망분리 환경에서의 IT 보안 위협 및 대응 방법 분석

김창석 · 김종민*

동신대학교

Analysis of IT security threats and countermeasures in a network-separated environment

Kim-chang Seok · Jong-min Kim*

Dongshin University

E-mail : rlackdtjr100@naver.com / dyuo1004@dsu.ac.kr

요 약

망분리 환경은 내부 업무망과 외부 인터넷망을 분리하는 네트워크 보안 설계시스템으로 인터넷이 연결된 네트워크와 연결되지 않은 업무용 네트워크로 분리하여 내부 업무망과 외부 인터넷망이 분리되어 보안적 측면에서 단일망에 비해 비교적 안전한 네트워크 구조이다. 하지만 내부 시스템, 네트워크 장비, 보안장비의 취약점을 이용하여 내부망을 감염시키는 사례가 빈번하게 발생하고 있다. 본 논문에서는 이러한 망분리 환경의 IT보안 위협 취약점을 분석하고 효과적인 보안관제를 위한 기술적인 방안을 제안한다.

ABSTRACT

The network separation environment is a network security design system that separates the internal business network from the external Internet network. It separates the internal business network from the external Internet by separating it into a business network that is not connected to the network to which the Internet is connected. The network is separated, and it is a relatively secure network structure compared to Danilman in terms of security. However, there are frequent cases of infecting internal networks by using vulnerabilities in internal systems, network devices, and security devices. In this paper, we analyze the vulnerability of IT security threats in such a network isolation environment and provide technical measures for effective security monitoring.

키워드

망분리, 이벤트 로그, 보안 위협 취약점 분석, 침해사고, 클라우드

Ⅰ. 서 론

망분리 환경은 공공기관/기업 등에서 전산망 마비 사태와 같은 해킹을 막을 수 있는 최선의 기술로써 인터넷망과 사내망을 따로 분리 하여 인터넷망을 통해 내부망으로 들어올 수 있는 경로를 차단하여 인터넷에는 인터넷 망으로만, 업무용 네트워크에서는 내부망으로만 접근 할 수 있도록 해주는 네트워크 환경이다. 망분리 환경은 외부 인터넷으로부터 들어올 수 있는 여러 취약점의 감염경로를 망분리를 통해 차단하기 때문에 망분리 환경을 도입한 이후에는 단일망 환경보다 보안사건/사고 발생이 현저히 줄어들었다.

하지만 망분리 환경 방식 또한 사람이 운용한다라는 점에서 보안위협에 대해 완벽하다고는 할 수는 없으며, 인터넷에서 사용자도 모르게 감염된 자료가 업무망 내부로 유입되는 사례 등과 같이 사람이 실수를 하거나 관리소홀로 인해 내부망과 외부망이 연결될 수 있는 부분에서 취약점이 언제든지 발생할 수 있다. 본 논문에서는 그러한 취약점을 분석하여 효과적인 보안을 위한 방안을 제시한다[1].

* corresponding author

II. 망분리 네트워크 구성

망분리 네트워크는 그림1과 같이 방화벽을 통해 외부망과 내부망을 분리하여 외부 인터넷망을 통한 불법 접근과 내부 정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 '망 차단 조치'를 하여 인터넷망과 업무망을 분리해 인터넷으로부터 유입되는 각종 사이버 공격을 막을 수 있도록 해주는 네트워크 구조이다. 그러나 인터넷에서 사용자 모르게 감염된 자료가 업무망 내부로 유입되어 업무망 기밀정보가 외부로 유출될 가능성이 존재하고 한 사람이 2개 이상 OS와 응용프로그램을 사용해야 하기 때문에 라이선스도 하나의 단말에서 사용하는 기기보다 훨씬 비싼 단점이 존재한다[2].

