(12) 특허협력조약에 의하여 공개된 국제출원

정정판

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2015 년 9 월 3 일 (03.09.2015)

WIPO | PCT

(10) 국제공개번호
WO 2015/129934 A8

(51) 국제특허분류:
*H04L 12/26* (2006.01) *H04L 12/24* (2006.01)

(21) 국제출원번호: PCT/KR2014/001551

(22) 국제출원일: 2014 년 2 월 26 일 (26.02.2014)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2014-0022130 2014 년 2 월 25 일 (25.02.2014) KR

(71) 출원인: (주)나루씨큐리티 (NARU SECURITY, INC.) [KR/KR]; 135-871 서울시 강남구 영동대로 621, 9 층, Seoul (KR).

(72) 발명자: 김혁준 (KIM, Hyukjoon); 138-949 서울시 송파구 송파대로 8 길 42, 1204 동 1301 호, Seoul (KR).

(74) 대리인: 유미특허법인 (YOU ME PATENT AND LAW FIRM); 135-912 서울시 강남구 테헤란로 115, 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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, RW, SD, SL, 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:

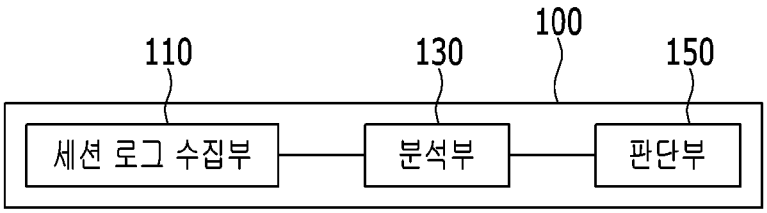
— 국제조사보고서와 함께 (조약 제 21 조(3))

(48) 본 정정판 공개일: 2015 년 11 월 5 일

(15) 정정사항에 관한 정보:
2015 년 11 월 5 일 자 공지 참조

(54) Title: APPARATUS AND METHOD FOR DETECTING COMMAND AND CONTROL CHANNELS

(54) 발명의 명칭 : 명령제어채널 탐지장치 및 방법




110 ... Session log collection unit
130 ... Analysis unit
150 ... Determination unit

(57) Abstract: A device for detecting command and control channels comprises: a session log collection unit for collecting log information of sessions generated between at least one communication device of a first network and at least one communication device of a second network; an analysis unit for generating inspection data for each session on the basis of the log information and calculating an inspection data distribution on the basis of the inspection data of the sessions; and a determination unit for extracting an inspection data value corresponding to abnormal distribution in the inspection data distribution on the basis of abnormal distribution determination criteria and estimating sessions associated with the extracted inspection data value as command and control channels.

(57) 요약서: 명령제어채널 탐지장치는 제 1 망의 적어도 하나의 통신장치와 제 2 망의 적어도 하나의 통신장치 사이에 생성되는 세션들의 로그 정보를 수집하는 세션 로그 수집부, 상기 로그 정보를 기초로 세션별 검사 데이터를 생성하고, 상기 세션들의 검사 데이터를 기초로 검사 데이터 분포를 계산하는 분석부, 그리고 비정상 분포 판단 기준을 기초로 상기 검사 데이터 분포에서 비정상 분포에 해당하는 검사 데이터 값을 추출하고, 추출한 검사 데이터값에 관계된 세션들을 명령제어채널로 추정하는 판단부를 포함한다.

WO 2015/129934 A8