방송·통신 : 2021. 6. 16.(수) 12:00 / 신문 : 2021. 6. 17.(목) 조간용		
가장 안전한 나라, 존경과 사랑받는 경찰 서울경찰청 보도자료 www.smpa.go.kr		
사이버수사과장 총경 이 병 귀 일반 02-700-5800, 경비 5800	담당 경정 서상혁 일반 02-700-5900, 경비 5900	2021년 6월 14일

랜섬웨어 제작·유포 일당 9명 검거(구속 2)

- 데이터 복구비 명목으로 3억6천만원 가로챈 수리기사들 -

❑ 서울경찰청 사이버수사과는,

○ '19. 12.~'21. 3. 성능저하 등의 문제로 수리의뢰 받은 PC에 **자체 제작한 랜섬웨어*를 감염시키거나**, 실제 랜섬웨어 공격을 당한 기업을 위해 해커와 협상하면서 요구받은 **복구비를 부풀리는 등의 방법**으로,

○ 피해자 40명으로부터 약 3억 6,200만원을 가로챈 **컴퓨터 수리업체 소속 수리기사 및 법인 10명을 입건**하고 그중 **2명을 구속**하였음

* 랜섬웨어(Ransomware)는 시스템의 내부 문서나 데이터를 암호화해 사용 불능 상태로 만드는 악성코드로, 범죄자들이 해독 프로그램 제공을 대가로 금전을 요구하는 공갈 범죄를 저지르는데 사용한다.(경찰청, 「사이버 수사용어집」, p.69)

적용법조

- 정보통신망법 제48조 제2항(악성프로그램 유포) ····· 7년↓, 7,000만원↓
- 정보통신망법 제48조 제1항(정보통신망 침입) ····· 5년↓, 5,000만원↓
- 정보통신망법 제49조(타인정보 훼손) ····· 5년↓, 5,000만원↓
- 정보통신망법 제75조(양벌규정) ····· 5,000만원↓
- 형법 제314조 제2항(컴퓨터등업무방해) ····· 5년↓, 1,500만원↓
- 형법 제347조 제1항(사기) ····· 10년↓, 1,500만원↓

