2018 한국차세대컴퓨팅학회
춘계학술대회

장　소 : 제주 제주한라대학교 컨벤션센터

일　시 : 2018. 5. 25(금) 12:40 ~ 5.26(토) 12:00

주최-주관　한국차세대컴퓨팅학회

후　　원　제주한라대학교 LINC+사업단

2018 한국차세대컴퓨팅학회 춘계학술대회

- **대 회 장** : 백성욱 교수(세종대학교)
- **조직 위원장** : 문석환 교수(제주한라대학교)
- **학술 위원장** : 김덕환 교수(인하대학교)
- **학술부위원장** : 노영태 교수(인하대학교)
- **조직 위원**

  노병희 교수 (아주대학교)
  노상욱 교수 (가톨릭대학교)
  신병석 교수 (인하대학교)
  이상웅 교수 (가천대학교)
  염성관 교수 (제주한라대학교)
  최린 교수 (고려대학교)

- **학술 위원**

  권구락 교수 (조선대학교)
  권준호 교수 (부산대학교)
  김동호 교수 (숭실대학교)
  김황남 교수 (고려대학교)
  나중채 교수 (세종대학교)
  박기웅 교수 (세종대학교)
  박남제 교수 (제주대학교)
  박운상 교수 (서강대학교)
  박준석 교수 (인하대학교)
  석준희 교수 (고려대학교)
  신석주 교수 (조선대학교)
  이문규 교수 (인하대학교)
  이미영 박사 (세종대학교)
  유성준 교수 (세종대학교)
  임완수 교수 (금오공과대학교)
  문인규 교수 (DGIST)
  조성제 교수 (단국대학교)
  최동완 교수 (인하대학교)
  한경식 교수 (아주대학교)
  김시우교수 (숭의여자대학교)

2018 한국차세대컴퓨팅학회 세부 프로그램

2018. 5. 25(금)		
12:40~13:10	등록	
13:10~14:00	Keynote Speech 국방 ICT융합 현황과 활성화방안 / 국방기술품질원 권경용 수석연구원	
14:00~14:30	개회식, 시상식(공로상, 우수논문)	
논문 발표	Oral Session 1	Oral Session 2
14:30~15:30	인터넷 뉴스 댓글 기반의 다중 감정 모델 개발 아주대학교 / 김우정, 한재호, 한경식	그룹 랜덤화를 통한 CCTV 객체 추적 데이터 보안 기법 설계 제주대학교 / 이동혁, 박남제
	컨테이너 이미지의 보안 취약성 데이터 수집 및 분석 경북대학교 / 탁병철	군집화 기반의 불균형 마케팅 데이터 분류 기법 고려대학교 / 손민재, 승원, 황인준
	XGBoost를 활용한 노인인지능력 변화 요인 해석 한국과학기술연구원 / 황혜진, 김수현, 송규원	고객의 소비 패턴 변화를 고려한 영화 추천 단국대학교 / 나연묵, 김민제
	Energy Efficient Adaptive Weighted Sum Function for Routing in WSN 조선대학교 / Madiha Razzaq, Seokjoo Shin	임베디드 환경에서 하드웨어 독립성 기반의 센서 플러그 앤 플레이 인하대학교 / 윤다빈, 박무동, 김덕환
15:30~15:45	Coffee break	
논문 발표	Oral Session 3	Oral Session 4
15:45~17:00	A Survey on Residual Network Evolution 조선대학교 / Abol Basher, Abu Naser Rashid Reza, Samsuddin Ahmed, Ho Yub Jung	무선 공유기 환경설정 트랜잭션 분석을 통한 안전한 무선 공유기 환경설정 자동화 시스템 연구 세종대학교, 공주대학교 / 이세한, 서창호, 박기웅
	블록체인 오픈 소스 SW 조사를 통한 블록체인 아키텍처 분석 아주대학교 / 정윤환, 길우근, 노병희	컨테이너 모니터링 툴 프로파일링을 통한 커버리지 영역 분석 세종대학교 / 김민석, 박기웅
	Efficient CNN based artistic style classifier 세종대학교 / Tanveer Hussain, Khan Muhammad, Ijaz Ul Haq, Irfan Mehmood, Sung Wook Baik	소프트맥스 함수를 이용한 통제되지 않은 환경에서의 강인한 실시간 얼굴 인식 가천대학교 / 원옥광, 사하데브 파우델, 서조드 누를라이브, 이상웅
	Ultrasonic Image Classification Based on Convolutional Neural Network 가천대학교 / Dong Yue Wang, Jun Jie Tian,Taeg Keun Whangbo	디지털 변전소를 위한 지능형 자율 네트워크 관리 기술 동향 인하대학교, 한국전기연구원 / 이왕우, 고화랑, 오휘명, 손상우, 김영선, 최성수, 노영태

