Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.4, Aug. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.4.859

망분리 환경에서 파일형식 변환을 통한 안전한 파일 전송 및 포렌식 준비도 구축 연구*

한 재 혁,[1†] 윤 영 인,[1] 허 지 민,[1] 이 재 연,[2] 최 정 인,[2] 홍 석 준,[2] 이 상 진[1‡]
[1]고려대학교 정보보호연구원, [2]한화시스템(주)

Secure File Transfer Method and Forensic Readiness by converting file format in Network Segmentation Environment*

Jaehyeok Han,[1†] Youngin Yoon,[1] Gimin Hur,[1] Jaeyeon Lee,[2] Jeongin Choi,[2]
SeokJun Hong,[2] Sangjin Lee[1‡]
[1]Institute of Cyber Security & Privacy (ICSP), Korea University,
[2]Hanwha Systems Co., Ltd.

요 약

최근의 사이버 보안 위협은 특정 표적을 대상으로 하는 특징이 있으며 보안을 강화시키기 위한 지속적인 노력에도 불구하고 APT 공격에 의한 피해 사례는 계속 발생하고 있다. 인터넷망과 업무망이 분리된 망분리 환경은 외부 정보의 유입을 봉쇄시킬 수 있으나 업무의 효율성과 생산성을 위해서는 현실적으로 외부 정보의 유입을 모두 통제할 수는 없다. 이에 망연계 시스템 등 보안 정책을 강화시키고 파일 내부에 포함된 불필요한 데이터를 제거할 수 있도록 CDR 기술이 적용된 솔루션을 도입하더라도 여전히 보안 위협에 노출되어 있다. 본 연구는 망분리 환경에서 망간 파일을 전송할 때 파일의 형식을 변환하여 전송함으로써 문서삽입형 악성코드의 보안 위협을 방지하는 방안을 제안한다. 또한 포렌식 준비도를 고려하여 문서파일이 원활한 사고대응을 위한 정보를 보관할 수 있는 기능을 포함하여 망분리 환경에서 활용할 수 있는 시스템을 제안한다.

ABSTRACT

Cybersecurity attack targeting a specific user is rising in number, even enterprises are trying to strengthen their cybersecurity. Network segmentation environment where public network and private network are separated could block information coming from the outside, however, it is unable to control outside information for business efficiency and productivity. Even if enterprises try to enhance security policies and introduce the network segmentation system and a solution incorporating CDR technology to remove unnecessary data contained in files, it is still exposed to security threats. Therefore, we suggest a system that uses file format conversion to transmit a secure file in the network separation environment. The secure file is converted into an image file from a document, as it reflects attack patterns of inserting malicious code into the document file. Additionally, this paper proposes a system in the environment which functions that a document file can keep information for incident response, considering forensic readiness.

Keywords: file format conversion, CDR, forensic readiness, network separation, malware, APT

Received(08. 01. 2019), Modified(08. 07. 2019), Accepted(08. 07. 2019)
* 본 연구는 한화시스템(주)의 재원을 지원받아 수행된 연구임

† 주저자, one01h@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

I. 서 론

최근의 사이버 보안 위협은 과거와 달리, 공격자 개인의 만족이나 금전적인 이익을 위한 불특정 다수를 대상으로 하는 공격보다는 정치적, 외교적, 군사적, 문화적, 금전적 이익 등 다양한 목적을 달성하기 위해 특정 공격 표적을 집요하게 공격하는 지능형 지속 위협(APT: Advanced Persistent Threat) 공격이 대부분이며[1], 공급망 공격(Supply Chain Attack)에 의한 피해 사례도 발생하고 있다.

사이버 보안 위협은 주로 기존 보안제품을 우회하거나 소프트웨어 취약점(Zero-Day 공격 등)을 이용하고, 특정 시스템에 접근할 수 있는 권한을 가질 수 있는 악성코드를 감염시키는 것을 시작으로 활동한다. 악성코드는 메일[2]이나 메신저에서 사용자가 첨부된 파일을 다운로드 받거나 신뢰할 수 없는 인터넷 사이트에 접속하거나 인가되지 않는 외부저장매체를 연결하는 방법 등으로 유입되고 이를 사용자가 실행시킴으로써 감염된다[3].

