

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국



(43) 국제공개일
2011년 1월 6일 (06.01.2011)

PCT

(10) 국제공개번호
WO 2011/002146 A3

- (51) 국제특허분류:
G06F 21/00 (2006.01) G06F 11/00 (2006.01)
- (21) 국제출원번호: PCT/KR2010/002375
- (22) 국제출원일: 2010년 4월 16일 (16.04.2010)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2009-0058960 2009년 6월 30일 (30.06.2009) KR
- (71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여):
(주)잉카인터넷 (INCA INTERNET CO., LTD.) [KR/KR]; 서울특별시 구로구 구로 3동 235-2 에이스하이엔드타워 1201호, 152-740 Seoul (KR).
- (72) 발명자: 김
(75) 발명자/출원인 (US 에 한하여): 김윤동 (KIM, Yun Dong) [KR/KR]; 인천광역시 부평구 갈산동 갈산주공 1단지 108동 303호, 403-080 Incheon (KR). 서성원 (SEO, Seong Won) [KR/KR]; 경기도 고양시 덕양구 성사2동 신원당 8단지아파트 802동 407호, 412-714 Gyeonggi-do (KR). 연성호 (YEON, Seong Ho) [KR/KR]; 서울특별시 구로구 구로 3동 792-107 대영아파트 402호, 152-875 Seoul (KR). 이지남 (LEE, Ji Nam) [KR/KR]; 서울특별시 관악구 신림 7동 673-43, 151-015 Seoul (KR). 정영석 (JUNG, Young Suk) [KR/

KR]; 경기도 안양시 만안구 박달 2동 대림한숲타운 105동 102호, 430-702 Gyeonggi-do (KR). 한명호 (HAN, Myeong Ho) [KR/KR]; 서울특별시 동대문구 휘경 2동 동성빌라 30동 302호, 130-092 Seoul (KR). 최재영 (CHOE, Jae Young) [KR/KR]; 대구광역시 동구 신암동 603-154, 701-010 Daegu (KR). 이재홍 (LEE, Jae Hong) [KR/KR]; 서울특별시 구로구 구로 3동 1130-26 503호, 152-880 Seoul (KR).

(74) 대리인: 전영일 (JEON, Young Il); 서울특별시 강남구 삼성동 무역센터 트레이드타워 1306호 코엑스국제특허법률사무소, 135-729 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.

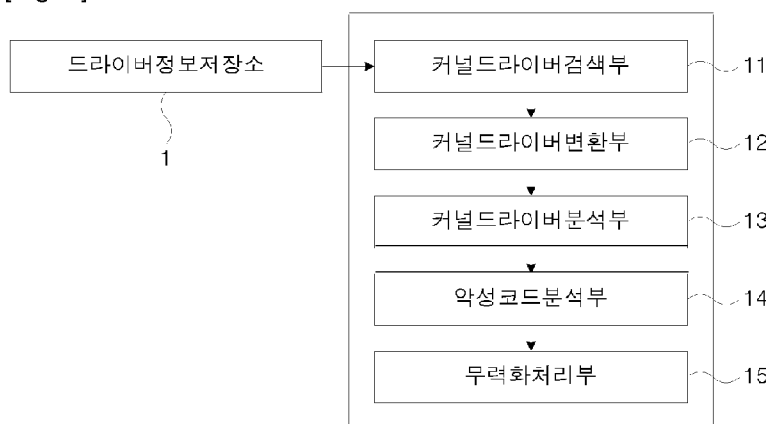
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[다음 쪽 계속]

(54) Title: SYSTEM AND METHOD FOR DETECTING MALICIOUS CODE

(54) 발명의 명칭: 악성코드 탐지시스템 및 방법

[Fig. 1]



- 1 ... Driver information storage
11 ... Kernel driver searcher
12 ... Kernel driver converter
13 ... Kernel driver Analyzer
14 ... Malicious code analyzer
15 ... Incapacitation processor

(57) Abstract: The present invention relates to a system and method which accurately detect whether or not an arbitrary application program includes malicious code by applying a heuristic technique. A system for detecting malicious code according to the present invention includes a kernel driver searcher that selects a search target driver, a kernel driver converter that checks API functions used by the search target driver, a kernel driver analyzer that analyzes whether or not a suspected malicious code API is included in the API functions used by the search target driver, and a malicious code analyzer that disassembles the suspected malicious code API used by the search target driver and a parameter value to analyze whether or not the suspected malicious code API is a malicious code API.

