최근 APT 공격의 형태 및 대응 방안 연구

임완호[1], 임형진[1],박종혁[1,*]
[1]서울과학기술대학교 컴퓨터공학과
[1]e-mail:{dladhsk, imhj9121, jhpark1}@seoultech.ac.kr

A Study On Schema Of Recent APT Attack And Plan For Reaction

Im Wan Ho[1], Hyungjin Im[1],Jong Hyuk Park[*]
[1]Dept. of Computer Science and Engineering and Dept. of interdisciplinary Bio IT Materials, SeoulTech, Korea

요 약

인터넷을 통한 악성코드의 확산이 나날이 증가하고 있는 가운데 특정 대상을 목표로 하여 지능적이고 지속적으로 공격하는 Advanced Persistent threat(APT) 공격이 이슈가 되고 있다. APT 공격은 특정 시스템을 목표로 하여 공격하기 때문에, 실제 공격이 성공 했을 시에는 그 피해가 더 치명적일 수 있다. 본 논문에서는 APT공격의 정의를 살펴보며, 최근에 발생하는 일반적인 APT 공격의 형태와 그 대응 방안에 대해 논의한다.

1. 서론

인터넷 기술이 발전함에 따라 인터넷의 이용률도 증가하고 있다. 사내 업무 처리에 쓰이는 중요한 서류들도 이메일을 통해 전달되곤 한다. 그런데 이러한 환경은 악성코드가 활동하기 좋은 환경이다. 단순한 웜이나 바이러스 수준에서 시작한 악성코드는 나날이 발전하여 더없이 정교해지고 복잡해지고 있다. 감염의 대상도 불특정 다수에서 특정 기업이나 기관, 사회기반 시설 등으로 바뀌고 있는 추세이며 그 파급력은 상당하다[1]. 본 논문에서는 이와 같이 특수한 목적을 가지고 정해진 타겟을 치밀하게 공격하는 최근 APT공격의 형태와 그 대응 방안을 논의한다.

2. APT공격

본장에서는 APT공격의 정의를 살펴보고 APT공격의 형태 및 특징에 대하여 논의한다.

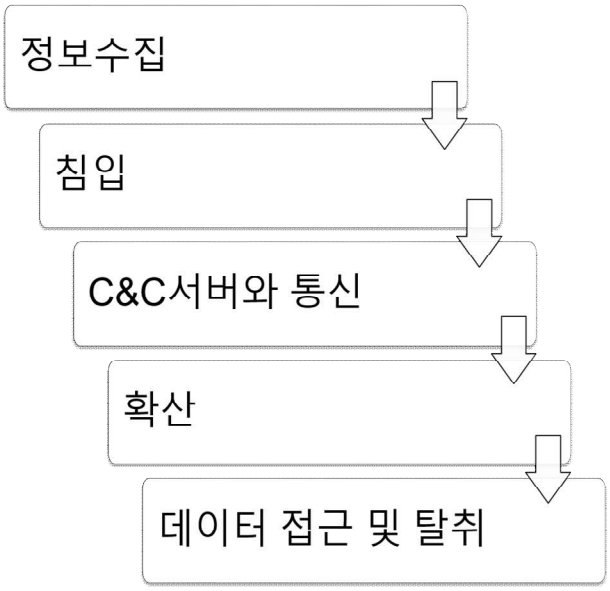
2.1 APT의 정의

APT의 그 명확한 의미에 대해서는 학자들마다 약간의 견해 차이는 있으나 공통적으로 인정하는 APT의 자격 요건은 '특정한 목적', '특정한 목표(타겟)', '지속적 공격'의 세 가지이다[2,3]. Distributed Denial of Service(DDOS) 또한 특정한 목표에 대해서 공격이 수행된다는 점에서 APT와 유사하나 DDOS가 단순히 서비스의 가용성을 해치는 수준에서 그치는 반면 APT는 DDOS를 포함하기도 하며 유출되어서는 안 될 중요한 데이터들을 탈취해 가기도 한다[2].