기업에서는 사이버 공격에 대응하기 위해 정보보호 시스템(방화벽, IDS, IPS 등)이나 보안 솔루션(ESM, SIEM 등)을 설치하고 보안 정책을 주기적으로 강화시키며 망을 분리하는 등의 방법으로 자산을 보호하기 위해 노력한다. 특히, 망분리(외부 인터넷망 차단)는 정보통신망법(정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령, 제15조 2항 3호), 개인정보보호법(개인정보 보호법 시행령, 제30조 1항 2호)에서 의무사항으로 법제화되었으며, 정부는 보안 강화를 위해 가이드를 배포하고 있다.

또한 안티바이러스(AV: Anti- Virus)이나 샌드박스(sandbox)와 같은 보안 기술로도 막아내지 못한 파일에 대비하기 위해 내부 콘텐츠 분석을 통해 악성코드 등 위험요소를 제거한 후 원본과 동일하게 열람할 수 있는 파일을 만드는 CDR (Content Disarm & Reconstruction) 기술이 개발되었으나, 현실적으로 파일형식을 완벽하게 이해하기 어렵고 원본과 동일하게 열람할 수 있는 파일을 만든다는 것이 쉽지 않으며 알려지지 않은 취약점이나 안티포렌식 기술에는 여전히 취약할 수밖에 없다. 이러한 조치들은 외부로부터 악성코드 유입 등 보안 취약점을 최소화하기 위함이지만, 그럼에도 불구하고 망간(외부 인터넷망↔내부 업무망) 파일 송수신 과정에서 보안 기능을 우회하는 사이버 공격에 의한 피해 사례[4]는 한수원 사이버테러 사건(2015년) 등 끊임없이 발생하고 있다.

Table 1. File formats mostly supported by CDR solutions

Type	File extension
Document	docx, pptx, xlsx
	doc, ppt, xls, odf
	pdf, hwp, html, rtf
Multimedia	mp3, mp4, wmv
AudoCAD	dxf, dwf

본 논문에서는 망분리 환경에서 악성코드를 감염시키려는 보안 취약점에 대응하기 위해 문서파일을 대상으로 파일형식을 변환시키는 방법으로 망간 안전하게 파일을 전송하는 기법을 연구하였다. 또한 보안 강화가 업무 편의성을 저하시킬 수 있다는 단점을 보완하고 포렌식 준비도(forensic readiness)를 고려한 적용 모델을 제시한다.

II. 배경지식 및 관련연구

망분리 환경을 구성하면 악성코드의 동작 범위를 한정시킴으로써 피해를 최소화시킬 수 있으며 업무망 내부의 데이터를 안전하게 보호할 수 있다는 장점이 있으나[5], 기존 보안 환경을 우회할 수 있는 신종·변종 악성코드가 등장하고 샌드박스를 우회하는 기술이 적용되기 때문에 실행파일 이외의 다양한 파일 형태의 공격에 대응하기 위한 기술로 CDR이 주목받기 시작했다. IT시장조사 전문기관인 가트너는 보안 이메일 게이트웨이(Secure Email Gateway) 시장에서 지속형 위협 방어(ATD: Advanced Threat Defense)[6] 솔루션으로 네트워크 샌드박스와 함께 CDR을 권장하고 있다[7].

CDR은 파일 구조를 분석하여 악성코드나 은닉된 데이터 등 추가되거나 파일을 열람하는 과정에서 필요하지 않은 데이터를 제거하는 기술이다. 과거에는 실행파일(예: PE, ELF 등)을 통한 공격이 주로 시도되었으나, 최근에는 안티바이러스의 성능 개선과 기업 내 보안 정책에 의해 차단되면서 업무 중 이메일이나 공유폴더를 통해 문서파일을 주고받는 경우가 많다는 특징을 이용하여 문서파일 내 데이터를 삽입하는 형태로 공격 패턴이 변화하고 있다. 문서파일을 이용한 악성코드 공격에는 취약점, 스크립트, EPS (Encapsulated PostScript), 객체 삽입(OLE:

Object Linking and Embedding) 등의 방법이 존재한다. 이를 탐지하기 위해 가상환경에서 직접 실행해서 행위를 분석하는 방식으로 악성 유무를 판별할 수 있으나 샌드박스를 우회하는 기술이 적용되어 있는 경우는 탐지되지 않을 수 있다[8].

