정 보 보 호 학 회 지
제 32 권 제3호, 2022. 6

랜섬웨어 피해 저감을 위한 공격 타임라인별 대응전략 및 기술

이 슬 기*, 김 동 욱*, 이 태 우*

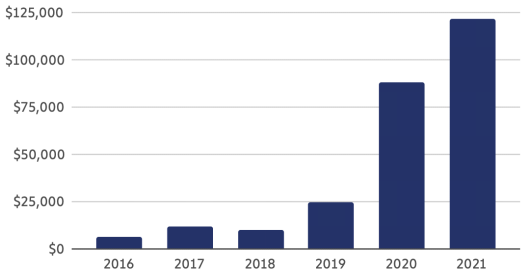
요 약

랜섬웨어 침해사고의 감염대상의 규모를 가리지 않는 특성과 폭발적인 증가세로 인해 전 세계적인 대응방안 마련의 공감대가 형성된 지 오래이다. 침해사고 분석 관점에서 랜섬웨어 사고는 기존 침해사고와 달리 랜섬웨어 악성코드가 사용되었다는 가장 큰 특징 이 외에 별다른 차이가 없다. 여타 침해사고와 동일하게 공격 도구를 생산하고 인프라를 구축하는 단계부터, 타겟 시스템으로의 최초 침투, 권한 상승, 내부 전파를 거쳐 최종적으로 랜섬웨어 악성코드가 실행되는 흐름을 보인다. 한편, 랜섬웨어 공격조직은 보다 원활한 공격을 위하여 점차 분업화, 조직화되는 동향을 보이기 때문에 공급 사슬을 차단하려는 노력도 수반되어야 한다. 본고에서는 랜섬웨어 위협을 공격 타임라인으로 나누어, 산학연관에서 어떠한 방향으로 대응 노력을 기울이고 있는지 소개한다.

Ⅰ. 서 론

랜섬웨어의 피해가 지속적으로 이어지며, 랜섬웨어를 대응하기 위한 각 계의 노력이 계속되고 있다. 오늘날 랜섬웨어는 공격조직이 대형화되어 가며 체계적으로 악성행위를 분업화하는 양상을 보인다. 보안회사 MANDIANT는 RaaS(Ransomware-as-a-Service)의 홍보 사례를 밝히며, 랜섬웨어 공격의 수익에 비례하여 협업기관 별 수익이 분배된다고 공개하였다[1].

또한, 분업화 이외에도 그림 1과 같이 평균 랜섬웨어 지불금액이 증가하는 양상을 보인다. 이 현상에 대해 Chainanalysis는 공격자들이 대규모 기관에 초점을 맞추어 공격을 수행하기 때문이라고 밝혔다. 이는 분업화를 통해 확보된 공격 효율성이 핵심 기관을 목표로 공격할 수 있게 만든 원동력이라고 추정할 수 있다.



〔그림 1〕 랜섬웨어 평균 지불액(2016-2021)〔2〕

본고에서는 위와 같은 랜섬웨어 공격의 변화에 대응하기 위하여 랜섬웨어 대응 분류를 타임라인 기준으로 나누어 각 계에서 어떠한 노력이 진행되고 있는지 공유한다. 2장에서는 랜섬웨어 사고의 발생현황 및 공격조직의 분업화를 중점으로 변화를 소개하고, 3장에서는 공격 타임라인별 대응방안과 대응현황을 공유한다.

Ⅱ. 랜섬웨어 동향

2.1. 랜섬웨어 사고 동향

과거 특정 랜섬웨어 공격조직이 사용하던 '이중 갈취' 수단이 보편화되며, 감염된 파일 뿐 아니라 고객의 신뢰를 인질로 삼아 복구비용을 요구하는 사례가 증가하고 있다. 새로운 공격 전략의 효용성이 입증되어 다른 범죄조직으로 전파되는 것처럼, 랜섬웨어 공격은 상호작용을 통해 광범위하게 확산되고 있다.

