



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년06월18일
(11) 등록번호 10-1156011
(24) 등록일자 2012년06월07일

(51) 국제특허분류(Int. Cl.)
H04L 12/22 (2006.01) G06F 21/20 (2006.01)
(21) 출원번호 10-2010-0134963
(22) 출원일자 2010년12월24일
심사청구일자 2010년12월24일
(56) 선행기술조사문헌
KR1020050068052 A*
KR100838799 B1
KR1020030035143 A
KR100942456 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울 성북구 안암동5가 1
한국인터넷진흥원
서울특별시 송파구 중대로 135 (가락동)
(72) 발명자
정현철
서울특별시 송파구 동남로23가길 8-7, 201호 (오금동, 멀티파크 B동)
임채태
서울특별시 송파구 송파대로 567, 주공아파트 528동 1107호 (잠실동)
(74) 대리인
특허법인다울
(뒷면에 계속)

전체 청구항 수 : 총 22 항

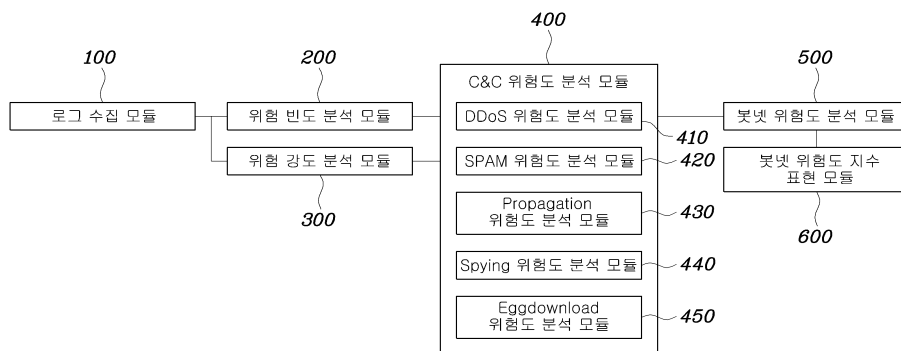
심사관 : 양찬호

(54) 발명의 명칭 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템 및 그 방법

(57) 요약

본 발명은 봇넷 위험도 산정 시스템 및 그 방법에 대한 것으로서, 특히, 네트워크 트래픽 분석을 통한 다양한 악성 행위에 대한 위험도 분석을 기초로 봇넷 위험도를 산정할 수 있는 봇넷 위험도 산정 시스템 및 그 방법에 관한 것이다. 본 발명은 봇넷의 다양한 악성 행위에 대한 위험도로 봇넷 위험도를 분석하여 봇넷의 오탐지 및 미탐지를 방지할 수 있다. 또한, 본 발명은 능동형 봇넷 탐지 및 관리를 하는데 있어 참조 위험 지수로 활용될 수 있으며, 기타 DNS 싱크홀에서의 관리에도 활용될 수 있는 봇넷 위험도 산정 시스템 및 그 방법을 제공할 수 있다.

대표도 - 도1



(72) 발명자

지승구

경기도 용인시 수지구 탄천상로 7, 7차 2단지 204동 902호 (죽전동, 인현마을현대홈타운)

오주형

서울특별시 송파구 중대로 135, 대동빌딩 (가락동)

강동완

서울특별시 구로구 개봉로17나길 100-4 (개봉동)

김도훈

서울특별시 성북구 안암로 145, 자연계캠퍼스 과학도서관 608B호 (안암동5가, 고려대학교)

인호

서울특별시 성북구 안암로 145, 자연계캠퍼스 과학도서관 604D호 (안암동5가, 고려대학교)

이 발명을 지원한 국가연구개발사업

과제고유번호 KI001863

부처명 지식경제부

연구사업명 IT산업원천 기술개발사업

연구과제명 신종 봇넷 능동형 탐지 및 대응 기술 개발

주관기관 한국인터넷진흥원

연구기간 2010.03.01 ~ 2011.02.28

특허청구의 범위

청구항 1

봇넷 탐지 시스템의 로그 데이터베이스로부터 봇넷의 악성 행위 탐지에 대한 로그 정보를 분류 및 수집하는 로그 수집 모듈과,

상기 로그 정보를 분석하여 단위 로그당 상기 봇넷의 악성 행위 발생 빈도인 위험 빈도를 분석하는 위험 빈도 분석 모듈과,

상기 로그 정보를 분석하여 단위 로그당 상기 봇넷의 악성 행위 발생 강도인 위험 강도를 분석하는 위험 강도 분석 모듈과,

상기 위험 빈도와 상기 위험 강도로 C&C 위험도를 분석하는 C&C 위험도 분석 모듈과,

상기 C&C 위험도로 봇넷 위험도를 분석하는 봇넷 위험도 분석 모듈을 포함하며,

상기 위험 빈도(F)는
$$F = \frac{M_{\log_n}}{M_{\log_{n-1}}}$$
 이고,

상기 $M_{\log_n}$ 은
$$M_{\log} = \frac{\sum send_count + \sum recv_count}{2}$$
 이며,

상기 $M_{\log_{n-1}}$ 은
$$M_{hour} = \frac{\sum send_count + \sum recv_count}{2} / (per\ hour)$$
 이고,

상기 $send_count$ 는 C&C가 유발하는 트래픽의 카운트 수이며,

상기 $recv_count$ 는 좀비가 유발하는 트래픽의 카운트 수인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 2

삭제

청구항 3

청구항 1에 있어서,

상기 위험 강도(s)는
$$S = \frac{Z_{ma}}{Cov_{at}}$$
 이고,

상기 Z_{ma} 는
$$Z_{ma} = \frac{\sum recv_count}{z}$$
 이며,

상기 Cov_{at} 는
$$Cov_{at} = C_{at} + Z_{at}$$
 이고,

상기 z 는 감염된 실제 좀비 개수이며,

상기 C_{at} 는
$$C_{at} = \frac{\sum send_byte}{z}$$
 이고,

상기 Z_{at} 는
$$Z_{at} = \frac{\sum recv_byte}{z}$$
 이며,

상기 $send_byte$ 는 C&C가 유발하는 트래픽이고,

상기 $recv_byte$ 는 좀비가 유발하는 트래픽인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 4

청구항 3에 있어서,

상기 C&C 위험도 분석 모듈은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와 상기 위험 강도 및 상기 위험 빈도로 DDoS 위험도를 분석하는 DDoS 위험도 분석 모듈을 포함하는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 5

청구항 4에 있어서,

상기 DDoS 위험도는 $DDoS_{\text{위험도}} = z' \sqrt{S \times F} - 1$ 이며,

상기 z' 은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 6

청구항 3에 있어서,

상기 C&C 위험도 분석 모듈은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와 상기 위험 강도 및 상기 위험 빈도로 SPAM 위험도를 분석하는 SPAM 위험도 분석 모듈을 포함하는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 7

