지능형 지속 위협 대응을 위한 외부 문서 유입 방안 연구

김종필*, 박상호**, 나원철***, 장항배****
*소프트캠프(주)
,*중앙대학교 융합보안학과
****중앙대학교 산업보안학과
e-mail:*jpkim@softcamp.co.kr
{**sanghopark, ***nastop, ****hbchang}@cau.ac.kr

A Study on Outer Document Flow for APT Response

JongPil Kim*, Sangho Park**, Onechul Na***, Hangbae Chang****
*SOFTCAMP Co., LTD
,*Department of Security Convergence, Chung-Ang University
****Department of Industrial Security, Chung-Ang University

요 약

최근 지능형 지속 위협(APT)은 명확한 공격 대상과 정교한 프로그램을 사용하여 치밀하게 공격하는 사회공학적 공격 기법을 사용함으로 상업용 탐지기술의 지속적인 발전과 개발에도 빠르게 증가되고 있다. 기존의 탐지 기법은 알려진 악성코드에 대하여는 효과적으로 대응 가능하나 아무런 정보가 없는 제로데이 공격 등의 악성코드는 탐지하기 어렵다. 특히 최근의 악성코드들은 빠르게 변종을 만들어냄으로 기존의 탐지 기법으로는 한계가 있다. 따라서 본 연구에서는 악성코드에 대한 경로 및 유형, 공격 방법 등을 분석하고 이를 탐지하고 분석하는 선행 기술들 조사하여 DAST 기반의 콘텐츠재구성을 통한 무해화 기술을 제안하였다.

1. 서론

인터넷의 보급률 확대와 급속한 인터넷 인프라 발전은 악성코드로부터 사용자 컴퓨터 환경을 위협하고 있으며 지속 위협은 시간이 지날수록 지능화, 다양화 되고 있다. 고성능 컴퓨터는 봇넷의 특정 좀비 컴퓨터로 이용당하거나 전염 대상 컴퓨터의 전달 매개로 이용되는 등 컴퓨터의 성능 발전에 따라 피해 속도도 빨라지고 있다[1][2].

이러한 환경의 변화에 따라 공기업 도면 유출과 금융권 개인정보유출 사고 등의 심각한 보안사고가 발생하고 있으며 기존 보안 기술을 무력화하고 대응할 수 없는 우회경로를 활용하여 피해를 입히고 있는데 이는 APT 공격에 의한 것으로 보고 있다. 지능형 지속 위협(APT, Advanced Persistent Threat)은 말 그대로 특정 기업 또는 기관의 핵심 정보통신 설비에 대한 중단 또는 핵심정보의 획득을 목적으로 공격자는 장기간 동안 공격대상에 대해 IT인프라, 업무환경, 임직원 정보 등 다양한 정보를 수집한다[3][4]. 이러한 고도화되고 지능적인 APT 공격에 대응하기 위하여 현재 시그니쳐기반과 함께 네트워크 트래픽 분석이나 가상환경을 활용한 행위 기반, 평판 분석 등의 다양한 보안기술을 접목한 솔루션이 개발되어 APT 방어 솔루션으로 출시되고 있으나 이는 모두 전문가 분석을 기반으로 한 것이어서 제로데이 공격과 같이 알려지지 않거나 지속적으로 고도화되어 변화하는 APT 공격을 예측하고 선제적으로 대응하기는 어렵다[5]. 따라서 본 연구에서는 끊임없이 변화하는 외부 공격에 대하여 시그니쳐, 행위 기반 분석 등을 통해 악성 여부를 판단하며 유입을 차단하는 것이 아닌 외부 유입 문서에 대하여 문서 재구성 기술(DAST, Document Attachment Sanitization Technology)을 사용한 문서를 무해(無害)하게 재구성하고 효율적으로 보호할 수 있는 기반 기술을 제안하고자 한다.

2. 선행연구

2.1 악성코드의 정의와 공격기술

멀웨어(Malware)란 Malicious Software의 줄임말로 악성 소프트웨어를 말하며 악의적인 목적으로 제작되어 컴퓨터에 악영향을 줄 수 있는 모든 소프트웨어를 칭한다. 이러한 소프트웨어는 사용자의 명령이나 승인 없이 설치되거나 실행되며 시스템 성능 저하 또는 개인 정보 유출 등 악의적인 행위를 수행한다. 국내에서는 멀웨어를 “악성코드”로 총칭하며 컴퓨터 Virus, Worm, Trojan Horse, Spyware, Rootkit 등이 모두 악성코드에 속한다[6].

악성코드의 공격 기술은 초기의 자기 과시욕에서 최근은 목적성과 대상을 정한 공격형으로 변하고 있으며 은닉과 우회, 위장을 위하여 다양한 기술로 발전해 왔다. 최근의 공격 기술은 제로데이 취약점과 같은 방식으로 사회공학적 공격 기법을 기반으로 한 공격형이 증가하고 있는 추세이다[6].

