



(51) International Patent Classification:

G06F 21/56 (2013.01)

(21) International Application Number:

PCT/US2021/016994

(22) International Filing Date:

08 February 2021 (08.02.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 10300 Energy Drive, Spring, Texas 77389 (US).

(72) Inventors: **GRAY, Tobias Edward Sebastian**; HP UK Development Ltd, 2nd & 3rd Floor Lockton House, Clarendon Road, Cambridge CB2 8FH (GB). **PANDEY, Ratnesh Kumar**; HP UK Development Ltd, 2nd & 3rd Floor Lockton House, Clarendon Road, Cambridge CB2 8FH (GB).

(74) Agent: **SU, Benjamin**; 3390 E Harmony Road, Fort Collins, Colorado 80528 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,

HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- as to the identity of the inventor (Rule 4.17(i))
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published:

- with international search report (Art. 21(3))

(54) Title: MALWARE SCANS

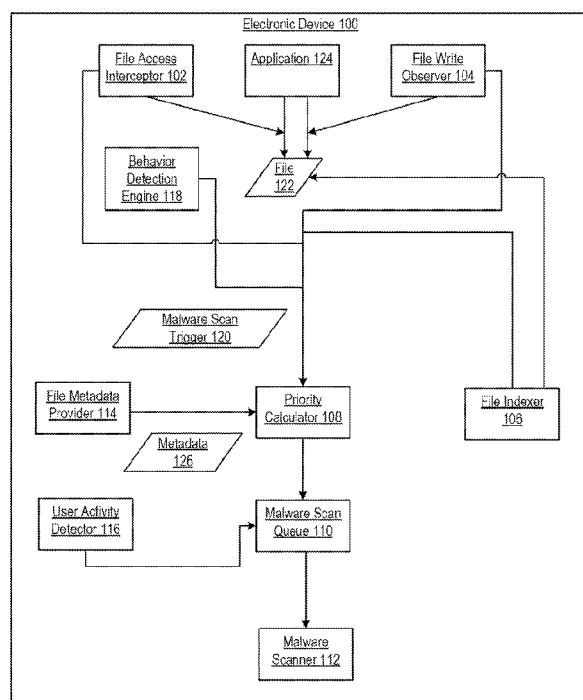


FIG. 1

(57) Abstract: An example non-transitory computer readable storage medium comprises instructions that when executed cause a processor of an electronic device to: in response to detecting a malware scan trigger associated with a file, determine a combined risk score associated with the file based on metadata of the file and a source of the malware scan trigger, where the source includes a file access interceptor, a file write observer, and a file indexer; determine a scan priority based on the combined risk score; and perform a malware scan on the file based on the scan priority.

MALWARE SCANS

BACKGROUND

[0001] Computer executable instructions that are specifically designed to cause damage to a computing device or steal data / information from a computing device are referred to as malware or virus.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Some examples of the present application are described with respect to the following figures:

[0003] FIG. 1 illustrates a functional block of an electronic device to scan for malware based on a scan priority of a file, according to an example;

[0004] FIG. 2 illustrates a method of scanning for malware based on a scan priority of a file, according to an example;

[0005] FIG. 3 illustrates an electronic device to scan for malware based on a scan priority of a file, according to another example;

[0006] FIG. 4 illustrates an electronic device to scan for malware based on a scan priority of a file, according to another example; and

[0007] FIG. 5 illustrates an electronic device to scan for malware based on a scan priority of a file, according to another example.

DETAILED DESCRIPTION

[0008] Antivirus application may be installed on a computing device to detect and protect against malware. An antivirus application may include a malware scanner to perform malware scans. To scan a file thoroughly for malware may take a significant amount of time, which can be detrimental to user experience. Examples described herein provide an approach to enable a computing device to perform a malware scan on a file based on a scan priority. The scan priority may

determine a scan depth and a number of scans that is suitable for the file. Thus, the impact on user experience due to malware scans may be reduced.

[0009] In an example, a non-transitory computer readable storage medium may include instructions that when executed cause a processor of an electronic device to: in response to detecting a malware scan trigger associated with a file, determine a combined risk score associated with the file based on metadata of the file and a source of the malware scan trigger, where the source includes a file access interceptor, a file write observer, and a file indexer; determine a scan priority based on the combined risk score; and perform a malware scan on the file based on the scan priority.

[0010] In another example, a non-transitory computer readable storage medium may include instructions that when executed cause a processor of an electronic device to: in response to detecting a malware scan trigger associated with a file, determine a scan priority associated with the file based on metadata of the file; determine a scan depth and a number of scans based on the scan priority; and perform a set of malware scans on the file based on the scan depth and the number of scans.

[0011] In another example, a non-transitory computer readable storage medium may include instructions that when executed cause a processor of an electronic device to: in response to detecting a malware scan trigger associated with a file, determine a scan priority associated with the file based on metadata of the file; determine user activity information, wherein the user activity information indicates if a user actively interacting with the electronic device; and determine if a malware scan of the file is to be delayed based on the scan priority and the user activity information.

[0012] Turning to FIG. 1, FIG. 1 illustrates a functional block of an electronic device 100 to scan for malware based on a scan priority of a file, according to an example. Electronic device 100 may be, for example, a laptop computer, a desktop computer, an all-in-one system, a tablet computing device, a mobile phone, an electronic book reader, a wearable computing device (e.g., a smart watch), or any other electronic device suitable to perform malware scan on a file.

[0013] Electronic device 100 may include a file access interceptor 102, a file write observer 104, a file indexer 106, a priority calculator 108, a malware scan queue 110, a file metadata provider 114, a user activity detector 116, and a behavioral detection engine 118. File access interceptor 102, file write observer 104, file indexer 106, priority calculator 108, malware scan queue 110, file metadata provider 114, user activity detector 116, and behavioral detection engine 118 may each be implemented using processor executable instructions, hardware devices (e.g., semiconductor-based microprocessors, integrated circuits, field-programmable gate arrays, application-specific integrated circuits, chipsets), or a combination thereof.