문서파일 내부에 악성코드를 삽입하는 방법은 주로 구조적으로 사용되지 않는 영역을 활용한다. 많이 사용되는 PDF(Portable Document Format)는 849개의 취약점(CVE; Common Vulnerabilities and Exposures, 2019년 7월 기준)이 알려져 있으며, 한글문서와 MS오피스문서(2003 이하)로 사용되는 복합파일이진형식(CFBF; Compound File Binary Format)은 데이터 은닉을 위한 공간으로 사용될 수 있는 미사용 영역, 슬랙 영역, 예약 영역이 존재한다[9]. 여기에서 의도적으로 삽입된 데이터는 다른 실행프로그램에 의해 악성코드의 요소로 활용될 수 있으므로 악성코드와 마찬가지로 제거되어야 하는 데이터이다. CFBF와 마찬가지로 개방형문서 형식(ODF; Open Document Foramt)이나 MS오피스문서(2007 이상)에서 사용되는 OOXML(Open Office XML)도 매크로나 VB스크립트를 활용하는 악성코드가 삽입될 수 있으며 문서 내부의 XML파일에 은닉된 데이터가 삽입될 수 있다[10].

CDR을 활용하여 문서파일에서 발생할 수 있는 사이버 보안 위협에 방어 효과를 일부 기대할 수 있으나, 단순히 파일 구조를 분석한 결과만으로 특정 영역의 데이터가 사용자가 입력한 내용인지 공격자가 의도적으로 삽입한 내용인지를 판단하기에는 예외사항이 많아 해당 데이터 제거 여부를 판단하고 자동화하여 처리하는데 어려움이 많다. 예를 들어, 문서파일 자체에 보안 기능이 설정되어 비밀번호를 입력해야 열람이 가능한 경우만 하더라도 CDR이 적용된 솔루션은 관리자에 의해 설정된 보안 정책을 참고하여 동작한다. 즉, CDR은 파일에 삽입된 파일구조를 파악한 후 위협요소를 제거함으로써 안전한 파일로 재생성하는 방법이지만 알려지지 않은 취약점이나 데이터 은닉 영역에 대한 탐지가 불가능하다.

III. 안전한 파일전송 적용 시스템 개발

망분리는 악성코드의 유입경로를 원천적으로 차단할 수 있는 물리적 망분리와 저렴한 비용으로 구축이 가능한 논리적 망분리로 구분된다[11]. 이렇게 구축된 망분리 환경은 인터넷망과 업무망을 나누어 관리하기 위한 정보보호조치이지만, 외부와의 네트워크 단절로 인해 업무의 편의성과 효율성을 저하시킬 수 있다는 단점이 있다. 이에 인가된 저장매체와 매체제어 솔루션을 추가로 도입하거나 망연계 시스템(secure gate)을 구축하여 망간 정보의 교환이 가능하도록 구성한다. 다시 말하면, 망분리 환경을 구축해놓더라도 인터넷망에서의 정보는 최종적으로 업무망으로 유입될 수 있는 것이며 사이버 보안 위협에의 노출을

