Title (en)

A COMPUTER-IMPLEMENTED METHOD, A SYSTEM AND A COMPUTER PROGRAM FOR IDENTIFYING A MALICIOUS FILE

Title (de)

COMPUTERIMPLEMENTIERTES VERFAHREN, SYSTEM UND COMPUTERPROGRAMM ZUM IDENTIFIZIEREN EINER BÖSARTIGEN DATEI

Title (fr)

PROCÉDÉ MIS EN OEUVRE PAR ORDINATEUR, SYSTÈME ET PROGRAMME INFORMATIQUE PERMETTANT D'IDENTIFIER UN FICHIER MALVEILLANT

Publication

EP 4004827 A1 20220601 (EN)

Application

EP 20744065 A 20200729

Priority

- EP 19382656 A 20190730
- EP 2020071334 W 20200729

Abstract (en)

[origin: WO2021018929A1] A computer-implemented method, a system and computer programs for identifying a malicious file are disclosed. The method comprises performing a static analysis of a potentially malicious file to obtain a set of features that provide an abstract view of the file; performing a static machine learning classification process using as inputs said set of features, to obtain a preliminary classification output; and performing a fuzzy inference procedure based on possibilistic logic using as input variables said set of features and said preliminary classification output, to generate an enhanced classification output that identifies the potentially malicious file as a malicious file or a benign file.

IPC 8 full level

G06N 3/08 (2006.01); **G06F 21/56** (2013.01); **G06N 3/04** (2006.01)

CPC (source: EP)

G06F 21/562 (2013.01); **G06N 3/043** (2023.01); **G06N 3/08** (2013.01); **G06N 5/048** (2013.01); **H04L 63/1416** (2013.01); **H04L 63/145** (2013.01); G06N 3/045 (2023.01)

Citation (search report)

See references of WO 2021018929A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

WO 2021018929 A1 20210204; EP 4004827 A1 20220601

DOCDB simple family (application)

EP 2020071334 W 20200729; EP 20744065 A 20200729