(57) 요약서: 이 발명은 경험적(heuristic) 기법을 적용하여 임의의 응용프로그램이 악성코드를 포함하는지 여부를 정확하게 탐지하는 시스템 및 방법에 관한 것이다. 이 발명에 따른 악성코드

탐지시스템은, 검사대상드라이버를 선택하는 커널드라이버검색부와, 상기 검사대상드라이버가 사용하고 있는 API 함수들을 확인하는 커널드라이버변환부와, 상기 검사대상드라이버가 사용하고 있는 API 함수들 중 악성코드의 의심 API가 포함되어 있는지를 분석하는 커널드라이버분석부와, 상기 검사대상드라이버가 사용하고 있는 악성코드의 의심 API 및 파라미터값을 디어셈블링하여 상기 악성코드의 의심 API가 악성코드 API 인지 분석하는 악성코드분석부를 포함한다.



ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— 청구범위 보정 기한 만료 전의 공개이며, 보정서를 접수하는 경우 그에 관하여 별도 공개함 (규칙 48.2(h))

(88) 국제조사보고서 공개일:

2011년 2월 17일

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2010/002375**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/00(2006.01)i, G06F 11/00(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 15/16; H04J 3/22; H04B 7/02

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: heuristic, experience, malignant code, virus, malware, middle finger, force, kernel, detection, API

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2004-0080845 A (AHNLAB, INC. et al.) 20 September 2004 Abstract, pages 3-5	1,2,4,5,7,8,10,12 ,13,15
Y	KR 10-2004-0083409 A (SAFEI CO., LTD.) 01 October 2004 Abstract, pages 6-7, figure 1	1,2,4,5,7,8,10,12 ,13,15
Y	WO 01-25870 A2 (INFRAWORKS CORPORATION et al.) 12 April 2001 Abstract, page 3 line 25 - page 12 line 8, figures 1-3	1,2,4,5,7,8,10,12 ,13,15
A	KR 10-2009-0025146 A (LIONIC CORPORATION) 10 March 2009 Abstract, paragraphs [0005], [0013]-[0018], figures 4, 5	1-16
A	KR 10-0628869 B1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 27 September 2006 Abstract, claims 1-5, page 3	1-16
A	US 2006-0021054 A1 (COSTA et al.) 26 January 2006 Abstract, paragraphs [0028]-[0034], [0109]-[0123], figures 1, 7, 16	1-16
A	WO 2004-003710 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V. et al.) 08 January 2004 Abstract, pages 6, 7	1-16



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

03 DECEMBER 2010 (03.12.2010)

Date of mailing of the international search report

06 DECEMBER 2010 (06.12.2010)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2010/002375

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-0666562 B1 (WAREPLUS CO., LTD. et al.) 09 January 2007 Abstract, pages 3-6, figures 2, 3	1-16