APT는 일반적으로 제로데이 취약점 등을 공략하여 정교하게 제작된 악성코드를 활용하므로 백신 프로그램을 비롯한 보안 제품들이 효력을 발휘하지 못한다[1,4].
국내의 대표적인 피해 사례로는 2013년 3월 20일 금융권 및 방송사를 대상으로 서비스 거부 공격을 포함하여 데이터 파괴까지 일으킨 '3.20 사이버테러'를 비롯하여, 2011년 SK커뮤니케이션즈 고객 3500만 명의 개인정보유출, 넥슨 고객 1320만 명의 개인정보유출 등이 있다[2,4].

2.2 일반적인 APT 공격의 형태

대부분의 APT공격은 (그림1)과 같은 절차를 밟는다[3].



(그림 1) APT 공격의 절차

- *정보수집 단계*

공격자가 타겟을 정하고 타겟에 대한 정보를 수집하는 단계이다. 이 단계에서는 타겟의 시스템이 어떤 취약점을 가지고 있는지 조사한다. 그리고 적절한 악성코드를 제작하거나 구매하여 테스트한다. 또한 침입을 위한 인적 네트워크 정보도 수집한다[3,5].

- *침입 단계*

타겟에 최초로 악성코드를 감염시키는 단계이다. 이 단계에서는 사회공학적인 기법을 이용해 타겟 조직의 일원을 감염시킨다. 주로 사용되는 사회공학적 기법은 스피어 피싱이다. 이는 악성코드를 포함하는 이메일을 보내는데 받는 사람이 신뢰할만한 지인이나 회사를 사칭하여 이메일을 확인하도록 만든다. 악성코드의 종류에 따라 이메일을 여는 것으로 악성코드에 감염되기도 하고 이메일에 첨부된 파일을 실행시킴으로써 감염되기도 한다[2,3,5].

- *C&C서버와 통신 단계*

감염된 PC의 악성코드가 외부에 있는 공격자의 C&C(Command and Control)서버와 통신하는 단계이다. 공격자는 C&C서버를 통해 감염된 PC의 정보를 비롯한 내부 네트워크 정보 등을 수집한다[3,5].

- *확산 단계*

악성코드를 내부 네트워크에 퍼트리는 단계이다. 이때 무차별적으로 감염시키기도 하고 보다 높은 권한을 갖는 대상을 선택적으로 감염시키기도 한다[3,5].

- *데이터 접근 및 탈취 단계*

확산 단계에서 상승된 권한을 통해 공격의 목적인 데이터에 접근하여 탈취하는 단계이다. 데이터의 탈취 후 원본 데이터를 파괴시키기도 한다[3,5].

3. 대응 방안

2장에서는 APT공격에 대해 상세히 알아보았다. 본 장에서는 APT 공격의 대응 방안에 대하여 논의한다.

3.1 APT공격 대응 원칙 및 방향

APT 공격에 효과적으로 대응하기 위해서 지켜야할 원칙은 <표1>과 같다[1,4,5].

<표 1> apt 공격 대응 원칙 및 방향

원칙	방향
보호대상의 선정	보호 대상을 명확히 함
보안 위협 모니터링	시스템, 네트워크 단에서 보안 위협징후가 발생하는지 모니터링
악성코드 침투대응	백신 프로그램, 웹 방화벽, IPS, IDS, 네트워크 대역 분리
엔드 포인트 보안	인터넷, 이메일, 메신저, P2P, USB 통제
접근권한 관리	접근 권한의 최소화, 책임 추적성 보장
중요 정보 암호화	중요한 정보의 암호화
정보 소유자의 보안 교육	정보 소유자의 보안교육 철저

특히 보안 위협 모니터링과 악성코드 침투대응이 중요하므로 3.2절과 3.3절에서 이와 관련한 기술에 대해 논의한다.

