랜섬웨어 공격이 정말 감소하는 추세일까요? 관점에 따라 다를 수 있습니다.

2021년 12월 20일 • ALLAN LISKA

Insikt Group®

먼저 몇 가지 사실을 짚고 넘어가겠습니다.

1. 2021년 랜섬웨어 공격은 2020년 공격 건수를 훨씬 넘어설 것입니다.
2. 이 데이터는 예비 데이터이며 공개된 데이터를 기반으로 하는데, 흥미로운 추세를 보여줍니다.
3. 랜섬웨어에는 항상 옵저버빌리티(observability) 이슈가 있습니다. 아무도 랜섬웨어 공격의 전체 그림을 파악하지 못합니다.

2021년에는 국제 공조 하에 랜섬웨어 그룹에 대해 전례 없는 제재가 단행되었습니다. 미국 주도 하에 30개국이 참여한 랜섬웨어 태스크포스가 거의 매주 랜섬웨어 그룹에 대한 제재 성과를 발표하는 등 초반부터 성과를 거두고 있는 것으로 보입니다(그림 1 참조).

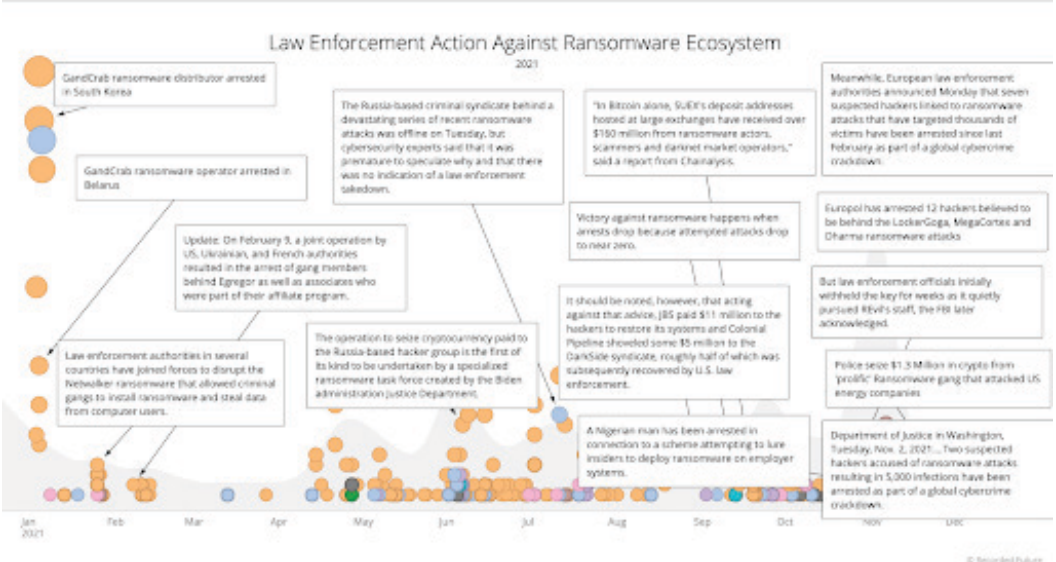

그림 1: 2021년 랜섬웨어 그룹에 대한 법 집행 조치 사례 (출처: Recorded Future)

랜섬웨어 그룹에 대한 지속적이고 일관된 법 집행 조치가 필요하다는 데에는 의심의 여지가 없으나, 이러한 조치가 실제로 랜섬웨어 공격을 감소시킬 수 있는지는 의문입니다.

아직 속단하기에는 이르지만 체포, 암호화폐 거래소 제재, 암호화폐 압수 등의 조치로 일부 지역에서 랜섬웨어 공격 횟수가 줄고 있다는 신호가 있습니다.

그림 2는 2021년 전 세계적으로 보고된 의료 기관 대상 랜섬웨어 공격을 보여줍니다. 2021년 11월 30일까지 레코디드 퓨처 데이터 세트는 의료 기관을 대상으로 한 114건의 랜섬웨어 공격을 파악했습니다(2020년의 경우는 한 해 통틀어 104건). 이 114건의 공격 중 63%가 2021년 1월부터 6월 사이에 발생했으며, 37%가 7월 1일 이후에 발생했습니다.

