에너지 기반시설 대상 랜섬웨어 공격 보안대책

주동규*, 뜩*, 이용준**, 양수미*
*극동대학교 해킹보안학과, **극동대학교 대학원 인공지능보안학과, ***극동대학교 친환경에너지학과
201763031@kdu.ac.kr, phamduc280897@gmail.com, 2020032@kdu.ac.kr,
esther4853@kdu.ac.kr

Security Countermeasures for Ransomware Attacks on Energy Infrastructure

Dong-Kyu Joo*, Pham Ngoc Duc*, Yong-Joon Lee**, Su-Mi Yang***
*Dept. of Hacking Security Far East University
**Dept. of AI Security Graduate School Far East University
***Dept. of Green Energy Engineering Far East University

요 약

최근 에너지 기반시설을 인질로 하여 산업 핵심기술을 탈취하려는 사이버공격이 지속 발생하고 있다. 특히 랜섬웨어는 에너지 기반시설의 컴퓨터에 침입하여 산업 기밀정보에 대해 무단으로 암호화하기 때문에 ICT 기술이 에너지 환경에 융합이 가속화 되면서 문서, 설계도면 등의 산업기밀 정보 중요성이 높아짐에 따라 그 피해가 증가하고 있다. 본 논문에서는 에너지 기반시설을 대상으로 하는 랜섬웨어에 대한 동향과 보안대책을 기술한다.

1. 서론

ICT 기술이 발전해가면서 산업기밀의 중요도는 계속 높아지고 있으며 사이버공격으로 인한 피해가 증가하고 있다. 특히 이메일 해킹을 주 공격방식이던 초기의 랜섬웨어와는 달리 최근에는 SNS, 메시지를 통해서도 전파되면서 피해가 증가하고 있다. 최근 에너지 기반시설에 대한 랜섬웨어 공격이 증가함에 따라서 랜섬웨어의 동향 및 보안대책을 제시한다.

2. 국내외 랜섬웨어 공격 사례

2.2 해외 사례

한국인터넷진흥원에서 발표한 2022년 1분기 랜섬웨어 동향 보고서[2]에 따르면, 해외 랜섬웨어로 인한 피해는 증가하고 있는데 22년 1월에서 3월까지 총7번의 피해사례가 발생하였다. 22년 1월에 두 차례의 피해사례가 발생했는데 대만의 전자제품 제조기업 Delta Electronics가 랜섬웨어에 감염되었고, 프랑스 법무부가 랜섬웨어 감염되는 사건이었다. 22년 2월에 영국의 식료품 생산기업인 KP Snacks, 스위스의 항공 서비스 기업인 Swissport International, 일본의 스포츠용품 제조기업인 Mizuno, 미국의 타이어 제조기업인 Bridgestone Americas가 랜섬웨어로 인해 피해를 입게 되었다. 2년 3월에는 일본의 자동차 부품 제조업체인 DENSO가 공격당한 사례가 있었다.

2.1 국내 사례

한국인터넷진흥원에서 발표한 랜섬웨어 최신 동향 분석 및 시사점[1]에 따르면, 20년 11월에는 백화점, 아울렛 등 이랜드그룹의 주요 매장이 클롭(Clop) 랜섬웨어 조직의 공격으로 인해 영업이 중단되는 사태가 발생했다. 랜섬웨어 감염 시스템이 일부 매장의 포스 단말기 등과 연동되어, 백화점과 아울렛의 매장 50여개 중 23개의 운영에 영향을 미치게 되었다. 21년 5월에는 부품 제조기업의 서버 및 직원 PC의 데이터를 암호화, 임직원의 개인정보 및 해외사업 데이터를 다크웹을 통해 유출, DDoS 공격으로 홈페이지를 마비시키는 등 총 세차례에 걸쳐 공격이 진행되었다. 21년 5월 국내 성형외과 의원이 랜섬웨어 공격을 받아, 병원 고객 연락처를 탈취한 공격자는 고객들과 직업 연락을 통해 취한 정황이 파악되는 등 2차 피해가 발생하였다.

