이 보도자료는 배포 즉시 보도하여 주시고, 공개되는 범죄사실은 재판에 의하여 확정된 사실이 아님을 유의하여 주시기 바랍니다.

검찰 PROSECUTION SERVICE

서울중앙지방검찰청

전문공보관 김종우

전화 02-530-4780 / 팩스 02-536-5410

보 도 자 료

2023. 11. 20.(월)

제 목

해커조직과 짜고 해킹 피해자 730명으로부터 26억 원을 갈취한 데이터복구 업체 운영자 등 구속기소

공소제기 후 공개의 요건 및 범위

☑ 피고인, 죄명, 공소사실 요지, 공소제기 일시, 공소제기 방식, 수사경위, 수사상황, 범행경과 및 수사의 의의 등(제11조 제1항)

☑ 제9조 제1항 제1호 내지 제6호의 어느 하나에 해당하고 미리 공개가 필요한 상당한 이유가 있다고 인정되어 소속 검찰청의 장의 승인이 있는 경우(제11조 제2항 제2호) 제7조 제2호 내지 제6호의 공개금지정보

- 서울중앙지검 정보·기술범죄수사부(부장검사 이춘)는 2023. 11. 14.(화) 해커조직과 결탁하여, 해킹 피해자 730명으로부터 총 26억여 원을 갈취한 데이터복구업체 대표 등 2명을 공갈죄로 구속 기소하였음

- 피고인들이 결탁한 해커조직은 피해자들의 컴퓨터에 악성프로그램의 일종인 메그니베르* 랜섬웨어**를 침투시켜 컴퓨터 내 모든 파일을 암호화 함으로써 피해자들이 해당 컴퓨터를 사용할 수 없게 만듦

  * 메그니베르 : 랜섬웨어의 일종으로 해킹 대상 컴퓨터의 파일이 암호화되며 파일 이름 뒤에 붙는 확장자가 변경됨(예시 : 파일명.hwp → 파일명.uqnqtbhv)

  ** 랜섬웨어 : 피해자의 컴퓨터를 해킹하여 모든 파일을 암호화 한 다음 **이를 풀어 주는 대가로 돈을 요구**하는 해킹수법에 사용되는 해킹프로그램

- 피고인들은 돈을 벌 목적으로 단순한 복구대행 업무에서 더 나아가 해커조직과 결탁하였음

  - 해커조직은 소수의 '데이터복구업체'를 선정해, 배포할 랜섬웨어에 파일이 감염되는 경우 나타나는 특징에 대한 정보를 제공함으로써 해당 업체가 랜섬웨어에 감염되어 암호화된 파일의 복구 대행을 선점할 수 있게 함

- 피고인들은 피해자들이 랜섬웨어 감염시 복구업체나 방법 등을 찾기 위해 랜섬웨어에 감염된 파일의 확장자를 키워드로 인터넷 검색을 하는 점을 이용해, 인터넷 포털사이트의 검색 광고 및 블로그 광고에 확장자를 '키워드'로 등록하여 수많은 피해자를 유인함

- 검찰은 이 사건을 수사하여 ▲ 오랜기간 해커조직으로부터 랜섬웨어 유포 시기와 확장자 정보 등을 제공 받고 이를 이용하여 복구대행업을 독점한 점, ▲광고를 통하여 피해자들을 직접 유인하는 등 적극 범행에 가담한 점, ▲해커조직에게 영업상황을 수시로 보고하고 실적에 따라 해커보다도 많은 수익을 배분받은 점 등을 밝혀내고 해커조직과의 공갈죄 공동정범으로 기소함

1 피고인 및 공소사실 요지

피고인

- A○○(34세, 구속, 甲 데이터복구업체 대표)

- B○○(34세, 구속, 甲 데이터복구업체 직원, 해커와 협상 담당)

