

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국



(10) 국제공개번호
WO 2023/017931 A1

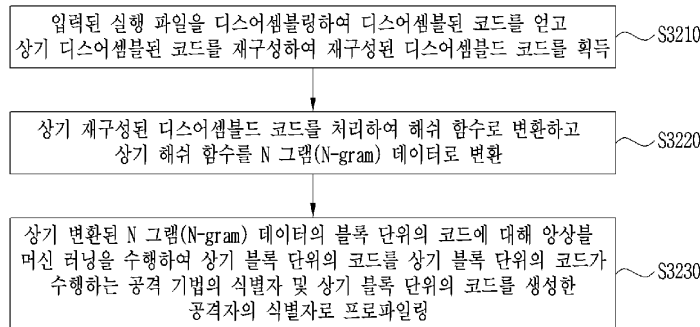
(43) 국제공개일
2023년 2월 16일 (16.02.2023)

- (51) 국제특허분류:
G06F 21/56 (2013.01) *G06N 20/20* (2019.01)
G06N 20/00 (2019.01)
- (21) 국제출원번호: PCT/KR2022/000955
- (22) 국제출원일: 2022년 1월 19일 (19.01.2022)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2021-0106216 2021년 8월 11일 (11.08.2021) KR
10-2021-0106217 2021년 8월 11일 (11.08.2021) KR
- (71) 출원인: 주식회사 샌즈랩 (SANDS LAB INC.) [KR/KR];
06143 서울특별시 강남구 선릉로 577, 4층, Seoul (KR).
- (72) 발명자: 김기홍 (KIM, Kihong); 07445 서울특별시 영등포구 시흥대로 595, 101동 1002호 (대림동, H HOUSE

- 대림 뉴스테이), Seoul (KR). 어성율 (EUH, Seongyul); 13628 경기도 성남시 분당구 미금일로 58, 403동 1301호 (구미동, 까치마을), Gyeonggi-do (KR). 박성은 (PARK, Sungun); 13628 경기도 성남시 분당구 미금로 177, 304동 1602호 (구미동, 까치마을), Gyeonggi-do (KR). 이현종 (LEE, Hyunjong); 06578 서울특별시 서초구 사평대로 154, 101동 507호 (반포동, 현대동궁아파트), Seoul (KR).
- (74) 대리인: 특허법인(유한)케이비케이 (KBK & ASSOCIATES); 05556 서울특별시 송파구 올림픽로 82 (잠실현대빌딩 7층), 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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KW,

(54) Title: CYBER THREAT INFORMATION PROCESSING DEVICE, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM

(54) 발명의 명칭: 사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체



- S3210 ... Disassemble input executable file to obtain disassembled code, and reconstruct disassembled code to obtain reconstructed disassembled code
- S3220 ... Convert reconstructed disassembled code into hash function and convert hash function into N-gram data
- S3230 ... Perform ensemble machine learning with respect to block unit code of converted N-gram data to profile block unit code with identifier of attack technique that block unit code performs, and identifier of attacker who has generated block unit code

(57) Abstract: The disclosed embodiment provides a cyber threat information processing device, a cyber threat information processing method, and a storage medium storing a cyber threat information processing program. One embodiment of the invention may provide a cyber security threat information processing method comprising: a step of disassembling an input executable file to obtain a disassembled code and reconstructing the disassembled code to obtain a reconstructed disassembled code; a step of converting the reconstructed disassembled code into a hash function and converting the hash function into N-gram data (where N is a natural number); and a step of performing ensemble machine learning with respect to a block unit code of the converted N-gram data to profile the block unit code

[다음 쪽 계속]



WO 2023/017931 A1

KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, 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, 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, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

with an identifier of an attack technique that the block unit code performs, and an identifier of an attacker who has generated the block unit code. According to an embodiment, it is possible to detect and respond to even a malicious code that does not exactly match data learned by artificial intelligence, and to respond to even a variant of a malicious code by identifying the malicious code, an attack technique, an attacker, and an attack prediction method in a very short time.

(57) 요약서: 개시하는 실시 예는 사이버 위협 정보 처리 장치, 사이버 위협 정보 처리 방법 및 사이버 위협 정보 처리하는 프로그램을 저장하는 저장매체를 제공한다. 발명의 일 실시 예로서 입력된 실행 파일을 디스어셈블링하여 디스어셈블된 코드를 얻고 상기 디스어셈블된 코드를 재구성하여 재구성된 디스어셈블드 코드를 얻는 단계; 상기 재구성된 디스어셈블드 코드를 처리하여 해쉬 함수로 변환하고 상기 해쉬 함수를 N 그램(N-gram, N은 자연수) 데이터로 변환하는 단계; 및 상기 변환된 N 그램(N-gram) 데이터의 블록 단위의 코드에 대해 앙상블 머신 러닝을 수행하여 상기 블록 단위의 코드를 상기 블록 단위의 코드가 수행하는 공격 기법의 식별자 및 상기 블록 단위의 코드를 생성한 공격자의 식별자로 프로파일링하는 단계;를 포함하는 사이버 보안 위협 정보 처리 방법을 제공할 수 있다. 실시예에 따르면 인공 지능으로 학습된 데이터와 정확하게 일치하지 않는 악성 코드라도 탐지하고 대응할 수 있고 악성 코드의 변종에 대응할 수 있고 악성 코드의 변종이라도 매우 빠른 시간 내에 악성 코드, 공격 기법, 공격자와 공격 예측 방법을 식별할 수 있다.