APT 해킹 공격에 대한 전조현상 분석 및 IP역추적

* 노정호· 박대우*

*호서대학교 벤처전문대학원

A Precursor Phenomena Analysis of APT Hacking Attack and IP Traceback

Noh Jung Ho · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : network87@daum.net · prof_pdw@naver.com

요 약

Log는 시스템을 사용하는 모든 자료에 남는 시스템 파일이다. 지금 IT에 이슈화 되고 있는 농협사태, Nate On 정보 유출, 언론기관 서버마비 등 해킹에 의한 범죄가 많이 일어나고 있다. 이에 로그를 전문적으로 분석하는 소프트웨어를 통해 일어나고 있는 해킹 사태에 대해 전문분석이 필요하다. 본 연구는 지능적으로 일어나는 APT 공격에 대해 로그분석으로 패턴을 분석해 이상 Log 발생 시 역추적 하여 사전에 예방하는 기술에 대해 기술한다.

ABSTRACT

Log is a file system, a system that uses all remaining data. Want situation now being issued in the IT, media Nate on information disclosure, the press agency server hack by numbness crime occurred. Hacking crisis that's going through this log analysis software professionally for professional analysis is needed. The present study, about APT attacks happening intelligently Log In case of more than traceback in advance to prevent the technology to analyze the pattern for log analysis techniques.

키워드

Packet Analysis, IP Traceback, Forensic, Hacking Attacks, Audit Log Record

Ⅰ. 서 론

2013 3.20 KBS, MBC, YTN 언론기관이 해킹 공격을 받아서 서버가 다운되고 그림1 3.20 대란 이어 방송사 전산사고 연발 신문자료와 같이

그림1 3.20 대란 이어 방송사 전산사고 연발

32,000 PC가 손상되어 부팅이 되지 않았다. 또한 신한은행과 NH농협의 금융 서버 일부가 마비되어 금융거래가 되지 않아 국민들이 불편을 겪었다. 정부는 3.20 사이버테러의 결과를 분석한 결과 공격자는 수개월동안 지속적으로 APT 공격(Advanced Persistent Threat)을 수행하여, 단말기를 감염시키고, PMS(Patch Management System)을 통해 악성코드를 전파하여 일순간에 공격을 실행 한 것으로 분석하였다고 발표했다.

이러한 사이버테러의 외부로 부터의 공격은 소읽고 외양간 고치기지만 그동안 사이버테러, NH농협 사태처럼 그림2 NH농협 전산망 마비 기사와 같은 사태에 대해서 만약 의심스러운 메일이나 패킷을 분석했다면 전조 증상은 파악 할 수 있었고, 특히 APT 공격에 대한 해킹 사고에 대한 사전 경고와 더불어 예방조치와 침해사고 대응조치를 해서 사이버테러로 부터의 피해를 최소화 했을 가능성이 높다.

NH농협 '전산망 마비'

(서울=뉴스1) 오대일 기자
입력 2013.03.20 15:44:33 | 최종수정 2013.04.04 21:00:38

기사스크랩:

(서울=뉴스1) 오대일 기자= KBS, MBC, YTN 등 주요 방송사와 신한은행, 농협 등 일부 금융사들의 전산망이 마비된 20일 오후 서울 여의도 국회의사당 내 NH농협은행 국회지점에서 은행 관계자가 ATM 기기에 전산장애 안내문을 부착하고 있다. 경찰청 사이버테러대응센터는 "전산장애 관련한 신고가 들어와 현장에 수사관을 투입했다"며 "현장에서 사이버테러 등 다양한 가능성을 열어두고 점검해볼 것"이라고 밝혔다. 2013.3.20/뉴스1

kkorazi@news1.kr

그림 2 NH농협 전산망 마비

따라서 본 논문에서는 APT 해킹공격에 대한 전조 현상을 연구한다. WireShark 분석도구를 사용하여 프로토콜 종류, Flags값, Source IP, Destination IP, TTL값, port 번호 등을 분석하고, 통계를 작성하여 사이버테러에 대한 APT 공격의 전조현상을 분석 연구한다. 그리고 전조현상이 시스템으로 분석 한 후, IP 역추적을 통하여 공격자를 찾고, 공격 자료에 대한 포렌식(Forensic) 자료를 확보하여 증거로 채택되게 하여, 공격자에 대한 법적인 책임을 지울 수 있는 보안 방법을 연구한다.