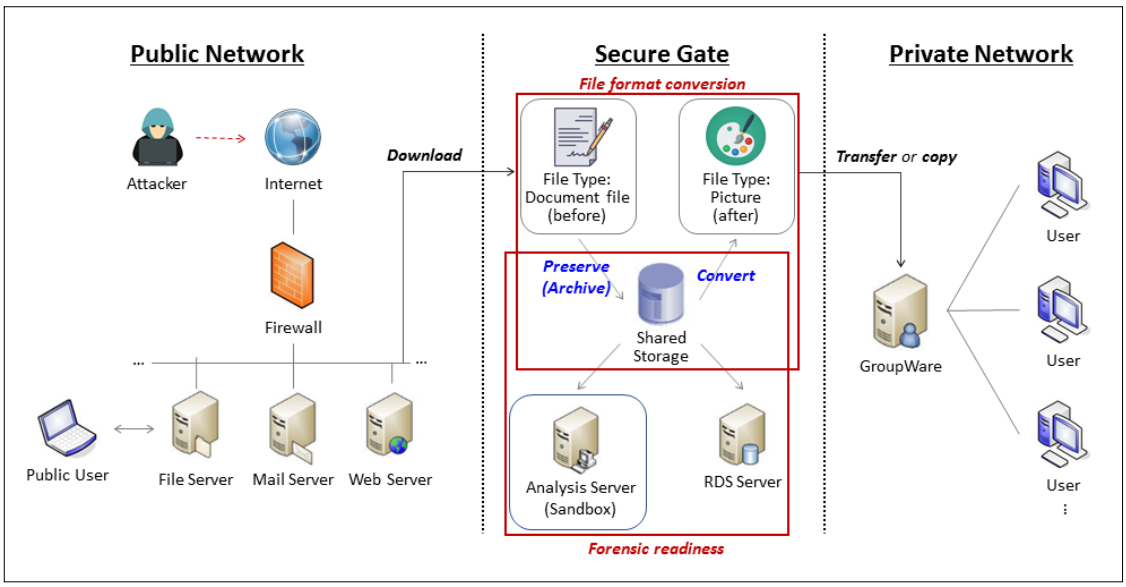

Fig. 1. Secure file transfer system by converting file format in network separation

Table 2. Document File Formats and File Signatures

Type	File Format	File Signature
PDF	pdf	0x25504446 ("%PDF")
CFBF	hwp, doc, xls, ppt, rem	0x50CF11E0 A1B11AE1
OOXML	docx, xlsx, pptx	0x504B0304 14000600 ("PK")

최소화하는 방법일 뿐, 정보보호 시스템이나 보안 솔루션에서 악성코드 탐지에 실패할 경우에는 여전히 보안 위협의 가능성이 있음을 의미한다.

따라서 망간 안전한 정보 교환을 위해서는 보안 위협이 되는 요소를 원천적으로 제거할 필요가 있다. 이에 업무에서 사용되는 정보로 많은 비중을 차지하는 문서파일을 대상으로 파일형식을 변환시키는 과정을 적용하여 Fig.1과 같이 시스템으로 구축하였다.

구축한 시스템에서 지원하는 문서파일은 업무에서 주로 사용되는 것을 선정하였으며, 각 파일은 파일 확장자와 파일 시그니처를 비교하여 파일 종류를 확인할 수 있다(Table 2). 문서파일의 파일형식을 변환하는 프로세스를 적용하면 원본의 파일구조에서 문서를 열람하였을 때 보이는 내용 이외에 추가된 데이터는 제거할 수 있으므로, 악성코드가 포함되었던 원본이더라도 악성코드 탐지 프로세스를 수행하지 않고도 안전한 파일로 생성할 수 있다. CDR의 한계점은 파일구조에 대한 완벽한 이해가 필요하고 알려지지 않은 취약점이나 데이터 은닉이 가능한 공간에 대한 보안 위협이 잔존할 수 있다는 것이다. CDR은 새로운 공격 방법에 대응하기 위해서 안티바이러스와 같이 주기적인 패치가 필수적이다. 이러한 한계를 극복하기 위해 안전한 파일전송 적용 시스템(Fig. 1)은 안전한 파일전송과 포렌식 준비도를 고려하여 다음 기능들을 지원하도록 구축하였다.

(1-1) 원본의 파일형식 변환: 문서 → 그림

(1-2) 문서편집 환경 제공, 악성코드 분석

(2) 원본 파일의 압축 보관, 해시값 저장

3.1 보안 위협 제거를 위한 파일형식 변환 기능

파일형식 변환은 문서 내부 구조를 분석하여 용지설정(layout), 글자·문단모양(formatting), 글꼴(font), 삽입된 그림(image) 등의 상태를 다른 파일형식으로 재구성하는 방식으로 동작한다. 일반적으로 사용되는 문서편집기에서 '다른 이름으로 저장하기(Save As, Export)' 기능과 유사하다. 하지만 이 시스템에서는 화면을 캡쳐하는 방식(screenshot)을 응용하여 그림파일형식의 파일을 생성하도록 개발하였다. 이 방식은 원본파일로부터 활용하는 데이터가 전혀 없이도 원본의 문서파일을 열람할 때와 새로 생성된 그림파일을 열람할 때와의 차이를 인지하기 어려울 정도로 동일한 파일 생성이 가능하고, 파일형식에 대한 자세한 구조분석 없이도 생성이 가능하므로 새로운 파일형식이 등장하거나 구조가 개선되어도 기존 시스템과의 호환성이 좋다.

