Akamai

인터넷 보안 현황 보고서
09권 | 04호

멈추지 않는 랜섬웨어

APJ 스냅샷

Akamai

목차

보고서의 핵심 인사이트

APJ 스냅샷은 대규모 랜섬웨어 SOTI 보고서인 멈추지 않는 랜섬웨어: 진화하는 악용 기술과 활발한 제로데이 공격(영어로만 제공됨)과 함께 제공되는 자료입니다. 랜섬웨어 그룹의 공격 트렌드, 방법론, 기법에 대한 자세한 분석, 공격 단계에 대한 설명과 기업을 보호할 수 있는 솔루션 및 권장 사항, 연구 방법론은 SOTI 보고서를 참조하시기 바랍니다.

개요

공격자들이 끊임없이 공격 기법을 계속 발전시키고 새로운 공격 기법을 도입하며, 공격표면을 확장하고 보안 예산이 부족하다는 점을 이용하고 있기 때문에 랜섬웨어는 기업에 지속적으로 막대한 피해를 입히며 피해 기업도 증가하고 있습니다. 대표적인 랜섬웨어 그룹과 이들의 공격 성공률이 높아지고 있다는 사실은 이런 위험한 트렌드의 여파를 잘 보여줍니다. APJ의 경우 2021년 4분기와 2022년 4분기 사이에 피해 기업 수는 50% 증가했고, 2022년 1분기와 2023년 1분기를 비교했을 때 피해 기업 수는 전년 동기 대비 204% 증가했습니다.

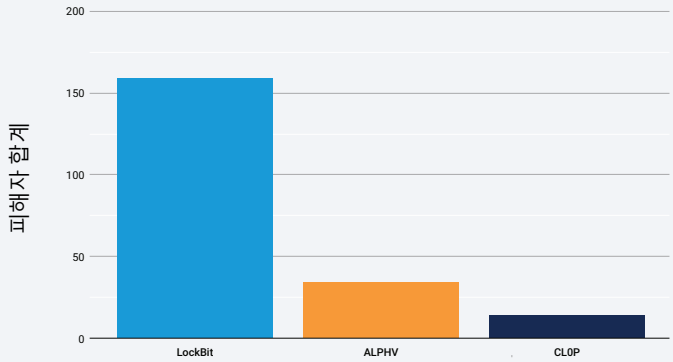
이번 APJ 스냅샷에서는 이와 같이 확장되는 위협에 대한 보다 효율적인 방어 전략과 리스크 관리를 위한 인사이트를 추가적으로 살펴봅니다.

- 2021년 10월부터 2023년 5월까지 LockBit는 랜섬웨어 분야를 지배했고 CL0P는 취약점을 공격적으로 악용하면서 증가세를 보였습니다. 공격 방식이 피싱에서 제로데이 및 원데이 취약점을 광범위하게 악용하는 것으로 변화하면서 피해자 수도 급증했습니다.
- 글로벌 수치와 마찬가지로 제조업계의 피해자가 가장 많았고 비즈니스 서비스가 그 뒤를 이었습니다
- 랜섬웨어 피해자 대부분은 매출이 미화 5천만 달러 이하인 작은 규모의 기업입니다. 그러나 가장 큰 규모의 기업도 공격을 받았습니다.

랜섬웨어 그룹 활동을 주도하는 LockBit

랜섬웨어에 대한 인식이 확산되고 랜섬웨어에 대처할 수 있는 툴 및 모범 사례가 많이 존재함에도 불구하고, APJ에서 랜섬웨어 피해 기업 수는 2021년 4분기와 2022년 4분기 사이에 50% 증가했으며, 2022년 1분기와 2023년 1분기를 비교하면 피해 기업의 수는 전년 동기 대비 204% 증가했습니다. 글로벌 보고서의 데이터 결과와 마찬가지로 2021년 10월 1일부터 2023년 5월 31일 사이에 피해자를 대상으로 한 공격의 대부분은 APJ 공격의 51%를 차지한 LockBit였으며 이와 더불어 ALPHV와 CL0P가 상위 3대 공격에 포함됐습니다(APJ 그림 1).

