중소벤처기업부 보도자료

보도시점 4.17.(금) 조간 < 4.16.(목) 12:00 >

국내 중소기업 대상 신규 랜섬웨어(Midnight, Endpoint) 범죄 확산에 따른 보안권고문 배포

- 중기부-경찰청-KISA, 신종 랜섬웨어 범죄방지 공동대응 -

중소벤처기업부(장관 한성숙, 이하 중기부), 경찰청(청장 직무대행 유재성), 한국인터넷진흥원(원장 이상중, Korea Internet & Security Agency, 이하 KISA)은 최근 국내 중소기업을 대상으로 한 신종 금품 요구 악성 프로그램 'Midnight(미드나이트)[Endpoint(엔드포인트)]' 감염 공격이 확인됨에 따라 관련 위협정보를 공개하고 각별한 주의를 당부했다.

※ 공격자는 '미드나이트', '엔드포인트' 2개 종류의 랜섬웨어를 유포 중

'Midnight(미드나이트)[Endpoint(엔드포인트)]' 랜섬웨어는 IT 시스템 구축·유지보수 업체를 먼저 침해한 뒤, 이를 통해 고객사를 감염시키는 방식을 사용하는 것이 특징이다. 피해자의 다수는 중소 제조업으로 확인되나, 유통·에너지·공공기관 등 분야의 피해도 확인되고 있어 전 업종의 주의가 필요한 상황이다.

이번 랜섬웨어 공격에 대한 합동 대응은 최근 대규모 해킹 등 정보통신망 침해범죄가 증가하고 있는 상황에서 사후 대응을 넘어 선제적 예방 중심의 대응이 필요하다는 판단에 따른 것이다. 경찰청은 사건 분석을 통해 확인한 정보를 토대로 피해 가능성이 높은 분야와 주요 위험 요소를 판별하였고, 범죄의 발생을 차단하기 위해 관계부처와 공동 대응체계를 구축했다.

특히 이번 권고문 배포는 수사 과정에서 위협 정보를 기반으로 부처간 협력을 통해 경찰청이 공식적으로 보안 권고를 발행하는 첫 사례이다.

□ 정보기술(IT) 유지보수 업체를 공격한 뒤 고객사로 확산

경찰청과 KISA의 분석에 따르면 공격자는 IT 구축·유지보수 업체를 대상으로 견적 문의, 입사 지원, 컨설팅 요청 등으로 위장한 악성 이메일을 발송해 내부 시스템에 침투한다. 피해자가 첨부파일을 실행할 경우 원격제어 악성코드가 설치돼 내부 정보와 계정 정보가 외부로 유출된다.

이후 공격자는 탈취한 정보를 활용해 해당 업체를 사칭한 악성 이메일을 고객사에 재차 발송하고, 이를 통해 고객사 내부 시스템 접근 권한을 확보한 뒤 랜섬웨어를 유포하는 것으로 나타났다.

특히 이번 랜섬웨어는 단순히 파일 암호화에 그치지 않고, 내부 데이터를 사전에 탈취한 뒤 금전을 요구하는 '이중 탈취형' 공격 방식을 사용하는 것으로 확인됐다. 이는 공격자가 데이터를 외부로 유출한 뒤 공개하겠다고 협박하는 방식으로 피해 기업의 협상 부담을 가중하는 전략이다.

□ 랜섬웨어 범죄 예방과 피해 최소화를 위한 보안 권고문 배포

경찰청과 KISA는 이번 랜섬웨어 위협에 선제적으로 대응하기 위해 공격 기법과 악성 전자우편 유형, 범죄 예방 및 대응 방안을 포함한 보안권고문을 마련해 관계기관과 기업, C-TAS 회원사에 배포했다.

※ C-TAS(Cyber Threat Analysis & Sharing, 사이버 위협정보 분석·공유) :
KISA에서 운영중인 국내 최대 규모의 사이버 위협정보 분석·공유 시스템(회원사 약 5천여개)

랜섬웨어는 초기 침투를 차단하는 것이 가장 효과적인 대응 방법으로, △출처가 불분명한 이메일 및 첨부파일 실행 금지 △VPN·원격접속 등 외부 접근 통제 △다중인증 적용을 통한 계정관리 강화 △안전한 백업체계 활성화 등 기업들의 기본적인 보안 수칙 준수가 무엇보다 중요하다. 특히 랜섬웨어 감염이 의심될 경우 공격자와 직접 접촉하지 말고 경찰과 KISA에 신속하게 신고해야 한다.

중기부는 중소기업을 대상으로 보안권고문을 스마트공장 보급사업, R&D 지원사업 등 기존 지원사업을 통해 확보된 기업 데이터베이스를 활용하여 보다 신속하고 체계적으로 전파할 계획이다. 또한, 지원사업별 설명회, 간담회, 교육 프로그램 등 중소기업이 참여하는 다양한 정책 접점을 활용하여 경찰청 및 KISA와 협업한 보안 교육을 연중 지속적으로 실시할 예정이다.

특히 스마트공장 도입기업 등 디지털 전환 제조기업과 스마트제조기술 기업을 중심으로 맞춤형 보안 교육을 강화하고, 이를 기반으로 우수 사례 확산을 통해 중소기업 전반의 사이버보안 대응 역량을 단계적으로 제고해 나갈 방침이다.

경찰청은 현재 'Midnight(미드나이트)[Endpoint(엔드포인트)]' 랜섬웨어와 관련된 공격을 수사하고 있으며, 추가 위협정보를 관계기관 및 기업에 신속하게 공유할 계획이다. 아울러 향후 유사한 랜섬웨어 공격에 대비해 민·관 협력체계를 강화하고 대응 역량을 지속적으로 높혀 나갈 방침이다.

붙 임 보안권고문 1부

담당 부서	경찰청 사이버테러대응과	책임자	경정	이승운	(02-3150-0053)
		담당자	경정	김영운	(02-3150-1459)
	중소벤처기업부 제조혁신과	책임자	과장	양승욱	(044-204-7260)
		담당자	서기관	기정희	(044-204-7271)
	한국인터넷진흥원 랜섬웨어대응팀	책임자	팀장	김기문	(02-405-4960)
		담당자	수석	조정식	(02-405-4963)