과거에 랜섬웨어는 스피어피싱 이메일 등을 통해 감염되는 단순한 공격 절차에 의해 수행되기도 하였으나, 이제는 APT 공격의 절차와 유사한 형태로도 랜섬

* 한국인터넷진흥원 (선임연구원, sglee@kisa.or.kr, 선임연구원, kimdw777@kisa.or.kr, 선임연구원, heavyrain@kisa.or.kr)

웨어 공격이 진행되고 있다.

랜섬웨어 공격조직의 핵심 목표가 금전적 이득이기 때문에, 최소한의 비용과 시간을 들여 낮은 비용을 청구할 수 있는 저비용 저임금의 중소기업 대상 공격과 대량의 자원을 활용하여 고비용을 청구할 수 있는 대기업 대상의 공격 모두 병행되고 있다. 결국 신속하게 공격 타겟을 감염시킬수록 이득을 확보할 수 있는 구조로 인해 랜섬웨어 공격은 항시 효율성을 추구하게 된다. 최종적으로 랜섬웨어 감염이 간단하게 진행되더라도 소액의 금액을 청구할 수 있으며, 나아가 기업 규모에 따라 보다 많은 금액을 청구할 수 있기 때문에 랜섬웨어로 인한 비즈니스 지속성 위협은 꾸준하게 제기되고 있다.

최근 2022년 1분기 랜섬웨어 사고 동향을 살펴보면 2022년 1월, Conti 랜섬웨어 공격조직이 대만의 전자제품 제조기업 Delta Electronics를 공격하고, LockBit 랜섬웨어 조직이 프랑스 법무부를 공격하였다. 이후, 영국 식료품 기업 KP Snacks, 스위스 항공 서비스 기업 Swissport International, 일본 스포츠 제조사 미즈노, 자동차 부품 제조업체 DENSO 등 끊이지 않는 랜섬웨어 공격이 이어지고 있다[3].

2.2. 랜섬웨어 공격 조직의 변화

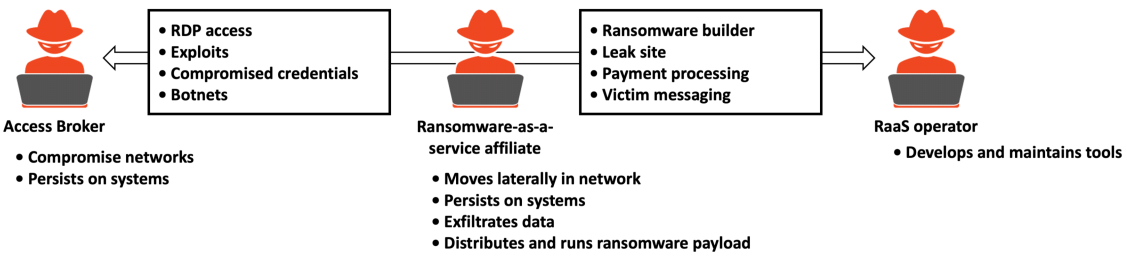
최근 Microsoft는 RaaS 제휴 모델을 구성하는 요소를 분석하여 RaaS 라이프 사이클에 대한 내용을 공유하였다[4]. RaaS 운영자는 랜섬웨어 악성코드를 제작하고, 감염자와 통신하기 위한 채널을 개설하는 등 랜섬웨어 공격에 필요한 도구를 개발하고 유지 보수하는 역할을 수행한다. 이러한 역할은 현재까지도 침해사고에 널리 이용되는 코발트 스트라이크와 같은 유료 도구를 제작하여 공급하는 역할이라고 볼 수 있다. 그림 2에서 정의하는 RaaS 운영자의 역할 중 지불 관련 내용은 대형 공격그룹에서는 세분화되어 자금세탁 전문 조직에게 위탁하는 경우도 존재한다.

