네트워크 보안 솔루션의 취약점을 이용한 공격시나리오 연구

황 호*, 문대성*,**
*과학기술연합대학원대학교(UST) 정보보호공학과
**한국전자통신연구원 지능보안연구그룹
e-mail:{kcats, daesung}@etri.re.kr

A Study on the attack scenario using vulnerability of network security solutions

Ho Hwang*, Dae-Sung Moon*,**
*Dept of Information Security Engineering, Korea University of Science and Technology(UST)
**Intelligence Security Group, Electronics and Communications Research Institute(ETRI)

요 약

국내 기업과 기관을 대상으로 하는 APT(Advanced Persistent Treat) 공격은 꾸준히 발생하고 있다. 이에 대응하기 위해 보안 담당자는 다양한 보안솔루션을 도입하고 있지만, 반대로 보안 솔루션에 의해 공격당하는 사례가 발생하고 있다. 보안 솔루션에 의한 침해사고는 백신과 같은 엔드 포인트(End Point) 보안 솔루션을 공격하는 사례가 많지만, 네트워크 보안솔루션의 취약점을 이용하여 직접적으로 공격할 수 있는 가능성이 충분히 있다. 본 논문은 네트워크 보안 솔루션을 분석하여 확인한 취약점을 바탕으로 공격 시나리오를 제시한다. 이를 통해 네트워크 보안 솔루션에 의한 공격을 사전에 고려하여 대비할 수 있도록 한다.

1. 서 론

국내 기업과 기관을 대상으로 하는 APT(Advanced Persistent Treat) 공격은 현재 꾸준히 발생하고 있다. APT 공격은 많은 자원과 깊은 전문 지식을 동원하여 다양한 경로로 지속적으로 타겟을 공격하는 기법이다. [1]. 이에 대응하기 위해 보안 담당자는 다양한 보안 솔루션을 도입하고 있지만, 반대로 보안 솔루션이 APT 공격의 침투 경로로 사용되는 사고가 발생하고 있다. 보안 솔루션에 의한 침해사고는 엔드 포인트 보안 솔루션과 PMS(Patch Management System)의 취약점을 이용한 사례가 대다수지만 네트워크 보안솔루션의 취약점을 이용한 공격이 발생할 가능성을 배제할 수 없다.

본 논문은 보안 솔루션을 이용한 공격 시나리오를 제시하여 침해사고를 사전에 대비할 수 있도록 한다. 본 논문의 구성은 2장에서 보안 솔루션 침해사고 사례를 소개하고, 3장에서 보안 솔루션을 통한 공격 시나리오를 제시한 후, 4장에서 결론을 맺는다.

2. 보안솔루션을 이용한 공격 사례

이 장에서는 각기 다른 보안 솔루션을 침투 경로로 이용한 침해사고를 살펴본다. 각각 인터넷 거래 암호화를 위한 Active X 클라이언트, 운영체제와 어플리케이션의 패치와 업데이트를 위한 PMS, 비정상적인 통신이나 공격을 보호하는 네트워크 보안 솔루션을 공격의 통로로 사용한 사례다.

2014년 11월 경 잉카인터넷 사의 '엔프로텍트 네티즌 v5.5'에서 원격코드실행(Remote Code Execution) 취약점이 확인됐다[2]. 해당 솔루션은 국내와 해외의 제 1,2 금융권과 전자결제 및 민원 등의 인터넷 상에서 서비스가 발생하는 사이트에 적용되어 일일 평균 4억 명의 클라이언트를 보호하는 솔루션이었으므로 이 사건은 높은 파급력을 가졌다.

2016년 9월 말 사이버사령부의 백신 중계 서버가 서버의 취약점을 이용하여 해킹 당했다. 백신 중계 서버는 전군 인터넷망 PC의 백신 업데이트를 담당하므로 약 2만여 대의 PC가 악성코드 감염 위험에 노출됐다. 더구나, 감염된 국방통합데이터센터의 내부 서버에 인터넷 망과 인트라넷 망이 동시에 연결되어 있어 내부 망으로 침투하는 경로가 되었다.

2016년 8월 중순 쉐도우 브로커스라는 해킹 단체가 크라우드 펀딩을 모집하는 과정에서 자신의 능력을 입증하기 위해 미국의 국가안보국(NSA; National Security Agency) 해킹 사실을 밝혔다[3]. 이때 시스코, 포티넷, 주니퍼 등 전 세계적으로 판매되는 외산 네트워크 보안 솔루션의 취약점을 NSA가 보유하고 있다는 사실이 공개되었다. 해당 취약점을 이용해서 타국의 기관과 기업의 내부 망을 침입했을 가능성을 배제할 수 없다.