II. 관련연구

2.1 Log분석

쌍용자동차나 반도체기술유출 사건에서와 같이 기업의 기술정보가 유출된 사례들이 증가하였다. 기술유출 사건의 조사에서 사용되는 것이 Log 분석이다. 중요서버에 접속자에 대한 IP, 접속자, 시간, 접속용도 등에 대한 log 분석이 필요하다[1].

통합 로그분석 시스템은 사전에 분석된 위협룰에 근거하여 기밀정보 유출 가능 행위들을 사전에 탐지하는 시스템으로, 보안 및 업무단위 시스템을 연동하여 사용자의 모든 행위 로그를 수집하는 로그수집 모듈, 룰에 의해 비정상 유출행위를 탐지하며 보안지수를 생성하는 로그분석 모듈, 탐지 결과 보고서를 생성하는 모듈로 구성된다[2].

2.2 IP 역추적

보안 시스템은 최근 능동적인 시스템으로 발전되고 있고 IP 역추적 기술을 이용한 능동적 보안 시스템으로 변하고 있다.

IP 역추적을 위해 ICMP 형태의 역추적 메시지를 사용한다. 해커는 자신의 Real IP주소의 노출을 피하기 위하여 우회적인 공격을 한다. 공격자를 발견하기 위해서는 IP 역추적을 실시해야 한다. Real IP역추적을 위하여 IP역추적 서버와 에이전트 모듈이 필요하다. 공격자의 Real IP는 Whois 서비스로 실체를 확인하고, 이를 법정의 증거자료로 삼기 위한 무결성과 신뢰성을 확보한 Forensic 자료를 생성한다[3].

2.3 감사기록

초고속 인터넷의 웹 서비스를 사용하여 WAS를 통한 DBMS 접근이 늘어나고 있다. WAS를 통해 DBMS에 우회접속을 하면 DBMS는 우회접속 사용자의 IP정보를 저장하지 못하고, 직전 시스템에 접속한 사용자인 WAS의 정보를 저장하게 된다. 보안 신뢰성의 향상 방법으로, log을 받아 Pattern 분석 후에 Rule을 만들어 적용하고, Module을 개발해 정보의 수집 및 압축을 통해 데이터 저장소에 보관한다. 보관된 정보는 지능형 DB보안 클라이언트를 이용한 분석과 정책 기반 관리 모듈의 통제를 통해 역추적의 오탐 확률을 최소화할 수 있게 한다[4].

불법 공격자인 해커가 자신의 위치추적을 피하기 위하여, 피해 시스템을 직접 공격하지 않고 우회 공격을 수행한다. 공격자인 이동단말에 대한 역추적을 할 때, 실시간 네트워크 로그 감사기록을 이용하고, TCP/IP와 네트워크 기반에서는 Thumbprint Algorithm, Timing based Algorithm, TCP Sequence number 등을 이용한 알고리즘 및 SWT 기법 등을 이용한 역추적 기법을 사용한다[5].

2,4 포렌식

GM대우차와 쌍용차에 관한 기술 유출 사고에서의 국가 경제적인 피해로 인하여 포렌식 e-Discovery 제도가 필요하다. e-Discovery가 도입되면 포렌식 자료[6]를 확보하기 위한 보안관제 시스템에서 증거 자료의 확보가 가능하다.

인터넷 이용자의 74%가 UCC를 이용하고 있고, You Tube를 이용한 총기범죄가 발생하였다. 인터넷 UCC속에 나타난 인터넷 범죄의 양태를 분석하고 추적하는 네트워크 포렌식 방법과 기법에 대한 기술이 필요하다[7].

III. APT 해킹공격에 대한 전조현상 분석

3.1 APT 공격 내용 분석

2013년 3월 20일 발생한 3.20 사이버테러 사건의 YTN, KBS, MBC 언론기관과 신한은행 NH농협 등 이 사이버 피해를 받았으며 피해분석 내용은 아래와 같다.

표 1. 3.20 사이버테러 사건일지

1보 (03/20 17:56)	2013년 3월 20일 오후 1:29:28 국내 금융권 및 방송사를 대상으로 전산 장애가 동시 다발적으로 발생하였으며 NSHC의 Red Alert팀은 최근 금융 / 공공기관을 대상으로 하는 신규 악송코드를 계속해서

