



(51) International Patent Classification:

G06F 21/00 (2006.01) G06F 11/30 (2006.01)
G06F 21/20 (2006.01)

(21) International Application Number:

PCT/US2012/036760

(22) International Filing Date:

7 May 2012 (07.05.2012)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/483,613 6 May 2011 (06.05.2011) US

(71) Applicant (for all designated States except US): **UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL** [US/US]; 308 Bynum Hall, Campus Box 4105, Chapel Hill, NC 27599-4105 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SNOW, Kevin** [US/US]; Department Of Computer Science, Fred Brooks

Building/sitterson Hall, Campus Box 3175, Chapel Hill, NC 27599 (US). **MONROSE, Fabian** [US/US]; Department Of Computer Science, Fred Brooks Building/Sitterson Hall, Rm Fb356, CB 3175, Chapel Hill, NC 27599 (US). **KRISHNAN, Srinivas** [IN/US]; 605 Jones Ferry Rd., Apt. Mm12, Carrboro, NC 27510 (US).

(74) Agent: **HUNT, Gregory, A.**; Jenkins, Wilson, Taylor & Hunt, P.A., Suite 1200, University Tower, 3100 Tower Boulevard, Durham, NC 27707 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) Title: METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR DETECTING INJECTED MACHINE CODE

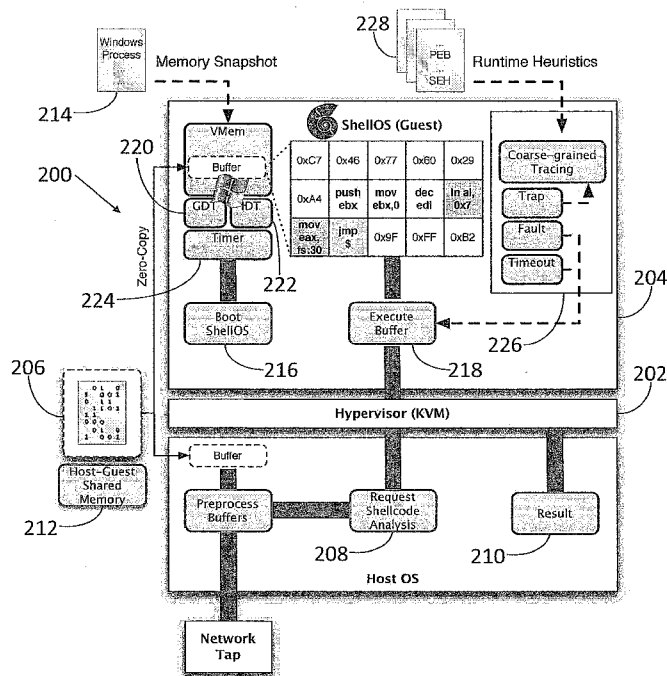


FIG. 2

(57) Abstract: According to one aspect, the subject matter described herein includes a method for detecting injected machine code. The method includes extracting data content from a buffer. The method also includes providing an operating system kernel configured to detect injected machine code. The method further includes executing, using the operating system kernel, the data content on a physical processor. The method further includes monitoring, using the operating system kernel, the execution of the data content to determine whether the data content contains injected machine code indicative of a code injection attack.



(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (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, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(88) Date of publication of the international search report:

21 March 2013

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/00(2006.01)i, G06F 21/20(2006.01)i, G06F 11/30(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/00; G06F 12/14; G06F 21/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: "code, injection, detect, buffer, malicious, kernel, monitor"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2009-0089497 A1 (BULYGIN YURIY et al.) 02 April 2009 See the abstrac, paragraphs 28-31, and figures 1-3.	1-25
A	US 2008-0040800 A1 (SEUNG BAE PARK) 14 February 2008 See the abstract, paragraphs 64-76, claim 1, and figure 3.	1-25
A	US 2008-0034429 A1 (JEROME L. SCHNEIDER) 07 February 2008 See the abstract, paragraphs 17-26, 39-41, claim 1, and figures 1, 5.	1-25
A	US 2010-0281273 A1 (LEE RUBY B. et al.) 04 November 2010 See the abstract, paragraphs 35-38, and figures 1-3.	1-25



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

22 NOVEMBER 2012 (22.11.2012)

Date of mailing of the international search report

23 NOVEMBER 2012 (23.11.2012)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan
City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Soak, Sang Moon

Telephone No. 82-42-481-8470



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2012/036760Patent document
cited in search reportPublication
datePatent family
member(s)Publication
date

US 2009-0089497 A1

02.04.2009

None

US 2008-0040800 A1

14.02.2008

None

US 2008-0034429 A1

07.02.2008

None

US 2010-0281273 A1

04.11.2010

None