Title (en)

INLINE MALWARE DETECTION

Title (de)

INLINE-MALWARE-DETEKTION

Title (fr)

DÉTECTION DE LOGICIEL MALVEILLANT EN LIGNE

Publication

EP 3999985 A1 20220525 (EN)

Application

EP 20843721 A 20200706

Priority

- US 2020040928 W 20200706
- US 201916517465 A 20190719
- US 201916517463 A 20190719

Abstract (en)

[origin: WO2021015941A1] Detection of malicious files is disclosed. A set comprising one or more sample classification models is stored on a networked device. N-gram analysis is performed on a sequence of received packets associated with a received file. Performing the n-gram analysis includes using at least one stored sample classification model. A determination is made that the received file is malicious based at least in part on the n-gram analysis of the sequence of received packets. In response to determining that the file is malicious, propagation of the received file is prevented.

IPC 8 full level

G06F 21/56 (2013.01)

CPC (source: EP KR)

G06F 21/561 (2013.01 - EP KR); **G06N 20/00** (2019.01 - EP); **H04L 63/0227** (2013.01 - EP KR); **H04L 63/1416** (2013.01 - EP); **H04L 63/1425** (2013.01 - EP KR); **H04L 63/145** (2013.01 - EP KR)

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 2021015941 A1 20210128; CN 114072798 A 20220218; EP 3999985 A1 20220525; EP 3999985 A4 20231213; JP 2022541250 A 20220922; JP 2024023875 A 20240221; JP 7411775 B2 20240111; KR 102676386 B1 20240620; KR 20220053549 A 20220429

DOCDB simple family (application)

US 2020040928 W 20200706; CN 202080051255 A 20200706; EP 20843721 A 20200706; JP 2022502913 A 20200706; JP 2023218442 A 20231225; KR 20227001606 A 20200706