APJ: 피해자 수를 기준으로 한 상위 3대 랜섬웨어 그룹
2021년 10월 1일~2023년 05월 31일



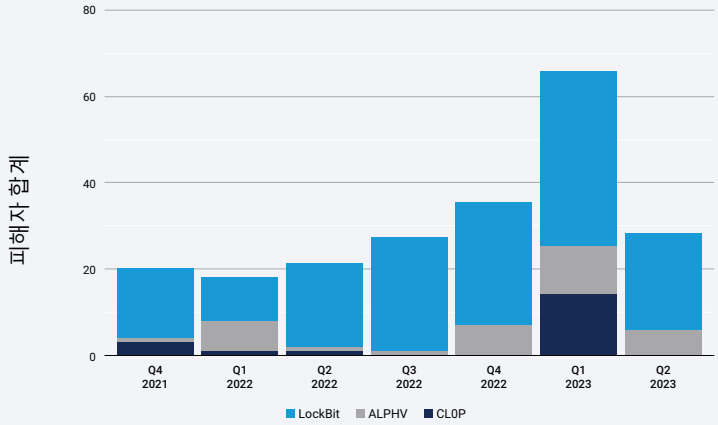
APJ 그림 1: APJ 랜섬웨어 공격의 피해를 입은 기업 대부분은 LockBit, ALPHV, CL0P의 공격을 받았습니다.

분기별 분석

LockBit가 확산되는 가운데 CL0P 랜섬웨어의 활동 역시 2021년 4분기부터 2022년 2분기까지 상당히 활발하게 이어졌습니다. 그러다 2023년 1분기에 급증하면서 APJ에서 세 번째로 활발한 랜섬웨어 그룹의 위치로 올라섰고 ALPHV의 자리를 위협했습니다(APJ 그림 2). CL0P의 활동이 급증한 이유는 진입 지점으로서 다양한 제로데이 취약점을 이용했기 때문으로 볼 수 있습니다. 지난 6개월 동안 공격 방식이 피싱에서 취약점 악용으로 변화하면서 피해자 수가 크게 증가하고 있습니다. 이 보고서를 작성하는 2023년 2분기*에는 일부 데이터만 사용할 수 있었습니다. 2023년 5월 31일 기준으로 CL0P 공격이 등록되지 않았는데 이는 2023년 1분기가 비정상임을 나타냅니다. 그러나 CL0P는 2023년 6월 MOVEit 취약점을 악용하면서 더 많은 피해자를 발생시켰는데 APJ의 몇몇 기업이 여기에 포함되었습니다.

*2023년 2분기는 2023년 5월 31일까지의 데이터만 포함하기 때문에 전체 분기를 반영하지 않습니다.

APJ: 피해자 수를 기준으로 한 상위 3대 랜섬웨어 그룹
분기별: 2021년 10월 1일~2023년 05월 31일

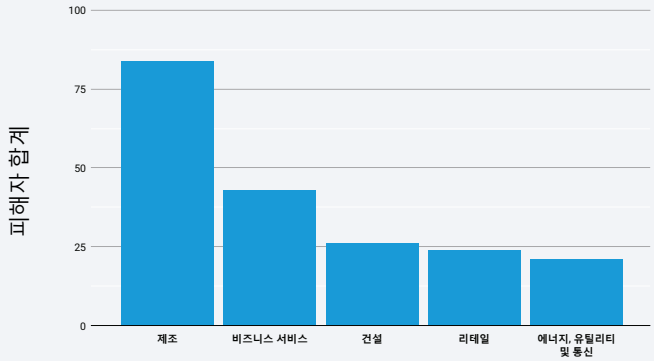


APJ 그림 2: APJ의 상위 3개 랜섬웨어 그룹의 분기별 피해자 수를 비교한 결과: LockBit, ALPHV, CL0P

위험에 처한 주요 업계

APJ에서 랜섬웨어의 위험에 노출된 상위 5대 핵심 업계는 제조, 비즈니스 서비스, 건설, 리테일, 에너지입니다. 이는 글로벌 기준으로 교육업계가 5위를 차지한 것을 제외하고는 글로벌 트렌드와 전반적으로 일치합니다. 또한 작년 글로벌 랜섬웨어 보고서에서 제조와 비즈니스 서비스가 1위와 2위를 차지했던 것과 대체로 일치합니다. 당시에는 Conti 랜섬웨어 그룹의 공격을 받았습니다. Conti가 사라진 후 빈 자리를 LockBit가 차지했습니다. 또한, 이전 DNS 보고서인 슈퍼 하이웨이 공격: 악성 DNS 트래픽 심층 분석에서 가장 많이 영향을 받은 업계와도 겹치는 부분이 있는데 이는 악성 C2(Command and Control) 트래픽과 랜섬웨어 공격 사이의 연관성을 반영합니다.