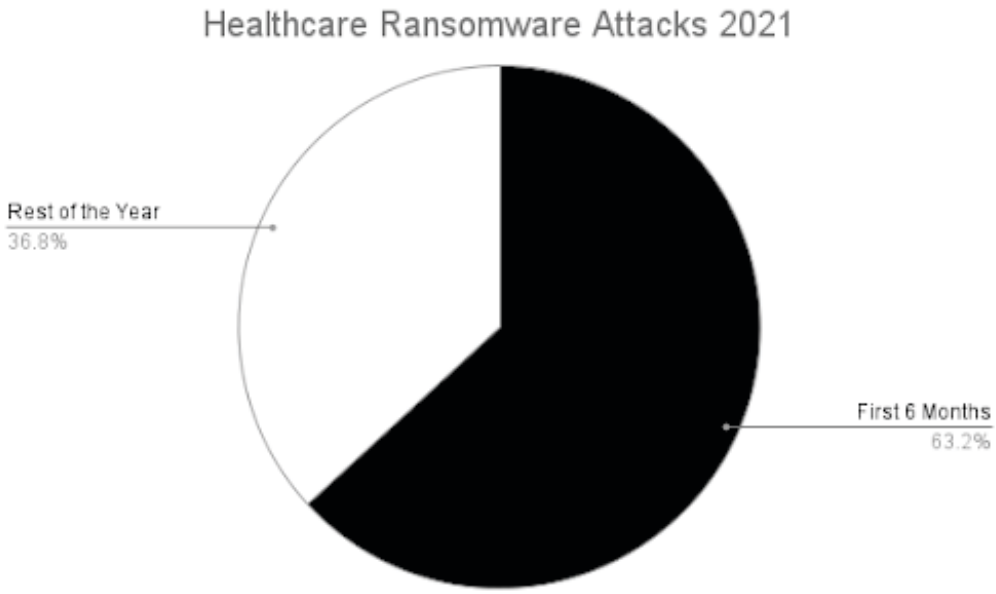

그림 2: 2021년 상반기와 2021년 하반기 전 세계 의료 기관 대상 랜섬웨어 공격 (출처: Recorded Future)

이 수치를 2020년과 비교하면 그림 3과 같이 2020년 하반기부터 랜섬웨어 공격이 증가하는 것을 확인할 수 있습니다.

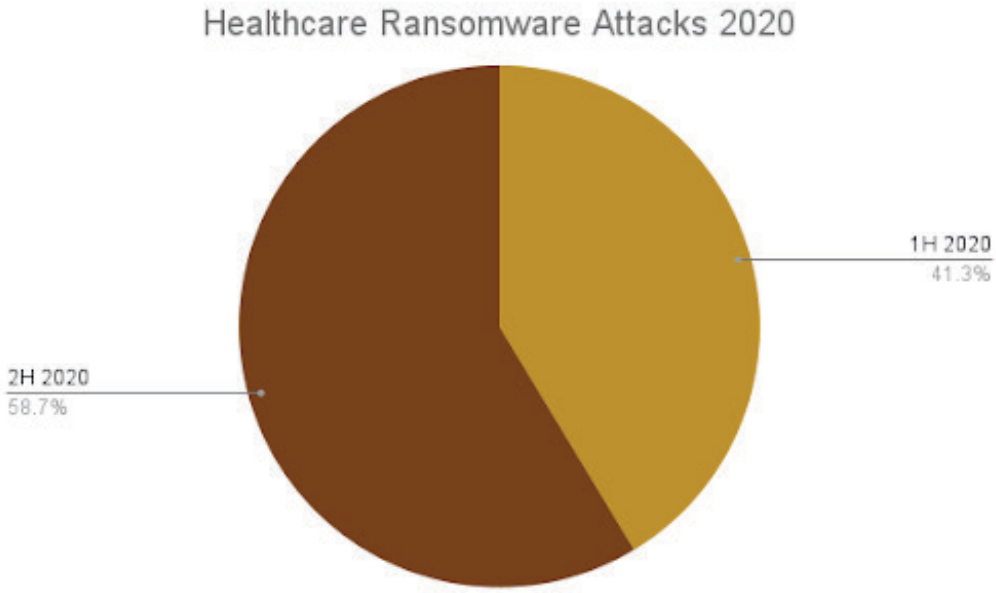

그림 3: 2020년 전 세계 의료 기관 대상 랜섬웨어 공격 (출처: Recorded Future)

이와 동일한 패턴이 전 세계 교육 기관 대상 랜섬웨어 공격에도 적용됩니다. 레코디드 퓨처는 2021년 11월까지 교육 기관을 대상으로 한 95건의 랜섬웨어 공격을 확인했습니다. 이는 2020년 64건에 비해 증가한 숫자입니다.

