NIDPS기반 대용량 트래픽 제로데이 공격 피해 최소화를 위한 궤환 시스템

정장현, 최성곤
충북대학교
wkdgus4788@daum.net, choisg@cbnu.ac.kr

Feedback System to Minimize Damage by Zero-Day High-Volume Attack based on NIDPS

Jang Hyeon Jeong, Seong Gon Choi
Chungbuk National Univ.

요 약

본 논문에서는 대용량 트래픽 제로데이 공격으로 인한 피해 최소화를 위해 NIDPS기반의 궤환 시스템을 제안한다. 제안된 시스템은 수신된 패킷으로부터 세션 정보를 추출하여 일시적으로 저장하고 Payload에서 대용량 트래픽 공격의 시그니처를 추출하는 기법을 적용한다. 추출된 대용량 트래픽 공격의 시그니처와 해당 패킷의 세션 정보를 통해 NIDPS의 룰을 생성하고 적용한다. 대용량 트래픽 공격으로 의심되는 패킷을 차단하는 룰을 feedback하여 NIDPS로 적용함으로써 실시간으로 대용량 트래픽 제로데이 공격을 방어 할 수 있다. 제안된 시스템은 기존 제로데이 공격 방어 룰 적용 방식보다 시간을 단축할 수 있다.

Ⅰ. 서 론

Cisco 비주얼 네트워킹 인덱스에서는 전 세계 IP 트래픽은 꾸준히 증가하는 추세였으며 2022년은 4.8제타바이트로 2017년 대비 3배 가까이 증가할 것으로 예상하였다 [1]. 이러한 트래픽 증가 추세와 더불어 DDoS(Distribued Denial of Service) 공격과 같은 대용량의 트래픽을 발생시키는 악성 프로그램으로 인해 피해 사례가 계속해서 증가하고 있다 [2]. 이러한 공격들을 방어하기 위해 최근 시그니처 기반의 NIDPS(Network Intrusion Detection Prevention System)를 사용한다. NIDPS는 패킷의 헤더뿐만 아니라 payload까지 검사하는 DPI(Deep Packet Inspection)가 가능한 시스템이다. 또한 NIDPS는 IDS(Intrusion Detection System)와 IPS(Intrusion Prevention System)기능을 모두 가지고 있다[3]. IDS는 공격 위험이 있는 패턴을 가진 패킷들을 탐지하고 IPS는 시스템을 보호하기 위해 공격 위험이 있는 패턴을 가진 패킷들을 탐지 할뿐만 아니라 패킷을 차단하여 시스템을 보호하는 기능이 있다 [3]-[6]. 하지만 NIDPS을 포함한 모든 보안장비들에는 침투를 탐지 할 수 없는 보안 사각 지대가 존재한다 [6],[7]. 알려지지 않은 공격 패킷들이 수신되어 공격하는 것을 제로데이 공격이라고 한다 [7]. 제로데이 공격은 해당 공격 패킷을 인지하고 해당 공격을 방어할 수 있는 룰이 생기고 적용되어야한다 [8]. 하지만 이 과정은 수 시간에서 수일이 걸릴 수 있다 [9]. 그 시간동안 수신되는 제로데이 공격 패킷을 차단할 수 없기 때문에 제로데이 공격 시그니처를 자동적으로 추출하는 방안이 필요하다 [9].

제로데이 공격에 대한 정보를 얻기 위해 공격자를 유인하여 공격자나 알려지지 않은 공격 패킷에 대한 정보를 얻기 위한 시스템 HoenyPot이 사용되고 있다[10]. 또한 [9]에서는 Double Heavy Hitters 알고리즘을 활용하여 대용량 트래픽 제로데이 공격 시그니처를 추출하는 연구가 수행되었다. 하지만 기존 시스템들은 대용량 트래픽 제로데이 공격 시그니처를 추출하지만 실시간으로 방어할 수 는 없다. 따라서 용량 트래픽 제로데이 공격 시그니처를 자동적으로 추출하고 방어까지 가능한 방안이 필요하다.

본 논문에서는 대용량 트래픽 제로데이 공격 시그니처를 추출하여 실시간으로 방어할 수 있는 시스템을 제안한다. 제안된 시스템은 수신되는 패킷 중 기존에 알려진 공격 패턴을 가진 패킷은 차단하여 제로데이 공격 위험성이 존재하는 패킷들을 대상으로만 대용량 트래픽 공격 위험성이 있는 패킷의 시그니처를 추출하여 NIDPS엔진의 rule format에 맞는 룰을 생성한다. 생성된 룰을 feedback하여 NIDPS엔진에 적용함으로써 이후 같은 패턴을 가진 패킷을 차단한다.

