(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2011 년 5 월 12 일 (12.05.2011)

PCT

(10) 국제공개번호
WO 2011/055945 A3

(51) 국제특허분류:
G06F 21/00 (2006.01) *H04L 12/22* (2006.01)

(21) 국제출원번호: PCT/KR2010/007608

(22) 국제출원일: 2010 년 11 월 1 일 (01.11.2010)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2009-0105344 2009 년 11 월 3 일 (03.11.2009) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **주식회사 안철수연구소 (AHNLAB., INC.)** [KR/KR]; 서울 영등포구 여의도동 12 CCMM 빌딩 6 층, 150-869 Seoul (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **오주현 (OH, Ju Hyun)** [KR/KR]; 서울 영등포구 대림 3 동 652 번지 성원아파트 101 동 1301 호, 150-073 Seoul (KR). **이창우 (LEE, Chang Woo)** [KR/KR]; 서울 마포구 공덕 2 동 175-100 203 호, 121-802 Seoul (KR). **박종필 (PARK, Chong Phil)** [KR/KR]; 서울 동작구 상도 1 동 522 번지 314 호, 156-031 Seoul (KR).

(74) 대리인: **장성구 (JANG, Seong Ku)**; 서울 서초구 양재동 275-7 번지 트러스트타워 19 층, 137-130 Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): 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, 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, RO, RS, RU, 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.

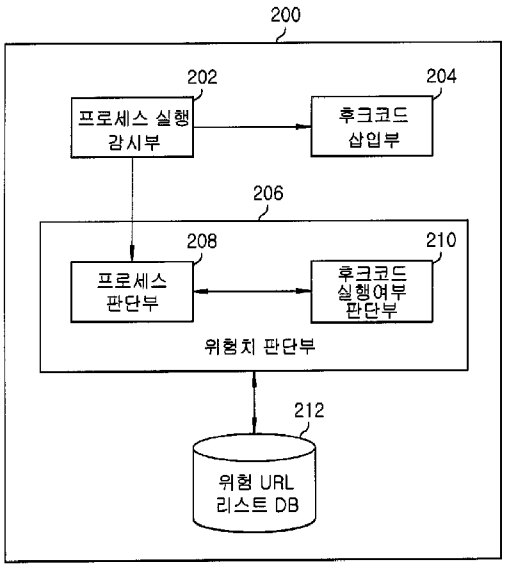
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

[다음 쪽 계속]

(54) **Title**: APPARATUS AND METHOD FOR DETECTING MALICIOUS SITES

(54) **발명의 명칭** : 악성 사이트 검출 장치 및 방법

[Fig. 2]



202 ... Process execution monitoring unit
204 ... Hook code insertion unit
206 ... Danger level determining unit
208 ... Process determining unit
210 ... Hook code execution determining unit
212 ... Dangerous URL list DB

(57) **Abstract**: The invention relates to an apparatus for detecting malicious sites, comprising: a monitoring unit for monitoring all processes being executed in a computing apparatus; a hook code insertion unit for inserting a hook code in a process executed in a browser when the execution of the browser is detected by the monitoring unit; a danger level determining unit that, upon the detection of a website movement, uses the hook code to inspect a stack structure of a process implemented according to the website movement and determine whether or not to perform the stack structure inspection, and determines whether or not the website to which the movement has been made is a malicious site; and a database for storing a list of sites determined to be malicious.

(57) **요약서**: 악성 사이트 검출 장치는, 컴퓨팅 장치 내에서 실행되는 모든 프로세스를 감시하는 감시부와, 상기 감시부에 의해 브라우저의 실행이 검지된 경우, 브라우저에서 실행되는 프로세스에 후크 코드를 삽입하는 후크 코드 삽입부와, 웹사이트의 이동이 검지될 경우, 상기 후크 코드를 이용하여, 웹사이트의 이동에 따라 발생되는 프로세스의 스택 구조를 검사하고 상기 스택 구조 검사의 수행 여부를 판단하여, 이동한 웹사이트가 악성 사이트인지 아닌지를 판단하는 위험치 판단부와, 판단된 악성 사이트 목록이 저장되는 데이터베이스를 포함한다.