CDR을 이용하여 생성된 파일에서는 데이터 은닉을 위해 사용할 수 있는 영역에 기록된 데이터가 여전히 저장된 상태로 출력되거나(CBFB, OOXML) 사용자가 추가로 설치한 글꼴이 포함된 경우 글꼴 개발사에서 배포하는 정상적인 파일임에도 불구하고 악성코드를 포함하는 문서로 분류하여 문서파일을 열람하는데 제한되는 경우(PDF)가 있는데 화면을 캡쳐하는 방식에서는 그러한 예외처리가 필요하지 않다.

파일형식을 변환하는 방식이 악성코드와 같은 보안 위협 제거에 대한 성능을 평가하기 위해 문서 삽입형 악성코드 샘플을 수집하여 실험을 진행하였다. 악성코드 샘플은 문서파일의 확장자로 태그를 설정하여 멀웨어즈닷컴(malwares.com)의 API를 이용하여 2,765개를 수집하였으며, VirusTotal에 조회하여 악성여부를 확인하였고 샌드박스 환경에서 악성코드를 동작시켜서 새로운 파일 생성, 레지스트리 키 변경, 네트워크 통신 등의 악성행위를 확인하였다. 악성코드 분석은 우분투(ubuntu ver. 14.04) 운영체제에서 cuckoo sandbox(ver. 1.2)을 사용하여

Table 3. Evaluation of file type conversion to eliminate security threats in the Documents

Before: Document		After: Picture		Malicious rate
file format	#	file format	#	
PDF (pdf)	1,090	JPG (jpg)	1,090	100%
CBFB (hwp, doc, ppt, xls)	866		866	100%
OOXML (docx, pptx, xlsx)	809		809	100%

```
Data: Document file
Result: How to convert a document file for User
initialization;
User make a request for download the document file;
Server download the file which were request by User;
while in the Secure Gate do
    Convert the file type and Transfer to the user;
    Calculate hash values of the files before and after conversion;
    Archive and Store the files in the Shared Storage;
    Execute SQL statement:
    "INSERT INTO files VALUES datetime, hash, user, source, ...);";
    if detect malware | edit document then
        go to Analysis Server with the file
    end
end
```

Fig. 2. How to convert a document file for user in the secure gate

진행하였으며, 파일형식을 변환시킨 샘플은 모두 악성행위가 작동되지 않음을 확인하였다.

파일형식의 변환으로 파일을 전송하면 업무망의 보안은 강화시킬 수 있으나, 업무의 편의성은 저하시킬 수 있다. 인터넷망으로 수신한 문서파일은 열람만 하는 것이 아니라 편집이 필요한 경우도 다수 있는데 그림형식의 문서파일에서 문자열 편집은 OCR (Optical Character Recognition)을 이용하거나 다른 그림으로 덮어쓰는 등의 방식으로는 제한적일 수 있다.

이에 본 시스템은 사용자가 문서파일의 편집이 필요한 경우에 대비하여 파일형식을 변환시키기 이전 상태(원본)로 파일을 저장한다. 원본 문서파일이 저장되어 있는 저장소에 접근하여 샌드박스 환경이 구성된 상태에서 편집을 하거나 인가된 저장매체에 원본을 복사하고 인터넷망이 연결된 PC에서 작업할 수 있도록 구성하였다. 이러한 방식은 물리적 망분리 환경과 동일한 보안 수준을 확보할 수 있으며 업무망은 안전한 네트워크 환경을 유지할 수 있도록 한다. 저장소에 보관되어 있는 원본은 파일을 변환시키는 과정에서 발생할 수 있는 문서내용의 차이를 파악하기 위한 용도로도 활용될 수 있다.

3.1 사고 대응을 위한 원본 파일 보관 및 로그 기록

악성코드 감염으로 인한 내부의 정보 유출이나 침해사고에 대응하기 위해서는 특정 파일을 처리한 이력 등 시스템 자원의 동작 내용을 관리하고 사용자 행위를 추적할 수 있는 정보를 사고가 발생하기 이전부터 생성할 필요가 있다. 최근 발생하는 APT 공격은 목표물에 최적화된 공격 기법을 사용하기 때문에 공격시점과 피해범위, 그리고 사고원인 등을 빠르게 감지하기 위해서 포렌식 준비도를 고려하여 사전에 대비해야 한다.