[0014] Malware Scan Trigger Generation

[0015] During operation, priority calculator 108 may detect a malware scan trigger 120 associated with a file 122. Malware scan trigger 120 may be generated when an attempt to access file 122 or an attempt to add file 122 to electronic device 100 is detected. In some examples, file 122 may be stored in a memory (not shown in FIG. 1) of electronic device 100. An application 124 executing in electronic device 100 may access file 122. When application 124 attempts to read file 122, file access interceptor 102 may intercept a read command associated with file 122 from application 124. In response to detecting the read command, file access interceptor 102 may generate malware scan trigger 120 and transmit malware scan trigger 120 to priority calculator 108. When application 124 attempts to write to file 122, file write observer 104 may intercept a write command associated with file 122 from application 124. In response to detecting the write command, file write observer 104 may generate malware scan trigger 120 and transmit malware scan trigger 120 to priority calculator 108.

[0016] In some examples, file 122 may be stored in an external storage device (not shown in FIG. 1), such as a flash memory storage device. When the external storage device is connected to electronic device 100, file indexer may index file 122 for electronic device 100. In response to attempting to index file

122, file indexer may generate malware scan trigger 120 and transmit malware scan trigger to priority calculator 108.

[0017] Scan Priority Determination

[0018] In response to detecting malware scan trigger 120, priority calculator 108 may determine a scan priority associated with file 122. Priority calculator 108 may compute a combined risk score to determine the scan priority. The combined risk score may be a numerical value that is determined based on a set of risk scores. In some examples, priority calculator 108 may determine the combined risk score based on an access risk score, a base risk score, a metadata risk score, a scan age risk score, or a combination thereof.

[0019] Access Risk Score

[0020] The access risk score may be determined based on a risk profile of an entity that attempts to access file 122. For example, behavioral detection engine 118 may generate a risk profile for application 124. The risk profile may indicate if application 124 is normal, suspicious, or malicious application. "Normal" may indicate that application 124 has a low likelihood of being a piece of malware application. "Suspicious" may indicate that application 124 has a medium likelihood (e.g., 50%) of being a piece of malware application. "Malicious" may indicate that application 124 has a high likelihood of being a piece of malware application. Behavioral detection engine 118 may generate a similar risk profile for an external storage device if file 122 is introduced to electronic device 100 via the external storage device.

[0021] When the risk profile is normal, priority calculator 108 may assign a first value to the access risk score. When the risk profile is suspicious, priority calculator 108 may assign a second value to the access risk score that is higher than the first value. When the risk profile is malicious, priority calculator 108 may assign third value to the access risk score that is higher than the second value.

[0022] Base Risk Score

[0023] The base risk score may be determined based on the source of malware scan trigger 120. In some examples, the source of malware scan trigger 120 may be the entity that generates malware scan trigger 120, such as file access interceptor 102, file write observer 104, and file indexer 106. When the source is file access interceptor 102, the base risk score may have a first value as assigned by priority calculator 108. When the source is file write observer 104, the base risk score may have a second value that is higher than the first value. When the source is file indexer 106, the base risk score may have a third value that is higher than the second value. The base risk score of each source may be arranged to reflect the potential risk of malware exposure associated with each source.

[0024] Metadata Risk Score

[0025] The metadata risk score may be determined based on metadata 126 associated with file 122. Metadata 126 may include any information related file 122 besides content of file 122. Priority calculator 108 may receive metadata 126 from metadata provider 114. In some examples, metadata 126 may include a first type of metadata corresponding to acquisition information of file 122. The acquisition information may describe where file 122 is acquired from, how file 122 is acquired, or a combination thereof.

[0026] In some examples, the acquisition information may describe a webpage that file 122 was downloaded from. The acquisition information may also describe how a user navigated to the webpage to download file 122 (e.g., whether the user searched for file 122 on a search engine or the user clicked on a link in an email to get file 122). Thus, priority calculator 108 may determine a value of metadata risk score based on how risky the webpage is and how risky the manner in which the user downloaded file 122. If the webpage is high risk (e.g., an Internet forum or a social network site) and the user downloaded file 122 from a link in the webpage, metadata risk score may have a first value. If the webpage is low risk (e.g., hosted on company intranet) and the user specifically searched for file 122, metadata risk score may have a second value different

from the first value. In some examples, the second value may be lower than the first value. In some examples, the second value may be higher than the first value.

[0027] In some examples, file 122 may be received as an email attachment. Thus, the acquisition information may describe the source of the email. Priority calculator 108 may determine a value of the metadata risk score based on the acquisition information. For example, priority calculator 108 may assign a first value to the metadata risk score if the email came from a first-time sender (i.e., high risk). Priority calculator 108 may assign a second value to the metadata risk score if the email came from a trusted source (i.e., low risk). Further, priority calculator 108 may further determine the value of the metadata risk score using routing information of the email, such as if the email passed the Domain Keys Identified Mail (DKIM) check (i.e., low risk if the email pass the DKIM check, high risk if the email did not pass the DKIM check).

[0028] In some examples, file 122 may be created by an application stored in electronic device 100. Thus, the acquisition information may include the type and/or identity of the application. Priority calculator 108 may determine the value of the metadata risk score using the acquisition information. For example, priority calculator 108 may assign a first value to the metadata risk score if the application is a file sharing application (i.e., high risk). Priority calculator 108 may assign a second value to the metadata risk score if the application is a desktop publishing application (i.e., low risk).

