빅데이터 분석을 통한 APT공격 전조 현상 분석

최찬영* · 박대우*

*호서대학교 벤처대학원

The Analysis of the APT Prelude by Big Data Analytics

Chan-young Choi* · Dea-woo Park*

*Hoseo Graduate School of Venture

E-mail : cchany@fsec.or.kr, prof_pdw@naver.com

요 약

2011년 NH농협 전산망마비 사건, 2013년 3.20 사이버테러 및 2015년 12월의 한국수력원자력 원전 중요자료 유출사건이 있었다. 이러한 사이버테러는 해외(북한)에서 조직적이고 장기간의 걸친 고도화된 APT공격을 감행하여 발생한 사이버테러 사건이다. 하지만, 이러한 APT공격(Advanced Persistent Threat Attack)을 방어하기 위한 탁월한 방안 아직 마련되지 못했다. APT공격은 현재의 관제 방식으로는 방어하기가 힘들다. 따라서, 본 논문에서는 빅데이터 분석을 통해 APT공격을 예측할 수 있는 방안을 연구한다. 본 연구는 대한민국 3계층 보안관제 체계 중, 정보공유분석센터(ISAC)를 기준으로 하여 빅데이터 분석, APT공격 및 취약점 분석에 대해서 연구와 조사를 한다. 그리고 외부의 블랙리스트 IP 및 DNS Log를 이용한 APT공격 예측 방안의 설계 방법, 그리고 전조현상 분석 방법 및 APT공격에 대한 대응방안에 대해 연구한다.

ABSTRACT

The NH-NongHyup network and servers were paralyzed in 2011, in the 2013 3.20 cyber attack happened and Classified documents of Korea Hydro & Nuclear Power Co. Ltd were leaked on December in 2015. All of them were conducted by a foreign country. These attacks were planned for a long time compared to the script kids attacks and the techniques used were very complex and sophisticated. However, no successful solution has been implemented to defend an APT attack thus far. Therefore, we will use big data analytics to analyze whether or not APT attack has occurred in order to defend against the manipulative attackers. This research is based on the data collected through ISAC monitoring among 3 hierarchical Korean defense system. First, we will introduce related research about big data analytics and machine learning. Then, we design two big data analytics models to detect an APT attack and evaluate the models' accuracy and other results. Lastly, we will present an effective response method to address a detected APT attack.

키워드

빅데이터 분석(Big Data Analytics), APT공격, 전조 현상(Prelude), 사이버테러

Ⅰ. 서 론

최근 북한의 핵실험, 중동의 ISIS 테러 등 물리적인 위협과 더불어 중국, 미국, 러시아 및 해외 등의 사이버테러는 현대의 디지털화된 사회에서 큰 위협으로 다가오고 있다.

일반적인 해킹공격은 그 피해가 제한적이지만, 사회 인프라에 피해를 유발하는, 국가적 사이버테러공격은 핵발전소에서 방사능 유출, 국민경제를 마비시키는 금융거래 중지 등의 피해가 커질 수 있다. 따라서, 보이지 않는 세계에서 발생하는 사이버테러는 보이는 세계에서 발생하는 물리적 전쟁과 마찬가지로 대비를 해야 한다.

현재까지 우리나라 대상 조직적 고도화된 공격인 APT공격이 여러 차례 있었으며 금융권 대상의 APT공격 중에 가장 큰 사건 2개는 NH농협 전산망마비와 3.20 사이버테러라 하겠다.

먼저 NH농협 전산망마비 사건을 살펴보면

APT공격자는 D-day(‘11.4.12) 7개월 전 외부업체 직원이 웹하드 무료 다운로드 쿠폰으로 업무 노트북에 영화를 다운로드 할 때 악성코드를 해당 노트북에 설치하게 하였고 그 후에는 추가적인 악성코드를 다운시켰으며 관리자 비밀번호 등 전산망 정보를 수집하였다. D-day에는 공격 명령 파일 설치 후 원격 공격을 감행하여 공격 개시 30분만에 운영 시스템의 절반을 파괴하였다[1].

