한국컴퓨터정보학회 동계학술대회 논문집 제25권 제1호 (2017. 1)

END-POINT에서의 탐지 및 차단을 통한 APT 공격의 서버 확산방지 개선

김우근O, 이상곤*
O*동서대학교 컴퓨터공학부
e-mail : hawo0216@naver.com, nok60@dongseo.ac.kr

A Improvement of Server Diffusion Prevention of APT Attack through the END-POINT Detection and Blocking

Woo Geun KimO, Sang-Gon Lee
O*Div. of Computer Engineering, Dongseo University

● 요 약 ●

본 논문에서는 APT 공격의 공격 시나리오와 그에 따른 방어 시나리오를 구상하여 기존 방어법의 문제점을 찾고 방어대책을 제시하고 솔루션을 구축하였다. 제안된 방어 프로세스는 기존의 방식과 달리 END-POINT에서 침투에 대해 모니터링을 통하여 APT공격에 대응하는 방식이다. 공격 툴 넷버스, 백오리피스, 서브세븐, 스쿨버스를 이용해서 공격을 시도 한 뒤 본 논문에서 구축한 방어 프로세스를 이용하여 방어 실험을 실시하였다.

키워드: APT 공격(APT Attack), 백도어(Back Door), 탐지(Detection), 차단(Block)

I. Introduction

APT(Advanced Persistent Threat) 란 네트워크 공격의 일종으로 지능적, 지속적, 위협적인 3개의 속성을 가진다[1]. APT 공격은 통신망을 타고 들어가 공격 목표 시스템 내부로 침투한 뒤, 한동안 이를 숨겨놓았다가 시간이지난 후 한꺼번에 동작시켜 주요 정보를 유출하거나 시스템을 무력화하는데 쓰인다[2,3].

APT 공격의 공격 시나리오와 그에 따른 방어 시나리오를 구상하여 공격과 방어 실험을 해봄으로써 기존 방어법의 문제점을 찾고 해결방안을 제시한다.

II. Preliminaries

현재 국내에서 사용되고 있는 APT 솔루션의 특징에 대해 알아보면 현재 국내에서 사용되고 있는 APT 솔루션에는 소프트 캠프의 실텍스, SK 인포섹의 센티넬, 안랩의 MDS 엔터프라이즈, 파이어아이의 HX 시리즈, 포터넷의 포티 샌드박스 등이 있다. 하지만 이와 같은 방법을 통해서도 완벽하게 방어
가 가능하지 않다. 그렇기 때문에 보다 나은 방비책을 강구하고자 한다.

III. The Proposed Scheme

지금 까지는 주로 네트워크를 통해 들어오는 악성코드가 END-POINT에 자리 잡지 못하게 하는 방안이 주를 이루었다. 하지만 외부인이 침투해서 USB를 통해 직접 악성코드를 심는 경우, 또는 내부 직원의 공모로 악성코드를 심고 다른 PC로 전이 시킨 다음 자신의 PC를 포맷하는 경우도 가정할 수 있다. 이러한 경우에는 네트워크 단에서는 악성코드를 전혀 인지할 수 없다. 그러므로 END-POINT에서 침투에 대해 모니터링을 통하여 APT 공격에 대응하고자 한다.

END-POINT에서 방어를 하게 되면 실제 사용자 PC에 감염 된 악성파일의 행위를 기반으로 차단, 치료하기 때문에 제대로 구축 될 경우 기존의 방식보다 더 안전한 방식이 될 수 있다는 점이다. 가상머신에서 탐지되지 않는 악성코드, 가상 사설망이나 SSL(Secure Sockets Layer)로 암호화되어 유입된 파일 등도 결국 악성행위를 위해 사용자 PC에서 복호화되는데, 이때 일망타진하는 방식이다.

본 논문에서 제안하는 APT 확산 방지 솔루션 프로세스의 전체적인 흐름도는 그림 1과 같다.