[0029] In some examples, metadata 126 may also include a second type of metadata corresponding to a security parameter of file 122. The security parameter may be digital signature information embedded in file 122. Priority calculator 108 may determine the value of the metadata risk score using the digital signature information. For example, priority calculator 108 may assign a first value to the metadata risk score if file 122 is not signed with a digital signature or is signed with an invalid digital signature (i.e., high risk). Priority calculator 108 may assign a second value to the metadata risk score if file 122 is signed with a valid digital signature from a trusted source (i.e., low risk), such as

an operating system provider. Thus, priority calculator 108 may determine the value of the metadata risk using the first type of metadata, the second type of metadata, or a combination thereof. Although one file metadata provider 114 is shown in FIG. 1, it should be understood that a plurality of file metadata providers may be used. Each distinct file metadata provider may provide a distinct type of metadata to priority calculator.

[0030] Scan Age Risk Score

[0031] The scan age risk score may be determined based on a length of time and the number of malware definition updates since a previous scan of file 122 (i.e., the last time file 122 was scanned for malware). For example, if file 122 is not on a recent scan list (indicating that file 122 was not scan in the latest malware scan) and there has been a malware definition update since the last time file 122 was scanned for malware (i.e., high risk), priority calculator 108 may assign a first value to the scan age risk score. If file 122 is not on the recent scan list (indicating that file 122 was not scanned in the latest batch of files scanned for malware) and there has been an update to the malware definition since the last time file 122 was scanned for malware (i.e., high risk), priority calculator 108 may assign a first value to the scan age risk score. If file 122 is on the recent scan list and there has not been a malware definition update since the last time file 122 was scanned for malware (i.e., low risk), priority calculator 108 may assign a second value to the scan age risk score. In some examples, malware scanner 112 may provide the recent scan list, information on malware definition update, or a combination thereof to priority calculator 108. In some examples, an operating system of electronic device 100 (not shown in FIG. 1) may provide the recent scan list, information on malware definition update, or a combination thereof to priority calculator 108.

[0032] Combined Risk Score

[0033] Priority calculator 108 may determine a value of the combined risk score based on the access risk score, the base risk score, the metadata risk

score, the scan age risk score, or a combination thereof. The values of the access risk score, the base risk score, the metadata risk score, and the scan age risk score may each be weighted to compute the value of the combined risk score. The weight of each of the scores may be different to reflect the level of risk the particular score represents. In some examples, the value of the combined risk score may be a sum of the weighted values of the access risk score, the base risk score, the metadata risk score, the scan age risk score, or the combination thereof. In some examples, the weights may also be adjustable. The weights may be adjustable manually by a user of electronic device 100, via a central management console, derived using machine learning based on historical data for previously known malicious files, etc.

[0034] Based on the value of the combined risk score, priority calculator 108 may determine a scan priority for file 122. For example, when the value of the combined risk score is within a first range (e.g., between 10 and 15), the scan priority may be a first scan priority. The first scan priority may represent high risk of malware exposure. For example, file 122 may have a high risk of malware exposure when file 122 has not been scanned yet and is being launched as a process. As another example, file 122 may have a high risk when file 122 is not scanned yet and is being loaded by another process for which section sync is created. As another example, file 122 may have a high risk when file 122 has been modified by a process that is flagged as suspicious or malicious.

[0035] When the value of the combined risk score is within a second range (e.g., between 5 and 9), the scan priority may be a second scan priority. The second scan priority may represent medium risk of malware exposure. As an example, file 122 may have a medium risk of malware exposure when file 122 is newly written by a process in electronic device 100 and is not being accessed by any process so far.

[0036] When the value of the combined risk score is within a third range (e.g., between 1 and 4), the scan priority may be a third scan priority. The third scan priority may represent low risk of malware exposure. As an example, file 122 may

have a low risk of malware exposure when file 122 is a headerless file, such as a text file, a database file, or log file, that is frequently updated by an application.

[0037] Malware Scan Queue

[0038] Malware scan queue 110 may store a list of files for malware scans by malware scanner 112. The list may be sorted by scan priority. When a file is to be scanned by malware scanner 112, such as file 122, the file may be removed from malware scan queue 110 to be scanned by malware scanner 112.

[0039] In some examples, malware scan queue 110 may remove a file for scanning based on user activity information provided by user activity detector 116 and a scan priority of the file. As described in more detail below, the user activity information may indicate if a user is actively interacting with electronic device 100. When the scan priority is the first priority (i.e., high risk) or the second priority (i.e., medium risk), malware scan queue 110 may remove the file for scanning regardless of the content of the user activity information. When the scan priority is the third priority (i.e., low risk), malware scan queue 110 may remove the file for scanning only when the user activity information indicates that the user is not actively interacting with electronic device 100; malware scan queue 110 may delay a malware scan of the file by keeping the file in malware scan queue 110 until the user activity information indicates that the user is no longer actively interacting with electronic device 100.

[0040] Malware Scanner

[0041] Malware scanner 112 may perform a set of malware scans on a file based on a scan priority of the file. In some examples, priority calculator 108 may determine a scan depth and a number of scans based on the scan priority. A scan depth may indicate how many levels of embedded / nested formats to scan for malware, how many malware detection rules to apply, how many forms of malicious behavior analysis to apply, other parameters associated with a malware scan, or a combination thereof.

[0042] When the scan priority is the first scan priority, priority calculator 108 may determine that the file, such as file 122, may be scanned immediately without delay by malware scanner 112 at a first scan depth. At the first scan depth, malware scanner 112 may use fewer detection rules (e.g., avoid scanning a word processing document with detection rules for malicious executable binary code) and may skip certain forms of analysis for malicious behavior (e.g., running executable code inside a sandbox environment in a virtual machine). Priority calculator 108 may also place the file in malware scan queue 110 for a second malware scan at a second scan depth at a subsequent time. Thus, malware scanner 112 may perform malware scan on the file twice, a first time at the first scan depth and a second time at the second scan depth, which is more thorough or in depth than the first scan depth.

