

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号
WO 2019/223637 A1

(43) 国际公布日
2019 年 11 月 28 日 (28.11.2019)

(51) 国际专利分类号:
G06F 21/36 (2013.01)

(21) 国际申请号: PCT/CN2019/087565

(22) 国际申请日: 2019 年 5 月 20 日 (20.05.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810503125.4 2018 年 5 月 23 日 (23.05.2018) CN

(71) 申请人: 深信服科技股份有限公司 (SANGFOR TECHNOLOGIES INC.) [CN/CN]; 中国广东省深圳市南山区学苑大道 1001 号南山智园 A1 栋一层, Guangdong 518055 (CN)。

(72) 发明人: 刘彦南 (LIU, Yannan); 中国广东省深圳市南山区学苑大道 1001 号南山智园 A1 栋一层, Guangdong 518055 (CN)。

(74) 代理人: 深圳市深佳知识产权代理事务所 (普通合伙) (SHENPAT INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市罗湖区南湖街道春风路庐山大厦 B 座 18C2、18D、18E、18E2, Guangdong 518001 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): 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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(54) **Title:** MALICIOUS FILE DETECTION METHOD, APPARATUS AND DEVICE, AND COMPUTER-READABLE STORAGE MEDIUM

(54) 发明名称: 恶意文件检测方法、装置、设备及计算机可读存储介质

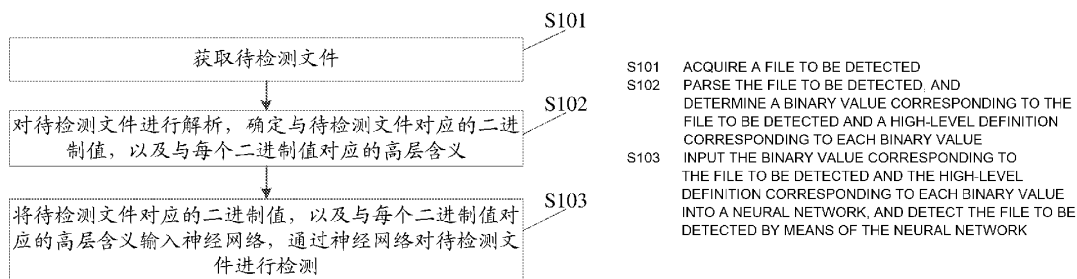


图 1

(57) **Abstract:** Provided are a malicious file detection method, apparatus and device, and a computer-readable storage medium. The method comprises: acquiring a file to be detected; parsing the file to be detected, and determining a binary value corresponding to the file to be detected and a high-level definition corresponding to each binary value, wherein the high-level definition is an additional attribute of the binary value; and inputting the binary value corresponding to the file to be detected and the high-level definition corresponding to each binary value into a neural network, and detecting the file to be detected by means of the neural network. It can be seen that in the present solution, when the file to be detected is detected, the binary value of the file is used, and the high-level definition corresponding to the binary value is further required to be used for comprehensive determination, thereby realizing determination of the file from multiple angles, and improving the accuracy of file detection and the effect of malicious file detection.

[见续页]

WO 2019/223637 A1

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (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)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 一种恶意文件检测方法、装置、设备及计算机可读存储介质, 包括: 获取待检测文件; 对所述待检测文件进行解析, 确定与所述待检测文件对应的二进制值, 以及与每个二进制值对应的高层含义; 其中, 所述高层含义为二进制值的附加属性; 将所述待检测文件对应的二进制值, 以及与每个二进制值对应的高层含义输入神经网络, 通过所述神经网络对所述待检测文件进行检测; 可见, 在本方案中, 在对待检测文件进行检测时, 不仅仅利用文件的二进制值, 还需要利用与二进制值对应的高层含义来进行综合判别, 从而实现了多种角度对文件进行判别, 提高了文件检测精度以及对恶意文件的检测效果。