Stealth 기능을 탑재한 LINK관절 IP역추적 방법

유재원* · 박대우**

*호서대학교

A Study of Backtracking of IPs and LINK Joints loaded with Stealth Functions

Jae-Won Yoo* · Dae-Woo Park**

*Heoseo Graduate School of Venture University

E-mail : peace.yoo@gmail.com · prof1@hoseo.edu

요 약

미국은 사이버전장을 육군, 해군, 공군, 우주군 다음으로 제5의 전장으로 선포하였다. 국가 사이버전쟁은 물리적 전쟁과 달리 아군과 적군이 구별되지 않고, 공격선과 방어선의 경계가 모호하다. 따라서 국가 사이버전쟁을 위해서는 사이버상에서 수행되는 모든 명령전달정보에 대한 신뢰성을 확인하여야 한다. 본 논문에서는 국가 사이버전쟁을 위해서 수행되는 명령들을 확인하고, 정보의 신뢰성을 위해서 지구와 달과 화성을 포함한 우주에 공인 IPv6를 부여하고, Stealth기능을 탑재한 LINK관절을 사용하여, 명령정보의 신뢰성을 확보하는 방안을 연구한다.

ABSTRACT

The USA has declared the cyber space as the 5th battlefield following land, sea, air, and space. In contrast to physical wars, in national cyberwarfare differentiation between friend and foe is impossible, and the boundaries between the lines of attack and defense are obscure. Therefore, to perform national cyberwarfare, credibility of all command delivery information performed in the cyber space should be confirmed. In this paper, the authors have determined the commands performed in national cyberwarfare, granted authorized IPv6 in space including the earth, moon and Mars for information credibility, and used LINK joints loaded with stealth functions to secure the credibility of command information.

키워드

IP역추적, Stealth 기능, link관절, 악성코드

Ⅰ. 서 론

사이버세계에서 국가의 경계를 넘어서, 보이지 않는 곳에서 그림 1처럼 해킹공격[1]은 실시되고 있다.

세계가 유선 인터넷과 우주를 포함하여 무선의 세계로 진화하고 있으며, 사이버공간은 지속 확장되고 있다. 특히, 미국방성은 2010년 7월 사이버공간을 제 5전장으로 선포하였다.

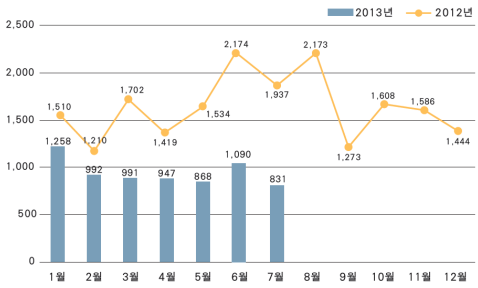

그림 1. 해킹사고 건수(KISA자료)

현실의 세계에서, 해킹공격에 대한 IP역추적[]은 법과 현실적인 제약으로 IP역추적 결과에 대한 문

제가 발생하고 있다. IP역추적의 중간 좀비나 숙주 라우터에서 증거수집의 어려움이 있다.

따라서 적극적인 IP역추적에 대한 연구가 필요하다.

본 논문에서는 중요정보의 링크관절구조를 제안한다. Low, Middle, High 링크관절로 연결된 중요정보는 Middle 관절에 중간라우팅 정보를 전달하고 전달된 정보의 log기록을 삭제한다, 최종 해커에게 중요정보가 전달되어 유출되면 Stealth기능이 작동되면(ex)MAC주소 확인등) 자폭되거나 백도어 작동, 랜섬웨어 등이 작동하고, Source IP를 역추적할 수 있는 기능을 탑재한다.

II. 관련연구

2.1 악성코드, Stealth 기능

정보통신기술의 발전에 정보의 증가하였다[]. 하지만, 정보가 증가하면서 이에 대한 부작용도 나타나고 있다. 즉, 컴퓨터바이러스 백신, 방화벽 등 정보보호장비를 우회하여 자료를 유출하는 악성코드 기술도 지속 증가하고 있다[1].

2.1.1 악성코드의 분류

악성코드는 호스트파일, 자기복제 여부에 따라 크게 웜(Worm), 트로이목마(Trojan Horse), 바이러스(Virus)로 표 1.과 같이 구분하고 있다.

표 1. 악성코드 분류

구분	호스트파일	자기복제
웜(Worm)	불필요	가능
트로이목마 (Trojan Horse)	필요	불가
바이러스(Virus)	필요	가능

2.1.2 악성코드 탐지회피기술

악성코드를 탐지하는 기술은 시그니처 방식과 휴리스틱 방식이 있으나, 이 두 가지 형식 모드는 상호 장 · 단점이 있다.

먼저, 시그니처 방식은 악성코드내 문자열 혹은 행동방식 등 특정 패턴을 이용하여 악성코드를 구분하는 방식으로 기존에 알려진 악성코드에 대해서는 탐지율이 우수하나 신종 악성코드를 탐지못하는 단점이 있다.