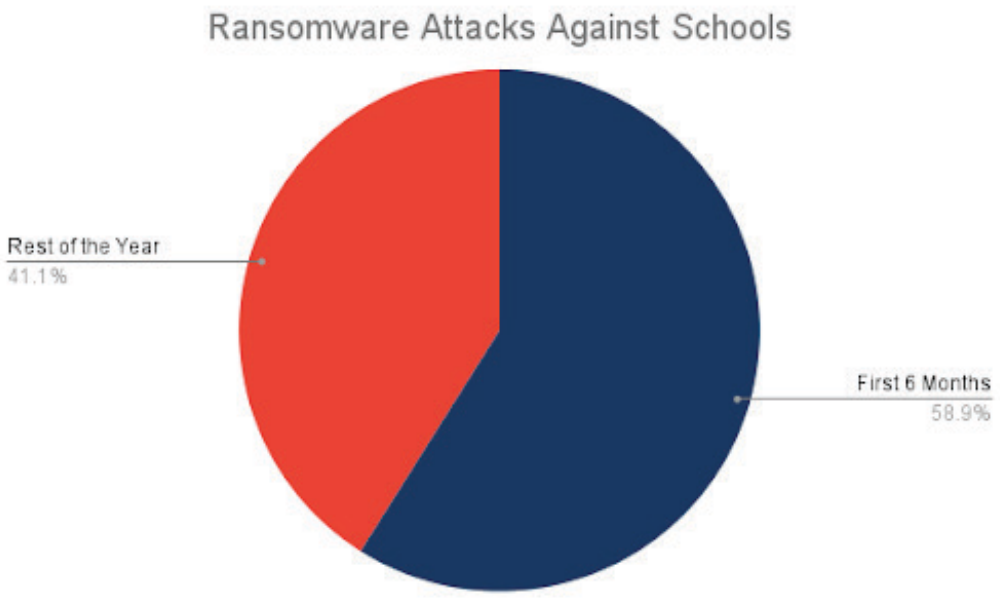

그림 4: 2021년 11월까지 파악된 전 세계 교육 기관 대상 랜섬웨어 공격 (출처: Recorded Future)

2021년 상반기에 전체 랜섬웨어 공격의 59%가 발생하였으며 하반기에 41%가 발생했습니다. 공공 기관 대상의 랜섬웨어 공격 역시 2021년에 전반적으로 감소하였으며, 하반기부터 줄어드는 패턴 또한 동일합니다. 레코디드 퓨처는 정부 및 공공 기관 대상 랜섬웨어 공격이 2020년 104건에서 2021년 87건으로 감소한 것을 확인했습니다.

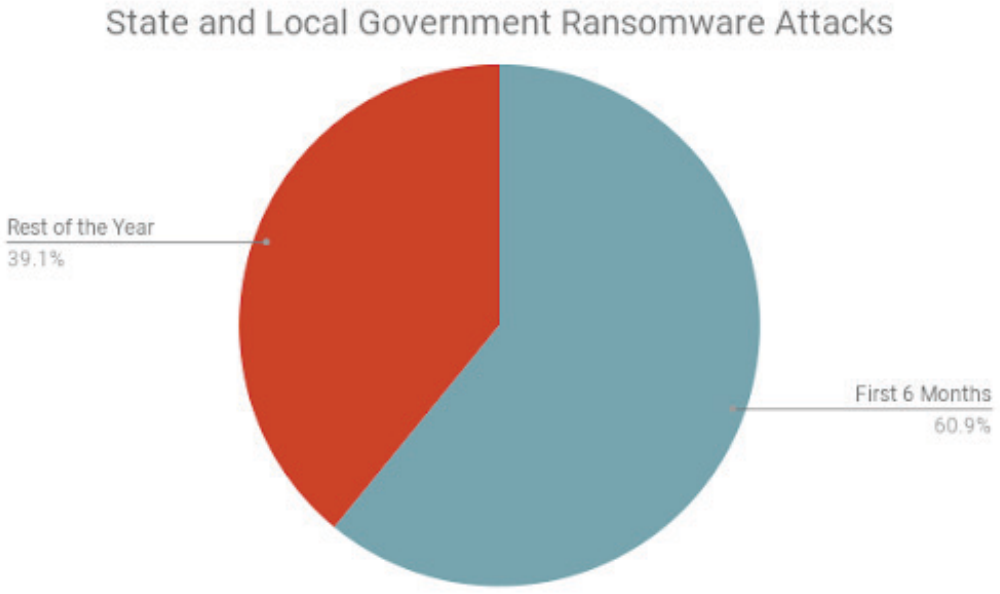

그림 5: 2021년 정부 및 공공 기관 대상 전 세계 랜섬웨어 공격 (출처: Recorded Future)

교육 기관 대상 랜섬웨어 공격 패턴과 유사하게 정부 및 공공 기관 랜섬웨어 공격 역시 61%가 2021년 상반기에 발생했으며 39%만이 하반기에 발생했습니다(그림 5 참조).