2.2 악성코드 탐지기법

최근의 악성코드 생성 방법을 살펴보면 비주얼 베이직(VB), mIRC스크립트, Java 스크립트 등 스크립트를 주로 이용하여 생성한다[7]. 이렇게 작성된 스크립트는 이메일을 통하여 주로 전파되며 이러한 스크립트를 사전에 탐지하여 차단하기 위해서는 시그니쳐 스캐닝에 의한 방법, 어플리케이션 변환 기법, 정적 분석에 의한 탐지 등을 사용하며 이중 시그니쳐기반의 탐지를 주로 사용한다. 악성코드 분석 기술은 호스트 기반 분석 기술, 네트워크 기반 분석의 기술 적용 대상에 따라 구분하며 분석 기술의 동작 특성으로 구분 시, 시그니쳐기반, 행위 기반으로 구분된다[6][7].

호스트 기반 악성코드 분석 기술은 각 호스트에 설치된 악성코드 탐지 프로그램을 사용하여 파일 혹은 시스템의 악성코드를 분석하는 방법이다. 이와 달리 네트워크 기반 악성코드 분석 기술은 네트워크의 경계에서 각 호스트로 전달되는 네트워크 트래픽을 수집하고 분석함으로써 악성코드를 분석하는 방법이다. 또한 시그니쳐기반 악성코드 분석 기술은 파일의 특정 부분 또는 고유한 부분을 대상으로 하여 이미 알려진 악성코드의 패턴과의 일치 여부를 분석하는 기법이며, 행위 기반 악성코드 탐지 기술은 시스템 내에서 일어나는 다양한 행동을 분석하여 악성코드 의심 파일을 탐지하는 방법이다.

3. DAST 기술 기반의 APT 대응을 위한 효율적인 외부 문서 유입방안 제안

APT 공격에 대비한 시장 규모는 점차 커지고 있다. 가트너 보고서에 따르면 APT 시장은 2012년 약 2억 달러에서 2017년 11억7천만 달러로 성장할 것으로 전망한다(연간성장률 42.2% 예상). 또한 사이버 공격 방어와 관련하여 악성코드, 멀웨어, 스팸메일 등을 검출하거나 가상환경으로 제공하여 분석하는 등의 각 원천 기술은 이미 많은 부분에서 활용되고 특허로 존재하고 있으나 대부분이 악성코드, 멀웨어, 스팸메일 등을 검출하는데 초점이 맞추어져 있다.

이에 반해 본 연구에서 제안하는 기술은 외부유입파일에 대한 어떠한 분석 없이, 해당 파일에 의해 로컬 시스템의 자원(중요파일, 레지스트리, 통신 등)이 접근되는 것을 상시 모니터링하고 차단하여 APT 공격으로부터 정보자산을 보호하고자 하는 것이며 선행 연구를 통하여 조사한 기존 검출 방식과는 전혀 다른 방식의 연구이다. 또한 기존의 분석이 파일 또는 어플리케이션에 대한 1회성의 분석이었다면, 본 연구에서는 1회성의 분석이 아닌 근본적인 APT에 대한 대응 연구를 제안하고자 한다.

본 연구에서 제안하고자 하는 핵심기술인 문서재구성 기술(DAST, Document Attachment Sanitization Technology)에 대한 연구는 지속적으로 발전하고 있는 악성코드에 대응하기 위해서 알려지지 않은 보안 위협에도 보호할 수 있는 선제적인 대책 마련이 필요하다. 그러나 선행 연구에서 조사하였듯이 현재 악성 코드에 대응하는 분석 방법은 보안정책에 따라 허가된 통신 및 매체 사용을 제어하는 수준(방화벽, NAC)이거나 이미 알려진 시그니쳐 기반으로 악성코드를 검출하는 수준으로 제로데이 공격이나 기존 알려진 패턴에서 변조된 공격에는 효과적으로 대응하지 못한다. 이러한 시그니쳐기반 분석의 한계점을 극복하기 위하여 행위기반, 평판 기반의 분석 기술을 접목하여 알려지지 않은 보안 위협에 대해 대응할 수 있는 APT 공격에 대한 분석 방법이 제시되고 있으나, 이 또한 위험 행위에 대한 판단을 위한 분석을 기반으로 예측하는 것으로 분석 사례가 없는 공격이나 탐지 우회 등에 대한 대응이 불가능하다.

본 연구에서는 DAST 기술을 활용한 콘텐츠재구성을 통해 APT에 효과적으로 대응할 수 있는 외부 문서 유입방안을 설계하는 것을 제안하고자 하며, DAST 기술을 활용한 콘텐츠재구성 기술 개발 시 시그니쳐와 행위 기반 분석의 단점을 보완한 패턴 업데이트가 필요 없으며 악성코드를 포함 할 수 있는 은닉 정보를 제거하고 분석 기술을 우회하지 못하도록 문서의 구조적 형태를 근본적으로 재구성하는 방식으로 DAST는 문서형 악성코드의 유입을 원천적으로 보호할 수 있다.