접근권한 중개인은 MITRE ATT&CK™ 기준으로, 랜섬웨어 공격조직이 활용할 수 있는 감염된 단말기, 서버 등 인프라를 제공하는 역할이라고 해석할 수 있다. 분업화되지 않은 조직이거나 대형 조직의 경우, 위의 인프라를 직접 구축하고 활용하기도 하지만, 최근에는 각 영역을 분리하여 공격을 수행하고 공격을 통해 확보한 금액을 분할하는 형태로 진행된다. 따라서 접근권한 중개인과 RaaS 운영자가 제공하는 공격도구, 인프라를 이용하여 RaaS 제휴사는 제공된 감염단말기에서 감염대상 확산을 위한 수평이동, 시스템에서의 종속성 유지, 이중 갈취 등을 위한 데이터 탈취 등을 수행하고, 최종적으로 랜섬웨어를 통한 전사 시스템 감염을 수행한다.

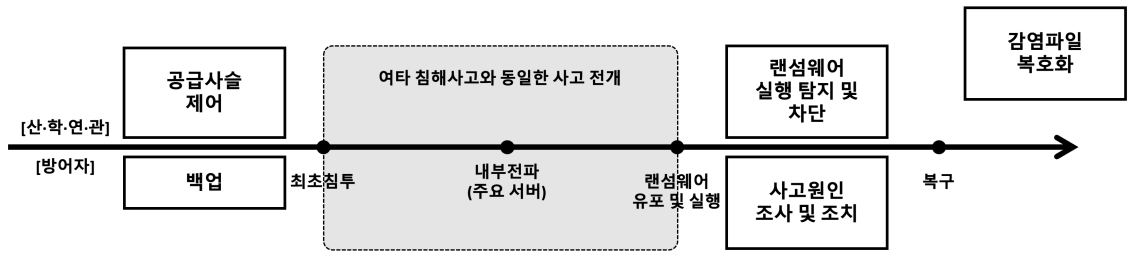
Ⅲ. 최근 랜섬웨어 대응 연구 동향

한국인터넷진흥원에서는 기업이 랜섬웨어 사고에 대응할 수 있도록 다양한 관점으로 분석하고 결과를 공유하고 있다. 특히, 우리나라 기업에서 널리 사용되는 Active Directory(AD) 서비스를 악용한 랜섬웨어 사고에 대하여 수차례 위험성을 지적하였고, 꾸준히 사고 내용을 공개하고 있다[5,6]. 마찬가지로, 해외 보안업체 MANDIANT에서도 다크사이드 랜섬웨어 조직의 TTPs를 정리하여 공유하였다. 해당 조직이 가지는 대표적 특징은 이미 외부에 공개되어 널리 활용되는 취약점과 도구를 사용하고 있다는 점이다. 현재 보안 관련 이해당사자들은 위와 같은 랜섬웨어 사고에 대한 분석 정보를 공개, 교류함으로써 범국가적 차원의 랜섬웨어 대응을 수행하고 있다.

본고에서는 ATT&CK에서 세부적으로 정의하고 있는 TTPs(Tactics, Techniques, and Procedures)의 기준



〔그림 2〕 RaaS 제휴 모델 구성 및 역할(Microsoft)〔4〕



〔그림 3〕 랜섬웨어 공격 타임라인별 대응 분류

을 추상화하여 조직 내부의 시스템으로 침투, 수평이동을 통한 전파, 랜섬웨어 감염, 복구를 주요 기점으로 나누어 랜섬웨어 대응을 분류한다. 우선, 최초침투 이전에 준비할 수 있는 피해 최소화 관점의 예방이 있다. 가장 중요한 랜섬웨어에 감염되더라도 복구할 수 있는 능력을 갖추는 것이 예방 노력의 일환이다. 또한, 방어자는 랜섬웨어가 유포, 실행된 이후에 사고원인을 조사하고 조치하는 대응을 수행할 수 있다.

범용 인프라 및 보안관련 이해당사자의 관점에서, 네트워크 인프라에서 보안제어가 가능한 ISP나 오픈소스 보안 인텔리전스 서비스를 제공하는 기관 등이 공공의 목적을 위해 공급사슬(Supply Chain)을 제어하는 역할을 수행할 수도 있다. 이후, 랜섬웨어가 실행될 때 탐지할 수 있는 기술 및 랜섬웨어에 감염된 파일을 복호화하는 기술 등을 산학연관에서 연구하고 있다.