청구항 6에 있어서,

상기 SPAM 위험도는 $SPAM_{\text{위험도}} = z' \sqrt{S \times F}$ 이며,

상기 z' 은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 8

청구항 3에 있어서,

상기 C&C 위험도 분석 모듈은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와 상기 위험 강도 및 상기 위험 빈도로 Propagation 위험도를 분석하는 Propagation 위험도 분석 모듈을 포함하는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 9

청구항 8에 있어서,

상기 Propagation 위험도는 $Propagation_{\text{위험도}} = z' \sqrt{S \times F}$ 이며,

상기 z' 은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 10

청구항 3에 있어서,

상기 C&C 위험도 분석 모듈은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와 상기 위험 강도 및 상기 위험 빈도로 Spying 위험도를 분석하는 Spying 위험도 분석 모듈을 포함하는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 11

청구항 10에 있어서,

상기 Spying 위험도는 $Spying \text{ 위험도} = z' \sqrt{S \times F}$ 이며,

상기 z' 은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 12

청구항 11에 있어서,

상기 C&C 위험도 분석 모듈은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와 상기 위험 강도 및 상기 위험 빈도로 Eggdownload 위험도를 분석하는 Eggdownload 위험도 분석 모듈을 포함하는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 13

청구항 12에 있어서,

상기 Eggdownload 위험도는 $Eggdownload \text{ 위험도} = z' \sqrt{S \times F}$ 이며,

상기 z' 은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 14

청구항 4 내지 청구항 13 중 어느 한 항에 있어서,

상기 C&C 위험도는 $CnC_n = \sqrt{\prod_{i=1}^j \text{악성 행위별 위험도}_i \times \text{가중치}(W_{ma})}$ 이며,

상기 악성 행위별 위험도는 상기 DDoS 위험도와, 상기 SPAM 위험도, 상기 Propagation 위험도, 상기 Spying 위험도, 및 상기 Eggdownload 위험도 중 적어도 어느 하나이고,

상기 j 는 C&C 위험도 산정에 이용된 악성 행위별 위험도의 개수이며,

상기 가중치는 상기 악성 행위별 위험도들에 대한 서로 상이한 가중치인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 15

청구항 14에 있어서,

상기 봇넷 위험도($BRI_{idx(n)}$)는 $BRI_{idx(n)} = \left\{ \sqrt{\prod_{i=1}^j (CnC_i)} \right\} \times 100$ 이며, 백분율로 표현되는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 16

청구항 15에 있어서,

상기 봇넷 위험도를 숫자와 문자, 색상 중 적어도 어느 하나를 포함하는 지수로 표현하는 봇넷 위험 지수 표현 모듈을 더 포함하는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템.

청구항 17

봇넷 탐지 시스템의 탐지 로그 데이터베이스로부터 봇넷의 악성 행위인 DDoS, SPAM, Propagation, Spying, 및 Eggdownload에 관한 로그 정보를 수집하는 단계와,

상기 악성 행위의 단위 시간당 발생 빈도인 위험 빈도를 분석하는 단계와,

상기 악성 행위의 단위 탐지 로그당 평균 악성 행위 건수로 악성 행위의 발생 강도인 위험 강도를 분석하는

단계와,

상기 위험 빈도와 상기 위험 강도로 C&C 위험도를 분석하는 단계와,

상기 C&C 위험도로 봇넷 위험도를 분석하는 단계를 포함하며,

상기 악성 행위의 단위 시간당 발생 빈도인 위험 빈도를 분석하는 단계;에서 상기 위험 빈도(F)는 $F = \frac{M_{\log n}}{M_{\log n-1}}$ 이고,

상기 $M_{\log n}$ 은 $M_{\log} = \frac{\sum send_count + \sum recv_count}{2}$ 이며,

상기 $M_{\log n-1}$ 은 $M_{hour} = \frac{\sum send_count + \sum recv_count}{2} / (per_hour)$ 이고,

상기 $send_count$ 는 C&C가 유발하는 트래픽의 카운트 수이며,

상기 $recv_count$ 는 좀비가 유발하는 트래픽의 카운트 수인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법.

청구항 18

삭제

청구항 19

청구항 17에 있어서,

상기 악성 행위의 단위 탐지 로그당 평균 악성 행위 건수로 악성 행위의 발생 강도인 위험 강도를 분석하는 단계;에서, 상기 위험 강도(S)는 $S = \frac{Z_{ma}}{Cov_{at}}$ 이고,

상기 Z_{ma} 는 $Z_{ma} = \frac{\sum recv_count}{z}$ 이며,

상기 Cov_{at} 는 $Cov_{at} = C_{at} + Z_{at}$ 이고,

상기 z 는 감염된 실제 좀비 개수이며,

상기 C_{at} 는 $C_{at} = \frac{\sum send_byte}{z}$ 이고,

상기 Z_{at} 는 $Z_{at} = \frac{\sum recv_byte}{z}$ 이며,

상기 $send_byte$ 는 C&C가 유발하는 트래픽이고,

상기 $recv_byte$ 는 좀비가 유발하는 트래픽인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법.

청구항 20

청구항 17에 있어서,

상기 위험 빈도와 상기 위험 강도로 C&C 위험도를 분석하는 단계는,

상기 위험 강도와 상기 위험 빈도 및 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수로 DDos 위험도를 분석하는 단계와,

상기 위험 강도와 상기 위험 빈도 및 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수로 SPAM 위험도를 분석하는 단계와,

상기 위험 강도와 상기 위험 빈도 및 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수로 Propagation 위험도를 분석하는 단계와,

상기 위험 강도와 상기 위험 빈도 및 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수로 Spying 위험도를 분석하는 단계와,

상기 위험 강도와 상기 위험 빈도 및 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수로 Eggdownload 위험도를 분석하는 단계를 포함하는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법.

청구항 21

청구항 20에 있어서,

상기 DDoS 위험도는 $DDoS_{\text{위험도}} = z' \sqrt{S \times F - 1}$ 이며,

상기 SPAM 위험도는 $SPAM_{\text{위험도}} = z' \sqrt{S \times F}$ 이고,

상기 Propagation 위험도는 $Propagation_{\text{위험도}} = z' \sqrt{S \times F}$ 이며,

상기 Spying 위험도는 $Spying_{\text{위험도}} = z' \sqrt{S \times F}$ 이고,

상기 Eggdownload 위험도는 $Eggdownload_{\text{위험도}} = z' \sqrt{S \times F}$ 이며,

상기 z' 은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법.