2021년 하반기에 랜섬웨어 공격이 둔화되고 있다는 주장과 반대되는 한 가지 데이터는 랜섬웨어 협박(Extortion) 웹사이트에 게시된 피해자의 수입니다. 레코디드 퓨처는 2021년 7월과 8월 사이에 전 세계적으로 파악된 공격 건수가 감소했음에도 불구하고 랜섬웨어 협박 웹사이트에 2,597명의 피해자 내역이 게시되었음을 2021년 11월 말 기준으로 확인했습니다.

그림 6에서 볼 수 있듯이 피해자의 45%는 2021년 상반기에, 55%는 하반기 5개월 동안에 발생했습니다. 이는 공개된 가장 큰 규모의 랜섬웨어 샘플이며, 피해자 수가 증가하는 것으로 보입니다.

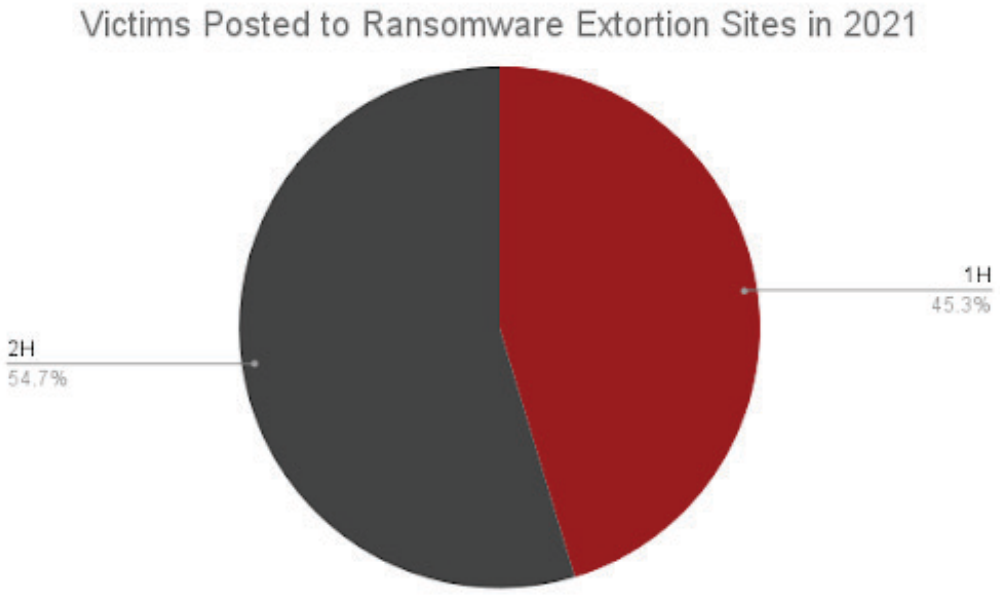

그림 6: 2021년 랜섬웨어 협박 웹사이트에 게시된 피해자 (출처: Recorded Future)

게시 시간은 랜섬웨어 공격이 발생한 시간이 아니라 피해자가 협박 웹사이트에 게시된 시간이라는 점에 유의해야 합니다. 연구원들은 랜섬웨어 협박 웹사이트에 게시되는 피해자 수가 상당히 지연되는 경향을 확인하고 있습니다.

랜섬웨어 공격과 랜섬웨어 협박 사이트 게시물 사이의 타이밍을 연구해 온 프랑스 연구원 Valéry Rieß-Marchive는 다음과 같이 말했습니다.

"…제가 본 바로는 RaaS(Ransomware-as-a-Service)와 대여자(affiliate, 랜섬웨어 개발자들로부터 서비스형 랜섬웨어를 대여받아 공격을 하는 공격자)에 따라 시간차는 0에서부터 4개월까지 다양합니다. 그리고 이전에 한 번도 공격을 겪은 적이 없는 랜섬웨어 피해자들이 일부 시장에서 나타나기 시작했습니다. 이는 지연이 훨씬 더 길 수 있음을 의미합니다."