3.1. 랜섬웨어 피해 최소화 관점의 예방

외부로부터 위험에 노출되어 있는 자산을 보호하기 위해서 기업에서 대응을 준비하는 단계이다. 기업에서는 최근 유행하는 랜섬웨어에 대한 적극적인 정보수집과 더불어, 외부의 악성코드가 침입하지 않도록 최초침투를 방지하기 위한 노력에 초점이 맞춰져 있다. 대부분의 침투시도가 위의 대응에 따라 방어가 가능하지만, 제로데이 취약점 악용 또는 패치가 불가능한 지점으로 침투하는 등 조직 내부 인프라로의 침투는 불가능하지 않다.

최초침투가 발생했다고 가정하더라도, 피해를 최소화하거나 진행 중인 침해사고를 인지할 수 있는 포인트가 존재한다. 공격자는 랜섬웨어 공격을 통해 획득 가능한 금전적 이득을 최대화하기 위하여 많은 양의 핵심 정보를 암호화 하는 것이 필요하기 때문에 DB서버, 중앙제어서버 등 핵심 자산으로의 내부전파를 시도한다. 아쉽게도 대부분의 조직에서는 관리의 편의성 확보를 위하여 주요 자산으로 접근성을 용이하게 설정하고 있어, 공격자의 수평이동 시점에 탐지할 수 있는 포인트를 놓치기 쉽다.

위의 문제를 해결할 수 있는 방안 중 하나는 최근 확산되고 있는 제로트러스트라는 요소이다. 제로트러스트는 접근하는 단말기의 네트워크 위상과 관계없이 사용자와 단말을 신뢰하지 않는다는 개념에서 출발하며, 정상 사용자·기기를 식별하고, 안전한지 컨텍스트를 확인하는 절차를 거친다. 각 기업에서는 이를 반영한 인프라로 기존 보안환경을 전환하려 노력하고 있다.

이 외에도 랜섬웨어에 감염되었다고 가정하였을 때, 피해를 복구하기 위한 백업서버 구축도 방어자의 노력 중 하나라고 볼 수 있다. 대기업의 경우, 백업 서버를 구축하기 위한 비용이 소요되더라도 마련할 수 있는 여력이 충분하지만, 중소기업의 경우 비용 마련의 문제로 백업서버를 구축하기 어려울 수 있다. 한국인터넷진흥원에서는 보안 역량이 취약한 중소기업의 랜섬웨어 피해예방을 위하여 데이터 금고 사업을 실시하고 있어, 중소기업은 정부에서 지원하는 사업을 통해 최소한의 예방(백업)을 준비할 수 있다[7].

3.2. 랜섬웨어 유포 인프라 제어 관점의 대응

2.2에서 소개한 것처럼 공격 조직은 유포 인프라를 CaaS(Crime-as-a-Service)를 통해 확보하기도 한다. 체계적으로 분업화된 랜섬웨어 조직일수록 세부적인 역할이 분배되어 있으며, 좀비PC를 다른 공격조직과 협업하여 사용하기도 한다.

그림 2의 접근권한 중개인이 제공하는 봇넷의 경우, 일반적인 침해사고에서도 활용되는 특성을 보인다. 그러나, 미국 법무부와 Microsoft가 ZLoader 봇넷을 차단하기 위해 공동으로 대응했던 사례는 Ryuk, DarkSide,

BlackMatter 랜섬웨어 등을 유포한 인프라를 차단했다는 점에서 랜섬웨어 대응 노력으로 해석할 수 있다[8].

랜섬웨어 공격의 라이프사이클 중 악성행위의 시작점이 되는 유포 인프라를 공급사슬이라 정의할 때, 공급사슬 제어를 통해 랜섬웨어 공격을 잠시 중단시킬 수 있는 효과가 있다. 프로파일링을 통해 공격자의 TTPs를 분석하여 공개하면, 공격자는 새로운 공격기법을 공부하고 수정해야 하므로 공격자에게 위협이 된다. 마찬가지로, 랜섬웨어 공격조직도 새로운 유포 인프라를 찾고, 협업관계를 재구축해야 하기 때문에 랜섬웨어 공급사슬 제어의 효과가 크다고 할 수 있다.