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2010/002375

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2004-0080845 A	20.09.2004	US 2004-0205411 A1	14.10.2004
KR 10-2004-0083409 A	01.10.2004	NONE	
WO 01-25870 A2	12.04.2001	AU 2000-76227 A1	10.05.2001
		AU 2000-77356 A1	10.05.2001
		AU 2000-77357 A1	10.05.2001
		AU 2000-77359 A1	10.05.2001
		AU 2000-77360 A1	10.05.2001
		AU 2000-77383 A1	10.05.2001
		AU 2000-77385 A1	10.05.2001
		AU 2000-78407 A1	10.05.2001
		AU 2001-13296 A1	10.05.2001
		AU 2001-14309 A1	10.05.2001
		CA 2352948-A1	12.04.2001
		CN 1345497 A0	17.04.2002
		EP 1183585 A2	06.03.2002
		JP 2003-511752 A	25.03.2003
		KR 10-2001-0109271 A	08.12.2001
		US 6553466 B1	22.04.2003
		US 6804784 B1	12.10.2004
		US 6986058 B1	10.01.2006
		US 7039806 B1	02.05.2006
		US 7096326 B1	22.08.2006
		US 7103783 B1	05.09.2006
		US 7484245 B1	27.01.2009
		WO 01-25870 A3	12.04.2001
		WO 01-25922 A1	12.04.2001
		WO 01-25925 A1	12.04.2001
		WO 01-25928 A1	12.04.2001
		WO 01-25930 A1	12.04.2001
		WO 01-25932 A1	12.04.2001
		WO 01-25937 A1	12.04.2001
		WO 01-25953 A1	12.04.2001
		WO 01-26276 A1	12.04.2001
		WO 01-26277 A1	12.04.2001
KR 10-2009-0025146 A	10.03.2009	CN 101382979 A	11.03.2009
		EP 2037384 A1	18.03.2009
		JP 2009-064443 A	26.03.2009
		US 2009-0064337 A1	05.03.2009
KR 10-0628869 B1	27.09.2006	US 2006-0129603 A1	15.06.2006
US 2006-0021054 A1	26.01.2006	CN 1725759 A	25.01.2006
		EP 1630710 A2	01.03.2006
		JP 2006-031718 A	02.02.2006
		KR 10-2006-0092832 A	23.08.2006
		US 2006-0031933 A1	09.02.2006

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2010/002375

Patent document cited in search report	Publication date	Patent family member	Publication date
WO 2004-003710 A1	08.01.2004	US 2006-021054 A1	26.01.2006
		US 2007-0006314 A1	04.01.2007
		US 7603715 B2	13.10.2009
		US 7634812 B2	15.12.2009
		US 7634813 B2	15.12.2009
		AU 2003-244947 A1	19.01.2004
		CN 1666163 A	07.09.2005
		CN 1666163 C0	25.06.2008
		EP 1520219 A1	06.04.2005
		EP 1520219 B1	03.11.2010
KR 10-0666562 B1	09.01.2007	JP 04-519642 B2	28.05.2010
		JP 2005-531079 A	13.10.2005
		KR 10-0947878 B1	17.03.2010
		US 2004-0003277 A1	01.01.2004
		US 7743257 B2	22.06.2010
		WO 2004-003710 A1	08.01.2004
		NONE	

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/00(2006.01)i, G06F 11/00(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/00; G06F 15/16; H04J 3/22; H04B 7/02

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: heuristic, 경험, 악성코드, 바이러스, 멀웨어, 중지, 무력, 커널, 탐지, API

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2004-0080845 A (주식회사 안철수연구소 외 1명) 2004.09.20 요약문, 페이지 3-5	1,2,4,5,7,8,10,12,13,15
Y	KR 10-2004-0083409 A ((주) 세이프아이) 2004.10.01 요약문, 페이지 6-7, 도면 1	1,2,4,5,7,8,10,12,13,15
Y	WO 01-25870 A2 (INFRAWORKS CORPORATION 외 3명) 2001.04.12 요약문, 페이지3 라인 25 - 페이지12 라인 8, 도면 1-3	1,2,4,5,7,8,10,12,13,15
A	KR 10-2009-0025146 A (라이오닉 코퍼레이션) 2009.03.10 요약문, 단락 [0005],[0013]-[0018], 도면 4,5	1-16
A	KR 10-0628869 B1 (한국전자통신연구원) 2006.09.27 요약문, 청구항 1-5, 페이지 3	1-16
A	US 2006-0021054 A1 (COSTA et al.) 2006.01.26 요약문, 단락[0028]-[0034],[0109]-[0123], 도면 1,7,16	1-16
A	WO 2004-003710 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V. 외 1명) 2004.01.08 요약문, 페이지 6,7	1-16

