경찰청 사이버 보안권고문

국내 중소기업을 대상으로 한 신규 랜섬웨어 MIDNIGHT(ENDPOINT) 위협정보 및 권고사항 안내

개요

경찰청 사이버테러대응과는 최근 새롭게 관찰된 *Midnight(Endpoint)* 랜섬웨어와 관련된 위협정보와 권고사항을 배포합니다. *Midnight(Endpoint)* 랜섬웨어를 유포하는 범죄 그룹은 중소기업의 IT 시스템 구축·유지보수 업체를 공격하여 정보를 탈취하고, 이를 통해 고객사인 중소기업을 대상으로 랜섬웨어를 유포하는 것으로 확인되었습니다.
경찰청은 공격자의 악성 이메일 정보를 공유함으로써 *Midnight(Endpoint)* 랜섬웨어를 예방하고 피해를 최소화하고자 합니다.

공격의 특성과 기법

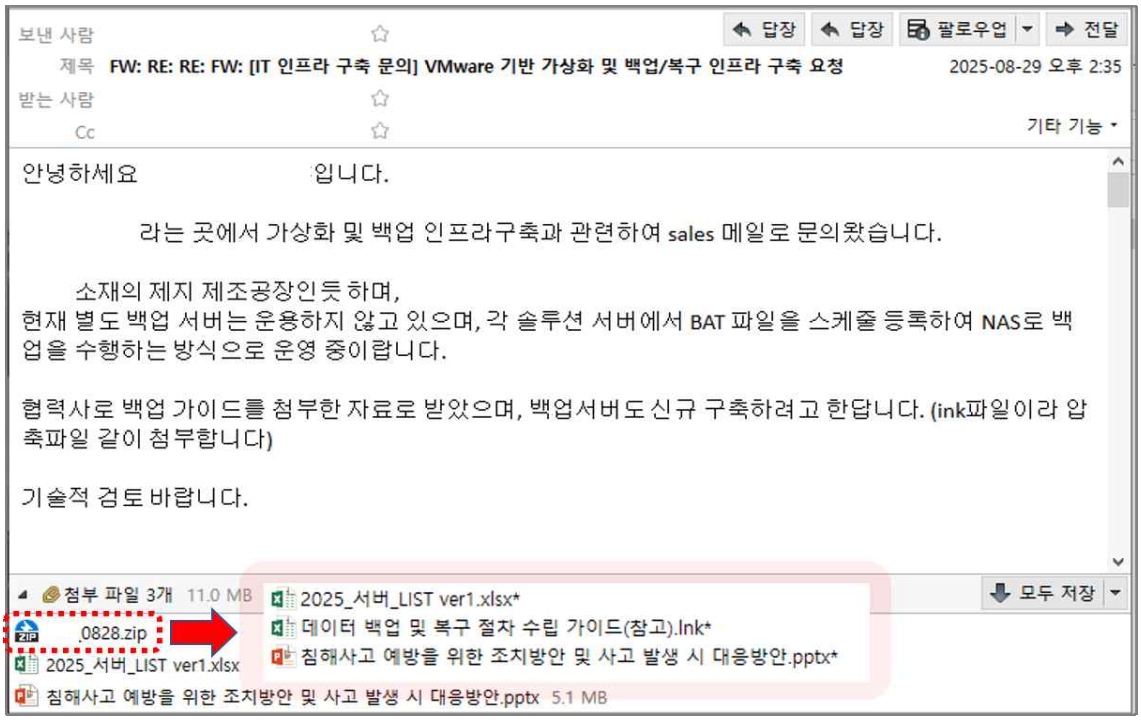
'25년 말부터 '26년 현재까지 *Midnight(Endpoint)* 랜섬웨어로 인해 다수의 국내 중소기업이 피해를 입은 것으로 확인되었습니다. 해당 랜섬웨어는 중소기업의 IT 시스템 구축·유지보수 업체와 중소기업을 대상으로 한 악성 이메일을 통해 유포되고 있으며, 랜섬웨어 감염과 동시에 정보 유출을 병행하여 피해자를 협박하는 '이중 탈취형(Double Extortion)' 공격을 진행합니다.

