ESM 상호연관분석을 통한 악성코드 탐지정책에 관한 연구

김학수*
*고려대학교 컴퓨터정보통신대학원
e-mail:securiter@korea.ac.kr

A Study on Malicious Code Detecting Policy by ESM Correlation

HakSoo Kim*
*Graduate School of Computer & Information Technology, Korea University

요 약

갈수록 심각해져가는 보안위협 속에 많은 기관들은 다양한 정보보호시스템을 구축하고, 이를 통합하는 통합보안관리시스템을 운영하고 있다. 이러한 통합보안관리시스템은 이기종간 보안로그를 상호연관분석 할 수 있는 기능을 다양한 방법을 통해 제공하고 있다. 이러한 다양한 상호연관분석 방법 중 다단계 상호연관분석 방법을 이용한 통합보안관리시스템에서 내부자원이 악성코드에 악용되는 걸 사전에 탐지할 수 있는 상호연관분석 정책을 제안한다.

1. 서론

대부분의 국가기관 및 금융, 기업체에서 운영 중인 통합보안관리시스템은 외부로부터의 공격에만 관심을 갖고 보안 정책을 외부 공격에 초점을 맞춰 수립한다. 또한 내부자원(PC)에 대한 보안정책으로 Anti-Virus 설치, 보안 USB 시스템 구축, OS 보안패치 시스템 등을 운영하는 것으로 내부자원(PC)보안이 완벽하게 수행된다고 생각하고 있다. 하지만 이러한 정책은 내부자원(PC)에 대한 보안정책이 Anti-Virus 제품 등에 의존적이며 내부자원(PC)이 악성코드에 악용되는 것에 대한 수동적 대응 자세이다.

본 논문에서는 내부 자원(PC)이 악의적인 공격에 악용되는 것을 사전에 탐지하여 추가적인 악용을 방지하기위한 능동적 대응 방법으로 통합보안관리시스템의 상호연관분석 기능을 이용한 악성코드 탐지 정책설정 방법을 제안한다. 2장에서는 지금까지 연구되어왔던 상호연관분석 기법을 소개하고, 3장에서는 내부자원(PC)의 악성코드 감염 탐지를 위한 상호연관분석 정책을 제안하며, 4장에서 결론을 맺는다.

2. 상호연관분석에 관한 관련연구

보안경보에 대한 연구는 단일 보안경보에 의해 침해시도여부를 탐지하는 방법과 개별적인 단일 보안경보 간의 연관성을 찾아 침해시도여부를 탐지하는 방법이 있다.

단일 보안경보에 의한 침해시도 탐지 방법은 침입탐지시스템을 이용한 방법이 주를 이루었으며, 이러한 침입탐지시스템의 가장 큰 단점으로 오탐에 의한 보안경보 플러딩 현상이 지적되어 왔다. 침입탐지시스템은 False Negative Detection (Rate)을 낮추기 위해 아주 작은 의심행위도 경보를 발생시키고, 이러한 경보는 높은 False Positive Detection (Rate)을 초래하게 되어 보안경보 플러딩이 발생한다. 이러한 보안경보 플러딩은 보안 담당자로부터 정확한 보안 상태를 파악하기 힘들게 하며, 보안 상태에 대한 적절한 상황판단을 하지 못하는 것은 통합보안관리시스템을 구축한 목적인 조기경보탐지를 이루지 못하는 결과를 가져오게 된다.[1]

위와 같은 단일 보안경보에 의한 탐지방법의 한계 때문에 많은 양의 보안경보로부터 의미 있는 데이터를 찾기 위한 경보 클러스터링 방법[2][3], 공격 시나리오 방법[4][5], 조건 비교 방법[6], 다단계 상호연관분석 방법[7] 등 상호연관성분석이 활발히 논의되고 있다.

이중 다단계 상호연관분석 시스템은 단일 보안시스템에서 발생하는 모든 보안경보를 통합된 서버에 수집한 후 상호연관분석을 실행하는 것이 아니라 센서단계에서 1단계 상호연관분석을 실시한 후 통합서버에서 2단계 상호연관분석을 실시함으로써 통합서버의 정보처리 부하를 분산시켜주며, 단계별 경보검증과정을 수행하기 때문에 상호연관분석결과의 정확도를 높일 수 있다.

하지만 이러한 다단계 상호연관분석 시스템은 상호연관분석의 정확도와 성능부하를 예방하기 위해 제안된 시스템이며, 적절한 상호연관분석 정책은 제시하지 못하고 있다. 적절하지 못한 정책은 오히려 수많은 보안경보 플러딩을 발생시키고 이로 인하여 적절한 조기탐지가 불가능하다.

이와 같은 문제점을 보완하기 위해 본 논문에서는 다단계 상호연관분석 시스템에 기반을 두고 단일 경보 시스템을 상호연관분석 하여, 보안경보 플러딩을 줄이면서 단일 경보 시스템에서는 탐지할 수 없는 악성코드 유포사이트를 탐지할 수 있는 상호연관분석 정책을 제안한다.

3. 악성코드 탐지를 위한 상호연관분석 정책 제안

본 논문에서 제안하는 상호연관분석 정책은 통합보안관리시스템을 이용하여 추가적인 악성코드 감염 탐지 및 변

형된 악성코드 감염 탐지 정책으로 단일 악성코드 감염보안경보와 비교하기 위해 동일한 네트워크 통신경로를 이용하는 내부자원(PC) 40,000대를 대상으로 20일간 비교분석하였다.