APJ: 랜섬웨어 그룹별 피해자 수 기준 상위 5대 업계
2021년 10월 1일~2023년 05월 31일



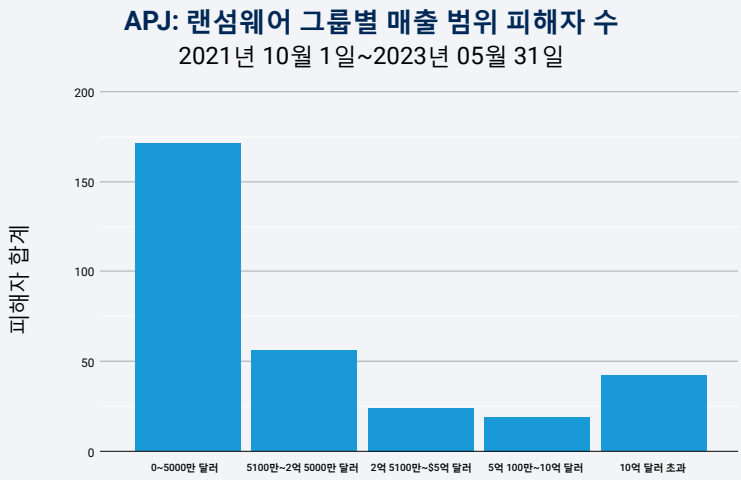
APJ 그림 3: 제조업계는 APJ에서 랜섬웨어 공격의 피해를 입은 기업의 수가 가장 많습니다.

*2023년 2분기는 2023년 5월 31일까지의 데이터만 포함하기 때문에 전체 분기를 반영하지 않습니다.

또한 LockBit는 특정 업계만 공격하지 않습니다. LockBit는 APJ의 모든 업계에서 가장 널리 퍼진 랜섬웨어로, 제조업에서 60%, 비즈니스 서비스에서 55.8%, 건설에서 57.7%, 리테일에서 45.8%의 공격 비율을 차지했습니다. LockBit가 공격의 28.6%를 차지하는 에너지 분야에서도 나머지 공격은 여러 랜섬웨어 그룹으로 분산되어 있으며, 14.3% 이상을 차지하는 그룹은 없습니다.

ROI에 집중하는 랜섬웨어 그룹

기업 규모나 매출과 관계없이 모든 기업은 랜섬웨어 공격의 위험에 노출되어 있습니다. 그러나 전 세계적인 트렌드를 반영하듯, 데이터에 따르면 공격자들은 APJ의 소규모 기업에 대한 공격을 성공적으로 시작했음을 보여줍니다(APJ 그림 4). 싱가포르 사이버 보안국의 보고서에 따르면 싱가포르에서 보고된 랜섬웨어 피해자의 대부분은 제조 및 리테일 분야의 중소기업이었습니다. 소규모 기업은 랜섬웨어의 위험에 대처할 수 있는 보안 리소스가 제한되어 있어 랜섬웨어에 더 취약하고, 침투하기 쉽고, 몸값을 지불할 여력이 있는 것으로 추정됩니다. 동시에 대기업도 공격을 받고 있으며, 연구에 따르면 피해 기업의 매출이 높을수록 몸값도 더 많이 지불하는 것으로 나타났습니다.



APJ 그림 4: APJ의 랜섬웨어 피해자 대부분은 매출이 최대 미화 5천만 달러인 기업입니다.

> 기업 규모나 매출과 관계없이 모든 기업은 랜섬웨어 공격의 위험에 노출되어 있습니다.

APJ 스냅샷 결론

랜섬웨어는 기업에 지속적으로 큰 피해를 끼치고 있습니다. 전 세계 및 지역 정부는 위협에 대응하고 보안 담당자가 조직을 보호하는 데 도움이 될 수 있는 기술을 강조하기 위해 연합 전선을 형성하고 있습니다. 호주, 인도, 일본 외무장관과 미국 국무장관은 성명을 발표해 랜섬웨어가 국가 안보와 모든 산업 부문에 미치는 영향을 시급히 완화하고, 기업이 사이버 보안 역량을 강화하고 복원력을 구축할 수 있도록 지원하는 프로그램을 시행하겠다는 약속을 강조했습니다. 올해 초 호주가 의장을 맡은 국제 랜섬웨어 대응 태스크포스는 사이버 위협 인텔리전스 공유 등 랜섬웨어의 확산과 영향에 대응하기 위해 36개 회원국과 EU 간의 협력을 강화하기 위해 설립되었습니다. 2022년 10월, 싱가포르는 점점 더 증가하는 랜섬웨어 공격으로부터 기업과 중요 인프라를 방어하기 위해 여러 정부 기관으로 구성된 최초의 기관 간 태스크포스를 구성했습니다.