☒ 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

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

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

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

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

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

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

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2010년 12월 03일 (03.12.2010)

국제조사보고서 발송일

2010년 12월 06일 (06.12.2010)

ISA/KR의 명칭 및 우편주소

 대한민국 특허청
(302-701) 대전광역시 서구 선사로 139,
정부대전청사
팩스 번호 82-42-472-7140

심사관

정연정

전화번호 82-42-481-8536



C (계속). 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-0666562 B1 (주식회사 웨어플러스 외 1명) 2007.01.09 요약문, 페이지 3-6, 도면 2,3	1-16

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2004-0080845 A	2004.09.20	US 2004-0205411 A1	2004.10.14
KR 10-2004-0083409 A	2004.10.01	없음	
WO 01-25870 A2	2001.04.12	AU 2000-76227 A1	2001.05.10
		AU 2000-77356 A1	2001.05.10
		AU 2000-77357 A1	2001.05.10
		AU 2000-77359 A1	2001.05.10
		AU 2000-77360 A1	2001.05.10
		AU 2000-77383 A1	2001.05.10
		AU 2000-77385 A1	2001.05.10
		AU 2000-78407 A1	2001.05.10
		AU 2001-13296 A1	2001.05.10
		AU 2001-14309 A1	2001.05.10
		CA 2352948-A1	2001.04.12
		CN 1345497 A0	2002.04.17
		EP 1183585 A2	2002.03.06
		JP 2003-511752 A	2003.03.25
		KR 10-2001-0109271 A	2001.12.08
		US 6553466 B1	2003.04.22
		US 6804784 B1	2004.10.12
		US 6986058 B1	2006.01.10
		US 7039806 B1	2006.05.02
		US 7096326 B1	2006.08.22
		US 7103783 B1	2006.09.05
		US 7484245 B1	2009.01.27
		WO 01-25870 A3	2001.04.12
		WO 01-25922 A1	2001.04.12
		WO 01-25925 A1	2001.04.12
		WO 01-25928 A1	2001.04.12
		WO 01-25930 A1	2001.04.12
		WO 01-25932 A1	2001.04.12
		WO 01-25937 A1	2001.04.12
		WO 01-25953 A1	2001.04.12
		WO 01-26276 A1	2001.04.12
		WO 01-26277 A1	2001.04.12
KR 10-2009-0025146 A	2009.03.10	CN 101382979 A	2009.03.11
		EP 2037384 A1	2009.03.18
		JP 2009-064443 A	2009.03.26
		US 2009-0064337 A1	2009.03.05
KR 10-0628869 B1	2006.09.27	US 2006-0129603 A1	2006.06.15
US 2006-0021054 A1	2006.01.26	CN 1725759 A	2006.01.25
		EP 1630710 A2	2006.03.01
		JP 2006-031718 A	2006.02.02
		KR 10-2006-0092832 A	2006.08.23
		US 2006-0031933 A1	2006.02.09

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
		US 2006-021054 A1	2006.01.26
		US 2007-0006314 A1	2007.01.04
		US 7603715 B2	2009.10.13
		US 7634812 B2	2009.12.15
		US 7634813 B2	2009.12.15
WO 2004-003710 A1	2004.01.08	AU 2003-244947 A1	2004.01.19
		CN 1666163 A	2005.09.07
		CN 1666163 C0	2008.06.25
		EP 1520219 A1	2005.04.06
		EP 1520219 B1	2010.11.03
		JP 04-519642 B2	2010.05.28
		JP 2005-531079 A	2005.10.13
		KR 10-0947878 B1	2010.03.17
		US 2004-0003277 A1	2004.01.01
		US 7743257 B2	2010.06.22
		WO 2004-003710 A1	2004.01.08
KR 10-0666562 B1	2007.01.09	없음	