청구항 22

청구항 21에 있어서,

상기 위험 빈도와 상기 위험 강도로 C&C 위험도를 분석하는 단계는 상기 DDoS 위험도와, SPAM 위험도, Propagation 위험도, Spying 위험도, 및 Eggdownload 위험도 중 적어도 어느 하나로 C&C 위험도를 분석하며,

상기 C&C 위험도는 $CnC_n = \sqrt[3]{\prod_{i=1}^3 \text{악성 행위별 위험도}_i \times \text{가중치}(W_{ma})}$ 이며,

상기 악성 행위별 위험도는 상기 DDoS 위험도와, 상기 SPAM 위험도, 상기 Propagation 위험도, 상기 Spying 위험도, 및 상기 Eggdownload 위험도 중 적어도 어느 하나이고,

상기 n 은 C&C 위험도 산정에 이용된 악성 행위별 위험도의 개수이며,

상기 가중치는 상기 악성 행위별 위험도들에 대한 서로 상이한 가중치인 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법.

청구항 23

청구항 22에 있어서,

상기 C&C 위험도로 봇넷 위험도를 분석하는 단계;에서, 상기 봇넷 위험도($BRI_{idx(n)}$)는

$BRI_{idx(n)} = \left\{ \sqrt[3]{\prod_{i=1}^3 (CnC_i)} \right\} \times 100$ 이며, 백분율로 표현되는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법.

청구항 24

청구항 23에 있어서,

상기 봇넷 위험도를 숫자와 문자, 색상 중 적어도 어느 하나를 포함하는 지수로 표현하는 단계를 더 포함하는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법.

기술 분야

[0001] 본 발명은 봇넷 위험도 산정 시스템 및 그 방법에 대한 것으로서, 특히, 네트워크 트래픽 분석을 통한 다양한 악성 행위에 대한 위험도 분석을 기초로 봇넷 위험도를 산정할 수 있는 봇넷 위험도 산정 시스템 및 그 방법에 관한 것이다.

배경 기술

[0002] 봇넷은 스팸메일이나 악성코드 등을 전파하도록 하는 악성코드 봇(Bot)에 감염되어 해커가 마음대로 제어할 수 있는 좀비 PC들로 구성된 네트워크를 의미한다. 일단 봇에 감염되는 실제 PC 사용자들은 자신의 컴퓨터가 감염된 것을 모르는 경우가 많고, 해커는 수많은 시스템(PC)에 명령을 전달해 특정 인터넷 사이트에 대량의 접속 신호를 보내는 DDoS 등의 공격으로 해당 사이트를 다운시키는 등의 방식으로 대규모 네트워크 공격을 수행할 수 있다.

[0003] 하지만, 대규모 망 관리자 입장에서 산발적이고 예측 불가능한 다양한 봇의 발현은 탐지 및 관리(대응)하는데 있어 많은 어려움이 따른다. 특히, 봇의 탐지의 가부를 네트워크 기반에서 구현하다 보면 많은 오용 탐지의 결과를 보일 수 있다. 뿐만 아니라 호스트 기반의 탐지 역시, 정해진 패턴이나 시나리오에서 벗어나는 행위가 있을 시에는 탐지의 어려움을 가져온다. 따라서 이러한 오용 탐지 및 미탐지의 문제를 해결하기 위해서는 비결정적 요인(확률 개념을 응용한 봇넷의 악성 행위 모델링)의 도입이 절실히 요구 된다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 목적은 봇넷의 오탐지 및 미탐지의 문제를 해결할 수 있는 봇넷 위험도 산정 시스템 및 그 방법을 제공하는 것이다.

과제의 해결 수단

[0005] 상술한 목적을 달성하기 위해 본 발명은 봇넷 탐지 시스템의 로그 데이터베이스로부터 봇넷의 악성 행위 탐지에 대한 로그 정보를 분류 및 수집하는 로그 수집 모듈과, 상기 로그 정보를 분석하여 단위 로그당 상기 봇넷의 악성 행위 발생 빈도인 위험 빈도를 분석하는 위험 빈도 분석 모듈과, 상기 로그 정보를 분석하여 단위 로그당 상기 봇넷의 악성 행위 발생 강도인 위험 강도를 분석하는 위험 강도 분석 모듈과, 상기 위험 빈도와 상기 위험 강도로 C&C 위험도를 분석하는 C&C 위험도 분석 모듈과, 상기 C&C 위험도로 봇넷 위험도를 분석하는 봇넷 위험도 분석 모듈을 포함하는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템

를 제공한다. 상기 위험 빈도(F)는 $F = \frac{M_{\log_n}}{M_{\log_{n-1}}}$ 이고, 상기 $M_{\log_n}$ 은 $M_{\log} = \frac{\sum send_count + \sum recv_count}{2}$ 이며, 상기

$M_{\log_{n-1}}$ 은 $M_{hour} = \frac{\sum send_count + \sum recv_count}{2} / (per\ hour)$ 이고, 상기 $send_count$ 는 C&C가 유발하는 트래픽의 카운트

수이며, 상기 $recv_count$ 는 좀비가 유발하는 트래픽의 카운트 수이다. 상기 위험 강도(s)는 $S = \frac{Z_{ma}}{Cov_{at}}$ 이고, 상

기 Z_{ma} 는 $Z_{ma} = \frac{\sum recv_count}{z}$ 이며, 상기 Cov_{at} 는 $Cov_{at} = C_{at} + Z_{at}$ 이고, 상기 z 는 감염된 실제 좀비 개수이며, 상기

C_{at} 는 $C_{at} = \frac{\sum send_byte}{z}$ 이고, 상기 Z_{at} 는 $Z_{at} = \frac{\sum recv_byte}{z}$ 이며, 상기 $send_byte$ 는 C&C가 유발하는 트래픽이고, 상기

$recv_byte$ 는 좀비가 유발하는 트래픽이다.

[0006] 상기 C&C 위험도 분석 모듈은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와 상기 위험 강도 및 상기 위험 빈도로 DDoS 위험도를 분석하는 DDoS 위험도 분석 모듈을 포함한다. 상기 DDoS 위험도는 $DDoS_위험도 = z' \sqrt{S \times F} - 1$ 이다. 상기 C&C 위험도 분석 모듈은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와 상기 위험 강도 및 상기 위험 빈도로 SPAM 위험도를 분석하는 SPAM 위험도 분석 모듈을 포함한다. 상기 SPAM 위험도는 $SPAM_위험도 = z' \sqrt{S \times F}$ 이다. 상기 C&C 위험도 분석 모듈은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와 상기 위험 강도 및 상기 위험 빈도로 Propagation 위험도를 분석하는 Propagation 위

협도 분석 모듈을 포함한다. 상기 Propagation 위험도는 $Propagation_{위협도} = z' \sqrt{S \times F}$ 이다. 상기 C&C 위험도 분석 모듈은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와 상기 위험 강도 및 상기 위험 빈도로 Spying 위험도를 분석하는 Spying 위험도 분석 모듈을 포함한다. 상기 Spying 위험도는 $Spying_{위협도} = z' \sqrt{S \times F}$ 이다. 상기 C&C 위험도 분석 모듈은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와 상기 위험 강도 및 상기 위험 빈도로 Eggdownload 위험도를 분석하는 Eggdownload 위험도 분석 모듈을 포함한다. 상기 Eggdownload 위험도는 $Eggdownload_{위협도} = z' \sqrt{S \times F}$ 이며, 상기 z' 은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수이다.

