(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 963 577 B8**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Bibliography INID code(s) 73

(48) Corrigendum issued on:
01.01.2020 Bulletin 2020/01

(45) Date of publication and mention of the grant of the patent:
27.11.2019 Bulletin 2019/48

(21) Application number: **15175151.8**

(22) Date of filing: **02.07.2015**

(51) Int Cl.:
G06F 21/56 *(2013.01)* ***G06F 21/50*** *(2013.01)*
H04L 29/06 *(2006.01)* ***G06F 16/00*** *(2019.01)*

(54) METHOD FOR MALWARE ANALYSIS BASED ON DATA CLUSTERING

VERFAHREN ZUR SCHADSOFTWAREANALYSE BASIERT AUF DATEN-CLUSTERING

PROCÉDÉ D'ANALYSE MALWARE BASÉE SUR REGROUPEMENT DE DONNÉES

(84) Designated Contracting States:
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

(30) Priority: **03.07.2014 US 201462020876 P**
29.08.2014 US 201414473552
29.08.2014 US 201414473920
15.09.2014 US 201414486991
15.09.2014 US 201414487021

(43) Date of publication of application:
06.01.2016 Bulletin 2016/01

(60) Divisional application:
19210661.5
19210688.8

(73) Proprietor: **Palantir Technologies Inc.**
Palo Alto, CA 94301 (US)

(72) Inventors:
- **COHEN, David**
  Palo Alto, CA California 94301 (US)
- **MA, Jason**
  Palo Alto, CA California 94301 (US)
- **FU, Bing Jie**
  Palo Alto, CA California 94301 (US)
- **NEPOMNYASHCHIY, Ilya**
  Palo Alto, CA California 94301 (US)
- **BERLER, Steven**
  Palo Alto, CA California 94301 (US)
- **SMALIY, Alex**
  Palo Alto, CA California 94301 (US)
- **GROSSMAN, Jack**
  Palo Alto, CA California 94301 (US)
- **THOMPSON, James**
  Palo Alto, CA California 94301 (US)
- **BOORTZ, Julia**
  Palo Alto, CA California 94301 (US)
- **SPRAGUE, Matthew**
  Palo Alto, CA California 94301 (US)
- **MENON, Parvathy**
  Palo Alto, CA California 94301 (US)
- **KROSS, Michael**
  Palo Alto, CA California 94301 (US)
- **HARRIS, Michael**
  Palo Alto, CA California 94301 (US)
- **BOROCHOFF, Adam**
  Palo Alto, CA California 94301 (US)

Printed by Jouve, 75001 PARIS (FR)

(Cont. next page)

(74) Representative: **Sayer, Robert David**
Venner Shipley LLP
200 Aldersgate
London EC1A 4HD (GB)

(56) References cited:
US-B1- 8 788 407

- **SHI LIANG ET AL: "A Scalable Implementation of Malware Detection Based on Network Connection Behaviors", 2013 INTERNATIONAL CONFERENCE ON CYBER-ENABLED DISTRIBUTED COMPUTING AND KNOWLEDGE DISCOVERY, IEEE, 10 October 2013 (2013-10-10), pages 59-66, XP032534147, DOI: 10.1109/CYBERC.2013.19 [retrieved on 2013-12-16]**
- **RICHARD A NOLAN ET AL: "MCARTA: A Malicious Code Automated Run-Time Analysis framework", HOMELAND SECURITY (HST), 2012 IEEE CONFERENCE ON TECHNOLOGIES FOR, IEEE, 13 November 2012 (2012-11-13), pages 13-17, XP032330331, DOI: 10.1109/THS.2012.6459819 ISBN: 978-1-4673-2708-4**
- **ROBERTO PERDISCI ET AL: "Behavioral Clustering of HTTP-Based Malware and Signature Generation Using Malicious Network Traces", USENIX,, 18 March 2010 (2010-03-18), pages 1-14, XP061010768, [retrieved on 2010-03-18]**