공소사실 요지

- '18. 10. 15. ~ '22. 7. 26. 매그니베르(Magniber) 랜섬웨어를 유포하는 해커조직과 공모하여, 불특정 다수 피해자들의 컴퓨터에 매그니베르를 감염시킨 후, 피해자들로부터 그 '**복구 비용**' 명목으로 총 730회에 걸쳐 합계 26억 6,489만여원을 교부받아 갈취【공갈】

※ '복구 비용'은 해커가 피해자에게 요구한 소위 '몸값(Ransom)'과 피고인들이 피해자들에게 청구한 서비스료(통상 해커가 요구한 몸값의 100%)를 합한 금액으로, 랜섬웨어에 감염된 피해자가 실제 부담한 피해 금액임

2 수사 경과

- ’20. 10. 5. 경찰청(본청) 보안수사과 수사 착수
- ’23. 10. 18. 구속영장 발부(‘23. 10. 16. 구속영장 청구)
- ’23. 10. 26. 경찰 사건송치 (송치죄명 : 공갈방조)
- ’23. 11. 14. 피고인 2명, **공갈 공동정범으로 구속기소**

3 특이 사항

- 랜섬웨어는 몸값(Ransom)과 악성소프트웨어(Malware)의 합성어로, 무단으로 피해자의 컴퓨터 파일을 암호화해 사용하지 못하도록 만드는 악성프로그램

  - 랜섬웨어 해커는 피해자의 컴퓨터 파일을 감염시킨 후, 소위 ‘**몸값**’으로 기한 내 일정량의 가상화폐를 전송해야만 파일 복구를 해주겠다고 협박하여 피해자로부터 몸값을 갈취

- ‘매그니베르(Magniber)’는 2017.경에 등장하여 한국어운영체제 및 한국 IP 주소를 사용하는 국내 이용자들을 주로 감염시키는 랜섬웨어

  - 매그니베르에 감염된 파일은 ‘**확장자**’가 5 ~ 10 자리로 된 알파벳 소문자 문자열로 변경되는데, 감염된 컴퓨터마다 각기 다른 문자열로 임의 변경되는 특징이 있어 해커 외에는 사전에 감염 파일의 확장자를 알 수 없음

  ※ 해커조직에 이체한 가상화폐 추적 결과, 일부가 북한해킹 조직의 전자지갑으로 일부 이체된 사실 확인, **매그니베르 유포조직은 북한 해커조직인 ‘라자루스’와 연계되어 있는 것으로 추정**

- 피고인들은 해커로부터 복호화 키를 전달받아 파일의 암호를 해제해주는 단순한 업무를 하였음에도, 피해자로부터 해커조직에 전달할 몸값과 동일한 금원을 서비스 수수료로 교부받음

  - 실제 피해자로부터 받은 몸값 중 80%만 전달하기로 사전에 해커조직과 협의하였음에도 이를 피해자에게 알리지 않은 채 몸값 전액을 교부받아

20%에 해당하는 금원을 추가로 착복, 해커보다 더 많은 수익을 얻기도 함

※ 해커조직과 데이터복구업체가 원격으로 각자의 역할을 분담하며 랜섬웨어 유포를 통해 공갈죄를 범한 최초 적발 사례임

- 송치 후 보완수사 등을 통해 피고인들을 해커조직과의 공갈죄 공동정범으로 기소함

- 단순히 해커들을 도와 범죄수익을 거두어 나누는데 그치지 않고, 매우 오랜 기간(4년)에 걸쳐 랜섬웨어 유포시기와 확장자 정보 등을 전속으로 제공받아 공유하며 복구대행을 독점하여 옴

- 해커조직에 영업상황을 수시로 보고하고 영업실적에 따라 수익을 나누어 가졌으며, 피고인들이 관여한 범행에서는 해커조직보다도 더 많은 범죄수익을 거두어들임

※ 경찰에서는 랜섬웨어 유포에는 직접 관여하지 않은 점 등을 이유로 '공갈방조'로 송치함 ▦