[0043] When the scan priority is the second scan priority or the third scan priority, priority calculator 108 may place the file in malware scan queue 110 for scanning. Malware scanner 112 may perform malware scan on the file at the second scan depth. Thus, in some examples, when the scan priority is the second scan priority or the third scan priority, a single malware scan may be performed. In some examples, malware scanner 112 perform malware scan as a background task that has a lower input/output and/or processor priority than other user tasks executing on electronic device 100.

[0044] User Activity Detector

[0045] User activity detector 116 monitor aspects of electronic device 100 to determine if a user is actively interacting with electronic device 100. User activity detector 116 may generate user activity information and provide the user activity information to malware scan queue 110 to determine a timing of malware scan as described above. The user activity information may be any information that indicates if electronic device 100 is actively used by a user.

[0046] In some examples, the user activity information may include power source information of electronic device 100 that indicates whether electronic device 100 is powered by a battery or an alternate current (AC) adapter. Battery

power is a finite resource and if a user has disconnected electronic device 100 from a power source (e.g., the AC adapter) then the user does not expect electronic device 100 to drain the battery power unnecessarily, therefore if electronic device 100 is on battery power then electronic device 100 may be considered to be actively used by the user. If electronic device 100 is connected to the AC adapter, then the power source information may be ignored as the power source information alone may not be sufficient to indicate if the electronic device 100 is actively used by the user.

[0047] In some examples, the user activity information may include a status of a security mechanism of electronic device 100. The security mechanism may include a lock screen, a physical device lock, or any other device or processor executable instructions that block access to electronic device 100 (e.g., by disabling input devices of electronic device 100) or reduce functionalities of electronic device 100 (e.g., by disabling an input/output port of electronic device 100) without an entry of a password, biometrics, or other authentication measures. If the status of the security mechanism is active, then electronic device 100 may be considered to not be actively used by the user. If the status of the security mechanism is inactive, then electronic device 100 may be considered to be actively used by the user.

[0048] In some examples, the user activity information may include a window size displaying content of a foreground application that is executing on electronic device 100. A foreground application may be an application that is designated by an operating system of electronic device 100 as active (e.g., after being selected by a user of electronic device 100). If the window size of the foreground application is maximized, then electronic device 100 may be considered to be actively used by the user. If the window size is not maximized, then electronic device 100 may be considered to not be actively used by the user.

[0049] In some examples, the user activity information may include a status of an input device of electronic device 100. The input device may be a keyboard, a touchscreen, a microphone, a touchpad, or any other device that is suitable to receive an input from a user. If the status of the input device is active, then

electronic device 100 may be considered to be actively used by the user. If the status of the input device is inactive, then electronic device 100 may be considered to not be actively used by the user. An input device may be considered active if the input device has received an input within a time window (e.g., 1 minute). An input device may be considered inactive if the input device has not received an input within the time window.

[0050] Thus, the user activity information may include the power source information, the status of a security mechanism, the window size, the status of an input device, or a combination thereof.

[0051] FIG. 2 illustrates a method 200 of scanning for malware based on a scan priority of a file, according to an example. Method 200 may be implemented by electronic device 100 of FIG. 1.

[0052] Method 200 may include receiving a malware scan trigger, at step 202. For example, priority calculator 108 may receive malware scan trigger 120 from file access interceptor 102. Method 200 may also include determining a combined risk score, at step 204. For example, priority calculator 108 may determine a combined risk score based on the access risk score, the base risk score, the metadata risk score, the scan age risk score, or a combination thereof.

[0053] Method 200 may further include determining a scan priority, at step 206. For example, priority calculator 108 may determine the scan priority based on the combined risk score. Method 200 may further include performing a malware scan based on the scan priority, at step 208. For example, malware scanner 112 may perform a malware scan on file 122 based on the scan priority.

[0054] FIG. 3 illustrates an electronic device 300 to scan for malware based on a scan priority of a file, according to another example. Electronic device 300 may implement electronic device 100 of FIG. 1. Electronic device 300 may include a processor 302 and a computer-readable storage medium 304.

[0055] Processor 302 may be a central processing unit (CPU), a semiconductor-based microprocessor, an integrated circuit (e.g., a field-programmable gate array, an application-specific integrated circuit), and/or other hardware devices suitable for retrieval and execution of instructions stored

in a computer-readable storage medium. Computer-readable storage medium 304 may be any electronic, magnetic, optical, or other physical storage device that contains or stores executable instructions. Thus, computer-readable storage medium 304 may be, for example, Random Access Memory (RAM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), a storage device, an optical disc, etc. In some examples, computer-readable storage medium 304 may be a non-transitory storage medium, where the term “non-transitory” does not encompass transitory propagating signals. Computer-readable storage medium 304 may be encoded with a series of processor executable instructions 306, 308, and 310.

[0056] Combined risk score determining instructions 306 may determine a combined risk score of a file. For example, referring to FIG. 1, priority calculator 108 may determine a value of the combined risk score based on the access risk score, the base risk score, the metadata risk score, the scan age risk score, or a combination thereof. Scan priority determining instructions 308 may determine a scan priority based on the combined risk score. For example, referring to FIG. 1, priority calculator 108 may determine a scan priority associated with file 122 based on a combined risk score. Malware scanning instructions 310 may perform a malware scan on the file based on the scan priority. For example, referring to FIG. 1, malware scanner 112 may perform a malware scan on file 122 based on the scan priority associated with file 122.

[0057] FIG. 4 illustrates an electronic device 400 to scan for malware based on a scan priority of a file, according to another example. Electronic device 400 may implement electronic device 100 of FIG. 1. Electronic device 400 may include a processor 402 and a computer-readable storage medium 404. Processor 402 may be similar to processor 302 of FIG. 3. Computer-readable storage medium 404 may be similar to computer-readable storage medium 304 of FIG. 3. Computer-readable storage medium 404 may be encoded with instructions 406, 408, and 410.