국내 침해사고에서 엔드 포인트와 서버 보안 솔루션을 공격하는 사례가 있었다. 이는 불특정 다수의 사용자를 공격하여 추가적인 공격을 수행하거나 특정 조직이 보유하는 서버의 취약점을 이용하여 내부 망을 손쉽게 점령하려는 사례다. 국내에서 네트워크 보안 솔루션의 취약점을 이용한 공격 사례는 찾아볼 수 없지만, 공개적으로 취약점을 관리하는 미국에서 취약점의 존재를 쉽게 확인할 수 있다[4]. 특히, NSA에서 유출된 네트워크 보안 솔루션의 취약점은 그 의미가 크다. 이는 공격자들이 네트워크 보안 솔루션을 구매하여 취약점 분석을 할 의사가 있으며, 다소 비용이 들더라도 파급력이 높은 공격을 원한다는 사실을 알 수 있다.

3. 네트워크 보안 솔루션을 이용한 공격 시나리오

네트워크 보안 솔루션의 취약점을 이용한 공격 시나리오는 국내에 공개된 적은 없지만 가까운 시일 내에 충분히 발생할 가능성이 있다. 외부의 접점이 되는 네트워크 보안솔루션의 취약점을 이용한다면 빠르게 내부 인프라를 점령할 수 있고, 타 보안솔루션에 탐지될 가능성도 적기 때문이다.

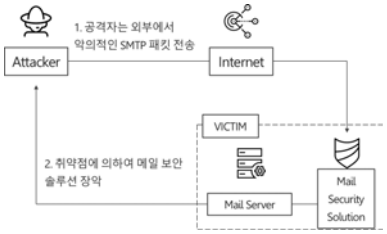
네트워크 보안 솔루션을 이용한 공격 시나리오는 국내 보안솔루션을 분석하여 도출한 취약점을 토대로 구성하였다. 표 1은 본 연구에서 확인한 국내 네트워크 보안 솔루션의 취약점과 개수를 나타낸다. 총 14개의 취약점을 확인하였으며 그 중 11개의 원격 코드 실행(Remote Code Execute) 취약점을 확인하였다.

<표 1> 국내 4개의 보안 솔루션의 취약점

취약점	A사	B사	C사	D사
원격코드 실행	1	7	1	2
파일 다운로드		1		
관리자 비밀번호 변경		1		
합계	1	10	1	2
총합	14			

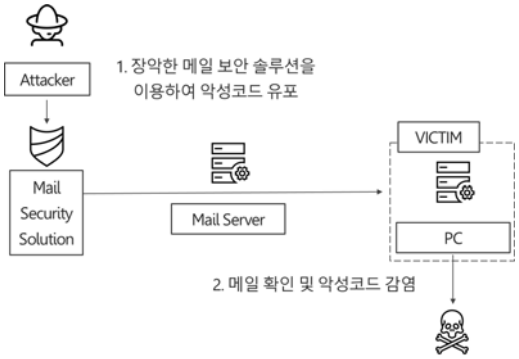
본 연구에서 도출한 취약점을 토대로 발생 가능한 네트워크 보안솔루션을 공격하는 시나리오를 구성하였다. 시나리오는 네트워크 보안 솔루션의 위치에 따라 2가지로 나뉜다. 하나는 외부에서 내부 사이에 위치하는 보안 솔루션을 공격하는 시나리오이고, 나머지 하나는 내부에 위치하는 보안 솔루션을 공격하는 시나리오다.

그림 1은 공격자가 외부와 내부 사이에 존재하는 네트워크 보안 솔루션 중 하나인 메일 보안솔루션에 악의적인 SMTP(Simple Mail Transfer Protocol)를 전송하여 장악하는 단계를 나타낸다. 이는 사용자의 메일 열람여부와 상관없이 메일 보안솔루션이 메일의 내용을 확인하는 과정



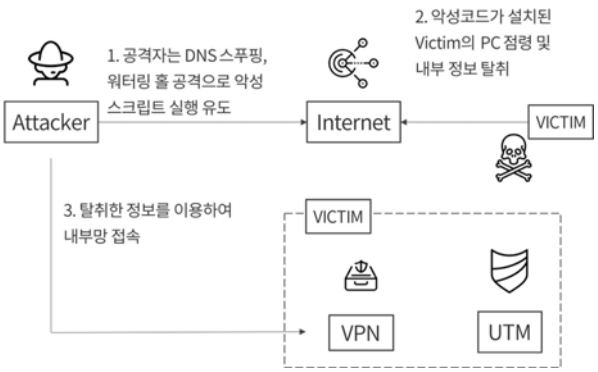
(그림 1) 외부에서 내부 사이에 위치하는 보안 솔루션 점령

에서 발생하는 취약점을 이용하므로 악성 SMTP를 보내기만 하면 솔루션을 장악할 수 있다.