3.2 시스템 및 네트워크 모니터링

- *시스템 모니터링*

시스템에서 보안 위협 징후가 발생하는지 효과적으로 모니터링하기 위해서는 변경에 민감한 파일, 레지스트리 등을 통합적으로 관리하여야 한다. 이를 통해 감시자는 민감한 파일들의 변경사항을 즉시 확인할 수 있어야하며 어떠한 프로세스에 의해 변경되었는지를 확인할 수 있어야 한다. 또한 OS의 어플리케이션 보안 관련 로그를 수집하고 분석하여 보안 위협 징후가 발생하는지 확인하여야 한다[1,5].

- *네트워크 모니터링*

APT와 같은 타겟 공격에 대응하기 위해서는 네트워크 전반에 걸쳐 감시, 분석, 통제가 필요하다. 네트워크 장비에서 모든 네트워크 트래픽을 미러링하여 모니터링 하여야 한다[5]. 감시자는 HTTP, IRC 등의 공격에 주로 쓰이는 트래픽에 대해서 이상 징후가 없는지 판단하고, 이상 징후를 발견하면 즉시 네트워크를 통제할 수 있어야 한다.

3.3 가상 머신을 이용한 공격탐지

APT공격에 사용되는 악성코드들은 하나의 타겟을 위해 제작되기 때문에 시그니쳐나 평판 기반의 분석은 큰 의미가 없다. 따라서 가상 머신을 이용한 행위 기반의 분석이 가장 효과적인 대응이라고 할 수 있다[2,4].
여러 대의 가상 머신을 실제 환경과 유사하게 설정하여 구동시킨다. 그리고 이 가상 머신을 모니터링하며 의심스러운 행위가 포착되면 이를 서버 내부에 있는 가상 머신에서 똑같이 재현한 후 실행되는 과정을 모두 기록한다. 이를 통해 그 행위가 악성인지 정상인지 판단할 수 있어 악성코드에 대한 실시간 판단 및 대응이 가능해진다[2].

4. 결론

본 논문에서는 최근 몇 년간 발생한 대규모 사이버 테러 및 정보 유출로 인해 이슈가 되고 있는 APT공격에 대해서 살펴보고 이를 효과적으로 막기 위한 대응 방안들을 논의하였다. 특히 모니터링과 가상 머신을 통한 행위 기반 분석 기술을 중요하게 다루었는데 보안 사고는 한 부분이 아닌 여러 지점에서 일어나기 때문에 나머지 부분에서도 철저하게 관리가 이루어져야한다[3,5] 또한 기술적인 측면 이외에도 조직 내부의 보안정책과 체계, 인적 보안 등 관리적 대책을 수립하여 적용하여야한다. 이러한 관리적, 기술적 보안이 조직이 식별하고 있는 모든 정보 및 정보자산들에 적용 되었을 때 APT 공격을 효율적으로 방어 할 수 있을 것이다. [6]

참고문헌

[1]Colin Tankard, “Advanced Persistent threats and how to monitor and deter them”, ScienceDirect, Network Security, Volume2011. Issue8, pp.16-19, 2011.

[2]“APT 그것이 궁금하다...소리없는 위험 APT를 막아라”, 2014, http://www.ajunews.com/view/20141022104454160.

[3]“지능적 지속 위협, 지능적으로 유유히 정보를 유출해 달아난다 APT공격”, 2013, http://navercast.naver.com/contents.nhn?rid=122&contents_id=32568.

[4]“APT 공격 대응 기술 노하우”, 2014, http://www.boannews.com/media/view.asp?idx=42349&kind=6.

[5]“APT 공격의 현재와 대응 방안”, 2014, http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=22113&key=&dir_group_dist=0&dir_code.

[6] 한성백, 홍선권 “APT공격에 대한 금융권에서의 대응 방안”, 정보보호학회지 제23권 제1호, pp.44-53, 2013.