[0058] Scan priority determining instructions 406 may determine a scan priority based on the combined risk score. For example, referring to FIG. 1,

priority calculator 108 may determine a scan priority associated with file 122 based on a combined risk score. Scan parameter determining instructions 408 may determine a scan depth and a number of scans based on the scan priority. For example, referring to FIG. 1, when the scan priority is the first scan priority, priority calculator 108 may determine that the file, such as file 122, may be scanned immediately without delay by malware scanner 112 at a first scan depth. Priority calculator 108 may also place the file in malware scan queue 110 for a second malware scan at a second scan depth at a subsequent time. When the scan priority is the second scan priority or the third scan priority, priority calculator 108 may place the file in malware scan queue 110 for scanning. Malware scanning instructions 410 may perform a set of malware scans on a file based on the scan parameters. For example, referring to FIG. 1, when the scan priority is the first priority, the set of malware scans may include a plurality of malware scans: a first scan at a first scan depth and a second subsequent scan at a second scan depth. When the scan priority is the second or third priority, the set of malware scans may include just a single scan at the second scan depth.

[0059] FIG. 5 illustrates an electronic device 500 to scan for malware based on a scan priority of a file, according to another example. Electronic device 500 may include a processor 502 and a computer-readable storage medium 504. Processor 502 may be similar to processor 302 of FIG. 3. Computer-readable storage medium 504 may be similar to computer-readable storage medium 304 of FIG. 3. Computer-readable storage medium 504 may be encoded with instructions 506, 508, and 510.

[0060] Scan priority determining instructions 506 may determine a scan priority based on the combined risk score. For example, referring to FIG. 1, priority calculator 108 may determine a scan priority associated with file 122 based on a combined risk score. User activity information determining instructions 508 may determine user activity information. For example, referring to FIG. 1, user activity detector 116 may generate user activity information and provide the user activity information to malware scan queue 110 to determine a timing of malware scan. Malware scan timing instructions 510 may determine if a

malware scan of a file is to be delayed based on the scan priority and the user activity information. For example, referring to FIG. 1, when the scan priority is the third priority (i.e., low risk), malware scan queue 110 may remove the file for scanning only when the user activity information indicates that the user is not actively interacting with electronic device 100; malware scan queue 110 may delay a malware scan of the file by keeping the file in malware scan queue 110 until the user activity information indicates that the user is no longer actively interacting with electronic device 100.

[0061] The use of "comprising", "including" or "having" are synonymous and variations thereof herein are meant to be inclusive or open-ended and do not exclude additional unrecited elements or method steps.

Claims

What is claimed is:

1. A non-transitory computer-readable storage medium comprising instructions that when executed cause a processor of an electronic device to:
in response to detecting a malware scan trigger associated with a file,
determine a combined risk score associated with the file based on metadata of the file and a source of the malware scan trigger, wherein the source includes a file access interceptor, a file write observer, and a file indexer;
determine a scan priority based on the combined risk score; and
perform a malware scan on the file based on the scan priority.
2. The non-transitory computer-readable storage medium of claim 1, where in the scan priority includes a first scan priority, a second scan priority, and a third scan priority.
3. The non-transitory computer-readable storage medium of claim 1, wherein the instructions when executed further cause the processor to:
determine a base risk score based on the source of the malware scan trigger;
determine a metadata risk score based on the metadata;
determine a scan age risk score based on a previous scan of the file; and
determine a combined risk score based on the base risk score, the metadata risk score, and the scan age risk score.
4. The non-transitory computer-readable storage medium of claim 3, wherein the base risk score has a first weight, the metadata risk score has a second weight, and the scan age risk score has a third weight.

5. The non-transitory computer-readable storage medium of claim 1, wherein the metadata includes a first type of metadata and a second type of metadata, wherein the instructions when executed further cause the processor to:

- determine an access risk score based on an entity that attempts to access the file;
- determine a base risk score based on the source of the malware scan trigger;
- determine a first metadata risk score based on the first type of metadata;
- determine a second metadata risk score based on the second type of metadata;
- determine a scan age risk score based on a previous scan of the file; and
- determine a combined risk score based on the access risk score, the base risk score, the first metadata risk score, the second metadata risk score, the scan age risk score, or a combination thereof.

6. The non-transitory computer-readable storage medium of claim 5, wherein the first metadata risk score is determined based on acquisition information of the file, and wherein the second metadata risk score is determined based on a security parameter of the file.

7. A non-transitory computer-readable storage medium comprising instructions that when executed cause a processor of an electronic device to:

- in response to detecting a malware scan trigger associated with a file,
 - determine a scan priority associated with the file based on metadata of the file;
- determine a scan depth and a number of scans based on the scan priority;
- and
- perform a set of malware scans on the file based on the scan depth and the number of scans.

8. The non-transitory computer-readable storage medium of claim 7, wherein the instructions when executed cause the processor to:

- when the scan priority is a first scan priority:
 - perform a first malware scan on the file having a first scan depth; and
 - perform a second malware scan on the file having a second scan depth, wherein the second scan depth is higher than the first scan depth, and wherein the second malware scan is subsequent to the first malware scan; and
- when the scan priority is a second scan priority that is lower than the first scan priority, perform a malware scan on the file having the second scan depth.

9. The non-transitory computer-readable storage medium of claim 7, wherein metadata includes a first type of metadata and a second type of metadata, and wherein the first type of metadata includes an application that generated or received the file, and wherein the second type of metadata includes digital signature information embedded in the file.

10. A non-transitory computer-readable storage medium comprising instructions that when executed cause a processor of an electronic device to:

- in response to detecting a malware scan trigger associated with a file,
 - determine a scan priority associated with the file based on metadata of the file;
- determine user activity information, wherein the user activity information indicates if a user actively interacting with the electronic device; and
- determine if a malware scan of the file is to be delayed based on the scan priority and the user activity information.