3.3. 클라이언트 단에서의 실행 탐지 및 차단

랜섬웨어가 감염되는 지점에서의 탐지 및 차단은 일반적인 악성코드 탐지와 큰 차이점이 없다. 탐지 방법은 시그니처 기반 탐지와 행위 기반 탐지로 나누어지는데, 최근에는 시그니처 탐지보다 행위 기반 탐지가 적극적으로 연구되고 있다. 공격자들은 제작한 악성코드를 공격에 활용하기 위해 백신엔진에 탐지되는지를 확인하는데, 하나라도 미탐이 존재할 경우 랜섬웨어 사고가 발현될 수 있으며 APT 공격으로의 진화도 가능하기 때문이다.

상기 탐지 방법 외에도 감염 사실을 모니터링하기 위한 미끼 파일을 준비하는 탐지 방안도 존재하지만, 백신업체 마다 공개되어 있는 미끼 파일을 감염 대상에서 제외하는 루틴을 추가하는 등 손쉽게 우회되기도 한다. 또한, 모듈화된 공격도구에서 외부 명령제어지로부터 랜섬웨어 페이로드를 다운로드 받아 실행하는 과정에서도 탐지가 가능하다.

그 외에도, 최종적으로 실행되는 랜섬웨어 악성코드 이전에 백신 프로그램을 강제종료하고, 이후 실행될 랜섬웨어를 탐지할 수 없도록 침해사고를 구성하기 때문에 클라이언트 단에서의 실행 탐지 및 차단은 한계점이 존재한다.

3.4. 감염파일 복호화 등 복구도구 제작

랜섬웨어 피해자의 노력과 별개로, 산학연관에서는 랜섬웨어의 암호화 과정에서 복호화를 할 수 있는 가능성을 찾고, 복구도구를 개발 및 공유하고 있다. 한국인터넷진흥원 차세대암호인증팀의 경우, Hive 랜섬웨어에 이어 5월 25일 Ragnar 랜섬웨어 복구도구를 공개하였다[9]. Chainanalysis 보고서에 따르면 Hive 랜섬웨어 공격조직이 2021년에 랜섬웨어 공격을 통해 공격조직 중 8위의 수입을 올렸다고 추정되기 때문에, 이를 복구할 수 있는 도구의 공개는 많은 피해자에게 원본 파일을 획득할 수 있는 기회가 될 것이다[2]. 하지만, 피해업체로부터 지속적으로 변화하는 랜섬웨어에 대한 신속한 복구가 요구되는 상황에서, 모든 랜섬웨어의 복구도구를 제작하기 어렵다는 현실적인 제약은, 다른 관점에서의 대응 노력이 필요하다고 결론지을 수 있다.

또한, 랜섬웨어 악성코드의 설계 및 구현상의 문제로 복호화가 가능한 경우가 과거에는 일부 존재했었지만, RaaS의 보편화 및 오픈소스화된 랜섬웨어의 존재로 인해 완성도 높은 랜섬웨어들이 개발되고 사용됨에 따라, 구현상의 허점을 통한 복구 가능성은 요원해졌고, 공개된 복구도구에 의존할 수밖에 없게 되었다.

3.5. 사고원인 조사 및 보안 조치 등 사후 대응

랜섬웨어에 감염된 이후, 피해자가 감염된 파일을 복구하기 위하여 채택할 수 있는 방법은 협상을 통해 복호화 키를 수신하거나, 외부에 공개되어 있는 복구도구를 통한 방법 등이 존재한다. 3.4에서 언급한 복구도구를 통한 복호화 외에, 협상을 통한 복호화 하는 경우, 복호화가 실패하는 경우가 존재하며 복구 성공을 보장할 수 있는 대상은 공격조직이므로 복호화 실패에 대한 책임을 물을 대상이 없다. 심지어, 신속한 감염을 목적으로 파일 데이터 일부를 삭제하고 잔여 데이터를 암호화하는 랜섬웨어 악성코드가 존재하기 때문에, 필요한 파일을 복호화할 수 없는 경우도 다수 존재한다.