즉, 랜섬웨어 공격과 협박 사이트 게시 사이의 지연으로 인해 이러한 공격 중 상당수가 실제로 2021년 상반기에 발생했지만 하반기에 협박 사이트에 게시되었을 가능성이 있습니다. 하지만 실제 랜섬웨어 공격과 협박 사이트 게시 사이에 상당한 시간차가 있다 하더라도, 이것만으로는 2021년 하반기에 전반적인 랜섬웨어 공격이 둔화되었다고 보기 어렵습니다.

이는 레코디드 퓨처가 독일의 랜섬웨어 공격에 대해 수행하고 있는 별도의 연구에서 입증되었습니다. 랜섬웨어 공격이 협박 사이트에 게시된 시점과 실제로 공격이 발생한 시점의 차이를 살펴보면 그림 7과 같이 매우 다른 2개의 타임라인이 표시됩니다.

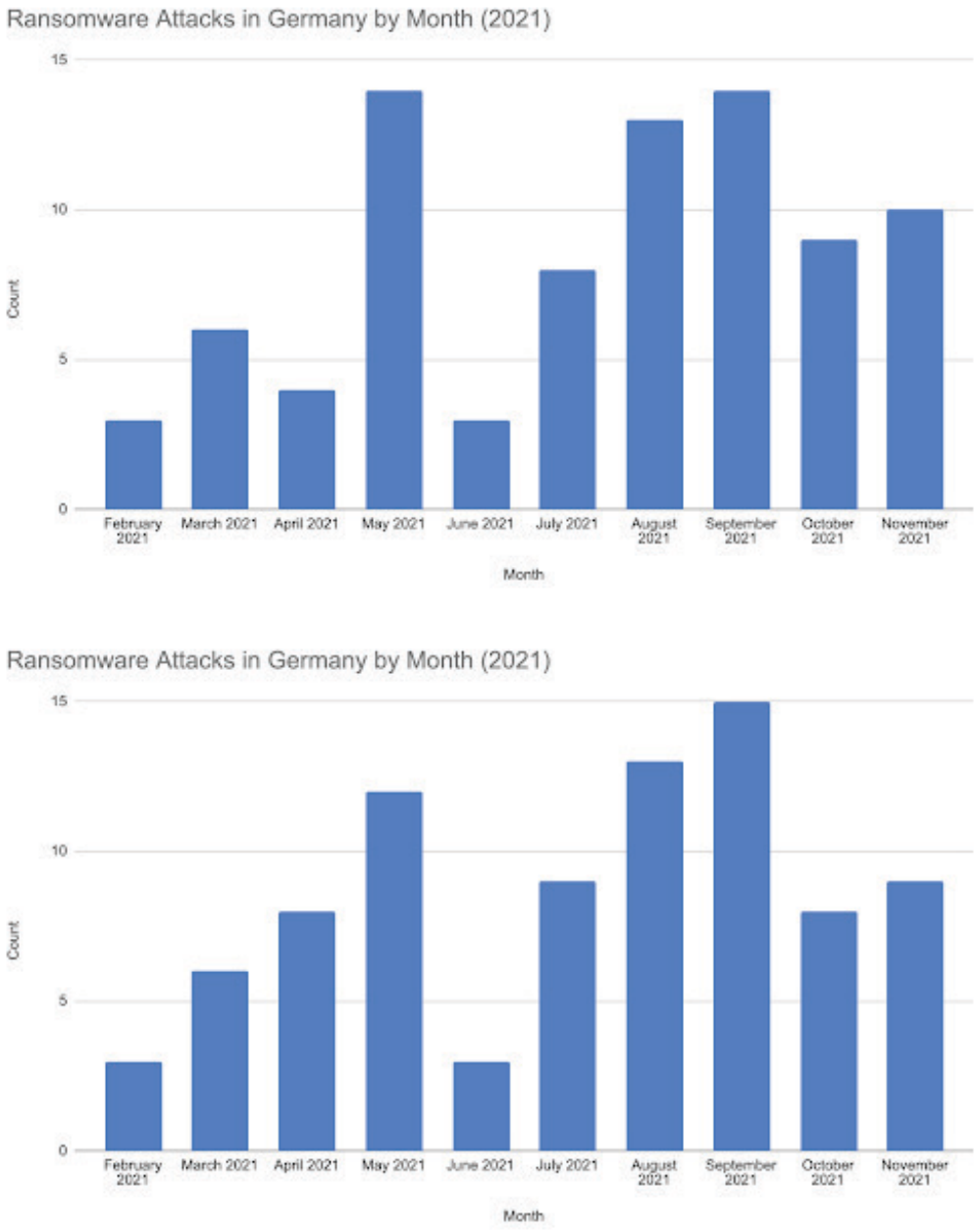

그림 7: 협박 사이트에 게시된 랜섬웨어 공격과 실제 공격 발생 시점의 비교

