Cisco XDR의 자동 랜섬웨어 복구

목차

랜섬웨어를 차단하는 가장 빠르고 가장 포괄적인 방법

공격자는 고가의 에셋에 도달할 수 없습니다. 공격자는 데이터 센터의 도메인 컨트롤러나 금융 서버를 직접 공격하고 싶어하지만 그럴 수 없습니다. 그래서 네트워크 엣지에 있는 직원의 디바이스나 인터넷 연결 라우터에서 공격을 시작하여 취약점을 악용하고, 지속적인 경로를 구축하며, 권한을 상승시킨 후 네트워크를 통해 횡적 확산을 시작합니다.

오늘날의 정교한 공격에서는 조기 탐지를 피하기 위해 MITRE ATT&CK LOLbins(Living Off the Land Binaries)와 같은 신뢰할 수 있는 운영 체제 바이너리와 HTTPS, RDP, SMB와 같은 합법적인 통신 프로토콜을 활용합니다. 공격자는 고가의 에셋에 도달하여 암호화할 때까지 완전히 합법적인 네트워크 트래픽으로 가장하므로, 사용자는 몸값 요구를 받을 때까지 이러한 트래픽이 있다는 사실을 모르는 경우가 많습니다.

현재까지 그렇습니다.

공격 체인 차단하기

Cisco XDR 자동 랜섬웨어 복구는 선도적인 엔터프라이즈 백업 및 복구 벤더와의 파트너십을 통해 악성코드에 선행하는 공격 체인을 식별하여 랜섬웨어 발생의 초기 징후를 탐지합니다. 어떻게 하면 가능할까요? 일반적으로 PowerShell을 사용하지 않는 프로세스에서 생성된 PowerShell 스크립트 같은 초기 지표에 집중하여 HTTPS 또는 SMB를 통해 내부 디바이스에 대한 비정상적인 네트워크 연결을 생성합니다. 일반적으로 이러한 '낮은 정확도' 이벤트는 네트워크 옵션을 중단할 수 있는 오탐에 대한 걱정 없이 보안 정책을 업데이트할 만큼 충분한 신호가 아닙니다. 독점적인 텔레메트리와 10년간의 애널리틱스 개발 결과를 적용한 Cisco XDR은 근접한 위치에서 발생하는 낮은 정확도 이벤트 여러 개를 결합하여 랜섬웨어 발생의 초기 징후를 정확하게 식별하므로 공격 체인을 차단하고 에셋을 보호할 수 있습니다.

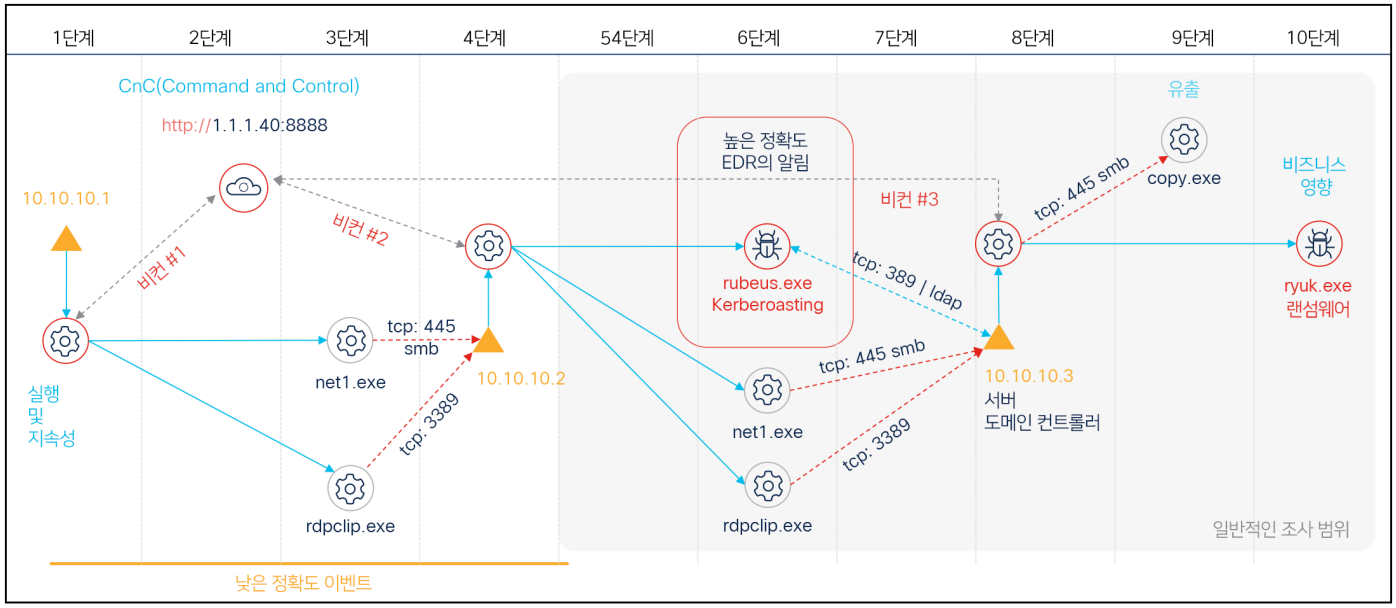

그림 1.
일반적인 랜섬웨어 복구 조사가 Cisco XDR 자동 랜섬웨어 복구 없이 진행되는 방식. 랜섬웨어 공격은 고가의 에셋을 검색하기 위해 정상적인 네트워크 트래픽으로 위장한 최고의 EDR 솔루션에 의한 탐지도 회피합니다.