11. The non-transitory computer-readable storage medium of claim 10, wherein the user activity information includes power source information that indicates whether the electronic device is powered by a battery or an alternate current (AC) adapter.

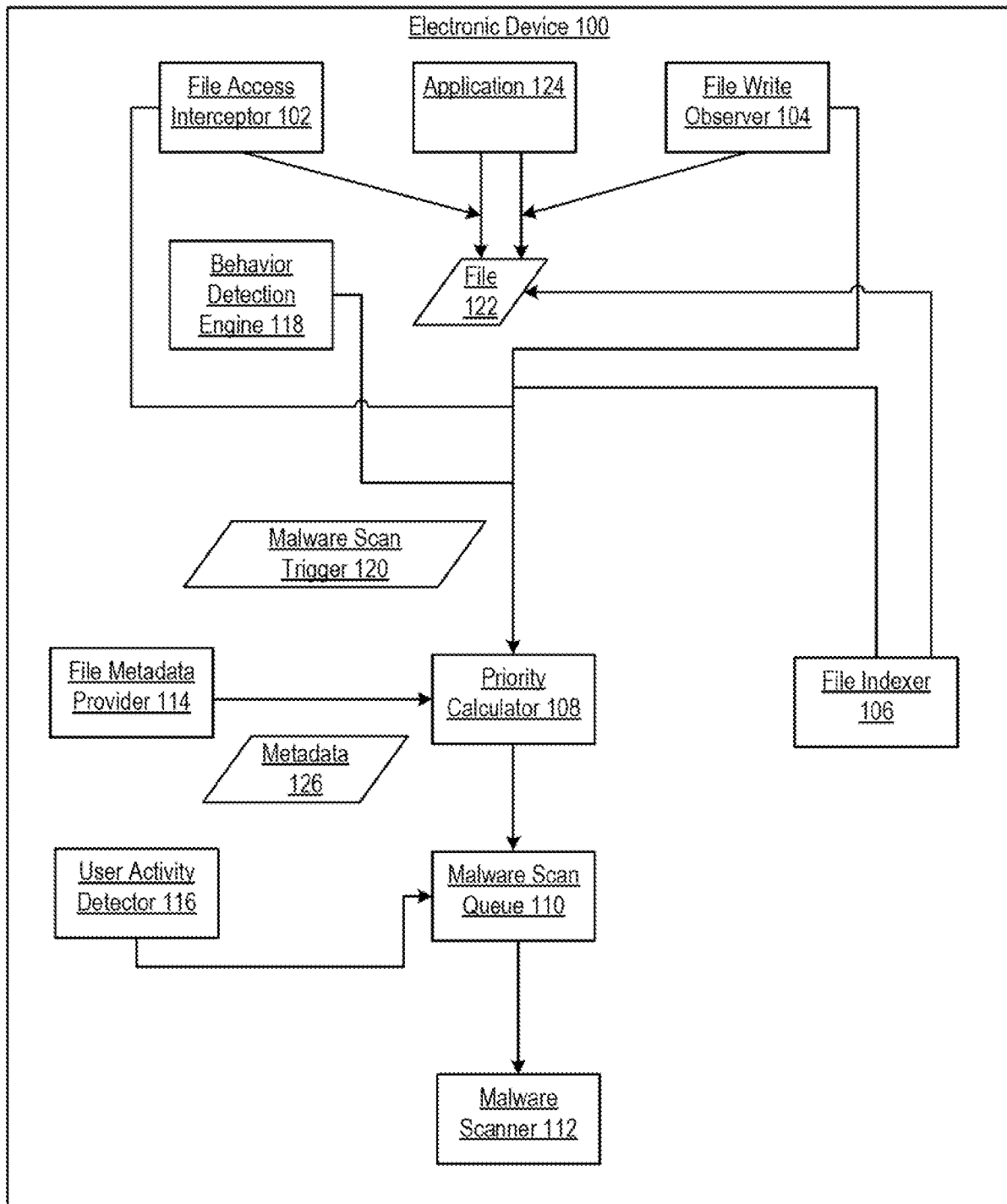
12. The non-transitory computer-readable storage medium of claim 10, wherein the user activity information includes a window size displaying content of a foreground application.

13. The non-transitory computer-readable storage medium of claim 10, wherein the user activity information includes a status of a lock screen.

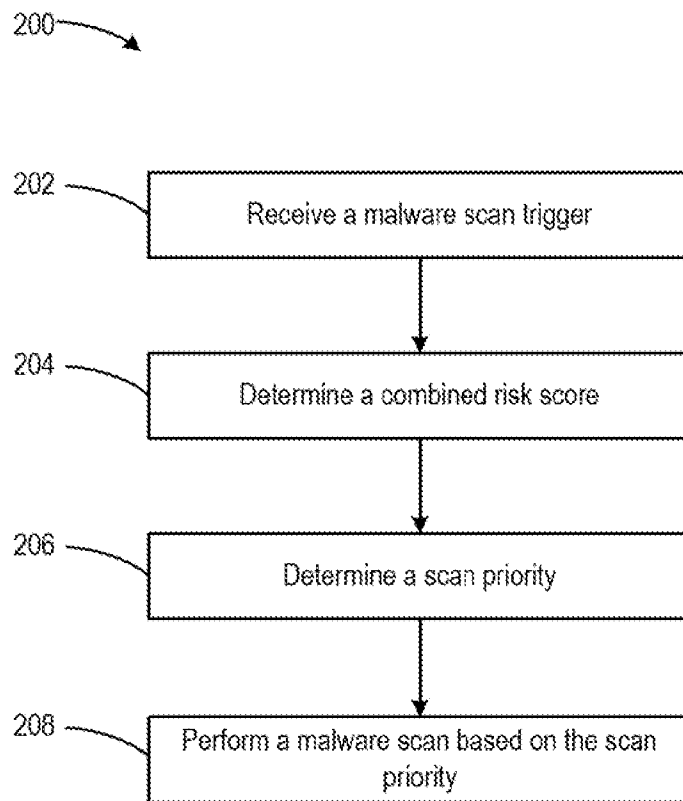
14. The non-transitory computer-readable storage medium of claim 10, wherein the user activity information includes a status of an input device of the electronic device.

