글로벌 기술 제조업체, 제로 다운타임으로 APT 공격 무력화

공격자가 TiltedTemple 캠페인의 일환으로 1만 개가 넘는 클라이언트의 엔드포인트 환경에 접속했을 때, Unit 42®는 그 영향을 발견하고 기업을 보호했습니다.

글로벌 기술 제조업체, 제로 다운타임으로 APT 공격 무력화

업종 기술 | 국가 미국

문제

법 집행 기관은 매우 은밀한 활동이 가능한 것으로 알려진 APT의 지표와 일치하는 네트워크 트래픽이 클라이언트 환경을 떠나는 것을 확인했으며, 그에 따라 철저한 특수 조사가 필요했습니다. Unit 42 덕분에 APT 조사가 진행되는 동안 고객은 다운타임을 전혀 겪지 않았습니다. 당사의 사고 대응 전문가는 다음과 같은 요청을 받았습니다.

- 위협 행위자를 격리 및 제거하고 초기 영향 이후의 수평 이동을 방지합니다.
- 근본 원인을 파악하고 공격의 범위를 측정합니다.
- 보안 제어를 강화하여 추가 피해를 완화합니다.

결과

0 다운타임

Unit 42는 클라이언트가 APT의 표적이 된 후에도 계속 안전하게 작동할 수 있도록 지원했습니다.

48시간

공격이 TiltedTemple의 캠페인이라는 것을 성공적으로 식별했습니다.

4일

영향 범위를 측정하고 환경을 보안화했습니다.

탁월한 결과를 위한 Unit 42의 엄격한 사고 대응 접근 방식

평가

Unit 42는 위협 행위자의 특성을 고려할 때 영향을 받는 환경뿐만 아니라 인접 환경과 더 넓은 네트워크에 대한 철저한 평가가 필요하다는 것을 알고 있었습니다.

조사

위협 행위자가 눈에 띄는 곳에 숨어 있는 것을 막기 위해 광범위한 위협 헌팅을 시작하여 즉시 지속적 액세스, 수평 이동, 데이터 유출을 찾아냈습니다.

보안화

연중무휴 24시간 위협 헌팅 및 사전 모니터링 설정을 통해 네트워크 및 모든 엔드포인트의 활동을 완벽하게 파악할 수 있었습니다.

복구

위협 행위자의 액세스가 제거되고 백도어가 차단되었으며, Unit 42는 고객에게 전체적인 영향을 알릴 수 있었습니다.

혁신

모회사와 영향을 받는 조직 간의 보안 관련 가시성 격차를 식별하고 이를 해결했습니다.

"Unit 42는 적절한 시점에 지식과 기술을 제공했으며, 덕분에 사고대응팀과 최고 경영진은 적극적 위협 행위자와 관련한 리스크가 완화되었다는 확신을 가질 수 있었습니다."

CIO

해결 타임라인

	0~1일차 위기 대응 시작	2~5일차 격리	6~10일차 복구
평가	인시던트의 범위와 심각성을 평가했고, 침해 지표(IoC)를 확인했으며, 위협 행위자를 식별했습니다.	Unit 42 위협 인텔리전스 및 IoC를 통해 위협 행위자는 TiltedTemple 캠페인의 중국 APT로 확인되었습니다.	
조사	영향을 받은 것으로 알려진 시스템에 대한 포렌식 조사를 수행하여 무단 활동을 모두 파악하고 기업 환경 전체를 대상으로 IoC를 찾았습니다.	알려진 IoC에 대한 위협 헌팅을 계속하고 새로운 TTP를 식별했습니다.	엔터프라이즈 환경 전반에서 광범위한 위협 헌팅을 수행하여 알려지지 않은 위협 행위자의 활동을 식별했습니다.
보안화	기존 도구를 활용하여 신속한 가시성을 확보하고 격차가 발생하는 부분을 파악했습니다.	가시성을 확대하기 위해 공백이 확인된 시스템에 Cortex XDR®을 배포했습니다.	잠재된 악의적 활동을 식별하기 위해 Cortex Xpanse®를 사용하여 빈도 및 이상 분석을 수행했습니다.
복구		식별된 위협을 격리하고 지속성 활동과 데이터 노출을 모니터링했습니다.	위협 행위자를 제거하고 위협을 근절했으며, 고객에게 사건의 영향에 대한 세부 정보를 제공했습니다.
혁신			취약점을 파악했으며, 취약점을 효과적으로 강화하여 고객의 보안 태세를 개선하는 방법을 조언했습니다.

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