[0007]

상기 C&C 위험도는 $CnC_n = \sqrt{\prod_{i=1}^j \text{악성 행위별 위험도}_i} \times \text{가중치}(W_{ma})$ 이며, 상기 악성 행위별 위험도는 상기 DDoS 위험도와, 상기 SPAM 위험도, 상기 Propagation 위험도, 상기 Spying 위험도, 및 상기 Eggdownload 위험도 중 적어도 어느 하나이고, 상기 n 는 C&C 위험도 산정에 이용된 악성 행위별 위험도의 개수이며, 상기 가중치는 상기 악성 행위별 위험도들에 대한 서로 상이한 가중치이다.

[0008]

상기 봇넷 위험도($BRI_{idx(n)}$)는 $BRI_{idx(n)} = \left\{ \sqrt{\prod_{i=1}^j (CnC_i)} \right\} \times 100$ 이며, 백분율로 표현된다. 상기 봇넷 위험도를 숫자와 문자, 색상 중 적어도 어느 하나를 포함하는 지수로 표현하는 봇넷 위험 지수 표현 모듈을 더 포함할 수 있다.

[0009]

또한, 본 발명은 봇넷 탐지 시스템의 탐지 로그 데이터베이스로부터 봇넷의 악성 행위인 DDoS, SPAM, Propagation, Spying, 및 Eggdownload에 관한 로그 정보를 수집하는 단계와, 상기 악성 행위의 단위 시간당 발생 빈도인 위험 빈도를 분석하는 단계와, 상기 악성 행위의 단위 탐지 로그당 평균 악성 행위 건수로 악성 행위의 발생 강도인 위험 강도를 분석하는 단계와, 상기 위험 빈도와 상기 위험 강도로 C&C 위험도를 분석하는 단계와, 상기 C&C 위험도로 봇넷 위험도를 분석하는 단계를 포함하는 것을 특징으로 하는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법을 제공한다.

[0010]

상기 악성 행위의 단위 시간당 발생 빈도인 위험 빈도를 분석하는 단계;에서 상기 위험 빈도(F)는 $F = \frac{M_{\log_n}}{M_{\log_{n-1}}}$

이고, 상기 $M_{\log_n}$ 은 $M_{\log} = \frac{\sum send_{count} + \sum recv_{count}}{2}$ 이며, 상기 $M_{\log_{n-1}}$ 은

$M_{hour} = \frac{\sum send_{count} + \sum recv_{count}}{2} / (perhour)$ 이고, 상기 $send_{count}$ 는 C&C가 유발하는 트래픽의 카운트 수이며, 상기 $recv_{count}$ 는 좀비가 유발하는 트래픽의 카운트 수이다. 상기 악성 행위의 단위 탐지 로그당 평균 악성 행위 건수

로 악성 행위의 발생 강도인 위험 강도를 분석하는 단계;에서, 상기 위험 강도(s)는 $S = \frac{Z_{ma}}{Cov_{at}}$ 이고, 상기 Z_{ma}

는 $Z_{ma} = \frac{\sum recv_{count}}{z}$ 이며, 상기 Cov_{at} 는 $Cov_{at} = C_{at} + Z_{at}$ 이고, 상기 z 는 감염된 실제 좀비 개수이며, 상기 C_{at} 는

$C_{at} = \frac{\sum send_{byte}}{z}$ 이고, 상기 Z_{at} 는 $Z_{at} = \frac{\sum recv_{byte}}{z}$ 이며, 상기 $send_{byte}$ 는 C&C가 유발하는 트래픽이고, 상기 $recv_{byte}$

는 좀비가 유발하는 트래픽이다. 상기 위험 빈도와 상기 위험 강도로 C&C 위험도를 분석하는 단계는, 상기 위험 강도와 상기 위험 빈도 및 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수로 DDoS 위험도를 분석하는 단계와, 상기 위험 강도와 상기 위험 빈도 및 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수로 SPAM 위험도를 분석하는 단계와, 상기 위험 강도와 상기 위험 빈도 및 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수로 Propagation 위험도를 분석하는 단계와, 상기 위험 강도와 상기 위험 빈도 및 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수로 Spying 위험도를 분석하는 단계와, 상기 위험 강도와 상기 위험 빈도 및 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수로 Eggdownload 위험도를 분석하는 단계를 포함한다. 상기

DDoS 위험도는 $DDoS_{위협도} = z' \sqrt{S \times F} - 1$ 이며, 상기 SPAM 위험도는 $SPAM_{위협도} = z' \sqrt{S \times F}$ 이고, 상기

Propagation 위험도는 $Propagation_{위협도} = z' \sqrt{S \times F}$ 이며, 상기 Spying 위험도는 $Spying_{위협도} = z' \sqrt{S \times F}$ 이고, 상

기 Eggdownload 위험도는 $Eggdownload_{위협도} = z' \sqrt{S \times F}$ 이며, 상기 z' 은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수이다. 상기 위험 빈도와 상기 위험 강도로 C&C 위험도를 분석하는 단계는 상기 DDoS 위험도와, SPAM 위험도, Propagation 위험도, Spying 위험도, 및 Eggdownload 위험도 중 적어도 어느 하나로 C&C 위험도

를 분석하며,

[0011]

상기 CnC 위험도는 $CnC_n = \sqrt[n]{\prod_{i=1}^n \text{악성 행위별 위험도}_i} \times \text{가중치}(W_{ma})$ 이며, 상기 악성 행위별 위험도는 상기 DDoS 위험도와, 상기 SPAM 위험도, 상기 Propagation 위험도, 상기 Spying 위험도, 및 상기 Eggdownload 위험도 중 적어도 어느 하나이고, 상기 n 는 CnC 위험도 산정에 이용된 악성 행위별 위험도의 개수이며, 상기 가중치는 상기 악성 행위별 위험도들에 대한 서로 상이한 가중치이다. 상기 CnC 위험도로 봇넷 위험도를 분석하는 단계에서, 상기 봇넷 위험도($BRI_{idx(n)}$)는 $BRI_{idx(n)} = \left\{ \sqrt[n]{\prod_{i=1}^n (CnC_i)} \right\} \times 100$ 이며, 백분율로 표현되는 것이 효과적이다. 상기 봇넷 위험도를 숫자와 문자, 색상 중 적어도 어느 하나를 포함하는 지수로 표현하는 단계를 더 포함할 수 있다.

발명의 효과

[0012]

본 발명은 봇넷의 다양한 악성 행위에 대한 위험도로 봇넷 위험도를 분석하여 봇넷의 오탐지 및 미탐지를 방지할 수 있는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템 및 그 방법을 제공할 수 있다.