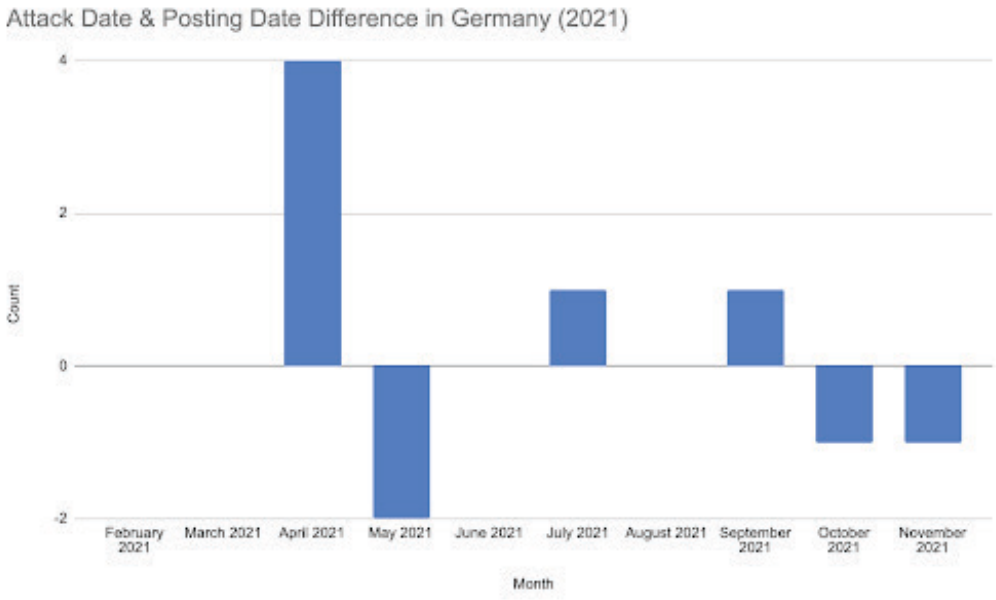

그림 8: 공격 보고 시점과 공격 발생 시점의 차이

그림 7의 왼쪽 그래프는 협박 사이트 게시물을 나타내고 오른쪽 그래프는 실제로 발생한 공격 시점을 보여줍니다. 여기서 주의할 점은 공격의 약 25%만이 공격 발생 시 바로 보고된다는 것입니다. 따라서 레코디드 퓨처의 랜섬웨어 연구원들은 그림 8에 나온 것처럼 레코디드 퓨처가 로깅한 전체 공격의 약 20%에 대해서만 공격 날짜 정보를 파악할 수 있었습니다. 이 데이터는 공격 발생과 협박 사이트 게시 사이의 시간 차이가 일관되게 한 달 이상이라는 것과 일치합니다(평균적으로 확실히 예외가 있음).

이러한 시간차를 감안하더라도 레코디드 퓨처가 식별할 수 있었던 2021년 11월 말까지 독일에서 공개적으로 보고된 110건의 랜섬웨어 공격 중 대부분은 그림 9와 같이 하반기에 발생했습니다.