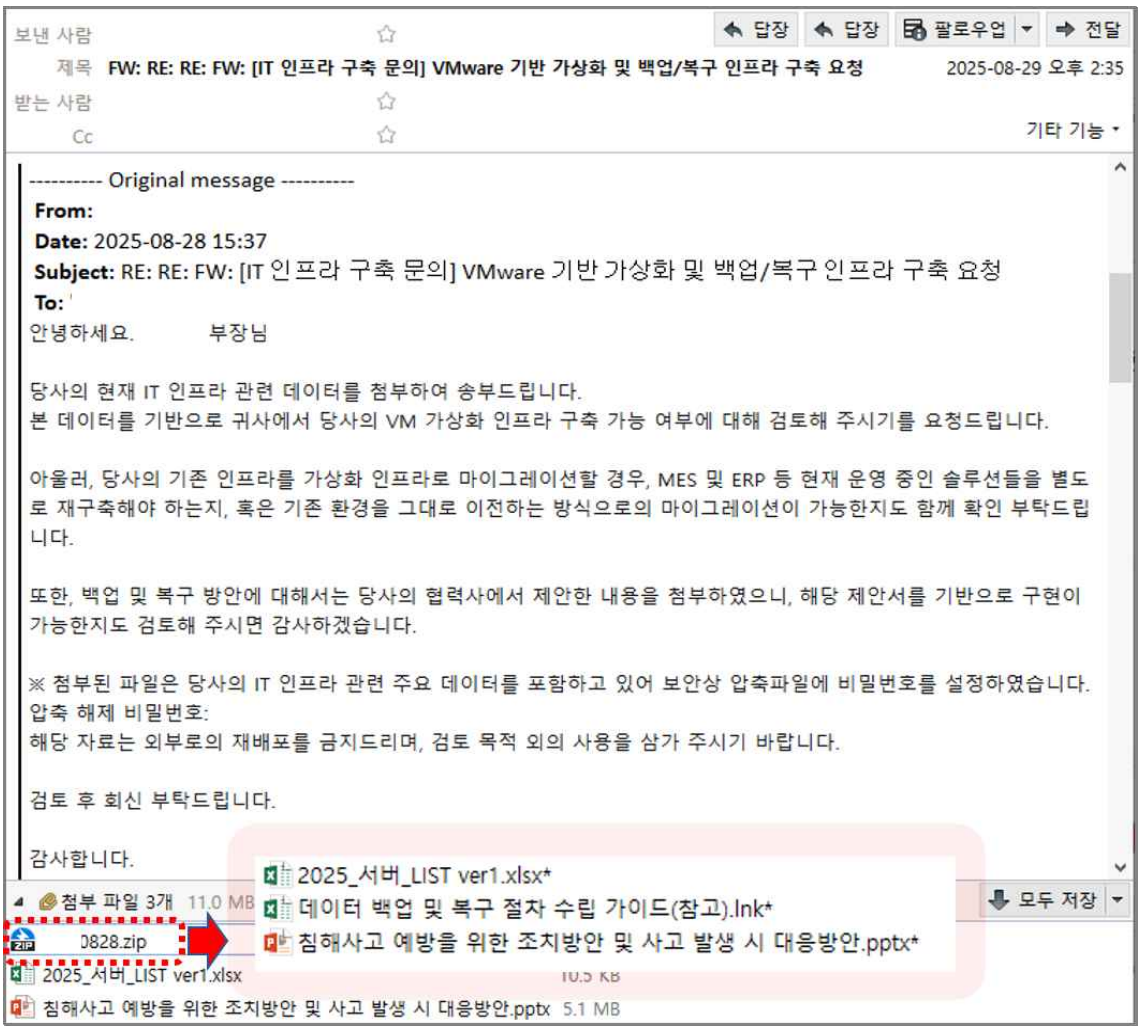
공격자는 (1) IT 시스템 구축·유지보수 업체를 대상으로 견적 문의 등을 위장한 악성 이메일을 유포하는 방식으로 고객사 정보를 탈취하고, (2) 이 업체를 사칭한 악성 이메일을 고객사에 재차 발송하여 접근권한을 탈취하는 방식으로 고객사 서버에 무단 접속 후 랜섬웨어를 유포합니다. 랜섬웨어에 감염된 경우 복호화 대가로 금전(가상자산)을 요구하는데, 통상 기업 매출액의 1% 수준을 제시하는 것으로 확인됩니다.