[0013]

또한, 본 발명은 능동형 봇넷 탐지 및 관리를 하는데 있어 참조 위험 지수로 활용될 수 있으며, 기타 DNS 싱크홀에서의 관리에도 활용될 수 있는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템 및 그 방법을 제공할 수 있다.

도면의 간단한 설명

[0014]

도 1은 본 발명에 따른 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템의 개념도.

도 2는 탐지 로그 내에서 단위 로그당 악성 행위별 정렬표이다.

도 3은 본 발명에 따른 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법의 순서도.

발명을 실시하기 위한 구체적인 내용

[0015]

이하, 도면을 참조하여 본 발명의 실시예를 상세히 설명하기로 한다.

[0016]

그러나 본 발명은 이하에서 개시되는 실시예에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이다. 도면상의 동일 부호는 동일한 요소를 지칭한다.

[0017]

도 1은 본 발명에 따른 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템의 개념도이고, 도 2는 탐지 로그 내에서 단위 로그당 악성 행위별 정렬표이다.

[0018]

본 발명에 따른 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템은 도 1에 도시된 바와 같이, 로그 데이터베이스로부터 봇넷 행위의 탐지를 결정짓는 로그를 분류 및 수집하는 로그 수집 모듈(100)과, 탐지된 봇넷 그룹의 단위 로그 데이터베이스를 분석하여 단위 로그당 출현빈도를 분석하는 위험 빈도 분석 모듈(200)과, 탐지된 봇넷 그룹의 단위 로그 데이터베이스를 분석하여 단위 로그당 출현강도를 분석하는 위험 강도 분석 모듈(300)과, 봇넷에 구성되어진 C&C별로 지니고 있는 악성행위를 분석 및 산정하는 C&C 위험도 분석 모듈(400)과, 분석된 C&C 위험도를 정규화하여 봇넷 위험도를 산정하는 봇넷 위험도 분석 모듈(500), 및 봇넷 위험 지수 표현 모듈(600)을 포함한다.

[0019]

로그 수집 모듈(100)은 봇넷 탐지 시스템의 탐지 로그 데이터베이스로부터 봇넷의 악성 행위인 DDoS, SPAM, Propagation, Spying, 및 Eggdownload에 관한 로그 정보를 수집한다. 이때 수집된 로그 정보는 도 2에 도시된 바와 같이, 단위 로그당 악성 행위별로 정렬될 수 있다. 또한, 도 2에서 탐지 로그에서 생성된 Botnet IDX 번호는 해당 봇넷 그룹의 번호로써, 실제로 위험도를 산정하고 표시한다. 물론, Botnet IDX 번호에 해당하는 단일 또는 다수개의 C&C가 존재할 수 있다.

[0020]

위험 빈도 분석 모듈(200)은 봇넷의 발생 가능한 이벤트, 즉, 악성 행위의 발생 빈도를 분석한다. 이는 아래의 수식식1과 같이, 단위 시간당 이벤트 발생 비율로 나타낼 수 있다.

수학식 1

$$F = \frac{M_{\log_n}}{M_{\log_{n+1}}}$$

[0021]

[0022] 수학식1에서 $M_{\log_n}$ 은 단위 탐지 로그당 평균 악성 행위 건수로서, 아래의 수학식2과 같이 C&C가 유발하는 트래픽의 카운트 수, 즉, C&C의 악성 행위 건수와, 좀비가 유발하는 트래픽의 카운트 수, 즉, 좀비의 악성 행위 건수로 표현될 수 있다.

수학식 2

$$M_{\log} = \frac{\sum send_count + \sum recv_count}{2}$$

[0023]

[0024] 수학식2에서 $send_count$ 는 C&C가 유발하는 트래픽의 카운트 수이고, $recv_count$ 는 좀비가 유발하는 트래픽의 카운트 수이다.

[0025] 또한, 수학식1에서 $M_{\log_{n+1}}$ 은 이전 단위 탐지로그와 현재 단위 탐지로그당 평균 악성 행위 건수로서, 아래의 수학식3과 같이, C&C가 유발하는 트래픽의 카운트 수와 좀비가 유발하는 트래픽의 카운트 수로 표현될 수 있다.

수학식 3

$$M_{hour} = \frac{\sum send_count + \sum recv_count}{2} / (perhour)$$

[0026]

[0027] 위험 강도 분석 모듈(300)은 이전 단위 탐지로그와 현재 단위 탐지로그당 평균 악성 행위 건수로 위험 강도를 분석한다. 이는 이전 탐지 로그와 현재 단위 탐지로그간의 좀비들이 유발한 발신(send_byte) 트래픽과 수신(recv_byte) 트래픽의 합의 평균을 나타내며, 궁극적으로 봇넷의 위험도는 시간당으로 표현 가능하다. 이러한 위험 강도는 아래의 수학식4와 같이 표현될 수 있다.

수학식 4

$$S = \frac{Z_{ma}}{Cov_{at}}$$

[0028]

[0029] 수학식4에서 Z_{ma} 는 좀비의 평균 악성 행위 건수로서, 아래의 수학식5와 같이 감염된 실제 좀비수와 좀비의 악성 행위 건수로 표현된다.

수학식 5

$$Z_{ma} = \frac{\sum recv_count}{z}$$

[0030]

[0031] 수학식5에서 $recv_count$ 는 좀비의 악성 행위 건수이며, z 는 감염된 실제 좀비수이다.

[0032] 또한, 수학식4에서 Cov_{at} 는 환산 악성 유발 평균 트래픽으로서, 아래의 수학식6과 같이 단위 탐지 로그당 C&C가 유발하는 평균 트래픽과 단위 탐지 로그당 전체 좀비가 유발하는 평균 트래픽으로 표현된다.

수학식 6

[0033]
$$Cov_{at} = C_{at} + Z_{at}$$

[0034] 수학식6에서, C_{at} 는 탐지된 봇넷 C&C의 IP가 유발하는 평균 트래픽을 의미하며, Z_{at} 는 단위 탐지 로그당 전체 좀비가 유발하는 평균 트래픽이다. 이때, C_{at} 는 수학식7과 같이, 감염된 실제 좀비수와 C&C가 유발하는 트래픽으로 표현되며, Z_{at} 는 수학식8과 같이, 감염된 실제 좀비수와 좀비가 유발하는 트래픽으로 표현된다.

수학식 7

[0035]
$$C_{at} = \frac{\sum send_{byte}}{z}$$

수학식 8

[0036]
$$Z_{at} = \frac{\sum recv_{byte}}{z}$$

[0037] 수학식7에서 $send_{byte}$ 는 C&C가 유발하는 트래픽으로서, 탐지된 봇넷 C&C의 IP가 유발하는 트래픽을 의미한다. 또한, 수학식8에서 $recv_{byte}$ 는 좀비가 유발하는 트래픽으로서, 탐지된 봇넷 그룹의 좀비들이 수신하는 트래픽을 의미한다.