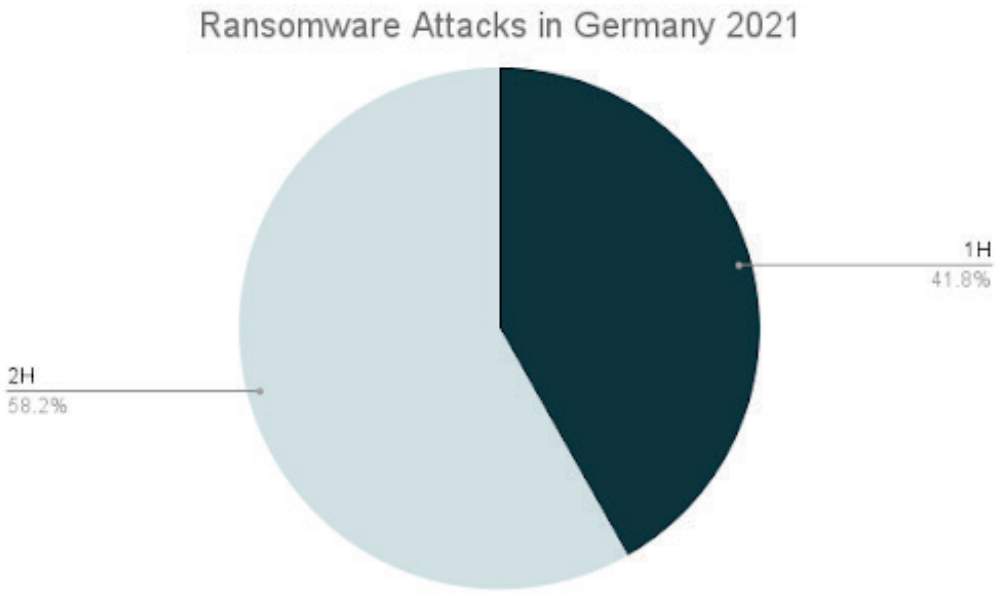

그림 9: 2021년 독일에서 보고된 랜섬웨어 공격 (출처: Recorded Future)

또 한 가지 지적해야 할 점은 의료 기관, 학교 등 주목받는 분야에 대한 랜섬웨어 공격이 줄어들고 있는 반면 전반적인 랜섬웨어 공격은 여전히 증가하고 있는 것으로 보인다는 점입니다. 특히 제조업, 건설, 식품 및 농업 등 2021년 큰 타격을 입은 것으로 보이는 부문들은 추적하기도 더 어렵습니다.

특정 산업이 랜섬웨어 그룹의 표적이 되는 것이 아니라, 강력한 보고 체계 또는 사이버 보안 인프라가 없는 국가가 표적이 될 수 있습니다. Emsisoft의 분석가인 Brett Callow는 "우리 데이터에서는 (아직) 랜섬웨어 둔화의 조짐을 볼 수 없습니다. 하지만 미국의 주요 인프라에 대한 공격은 줄어들고 있습니다"라고 말합니다. 이는 2021년 하반기에 공격 증가세를 보인 프랑스와 독일의 상황과 일치합니다(또는 보고가 적극적으로 이루어졌다는 표시일 수 있음).

공격이 둔화되고 있다는 인식은 관측, 즉 옵저버빌리티(observability)의 일면에 국한된 것일 수 있습니다. 조직마다 랜섬웨어 발생에 대해 서로 다른 견해를 갖고 있으며 이로 인해 시야가 제한적일 수 있습니다. 공격 보고가 전반적으로 줄어들 수 있습니다. 프랑스에서 관찰된 랜섬웨어 공격에서 이를 확인할 수 있습니다.

Rieß-Marchive에 따르면 2021년 11월 말까지 프랑스에서 보고된 랜섬웨어 공격은 242건이었습니다. 반기별 내역을 보면 이 보고서의 다른 차트와 매우 유사합니다. 공격의 63%가 2021년 상반기에, 37%가 하반기에 발생했습니다.

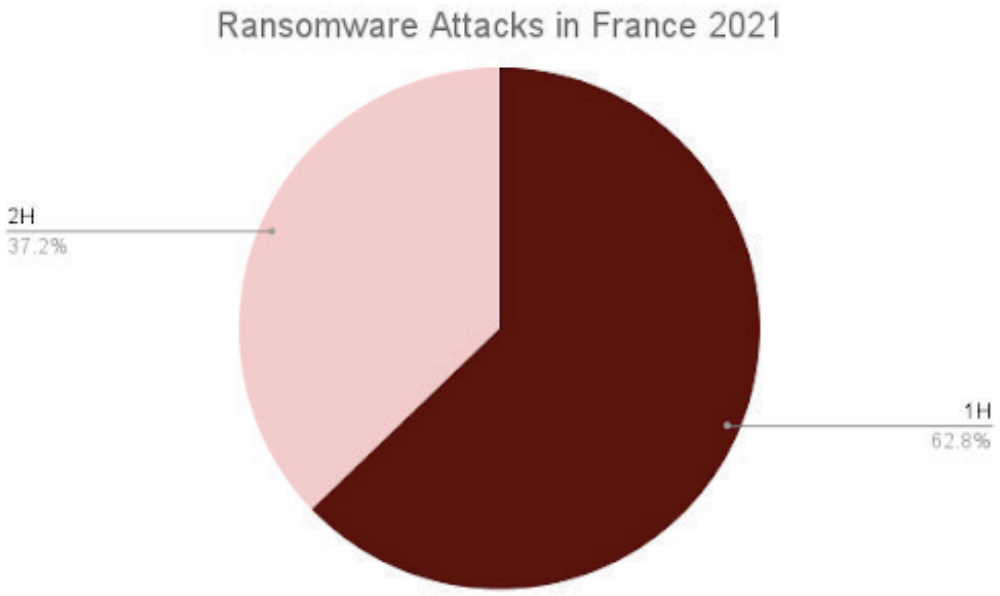

그림 10: 프랑스에서 보고된 랜섬웨어 공격 (출처: Recorded Future)

그러나 프랑스와 관련해서 검토해야 할 두 번째 데이터 세트가 있습니다. Cybermalveillance.gouv.fr은 사이버 범죄 피해자가 사건을 보고하고 도움을 받을 수 있는 기관입니다. Cybermalveillance.gouv.fr에 랜섬웨어 공격 관련 지원을 요청한 조직의 숫자(1,522)는 그림 11에 나와 있습니다.