3.20 사이버테러는 백신 등의 S/W 중앙배포서버를 이용하여 ‘13.3.20일 전산장비 파괴용 악성코드를 공격대상 PC 및 서버에 8개월간 설치한 장기간의 고도화된 APT공격이었다. 동 공격에 사용된 악성코드는 67종에 이르며 파악된 해킹 경유지만 해외 24곳, 국내 25곳에 이른다[2].

2015년 한국수력원자력 원전 중요자료 유출사건은 해킹공격 기간은 4개월 정도로 타 APT공격과 비교하여 짧다. 하지만, ‘한글’ 프로그램의 제로데이 취약점을 이용하였고 한국수력원자력 직원 3,571명을 대상으로 하였다[3]. 해킹에 대한 피해는 거의 없었으나 해킹공격으로 방사능 유출도 될 수 있다는 불안감을 준 사건이었다.

정부와 한국인터넷진흥원 등에서는 사이버테러에 대한 IP를 역추적하여 공격자에 대한 블랙리스트(Blacklist)를 만든 후 해당 정보 공유하여 라우터와 침입차단시스템에서 이용하도록 하는 등의 노력을 하고 있다. 하지만, 이러한 대규모 APT공격을 사전에 분석・탐지하지 못했다는 점에서 기존 관제의 한계를 알 수 있으며, 날로 고도화되고 있는 APT공격에 맞춰 빅데이터 분석 등을 이용한 APT공격 분석도 고도화가 필요하다고 하겠다.

본 연구에서는 먼저 빅데이터 분석을 이용한 APT공격 분석에 관련된 연구에 대해 살펴보고 통합보안관제선터 모니터링 환경에서 효율적일 것으로 판단되는 APT공격 분석 방법 2가지를 제안하고자 한다. 또한, APT공격이라고 의심되는 건을 발견 시 취해야 할 대응방안에 대해서도 제안하고자 한다.

Ⅱ. 관련 연구

2.1 빅데이터 분석

가트너는 ‘12년에 Volume(대용량), Velocity(실시간 변경), Variety(비정형)의 3Vs를 가진 데이터를 빅데이터라고 정의하였다[4]. 이러한 빅데이터를 이용하는 대표적인 과학은 예측적인 데이터 분석(Predictive Data Analytics)로 빅데이터에서 특정 패턴을 찾고 예측하는 것을 말한다[5]. 예측적인 데이터 분석을 하는 대표적인 방법이 머신러닝이며 머신러닝은 이러한 특정 패턴을 자동으로 찾게 만드는 것을 말한다.

김원필은 IEEE 논문 정보를 이용해 정보보안 분야 트렌드를 빅데이터 분석으로 분석하였다[6]. 분석 결과 정보보안에 유망한 기술로 안드로이드 플랫폼, 사물인터넷, 클라우드 컴퓨팅과 함께 빅데이터가 도출되었다.

최도현외 1명은 사용자들의 거래 성향을 빅데이터 분석을 통해 분석하였다[7]. Naive Bayes Algorithm 및 Aproiri Algorithm 등을 상호 응용하여 분석하였고, 분석 결과 제품별 긍정, 부정 성향 및 성향별 관심의 정도를 도출하였다. 이와 같이 빅데이터 분석을 통해 무의미하게 보이는 대량의 데이터에서 의미있는 정보를 수치화할 수 있음을 알 수 있다.

2.2 보안관제에서의 머신러닝 방법

보안관제에서의 머신러닝은 일반적인 비즈니스와 달리 의도적인 공격을 찾는 것이며 또한 보안관제 장비들의 로그를 분석해야 하기에 분석 방법도 보안관제에 특화되어야 한다.

Sumeet Dua외 1명은 머신러닝을 이용한 보안관제는 ①오용/시그니처 탐지(Misuse/Signature Detection), ②이상 탐지(Anomaly Detection), ③하이브리드 탐지(Hybrid Detection), ④네트워크 스캔 탐지(Network Scan Detection), ⑤프로파일링 모듈(Profiling Module)의 5가지 방법이 있다고 하였다[8]. 본 연구는 Sumeet Dua외 1명의 방법을 참고하여 APT공격 분석을 진행한다.