악성코드 분석을 위한 서버는 시그니처 기반 분석 및 행위기반 분석을 적용하거나 이메일 백신 클라우드 시스템을 이용하여 첨부파일을 분석하는 가상화 기술을 활용하되[12], 본 연구에서는 악성코드를 포함하는 파일을 탐지하고 분석하는 방법을 구체적으로 논하지 않고 사고 대응을 위한 기반 정보로써 다음 항목을 포함하여 기록(윈도우 이벤트로그 포함)이 쌓이도록 시스템을 구성하였다.

- 서버로부터 다운로드 받은 문서파일
- 파일형식을 변환한 그림파일
- 파일을 요청한 사용자 정보
- 사용자가 파일을 요청한 시각, 다운로드가 완료된 시각, 파일형식 변환이 완료된 시각, 전송시각
- 파일의 해시값, 파일 출처(서버 정보 등)

파일형식을 변환하기 전후의 파일은 사고가 발생하였을 때 대상 파일을 식별하기 위함이며, 사용자

정보는 해당 파일의 전송을 요청한 대상을 확인할 수 있다. 여러 개의 시각 정보는 파일의 이력과 흐름 시점을 감시할 수 있게 하며, 파일의 해시값은 참조 데이터 세트(RDS; Reference Data Set)를 구축할 수 있게 한다. RDS는 디지털 포렌식 조사의 효율성을 높이기 위해 특정 파일은 분석 대상에서 제외하기 위해 사용하는 데이터 세트이다[13]. 이전에 업무망으로 유입되었던 파일의 악성여부 등을 신속하게 식별할 수 있으며 특정 조건과 관련 있는 파일들을 선별하고 해당 파일에 대한 이력정보를 지속적으로 추가시키는 방식으로 관리할 수 있다.

이러한 기능들이 포함된 안전한 파일전송 적용 시스템은 망연계 시스템 내에서 Fig. 2가 적용되어 동작한다. ① 사용자는 열람이 필요한 문서파일을 서버에 다운로드를 요청하고 ② 서버는 이에 대한 응답으로 해당 파일을 다운로드한다. ③ 이 파일을 그림파일형식으로 변환을 시켜서 사용자에게 전달하고 ④ 원본은 파일 해시값을 계산한 후 압축된 형태로 저장시킨다. ⑤ 만약 악성코드 여부를 확인하기 위한 분석이나 사용자로부터 문서편집을 추가로 요청받을 경우 샌드박스(또는 가상머신)로 구축된 분석서버로 원본을 조작할 수 있도록 전송함으로써 외부의 보안 위협을 점검할 수 있게 한다. 이러한 과정으로 망분리 환경에서 파일형식 변환을 통해 알려지지 않은 보안 위협이 제거된 파일을 업무망으로 신속하게 전송할 수 있고, 해당 파일 및 사용자와 관련이 있는 이력을 관리할 수 있으며 악성코드 탐지를 위한 분석 환경을 지원함으로써 포렌식 준비도를 위한 체계를 구축할 수 있다.

IV. 결 론

사이버 보안 위협의 증가로 인해 정보보호 시스템이나 보안 솔루션으로 보안을 강화시키고 있으며 의무적으로 망분리 환경을 구축해야 한다. 이러한 노력에도 불구하고 APT 공격에 의한 피해 사례는 계속 발생하고 있기 때문에 망분리 환경에서 악성코드의 유입을 방지할 수 있는 방안이 요구되고 있다. 최근에는 이메일이나 공유폴더를 통해 문서파일을 주고받는 형태의 업무방식이 많다는 특징을 이용하여 문서파일에 악성코드를 삽입하는 방식의 공격 패턴이 발생하고 있다.

본 연구에서는 인터넷망에서 생성된 문서파일이 업무망으로 안전하게 전송될 수 있도록 파일형식을 변환하는 방식을 사용하여 시스템을 구축하였으며, 문서파일 내의 특이한 데이터를 제거하여 재생성하는 기술인 CDR이 가지고 있는 한계의 대안으로 사용될 수 있음을 확인하였다. CDR은 완벽하게 구현하기가 어렵고 현재 출시되어 있는 솔루션에서도 예외사항이 발생하고 있으나, 본 연구에서 제안하는 방식은 알려지지 않은 취약점과 은닉된 데이터와 같은 보안 위협이 될 수 있는 요소를 보다 확실하게 제거하고 호환성을 확보할 수 있으며 예외처리가 쉽다는 장점을 가진다. 다만, 사용자가 문서파일을 열람만 하는 것이 아니라 편집을 위해서는 물리적 망분리 환경과 같이 업무처리 효율성이 저하될 수 있다는 단점을 가지므로 향후에는 이를 보완할 수 있는 모델이 추가적으로 연구될 필요가 있다.