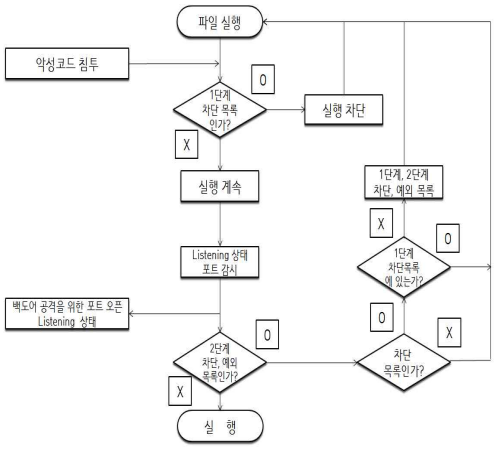


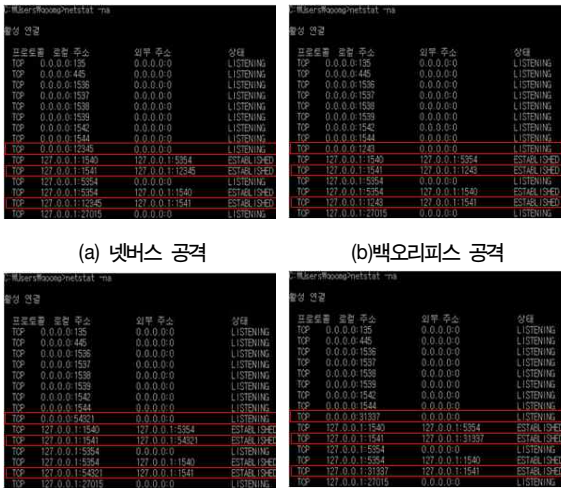
Fig 1. Defending process against APT attack

END-POINT 모니터링을 통해 실행 파일을 실시간으로 감시하여 악성코드의 침투 및 Listening 상태 포트를 감시하고, 차단/예외 목록을 생성하여 차단 목록에 등록 된 파일을 차단하여 지속적인 침투 및 공격을 차단한다.

IV. Attack and Defense Experimets

그림 2는 넷버스, 백오리피스, 스쿨버스, 서브세븐 등 4 가지의 공격 툴을 사용한 APT 공격 결과를 보여준다. 공격 툴을 사용한 공격 방법들 외에도 해킹 툴 서버 파일을 사진, 동영상, 문서 등에 합쳐 보내는 등 다양한 공격 방법과 가상환경을 통해 방어하는 방법 등 여러 가지 방법들을 알 수 있었다.

그림 3은 본 논문에서 제안한 방어 프로세스를 적용한 이후 공격목표 시스템의 포트 상태를 나타낸다. 공격 툴이 사용하던 포트가 열려 있지 않음을 확인 할 수 있다.



(a) 넷버스 공격 (b)백오리피스 공격

(c)스쿨버스 공격 (d)서브세븐 공격

Fig. 2. APT Attacks

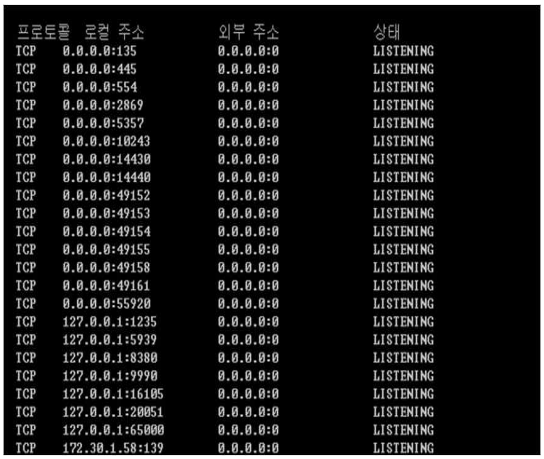


Fig. 3. Port Status after applying APT defence

V. Conclusions

APT 공격에 대해서 완벽한 방어법이 없는 만큼 피해를 최소한으로 할 수 있도록 여러 방법을 강구해 보았다. 직접 공격 시나리오와 방어 시나리오를 통해서도 실험을 하면서 여러 가지 공격 방법과 방어 방법을 도출 할 수 있었다. 향후 목표로는 가상머신 상황을 인지하여 악성행위를 하지 않는 악성코드에 대한 탐지를 가능토록 하는 것 이다.

References

[1] Cho Won Young "APT Attack Techniques and Countermeasures: Sophisticated APT Attacks, All-round Security Required", Network Times. Civil Rights 225. pp.180-185, 2011. 5

[2] http://www.kisa.or.kr/uploadfile/201312/201312041443047984.pdf

[3] 이문구, 배춘석 “APT 공격의 주요사례에 대한 연구”, 2013년도 대한전자공학회 추계종합학술대회, pp.939- 942, 2013. 11