	특이 문구 검출을 고려한 LSTM 기반한국어 웹 게시판 조회수 예측 고려대학교 / 김규형, 황인준	인터넷 커뮤니티 분석을 통한 이슈 판별 기법 세종대학교 / 이재유, 박나리
2018. 5. 26(토)		
논문 발표	**Poster Session 1**	**Poster Session 2**
10:00~12:00	조이스틱으로 방향 조정이 가능한 소총 움직임 제어 임베디드 시스템 구현 금오공과대학교 / Angsanto Stephen Ryan, 김명식, 전일수, 임완수	영상의 부분적 영역 추출을 이용한 영상정보 증가 기법 세종대학교 / 우현준, 김미선, 한동일
	온라인 빅데이터를 통한 소비자 선호도의 딥러닝 기반 분석기법 연구 세종대학교 / Dang Lien Minh, 민경복, 임수현, 문현준	LSTM을 이용한 자기장 기반 실내위치인식시스템 고려대학교 / 배한준, 최린
	딥 러닝 기반 사용자 편의 중심의 유실물 통합 관리 시스템의 설계 및 구현 세종대학교 / 유태우, 정하민, 유현수, 김윤욱, 안용학	TPC-H를 활용한 Goldilocks와 MySQL 성능 비교 단국대학교 / 장시형, 최원석, 전성환, 박성원, 신희성, 나연묵
	일반 데스크탑 PC 기반 풀링 기법을 활용한 딥 러닝 네트워크의 성능 향상 세종대학교 / 조주연, 김미선, 우현준, 한동일	영상 인식을 이용한 길고양이 자동급식기 세종대학교 / 이준형, 배연진, 진승언, 정순혁, 권기학, 문현준
	사진 데이터를 이용한 인공지능 사상체질 판별 시스템 가천대학교 / 최규남, 윤경목, 황보택근	A feature-level data fusion method for predicting stock price: a hybrid model based on stacked denoising autoencoders and deep neural network 세종대학교 / Sang Il Lee, Seong Joon Yoo
	oneM2M 표준기반 IoT 플랫폼을 활용한 커넥티비티 환경 및 위치정보 데이터 관리 인하대학교 / 윤준혁, 윤다빈, 박무동, 김덕환	위성 네트워크의 전송지연 최소화를 위한 물리계층 네트워크 코딩 기술 조선대학교, Iowa State University / 최우열, 김태운
	시뮬레이션을 통한 중도 절단된 두 사건의 선행성 분석 고려대학교 / 김유중, 석준희	구글 검색 엔진을 활용한 기술 키워드 관련 기업 검색 시스템 설계 세종대학교 / 이여진, 유성준, 구영현, 정원희, 장다운, 민아영
	열화상 카메라 기반의 영상 분석 및 동체 인지를 통한 가상펜스 설계 세종대학교 / 임수현, 민경복, 남준영, 문현준	VoiceLock:화자인식을 이용한 스마트 자물쇠 세종대학교 / 김도현, 이하영, 정수진, 권기학, 문현준
	랜섬웨어 탐지원리 분석을 통한 탐지 기법 분류 및 한계점 제시 세종대학교, 공주대학교 / 박건호, 최대선, 박기웅	산학협력을 위한 빅데이터 인프라 실증연구 세종대학교, 한국컴퓨팅산업협회 / 신병주, 유성준, 전석봉, 노재춘, 백성욱, 장윤, 우종필, 최준연, 이미영, 강유진, 공영지

	Container Registry를 활용한 CVE 컨테이너 기반 CTF 플랫폼 디자인 세종대학교 / 박준규, 최상훈, 박기웅	PLC 보안성을 강화하기 위한 Sanitizer 구현 단국대학교, 건국대학교 / 최광준, 박준상, 이명건, 조성제, 박민규
	사람 관련 정보를 배제한 이미지 기반 연령 및 성별 예측 모델링 아주대학교 / 조용걸, 전영승, 김보관, 한경식	환경과 활동센싱의 멀티센서를 융합한 인공지능 기반 개인화된 디지털 테라피 케어시스템 설계 아주대학교 / 이주영, 성지훈, 최선탁, 양기훈, 조위덕
	시각 주의 모델을 이용한 비디오 키 프레임 추출에 관한 연구 세종대학교 / Anvarjon Tursunov, Uyen Tran, Nam Pham, Alexandre Larzat, Soonil Kwon, Oh-Jin Kwon, Sung Wook Baik	딥러닝 기반 주식 가격 경향 예측 프레임워크 세종대학교 / 등연명, Syed Ibrahim Hassan, Duong Minh Duc, 문현준
	로그 분석을 위한 로그 템플릿 추출 기법 경북대학교 / 탁병철	블록체인을 활용한 역경매 봉사활동 크레딧 관리시스템 숭의여자대학교 / 김시우, 장명훈
	무선충전 시스템 사용 권한 검증을 위한 보안 요구사항 도출 세종대학교, 전북대학교 / 이양재, 양동민, 박기웅	스마트 미러 스토어 개발 연구 세종대학교 / 양경석, 심효빈, 임다영, 이영걸, 양효식, 주철휘
	Comparison of enhancement techniques for brain Magnetic Resonance Imaging (MRI) Chosun University / Waqas Ellahi, Bumshik Lee	멀티플랫폼을 위한 GIS 애플리케이션 기획 및 구현 세종대학교 / 서성준, 천슬별, 고정민, 남기범, 조상욱
	LSTM을 이용한 주택시장의 순환국면 예측 한국과학기술연구원 / 이관훈, 김수현, 송규원	Python-MATLAB 인터페이스를 이용한 센서데이터의 수치 연산 조선대학교 / 황용운, 이충규
	움직이는 차량에 드론 착륙 방법에 관한 연구 세종대학교 / 박준렬, 우현준, 전영민, 박성호, 김영배, 권기학	무선 센서 네트워크를 위한 반딧불이 생태모방 기반의 동기화 시뮬레이터 설계 및 이의 성능 분석 아주대학교 / 이인태, 노병희
	IoT 빅데이터 딥러닝 시스템 설계 이화여자대학교 / 김경주, 송지현, 이민수	영상에서 슬라이딩 윈도우와 딥러닝 분류 기법을 결합한 드론 인식 기법 세종대학교 / 우현준, 전영민, 박준렬, 권기학
	CNN과 학습전이를 이용한 알츠하이머병의 분류 조선대학교 / 유브라즈 굽타, 권구락	확률론적 허프 변환을 이용한 광전지 모듈 검출 가천대학교 / 크리스 헨리, 박현철, 김세원, 이상웅
	A Brief Overview of Deep Metric Learning Methods 조선대학교 / Samsuddin Ahmed, Abol Basher, Abu Naser Rashid Reza, Ho Yub Jung	A video hash method using SHA-2 for verifying video integrity Chosun University / Sarala Ghimire, Bumshik Lee
	IoT 빅데이터 처리를 위한 규칙 모델 설계 이화여자대학교 / 송지현, 김경주, 이민수	영상처리를 이용한 부표 검출 시스템 동명대학교 / 김경성, 박성은, 전수진, 유종명, 김민철, 신신재, 유선진