❑ 사건의 개요

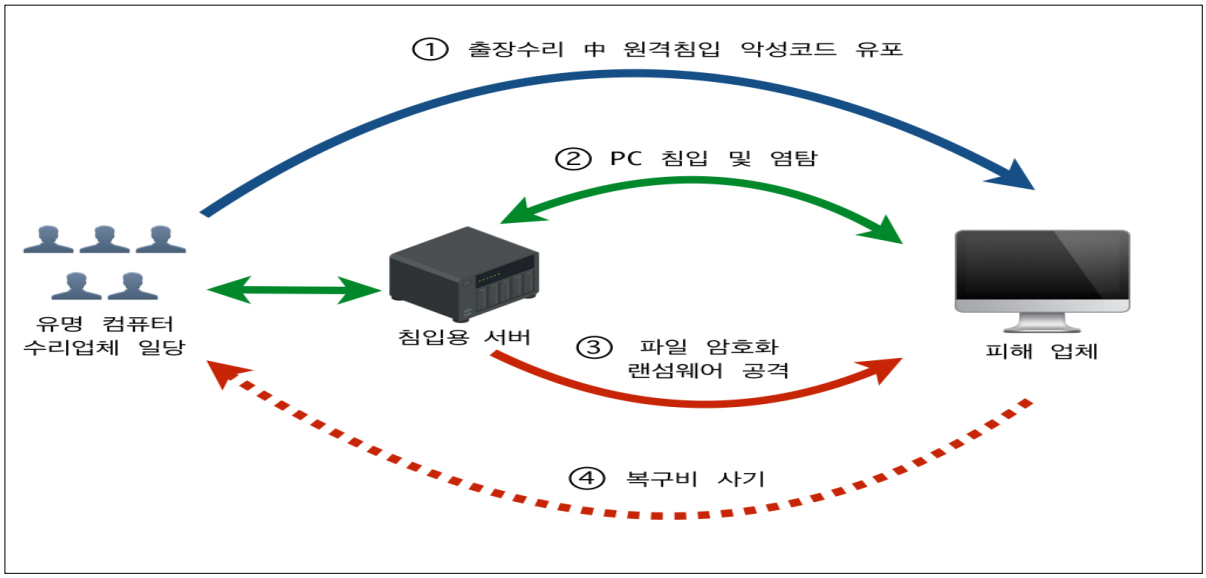
【수사착수 경위】

○ 경찰은 '20. 12월 해커의 랜섬웨어 공격을 당한 피해업체의 신고를 접수하고, 해커들의 흔적을 뒤쫓던 중 피의자들의 범죄를 포착하여 수사에 착수하게 되었음

【피의자들의 지위】

○ 피의자들은 전국적으로 50여 명의 수리기사를 두고 있는 컴퓨터 수리업체 소속 수리기사들로, 데이터 복구나 수리를 위해 인터넷 검색으로 업체를 찾은 고객들을 범행대상으로 삼았음

연번	피의자	주요혐의	비고
1	A (43세)	랜섬웨어 유포, 이메일 변작, PC 고의감염, 복구비 부풀리기	구속
2	B (44세)	랜섬웨어 유포, PC 파티션 훼손, 복구비 부풀리기	구속
3	C (43세)	랜섬웨어 제작·유포, 복구비 부풀리기	
4	D (37세)	랜섬웨어 유포, 복구비 부풀리기	
5	E (48세)	랜섬웨어 유포, 복구비 부풀리기	
6	F (45세)	복구비 부풀리기	
7	G (48세)	복구비 부풀리기	
8	H (48세)	복구비 부풀리기	
9	I (37세)	복구비 부풀리기	
10	J (법인)	정통망법 양벌규정	



【랜섬웨어 제작·유포】

○ A~E는 '20. 12말경 문서·이미지 등 파일들을 **'.enc' 확장자로 암호화시키는 랜섬웨어를 자체적으로 제작**하고, 이를 **원격 침입 악성코드를 이용해 고객의 컴퓨터에 감염시키기로 공모**하였음

○ 이들은 '21. 1월~2월 고객의 요청을 받아 출장 수리 중 **20개 업체의 컴퓨터에 원격 침입 악성코드를 설치하여** 저장된 데이터는 물론 접속기록 등 고객들의 사생활을 염탐하여 범행시기를 결정함

○ 이후, 설치된 악성코드로 **자체 제작한 랜섬웨어를 실행**하여 컴퓨터의 **파일들을 암호화**시키고, 복구를 의뢰한 피해업체들에게 해커의 범행이라고 속여 4개 업체(ⓐ~ⓓ)로부터 3,260만원을 부당취득하였음

【랜섬웨어 복구비용 편취】

○ A~I는 자체 제작한 랜섬웨어 유포 범행 외에 실제로 랜섬웨어 공격을 당해 복구를 의뢰한 21개 업체 **데이터 복구 과정에서 피해자를 속여 아래와 같이 총 3억 3천만원의 이익을 취득하기도 하였음**

- **(협상 이메일 조작)** A,B,F,G,H,I는 해커와의 협상을 **피해자들이 알지 못하게 단독으로 수행하면서 협상 이메일 내용을 조작하는** 등 17개 업체로부터 2억 5,300만원을 편취하였음

▸ ⓔ업체 복구 당시 해커가 **0.8BTC를 요구**하였으나 **8BTC를 요구한 것처럼 이메일을 조작**하여 복구비 약 1억 3천만원 부당취득

▸ ⓕ업체 복구 당시 해커가 지정한 가상자산 지갑 주소를 A의 개인 **지갑 주소로 조작**하여 0.5BTC(1,300만원) 부당취득

- **(고의 추가감염)** A,B,F는 랜섬웨어 복구 및 컴퓨터 수리 명목으로 회사에 **입고한 PC**에 랜섬웨어를 **고의로 추가감염**시킨 후 **해커 소행이라고 속이고** 3개 업체로부터 추가 복구비 4천만원을 편취함