15. The non-transitory computer-readable storage medium of claim 10, wherein the instructions when executed further cause the processor to:

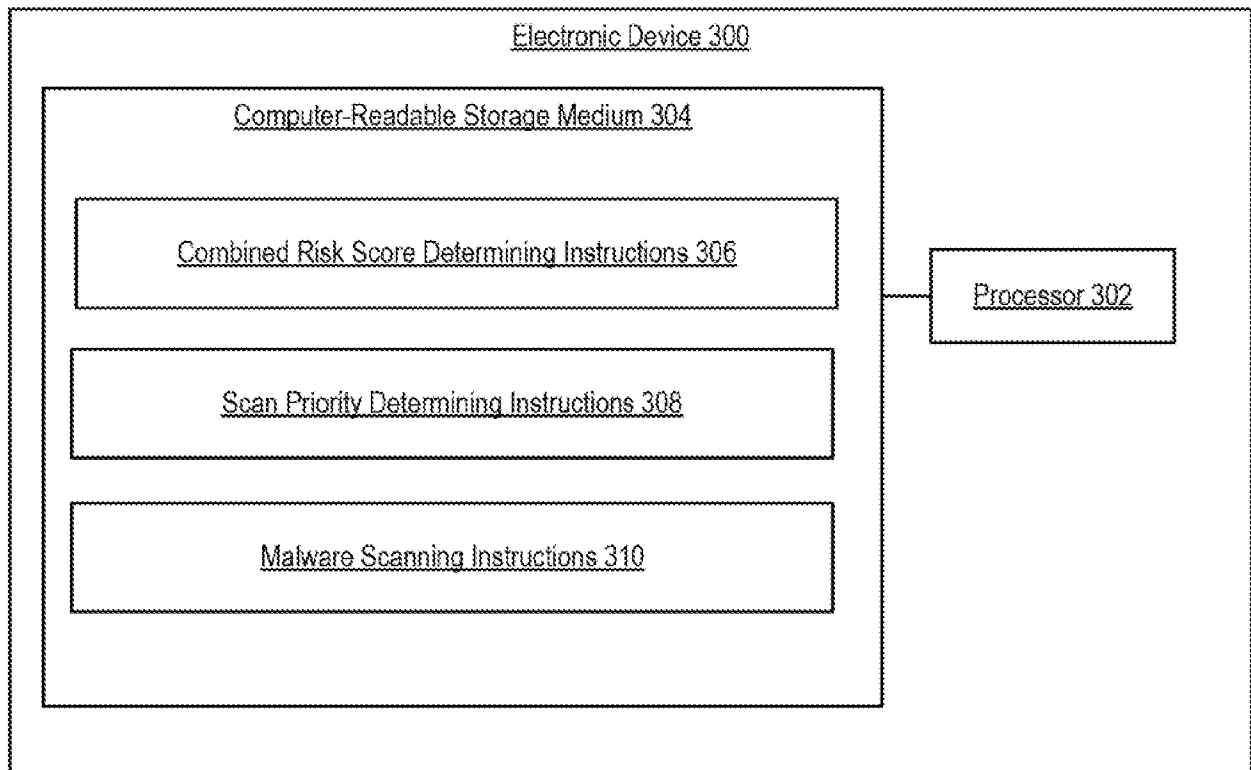
- when the scan priority is a first scan priority, perform the malware scan without delay; and
- when the scan priority is not the first scan priority and the user activity information indicates that the user is actively interacting with the electronic device, delay the malware scan until the user activity information indicates that the user is no longer actively interacting with the electronic device.