	연구 하였으며 본 사태의 원인으로 대한민국 주요 기반 시설 전산망을 상대로 한 북한의 “사이버 테러”일 가능성에 비중을 두고 있다. 현재 NSHC는 금융 고객사의 정보 제공을 통해 전문 보안 전문가를 현장에 급하 했으며 관련 기관들과 협조를 통해 데이터를 복구, 침해 사고 원인인 악성 코드를 분석 중.
2보 (03/20 20:45)	악성코드 샘플을 수집하여, 샘플에 대한 정보 및 스트링 분석 결과를 업데이트 하였고, 동적 분석 및 정적 분석을 진행 중.
3보 (03/21 00:37)	악성코드 샘플 분석결과 마스터 부트 레코드(MBR)영역을 포함하여, 볼륨 부트 레코드(VBR)까지 손상 됨 악성코드의 동작을 요약하면, 특정 프로세스를 종료시키고 MBR 영역과 VBR 영역을 Overwriting 한 후 시스템 재부팅을 유도.
4보 (03/21 06:57)	최조 확인된 악성코드 샘플과 유사한 동작을 하느 파일을 확인 하였으나 유포 경로에 대해서는 현재까지 파악이 안되었으며 이와 관련된 추측성 정보가 여럿 확인되지만 근거를 제시하기에 부족한 부분이 있다고 판단 그래서 기술적인 피해 분석 및 복구에 초점을 맞추고 작업을 진행 예정 추가로 피해 시스템의 손상된 데이터 복구 지원을 위해 복구 자동화 솔루션을 개발 완료상태.

표 1은 3.20 사이버테러 사건일지를 나타낸다.

3.2 실시간 모니터링

APT 공격에 대한 사전에 전조현상을 분석하기 위해서는, 그림 3처럼 침입 이벤트에 대한 실시간 모니터링을 실시하여야 한다.

그림 3 침입 이벤트에 대한 실시간 모니터링

접속자의 권한과 가용성에 따른 시간과 접속 패킷, 접속 보안 등급별 패킷을 분석 할 수 있다.

3.3 APT 공격에 대한 전조 현상분석

APT 공격에 대한 전조 현상분석을 위하여, 로그 분석을 통해 실시간으로 해당 지역마다 로그의 양을 한눈에 알아 볼 수 있으며 공격 탐지 현황을 통해 침해사고에 대한 전조현상을 조기 탐지를 할 수 있다.

로그분석 시스템을 통해 그림 4처럼 위협/장애에 대한 접수 이벤트를 통해 각 시스템에 발생한 보안사고 발생에 대해 사전 감지를 하며 감지한 정보들은 관리자에게 위협분석 목록 리스트로 보여주며 각 위협 정보들의 통계로 그래프 형태로 표현해 준다.

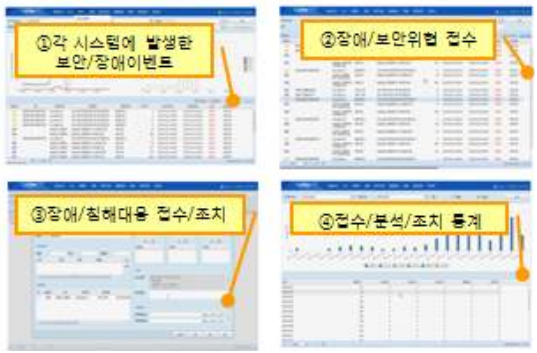

그림 4. 위협/장애에 대한 접수 이벤트

Ⅳ. 패킷 분석과 IP 역추적

4.1 패킷분석

IP의 주소를 그림5처럼 WireShark를 이용한 분석을 할 수 있으며 세부적으로 분석으로는 IP에 대한 프로토콜 종류, Flags값, Source IP, DestinationIP, TTL값을 분석 할 수 있다.

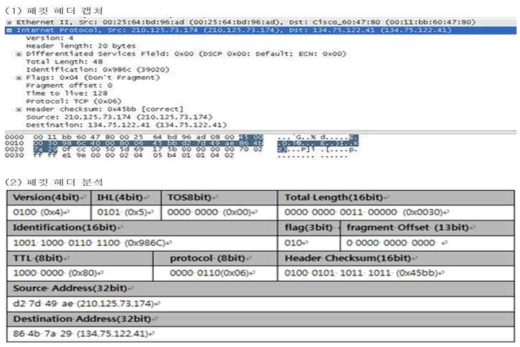

그림 5. WireShard를 이용한 분석

4.2 시스템 자원 분석

로그 분석 시스템은 그림6처럼 구글 맵과 로그 솔루션 연동을 통해 관제화면을 구성하며 이렇게 구현된 관제 화면은 보안/장애 등의 다양한 이벤트를 토폴로지 상에서 시스템 자원을 보여줌으로써, 개별 장비 및 장비간의 연계된 이벤트 상황을 쉽게 파악하고, 즉시 대응/조치 함 으로써 서비스 장애를 최소화 할 수 있다