정책적인 관점에서, 미국에서는 랜섬웨어 조직에게 몸값을 지불하지 못하도록 정책이 발표되었다. 또한, 랜섬웨어 공격 조직에게 몸값 지불은 가상자산으로 이루어지는데, 전 세계적으로 가상자산의 송수신인 관련 정보를 의무적으로 제공해야하는 트래블 룰이 엄격하게 적용되고 있다. 따라서 표면상에 드러난 환경에서 공격조직에게 몸값 지불이 어렵기 때문에 향후 공격조직과의 협상을 통한 복호화 키 수신은 어려워질 것으로 예상된다. 이에 따라, 복구업체를 대리인으로 지정하여, 복구업무 일체를 위탁하는 프로세스도 점진적으로 축소

될 것으로 예상되고 있다.

랜섬웨어 복구 이외에도, 피해기업의 랜섬웨어 대응은 재발 가능한 영역을 제거하기 위하여 자사의 인프라 내부에 공격자의 백도어가 잔류하고 있는지를 점검하는 것과 최초침투를 허용한 원인을 파악하고 조치하는 행위도 포함된다. 공격의 지속성 유지를 위한 백도어 및 최초침투를 가능하게 만든 위협 포인트는 향후 랜섬웨어 재발이 가능한데, 실제로도 랜섬웨어 공격조직의 재공격이 이어진 사례가 존재한다. 따라서 랜섬웨어의 피해자는 사고의 원인을 정확히 파악하고 향후 재발 가능한 사고를 신속히 준비해야 한다.

Ⅳ. 결 론

본고에서는 기업의 비즈니스를 위협하는 랜섬웨어 사고의 특징을 공격 타임라인으로 나누어 대응방안을 분류하였다. 또한, 정부부처, 학교, 연구소, 기업 등 각 이해당사자들이 랜섬웨어를 어떻게 대응하려고 노력하는지 소개하였다. 각 기관들이 보유한 인적, 물적 자산의 특장점과 한계점을 상호협력 및 공유를 통해 전반적인 랜섬웨어 공격의 대응수준 향상을 기대한다.

참 고 문 헌

[1] MANDIANT, https://www.mandiant.com/resources/shining-a-light-on-darkside-ransomware-operations, May 2021.

[2] Chainanalysis, “The 2022 Crypto Crime Report”, Feb 2022.

[3] 한국인터넷진흥원, “2022년 1분기 랜섬웨어 동향 보고서”, May 2022.

[4] Microsoft, https://www.microsoft.com/security/ blog/2022/05/09/ransomware-as-a-service-under standing-the-cybercrime-gig-economy-and-how-to-protect-yourself/, May 2022.

[5] 한국인터넷진흥원, “AD 서버 악용 내부망 랜섬웨어 유포 사례 분석”, Apr 2019.

[6] 한국인터넷진흥원, “TTPs#5 AD 환경을 위협하는 공격 패턴 분석”, June 2021.

[7] 한국인터넷진흥원, https://safe.kisa.or.kr/

[8] Microsoft, https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/

[9] 한국인터넷진흥원, https://safe.kisa.or.kr/kisa/adverse/reference.do

〈저 자 소 개〉

이 슬 기 (Seulgi Lee)

정회원

2013년 2월 : 충남대학교 컴퓨터 공학과 졸업

2019년~현재 : 고려대학교 빅데이터응용및보안학과 석사과정

2012년 10월 ~ 현재 : 한국인터넷진흥원 선임연구원

<관심분야> 위협 프로파일링, 악성코드, AI 보안, SW 보안

김 동 욱 (Dongwook Kim)

2014년 2월 : 한양대학교 컴퓨터공학과 졸업

2013년 12월~현재 : 한국인터넷진흥원 선임연구원

<관심분야> 위협 프로파일링, 코드 분석, 디지털 포렌식, 침해사고 대응

이 태 우 (Taewoo Lee)

2015년 2월 : 호서대학교 정보보호학과 졸업

2014년 6월~2016년 5월 : 하우리 침해대응센터 연구원

2016년 6월 ~ 현재 : 한국인터넷진흥원 선임연구원

<관심분야> 사이버 위협 프로파일링, 악성코드 분석, 침해사고 대응