통신 제공업체 Black Basta 공격 격리 및 운영 복구

고객은 Unit 42®에 무단 액세스 범위를 파악하고 금액을 협상하여 위협을 근절할 것을 요청했습니다.

통신 제공업체 Black Basta 공격 격리 및 운영 복구

업종 통신 | 국가 미국

문제

이 고객은 13시간 동안 수만 대에 달하는 시스템의 파일을 암호화하고 중요 데이터를 유출하는 심각한 랜섬웨어 공격을 받았으며, 그 결과 비즈니스 운영의 50%가 중단되는 피해를 입었습니다. 고객은 Unit 42에 다음에 대한 도움을 요청했습니다.

- 위협을 격리하고 추가 데이터 유출을 방지합니다.
- 위협 행위자를 제거합니다.
- 근본 원인을 조사하고 비즈니스 운영 복구를 지원합니다.

결과

3일

50만개의 엔드포인트 환경에서 공격 벡터 파악

80% 감소

영향을 받은 데이터에 대한 전문가 협상

2일

위협 격리 및 비즈니스 운영의 연속성 보장

탁월한 결과를 위한 Unit 42의 엄격한 사고 대응 접근 방식

평가

고객은 기업 환경에서 암호화된 파일과 랜섬 메모를 확인했으며, 랜섬웨어의 영향을 받았다는 사실을 깨달았습니다. Unit 42는 2시간 이내에 공격을 평가하기 시작했습니다.

조사

포렌식 및 위협 헌팅을 통해 신속하게 Black Basta 랜섬웨어, 초기 피싱 이메일, 무단 액세스 범위를 밝혀냈습니다.

보안화

96시간 이내에 영향을 받은 환경을 대상으로 Cortex XDR을 배포하여 공격을 억제함으로써 Unit 42 MDR 팀이 24시간 연중무휴 모니터링 및 위협 헌팅을 시작할 수 있는 환경을 구축했습니다.

복구

공격자의 초기 요구액을 80% 인하하여 협상하고 암호 해독 키를 확보하여 테스트하고 구현했습니다.

혁신

네트워크 세분화, 자격 증명 제어, 엔드포인트 보안, 보안 가시성 측면에서 부족한 부분을 파악하고 방화벽 및 액세스 제어 기술을 추가로 배포했습니다.

해결 타임라인

	0~4일차 위기 대응	5~7일차 암호 해독	8~14일차 복구	15~30일차 강화
 평가	지표 및 포렌식 수집을 위한 기업 전반의 가시성을 확보하기 위해 Cortex XDR 및 Xpanse를 배포했습니다.	Cortex XDR 포렌식 분석을 통해 사고의 범위와 심각도, 성격을 파악했습니다.		
 조사	Unit 42 위협 인텔리전스를 활용하여 Black Basta TTP 및 IOC를 식별하여 공격자를 빠르게 격리했습니다.	근본 원인이 QBot 피싱 이메일인 것으로 밝혀졌으며, 유출된 데이터의 범위를 확인했습니다.	영향을 받는 환경 전반에서 위협 행위자의 전체 활동을 파악했습니다.	
 보안화	위협 행위자와 연락을 취하고 초기 요구액에서 80% 감액 협상을 진행했습니다.	SSL 복호화/검사가 활성화된 NGFW 방화벽을 사용하여 고객 본사에서 네트워크 세분화 및 격리를 구현했습니다.	환경에서 위협 행위자를 완전히 격리하고 제거했습니다.	IR 및 MDR은 24시간 연중무휴 모니터링을 위해 그대로 유지됩니다. Xpanse 매핑에서 확인된 취약점을 수정하기 시작했습니다.
 복구	영향을 받지 않는 사이트에 대한 보안 연결을 설정했습니다.	타사 복호화 유틸리티를 사용하여 복호화를 시작하고 네트워크 전체의 자격 증명을 재설정했습니다.	중요한 비즈니스 운영이 복구되고 우선순위가 낮은 지원 시스템으로 암호 해독 작업이 이전되었습니다.	영향을 받은 서버와 워크스테이션을 지속적으로 재구축하고 복구합니다.
 혁신			Prisma Access로 원격 사이트에 대한 보안 연결을 구축했습니다.	30,000개가 넘는 엔드포인트에 걸쳐 전사적으로 Cortex XDR을 배포하여 완벽한 가시성, 알림 및 보호를 보장했습니다.

paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS

위협 정보에 기반한 인시던트 대응

Unit 42 인시던트 대응을 통해 위협에 한발 앞서 대응하고 문제를 예방하세요. 세계 최고 수준의 사이버 보안 기업이 제공하는 전폭적인 지원을 바탕으로 그 어느 때보다 빠르게 인시던트를 조사, 격리 및 복구하고 위협에서 벗어나세요. 당사와 파트너십을 맺고 평안을 누리세요.

업계 최고 수준의 지원

위협 인텔리전스

신속한 조사 및 해결을 위한 광범위한 원격 측정 및 인텔리전스

기술

심층적 가시성을 제공하여 더 빠르게 위협 요소를 발견하고, 차단, 제거하며 운영 중단을 최소화하는 Palo Alto Networks 플랫폼

경험

연간 1,000건이 넘는 인시던트에 신속하게 대응하고 단호하게 대처하는 신뢰할 수 있는 전문가