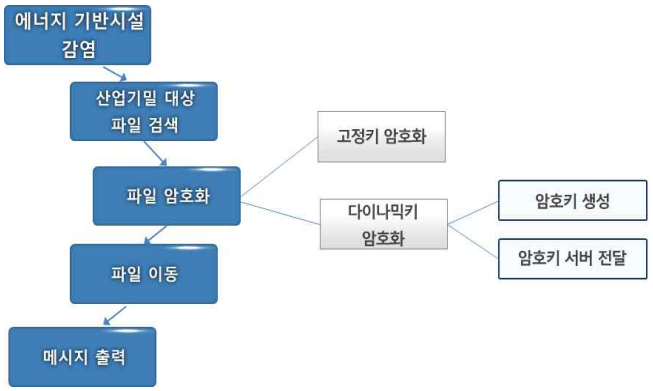
3. 랜섬웨어 공격방식 분석

3.1 랜섬웨어의 개념

랜섬웨어란 몸값(Ransom)과 소프트웨어(Software)의 합성어로 컴퓨터를 감염시켜서 접근이나 데이터의 사용을 제한하고 몸값을 요구하는 일종의 악성 소프트웨어이다. 랜섬웨어는 암호화 알고리즘을 이용하여 작동하는데, 이로 인해 파일 데이터를 암호화하여 사용할 수 없게 만든다. 파일을 암호화 시킨 후, 감염된 기기의 바탕화면에 협박성 문구를 띄우는 방식으로 피해자에게 가상화폐 등의 금전적인 요구를 하며 갈취하는 방식이 일반적인 랜섬웨어 공격 방식이다.

3.2 랜섬웨어의 작동 원리

랜섬웨어의 작동 원리나 특징은 랜섬웨어의 종류에 따라 다른 형태를 보일 수 있지만, 일반적으로는 [그림 1]과 같은 흐름을 따라 이루어진다[3].



[그림 1] 랜섬웨어 공격 흐름

랜섬웨어는 에너지 기반시설 기기를 감염시킨 후, 가장 첫 번째로 수행하는 단계는 대상 파일검색이다. 이 단계에서는 공격 대상이 될만한 파일을 검색해내는 작업을 수행한다. 두 번째 단계인 파일 암호화 단계는 전 단계에서 공격 대상으로 삼은 파일들을 암호화시키는 작업을 수행한다. 파일의 암호화시키는 방법으로는 고정키 암호화와 다이나믹키 암호화가 있다. 고정키 암호화는 고정된 단일키로 수행되는 암호화로 가장 단순한 방식을 보인다. 다이나믹키 암호화는 시스템의 환경이나, 파일명, 속성 등을 고려해 개별 암호화키를 만들어내 사용하는 방식이다. 해킹그룹이 비용을 요구하고 데이터를 정상적으로 복원해주게 된다. 파일을 복원하기 위한 암호화키 목록 파일을 생성하게 되는데 이 경우 암호화키를 해킹그룹의 서버로 전송하여 관리한다. 세 번째 단계에서 공격자는 암호화된 파일을 바탕화면으로 이동시켜 피해자가 파일들이 정상적으로 열리지 않는다는 사실을 확인하하여 공격당했다는 사실을 인지하게 만든다. 마지막 단계에서 산업기밀 자료의 복원을 원한다면 금전적인 비용을 지불하라는 협박성 메시지를 출력한다.

4. 랜섬웨어 유형별 특징 분석

한국인터넷진흥원에서 발표한 2022년 1분기 랜섬웨어 동향 보고서[2]에 따르면, 2022년 1분기에는 70종의 랜섬웨어에 의한 공격이 발생하였고, 이 중 50종은 기존 랜섬웨어의 변종, 나머지 20종은 새로운 형태의 랜섬웨어이다. 이 보고서에서는 1분기에 발견된 신종·변종 랜섬웨어 중 3종을 선정하고 분석하였는데, 첫 번째는 BlackCat, 두 번째는 DeadBolt, 마지막은 Sugar이다.