	웹 기반 졸업 관리 시스템의 설계 및 구현 세종대학교 / 김효준, 이승용, 고용국, 심재훈, 안용학	Analysis on the effect of patch selection for prediction of Alzheimer's disease Chosun University / Muhammad Ammar Malik, Bumshik Lee
	기계학습을 이용한 전자전 위협체의 역추정 모델링 가톨릭대학교 / 장지원, 박헌우, 노상욱	블록체인 오픈소스SW의 임베디드시스템 구현 및 응용 아주대학교 / 고광표, 노병희
	IoT 서버의 자동차 산업 분야 활용 조선대학교 / 정동일, 정지성, 이충규	게임을 이용한 창의적 코딩교육 시스템 숭의여자대학교 / 김시우
	영아 돌연사 증후군 예방 솔루션 세종대학교 / 육문수, 김태균, 박효완, 신우성, 권기학, 문현준	빅데이터 포털 사이트 온라인 시각화 방법에 관한 연구 세종대학교 / 박성호, 이미영, 이경수, 황준철, 백성욱
	Multi-Site 환경에서 전력 사용량 예측을 위한 프라이버시 보장형 패턴 시퀀스 기반 예측 인하대학교 / 권희용, 임종혁, 이문규	Review on Generative Adversarial Networks Chosun University / Abu Naser Rashid Reza, Samsuddin Ahmed, Abol Basher, Ho Yub Jung
	유사도 기반 검색 결과 개수 비례 순위 기법을 적용한 병해충 검색 시스템 설계 및 구현 세종대학교, 국립원예특작과학원 / 이건훈, 유성준, 구영현, 박철호, 윤학림, 박종한	

Poster Session 1 - (26일/토 10:00 ~ 12:00)

- 조이스틱으로 방향 조정이 가능한 소총 움직임 제어 임베디드 시스템 구현
  / 금오공과대학교 / Angsanto Stephen Ryan, 김명식, 전일수, 임완수

- 온라인 빅데이터를 통한 소비자 선호도의 딥러닝 기반 분석기법 연구
  / 세종대학교 / Dang Lien Minh, 민경복, 임수현, 문현준

- 딥 러닝 기반 사용자 편의 중심의 유실물 통합 관리 시스템의 설계 및 구현
  / 세종대학교 / 유태우, 정하민, 유현수, 김윤욱, 안용학

- 일반 데스크탑 PC 기반 풀링 기법을 활용한 딥 러닝 네트워크의 성능 향상
  / 세종대학교 / 조주연, 김미선, 우현준, 한동일

- 사진 데이터를 이용한 인공지능 사상체질 판별 시스템
  / 가천대학교 / 최규남, 윤경목, 황보택근

- oneM2M 표준기반 IoT 플랫폼을 활용한 커넥티비티 환경 및 위치정보 데이터 관리
  / 인하대학교 / 윤준혁, 윤다빈, 박무동, 김덕환

- 시뮬레이션을 통한 중도 절단된 두 사건의 선행성 분석
  / 고려대학교 / 김유중, 석준희

- 열화상 카메라 기반의 영상 분석 및 동체 인지를 통한 가상펜스 설계
  / 세종대학교 / 임수현, 민경복, 남준영, 문현준

- 랜섬웨어 탐지원리 분석을 통한 탐지 기법 분류 및 한계점 제시
  / 세종대학교, 공주대학교 / 박건호, 최대선, 박기웅

- Container Registry를 활용한 CVE 컨테이너 기반 CTF 플랫폼 디자인
  / 세종대학교 / 박준규, 최상훈, 박기웅

- 사람 관련 정보를 배제한 이미지 기반 연령 및 성별 예측 모델링
  / 아주대학교 / 조용걸, 전영승, 김보관, 한경식

- 시각 주의 모델을 이용한 비디오 키 프레임 추출에 관한 연구
  / Sejong University, Higher Studies of Engineering / Anvarjon Tursunov, Uyen Tran, Nam Pham, Alexandre Larzat, Soonil Kwon, Oh-Jin Kwon, Sung Wook Baik

