스피어 피싱 대응을 위한 엔드포인트 에이전트 시스템 모델에 관한 연구

김창홍* · 김상필** · 김종배***

*,**,***숭실대학교

E-mail : kjb123@ssu.ac.kr

요 약

기존의 정보보호시스템들은 이미 확보된 시그니처 또는 이전에 분석된 정보를 기반으로 악성코드에 대응하고 있기 때문에, 시그니처가 알려지지 않은 악성코드 또는 변형된 악성코드의 경우, 탐지 및 식별에 한계를 지니고 있다.

본 연구는 이와 같은 문제를 해결하기 위해, 무결성을 검증하는 화이트리스트 기반의 응용프로그램 실행제어, 매체제어, 레지스트리 보호, 중요 파일 변경 방지, 프로세스 접근 역접속 IP/포트 통제 등의 기술을 복합적으로 적용하여, 악성코드의 침입뿐만 아니라 운영체제 및 응용프로그램 취약점을 기반으로 한 익스플로잇 공격으로부터 단말 PC를 더욱 확실하게 보호할 수 있도록 한 엔드포인트 응용프로그램 실행 통제 방안을 제시하였다.

본 연구의 결과는 프로토타입 형태로 개발하여 실 환경에서 통합테스트를 하여 공공기관, 금융기관, 통신사 등 실제 환경에 적합한 기술 및 기능임을 확인하였다. 본 연구를 통해, 실행 전 응용프로그램 무결성 검증과 실행 후 응용프로그램 실행 흐름 통제를 복합적으로 사용하여 알려진 악성코드 시그니처 정보에 의존한 기존 정보 보호 시스템과는 달리 알려지지 않은 악성코드까지 원천적으로 차단할 수 있을 것으로 기대된다.

Ⅰ. 서 론

사이버 공격의 증대에 따라, 이에 대응하기 위한 보안 정책의 방향도 변화되고 있다. Ponemon연구소가 IT와 보안 담당자들을 대상으로 실시한 조사에 따르면, 응답자들의 83%가 본인이 속한 조직이 APT공격을 받은 것으로 추정하였다.[1] APT공격의 진화와 사회공학적 기법을 활용한 스피어 피싱(Spear-phishing) 방법으로 단말 PC에 설치된 악성코드에서 개인정보 유출 및 보유 시스템 파괴가 시작되므로, 인가된 응용프로그램 실행 여부, 인가된 응용프로그램의 악의적인 위/변조 여부, 운영체제의 중요파일에 대한 악의적인 변경 여부를 식별하고 차단하는 기술이 필요하다.

알려지지 않은 악성코드를 식별하고 차단하기 위해서는 응용프로그램을 구성하는 실행파일의 해시정보를 기반으로 한 무결성 검증, 파일의 속성정보 및 경로 정보, 파일의 전자 서명 검증과 같은 정적 정보 분석과 응용프로그램 실행 이후 비정상적 프로세스 실행흐름을 탐지하기 위한 동적 정보 분석을 복합적으로 사용한 분석 및 탐지 기술이 필요하다.[2]

Ⅱ. 관련 연구

악성코드는 정적(Static)분석, 동적(Dynamic)분석, 그리고 정적분석과 동적분석의 특성을 합친 하이브리드(Hybrid)분석으로 나뉜다.[3]

정적 분석 방법은 악성코드 구성요소들의 연관성이나 호출 관계 등을 분석해서 악성코드의 전체적인 구조 및 흐름을 분석하는 방법이다.

동적 분석 방법은 악성코드를 실제로 실행시켰을 때 수행되는 내용을 분석하는 방법이다. 동적 분석 기법은 실제 컴퓨터 상에서 검사를 하지만 시스템 내부에 가상 CPU와 가상 메모리 등의 환경을 제공하여 실행 파일을 실행하고 정보를 수집함으로 실제 컴퓨터 시스템에서는 어떠한 감염피해도 발생하지 않는다.

하이브리드 분석을 이용한 탐지기법으로는 악성코드의 공통속성을 이용하거나 공격용 툴킷의 특징을 이용하는 방법 등[4][5]이 제안되었다.