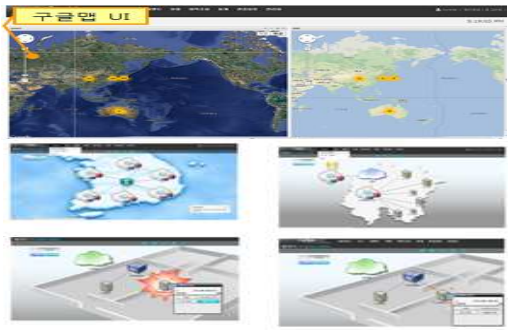

그림 6. 구글 맵과 로그 솔루션 연동

4.3 시스템 사용이력 분석 및 역추적

로그 분석을 통해 작업에 대한 처리내역에 대한 정보를 그림7처럼 시스템 사용이력 및 메일발송 이력을 통해 시스템 사용한 Source IP, Destination IP, Source Port, Destination Port, 사용한 시간, 작업유형, 작업일시에 대한 이력 및 메일발송이력을 한눈에 파악을 함으로써 각각의 사용내역을 기간별로 조회하여 관리자는 시스템에 대한 모든 이력을 관리하는 기능으로 누가 언제 시스템에 사용을 했는지 알 수 있다.

그림 7. 시스템 사용이력 및 메일발송 이력

4.4 포렌식 보고서 작성

시스템을 사용하는 관리자가 로그 분석 솔루션을 통해 그림 8과 같이 시스템에 접근한 사용자 이력에 대해 일일 보고서 목록으로 확인 할 수 있으며 그 외에 각 시스템에 대한 성능보고 와 일반 사용자에 대한 계정승인을 보고 하는 기능을 보여준다.

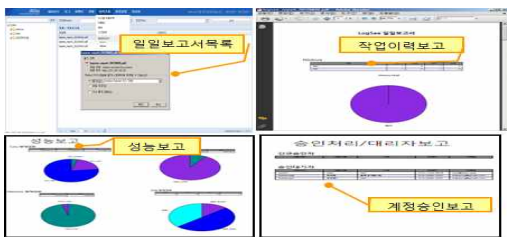

그림 8. 시스템에 접근한 사용자들 이력

V. 결 론

본 연구는 지능적으로 일어나는 APT 공격에 대해 로그분석으로 패턴을 분석해 이상 Log 발생 시 역추적 하여 사전에 예방하는 기술에 대해 기술하였다.

향후 연구로는 로그를 전문적으로 분석하는 소프트웨어를 이용하여 APT공격을 분석하고 추적하는 연구가 필요하며

로그 분석을 통해 APT 공격을 하는 IP 목적지가 확실하게 파악이 되면 역으로 DOS 공격을 하여 해당 공격자 PC를 파괴 하는 방법을 연구 하여야 할 것이다.

참고문헌

[1] "Korea Internet White Paper",Korea Internet and Security Agency(2012), pp.311-316, 2012.10,

[2] Jae-Yong Lee, Soo young Kang , “Design and Verification of the Integrated Log Analysis System for Enterprise Information Security”, Journal of digital contents society, Vol.9, No.3, pp.491-498, 2008.

[3] Jae Dong Kim, Jeon Ju Chae, Jea Kwang Lee,“Active Security System using IP Traceback Technology”, The journal of the Korea Institute of Maritime Information & Communication Sciences , Vol.11, No.5, pp.933-939, 2007.

[4] Jong Il Baek, Dea-Woo Park, “A Study on Traceback by WAS Bypass Access Query Information of DataBase ”, Journal of the Korea society of computer and information, Vol.14, No.12=No.69, pp.181-190, 2009.

[5] Dea-Woo Park, Seung Rin Lim, “A Study of the Back-tracking Techniques against Hacker's Mobile Station on WiBro”, Journal of the Korea society of computer and information, Vol.12 No.3=No.47, pp.185-194, 2007.

[6] Woo Sung Chun, Dea-Woo Park, “A Study of Authentication and encryption for e-Discovery Forensic Data”The Korea Society of Computer and Information, Vol.19, No.2, pp.185-189, 2011.6.30

[7] Kyu Ahn Lee, Dea-Woo Park, Yong Tae Sin, “A Study of Network Forensics related to Internet Criminal at UCC”, Journal of the Korea society of computer and information, Vol.13, No.2=No.52 pp.143-151, 2008.