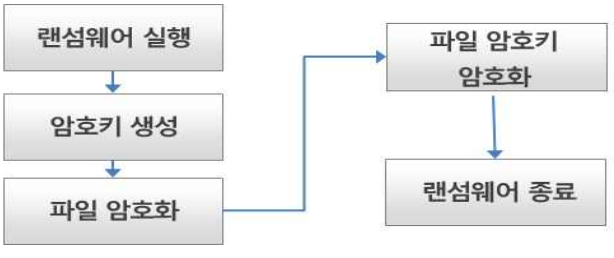
4.1 BlackCat 랜섬웨어

독일의 연방정보기술보안청(BSI) 보고서[4]에 따르면 BalckCat 랜섬웨어 그룹은 독일 북부지역에서 수백 개의 주유소를 운영 중인 독일의 석유기업 2개를 공격했다. 이 외에도 BlackCat 랜섬웨어는 이탈리아 패션 브랜드인 Moncler[5], 스위스 항공 서비스 기업인 Swissport[6] 등 다양한 기업을 대상으로 공격하였다. BalckCat 랜섬웨어는 C, Java, Python과 같은 프로그래머가 일반적으로 사용하는 언어들이 아닌 Rust라는 언어를 사용하여 만들어졌고[7], <표 1>과 같이 4가지 암호화 모드로 설정 가능하다.

<표 1> BlackCat 랜섬웨어 암호화 모드

암호모드	랜섬웨어 방식
Full	전체 파일 암호화
Fast	파일 첫 부분에서 특정 크기만 암호화 (MB단위)
DotPattern	파일을 특정 크기로 몇 회 반복하여 암호화 (MB 단위)
Auto	파일의 유형과 크기에 따라 파일 암호화에 가장 적합한 방법 선택

파일 암호화 시에는 AES 블록 암호 또는 ChaCha20 스트림 암호를 사용한다. Auto 모드에서는 랜섬웨어 실행파일이 AES 블록 암호의 암·복호화에 대해 하드웨어 가속 지원 여부를 검사하는데, 지원하는 경우는 AES 블록 암호를, 그렇지 않은 경우엔 ChaCha20 스트림 암호를 사용한다. 사용한 암호키는 RSA-2048 공개키 암호로 암호화된다.



[그림 2] BlackCat 랜섬웨어 암호화 과정

BlackCat 랜섬웨어는 파일을 암호화할 때 방해되는 프로세스와 윈도우 서비스를 종료하는데, 주로 백업 소프트웨어, Veeam, Microsoft Exchange, 데이터베이스 서버, 메일 클라이언트, 오피스 프로그램 등과 관련된 프로세스들이 종료된다.

4.2 DeadBolt 랜섬웨어

2022년 1월, DeadBolt 랜섬웨어 공격이 가장 활발했을 때 인터넷에 있는 13만 개의 QNAP 장비 중 4,988개의 장비가 DeadBolt 랜섬웨어에 감염되었다[8]. DeadBolt 랜섬웨어는 '/mnt/Had_ROOT/' 폴더에 악성 행위를 수행하는 실행파일을 생성한다. 초기에는 파일 암호화 시에 사용하는 암호키를 포함해 다양한 데이터를 가진 구성 파일 형태로 실행된다. DeadBolt 랜섬웨어가 파일을 암호화시키기 위해 AES-128 블록 암호를 사용하는데, 파일 암호화에 사용되는 초기 명령어는 '[random_file_name] -e [config]/share' 이다. 여기서 'share' 폴더는 QNAP NAS 장비가 사용자의 파일을 저장하는 폴더이다.

4.3 Sugar 랜섬웨어

2022년 2월 미국의 다목적 대형 도소매 기업인 Wlamart가 Sugar 랜섬웨어에 의해 공격당했다. Sugar 랜섬웨어는 Delphi 프로그래밍 언어를 사용하여 개발된 것으로 추정하며, 다른 RaaS보다도 더 많은 옵션을 제공한다[9]. Sugar 랜섬웨어는 7가지 다른 방법으로 생성한 데이터를 결합한 값의 MD5 해시 값을 암호키로 사용하는데, 해당 암호키의 크기는 128Bytes이며 값은 PC마다 다르다.