- 로그 분석을 위한 로그 템플릿 추출 기법
  / 경북대학교 / 탁병철

- 무선충전 시스템 사용 권한 검증을 위한 보안 요구사항 도출
  / 세종대학교, 전북대학교 / 이양재, 양동민, 박기웅

- Comparison of enhancement techniques for brain Magnetic Resonance Imaging (MRI)
  / Chosun University / Waqas Ellahi, Bumshik Lee

- LSTM을 이용한 주택시장의 순환국면 예측
  / 한국과학기술연구원 / 이관훈, 김수현, 송규원

- 움직이는 차량에 드론 착륙 방법에 관한 연구
  / 세종대학교 / 박준렬, 우현준, 전영민, 박성호, 김영배, 권기학

- IoT 빅데이터 딥러닝 시스템 설계
  / 이화여자대학교 / 김경주, 송지현, 이민수

- CNN과 학습전이를 이용한 알츠하이머병의 분류
  / 조선대학교 / 유브라즈 굽타, 권구락

- A Brief Overview of Deep Metric Learning Methods
  / 조선대학교 / Samsuddin Ahmed, Abol Basher, Abu Naser Rashid Reza, Ho Yub Jung

- IoT 빅데이터 처리를 위한 규칙 모델 설계
  / 이화여자대학교 / 송지현, 김경주, 이민수

- 웹 기반 졸업 관리 시스템의 설계 및 구현
  / 세종대학교 / 김효준, 이승용, 고용국, 심재훈, 안용학

- 기계학습을 이용한 전자전 위협체의 역추정 모델링
  / 가톨릭대학교 / 장지원, 박헌우, 노상욱

- IoT 서버의 자동차 산업 분야 활용
  / 조선대학교 / 정동일, 정지성, 이충규

- 영아 돌연사 증후군 예방 솔루션
  / 세종대학교 / 육문수, 김태균, 박효완, 신우성, 권기학, 문현준

- Multi-Site 환경에서 전력 사용량 예측을 위한 프라이버시 보장형 패턴 시퀀스 기반 예측 / 인하대학교 / 권희용, 임종혁, 이문규

- 유사도 기반 검색 결과 개수 비례 순위 기법을 적용한 병해충 검색 시스템 설계 및 구현 / 세종대학교, 국립원예특작과학원 / 이건훈, 유성준, 구영현, 박철호, 윤학림, 박종한

랜섬웨어 탐지원리 분석을 통한 탐지 기법 분류 및 한계점 제시

Classification and Limitations of Ransomware Detection Through Detection Principle Analysis

박건호[1], 최대선*, 박기웅†

Keon-Ho Park, Daeseon Choi, and Ki-Woong Park

세종대학교 시스템보안연구실[1], 공주대학교 의료정보학과*, 세종대학교 정보보호학과†

imguno0629@naver.com, sunchoi@kongju.ac.kr, woongbak@sejong.ac.kr

요 약

랜섬웨어는 시스템의 파일을 암호화하고 몸값을 요구하는 악성코드의 일종으로 몸값을 지불하는 것 이외의 방법으로 시스템을 복구하는 것은 난이도가 상당히 높다. 랜섬웨어에 감염된 시스템을 복구하는 난이도가 높은 만큼 감염을 예방 및 차단하기 위해 효과적인 랜섬웨어 탐지 기법의 필요성이 대두된다. 본 논문에서는 랜섬웨어의 감염 과정을 나열하고, 랜섬웨어 감염 과정 도중 감염 사실을 실시간으로 탐지하는 기법의 원리에 대하여 분석한 뒤 분류한다. 이를 바탕으로 기존 랜섬웨어 탐지 기법의 한계점을 제시하고 실제 사용자 환경에서 랜섬웨어를 효과적으로 탐지하기 위하여 기존 랜섬웨어 탐지 기법들이 극복해야할 과제들을 도출한다.