주요 피해 대상은 중소기업의 가상화 구축, 서버 등을 납품하는 IT 시스템 구축·유지보수 업체와 이 업체들의 고객사인 중소기업입니다. 공격은 주로 제조업을 표적으로 하고 있지만, 유통·에너지·공공기관 등 분야의 피해 사례도 있는 만큼 모든 업종의 주의가 필요합니다.

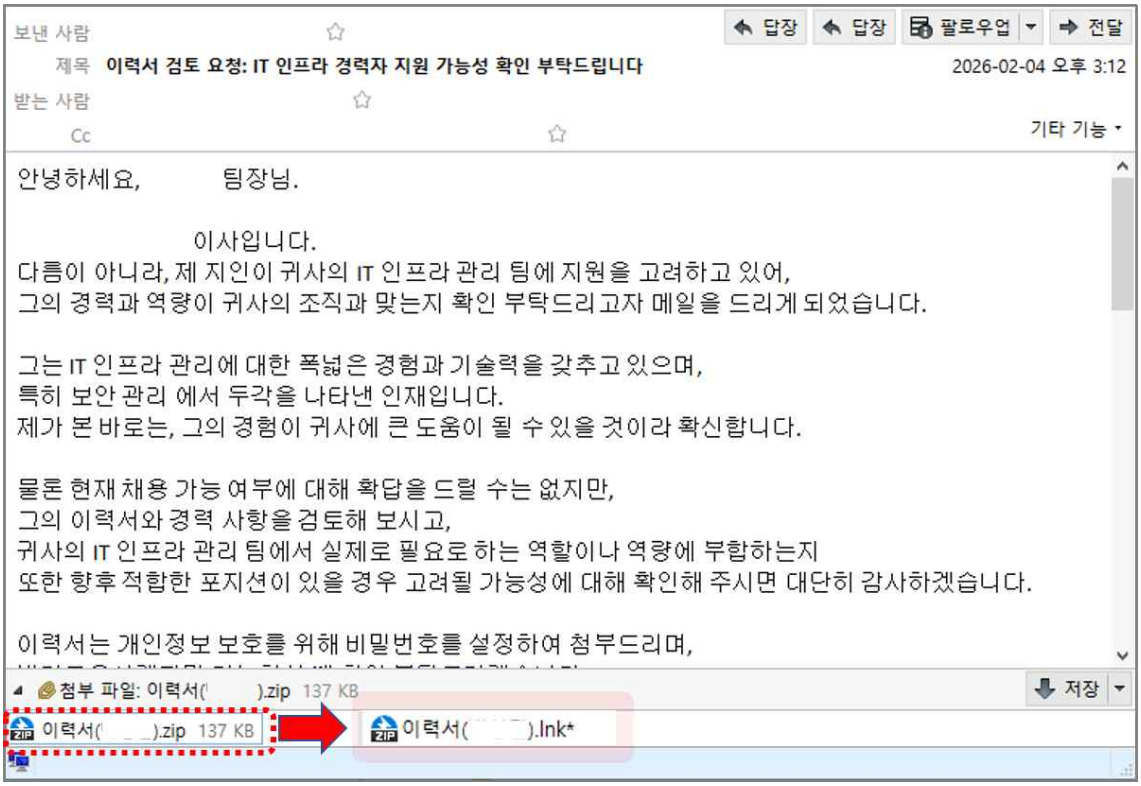
악성 이메일 예시

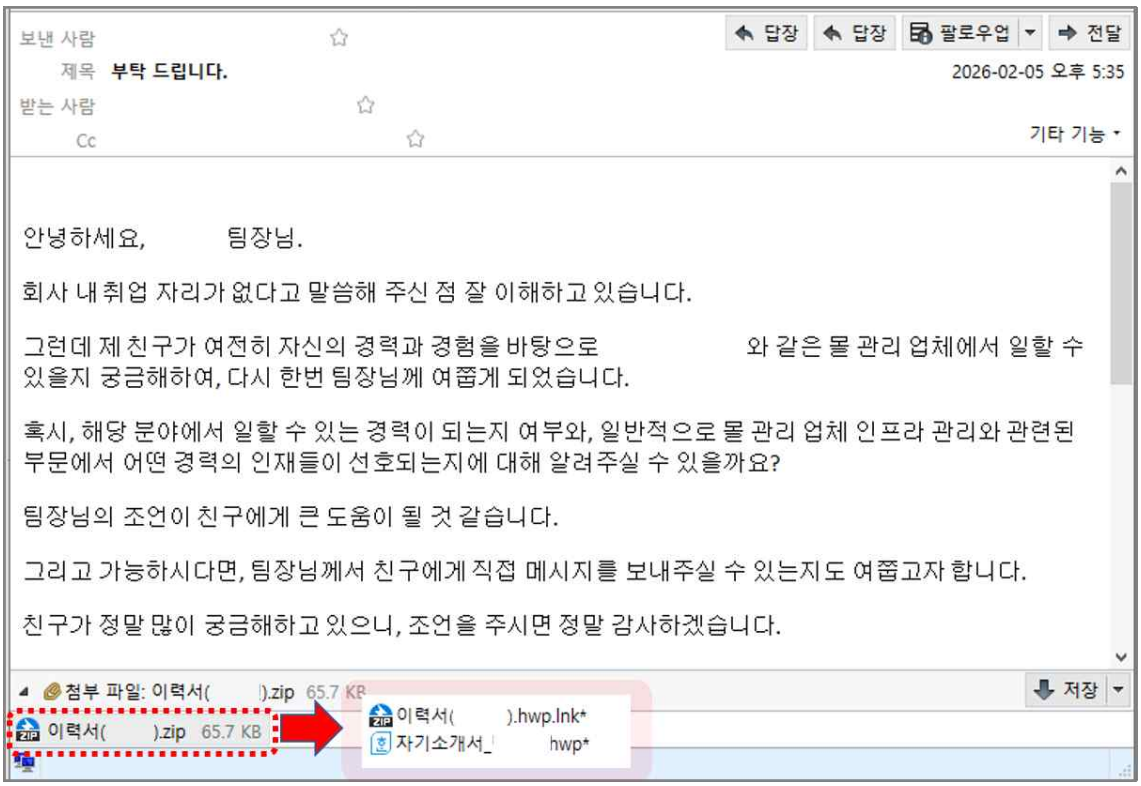