**FIG. 1**

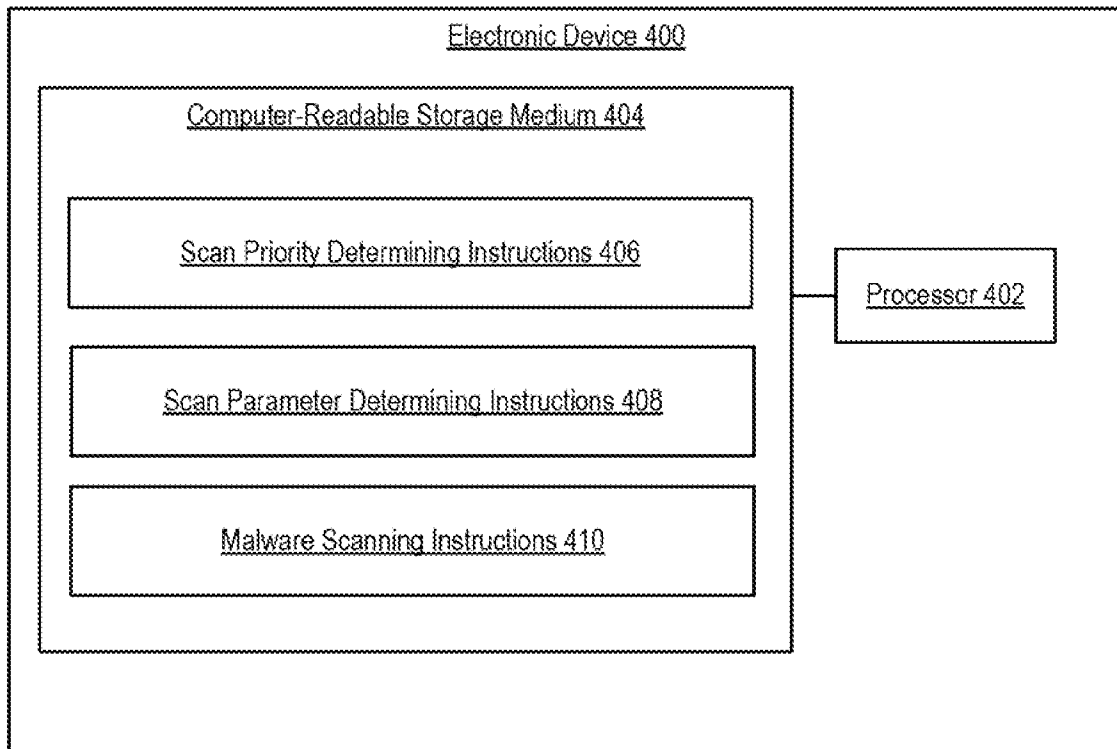
2/5

**FIG. 2**

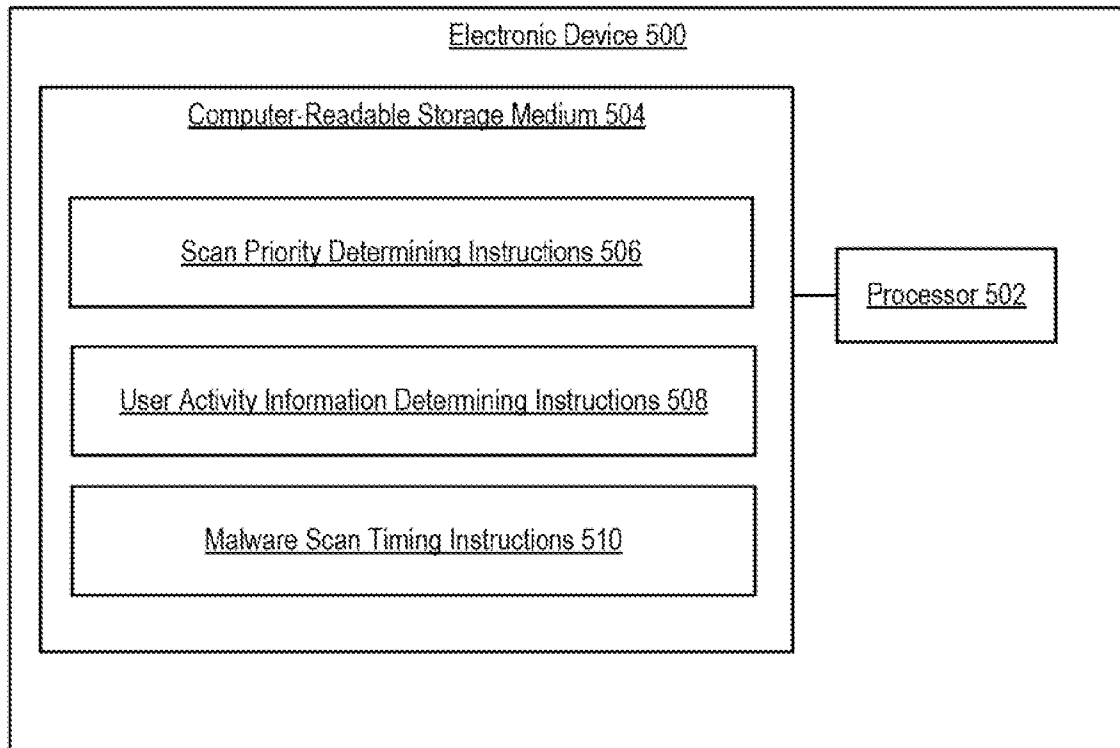
3/5

**FIG. 3**

4/5

**FIG. 4**

5/5

**FIG. 5**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2021/016994

A. CLASSIFICATION OF SUBJECT MATTER		
G06F 21/56 (2013.01)		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
G06F 11/00, 17/00, 21/00, 21/10, 21/50, 21/55, 21/56, G06N 99/00, H04L 29/00, 29/02, 29/06, 29/08		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
PatSearch (RUPTO Internal), USPTO, PAJ, Espacenet, Information Retrieval System of FIPS		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 10791138 B1 (FIREEYE INC.) 29.09.2020, column 4, lines 5-24, column 6, line 41-column 7, lines 16, 46-67, column 8, lines 30-54, column 9, lines 20-50, column 10, line 53-column 11, line 52, column 13, line 58-column 14, line 10, column 16, lines 39-57, column 18, lines 14-67, column 20, lines 19-67, column 24, line 57-column 25, line 16, column 27, lines 14-45, column 29, lines 4-33, 47-column 30, line 29	1-10
Y		11-15
Y	US 2017/0063888 A1 (SPLUNK INC) 02.03.2017, paragraphs [0175], [0182], [0272], [0316], [0350]-[0352], [0449], [0450], [0520]-[0522], [0539]	11-15
A	US 2016/0308944 A1 (DROPBOX INC) 20.10.2016	1-15
A	US 2011/0219451 A1 (RAYTHEON COMPANY) 08.09.2011	1-15
A	US 2018/0048657 A1 (NETSKOPE INC) 15.02.2018	1-15
☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.		
* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family	
"A" document defining the general state of the art which is not considered to be of particular relevance		
"D" document cited by the applicant in the international application		
"E" earlier document but published on or after the international filing date		
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)		
"O" document referring to an oral disclosure, use, exhibition or other means		
"P" document published prior to the international filing date but later than the priority date claimed		
Date of the actual completion of the international search	Date of mailing of the international search report	
08 October 2021 (08.10.2021)	28 October 2021 (28.10.2021)	
Name and mailing address of the ISA/RU: Federal Institute of Industrial Property, Berezhkovskaya nab., 30-1, Moscow, G-59, GSP-3, Russia, 125993 Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37	Authorized officer A. Kulikov Telephone No. 8(495)531-64-81	