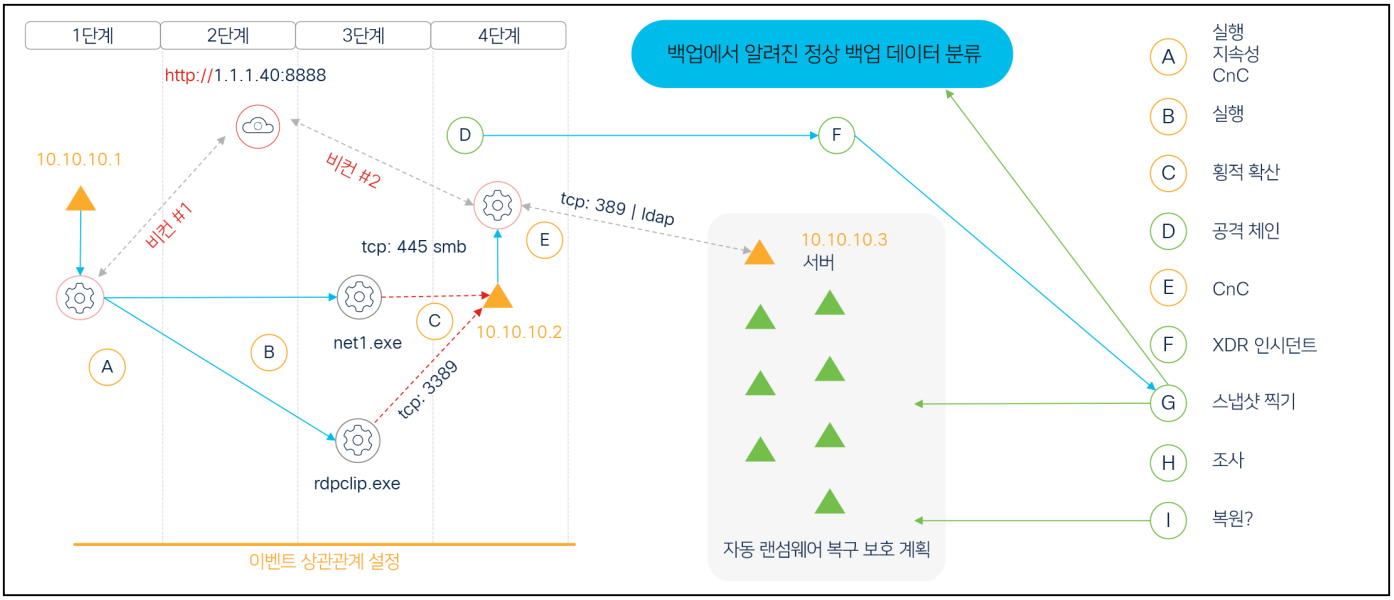

그림 2.
조기에 사전 대응하는 Cisco XDR 자동 랜섬웨어 복구. 랜섬웨어 공격 징후가 탐지되면 Cisco XDR은 대상 에셋에 대한 스냅샷 요청을 트리거하여 깨끗한 최신 백업을 확보합니다.

Cisco XDR 자동 랜섬웨어 복구 워크플로우는 엔터프라이즈 백업 및 복구 솔루션에 요청을 트리거하여 감염이 발생하기 전에 조직의 고가 에셋을 자동으로 백업합니다. 기존의 엔드포인트 탐지 및 대응(EDR) 툴이 공격을 식별하고 요청을 트리거하는 데 몇 시간 또는 며칠이 걸리는 것과 달리 Cisco XDR은 공격의 초기 징후 탐지 시 백업을 시작합니다.

안심할 수 있는 환경 제공 및 다운타임 감소

Cisco XDR과 통합 백업 복구 솔루션은 실시간으로 스냅샷을 생성하여 복구 지점 목표(RPO)와 복구 시간 목표(RTO)를 거의 0에 가깝게 줄일 수 있습니다. 따라서 일반적으로 이벤트 발생 24시간 또는 48시간 전인 마지막 백업 이후에 비즈니스 크리티컬 데이터의 손실에 대해 더 이상 걱정할 필요가 없습니다. Cisco XDR은 마지막으로 알려진 정상 구성을 복원하여 다운타임을 최소화하고 엄청난 몸값을 지불하지 않고도 조직을 백업하고 가동할 수 있도록 합니다. 그렇다면 오탐은 어떤가요? Cisco XDR은 오탐을 제거하고 낮은 정확도 신호가 완전히 정상인 것으로 판명되면 통합 복구 솔루션이 백업을 삭제하고 서버의 공간을 확보합니다.

이것이 바로 보안 탄력성이고, Cisco XDR의 자동 랜섬웨어 복구입니다.

시작하는 방법

자동 랜섬웨어 복구는 Cisco XDR의 Advantage 및 Premier 라이선스 계층에 제공되며 인증된 백업 및 복구 솔루션과의 통합(Cisco XDR 라이선스에 포함되지 않음)이 필요합니다.

Cisco XDR의 자동 랜섬웨어 복구 데모와 시스코의 백업 복구 파트너를 확인하십시오.

자세한 내용은 Cisco 영업 담당자에게 문의하거나 Cisco XDR 웹 페이지(cisco.com/go/xdr)를 확인하십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose, CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 주소, 전화 번호 및 팩스 번호는 Cisco 웹사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C45-4143504-00 12/23