Ⅲ. 스피어피싱의 현황

세계적인 보안업체인 트렌드마이크로는 APT 표적공격의 91%가 스피어 피싱 이메일로 시작된다고 밝혔다. 스피어 피싱 메일의 94%는 파일일 첨부하고 있으며, 공격대상의 76%가 기업이나 정부기관

인 것으로 조사되었다.[6] 이메일을 통해 업무를 공유하는 부분이 많은 점을 노려 워드, 엑셀, 한글파일을 이메일에 첨부하는 방식을 이용했다. 실행파일(.exe) 같은 경우에는 조직의 보안시스템에 탐지 및 차단이 되므로, 실행파일 대신 압축파일을 사용하는 추세이다. 스피어 피싱 공격의 경비는 1000명 대상 스피어 피싱 비용이 100만 명 대상 일반 피싱보다 10배나 많은 비용이 소모됨에도 불구하고 대규모 스팸 메일보다 클릭할 확률이 10배 이상 높다고 조사되었다.[7]

기존에 알려지지 않은 취약점을 이용하여 새로운 악성코드를 작성하는데 불과 몇시간 밖에 걸리지 않는다. 사이버 범죄자의 대부분은 시스템과 응용프로그램의 취약점을 직접 찾지 않고 보안연구자나 소프트웨어 업체가 취약점 정보를 공개할 때까지 기다렸다 기업이나 기관에서 대응하기 전에 해당 취약점을 이용한 악성코드를 제작해 사용하는 경우가 대부분이다.[8]

Ⅳ. 스피어 피싱의 대응 시스템 모델

4.1 엔드포인트 에이전트 대응기법

현재 적용되고 있는 정보보호시스템은 최근의 단말 PC를 대상으로 한 악성코드 대응에 한계를 보이고 있다. 즉, 이미 확보된 시그니처 또는 이전에 분석된 정보를 기반으로 대응하고 있기 때문에 시그니처가 알려지지 않은 악성코드, 운영체제 및 응용프로그램의 취약점을 기반으로 한 익스플로잇 공격뿐만 아니라, 기존 악성코드의 변경만으로도 탐지 및 식별에 한계를 지니고 있다.

블랙리스트 방식의 시그니쳐 기반의 진단 기능의 경우 악성 샘플이 수집되어야만 진단할 수 있고 해당 샘플에 대한 분석과 엔진 빌드 및 백신이 설치된 PC까지 엔진이 반영되는 시간까지의 소요시간이 발생하기 때문에 제로데이 취약점을 이용한 악성 샘플을 진단하는데 한계가 있다. 화이트리스트 방식이 아니기 때문에 알려지지 않은 신종 악성코드에 대해 원천적인 차단이 불가하며 악성코드 제작자의 경우 신종 악성코드 제작 후 여러 플랫폼 검증을 통하여 진단이 불가한 샘플만 공격에 이용한다.

단말 PC에 설치된 에이전트는 응용프로그램 실행 이후, 실행 제어 정책에 따른 프로세스 실행 흐름을 검증한다. 구체적으로, 응용프로그램 실행 이후에 에이전트는 프로세스가 지정된 레지스트리 변경여부, 중요 파일 변경 여부, 제한된 역접속 IP/포트로 접속 시도를 탐지하여 실행 제어 정책에 위배된 경우로 판단되면 그 실행을 차단한다. 화이트리스트 기반의 응용프로그램 실행제어, 응용프로그램에 종속된 파일 해시 및 속성, 전자서명 유효성 여부, 정책에 따라 프로세스가 미리 지정된 레지스트리 보호, 역접속 탐지 통제, 중요 파일 보호, 미리 지정된 매체제어, 프로세스 역접속 IP/포트 통제의 기능 외에, 에이전트 고유기능으로 에이전트 자체 보호 기능을 수행한다.

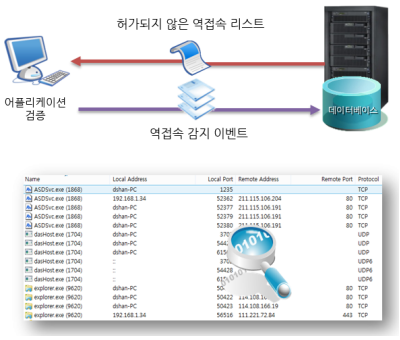

그림 4-1. 에이전트 어플리케이션 실행제어

[그림 4-1]와 같이 화이트리스트에 미 등록된 비인가 프로그램 및 미식별 실행파일은 실행되지 못하도록 차단하는 단계에서 단말 PC에 설치된 에이전트를 통해 화이트리스트의 실행파일 해시 정보, 파일 속성정보, 전자서명 정보 중 적어도 하나의 정보를 추출 비교하여 비인가 프로그램 및 미식별 실행파일은 실행 되지 못하도록 한다.

프로그램 실행제어 절차를 살펴보면, PE(Portable Executable)정보로 실행파일 여부를 확인하며, 파일 해시, 파일 속성, 전자서명 정보를 통한 유효성 검증 및 비허용 프로그램을 차단한다. 또한 스피어 피싱 코드를 차단하여, 역접속을 통해 해킹 및 악성코드의 확산을 방지한다.

프로그램 실행 후, 정책 기반의 지정된 레지스트리 변조 방지 과정에서 지정된 레지스트리 보호를 하나의 옵션 기능으로서 제공하고, 중요한 레지스트리 키 값을 정책에 등록하여 레지스트리 키 변경 모니터링 및 단말 PC와 실행 제어 정책에 포함하여 동기화 처리한다.