먼저 단일 보안경보에 의한 악성코드 탐지 건수를 보면 일평균 355건의 단일 보안경보가 발생하였으며, 내부자원(PC)가 거의 사용되지 않는 주말을 제외한 평일 15일의 평균 단일 보안경보는 456건이나 되었다. 또한 특정 악성코드가 확산되었던 17일에는 평일 평균의 2배에 가까운 919건의 보안경보가 발생하였다. 이러한 많은 양의 단일 보안경보는 악성코드에 감염 된 내부자원(PC)을 발견한 후 외부로 접속한 IP를 방화벽로그에서 따로 찾아야 하기 때문에 조기 탐지에 한계성을 보여준다.

제안하는 다단계 상호연관분석 방법을 이용한 악성코드 탐지 방법은 Anti-Virus와 방화벽을 기반으로 Anti-Virus와 방화벽에서 발생하는 단일 경보를 이용하여 단계별로 상호연관분석한다.

- 1단계 : 단일 보안경보수집
  - Anti-Virus : 1 건/min
  - 방화벽 : 20 건/min
- 2단계 : 1단계 결과를 기반으로 상호연관분석 실시
  - Same Source IP, Same Destination IP

상호연관분석을 이용한 악성코드 감염 탐지 정책을 40,000여대의 PC를 관리하고 있는 통합보안관리시스템에 20일간 적용한 결과 총384건의 상호연관분석 경보가 발생하였으며, 그 중 20건이 악성코드를 추가로 유포하는 사이트로 확인되었다. 이 결과는 40,000여대 PC에 추가적인 악성코드 감염 위험을 사전에 방지 할 수 있었다.

또한 악성코드 감염 탐지에 대한 단일 보안경보와 상호연관분석경보 건수를 비교한 결과 <표 1>과 같은 결과를 얻을 수 있었다.

<표 1> 보안경보 플러딩 감소 비율

구분	단일경보(건)	상호연관분석경보(건)	감소비율(%)
1일	437	11	39.7
2일	445	19	23.4
3일	499	73	6.8
4일	424	29	14.6
5일	84	5	16.8
6일	40	3	13.3
7일	377	36	10.5
8일	396	17	23.3
9일	429	16	26.8
10일	417	24	17.4
11일	415	31	13.4
12일	29	1	29.0
13일	40	2	20.0
14일	539	22	24.5
15일	374	25	15.0
16일	341	12	28.4
17일	919	24	38.3
18일	577	32	18.0
19일	259	1	259.0
20일	60	1	60.0
총계	7,101	384	18.5

<표 1>의 결과를 분석한 결과 Worst-Case인 경우인 3일에는 단일 보안경보는 499건이지만 상호연관분석경보는 73건으로 보안경보 감소비율이 7.3%밖에 되지 않았지만, Best-Case인 19일에는 단일 보안경보는 259건이지만 상호연관분석경보는 1건으로 보안경보 감소비율이 259%라는 결과를 확인할 수 있었다.

5. 결론

본 논문에서 제안한 다단계 상호연관분석을 이용한 악성코드 탐지 정책은 많은 양의 보안경보 플러딩에서 유효한 경보만을 골라내어 보안 관리자에게 알려줌으로써 보안 관리자로 하여금 보다 정확한 판단을 할 수 있는 근거를 제공하는 효과를 얻을 수 있었으며, Anti-Virus에서 발생한 경보와 방화벽 경보를 상호연관분석을 통해 조기 탐지의 효과를 획득할 수 있다. 또한 단일 보안경보에서는 발견할 수 없었던 악성코드를 유포하는 사이트를 탐지 할 수 있어 악성코드가 다른 내부자원(PC)으로 위험이 확산되는 걸 사전에 방지할 수 있었다.

본 논문에서 제안한 다단계 상호연관분석을 이용한 악성코드 탐지 정책 기술의 정확도를 높이기 위해 향후 탐지 정책 중 신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크에 대한 정확한 분류 기준을 세우는 연구가 필요하며, 또한 악성코드 탐지 수행을 위해 감염된 악성코드를 조치하는 방법에 따라 정책을 세분화하는 연구가 추가적으로 진행되어야 할 것이다.

참고문헌

[1] Stefan Axelsson. Intrusion Detection Systems: A Survey and Taxonomy, Technical report 99-15. Chalmers University of Technology, Sweden, March 2000.

[2] A. Valdes, K. Skinner, "Probabilistic Alert Correlation", RAID 2001.

[3] O. Dain, R. Cunninghan, "Building Scenarios from a Heterogeneous Alert Stream", IEEE Workshop on Information Assurance and Security, 2001

[4] H. Debar, A. Wespi, "Aggregation and Correlation of Intrusion-Detection Alerts", RAID 2001

[5] B. Morin, H. Debar, "Correlation of Intrusion Symptoms : an Application of Chronicles", RAID 2003

[6] F. Cuppens, A. Miege, "Alert Correlation in a Cooperative Intrusion Detection Framework", In IEEE Symposium on Security and Privacy, 2002

[7] 최대수, 이용균, "보안경보 검증을 확장한 다단계 상호연관분석에 관한 연구", 정보처리학회 제12권 제2호, pp.1059~1062, 2005