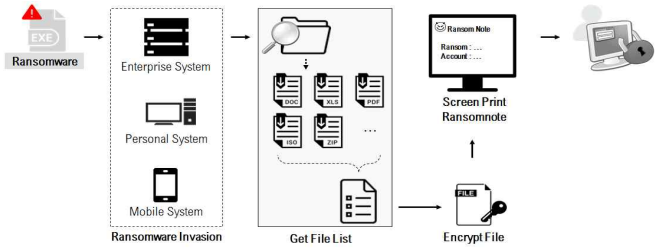
1. 서론

우리가 흔히 말하는 랜섬웨어(Ransomware)는 시스템의 파일을 특정한 암호키로 암호화하고 암호화된 파일을 인질로 삼아 복구(복호화)에 필요한 키를 제공하는 조건으로 몸값을 요구하는 크립토 랜섬웨어(Crypto-Ransomware)이다. 랜섬웨어 감염은 대체적으로 (그림 1)과 같이 진행된다. 먼저, 랜섬웨어는 시스템, 브라우저의 취약점 혹은 메일의 첨부파일을 통한 악성코드 침입과 같은 방법 등을 사용하여 시스템에 침입한다. 두 번째로, 시스템의 파일 및 디렉터리를 스캔하여 감염시킬 대상 파일 선정하고 이 파일에 대한 리스트를 생성한다. 그 다음, 생성한 파일 리스트의 파일들을 암호화하고 파일 리스트의 파일이 모두 암호화가 되면, 랜섬웨어에 감염되었다는 메시지와 함께 암호화된 파일을 복구하기 위해 지불할 금전적인 대가인 몸값과 송금할 계좌 등을 담은 랜섬노트(Ransomnote)를 화면에 출력한다. 일부 랜섬웨어는 위의 감염 과정과 상이한 특징을 가지는 경우가 있지만 대체적으로 위의 과정을 따라 랜섬웨어 감염이 진행된다.

본 논문에서는 랜섬웨어로부터 시스템을 보호하기 위한 랜섬웨어 탐지 기법을 랜섬웨어 탐지원리 분석을 통해 분류하고 이에 대한 한계점을 제시한다. 본 논문의 구성은 다음과 같다. 2장에서는 랜섬웨어 탐지 기법의 필요성에 대해 설명하고, 3장에서는 랜섬웨어 탐지 기법을 탐지원리 분석을 통해 분류하고 이에 대한 한계점을 제시한다. 4장에서는 3장의 내용을 바탕으로 결론을 제시한다.

2. 랜섬웨어 탐지 기법 필요성

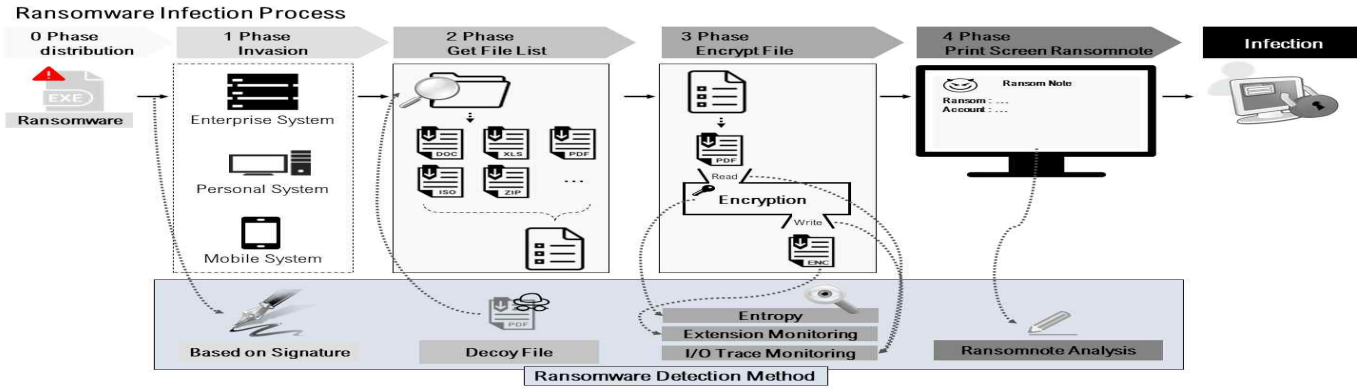
랜섬웨어는 다른 악성코드와 다르게 몸값을 받기 위해 감염 여부를 사용자에 알린다. 시스템 내 은닉하여 지속적인 악성 행위를 하는 악성코드와 비교하였을 때 랜섬웨어는 감염되었다는 사실을 확실히 알 수 있기 때문에 감염 여부를 파악한 후 시스템을 복구할 수 있다면 공격에 대한 피해는 사라지게 된다.



(그림 1) Ransomware Infection Process

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

이 논문은 한국연구재단 지원사업 2016R1A4A1011761 및 2017R1C1B2003957의 연구수행 결과물임



(그림 2) Mapping between Ransomware Infection Process and Detection Method

하지만 시스템이 랜섬웨어에 감염된 후 암호화된 파일에 대한 몸값 지불 없이 복구하는 것은 상당히 어려운 과제에 속한다. 전통적인 보안 영역의 연구 분야인 “암호 기술”이 랜섬웨어의 공격 기술에 포함되기 때문에 암호 기술의 발전이 랜섬웨어 공격 기술의 발달로 이어지는 아이러니한 상황이 발생한다. 암호 기술은 암호문에 대한 복호화에 필요한 키의 정보 없이 암호문을 복호화하는 것이 불가능에 가깝도록 높은 강도를 가지는 방향으로 연구가 진행되고 있다. 최신 암호 기술을 사용하는 랜섬웨어에 감염되어 몸값을 지불하지 않기 위해 암호화된 시스템을 복호화 키의 정보 없이 원상태로 복구하는 것은 최신 암호 기술에 대한 취약점을 발견하는 것을 뜻하며 현재 기술 수준으로 불가능에 가까운 일이다. 또한 사전에 저장시켜놓은 백업 데이터를 이용하여 몸값을 지불하지 않고 감염된 시스템에 대해 복구하는 행위를 불가능하게 하기 위하여 시스템의 파일 뿐만 아니라 백업 데이터까지 암호화하는 랜섬웨어가 등장하였다.