2.2 APT공격

손경호외 2명은 APT공격 분석 방법으로 연관성 분석이 주요한 방법이며 이러한 연관도 분석 방법에는 로그 유사속성 비교 방법[9, 10], 공격 초기의 이벤트 설정 탐지 방법[11, 12, 13], 시간 흐름별 공격의 통계적 원인분석 방법[14, 15], 개별 이벤트를 군집하여 침해시도 여부를 결정하는 방법[16, 17] 등 다양한 방법이 있다고 하였다[18]. 악성코드에 감염된 PC의 트래픽을 분석하는 방법으로 주기적 접속시도 탐지 방법을 제안하였다.

한성백외 1명은 APT공격에 대한 금융권의 대응방안 연구에서 관리적 측면, 기술적 측면, 솔루션 측면에서 대응방안을 정리하였다[1]. APT공격은 사전조사, 제로데이 취약점 공격, 사회공학 기법 적용, 은닉, 적응, 지속 등의 공격기법을 조합한다고 하였으며, APT공격 대응솔루션은 모든 트래픽을 수집하고 행위기반의 파일 분석을 통한 1차 분석 후 가상분석 OS에 실행하여 악성여부를 2차로 판단한다고 하였다.

본 연구에서는 APT솔루션의 1차 분석 단계인 행위기반 파일 분석 등과 같이 악성코드 분석 등의 심층 분석 전 단계에 집중하여 연구할 계획이다. 또한, 파일 분석이 아닌 통합보안관제에서의 관제데이터 및 트래픽데이터를 이용한 빅데이터 분석에 대해 연구할 계획이다.

2.3. 취약점 분석

취약점 분석은 보호하려는 대상에 보안취약점

이 존재하는지를 분석하는 것이다. 취약점 분석대상에 따라 H/W와 S/W로 분류할 수 있다. H/W 취약점 분석대상은 서버, 네트워크 장비, 방화벽 등이며, S/W 취약점 분석대상은 웹페이지, 애플리케이션, 소스코드(시큐어 코딩 점검) 등이다.

취약점 분석을 통해 공격을 미연에 방지할 수도 있으며 공격이 이미 감행된 경우에는 해당 공격이 유효했는지 여부를 판단할 수 있는 근기를 제공한다.

APT공격 분석 관점에서 취약점 분석 관련 연구조사 사례는 거의 없다. 이러한 이유는 APT공격이 알려지지 않은 취약점인 제로데이 취약점을 이용하기에 현재의 취약점 분석 방법으로 APT공격 취약점을 찾아내기가 어려워서일 것이다. 하지만, 빅데이터 분석 등을 이용한 취약점 분석 고도화로 APT공격 가능성을 제거할 수 있을 것으로 판단된다.

일례로, APT공격은 이메일, SMS 등의 사회공학적 방법을 이용하므로 기존 기술적 취약점을 찾는 것과 함께 빅데이터 분석을 통해 관리적 측면의 취약점을 찾는 방법을 고려해 볼 수 있다. 모의해킹훈련을 수행 후 훈련결과를 빅데이터 분석하여 어떠한 유형의 수신자가 취약한지 밝혀낸다. 이러한 분석결과로 정보보안 정책 수립·개정 및 관련 솔루션을 개발한다면 APT공격 예방효과가 있을 것으로 판단된다.

Ⅲ. APT공격 전조 현상 분석 설계

3.1 블랙리스트 IP 매칭 설계

블랙리스트 IP 제공업체의 정보를 RDBMS Relational Database Management System)에 저장한 후 빅데이터 분석시스템(스플렁크)에 저장된 회원사들의 트래픽정보 IP와 매핑한다. 매핑된 트래픽정보의 패킷을 빅데이터 분석하여 APT공격과의 연계성을 분석하는 방법이다.

동 방법은 APT공격자들이 공격 준비 및 탐지 우회를 위해 주로 보안이 취약한 해외서버를 먼저 공격하여 교두보를 확보한 후 공격할 경우 효과가 있을 수 있다.

동 방법의 관건 중 하나는 신뢰성이 떨어지는 외부 블랙리스트IP의 신뢰성 확보이며 이 또한 빅데이터 분석을 통해 확보되어야 할 것이다.