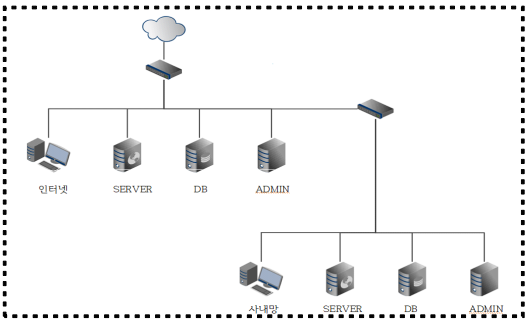

그림 1. 망분리 네트워크 구성도

III. 망분리 환경 지능형 해킹 사례

망분리 환경은 지능적인 방법을 사용해서 지속적으로 특정 대상을 공격하여 침입을 성공할 때까지 다양한 IT 기술과 공격방식을 기반으로 여러 보안 위협을 생산하여 공격을 멈추지 않고 오랫동안 피해자가 알지 못하도록 그림2 와 같이 사회공학적 기법을 이용해 회사로 가장하여 악성코드가 첨부된 메일을 보내는 등과 같은 방법으로 정보를 수집하고 침입하여 C&C 서버와 같은 백도어 프로그램을 통해 C&C서버와 통신하여 정보들을 수집하여 점점 높은 권한을 획득하여 내부 시스템을 장악하고 확산한 뒤 중요 데이터에 접근 가능한 관리자급 권한을 획득하였다면 실제 중요 데이터가 저장되어 있는 시스템에 접근하여 데이터를 유출 또는 파괴를 시킨다.

이러한 지능형 공격은 내부 사용자들의 허점 및 관리 시스템의 취약점을 이용하여 은밀하게 침투하므로 본인도 감염 사실을 알기 어렵다[4].

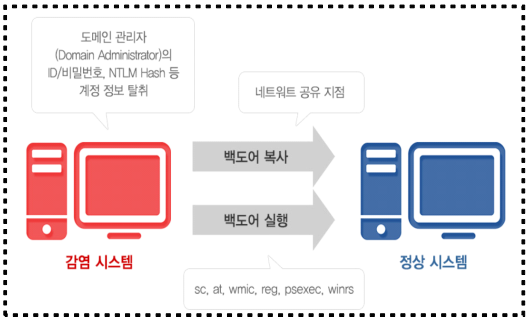

그림 2. 망분리 환경 공격 내부 확산 과정[5]

1. 평창 동계 올림픽 개막식 공격

개막식 1개월 전인 2018년 1월 올림픽 운영 전산실과 연결된 라우터에 비휘발성 저장장치로 알려진 하드디스크에 자신의 정보를 저장하지 않고 휘발성 저장 장치인 램의 특정 메모리 영역인 프로 세스에 삽입하여 악성행위를 일으키는 인 메모리 악성코드를 사용하여 그림3과 같이 내부 pc 를 감염시킨 후 내부에서 사용하는 계정 정보를 탈취하여 서버 접근 권한을 획득하고 개막식 시작 시간에 맞추어 DDoS(Distributed Denial of Service) 공격을 이용하여 서버 내의 데이터를 복구 불가능하게 지워버린 후 부팅이 불가능하게 파괴해버린 사건이다[6].

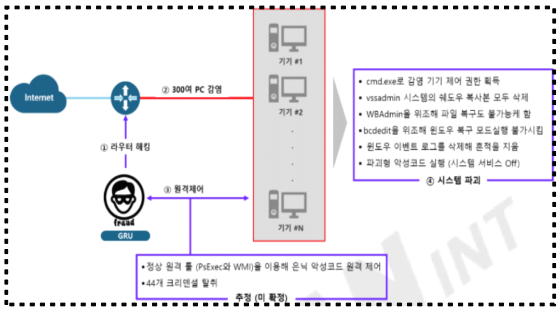

그림 3. 평창 동계 올림픽 개막식 사이버 공격 구성도[6]

2. 코니의 스피어 피싱 공격

이메일에 악성 DOC 문서 파일을 첨부하는 방식을 사용한 것으로 추정되며 일본 패럴림픽 관련 문서의 파일명을 실존하는 자선 단체를 사칭하여 메일 수신자가 신뢰하고 문서를 열어보도록 유도하여 사용 버튼을 클릭하게 되면 내부에 포함된 악의적인 VBA 코드가 활성화 되면서 정상적인 문서 내용을 보여줌과 동시에 악성코드가 은밀하게 실행되어서 공격자가 임의로 지정한 FTP서버로 사용자 PC 시스템의 주요 정보를 업로드 하는 사건이다.

이러한 스피어 피싱은 공격자가 추가 명령에 따라 원격제어가 가능한 RAT 감염 등 2차 피해로

이어질 수 있다[7].