반면, 휴리스틱방식은 네트워크 트래픽증가 등 이상행동을 탐지하는 방식으로 신종 악성탐지에 우수한 점이 있으나, 정상적인 코드를 악성코드로 오인탐지하여 구성형식에 따라 신뢰성이 떨어진다.

2.2 해킹과 정보보호체계

해킹은 이윤추구, 저항 혹은 호기심 등 다양한 이유를 컴퓨터나 네트워크의 취약점으로 찾아내고 악용하는 행위로 정의하며, 이런 해킹을 하는 인원들을 일반적으로 해커라 칭하고 있다.

특히, 정치・사회적 목적으로 이루기 위해 목표물인 서버컴퓨터를 해킹하거나 무력화하는 핵티비즘(Hacktivism)으로 확산되었다.

핵티비즘에 참여하는 해커들은 불법적으로 중요정보자산을 탈취하여 자신의 이익이나 조직논리에 의해 인터넷에 노출시키거나 적국에 제공하고 있어 많은 사회적 이슈를 만들고 있다[위키리크스].

이에 대해, 각급 기관들은 수동적으로는 중요정보자산에 대해 보호하기 방화벽, 침입차단시스템 등 정보보호장비를 구비하여 운영하고 있으며[행안부 CERT고시], 능동적으로 허니팟 · 넷 운용 및 IP역추적 등을 통해 사전적으로 해킹을 감시하고 있다[KISA].

2.2.1 허니팟 · 넷

허니팟 · 넷은 외부의 공격을 유인해서 현재 벌어지고 있는 해킹 상황을 확인할 수 있도록 구성한 가상 시스템 · 네트워크이다. 마치 꿀로 벌을 유인하는 것과 같이 해커를 가상의 체계로 유인해 최신 해킹 경향을 파악할 수 있도록 하는 것을 목적으로 한다.

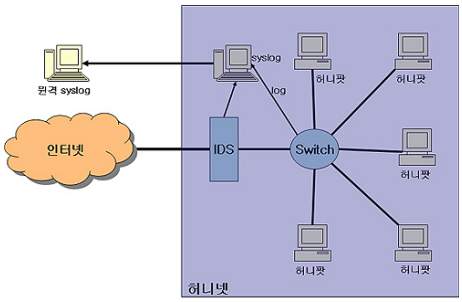

그림 2. 허니넷의 네트워크 구조

2.2.2 IP역추적

IP역추적기술은 IP를 기반으로 공격자 호스트를 찾아 필터링을 수행하거나 제거하는 기술로 다양한 연구가 이루어져 왔다. 하지만 이런 연구들은 대부분 네트워크 상의 IP헤더를 조작하여 추적자

에게 제공하는 방법이었다[2].

대표적으로 패킷에 대한 확률적 마킹(PPM : Probability Packet Marking) 기법[]과 전통적인 ICMP 메시지를 변형한 iTrace(ICMP Traceback) 기법[] 등이 있다.

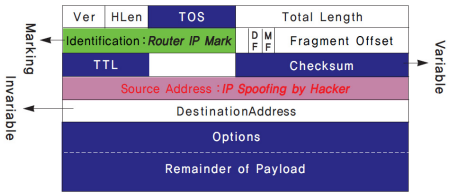

그림 3. IP 헤더 형태

2.3 역공학

역공학을 통해 악성코드, 패킷정보 등에서 해킹에 사용된 중간 경유지나 C&C 서버 IP주소 등 각종 증거자료를 수집할 수 있다. 악성코드의 분석은 디스어셈블(Disassemble) 혹은 디컴파일(Decompile)을 통하는 정적방식과 실제로 동작을 시켜보며 나타나는 외적요소를 확인하는 정적분석으로 나누어 진다[3].

2.4 보안이벤트 분석

보안이벤트를 분석하는 기술에는 실시간 보안이벤트 필터링 기술, 보안이벤트에 대한 상호연관분석 기술, 보안이벤트에 대한 시각화 분석 기술 등이 있다.

2.4.1 실시간 보안이벤트 필터링 기술

통합보안관제 솔루션은 보안시스템에서 생성하는 보안이벤트를 실시간으로 수집하여 분석할 수 있는 솔루션으로 이벤트를 종류별 또는 이벤트간 공통요소를 기반으로 분석이 가능하다. 즉, 동일 시간에 각종 정보보호시스템에서 동일한 공격대상 시스템에 대해 관련 보안이벤트가 발생하게 되면 이를 실시간으로 분석할 수 있다[4].

2.4.2 보안이벤트 상호연관분석 기술

보안이벤트 상호연관분석 기술은 ESM의 가장 핵심적인 기술로 다양한 보안이벤트 간의 상호연관 요소를 기반으로 침입을 추론하는 기술이며, 이에 대해서는 학문적, 상업적으로 활발한 연구가 진행되고 있으며, 관련 사례는 다음과 같다[5].