Ⅱ. 본론

본 논문에서 제안하는 대용량 트래픽 제로데이 공격 피해 최소화를 위한 NIDPS기반의 궤환 시스템의 구성도는 그림 1과 같다.

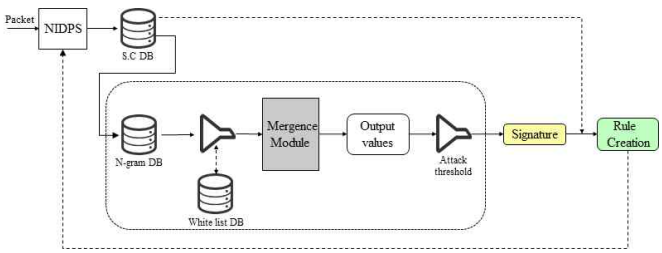

그림 1. NIDPS기반의 궤환 시스템 구성도

제안하는 시스템에서 이미 알려져 있는 공격 위험 패턴을 가진 패킷들을 NIDPS 엔진에 의해 차단된다. NIDPS 엔진을 통과한 패킷은 정상적인 패킷이거나 제로데이 공격 위험성이 있는 패킷일 수 있다. 제로데이 공격 위험성이 있는 패킷에 대한 대응을 하기 위해 S.C DB(Session Connectivity DataBase)는 수신되는 패킷의 Session정보를 일시적으로 저장하고 패킷의 payload에서 대용량 트래픽 제로데이 공격패턴을 추출하기 위해 N-gram DB로 payload를 전달한다. N-gram DB는 반복되는

문자열을 확인하기 위해 연속된 N개의 문자를 저장한다. Whitelist DB를 참조하여 N-gram DB에 저장된 연속되는 문자열 중 공격 위험성이 없는 문자열은 N-gram DB에서 삭제한다. Mergence Module은 연속적으로 반복되는 N길이 이상의 문자열을 병합하고 병합된 문자열이 threshold값 이상으로 빈번하게 반복되면 해당 패킷은 대용량 트래픽 제로데이 공격위험을 가진 패킷이라 판단한다. S.C DB에 저장되어있던 session 정보와 Output values, threshold로 추출된 시그니처를 임의의 NIDPS엔진의 rule format에 맞는 룰을 생성하여 NIDPS로 적용함으로써 이후 동일한 패턴을 가진 패킷을 차단할 수 있도록 한다.

제안된 시스템에 수신되는 TCP 패킷이 그림 2와 같고 N의 값은 4, threshold의 값은 6으로 설정할 때, 시스템의 동작을 설명한다.

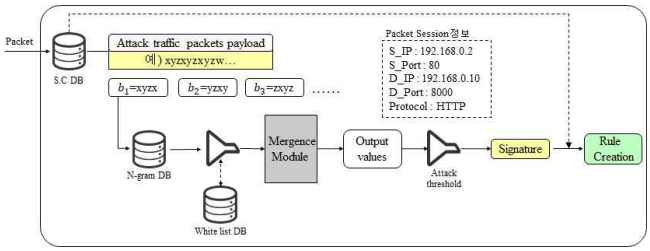

그림 2. 대용량 트래픽 제로데이 공격 차단 룰 생성

S.C DB는 해당 패킷의 session 정보를 추출하여 저장하고 패킷의 payload를 N-gram DB로 전달한다. Payload의 시작부분부터 4개의 연속된 문자 'xyzx'가 N-gram DB에 저장되어 있지 않으므로 새로 저장된다. 이후 한 인덱스를 이동하여 4개의 연속된 문자 'yzxy'도 N-gram DB(310)에 저장되어 있지 않으므로 새로 저장된다. 마찬가지로 한 인덱스를 이동하여 'zxyz' 또한 새로 저장된다. 이후 한 인덱스를 이동하면 'xyzx'가 나오는데 이 문자열은 이미 N-gram DB에 저장되어 있으므로 whitelist DB를 참조하여 'xyzx'가 무해한 데이터인지 확인한다. whitelist DB에 등록되어있지 않다면 Mergence Module로 이동한다. 만약 whitelist DB에 등록되어 있는 문자열이면 N-gram DB에서 해당 문자열을 삭제한다. Mergence Module에서 또 한 인덱스를 이동하여 'yzxy'가 N-gram DB에 등록되어 있으므로 'xyzx'와 'yzxy'가 빈번하게 연속해서 나오는 것을 확인하고 두 문자열을 병합해서 'xyzxy'를 만든다. 위의 방식으로 시스템 동작이 완료 되면 Output values는 'xyzxyz' 값을 가지게 된다. 전체 payload에서 'xyzxyz' 값이 threshold로 설정한 6번 이상 나온다면 해당 문자열은 알려지지 않은 대용량 트래픽 공격 패턴을 가진 패킷의 시그니처로 판단되고 S.C DB에 저장되어 있던 session 정보와 Output values, threshold를 사용하여 NIDPS엔진에 맞은 새로운 룰 생성하고 S.C DB와 N-gram DB를 초기화한다.