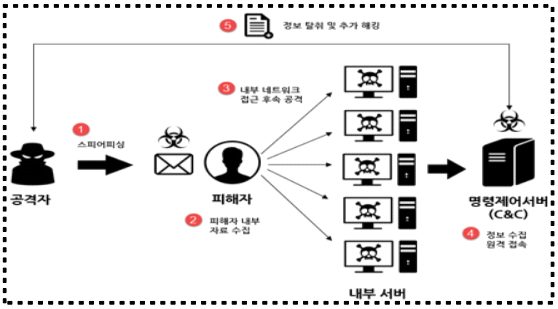

그림 4 스피어피싱 공격 구성도[8].

Ⅳ. 클라우드 보안 탐지 모델

위의 사례들과 같이 망분리 환경에서의 보안위협은 사용자를 속여 사용자 PC에 접근하는 방식으로 공격이 이루어 졌다. 또한 공격이 발생한 이후 수개월 이상 경과한 뒤 인지하는 경우가 발생하고 있으며, 시스템을 분석 시 연결되어진 모든 데이터를 분석해야 하기때문에 상당한 시간이 소요된다.

따라서, 이러한 문제점들을 해결할 수 있는 클라우드 보안 탐지 모델을 제안한다.

그림 5는 AWS 보안 서비스 워크플로우이며, 식별, 방어, 검출, 반응, 복구의 단계로 이루어진다.

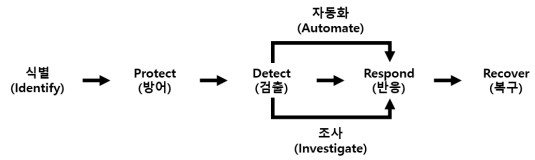

그림 5 AWS Secrity Value Chain[9].

제안된 클라우드 보안 서비스 모델을 도입 하게 되면, 망분리에서의 문제점으로 지적하였던 보안위협의 인지에 대한 문제 같은 경우, 인공지능 기반의 탐지 규칙을 이용해 손쉽게 탐지를 할 수 있으며, 또한 자동화를 통한 보안위협에 대해 자동으로 격리를 함으로써, 데이터 분석에 있어 상당한 시간을 줄일 수 있을 것이다.

또한 클라우드에서 발생하는 이벤트들을 학습함으로써, 비정상적인 이벤트들에 대한 즉각적인 모니터링 및 원인분석이 가능하다.

Ⅴ. 결 론

본 연구에서는 망분리 환경에서의 IT 보안 위협 사례들을 분석하고 문제점들을 도출하였다.

망분리 환경에서의 보안위협에 대응방법은 보안 시스템에서 위협을 판단하게 되면, 이후에 사람이 판단을 하고 대응하여 수동적인 방법으로 대응하여야 했다.

하지만 클라우드 기반 보안 탐지 모델을 적용을 하게 되면 보안위협에 대해 인공지능이 판단하여 탐지하고, 자동으로 격리함으로써, 빠른 시간내에 위협에 대해 대응할 수 있다.

또한, 클라우드 같은 경우 서버에서 동작을 하기 때문에 서버자체가 장악 당하게 되면, 모든 자료에 대한 권한을 넘겨주게 된다. 그렇지만 클라우드 환경에서는 백업을 통해 감염된 서버를 OFF하고 백업된 서버를 ON하면 바로 직전의 환경을 구성할 수 있기 때문에 신속한 대처가 가능하게 된다.

Acknowledgement

본 과제(결과물)는 2020년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다.

References

[1] https://www.boannews.com/media/view.asp?idx=54952
[2] https://nakyungpapa.tistory.com/tag/%EB%A7%9D%EC%97%B0%EA%B3%84%20%EB%8B%A8%EC%A0%90
[4] https://m.blog.naver.com/PostView.nhn?blogId=daouidc&logNo=220773045311&proxyReferer=https:%2F%2Fwww.google.com%2F
[5] http://www.igloosec.co.kr/BLOG_APT%20%EA%B3%B5%EA%B2%A9%EA%B3%BC%20%EB%8C%80%EC%9D%91%EB%B0%A9%EC%95%88?searchItem=&searchWord=&bbsCateId=1&gotoPage=1
[6] https://brunch.co.kr/@ka3211/25
[7] https://www.dailysecu.com/news/articleView.html?idxno=98541
[8] http://www.epnc.co.kr/news/articleView.html?idxno=66614
[9] https://dev.classmethod.jp/articles/amazon-guardduty-explained-korean/