앞에서 설명한 시그니쳐와 행위 기반의 분석을 비교하고 본 연구에서 제안하는 DAST 기반의 콘텐츠재구성 기술의 차별성을 비교하면 아래 <표 1>과 같다.

<표 1> 기존 악성코드 분석방법과의 차이점

구분	시그니쳐기반	행위 기반
주요 기능	• 이미 알려진 시그니쳐기반으로 유입파일에 대한 악성코드 포함 여부 탐지 후, 탐지된 경우 별도 격리 및 차단/삭제 처리 • 악성코드에 대한 치료	• 네트워크로 유입되는 트래픽 분석/탐지 • 가상환경(Sandbox)에서의 행위 분석/탐지 • 블랙리스트/화이트리스트 분류 및 정책 업데이트 • 악성코드에 대한 치료
장점	• 시그니쳐 방식으로 기 알려진 악성코드에 대한 탐지 성능이 높음	• N/W Traffic 분석/탐지(일부 기능) • 일반적으로 Appliance 장비 형태로 구축과 관리가 편리
단점	• 제로데이 등의 알려지지 않은 공격에 무방비 • 검사(분석)이 통과하여 내부에 유입한 경우 별도 관리 및 통제 불가	• 주문형 Sandbox 환경의 제약으로 특정 환경만 분석 가능 • 분석을 위해 과도한 행위 로그 수집 필요 • 가상환경 우회 시 무방비 • 통신이 아닌 이동매체를 통해 유입되는 악성코드에 대한 탐지 어려움 • 분석을 통과한 파일에 대해 별도 관리/통제 불가능 • 내부에 유입되어 사전에 감염된 악성코드에 대해 대응 방안이 없음
본 연구의 차별점	• 두 기반의 단점을 보완한 선제적, 능동적 방어기술 • 악성코드에 대한 분석/탐지 방식이 아닌, 외부유입파일의 위협 행위 제거 기술 • 패턴 업데이트가 필요 없는 방식의 파일 구조 개선 방식 • Visible Contents를 추출하는 과정을 통한 은닉 요소(악성코드) 제거로 행위 분석 필요 요소에 대한 사전 제거로 인한 선제적 대응 기술 • 문서 Hidden Attachment 제거를 통한 문서 재구성 기술 • 원본 확장자의 형태 유지 • 악성코드 포함 파일 폐기 및 차단 • 최소의 자원으로 신속한 대응과 분석 • 분석 통과 후 사후(유입 후) 방어 지속적 유지 구조	

4. 결론 및 향후연구

본 연구에서는 외부 유입문서의 내부 반입 시 DAST 기술에 기반하여 안전한 콘텐츠(Visible Contents로 텍스트, 이미지 등을 말함)만을 추출하여 문서를 재구성하는 기술개발을 제안하였으며, 기술개발 시 외부로부터 유입되는 다양한 경로의 문서에 적용이 가능하고 숨은 악성코드를 제거하여 선행 연구들이 갖고 있는 한계를 개선하고 대응 할 수 있을 것으로 기대하고 있다. 향후 연구를 통해 실험 환경을 구성하여 DAST를 적용한 콘텐츠재구성 기술을 실험하고 그 결과를 기반으로 효과성 분석을 분석해야 할 것이다.

감사의 글

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (H8501-17-1018)

참고문헌

[1] Vinod Ganapathy Sanjit A Sechia, “Automatic Discovert of Api Level Exploits”, ICSE, 2005.

[2] Birdman, “The Evolution of Windows Spyware Techniques”, HIT2005 July, 2005.

[3] Junesung Choi, Kwangho Kook, “Analysis of APT Attack Cases”, 2012 Conference Proceedings Korean Operations Research and Management Science Society, pp.1467-1477, 2012.

[4] Junesung Choi, Wonhyung Park, Kwangho Kook, “Analysis of the Advanced Persistant Threat(APT)”, Journal of the Korean Association of Defnce Industry Stuidies, Vol.19, No.2, pp.73-89, 2012.

[5] A.Sung, J.Zu, P.Chavez, S.Mukkamala, “Static Analyzer for Vicious Executables(SAVE)”, 20th Annual Computer Security Applications Conference, pp.326-334, 2014.

[6] “악성코드 유사 및 변종유형 예측방법 연구”, 한국인터넷진흥원, 2011.

[7] 우종우, 하경휘, “시그니쳐 패턴 기반의 악성코드 탐색 도구의 개발”, 한국컴퓨터정보학회 논문지, Vol.10, No.6, pp.127-135, 2008.