[0038] C&C 위험도 분석 모듈(400)은 위험 빈도 분석 모듈(200)에서 분석된 위험 빈도와 위험 강도 분석 모듈(300)에서 분석된 위험 강도를 이용하여 악성 행위들에 대한 각각의 위험도를 분석하고, 이를 이용하여 C&C 위험도를 분석한다. 이때, 위험도는 단일 로그 분석시마다 위험도가 산정될 수 있으며, 초기 시간이 1일 때는 분석을 수행하지 않고 초기 시간 이후, 즉, 다음 시간부터 분석을 수행하여 위험도를 산정한다. 최종적으로는 단위 시간당 대표 위험도를 산출하고, 경보 단계를 설정할 수 있다. 이를 위해, C&C 위험도 분석 모듈(400)은 DDoS 위험도 분석 모듈(410)과, SPAM 위험도 분석 모듈(420), Propagation 위험도 분석 모듈(430), Spying 위험도 분석 모듈(440), 및 Eggdownload 위험도 분석 모듈(450)을 포함한다.

[0039] DDoS 위험도 분석 모듈(410)은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와, 위험강도 및 위험빈도로 DDoS 위험도를 구한다. 이는 아래의 수학식9와 같이 표현될 수 있다.

수학식 9

[0040]
$$DDoS \text{ 위험도} = z' \sqrt{S \times F - 1}$$

[0041] 수학식9에서 z' 은 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수이다. 이때, z' 과 전술된 z 는 동일한 값일 수 있다. 또한, s 는 봇넷이 가지고 있는 잠재적 피해 강도를 의미하는 위험강도로서, 전술된 수학식4와 같이 좀비의 평균 악성 행위 건수와 환산 악성 유발 평균 트래픽으로 표현되며, f 는 위험빈도로서, 전술된 수학식1과 같이 단위 탐지 로그당 평균 악성 행위 건수와 이전 단위 탐지로그와 현재 단위 탐지로그당 평균 악성 행위 건수로 표현된다.

[0042] 또한, SPAM의 위험도와, Propagation의 위험도, Spying의 위험도, 및 Eggdownload의 위험도 역시 아래의 수학식10 내지 수학식13과 같이, 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와, 위험강도 및 위험빈도로 각각 표현될 수 있다.

수학식 10

$$SPAM \text{ 위험도} = {}^{z'}\sqrt{S \times F}$$

수학식 11

$$Propagation \text{ 위험도} = {}^{z'}\sqrt{S \times F}$$

수학식 12

$$Spying \text{ 위험도} = {}^{z'}\sqrt{S \times F}$$

수학식 13

$$Eggdownload \text{ 위험도} = {}^{z'}\sqrt{S \times F}$$

한편, 전술된 DDoS 위험도를 제외한 SPAM 위험도와, Propagation 위험도, Spying 위험도, 및 Eggdownload 위험도는 모두 함수가 동일하다. 하지만, 각각의 악성 행위는 그 위험도가 서로 상이하다. 따라서, 본 발명은 각각의 악성 행위에 가중치를 부여하며, 이를 위해서, 본 발명은 가중치 부여 모듈을 포함할 수 있다.

표1은 악성 행위별 가중치를 설명한 것이다.

표 1

악성 행위	가중치(Wma)	산정 기준
DDoS	1.0	DDoS 공격시를 최대 위험도로 기준
SPAM	0.7	DDoS에 비해 상대적으로 작은 위험도를 가짐
Propagation	0.5	봇넷 확장을 위한 사전행위로써 간접적인 위험도를 가짐
Spying	0.4	특정 PC의 정보탈취를 목적으로한 위험도를 가짐
Eggdownload	0.3	악성행위를 하기 위해 명령어 및 파일을 송/수신함

표1을 참조하면, 각각의 악성 행위는 DDoS의 위험도에 상대적 위험도를 가진다. 이는 DDoS가 발생시키는 트래픽과 피해 정도는 다른 악성 행위에 비해 월등히 높기 때문에 DDoS의 가중치를 1.0으로 하고, 이를 기준으로 다른 악성 행위의 가중치를 상대적으로 산정하였다.

CnC 위험도 분석 모듈(400)은 각각의 CnC는 단일 또는 다수의 악성 행위에 대한 위험도를 가지고 있으며, DDoS 위험도 분석 모듈(410)과, SPAM 위험도 분석 모듈(420), Propagation 위험도 분석 모듈(430), Spying 위험도 분석 모듈(440), 및 Eggdownload 위험도 분석 모듈(450)에서 분석된 각각의 악성 행위에 대해 가중치를 적용한 후, CnC별로 정규화한다. 이때, CnC 위험도는 아래의 수학식14와 같이 악성 행위별 위험도와 각각의 악성 행위별 위험도의 가중치로 표현될 수 있다.

수학식 14

$$CnC_n = {}^j\sqrt{\prod_{i=1}^j \text{악성 행위별 위험도}_i \times \text{가중치}(W_{ma})}$$

수학식14에서 악성 행위별 위험도는 전술된 DDoS 위험도와, SPAM 위험도, Propagation 위험도, Spying 위험도, 및 Eggdownload 위험도를 의미한다. 또한, 수학식14에서 가중치는 표1의 악성 행위별 위험도에 따른

가중치를 의미한다. α 는 C&C 위험도 산정에 이용된 악성 행위별 위험도의 개수이다.

[0054] 수학식14에 표현된 C&C 위험도 함수를 이용하여 DDoS 위험도와 SPAM 위험도, Eggdownload 위험도에 따른 C&C 위험도를 예시적으로 산출하면, 아래의 수학식15와 같다.

수학식 15

$$CnC_2 = \sqrt[3]{DDoS_{\text{위험도}} \times 1.0 \times SPAM_{\text{위험도}} \times 0.7 \times Eggdownload_{\text{위험도}} \times 0.3}$$

$$= \sqrt[3]{0.9 \times 1.0 \times 0.84 \times 0.7 \times 0.6 \times 0.3} \approx 0.46$$

[0056] 수학식15에서, DDoS의 위험도는 0.9, SPAM의 위험도는 0.84, Eggdownload의 위험도는 0.6으로 계산된 것을 예시하였다. 또한, 3개의 악성 행위별 위험도로 C&C 위험도를 산출한 것이므로 수학식14에서 α 는 3이 된다. 이에 따라, 최종적인 C&C 위험도는 0.46으로 근사화된 것을 알 수 있다.

[0057] 또한, SPAM의 위험도와 Eggdownload의 위험도로 C&C 위험도를 산출할 경우, 아래의 수학식16과 같이 적용될 수 있다.

수학식 16

$$CnC_5 = \sqrt[2]{SPAM_{\text{위험도}} \times Eggdownload_{\text{위험도}}}$$

$$= \sqrt[2]{0.74 \times 0.56} \approx 0.29$$

[0059] 또한, DDoS의 위험도와, SPAM의 위험도, Propagation의 위험도, Spying의 위험도, 및 Eggdownload의 위험도로 C&C 위험도를 산출할 경우, 아래의 수학식17과 같이 적용될 수 있다.