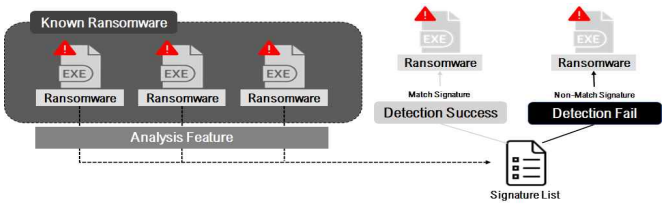
랜섬웨어 공격의 고도화로 인해 시스템에서 사전 예방 또는 탐지를 통한 랜섬웨어 차단을 실패하여 시스템이 감염되었을 경우, 시스템의 파일을 복구하기 위해서는 공격자가 요구하는 몸값의 지불을 피할 수 없게 되었다. 희생자가 몸값을 지불하게 된다면 희생자는 랜섬웨어에 감염된 시스템을 복구하고 공격자는 몸값을 지불받는다는 의미 외에도 다른 공격자에게 랜섬웨어가 가치 있는 공격이라는 의미를 전달하여 새로운 랜섬웨어 공격의 등장을 유도할 수 있다. 따라서 이런 악순환을 반복하지 않기 위해 랜섬웨어 탐지 기술이 중요하다.

3. 랜섬웨어 탐지 원리 분석을 통한 탐지기법 분류 및 한계점 제시

본 장에서는 기존 랜섬웨어 탐지에 관한 연구에서 제시한 랜섬웨어 탐지 기법을 랜섬웨어 감염 과정과 연결하여 분류하여 탐지원리 분석을 통해 탐지 기법을 분류하고 이에 대한 한계점을 제시한다. 랜섬웨어 감염 5단계 과정 중 랜섬웨어 배포와 시스템 침입을 한 과정으로 보고, 각 4단계에서 랜섬웨어의 감염 과정과 탐지 기법을 (그림 2)와 같이 연결한다.

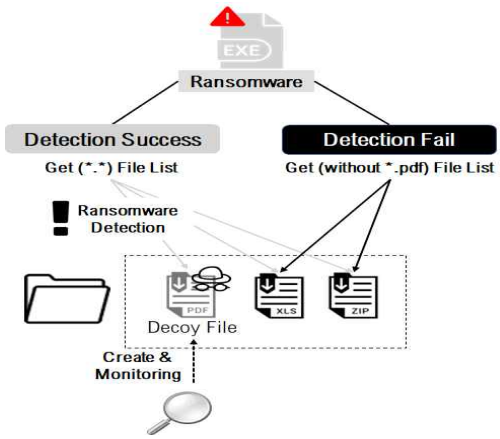
3.1 배포-침입 단계

배포-침입 단계에서는 시그니처 기반 탐지 기법[4][7]을 사용하여 랜섬웨어를 탐지할 수 있다. 시그니처 기반 탐지 기법은 (그림 3)과 같이 기존의 랜섬웨어의 특징을 분석하여 정상 소프트웨어와 비교되는 특징을 시그니처로 만들어 이를 기반으로 랜섬웨어를 탐지한다. 특징에는 문자열, API 호출, 서명값 등이 있으며 이를 기반으로 시그니처 목록을 만들어 관리한다. 시그니처 기반 탐지 기법은 시그니처가 생성된 랜섬웨어(알려진 랜섬웨어)나 그와 비슷한 특징을 가진 랜섬웨어를 탐지하는 데 좋은 성능을 가지지만, 시그니처가 없는 새로운 형태의 랜섬웨어를 탐지하기에 어렵다는 한계점이 있다. 또한 시그니처를 항상 최신 상태로 업데이트해야 하는 한계점이 있어, 시그니처 양이 많아진다면 다수의 시그니처 데이터를 관리하는 데 어려움을 가진다.



