

(12) МЕЖДУНАРОДНАЯ ЗАЯВКА, ОПУБЛИКОВАННАЯ В
СООТВЕТСТВИИ С ДОГОВОРом О ПАТЕНТНОЙ КООПЕРАЦИИ (РСТ)

(19) Всемирная Организация
Интеллектуальной Собственности
Международное бюро

(43) Дата международной публикации
26 августа 2021 (26.08.2021)



(10) Номер международной публикации
WO 2021/167483 A1

(51) Международная патентная классификация:
G06F 21/56 (2013.01) **G06F 16/00** (2019.01)

Сколково, Большой бульвар, 42, стр. 1, эт. 0, пом. 263
Москва, 121205, Moscow (RU).

(21) Номер международной заявки: РСТ/RU2020/000089
(22) Дата международной подачи:
25 февраля 2020 (25.02.2020)

(72) Изобретатель: ПРУДКОВСКИЙ, Николай Сергеевич (PRUDKOVSKIY, Nikolay Sergeevich); ул. Профсоюзная, 92, кв. 33 Москва, 117485, Moscow (RU).

(25) Язык подачи: Русский
(26) Язык публикации: Русский

(74) Агент: КОТЛОВ, Дмитрий Владимирович (KOTLOV, Dmitry Vladimirovich); ООО "ЦИС "Сколково", Территория инновационного центра "Сколково", д. 4, оф. 402.1 Москва, 143026, Moscow (RU).

(30) Данные о приоритете:
2020107922 21 февраля 2020 (21.02.2020) RU

(81) Указанные государства (если не указано иначе, для каждого вида национальной охраны): 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,

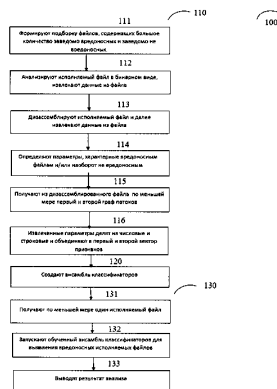
(71) Заявитель: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ГРУППА АЙБИ ТДС" (LIMITED LIABILITY COMPANY "GROUP IB TDS") [RU/RU]; территория Инновационного Центра

(54) Title: METHOD AND SYSTEM FOR DETECTING MALICIOUS FILES IN A NON-ISOLATED ENVIRONMENT

(54) Название изобретения: СПОСОБ И СИСТЕМА ВЫЯВЛЕНИЯ ВРЕДНОСНЫХ ФАЙЛОВ В НЕИЗОЛИРОВАННОЙ СРЕДЕ

(57) Abstract: The invention relates to the field of computing. A computer-implemented method comprises: a preparatory step in which: a selection of files is generated, containing a malicious executable file and a non-malicious executable file; an executable file is subjected to analysis, during which data is extracted from a binary form and from a disassembled form of the executable file, wherein, using a statistical method, parameters that are characteristic of malicious and/or, conversely, non-malicious files are additionally determined, and wherein a first flow graph and a second flow graph are additionally extracted; on the basis of the parameters obtained, a first attribute vector and a second attribute vector are constructed; and an ensemble of classifiers is formed from: a first classifier trained on the first attribute vector, a second classifier trained on the second attribute vector, a third classifier trained on the first flow graph, and a fourth classifier trained on the second flow graph, wherein a deciding priority is predetermined for each classifier; and a working step in which: an executable file is obtained; the ensemble of classifiers trained in the preparatory step is launched in order to identify malicious executable files; and the analysis results are displayed.

(57) Реферат: Изобретение относится к области вычислительной техники. Компьютерно-реализуемый способ содержит: подготовительный этап, на котором: формируют подборку файлов, которая содержит вредоносный исполняемый файл и не вредоносный исполняемый файл; анализируют исполняемый файл, при этом: извлекают данные из бинарного и дизассемблированного видов исполняемого файла, причем дополнительно статистическим методом определяют параметры, характерные вредоносным файлам и/или наоборот не вредоносным; причем дополнительно извлекают первый и второй граф потоков; на основе полученных параметров строятся первый и второй вектор признаков; создают ансамбль классификаторов из: первого обученного



Фиг. 2

- 111 Selection of files generated, containing a large number of files known to be malicious and a large number of files known to be non-malicious.
112 Executable file analyzed in binary form; data extracted from file.
113 Executable file disassembled and data further extracted from file.
114 Parameters characteristic of malicious files and/or, on the contrary, non-malicious files determined.
115 At least a first and a second flow graph obtained from disassembled file.
116 Extracted parameters split into number and line parameters and grouped into a first attribute vector and a second attribute vector.
120 Ensemble of classifiers generated.
121 At least one executable file obtained.
122 Trained ensemble of classifiers launched to identify malicious files.
123 Analysis results displayed.

WO 2021/167483 A1

[продолжение на следующей странице]

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) Указанные государства (если не указано иначе, для каждого вида региональной охраны): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), евразийский (AM, AZ, BY, KG, KZ, RU, TJ, TM), европейский патент (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).

Опубликована:

— с отчетом о международном поиске (статья 21.3)

классификатора на основе первого вектора признаков, второго обученного классификатора на основе второго вектора признаков; третьего классификатора, обученного на основе первого графа потоков, четвертого классификатора, обученного на втором графе потоков причем для каждого классификатора заранее определяют решающий приоритет; рабочий этап, на котором: получают исполняемый файл; запускают обученный на подготовительном этапе ансамбль классификаторов, для выявления вредоносных исполняемых файлов; выводят результат анализа.