규제 당국이 사이버 보안 표준을 강화하기 위한 이니셔티브와 정책을 시행함에 따라, 해당 지역의 보고 요구사항을 확인해 플레이북 및 위기관리 계획에 포함시키고, 멀티레이어 방어를 활용해 리스크를 방어할 기회를 파악해야 합니다.

자세한 내용은 글로벌 랜섬웨어 SOTI 보고서 멈추지 않는 랜섬웨어: 진화하는 악용 기술과 활발한 제로데이 공격을 확인하세요.

방법론

랜섬웨어 데이터

이 보고서에서 사용된 랜섬웨어 데이터는 약 90개 랜섬웨어 그룹의 유출 사이트에서 수집한 것입니다. 이들 그룹은 일반적으로 타임스탬프, 피해자 이름, 피해자 도메인 등 공격에 대한 세부 정보를 공개합니다. 이런 정보는 각 랜섬웨어 그룹이 공개하고자 하는 내용에 따라 달라질 수 있다는 점에 유의해야 합니다. 이번 연구에는 보고된 공격의 성공 여부는 포함되지 않았습니다.

대신 보고된 피해자에 초점을 맞추었습니다. 그룹별로 피해자 수를 측정하고 분석했습니다. 이 피해자 데이터를 ZoomInfo에서 얻은 데이터와 결합해 위치, 매출 범위, 업계 등 각 피해자에 대한 추가 세부 정보를 파악했습니다.

모든 데이터는 2021년 10월 1일부터 2023년 5월 31일까지의 20개월 기간에 해당하는 자료입니다.

저자 소개

편집 및 작성

오리 데이비드
(Ori David)
바데트 트리비
(Badette Tribbey)
샬롯 펠리치아
(Charlotte Pelliccia)
랜스 로즈
(Lance Rhodes)

검토 및 주제별 기여

모쉬 코헨
(Moshe Cohen)
시란 게즈
(Shiran Guez)
오피르 하르파즈
(Ophir Harpaz)
루벤 코(Reuben Koh)
리차드 메우스
(Richard Meeus)
스티브 윈터펠드
(Steve Winterfeld)
막심 자보드치크
(Maxim Zavodchik)

데이터 분석

첼시 터틀(Chelsea Tuttle)

마케팅 및 출판

킴벌리 고메즈(Kimberly Gomez)
조지나 모랄레스 햄프(Georgina Morales Hampe)
쉬방기 사후(Shivangi Sahu)

더 많은 인터넷 보안 현황 보고서

지난 보고서를 읽고 Akamai의 다음 인터넷 보안 현황 보고서를 확인하세요.
akamai.com/soti

Akamai 위협 리서치 자세히 알아보기

최신 위협인텔리전스 분석, 보안 보고서, 사이버 보안 리서치를 확인하세요.
akamai.com/security-research

Akamai의 이 보고서의 데이터

이 보고서에 참조로 사용된 그래프와 차트의 고품질 버전을 확인하세요. Akamai가 제공한 소스라는 점이 정식으로 인정되고 Akamai 로고가 보존되는 경우 이러한 이미지를 무료로 사용 및 참조할 수 있습니다.
akamai.com/sotidata

Akamai 솔루션 자세히 알아보기

랜섬웨어에 대한 Akamai 솔루션을 자세히 살펴보려면 **보안 솔루션** 페이지를 참조하세요.

Akamai는 온라인 라이프를 지원하고 보호합니다. 전 세계 대표적인 기업들은 매일 수십억 명의 사람들의 생활, 업무, 여가를 지원할 디지털 경험을 구축하고, 전송하고, 보호하기 위해 Akamai를 선택합니다. Akamai Connected Cloud는 대규모 분산 엣지 및 클라우드 플랫폼으로 앱과 경험을 사용자와 더 가까운 곳에 배치하고 위협을 멀리서 차단합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com와 akamai.com/blog를 확인하거나 Twitter와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2023년 08월 발행.