus checking data starts from an offset address corresponding to the respective offset address of a first virus sample, and has a

length equal to a respective length of a respective virus signature of the first virus sample;

making a comparison of the respective virus checking data with the respective virus signature of the first virus sample; and

determining that the respective decompressed data of the first respective sub-portion contains the first virus sample when the virus checking data is consistent with the respective virus signature of the first virus sample.

~~4.~~3. The method of claim ~~3~~2, wherein the acquiring further comprise:

identifying, from among the respective uncompressed sub-portions of the application installation package, a next uncompressed sub-portion for which virus checking has not been performed;

determining whether the corresponding decompressed data of the identified next uncompressed sub-portion has a length greater than or equal to the respective length of the respective virus signature of the first virus sample, starting from the offset address corresponding to the respective offset address of the first virus sample; and

in accordance with a determination that the corresponding decompressed data of the identified uncompressed sub-portion does not have a sufficient length starting from the offset address corresponding to the respective offset address of the first virus sample, acquiring, the virus checking data from the corresponding uncompressed data of at least one additional uncompressed sub-portion for which virus checking has not been performed, wherein the virus checking data includes decompressed data corresponding to all offset addresses between a starting offset address and an ending offset address, wherein the starting offset address is the respective offset address of the first virus sample, and the ending offset address is an offset address formed by the starting offset address plus the respective length of the respective virus signature of the first virus sample.

~~5~~4. The method of claim 1, further comprising:

continuing the decompression of the respective uncompressed sub-portions and the checking of the corresponding decompressed data of the respective uncompressed sub-portions, one sub-portion at a time, until it is determined that the application installation package is a virus-infected file or rogue software.

~~6~~5. The method of claim 1, further comprising:

continuing the decompression of the respective uncompressed sub-portions and the checking of the corresponding decompressed data of the respective uncompressed

sub-portions, one sub-portion at a time, until the decompression and checking of the application installation package is completed.

~~7~~6. The method of claim 1, further comprising:

continuing the decompression of the respective uncompressed sub-portions and the checking of the corresponding decompressed data of the respective uncompressed sub-portions in parallel, until the decompression of the application installation package is completed.

~~8~~7. A non-transitory computer-readable medium, having instructions stored thereon, the instructions, when executed by one or more processors, cause the processors to perform operations comprising:

identifying respective uncompressed sub-portions of an application installation package in accordance with a predetermined threshold size established for each uncompressed sub-portion;

decompressing the respective uncompressed sub-portions one sub-portion at a time to acquire corresponding decompressed data for each respective uncompressed sub-portion;

before completing the un-compression of all sub-portions of the application installation package, checking the corresponding decompressed data of a first respective sub-portion of the application installation package according to virus samples in a virus feature library; and

concluding that the application installation package is a virus-infected file or rogue software in accordance with a determination that the corresponding decompressed data of the first respective sub-portion includes respective features of at least one of the virus samples;

wherein each of the virus samples includes an offset address and a virus signature;

wherein checking the corresponding decompressed data of the first respective sub-portion according to the virus samples in the virus feature library comprises:

when the length of data with the offset address as its starting point in the decompressed data is shorter than a length of the virus signature, acquiring, from at least two of the sub-portions, virus checking data having the offset address as its starting point and a length equal to the length of the virus signature, and making a comparison of the virus checking data with the virus signature.

~~9. The computer-readable medium of claim 8, wherein each of the virus samples includes a respective offset address and a respective virus signature.~~

~~10~~8. The computer-readable medium of claim ~~9~~7, wherein checking the corresponding

decompressed data of the first respective sub-portion according to the virus samples in the virus feature library further comprises:

acquiring, from the corresponding decompressed data of the first respective sub-portion, respective virus checking data, wherein the respective virus checking data starts from an offset address corresponding to the respective offset address of a first virus sample, and has a length equal to a respective length of a respective virus signature of the first virus sample;

making a comparison of the respective virus checking data with the respective virus signature of the first virus sample; and

determining that the respective decompressed data of the first respective sub-portion contains the first virus sample when the virus checking data is consistent with the respective virus signature of the first virus sample.

~~11~~9. The computer-readable medium of claim ~~10~~8, wherein the acquiring further comprise:

identifying, from among the respective uncompressed sub-portions of the application installation package, a next uncompressed sub-portion for which virus checking has not been performed;

determining whether the corresponding decompressed data of the identified next uncompressed sub-portion has a length greater than or equal to the respective length of the respective virus signature of the first virus sample, starting from the offset address corresponding to the respective offset address of the first virus sample; and

in accordance with a determination that the corresponding decompressed data of the identified uncompressed sub-portion does not have a sufficient length starting from the offset address corresponding to the respective offset address of the first virus sample, acquiring, the virus checking data from the corresponding uncompressed data of at least one additional uncompressed sub-portion for which virus checking has not been performed, wherein the virus checking data includes decompressed data corresponding to all offset addresses between a starting offset address and an ending offset address, wherein the starting offset address is the respective offset address of the first virus sample, and the ending offset address is an offset address formed by the starting offset address plus the respective length of the respective virus signature of the first virus sample.

