

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

(19) Всемирная Организация
Интеллектуальной Собственности
Международное бюро

(43) Дата международной публикации
05 августа 2021 (05.08.2021)



WIPO | PCT



(10) Номер международной публикации
WO 2021/154114 A1

(51) Международная патентная классификация:
G06F 21/56 (2013.01) *G06F 12/14* (2006.01)

(21) Номер международной заявки: PCT/RU2020/000044

(22) Дата международной подачи:
31 января 2020 (31.01.2020)

(25) Язык подачи: Русский

(26) Язык публикации: Русский

(30) Данные о приоритете:
2020103269 27 января 2020 (27.01.2020) RU

(71) Заявитель: **ОБЩЕСТВО С ОГРАНИЧЕННОЙ
ОТВЕТСТВЕННОСТЬЮ "ГРУППА АЙБИ ТДС"**
(**LIMITED LIABILITY COMPANY "GROUP IB
TDS"**) [RU/RU]; территория Инновационного Центра
Сколково, Большой бульвар, 42, стр. 1, эт. 0, пом. 263
Москва, 121205, Moscow (RU).

(72) Изобретатели: **ВОЛКОВ, Дмитрий Александрович**
(**VOLKOV, Dmitry Aleksandrovich**); ул. Генера-
ла Белова, 29, корп. 2, кв. 113 Москва, 115563,
Moscow (RU). **МИЛЕШИН, Филипп Алексеевич**
(**MILESHIN, Philipp Alekseevich**); пер. Бескудников-
ский, 1, корп. 1, кв. 3 Москва, 127474, Moscow (RU).

(74) Агент: **КОТЛОВ, Дмитрий Владимирович**
(**KOTLOV, Dmitry Vladimirovich**); ООО "ЦИС "Скол-

ково", Территория инновационного центра "Сколково",
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,
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)

(54) Title: METHOD AND SYSTEM FOR DETECTING AN INFRASTRUCTURE OF MALWARE OR A CYBERCRIMINAL

(54) Название изобретения: СПОСОБ И СИСТЕМА ВЫЯВЛЕНИЯ ИНФРАСТРУКТУРЫ ВРЕДНОСНОЙ ПРОГРАММЫ
ИЛИ КИБЕРЗЛОУМЫШЛЕННИКА

(57) Abstract: The claimed method for detecting an infrastructure of malware or a cybercriminal, comprises steps in which: a request is received comprising an infrastructure element and a tag for affiliating said element to malware or a cybercriminal; a parameter of the received infrastructure element, an additional infrastructure element used by the same malware or cybercriminal as the received infrastructure element and a parameter of the additional infrastructure element are extracted from a data base; the received infrastructure element and the parameter interconnected therewith and the additional infrastructure element and the parameter interconnected therewith are analyzed; on the basis of the analysis, statistical connections are identified between the parameter of the received infrastructure element and the parameter of the additional infrastructure element; rules for searching for new infrastructure elements of are formulated on the basis of the identified statistical connection; by means of a formulated rule, new infrastructure elements are extracted from the data base; the new elements are assigned tags corresponding to the specific malware or cybercriminals, and results are saved in the data base.

(57) Реферат: Заявленный способ выявления инфраструктуры вредоносной программы или киберзлоумышленника, содержащий этапы, на которых: получают запрос, содержащий элемент инфраструктуры и тэг о принадлежности данного элемента вредоносной программе или киберзлоумышленнику; извлекают из базы данных параметр полученного элемента инфраструктуры, дополнительный элемент инфраструктуры, используемый той же вредоносной программой или киберзлоумышленником, что и полученный элемент инфраструктуры, и параметр дополнительного элемента инфраструктуры; анализируют полученный элемент инфраструктуры и взаимосвязанный с ним параметр и дополнительный элемент инфраструктуры и взаимосвязанный с ним параметр; на основе анализа выявляют статистические связи между параметром полученного элемента инфраструктуры и параметром дополнительного элемента инфраструктуры; формируют правила поиска новых элементов инфраструктуры на основании выявленной статистической связи; извлекают, посредством сформированного правила, из базы данных новые элементы инфраструктуры; присваивают новым элементам тэги, соответствующие определенным вредоносным программам или киберзлоумышленникам, и сохраняют результаты в базе данных.

WO 2021/154114 A1