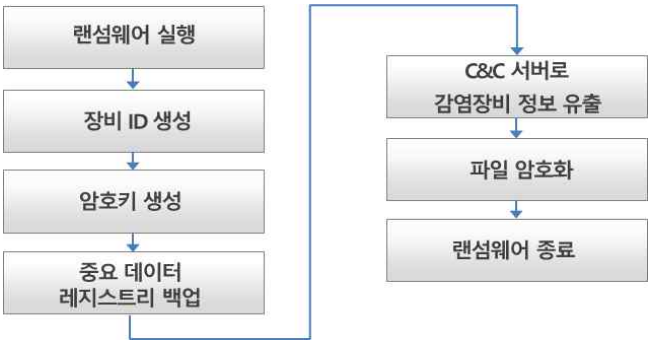
<표 2> 암호키 생성 시 사용하는 데이터

데이터명	데이터 정의
ID	감염된 장비의 12자리 ID
TICK	시스템 Tick Count 값
RAN	난수
GEN	암호학적 난수
COUNT	성능 카운터와 현재 시간을 더한 값
CURSOR	현재 마우스 커서의 X축과 Y축
TIME	현재 시간

Sugar 랜섬웨어는 파일 암호화 시 아래의 RC6, SCOP, Salsa20 암호 알고리즘 중 선택해서 사용한다.

- RC6 : 생성된 암호키의 상위 48 Bytes 크기를 암호키로 사용
- SCOP : 생성된 암호키의 상위 48 Bytes 크기를 암호키로 사용
- Salsa20 : 생성된 암호키의 상위 40Bytes 크기를 암호키로 사용

파일 암호화에 사용된 암호키는 이후 RSA나 ElGamal 공개키 암호로 암호화된다. Sugar 랜섬웨어의 감염과정은 다음과 같다[10].



[그림 3] Sugar 랜섬웨어 감염 과정

BlackCat, DeadBolt, Sugar 랜섬웨어들의 특징은 다음과 같다.

<표 3> 주요 랜섬웨어 특징 비교

랜섬웨어 유형	주요 특징
BlackCat	AES 블록 암호 또는 ChaCha20 스트림 암호 사용, 사용한 암호키를 RSA-2048 공개키 암호로 암호화
DeadBolt	AES-128 블록 암호 사용
Sugar	생성한 데이터를 결합한 값의 MD5 해시 값을 암호키로 사용

5. 대책방안

랜섬웨어로 인해 암호화된 파일은 백업해놓은 파일이 없다면 암호화키 없이는 현재로서는 완벽히 복구하기가 힘들다. 그렇기에 랜섬웨어에 대한 대응방안으로는 사후 대처가 아닌 사전에 예방하는 방향으로 많은 연구가 진행되어왔다. 랜섬웨어에 대한 대책방안은 다음과 같다.

5.1 중요 산업기밀 파일 사전 백업

현재까지 랜섬웨어에 대응하기 위해 많은 연구가 이루어졌지만 그럼에도 랜섬웨어에 의해 암호화된 파일을 완벽하게 복호화해내는 방법은 없다. 따라서 랜섬웨어에 감염되기 전에 산업기밀 파일은 미리 백업해두고 감염된 이후 백업해둔 파일을 이용해 복원해야 한다.

5.2 소프트웨어나 및 OS 최신 업데이트

랜섬웨어는 기본적으로 사용자 PC에 설치되어 있는 소프트웨어, OS의 취약점을 이용한 공격이다. 소프트웨어, OS는 모두 노출된 취약점에 대해 패치를 진행하기 때문에 항상 최신 업데이트를 유지하는 것이 랜섬웨어에 감염될 가능성을 줄여준다.

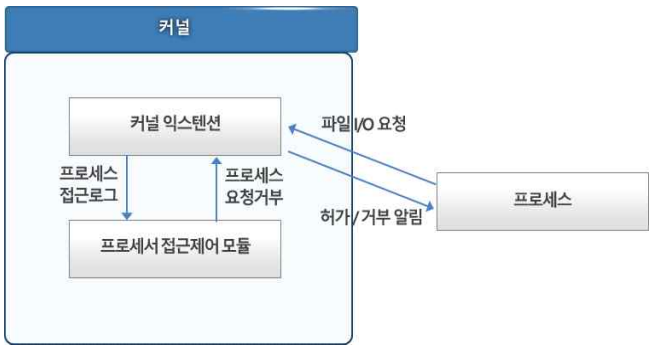
5.3 백신 소프트웨어 설치

감염 파일의 다운로드 및 실행과 함께 시작되는 랜섬웨어

공격을 방지하기 위한 방법으로는 백신 소프트웨어 설치를 제시할 수 있다. 백신 소프트웨어는 신뢰하지 못하는 사이트에서 다운받은 파일인 경우 악성 파일을 삭제해주는 조치를 취한다. 주기적으로 PC 악성코드 검사를 수행하는 것도 중요하다.