- 두 시스템간의 관계적인 요소 기반 분석
- 두 시스템간의 원인과 결과적 요소 기반 분석
- 세 시스템간의 원인과 결과적 요소 기반 분석

2.4.3 보안이벤트 시각화 분석 기술

보안이벤트 시각화 분석 기술은 네크워크상의 보안이벤트, 트래픽 정보들을 정보 시각화 기법을 이용하여 기존 텍스트 기반의 네트워크 정보시스템에서 찾기 어렵던 네트워크의 장애를 신속히 발견하여 신속하고 적적한 대처를 할 수 있게 해준다[6].

Ⅲ. Stealth기능 탑재 LINK관절 정보 설계

3.1 LINK관절 정보(자산) 설계

주요 정보자산의 자원식별번호 및 유통경로 등급을 포함하여 Self-Extracting 형태의 코드가 정보자산을 포함된다.

LINK관절 정보는 上記 정보가 유통될 수 있는 구역을 사전에 지정하고 있으며, 구역정보가 벗어나서 실행될 경우 자폭하거나 백도어가 작동되어 실행환경에 대한 정보를 브로드캐스팅하여 전달한다.

LINK관절 정보는 중요 정보자산에 캡슐형태로 제공되며, 중요 정보자산에 Key-chain으로 연결되어 임의 개봉 · 열람을 방지한다.

3.2 LINK관절에 Stealth기능 탑재 설계

LINK관절은 국가 및 공공기관에서 인정하는 네트워크상 경유지를 대상으로 하며, 경유지에서는 중요 정보자산의 다음 경유지 혹은 목적지까지 안전한 전송을 보증하며 처리결과를 최초 발신지로 정보를 제공한다.

3.3 Common(Plain) Data에 적용

LINK관절과 Key-Chain으로 중요정보가 생산될 경우, 문서의 특성 및 생산환경 정보 등 메타정보가 자동을 첨부된다.

중요정보에 LINK관절정보를 결합시 문서의 메타정보를 토대로 캡슐화되어 중요 정보자산을 보호한다.

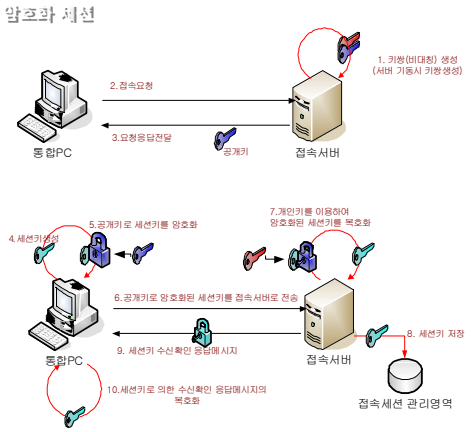

그림 4. 클라이언트와 서버간 암호화 세션

Ⅳ. Stealth기능 탑재 LINK관절 중요정보 구축

4.1 중요정보 Low, Middle, High flow

중요 정보자산의 중요도에 따라 중간 LINK관절에서 보안도가 강화된다.

High의 경우, 정보자산의 flow동안 해당 라우팅 경로에 다른 flow가 사용이 불가하도록 전용선의 서비스를 제공하며, Middle의 경우는 라우팅경로상 다른 Middle급 정보가 같이 존재할 수 있다. Low급 flow는 라우팅 경로를 다른 패킷과 공유하여 등급을 포함한다.

4.2 LINK관절 Stealth 기능 flow

현 LINK관절에서는 다음 LINK경유지까지 흐름간에 정보전송시 기존 LINK캡슐을 제거 후 새로운 LINK경유지의 정보를 재가공하여 정보전송을 한다.

재가공관련 정보를 최초 발신지에게 발신하여 정보의 흐름을 지속관찰 할 수 있도록 한다.

Ⅴ. 결 론

본 논문에서는 중요 정보자산을 확보하고 있는 국가 · 공공기관에서 자료전송간 정보유출을 방지하고 실시간으로 역추적할 수 있도록 LINK관절 시스템개념을 설계해보았다.

향후 연구로는 증권거래 패킷의 암복호화시 일어날 수 있는 취약점을 로그 분석하여 역추적하는 연구를 하여야 할 것이다.

참고문헌

[1] 한국인터넷진흥원 “2013년 7월 인터넷 침해사고 대응통계”, pp145. , 2012년 9월.

[2] 최대수, 이용균, “ESM에서 보안이벤트 분석 기술에 관한 연구”, 한국컴류터종합학술대회 논문집, Vol. 34, Np. 1(D), 2007년

[3] ㈜코스콤 PB시스템부, “코스콤 PowerBASE 암호화 대상 내역”, 2010년 10월.

[4] ㈜코스콤 증권ISAC, “2013년 3월 증권계 주요 경보이벤트 분석 결과”, 2013년 4월.

[5] Sterling, Bruce (1993). “Part 2(d)“. The Hacker Crackdown. McLean, Virginia: IndyPublish.com. p. 61. ISBN 1-4043-0641-2.

[6] Krapp, Peter (MIT Press Fall 2005). ““Terror and Play, or What was Hacktivism?“ Grey Room“. Retrieved 2013-02-28.