References

[1] Eun-hye Han and In-seok Kim, “Efficient Operation Model for Effective APT Defense.” Journal of The Korea Institute of information Security & Cryptology, 27(3), pp. 501-519, June. 2017.

[2] AhnLab, “Beware of APT Attacks Using E-mail”, https://asec.ahnlab.com/814, June. 2012.

[3] KISA, “Ransomware Guidelines.”, 2018.

[4] C. Tankard. “Advanced Persistent threats and how to monitor and deter them.” Network security, Vol. 2011. Issue 8, pp. 16-19. Aug. 2011.

[5] Byeong-joo Cho, Jang-ho Yun, Kyeong-ho Lee, “Study of effectiveness for the network separation policy of financial companies.” Journal of The Korea Institute of information Security & Cryptology, 25(1), pp. 181-195, Feb. 2015

[6] McAfee, “McAfee Advanced Threat Defense: Detect advanced malware”, Nov. 2018.

[7] Gartner, “Spamina recognized in the Market Guide for Secure Email Gateways”, 2017.

[8] Je-Seong Jeong, Kwangjo Kim, “A

Study on Detection of Evasive Malware in Cuckoo Sandbox", CISC-S'15, June. 2015.
〔9〕 Eunkwang Kim, Sangjun Jeon, Jaehyeok Han, Minwook Lee, Sangjin Lee, "An effective detection method for hiding data in compound- document files." Journal of The Korea Institute of information Security & Cryptology, 25(6), pp. 1485-1494, Dec. 2015.
〔10〕 Kiwon Hong, Jongsung Kim, "Improved Data Concealing and Detecting Methods for OOXML Document." Journal of The Korea Institute of information Security & Cryptology, 27(3), pp. 489-499, June. 2017.
〔11〕 Jungeun Jee and Yongtae Shin, "A Logical Network Partition Scheme for Cyber Hacking and Terror Attacks." Journal of KIISE, 39(1), pp. 95-101, Feb. 2012.
〔12〕 Choon Sik Park, "An Email Vaccine Cloud System for Detecting Malcode-Bearing Documents", Journal of Korea Multimedia Society 13(5), pp. 754-762, May. 2010.
〔13〕 NIST, "National Software Reference Library (NSRL).", https://www.nist.gov/software-quality-group/national-software-reference-library-nsrl

〈저자소개〉

한 재 혁 (Jaehyeok Han) 학생회원
2011년 2월: 서울시립대학교 수학과 졸업
2016년 2월: 고려대학교 정보보호대학원 정보보호학과 공학석사
2016년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 박사과정
〈관심분야〉 디지털 포렌식, 파일시스템, 데이터 마이닝

윤 영 인 (Youngin Yoon) 학생회원
2015년 2월: 고려대학교 컴퓨터통신공학 공학사
2015년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석박사통합과정
〈관심분야〉 디지털 포렌식, 침해사고대응

허 지 민 (Gimin Hur) 학생회원
2015년 2월: 한양대학교 컴퓨터공학 공학사
2015년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석박사통합과정
〈관심분야〉 디지털 포렌식, 역공학

이 재 연 (Jaeyeon Lee) 정회원
2002년 2월: 가톨릭대학교 정보통신공학 공학사
2004년 2월: 광주과학기술원 정보통신공학 공학석사
2004년~현재: 한화시스템 수석 연구원
〈관심분야〉 사이버 상황인식, 정보보호, 시스템 침입분석

최 정 인 (Jeongin Choi) 정회원
1994년 4월: 삼성전자(주) 연구원
1999년 2월: 영남대학교 정보통신공학 공학석사
2001년 7월~현재: 한화시스템 수석 연구원
〈관심분야〉 보안OS, 정보보호, 임베디드 시스템 침입분석

홍 석 준 (Seokjun Hong) 정회원
1997년 2월: 광운대학교 전자공학 공학사
2006년 2월: 연세대학교 전자공학 공학석사
2008년~현재: 한화시스템 수석 연구원
〈관심분야〉 정보보호, 정보보안체계, 통합보안관제

이 상 진 (Sangjin Lee) 종신회원
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털 포렌식, 심층암호, 해시함수