~~12~~10. The computer-readable medium of claim ~~8~~7, wherein the operations further comprise:

continuing the decompression of the respective uncompressed sub-portions and the checking of the corresponding decompressed data of the respective uncompressed

sub-portions, one sub-portion at a time, until it is determined that the application installation package is a virus-infected file or rogue software.

~~13~~11. The computer-readable medium of claim ~~8~~7, wherein the operations further comprise:

continuing the decompression of the respective uncompressed sub-portions and the checking of the corresponding decompressed data of the respective uncompressed sub-portions, one sub-portion at a time, until the decompression and checking of the application installation package is completed.

~~14~~12. The computer-readable medium of claim ~~8~~7, wherein the operations further comprise:

continuing the decompression of the respective uncompressed sub-portions and the checking of the corresponding decompressed data of the respective uncompressed sub-portions in parallel, until the decompression of the application installation package is completed.

~~15~~13. A system, comprising:

one or more processors; and

memory having instructions stored thereon, the instructions, when executed by the one or more processors, cause the processors to perform operations comprising:

identifying respective uncompressed sub-portions of an application installation package in accordance with a predetermined threshold size established for each uncompressed sub-portion;

decompressing the respective uncompressed sub-portions one sub-portion at a time to acquire corresponding decompressed data for each respective uncompressed sub-portion;

before completing the un-compression of all sub-portions of the application installation package, checking the corresponding decompressed data of a first respective sub-portion of the application installation package according to virus samples in a virus feature library; and

concluding that the application installation package is a virus-infected file or rogue software in accordance with a determination that the corresponding decompressed data of the first respective sub-portion includes respective features of at least one of the virus samples;

wherein each of the virus samples includes an offset address and a virus signature;

wherein checking the corresponding decompressed data of the first respective sub-portion according to the virus samples in the virus feature library comprises:

when the length of data with the offset address as its starting point in the

decompressed data is shorter than a length of the virus signature, acquiring, from at least two of the sub-portions, virus checking data having the offset address as its starting point and a length equal to the length of the virus signature, and making a comparison of the virus checking data with the virus signature.

~~16. The system of claim 15, wherein each of the virus samples includes a respective offset address and a respective virus signature.~~

~~17~~14. The system of claim ~~16~~13, wherein checking the corresponding decompressed data of the first respective sub-portion according to the virus samples in the virus feature library further comprises:

acquiring, from the corresponding decompressed data of the first respective sub-portion, respective virus checking data, wherein the respective virus checking data starts from an offset address corresponding to the respective offset address of a first virus sample, and has a length equal to a respective length of a respective virus signature of the first virus sample;

making a comparison of the respective virus checking data with the respective virus signature of the first virus sample; and

determining that the respective decompressed data of the first respective sub-portion contains the first virus sample when the virus checking data is consistent with the respective virus signature of the first virus sample.

~~18~~15. The system of claim ~~17~~14, wherein the acquiring further comprise:

identifying, from among the respective uncompressed sub-portions of the application installation package, a next uncompressed sub-portion for which virus checking has not been performed;

determining whether the corresponding decompressed data of the identified next uncompressed sub-portion has a length greater than or equal to the respective length of the respective virus signature of the first virus sample, starting from the offset address corresponding to the respective offset address of the first virus sample; and

in accordance with a determination that the corresponding decompressed data of the identified uncompressed sub-portion does not have a sufficient length starting from the offset address corresponding to the respective offset address of the first virus sample, acquiring, the virus checking data from the corresponding uncompressed data of at least one additional uncompressed sub-portion for which virus checking has not been performed, wherein the virus checking data includes decompressed data corresponding to all offset addresses

between a starting offset address and an ending offset address, wherein the starting offset address is the respective offset address of the first virus sample, and the ending offset address is an offset address formed by the starting offset address plus the respective length of the respective virus signature of the first virus sample.

~~19~~16. The system of claim ~~15~~13, wherein the operations further comprise:

continuing the decompression of the respective uncompressed sub-portions and the checking of the corresponding decompressed data of the respective uncompressed sub-portions, one sub-portion at a time, until it is determined that the application installation package is a virus-infected file or rogue software.

~~20~~17. The system of claim ~~15~~13, wherein the operations further comprise:

continuing the decompression of the respective uncompressed sub-portions and the checking of the corresponding decompressed data of the respective uncompressed sub-portions, one sub-portion at a time, until the decompression and checking of the application installation package is completed.