(1) 인프라 구축 요청



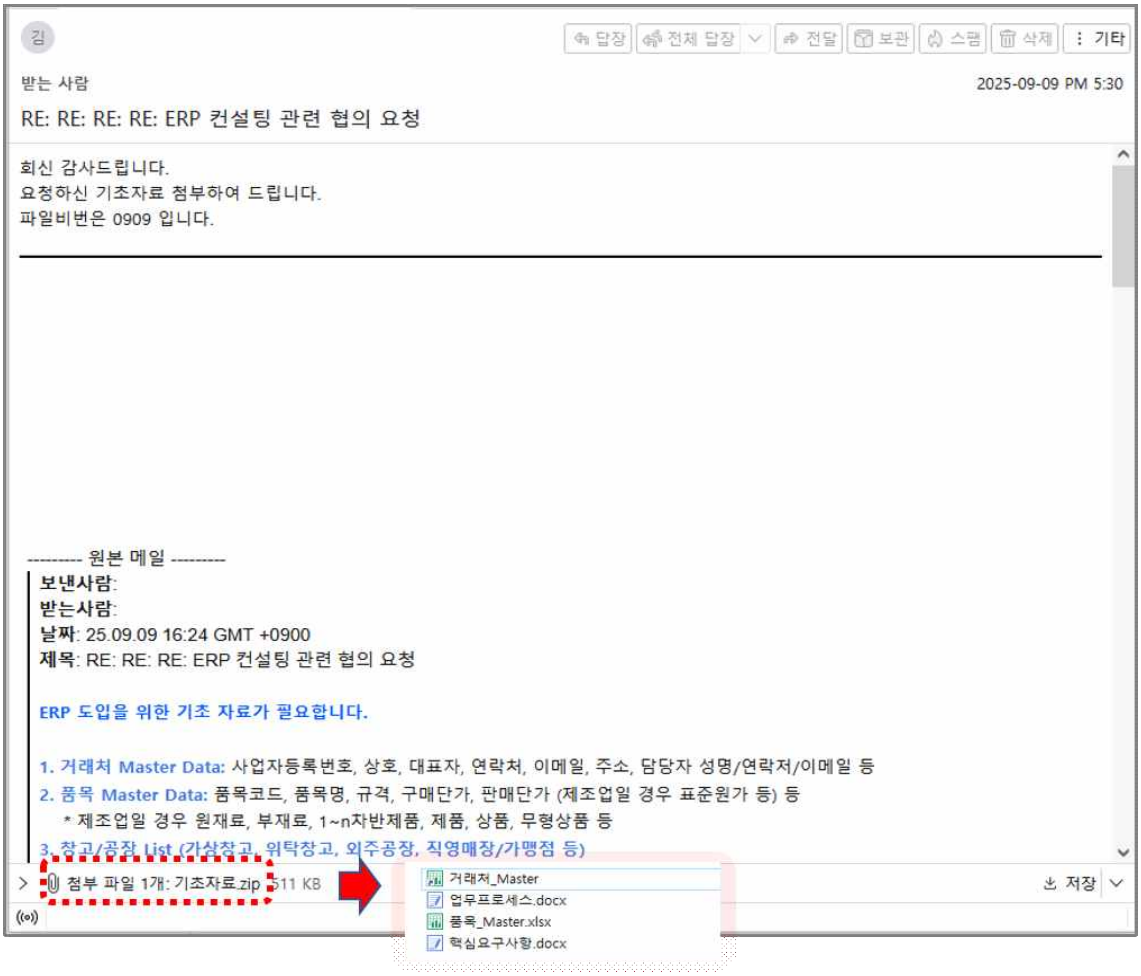


(2) 입사 지원 문의

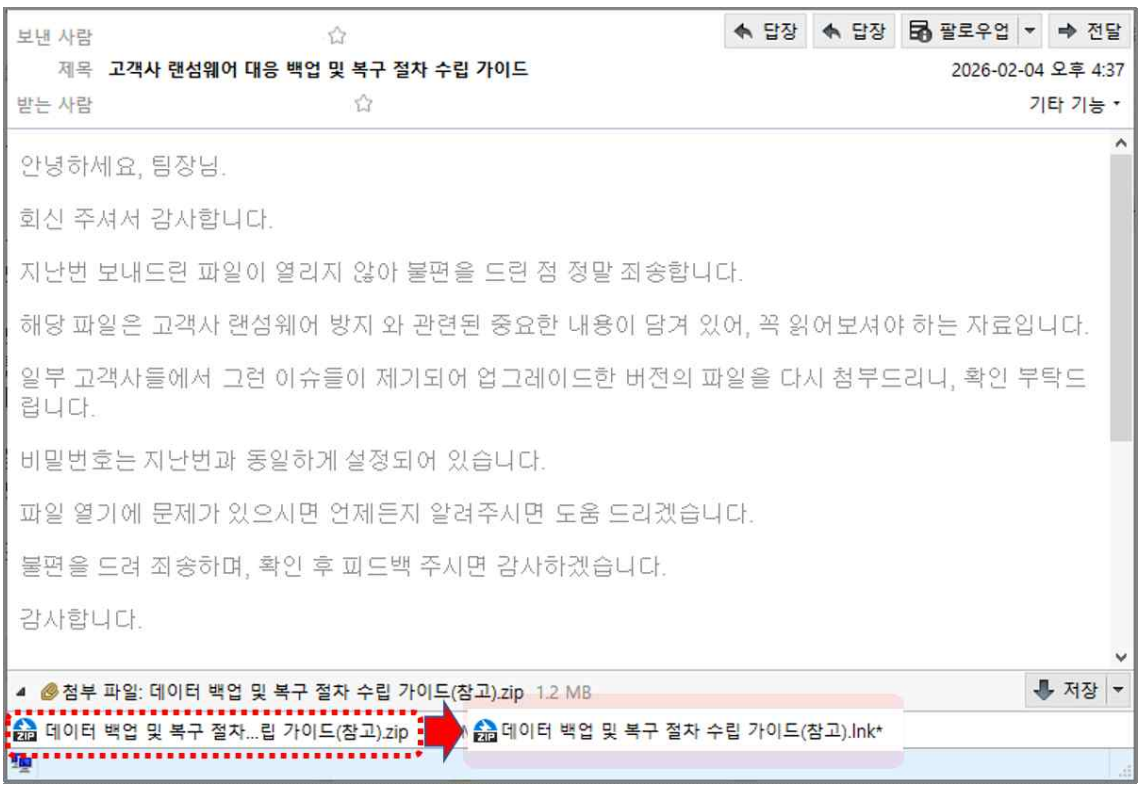

보낸 사람
답장
답장
팔로우업
전달
제목 이력서 검토 요청: IT 인프라 경력자 지원 가능성 확인 부탁드립니다
2026-02-04 오후 3:12
받는 사람
Cc
기타 기능
안녕하세요, 팀장님.
이사입니다.
다름이 아니라, 제 지인이 귀사의 IT 인프라 관리 팀에 지원을 고려하고 있어,
그의 경력과 역량이 귀사의 조직과 맞는지 확인 부탁드리고자 메일을 드리게 되었습니다.
그는 IT 인프라 관리에 대한 폭넓은 경험과 기술력을 갖추고 있으며,
특히 보안 관리 에서 두각을 나타낸 인재입니다.
제가 본 바로는, 그의 경험이 귀사에 큰 도움이 될 수 있을 것이라 확신합니다.
물론 현재 채용 가능 여부에 대해 확답을 드릴 수는 없지만,
그의 이력서와 경력 사항을 검토해 보시고,
귀사의 IT 인프라 관리 팀에서 실제로 필요로 하는 역할이나 역량에 부합하는지
또한 향후 적합한 포지션이 있을 경우 고려될 가능성에 대해 확인해 주시면 대단히 감사하겠습니다.
이력서는 개인정보 보호를 위해 비밀번호를 설정하여 첨부드리며,
첨부 파일: 이력서( ).zip 137 KB
저장
이력서( ).zip 137 KB
이력서( ).lnk*