수학식 17

$$CnC_7 = \sqrt[5]{DDoS_{\text{위험도}} \times 1.0 \times SPAM_{\text{위험도}} \times 0.7 \times Eggdownload_{\text{위험도}} \times 0.3 \times Spying_{\text{위험도}} \times 0.4 \times Propagation_{\text{위험도}} \times 0.5}$$

$$= \sqrt[5]{0.89 \times 1.0 \times 0.77 \times 0.7 \times 0.67 \times 0.3 \times 0.84 \times 0.4 \times 0.94 \times 0.5}$$

[0060] ≈ 0.81

[0061] 봇넷 위험도 분석 모듈(500)은 최종 봇넷 위험도 산정을 위해서 C&C 위험도 분석 모듈(400)에서 분석된 C&C 위험도를 정규화시킨다. 이는 아래의 수학식18과 같이 C&C의 위험도를 이용하여 백분율로 표현함으로써 수행될 수 있다.

수학식 18

$$BRI_{idx(n)} = \left\{ \sqrt[4]{\prod_{i=1}^4 (CnC_i)} \right\} \times 100 = \text{백분율 표현}$$

[0063] 수학식18에 표현된 최종 봇넷 위험도를 이용하여 실제 최종 봇넷 위험도를 예시적으로 계산하면 아래의 수학식19와 같이 나타낼 수 있다.

수학식 19

$$BRI_{idx(5)} = \left\{ \sqrt[2]{(CnC_2) \times (CnC_5) \times (CnC_7)} \right\} \times 100 = 47.8\%$$

[0065] 수학식19에서 최종 봇넷 위험도는 전술된 C&C 위험도의 예시를 적용하여 계산하였다.

[0066] 봇넷 위험 지수 표현 모듈(600)은 사용자가 최종 봇넷 위험도를 쉽게 알 수 있게 하기 위해서, 백분율로 표현된 최종 봇넷 위험도를 백분율이 아닌 숫자 등으로 표현한다.

[0067] 표2는 최종 봇넷 위험도에 따른 표현 방법을 나타낸 것이다.

표 2

[0068]

위험지표	최종 봇넷 위험도	표현법
하	0% ~ 20%	1
중	20% ~ 60%	2
상	60% ~	3

[0069] 표2를 참조하면, 최종 봇넷 위험도가 0% 내지 20% 내일 경우, 위험지표로는 위험도가 '하'수준이며, 이는 '1'로 표현될 수 있다. 또한, 최종 봇넷 위험도가 20% 내지 60%일 경우, 위험지표로는 위험도가 '중'수준이며, 이는 '2'로 표현될 수 있으며, 최종 봇넷 위험도가 60% 이상일 경우, 위험지표로는 위험도가 '상'수준으로서 '3'으로 표현될 수 있다. 물론, 이러한 최종 봇넷 위험도에 따른 표현 방법은 예시일 뿐이며, 최종 표현은 숫자를 포함하는 문자, 색상 또는 이들의 조합을 포함할 수 있다. 또한, 최종 봇넷 위험도의 표현은 단위 시간당 출력되는 봇넷 위험도들 중 가장 큰 최대값을 그 시간대의 봇넷 그룹의 최종 봇넷 위험도로 최종 결정하여 표현한다.

[0070] 상술한 바와 같이, 본 발명은 봇넷의 다양한 악성 행위에 대한 위험도로 봇넷 위험도를 분석하여 봇넷의 오염 지 및 미탐지를 방지할 수 있는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템을 제공할 수 있다. 또한, 본 발명은 능동형 봇넷 탐지 및 관리를 하는데 있어 참조 위험 지수로 활용될 수 있으며, 기타 DNS 싱크홀에서의 관리에도 활용될 수 있는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템을 제공할 수 있다.

[0071] 다음은 본 발명에 따른 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법에 대해 도면을 참조하여 설명하기로 한다. 후술할 내용 중 전술된 본 발명에 따른 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 시스템의 설명과 중복되는 내용은 생략하거나 간략히 설명하기로 한다.

[0072] 도 3은 본 발명에 따른 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법의 순서도이다.

[0073] 본 발명에 따른 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법은 도 3에 도시된 바와 같이, 로그를 수집하는 단계(S1)와, 위험 빈도를 분석하는 단계(S2)와, 위험 강도를 분석하는 단계(S3)와, C&C 위험도를 분석하는 단계(S4)와, 봇넷 위험도를 분석하는 단계(S5)를 포함한다. 또한, 이에 더하여 봇넷 위험 지수를 표현하는 단계(S6)를 더 포함할 수 있다.

[0074] 로그를 수집하는 단계(S1)는 봇넷 탐지 시스템의 탐지 로그 데이터베이스로부터 봇넷의 악성 행위인 DDoS, SPAM, Propagation, Spying, 및 Eggdownload에 관한 로그(Log) 정보를 수집한다. 이때, 수집된 로그 정보로부터 분석에 필요한 정보들만을 추출하기 위해 각 악성 행위별 시계열 로그 정보를 추출한다. 이는 이후, 단위 로그당 위험도를 산출하기 위해서 필요하다.

[0075] 위험 빈도를 분석하는 단계(S2)는 봇넷의 발생 가능한 이벤트, 즉, 악성 행위의 발생 빈도를 분석한다. 이러한 위험 빈도를 분석하는 단계는 단위 시간당 봇넷의 발생 가능한 이벤트 비율을 이용할 수 있으며, 전술된 수학적식1과 같이 구해질 수 있다.

[0076] 위험 강도를 분석하는 단계(S3)는 이전 단위 탐지로그와 현재 단위 탐지로그당 평균 악성 행위 건수로 위험 강도를 분석한다. 이는 이전 탐지 로그와 현재 단위 탐지로그간의 좀비들이 유발한 발신(send_byte) 트래픽과 수신(recv_byte) 트래픽의 합의 평균을 나타내며, 궁극적으로 봇넷의 위험도는 시간당으로 표현 가능하다. 위험 강도를 분석하는 단계(S3)에서 위험 강도는 전술된 수학적식4와 같이 좀비의 평균 악성 행위 건수와 환산 악성 유발 평균 트래픽으로 구해질 수 있다.