그림 2의 결과로 추출된 시그니처를 NIDPS엔진의 일종인 suricata의 룰로 생성하게 되면 그림 3과 같은 룰이 생성될 수 있다. 그림 3의 룰을 그림 1과 같이 feedback하여 suricata에 적용하게 되면 그림 2의 패턴을 가진 http response 패킷을 차단 할 수 있다.

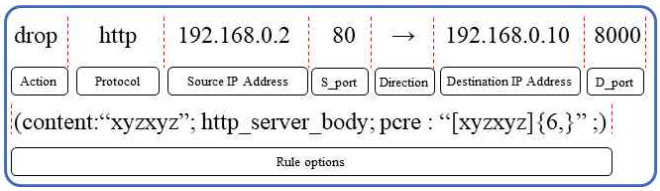

그림 3. 대용량 트래픽 공격 차단을 위한 suricata 룰

Ⅲ. 결론

본 논문에서는 대용량 트래픽 제로데이 공격으로 인한 피해 최소화를 위해 NIDPS기반의 궤환 시스템을 제안하였다. 제안된 시스템은 시그니처 기반의 NIDPS엔진을 사용하여 알려진 공격 패턴을 가진 패킷은 차단하고 제로데이 공격 위험이 있는 패킷들 중 대용량 트래픽 공격 패턴을 가진 패킷의 시그니처를 추출한다. 추출한 시그니처와 session 정보를 기반으로 NIDPS 엔진의 룰 포맷에 맞는 룰을 생성한다. 이렇게 생성된 룰을 feedback 하여 NIDPS 적용한다. 이를 통해 제로데이 대용량 트래픽 공격 방어를 위한 룰 업데이트 시간을 기존 방식보다 단축할 수 있다. 결과적으로, 제안된 시스템은 대용량 트래픽 제로데이 공격 피해를 최소화 할 수 있다.

ACKNOWLEDGMENT

"이 논문은 2020년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2020R1A6A1A12047945),

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학 지원사업의 연구결과로 수행되었음"(2019-0-01183)

*교신저자 : choisg@cbnu.ac.kr

참 고 문 헌

[1] Cisco Visual Networking Index, "Cisco 비주얼 네트워킹 인덱스 2017 ~ 2022년 전망 및 추세"

[2] 이우식, 오현석, 김남기, 최윤호, "다양한 대용량 공격 트래픽을 효과적으로 차단하기 위한 보안 서비스 체이닝 기술", 한국통신학회 학술대회 논문집, Jan. 2014, pp. 798-799

[3] Jang Hyeon Jeong, Seong Gon Choi"Rule conversion system between NIDPS engines", Kics 추계종합학술발표회 no.11, 2019

[4] kash Garg and Prachi Maheshwari, "A hybrid intrusion detection system: A review", 2016 10th International Conference on Intelligent Systems and Control (ISCO), Jan. 2016.

[5] Alaa Hussein Al-Hamami, Ghossoon M. Waleed Al-Saadoon, "Development of a network-based: Intrusion Prevention System using a Data Mining approach", 2013 Science and Information Conference, pp. 641-644, Oct. 2013.

[6] Jang Hyeon Jeong, Seong Gon Choi"SCA System for minimizing damage of Zero-Day attack", 2020년도 한국통신학회 동계종합학술발표회 논문집, Feb. 2020, pp. 100-101

[7] (2019) The Xabyss website [Online]. Available: http://www.xabyss.com/

[8] Nisreen Innab, Eman Alomairy, Lamya Alsheddi, "Hybrid System Between Anomaly Based Detection System and Honeypot to Detect Zero Day Attack", 2018 21st Saudi Computer Society National Computer Conference (NCC)

[9] Yehuda Afek, Anat Bremler-Barr, Shir Landau Feibish, "Zero-Day Signature Extraction for High-Volume Attacks", IEEE/ACM Transactions on Networking, Vol: 27, Issue: 2, April 2019, pp.691-706