3.2 DNS Log를 이용한 악성코드 분석 설계

DNS Log 중 정상적인 DNS Log의 특징 분석 후 비정상 DNS Log를 추출하여 APT공격와의 연계성을 스플렁크로 분석하는 방법이다. 또한, 기존 보안관제 솔루션 제품에서 이용하고 있는 빅데이터 분석 방법도 스플렁크를 이용 통합보안관제에 개선·적용하는 등 여러 회원사 DNS Log를 이용하여 APT공격을 분석하는 방법이다.

Ⅳ. 빅데이터 분석을 통한 APT공격 전조 현상 분석

4.1 블랙리스트 IP DB 구축 및 IP matching에 의한 Payload 분석 방법

먼저 블랙리스트IP의 신뢰성 확보를 외부 블랙리스트IP들 중 2개 이상의 외부업체에서 지목한 블랙리스트IP를 트래픽정보와 매핑시킨다. 만약 이에 해당되는 외부업체 블랙리스트IP수가 많은 경우 3개 또는 4개 이상으로 기준을 높여 매핑시킴으로써 빅데이터 분석 성능을 향상시킨다.

매핑되는 트래픽정보가 미존재할 경우 공격자들이 하나의 IP가 아닌 C클래스 대역의 IP를 바꿔가며 공격하는 특징을 감안하여 외부 업체 블랙리스트IP의 C클래스 대역 IP도 매핑한다.

매핑 후에는 해당 패킷의 헤더 정보나 페이로드 정보 중 정상적인 패킷과 다른 특이점이 있는지 지도학습, 비지도학습 머신러닝 방법 등을 적용하여 조사한다.

4.2 통합보안관제에서의 DNS Log 분석 방법

정상적인 DNS Log의 특성을 찾아내기 위해 빅데이터 분석으로 정상적인 DNS Log의 대표적인 특성을 찾는다.

그리고 보안관제 솔루션 제품의 DNS Log를 이용한 빅데이터 분석 방법 등을 1개의 회원사에 개선·적용하여 분석효과를 측정하고 여러 회원사에도 적용하여 회원사간의 분석효과를 연관분석하면서 분석 효과를 향상시킨다.

DNS Log 분석 방법으로는 정보유출이나 Beacon통신이 의심되는 주기적인 DNS Log가 있을 경우나 악성코드의 C&C서버 IP 은닉을 위한 빈번한 URL-IP맵핑 변경을 검색·분석하는 방법이 있을 수 있다.

동 방법 분석결과는 통합보안관제센터의 트래픽정보, IDS이벤트들과 맵핑하여 분석 효과를 향상시킬 수 있다.

4.3 APT공격 전조 현상 분석

4.1 또는 4.2의 방법으로 분석하여 APT공격이 의심되는 경우에는 이를 입증할 확실한 증거가 필요하다. 일반적으로 APT공격임을 확신하기 위해서는 관련 악성코드가 필요하며 악성코드는 4.1 또는 4.2 분석에서 찾아낸 관련 IP들에 대해 포렌식을 수행하여 악성코드를 확보해야 한다.

4.4 APT공격 차단 및 예방 방안

4.3에서 APT공격을 분석하여 APT공격으로 판단되는 경우 우리나라 3선 보안관체 체계에서 ISAC(Information Sharing & Analysis Center)은 대응매뉴얼에 따른 신속한 전파가 매우 중요하다.

가장 우선적으로 해야 할 것은 유관 상급기관(정부)에 보고하여 해당 공격이 국가적으로 어느정도 위험성이 있는지 확인한다. 위험성 확인 후에는 ISAC 회원들에게 해당 공격에 대한 정보를 공유하여 APT공격을 차단하거나 예방하여야 하겠다.

해당 APT공격이 특정 프로그램의 취약점을 이용한 경우 해당 프로그램을 사용하고 있는 ISAC 회원사를 조사하고 이미 해킹이 되었는지 포렌식 등을 통해 파악하는 것이 중요하다.

공격정보 전파시 언론에 해당 공격을 보도 요청할 경우에는 APT공격자가 공격실패에 대해서 인지하고 다른 방법으로 공격을 감행할 수 있으므로 정부와 해당 공격에 대한 보도 여부 사전협의가 필요할 것으로 판단된다.

또한 2.3에서 언급된 취약점 분석 고도화 방안을 연구하는 것도 공격 예방을 위해 필요하다.