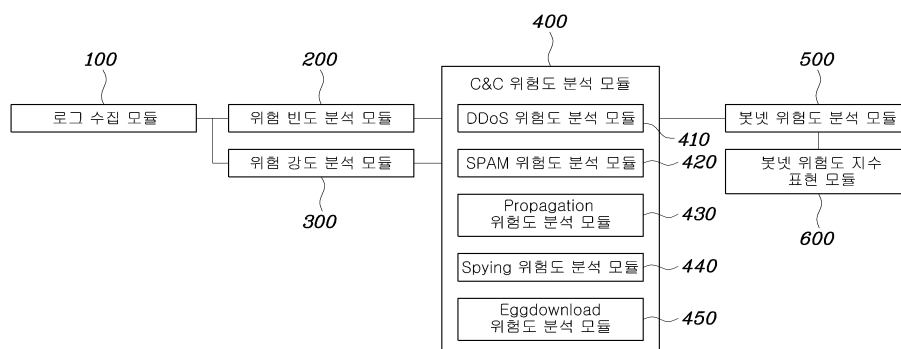
[0077] C&C 위험도를 분석하는 단계(S4)는 위험 빈도를 분석하는 단계(S2)와 위험 강도를 분석하는 단계(S3)에서 분석된 위험 빈도와 위험 강도로 C&C 위험도를 분석한다. 이때, C&C 위험도는 DDoS 위험도와 SPAM 위험도, Propagation 위험도, Spying 위험도, 및 Eggdownload 위험도를 각각 분석하여 분석할 수 있다. 또한, 이에 따라, C&C 위험도를 분석하는 단계(S4)는 DDoS 위험도를 분석하는 단계(S4-1)와, SPAM 위험도를 분석하는 단계(S4-2)와, Propagation 위험도를 분석하는 단계(S4-3)와, Spying 위험도를 분석하는 단계(S4-4), 및

Eggdownload 위험도를 분석하는 단계(S4-5)를 포함한다.

- [0078] DDoS 위험도를 분석하는 단계(S4-1)는 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와, 위험강도 및 위험빈도로 DDoS 위험도를 구한다. 이는 전술된 수학식9와 같이 구해질 수 있다.
- [0079] SPAM 위험도를 분석하는 단계(S4-2)는 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와, 위험강도 및 위험빈도로 SPAM 위험도를 구한다. 이는 전술된 수학식10과 같이 구해질 수 있다.
- [0080] Propagation 위험도를 분석하는 단계(S4-3)는 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와, 위험강도 및 위험빈도로 Propagation 위험도를 구한다. 이는 전술된 수학식11과 같이 구해질 수 있다.
- [0081] Spying 위험도를 분석하는 단계(S4-4)는 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와, 위험강도 및 위험빈도로 Spying 위험도를 구한다. 이는 전술된 수학식12와 같이 구해질 수 있다.
- [0082] Eggdownload 위험도를 분석하는 단계(S4-5)는 감염된 좀비 중 실제 악성 행위를 하는 좀비의 개수와, 위험강도 및 위험빈도로 Eggdownload 위험도를 구한다. 이는 전술된 수학식13과 같이 구해질 수 있다.
- [0083] 또한, C&C 위험도를 분석하는 단계(S4)는 구해진 DDoS 위험도와 SPAM 위험도, Propagation 위험도, Spying 위험도, 및 Eggdownload 위험도를 이용하여 C&C 위험도를 분석한다. 이러한 C&C 위험도는 전술된 수학식14와 같이 구해질 수 있다. 여기서, 수학식14에 따른 C&C 위험도는 가중치가 필요하며, 이를 위해, C&C 위험도를 분석하는 단계는 DDoS 위험도와 SPAM 위험도, Propagation 위험도, Spying 위험도, 및 Eggdownload 위험도에 가중치를 부여하는 단계를 포함할 수 있다. 가중치에 대한 내용은 전술된 표1에 설명되었으므로, 이에 대한 설명은 생략한다.
- [0084] 봇넷 위험도를 분석하는 단계(S5)는 최종 봇넷 위험도 산정을 위해서 C&C 위험도를 분석하는 단계에서 분석된 C&C 위험도를 정규화시킨다. 이는 전술된 수학식18과 같이 C&C의 위험도를 이용하여 백분율로 표현하여 수행할 수 있다.
- [0085] 봇넷 위험 지수를 표현하는 단계(S6)는 사용자가 최종 봇넷 위험도를 쉽게 알 수 있게 하기 위해서, 백분율로 표현된 최종 봇넷 위험도를 백분율이 아닌 숫자 등으로 표현한다.
- [0086] 상술한 바와 같이, 본 발명은 봇넷의 다양한 악성 행위에 대한 위험도로 봇넷 위험도를 분석하여 봇넷의 오염지 및 미탐지를 방지할 수 있는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법을 제공할 수 있다. 또한, 본 발명은 능동형 봇넷 탐지 및 관리를 하는데 있어 참조 위험 지수로 활용될 수 있으며, 기타 DNS 싱크홀에서의 관리에도 활용될 수 있는 네트워크 트래픽 분석을 통한 봇넷 위험도 산정 방법을 제공할 수 있다.
- [0087] 이상에서는 도면 및 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 본 발명의 기술적 사상으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

도면1



도면2

detection_time	cnc_ip	action	domain	zombie_ip	send_byte	send_count	recv_byte	recv_count
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.4.11	32524702	125578	89917588	125420
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.4.12	32537652	125628	90231292	125412
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.4.13	32441304	125256	89953594	125114
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.4.14	32529148	125572	91628914	125398
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.6.11	25594380	98820	70973488	98688
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.6.12	27873062	107618	78017984	107704
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.6.13	28106162	108518	78802084	108496
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.6.14	27996346	108094	78152430	107938
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.6.15	28411264	109696	79522792	109580
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.6.16	27909322	107758	77719604	107580
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.6.17	27314140	105460	76128918	105314
2010-02-03 17:18	192.168.7.100	DDOS	192.168.7.100	192.168.6.18	28097874	108486	78304072	108352
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.4.11	49850248	192472	138805837	192639
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.4.12	49851802	192478	139466934	192744
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.4.13	49759080	192120	138795553	192387
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.4.14	49827974	192386	140665183	192705
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.6.11	41701849	161011	116555234	161410
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.6.12	44286669	170991	124270523	171535
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.6.13	44352973	171247	124584935	171713
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.6.14	44378096	171344	124553196	171696
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.6.15	44308943	171077	124322600	171400
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.6.16	44243157	170823	123763567	171079
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.6.17	42981309	165951	120160043	166285
2010-02-03 17:19	192.168.7.100	DDOS	192.168.7.100	192.168.6.18	43042433	166187	120439997	166449
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.4.11	34653682	133798	97842083	134503
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.4.12	34629077	133703	98557674	134754
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.4.13	34643581	133759	97773402	134636
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.4.14	34609652	133628	98170219	134713
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.6.11	32214938	124382	91260856	125544
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.6.12	32831358	126762	92607996	127764
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.6.13	32500356	125484	91675683	126543
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.6.14	32768680	126520	92910629	127625
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.6.15	31797430	122770	89688341	123731
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.6.16	32672332	126148	92168829	127083
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.6.17	31341072	121008	88163650	122046
2010-02-03 17:20	192.168.7.100	DDOS	192.168.7.100	192.168.6.18	29899219	115441	84364236	116286

도면3