5.4 커널을 이용한 파일 I/O 모니터링 및 제어 모델

커널을 이용한 파일 I/O 모니터링 및 제어 모델[11]은 프로세스의 행동을 탐지하고 제어하기 위해 커널의 기능을 이용한다. 랜섬웨어는 파일을 암호화하기 위해 프로세스를 생성해 파일을 탐색하고, 변경하게 된다. 이러한 파일의 변경 행위는 커널에서 탐지와 제어가 가능하며, 이는 MS사의 윈도우 제품군에서는 드라이버라는 개념으로, 애플사의 OSX 제품군에서는 커널 익스텐션이라는 개념으로 제공된다. 프로세스로부터 파일 처리의 요청이 발생했을 경우, 커널에서 이를 탐지하여 프로세스의 파일 접근정보를 모두 제어 모듈로 전달하게 된다. 특정한 pid(process identifier, 프로세스 인식자)값을 통해 각각의 프로세스를 식별할 수 있으며, 이를 이용해 특정 프로세스의 접근을 제어할 수 있다. 또한 pid와 관계없이 특정한 파일을 기준으로 파일에 접근하려하는 프로세스를 제어 할 수 있다.



[그림 4] 파일 I/O 모니터링 및 제어 모델

6. 결론

본 논문에서는 랜섬웨로 인한 국내외 공격 사례, 랜섬웨어의 공격 방식과 유형별 특징을 분석하였고, 대책 방안에 대해 기술하였다. 랜섬웨어의 기본적인 작동원리에 대해 분석해보았으며, 거기서 파생되어 여러 유형으로 나누어진 서로 다른 랜섬웨어에 대해서도 분석하였다. 신종 랜섬웨어 3종 BalckCat, DeadBolt, Sugar에 대해서도 분석하였고, 각각 기존의 랜섬웨어에서 다른 방향으로 진화하여 서로 다른 랜섬웨어로 진화하였다는 것을 알 수 있었다. 진화해가는 랜섬웨어에 대응하기 위한 방안에 대해서 조사하였는데, 랜섬웨어로 인해 암호화된 파일은 암호화키를 확보하지 못한다면 복구하기 어렵다. 랜섬웨어에 대한 대응방안으로 산업기밀 파일은 미리 백업해놓거나 소프트웨어와 OS를 항상 최신 업데이트 상태로 유지하고 백신 소프트웨어를 이용하고 랜섬웨어를 탐지하기 위한 모델인 파일 I/O 모니터링 및 제어 모델을 통해 사전 대응이 가능하다. 향후 에너지 기반시설에 대한 랜섬웨어 공격으로 인한 취약점 보완 및 대응 방안에 대한 연구가 필요할 것으로 예상된다.

참고문헌

[1] 한국인터넷진흥원, “랜섬웨어 최신 동향 분석 및 시사점”, 2021.
[2] 한국인터넷진흥원, “2022년 1분기 랜섬웨어 동향 보고서”, 2022.
[3] 조영주, 김진혁, 오지훈, 소윤정, 선아영, “랜섬웨어의 동작원리와 예방 대책”, 한국콘텐츠학회 종합학술대회 논문집, pp. 91-92, 2017.
[4] ZDNet, “https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/”
[5] SecureBlink, “https://www.secureblink.com/cyber-security-news/moncler-group-becomes-the-first-victim-of-alphv-(blackcat)-raas-following-the-data-leak”
[6] BleepingComputer, “https://www.bleepingcomputer.com/news/security/blackcat-alphv-claims-swissport-ransomware-attack-leaks-data/”
[7] cybereason, “https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware”
[8] Censys, “https://censys.io/deadbolt-ransomware-is-back/”
[9] 보안뉴스, https://www.boannews.com/media/view.asp?idx=104529
[10] Medium, “https://medium.com/s2wblog/tracking-sugarlocker-ransomware-3a3492353c49#7ee1”
[11] 윤정무, 조제경, 류재철, “파일 I/O Interval을 이용한 랜섬웨어 공격 차단 방법론”, 정보보호학회논문지, pp. 645-653, 2016.