WO 2011/055945 A3

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).

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

(88) 국제조사보고서 공개일: 2011 년 11 월 3 일

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2010/007608

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00(2006.01)i, H04L 12/22(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 11/30; G06F 15/00; G06F 17/60; G06F 11/08; G06F 11/36; G06F 11/00; 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: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

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

eKOMPASS (KIPO internal) & Keywords: process, hook, browser, site, insertion, stack, risk, mal*, code, hooking, stack, factor, level

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2009-0111416 A (AHNLAB, INC.) 27 October 2009 Abstract, pages 5-8, figures 4,6	1,7,13
Y	JP 2003-337797 A (NEC CORP) 28 November 2003 Abstract, paragraphs [0038]-[0058], figure 2	1,7,13
A	KR 10-2008-0043201 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 16 May 2008 Abstract, pages 4-5, claims 1-3, figures 1,2	1-13
A	KR 10-2009-0096823 A (AHNLAB, INC.) 15 September 2009 Abstract, pages 3-5, figure 2	1-13
A	KR 10-2004-0098902 A (AHNLAB, INC.) 26 November 2004 Abstract, pages 3-5, claim 6, figures 1,2	1-13
A	KR 10-2004-0104112 A (AHNLAB, INC.) 10 December 2004 Abstract, page 3, figures 1,2	1-13

☐ 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 another 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	Date of mailing of the international search report
23 JUNE 2011 (23.06.2011)	**23 JUNE 2011 (23.06.2011)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2010/007608

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2009-0111416 A	27.10.2009	NONE	
JP 2003-337797 A	28.11.2003	JP 4052007 B2	27.02.2008
KR 10-2008-0043201 A	16.05.2008	US 2008-0115219 A1	15.05.2008
KR 10-2009-0096823 A	15.09.2009	NONE	
KR 10-2004-0098902 A	26.11.2004	NONE	
KR 10-2004-0104112 A	10.12.2004	NONE	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2010/007608

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/00(2006.01)i, H04L 12/22(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06F 21/00; G06F 11/30; G06F 15/00; G06F 17/60; G06F 11/08; G06F 11/36; G06F 11/00; G06F 21/22

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 프로세스, 후크, 브라우저, 사이트, 삽입, 스택, 위험치, mal*, code, hooking, stack, factor, level

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2009-0111416 A (주식회사 안철수연구소) 2009.10.27 요약문, 페이지 5-8, 도면 4,6	1,7,13
Y	JP 2003-337797 A (NEC CORP) 2003.11.28 요약문, 단락[0038]-[0058], 도면 2	1,7,13
A	KR 10-2008-0043201 A (한국전자통신연구원) 2008.05.16 요약문, 페이지 4-5, 청구항 1-3, 도면 1,2	1-13
A	KR 10-2009-0096823 A (주식회사 안철수연구소) 2009.09.15 요약문, 페이지 3-5, 도면 2	1-13
A	KR 10-2004-0098902 A (주식회사 안철수연구소) 2004.11.26 요약문, 페이지 3-5, 청구항 6, 도면 1,2	1-13
A	KR 10-2004-0104112 A (주식회사 안철수연구소) 2004.12.10 요약문, 페이지 3, 도면 1,2	1-13

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2011년 06월 23일 (23.06.2011)	**2011년 06월 23일 (23.06.2011)**

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
정부대전청사
팩스 번호 82-42-472-7140

심사관
경연정
전화번호 82-42-481-8536

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2010/007608

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2009-0111416 A	2009.10.27	없음	
JP 2003-337797 A	2003.11.28	JP 4052007 B2	2008.02.27
KR 10-2008-0043201 A	2008.05.16	US 2008-0115219 A1	2008.05.15
KR 10-2009-0096823 A	2009.09.15	없음	
KR 10-2004-0098902 A	2004.11.26	없음	
KR 10-2004-0104112 A	2004.12.10	없음	