Title (en)

SYSTEMS AND METHODS FOR GENERATING NETWORK THREAT INTELLIGENCE

Title (de)

SYSTEME UND VERFAHREN ZUR ERZEUGUNG VON NETZWERKBEDROHUNGSINTELLIGENZ

Title (fr)

SYSTÈMES ET PROCÉDÉS DE GÉNÉRATION D'UNE INTELLIGENCE CONTRE LES MENACES DANS UN RÉSEAU

Publication

EP 3281116 A4 20180815 (EN)

Application

EP 16777161 A 20160406

Priority

- US 201514683964 A 20150410
- US 2016026131 W 20160406

Abstract (en)

[origin: WO2016164403A1] Implementations described and claimed herein provide systems and methods for generating threat intelligence based on network security data. In one implementation, a network traffic dataset representative of network traffic for an Internet Protocol address across one or more ports of a primary network is obtained. A content distribution network log associated with a content distribution network is obtained. The content distribution network log includes a history of content requests by the Internet Protocol address. The network traffic dataset is correlated with the content distribution network log based on the Internet Protocol address to obtain network security data. One or more threat attributes representative of malicious activity are identified from the network security data. The one or more threat attributes are weighted. Network threat intelligence is generated based on the weighted threat attributes using a processing cluster.

IPC 8 full level

G06F 12/00 (2006.01); **H04L 29/06** (2006.01); **H04W 12/12** (2009.01)

CPC (source: EP)

G06F 21/577 (2013.01); **H04L 63/1408** (2013.01); **H04L 63/1433** (2013.01); **H04L 63/1441** (2013.01); G06F 2221/034 (2013.01)

Citation (search report)

- [I] US 2013074143 A1 20130321 - BU ZHENG [US], et al
- [I] US 2013254260 A1 20130926 - STEVENS MATTHEW J [US], et al
- [A] US 2014059683 A1 20140227 - ASHLEY PAUL ANTHONY [AU]
- [A] US 2011173699 A1 20110714 - FIGLIN IGAL [IL], et al
- [A] US 8881281 B1 20141104 - MITCHELL DAVID JAMES [US]
- [A] MANOS ANTONAKAKIS ET AL: "Building a Dynamic Reputation System for DNS", USENIX,, 4 June 2010 (2010-06-04), pages 1 - 17, XP061011124
- See references of WO 2016164403A1

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

DOCDB simple family (publication)

WO 2016164403 A1 20161013; CA 2982107 A1 20161013; EP 3281116 A1 20180214; EP 3281116 A4 20180815; HK 1249603 A1 20181102

DOCDB simple family (application)

US 2016026131 W 20160406; CA 2982107 A 20160406; EP 16777161 A 20160406; HK 18108921 A 20180710