(그림 3) Ransomware Detection Based on Signature

3.2 파일 리스트 생성 단계



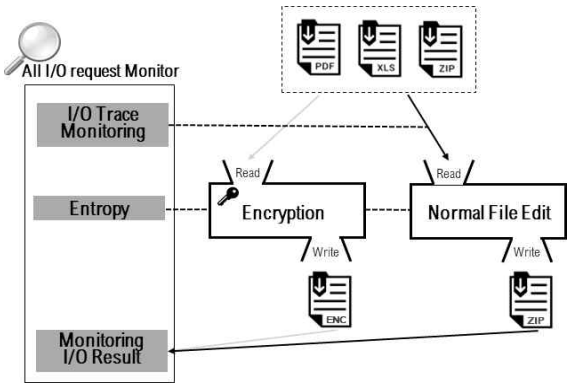
(그림 4) Detection Method using Decoy File

파일 리스트 생성 단계의 특징을 이용한 탐지 기법은 (그림 4)과 같은 미끼파일을 이용한 기법[2]이 있다. 미끼파일을 사용한 기법은 임의의 폴더와 파일을 생성하고 감염 대상 파일을 선정하는 파일 리스트 획득 단계에서는 해당 미끼파일이 랜섬웨어 감염 대상으로 선정되게끔 하는 기법이다. 해당 기법은 시스템 전체를 모니터링하지 않고, 임의로 생성한 미끼 파일만 모니터링하면 되어, 모니터링에 대한 오버헤드는 적다. 하지만 랜섬웨어는 특정한 확장자나 파일 사이즈, 파일 경로 등을 감염 대상 제한하여 선정하는 경우가 있어, 미끼 파일이 감염 대상으로 선정되지 않을 가능성이 있고, 또한 모든 경우의 수를 고려하여 미끼 파일을 생성하게 된다면 시스템 저장 공간의 낭비로 이어질 수 있다는 한계점이 있다.

3.3 암호화 단계

암호화 단계에서는 (그림 5)와 같이 파일 입/출력 추적 모니터링, 엔트로피 측정, 파일 입/출력 결과 모니터링을 이용한 탐지 기법을 적용할 수 있다.

파일 입/출력 모니터링 기법[1][3]은 랜섬웨어 파일 입/출력 형태를 사전에 정의하고 시스템의 파일 입/출력을 모니터링하여 랜섬웨어를 탐지한다. 가장 큰 예로 랜섬웨어는 합법적인 파일 입/출력과 비교되게 삭제 과정이 다수 발생한다는 특징이 있다. 랜섬웨어와 가장 비슷한 합법적인 시스템 사용인 압축과 비교하여, 압축 후 기존 파일을 유지하는 것과 달리 랜섬웨어는 암호화 후 기존 파일을 삭제한다. 해당 방법은 일종의 시그니처 기반 탐지 기법으로 사전에 정의된 파일 입/출력과 다를 경우 탐지가 어렵다는 한계점이 있다.



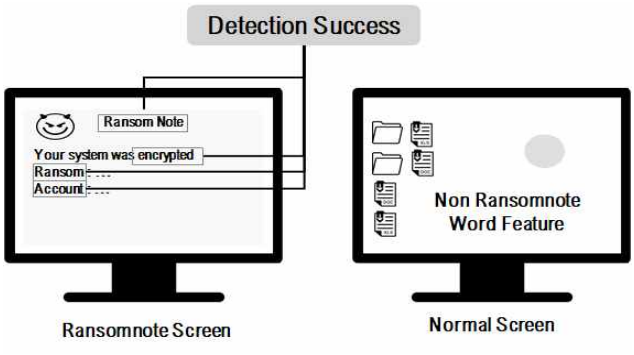
(그림 5) Detection Method in Encrypt File Phase

엔트로피를 이용한 탐지 기법[1][3]은 암호화 과정에서 발생하는 암호학 특징을 이용한 기법이다. 암호화 과정에서 바이트 단위 바이너리 값은 0x00부터 0xFF까지 고른 분포를 가지게 변형된다. 이런 특성을 이용하여 정보의 불확실성을 나타내는 엔트로피를 이용한 방법은 파일의 암호화를 판단하기에 적합한 방법이다. 하지만 한 파일의 엔트로피를 측정하기 위해서는 파일 전체를 읽어야 하기 때문에, 시스템에서 발생하는 모든 파일 입/출력 모니터링하고 엔트로피를 연산하는 과정에서 발생하는 오버헤드로 시스템의 가용성을 저해할 수 있다.

파일의 입/출력 결과 모니터링을 이용한 탐지 기법은 $UsnJrnl을 이용한 탐지 기법[5]과 확장자를 이용한 탐지 기법[6]이 있다. $UsnJrnl을 이용한 탐지 기법은 NTFS 파일 시스템에서 특정한 파일에 대한 조작이 발생하였을 경우, 이에 대한 데이터를 기록하는 $UsnJrnl을 이용하여 해당 부분을 지속적으로 모니터링하여 랜섬웨어를 탐지한다. 확장자를 이용한 탐지 기법은 랜섬웨어가 파일을 암호화하고 암호화된 파일을 생성 또는 덮어쓰기 한 후에 생성하는 파일의 확장자를 모니터링하는 방법이다. 해당 기법은 알려진 랜섬웨어가 암호화된 파일을 생성할 때 사용하는 확장자에 대한 리스트를 생성하고 시스템 파일의 확장자를 주기적으로 모니터링한다. 모니터링 과정에서 랜섬웨어 확장자 리스트에 존재하는 확장자의 파일이 생성될 시 랜섬웨어에 감염되었다고 판단한다. 확장자를 이용한 랜섬웨어 탐지 기법의 한계점은 기존의 모든 랜섬웨어에서 사용된 확장자를 지속적으로 업데이트해야하는 문제와 새로운 랜섬웨어 공격에서 기존에 없던 확장자를 사용하는 경우 탐지를 하지 못한다는 한계점이 있다.