마지막으로 본 논문에서 연구 중인 빅데이터 분석 이용 APT공격 탐지 방법을 지속적으로 연구해야 APT공격 예방에 성공할 것으로 판단된다.

Ⅴ. 결 론

나날이 고도화되고 있는 APT공격을 분석하기 위해 빅데이터 분석을 이용한 보안관제 고도화 2가지 방법을 제안하였다. 본 연구는 개별보안관제가 아닌 통합보안관제 상황에서의 분석 방법을 연구하는 것이며 앞으로 제안한 분석 방법이 APT공격 탐지에 어느정도 효과가 있는지 측정하고 효과가 미흡한 경우에는 분석 방법을 변경하여 효과를 극대화시키도록 할 계획이다.

본 연구에서 구현할 2가지 방법 외에 Sumeet Dua외 1명의 머신러닝을 방법들을 이용한 추가적인 APT공격 분석 방법의 제안 및 연구를 통해 APT공격 분석 성공률을 향상시켜야 할 것이다.

빅데이터 분석은 난이도가 높은 분야이며 APT공격은 조직적으로 알려지지 않은 공격을 이용해 장기간 수행하는 공격이므로 본 연구에서 제안하는 방법으로도 APT공격 분석이 어려울 수 있다. 하지만, 이러한 APT공격 분석 노력이 계속 될 때 근래 알파고가 인간 고수를 이긴 것처럼 APT공격을 성공적으로 분석하는 날이 올 것으로 생각한다.

참고문헌

[1] Sung-baek Han et al., “Financial Services Industry’s Reaction Plan to Defend APT Attack“, J. Korea Inst. Info. Security & Cryptology, Vol 2, no 1, 2013

[2] “3.20 Cyberterror Investigation Interim Report”, Ministry of Science, ICT and Future Planning, 2013

[3] “KHNP Cyberterror Incident Investigation Interim Report”, Privacy Info. Crime Gov. Joint Investigation Dept., 2015

[4] Peter Zadrozny et al., “Big Data Analytics Using Splunk”, Apress, 2013

[5] John D. Kelleher et al., “Fundamentals of Machine Learning for Predictive Analytics”, The MIT Press, 2015

[6] Won-pil Kim, “Analysis of Global Research Trend on Information Security“, J. Korea Inst. Inf. Commun. Eng) Vol 19, No. 5, 2015

[7] Do-hyeon Choi et al., “Tha Application Method of Machine Learning for Analyzing User Transaction Tendency in Big Data environment“, J. Korea Inst. Inf. Commun. Eng Vol 19, No. 10, 2015

[8] Sumeet Dua et al., “Data Mining and Machine Learning in Cybersecurity”, Auerbach Publications, 2011

[9] Elshoush et al., “Alert correlation in collaborative intelligent intrusion detection systems - A survey.“, Applied Soft Computing In Press, 2011.

[10] K. Julish, “Mining alarm clusters to improve alarm handling efficiency.“, Proceedings of the 17th Annual Conference on Computer Security Applications, 2001.

[11] S. Cheung et al., “Modeling multistep cyber attacks for scenario recognition.“, DARPA Information Survivability Conference and Exposition. pp.284-292, 2003

[12] H. Debar et al., “Aggregation and correlation of intrusion detection alerts“, Proceedings of the International Symposium on Recent Advances in Intrusion Detection, pp.85-103, 2001

[13] B. Morin et al., “M2D2: A formal data model for IDS alert correlation“, Proc. Recent Advances in Intrusion Detection, pp.115-137, 2002

[14] X. Qin et al., “Statistical causality of infosec alert data.“ Proceedings of Recent Advances in Intrusion Detection, 2003

[15] W.L. Xinzhou Qin, “Statistical causality analysis of infosec alert data“, Lecture Notes in Computer Science, 2003

[16] A. Valdes et al., “Probabilistic alert correlation“, RAID, 2001

[17] O. Dain et al., “Building scenarios from a heterogeneous alert stream“, IEEE Workshop on Information Assurance and Security, 2001

[18] Kyungho Son et al., “Design for Zombie PCs and APT Attack Detection based on traffic analysis“, pp.2, J. Korea Inst. Info. Security & Cryptology vol 24, no 3, 2014