그림 11에서 볼 수 있듯이 공개적으로 보고된 공격과 비공개적으로 보고된 공격 사이에는 큰 차이가 있습니다. 랜섬웨어 공격이 계속 증가할 수 있지만 공개적으로 보고되는 공격은 적습니다. 교육 기관이나 의료 기관과 같이 면밀히 추적되는 부문에서 데이터 왜곡이 발생하는 것도 바로 이 때문입니다. 랜섬웨어 그룹은 이러한 공격이 큰 관심을 끈다는 것을 알고 있으며, 이로 인한 불필요한 주목을 피하기 위해 상대적으로 덜 비난 받는 부문으로 대상을 옮겨가고 있습니다.

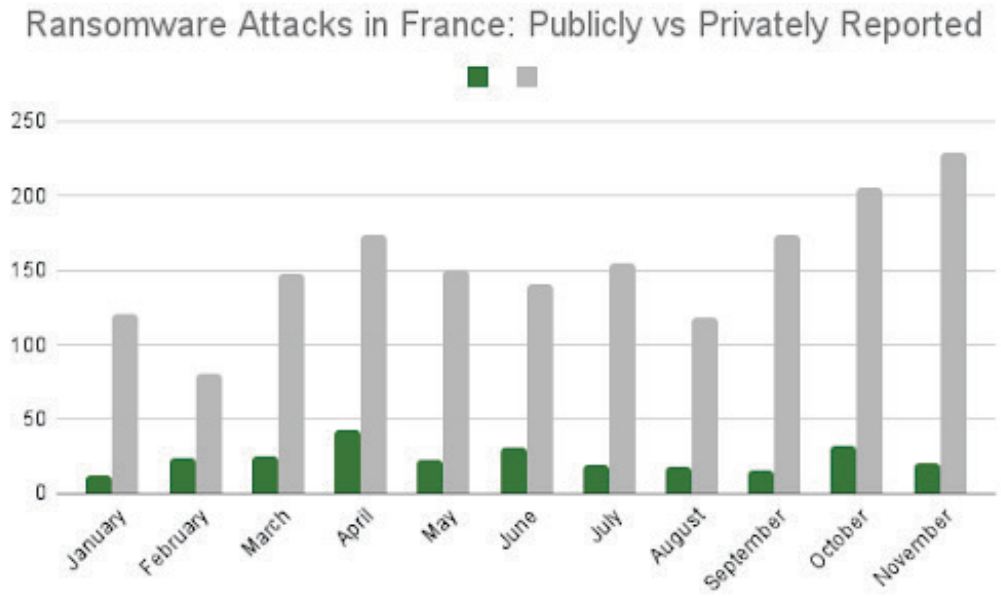

그림 11: 2021년 프랑스에서 공개적으로 보고된 랜섬웨어 공격과 비공개로 보고된 랜섬웨어 공격 (출처: Recorded Future)

간단히 말해서, 랜섬웨어 공격이 둔화되는 것처럼 보이지만 적어도 일부 부문에서는 전반적인 공격이 줄어들지 않을 수 있으며 감소세 여부는 랜섬웨어 공격면(attack surface) 어디를 보느냐에 따라 달라질 수 있습니다.

랜섬웨어 공격이 전반적으로 감소하고 있다면 그것은 강화된 법적 제재 때문만은 아닐 것입니다. 사이버 보험 회사가 보험 계약자에게 보험 갱신 전에 더욱 엄격한 사이버 보안 시행을 요구한다는 사례 증거가 있습니다. Gartner에 따르면 올해 기업 사이버 보안 지출이 12% 증가했습니다. 이처럼 법 집행 활동, 효과적인 사이버 보안 지출, 사이버 보험 회사의 엄격한 통제가 복합적으로 결합되어 공격 감소를 가져올 수 있습니다.

이것은 예비 데이터지만 주목할만한 추세이며, 레코디드 퓨처는 계속해서 모니터링하고 업데이트할 것입니다.