▸ 랜섬웨어 공격을 당한 ⓖ업체의 데이터 복구를 위해 업체에 입고한 서버의 일부 파일을 암호화시킨 후에, 조작한 이메일로 해커가 추가로 1.5BTC를 요구한다고 속여 약 3,300만원을 부당취득

- **(수리증상 속임)** A,B는 접촉 불량, 부팅 장애 등 일반적인 고장임에도 **랜섬웨어에 감염되었다고 속이고** 4개 업체로부터 랜섬웨어 복구비로 3,700만원을 편취함

▸ 컴퓨터 속도가 느려 수리를 의뢰한 ⓗ업체를 방문하여 출장수리를 하면서 피해자 몰래 서버의 케이블을 뽑고, 파티션을 숨겨 연결을 끊은 후 랜섬웨어에 감염되었다고 속이고 복구비(3,200만원)를 부당취득

❑ 사건의 특징

○ 랜섬웨어 범행은 시스템 자체에 접근할 수 없게 하거나, 중요 파일을 암호화한 다음 데이터 복구를 빌미로 금전을 갈취하는 범행으로 **최근 급증**하여 **사회적 문제로 대두**되고 있음

※ 과기정통부는 최근 랜섬웨어 급증에 따라 한국인터넷진흥원에 **'랜섬웨어 대응 지원반'을 신설**하였음

○ 랜섬웨어 범행은 해외 해커의 소행인 경우가 다수인데, 이번 사건은 국내 컴퓨터 수리기사들이 **직접 제작한 랜섬웨어를 유포한 사안으로,**

- 경찰은 피의자들이 범행에 착수한 초기에 수사력을 집중하여 **신속히 검거하고** 범행에 사용된 **랜섬웨어 및 원격 침입 악성코드 24개를 모두 압수하여** 피해의 확산을 막을 수 있었음
- 또한, **사안의 중대성을 고려하여** 위 범죄이익을 공유한 **업체**에 대해서도 **양벌규정을 적용**하였음

○ 특히, 적극행정의 일환으로 피해 사실을 모르던 **전국 39개 피해 업체들을 찾아내고** 암호화된 파일들로 인해 업무에 지장을 겪고 있는 피해업체 3곳은 **파일들을 복구**해주기도 하였음

○ 이번 수사는 정보통신망에 대한 사회적 신뢰를 무너뜨리는 **랜섬웨어 범죄 척결에 대한 경찰의 적극적 수사 의지가 반영된 사안**으로, 앞으로도 랜섬웨어 관련 범죄를 끝까지 추적·검거하겠음

❑ 당부사항

○ 랜섬웨어 범행을 예방하기 위해 아래 5대 수칙을 숙지하고 실천하여 **PC 보안에 각별한 주의**를 기울일 필요가 있으며,

○ 랜섬웨어 몸값을 지불하는 경우 국내기업이 해커의 지속적인 공격대상이 될 수 있는 만큼 협상보다는 **랜섬웨어 공격을 당한 즉시 신속히 경찰에 신고**해주실 것을 당부함

한국인터넷진흥원 랜섬웨어 피해예방 5대 수칙

❖ 모든 소프트웨어는 최신 버전으로 업데이트하여 사용합니다.
❖ 백신 소프트웨어를 설치하고, 최신 버전으로 업데이트합니다.
❖ 출처가 불명확한 이메일과 URL 링크는 실행하지 않습니다.
❖ 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의합니다.
❖ 중요 자료는 정기적으로 백업합니다.

※ 제공가능 자료 : 피의자 유포 랜섬웨어 암호화 및 복호화 과정 시연
(6.15.(화) 14:00 서울청 지하1층 어울림홀)

이 보도자료와 관련하여 더욱 자세한 내용이나 취재를 원하시면 서울경찰청 사이버수사1대 경정 서상혁 (☎ 02-700-5900)에게 연락해주시기 바랍니다.