

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

(19) Всемирная Организация
Интеллектуальной Собственности
Международное бюро

(43) Дата международной публикации
16 сентября 2021 (16.09.2021)



(10) Номер международной публикации
WO 2021/182986 A1

(51) Международная патентная классификация:
G06F 21/56 (2013.01) *G06N 20/20* (2019.01)

(21) Номер международной заявки: РСТ/RU2020/000140

(22) Дата международной подачи:
16 марта 2020 (16.03.2020)

(25) Язык подачи: Русский

(26) Язык публикации: Русский

(30) Данные о приоритете:
2020110068 10 марта 2020 (10.03.2020) RU

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

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

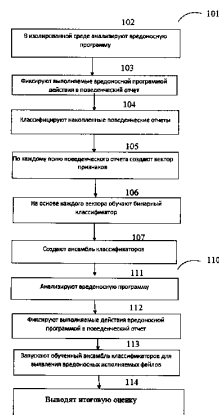
(72) Изобретатели: **ПРУДКОВСКИЙ, Николай Сергеевич (PRUDKOVSKIY, Nikolay Sergeevich)**; ул. Профсоюзная, 92, кв. 33 г. Москва, 117485, g. Moscow (RU).
ВОЛКОВ, Дмитрий Александрович (VOLKOV, Dmitry Aleksandrovich); ул. Генерала Белова, 29, корп. 2, кв. 113 Москва, 115563, Moscow (RU).

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

(54) Title: METHOD AND SYSTEM FOR SEARCHING FOR SIMILAR MALICIOUS PROGRAMS ON THE BASIS OF DYNAMIC ANALYSIS RESULTS

(54) Название изобретения: СПОСОБ И СИСТЕМА ПОИСКА СХОЖИХ ВРЕДНОСНЫХ ПРОГРАММ ПО РЕЗУЛЬТАТАМ ИХ ДИНАМИЧЕСКОГО АНАЛИЗА



Фиг.2

102 Analyzing a malicious program in an isolated environment
103 Recording the actions performed by the malicious program in a behavioural report
104 Classifying accumulated behavioural reports
105 Generating an attribute vector on the basis of each field of a behavioural report
106 Training a binary classifier on the basis of each vector
107 Creating an ensemble of classifiers
111 Analyzing a malicious program
112 Recording the actions performed by the malicious program in a behavioural report
113 Launching the trained ensemble of classifiers in order to detect malicious executable files
114 Displaying a final evaluation

(57) Abstract: The present technical solution relates to a method and system for searching for similar malicious programs on the basis of the results of a dynamic analysis thereof. The computer-implemented method comprises: a preparatory step that involves: analyzing malicious programs in an isolated environment; recording the actions performed by a malicious program in a behavioural report; dividing accumulated behavioural reports into groups, where a group comprises reports which contain similar actions and which relate to one known malware family; generating an attribute vector for a given known malware family on the basis of selected fields of a behavioural report; training a binary classifier on the basis of each of the resulting attribute vectors; and creating an ensemble of binary classifiers on the basis of the pre-trained binary classifiers; and a working step that involves: analyzing malicious programs; recording the actions performed by a malicious program in a behavioural report; launching the ensemble of binary classifiers trained in the preceding step; and forming, by means of said ensemble of binary classifiers, an evaluation as to whether the malicious program under analysis belongs to a known family of malicious programs.

(57) Реферат: Настоящее техническое решение относится к способу и системе поиска схожих вредоносных программ по результатам их динамического анализа. Компьютерно-реализуемый способ содержит: подготовительный этап, на котором: в изолированной среде анализируют вредоносные программы; фиксируют выполняемые вредоносной программой действия в поведенческом отчете; разделяют накопленные поведенческие отчеты таким образом, что в группе находятся отчеты, содержащие похожие действия и относящиеся к одному известному вредоносному семейству; по выбранным полям поведенческого отчета создается вектор признаков по данному известному вредоносному семейству; на основе каждого из полученных векторов признаков обучается бинарный классификатор; создают ансамбль бинарных классификаторов на основе ранее обученных бинарных классификаторов; и рабочий этап, на котором: анализируют вредоносные программы; фиксируют выполняемые вредоносной программой действия в поведенческом отчете; запускают обученный на

[продолжение на следующей странице]

WO 2021/182986 A1

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, 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 отчётом о международном поиске (статья 21.3)

подготовительном этапе ансамбль бинарных классификаторов; ансамбль бинарных классификаторов формирует итоговую оценку, что анализируемая вредоносная программа принадлежит к известному семейству вредоносных программ.