보낸 사람
답장
답장
팔로우업
전달
제목 부탁 드립니다.
2026-02-05 오후 5:35
받는 사람
Cc
기타 기능
안녕하세요, 팀장님.
회사 내 취업 자리가 없다고 말씀해 주신 점 잘 이해하고 있습니다.
그런데 제 친구가 여전히 자신의 경력과 경험을 바탕으로 와 같은 몰 관리 업체에서 일할 수
있을지 궁금해하여, 다시 한번 팀장님께 여쭙게 되었습니다.
혹시, 해당 분야에서 일할 수 있는 경력이 되는지 여부와, 일반적으로 몰 관리 업체 인프라 관리와 관련된
부문에서 어떤 경력의 인재들이 선호되는지에 대해 알려주실 수 있을까요?
팀장님의 조언이 친구에게 큰 도움이 될 것 같습니다.
그리고 가능하시다면, 팀장님께서 친구에게 직접 메시지를 보내주실 수 있는지도 여쭙고자 합니다.
친구가 정말 많이 궁금해하고 있으니, 조언을 주시면 정말 감사하겠습니다.
첨부 파일: 이력서( ).zip 65.7 KB
저장
이력서( ).zip 65.7 KB
이력서( ).hwp.lnk*
자기소개서_ hwp*

(3) 컨설팅 문의



(4) 보안 가이드라인 배포



권고사항

경찰청은 랜섬웨어 범죄를 예방하고 감염시 피해를 최소화하기 위해 다음과 같은 대응 조치를 권고합니다.

- 이메일 보안 강화
  - 출처가 불분명한 이메일 및 첨부파일 실행 금지
  - 이메일 수신시 출처가 불분명한 사이트 주소 클릭 자제
  - 신뢰관계자간 이메일 첨부파일 재확인
  - 이메일 보안솔루션 사용하여 유해성 확인 및 악성 이메일 차단
- 외부 접속 관리 강화
  - 인프라 노출 최소화 및 가상 인프라 노출 감소
  - 원격접속(RDP, VPN) 접근통제 강화
  - 유지보수를 위한 원격제어 접근관리 철저
  - 공정제어나 경영지원시스템을 원격 관리하는 PC의 인터넷을 차단하고 별도 분리하여 설치·운영
- 계정 보호 및 관리 강화
  - 주요 시스템 접속에 다중인증(MFA) 적용
  - 소프트웨어 설치 시 기본 비밀번호 및 자격증명 제거, 비밀번호 주기적 변경
  - 고객사 정보, 개인정보 암호화 및 별도 관리
- 백업 관리 강화
  - 오프사이트(Off-Site) 또는 오프라인 백업 구축
  - 중요 데이터 네트워크와 분리된 별도 백업 수행
- NAS 등 사용한 중요 자료 공유 금지
- 소프트웨어 설치 제한 및 PowerShell 및 스크립트 실행 통제
- 백신 및 EDR/XDR 솔루션 운영 및 최신 업데이트 상태 유지

랜섬웨어 대응을 위한 보다 자세한 조치 및 권고사항은 한국인터넷진흥원(KISA) 보호나라(www.boho.or.kr)에서 제공하는 가이드라인을 통해 확인할 수 있습니다.

범죄 신고 및 정보보호 서비스 안내

랜섬웨어 공격을 탐지하였거나 본 경보문 내용과 관련된 정보를 보유하고 있는 경우, 즉시 경찰청에 신고해주시기 바랍니다. 범죄 신고는 가까운 경찰서나 시도청 민원실을 방문하거나, 전화(112) 또는 인터넷 사이버범죄신고시스템(www.ecrm.police.go.kr)으로도 가능합니다.

한국인터넷진흥원(KISA)은 침해사고 신고(www.boho.or.kr)와 더불어 보안관리 인력이 부족한 중소기업을 대상으로 홈페이지 보안강화, 보안상담 등 다양한 정보보호 서비스를 제공하고 있습니다.

기타

본 문서는 한국인터넷진흥원(KISA)과 공동으로 작성되었으며, **TLP:CLEAR**로 지정되어 있습니다. 문서에 기재된 정보는 공개정보로 공유·배포할 수 있습니다.

발행일자 | 2026. 4. 16
발행부처 | 경찰청 사이버테러대응과, 한국인터넷진흥원 랜섬웨어대응팀
연 락 처 | ctrd@police.go.kr, stopransom@kisa.or.kr