4.2 최종 사용자 대응기법

인간의 심리를 이용한 스피어 공격은 신뢰된 소스로부터 이메일이 오기 때문에 일부 사람이 공격에 당하는 것은 피할 수 없다. 그러나 문제는 단 한 사람이라도 악의적인 링크를 클릭하거나 악성코드를 감염시키는 첨부파일을 다운로드 받는 경우, 전체 조직에 주요한 명성과 경제적 손실을 입히는 위험에 처하게 만든다. 즉, 한대의 PC를 감염시킴으로써 전체 네트워크 보안 대책을 우회하는 것이 가능하다.

그림 4-2. 데이터 계층적 보안 시스템

[그림 4-2]와 같이 계층적 보안 시스템을 구축을 해서 사용자들이 자연스럽게 보안의식을 가지게 되고, 실수를 하게 되더라도 단계적으로 막아줄 수 있는 환경도 필요하다. 데이터 암호화, 어플리케이션 사용 통제, 매체 및 출력 통제 제어, 네트워크 사용통제, 네트워크 접근 통제 등 단계적인 보호 장치가 필요하다.

정보보안 조직 위주의 활동이 아닌 전사차원에서 정보 보호 관리 교육이 필요하다. 정보보안 교육 대상을 고려해서 일반 과정, 책임자 과정, 실무자 과정으로 구별해서 훈련 및 교육을 수립하여야 하고 직위와 담당업무를 고려해 교육계획을 편성, 교육을 실시해야 한다. 정해진 목표를 노리고 공격하는 스피어 피싱 공격에 대비하기 위한 대응방안과 교육도 중요하지만 보안사고 신고 대응에 대해서도 교육이 필요하다. 발생할 수 있는 스피어 피싱 유형에 관해 대응훈련을 정기적으로 실시하여야 하며, 이를 통해 보안 위기 상황을 가정한 조직 내 각 부문 및 담당자의 역할 및 책임, 행동요령 등을 숙지시킴으로써 능동적인 대응 실습을 통한 역량강화를 기대할 수 있다.

Ⅴ. 결 론

블랙 리스트 방식의 시그니처 기반 탐지 기법은 신종 악성 코드 탐지가 불가능하고 샘플이 수집 되더라도 분석과 업데이트에 시간이 소요되기 때문에 효과적으로 대응하는데 한계가 많다. 화이트 리스트 방식은 관리자가 승인한 프로그램 이외에는 실행 자체가 불가능하기 때문에 사전예방이 가능하다.

본 연구에서 제안한 엔드포인트 에이전트 방법을 이용하면, 높은 확률로 악성코드를 탐지할 수 있다. 이상 징후가 탐지되고 의심이 되면 에이전트에 의해서 사용자가 보다 빠르게 대처할 수 있다. 스피어 피싱의 가장 큰 공격 목표인 정부는 기존의 보안 솔루션들에 의존하는 경향이 있는데, 스피어 피싱 공격에 대한 지속적인 관심과 사용자 보안교육 대책이 필요하다.

향후 사용자의 행동 보안 취약점 분석 시스템과 엔드포인트 에이전트가 동시다발적인 분석을 수행한다면, 위험 수준을 낮추면서 더욱 효율적인 스피어 피싱 보안에 기여할 수 있을 것이다.

참고문헌

[1] Herndon, Va. Ponemon Institute Discovers Majority of Business Leaders Underestimate Risk of Advanced Cyber Threats. http://www.prnewswire.com/news-releases

[2] Chang-Hong Kim, Jeong-Hyun Yi, and Jong-Bae Kim. “A Study of Program Execution Control based on Whitelist”, KIICE, 2014

[3] Jaeho Lee, Sangjin Lee. “A Study on Unknown Malware Detection using Digital Forensic Techniques”, CIST, 2014

[4] Seong-Bin Park, Min-Soo Kim, and Bong-Nam Noh. “Detection method using common features of malware variants generated by automated tools,“ journal of Korean institute of information technology, 10(9), pp. 67-75, Sept. 2012.

[5] Yong-Wook Chung and Bong-Nam Noh. “Selecting features for measuring similarity between attack toolkits and polymorphic codes,“ Journal of Security Engineering, 9(1), Feb. 2012.

[6] Trend micro, Spear-Phishing Email: Most Favored APT Attack Bait, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear phishing-email-most-favored-apt-attack-bait.pdf

[7] FireEye, Inc. “Spear Phishing Attacks Why They are Successful and How to Stop Them”, White Paper, 2012

[8] IBM Software Thought Leadership, “Proactive response to today’s advanced persistent threats“, White Paper, 2013