(그림 2) 외부에서 내부 사이에 위치하는 보안 솔루션을 이용한 사용자 PC 공격

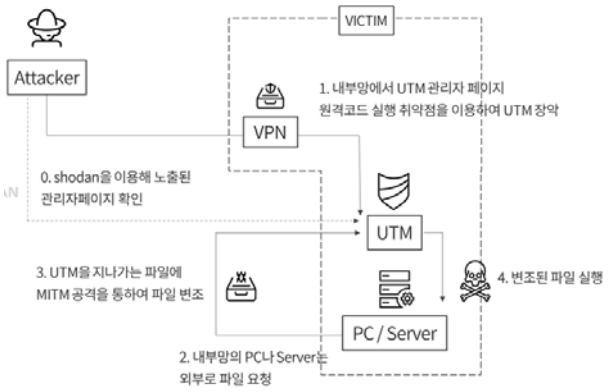
그림 2는 메일 보안솔루션을 장악하여 내부 인프라를 공격하는 시나리오를 나타낸다. 메일 보안솔루션은 메일의 내용을 수정하고 삭제할 수 있으므로 이 기능을 이용하여 정상적인 파일을 악성코드로 변경하여 보안 솔루션이 보호하는 내부 인프라의 사용자 PC를 점령할 수 있다.



(그림 3) 내부에 존재하는 보안솔루션을 공격하기 위한 진입

그림 3은 내부에 존재하는 보안솔루션인 UTM(United Threat Management)에 접근하기 위해 VPN(Virtual Private Network)을 공격하여 내부 망에 침투하는 단계를

나타낸다. 이 VPN은 SSL(Secure Socket Layer) VPN으로 가용성을 제공하기 위해 해당 솔루션을 사용하는 기관의 특정 사이트에서 다운로드 받을 수 있으며, 대부분 Active X와 같은 형태로 제공된다. 그러므로 공격자는 이 페이지에 외부에서 접근하여 해당 솔루션을 다운받아 분석할 수 있다. 사용자가 Active X의 취약점을 동작시키는 악성 스크립트를 설치한 사이트에 접속하도록 유도하기 위해 DNS(Domain Name System) 스푸핑을 하거나 워터링 홀 공격(Watering Hole Attack)을 한다. 이를 통해 사용자의 PC를 점령하고 정보를 탈취하여 내부 망에 접속한다.



(그림 4) 내부에 존재하는 보안솔루션을 점령

그림 4는 내부에 존재하는 보안솔루션인 UTM을 점령하는 단계다. 관리자 페이지에 존재하는 원격코드 실행 취약점을 이용하여 UTM을 점령한다. 관리자의 부주의로 해당 관리자 페이지를 외부에서도 접근 가능하다면 그림 3과 같은 단계를 거치지 않고 UTM에 바로 접근할 수 있다. UTM은 패킷을 모두 확인하고 차단하기 위해 인라인(inline) 방식으로 설치되는 경우가 많다. 그러므로 감시하는 모든 패킷을 조작도 가능하고, 이를 통해 MITM(Man In The Middle) 공격을 할 수 있다.

4. 결 론

본 연구는 분석을 통해 도출한 취약점을 토대로 네트워크 보안 솔루션의 취약점을 이용한 두 가지 공격 시나리오를 제시했다. 이를 통해 자원과 자산을 보호하기 위해 도입한 보안솔루션이 공격의 통로로 사용될 뿐만 아니라 공격에 사용 가능하다는 위험을 보였다.

이에 대응하기 위한 현실적인 방법은 기업과 기관이 선별적으로 공개되는 국가 보안 취약점 데이터베이스에서 보안 솔루션의 취약점 공개를 활성화하고 국가에서는 보안 솔루션의 취약점을 선별적으로 관리하는 제도를 마련하는 것이다. 뿐만 아니라 보안 담당자들도 보안 솔루션을 이용하여 있다는 사실을 유념하고 이를 이용한 공격에 대비하여 피해를 최소화할 수 있는 방안을 마련해야 한다.

Acknowledgement

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00213, 능동적 사전보안을 위한 사이버 자가변이 기술 개발)

참고문헌

[1] NIST, Special Publication 800-30 Revision 1, “Guide for Conducting Risk Assessments,” http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[2] KISA, “Cyber Security Issue 14년 11월동향”, 2014. 11.

[3] KISA. “Power Review 2016 9월 1주차”, 2016. 09

[4] https://cve.mitre.org/Roger S. Pressman ″Software Engineering A Practltiners′ Approach″ 3rd Ed. McGraw Hill