암호화 단계에서 사용하는 랜섬웨어 탐지 기법은

시스템 전체의 파일 입/출력을 모니터링하여야 한다.



(그림 6) Detection Scheme through Ransomnote Analyze

하지만 시스템 전체를 모니터링하는 것은 시스템의 가용성을 저해하는 요소이며, 이런 한계점 때문에 실제 사용자 환경에서 해당 기법을 적용하기 위해서 모니터링 및 연산 과정의 오버헤드를 줄이는 것이 가장 큰 과제이다.

3.4 랜섬노트 출력 단계

랜섬노트 출력 단계에서는 랜섬노트 분석을 통한 랜섬웨어 탐지 기법[1]을 사용한다. [그림 6]과 같이 랜섬노트에는 랜섬웨어 감염 여부(“Encrypt”), 몸값(“Ransom”), 계좌(“Account”) 등의 가진 문자열이 포함되어 있으며, 바탕화면을 주기적으로 모니터링하여 해당 문자열이 등장할 경우 랜섬웨어에 감염되었다고 판단한다. 해당 기법은 랜섬웨어 감염 여부를 판단하기에 가장 좋은 기법이지만, 실제 사용자 환경에서 랜섬노트가 출력되었다는 것은 곧 시스템에 대한 감염이 완료되었다는 것을 의미하기 때문에 실제 사용자 환경의 랜섬웨어 탐지를 위해 사용하기에는 부적합하다.

4. 결론

최근 빅데이터 기술의 상용화로 데이터에 대한 가치가 증가하였다. 또한 비트코인과 같은 암호화폐(가상화폐)의 등장으로 추적을 피하면서 몸값을 지불받을 수 있는 방법이 나타났다. 이에 따라 새로운 형태의 랜섬웨어가 계속적으로 등장할 것으로 예상되며, 이를 탐지하기 위한 탐지 기법에 대한 연구가 필요하다.

이에 본 논문에서는 기존 랜섬웨어 탐지 기법을 랜섬웨어 감염 과정과 연결하여 탐지원리 분석을 통해 분류하고 한계점을 제시하였다. 시그니처 기반 랜섬웨어 탐지 기법의 경우 새로운 특징(시그니처)을 가진 랜섬웨어 탐지가 어렵다는 한계점이 있었으며, 미끼파일을 이용한 탐지 기법은 미끼파일을 감염 대상으로 포함하지 않을 경우 탐지가 불가능하다는 한계점이 있었다. 또한 암호화 단계에서 사용하는 랜섬웨어 탐지 기법은 시스템 전체를 모니터링하고 연산을 해야 하기 때문에 시스템의 가용성을 저해할 수 있는 요소가 존재한다는 한계점이 있었으며, 랜섬노트 출력 단계의 탐지 기법은 이미 감염이 완료된 상태에서 사용하는 탐지 기법이므로 실제 사용자 환경에서 사용하기에는 적합하지 않다는 한계점이 있다.

랜섬웨어의 목적은 파일을 암호화하고 몸값을 요구하는 것으로 단순화 할 수 있다. 모든 형태의 랜섬웨어는 암호화 과정이 필수적으로 포함된다. 기존 암호화 단계의 랜섬웨어 탐지 기법은 모니터링과 연산의 오버헤드로 인해 실제 사용자 환경에서 적용하기에 한계가 있다. 랜섬웨어에 특화된 탐지를 위해 암호화 단계의 탐지 기법에 대한 한계점을 극복하는 연구가 필요하다. 향후 암호화 단계의 탐지 기법의 한계점을 극복하는 모니터링 및 연산에 대한 오버헤드를 줄이는 연구를 진행할 계획이다.

참고문헌

[1] Kharraz, Amin, et al. "UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware." USENIX Security Symposium. 2016.

[2] Moore, Chris. "Detecting ransomware with honeypot techniques." Cybersecurity and Cyberforensics Conference (CCC), 2016. IEEE, 2016.

[3] Scaife, Nolen, et al. "Cryptolock (and drop it): stopping ransomware attacks on user data." Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on. IEEE, 2016.

[4] Sgandurra, Daniele, et al. "Automated dynamic analysis of ransomware: Benefits, limitations and use for detection." arXiv preprint arXiv:1609.03020 (2016).

[5] 김형규, et al. "$UsnJrnl 기반 랜섬웨어 암호화 패턴 유형화 및 탐지 모델." 디지털포렌식연구 11.3 (2017): 71-80.

[6] 윤정무, and 류재철. "MacOS 에서 파일확장자 관리를 통한 랜섬웨어 탐지 및 차단 방법." 정보보호학회논문지 27.2 (2017): 251-258.

[7] 이규빈, 옥정윤, and 임을규. "랜섬웨어 동적 분석을 위한 시그니처 추출 및 선정 방법." 정보과학회 컴퓨팅의 실제 논문지 24.2 (2018): 99-104.