A신용보증기업 랜섬웨어 감염으로 전산서비스 전면 중단 전세·사업대금보증 지연원인 GUNRA 랜섬웨어

1. 7월14일 00:40, A신용보증기업에서
   데이터베이스 내 이상징후를 통해 감염사실 인지,
   사흘간 전세·사업대금 등 보증관련 서비스 전면마비.

2. 7/17일 10:00, 복구완료 및 보증서 발급업무 정상화.
   피해복구까지 약 81시간 소요.

3. **GUNRA 랜섬웨어**는 탐지 우회 및 은닉에 특화됨.
   백신 프로세스 강제종료, 보안솔루션 분석환경 실행회피.
   암호화 파일 복구 방해목적으로 볼륨 섀도우 복사본 삭제.

4. 은닉성이 강한 랜섬웨어 이므로
   일반적인 안티바이러스로는 탐지 불가하며
   행위기반 EDR 솔루션으로는 검출 및 격리 가능

1. GUNRA 랜섬웨어 특징

1) GUNRA는 올해 4월 등장한 신종 랜섬웨어 조직
의료, 전자, 부동산 등 산업군 대상으로 공격 수행

2) **이중 강탈** 랜섬웨어 기법을 통해
파일 위변조 및 정보유출, 데이터 판매로 수익을 취득.
개인수익 목적으로 공격을 수행하며,
국가 간 인프라테러 목적은 아닌 것으로 추측.

3) GUNRA 랜섬웨어는
탐지 우회 및 은닉기능을 탑재 함.
보안제품 우회를 위해 **백신 프로세스 강제종료,**
분석 솔루션 설치 환경에서는 **실행 회피,**
'Stopmarker' 파일 발견 시 **암호화 중단**
파일복구를 방해하기 위해
볼륨 섀도우 복사본 자체를 삭제 → 복구에 3일 소요

2. 침입 및 위변조 과정

침입	무작위 로그인을 통해 SSL-VPN 장비 침투하여 내부망 접속
은닉/탐지회피	APT 솔루션, 샌드박스, EDR 등 악성행위 분석 가능한 환경에서는 실행 회피 ‘StopMarker’ 발견 시 암호화 중단
권한획득 및 AV 강제종료	권한상승 후 백신 프로세스 강제종료
파일탐색 및 암호화	파일 용량에 따라 암호화 방식 세분화 • 1mb이하 : 전체 암호화 • 5mb 이하 : 1mb 용량만 암호화 • 5mb 이상 : 파일크기 7%씩 3청크 암호화
쉐도우 카피 삭제	볼륨 섀도우 복사본 삭제하여 암호화된 데이터 복구 불가
파일유출을 통한 이중갈취	몸값협상 매커니즘 보유 개인수익 목적 추정. (국가 간 인프라테러 목적 아닌 것으로 추측)

3. 대응 및 재발방지 방안

SSL-VPN 장비 침투를 통한 내부망 접속

- VPN **2-Factor 인증강화**
- VPN으로 내부망 접속 시
  논리적 망분리 경유하여 접속하도록 조치

PC 내 AV·EDR 솔루션 구축을 통해 보안성 강화

- **볼륨 섀도 복사본 삭제, 데이터 위변조 행위**
  엔드포인드 단에서 **실시간 탐지 및 차단**
- **데이터 백업**은 볼륨 섀도우 방식이 아닌
  실시간 백업을 통해 복구

GUNRA 랜섬웨어에 관한 상세내용을 원하실 경우,
소만사 악성코드 분석센터에서 직접 테스트하고 분석한
'악성코드 분석리포트'를 보내 드립니다.

신청방법 : privacy@somansa.com으로 자료요청
또는 영업담당자에게 직접 문의

SOMANSA

4. 참고자료

[소만사 악성코드 분석리포트] GUNRA 랜섬웨어
(상세 내용은 소만사 영업담당자에게 직접 문의)

A신용보증기업 해킹, 이렇게 당했다
https://www.boannews.com/media/view.asp?idx=138199

A신용보증기업 랜섬웨어, 최초 침투 경로는 'SSL-VPN' 로그인 횟수 제동 장치 없었다
https://www.boannews.com/media/view.asp?idx=138214&kind=1

韓 강타한 랜섬웨어 공격…사흘째 '시스템 장애'
https://www.ddaily.co.kr/page/view/20250716094144374 27?utm_source=chatgpt.com

A신용보증기업 마비 '그 밤의 악몽'…랜섬웨어에 속수무책 당했다
https://www.news1.kr/finance/general-finance/5847660