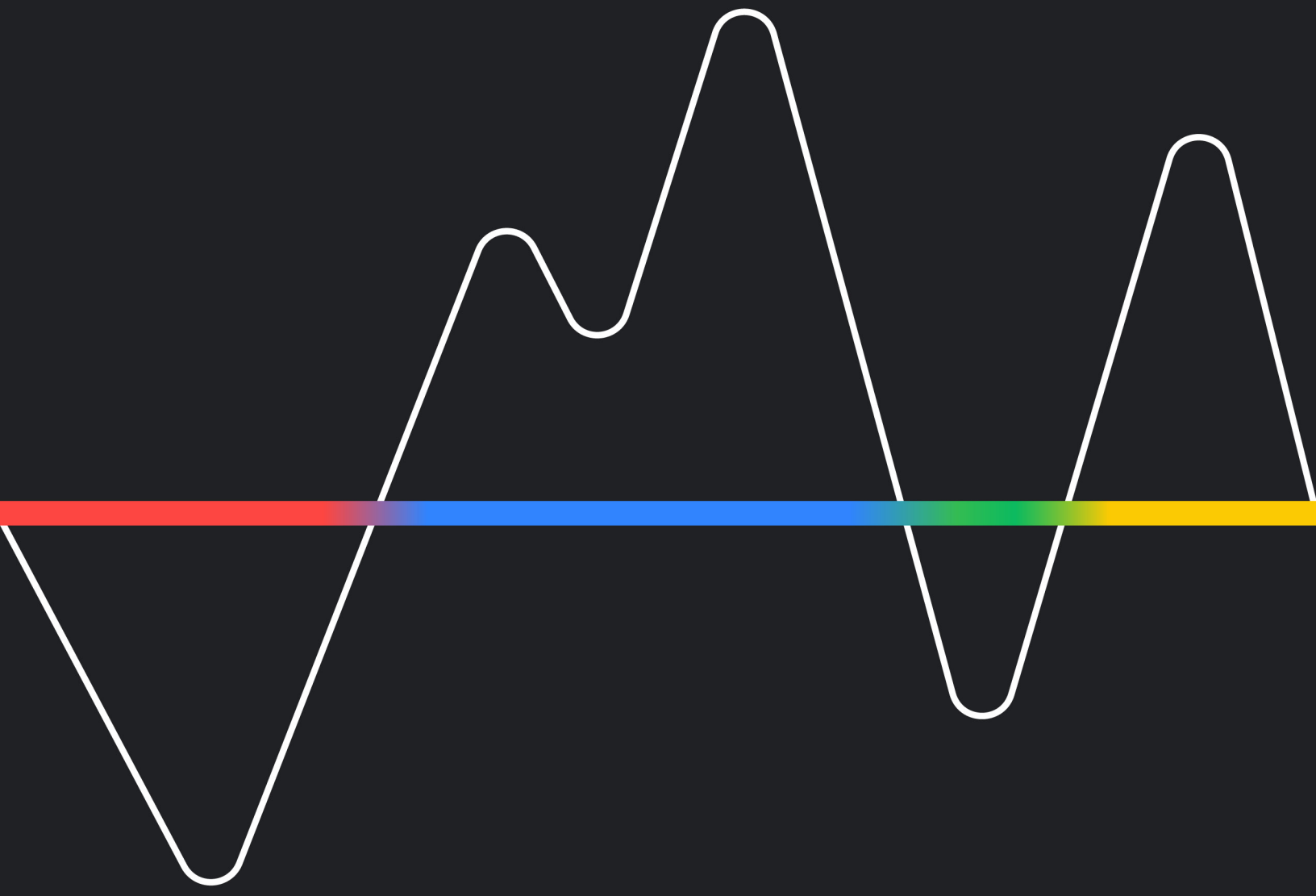
Mandiant

Google Cloud Security

M-Trends

2026 보고서

핵심 요약



M-Trends 2026 핵심 요약

서문

M-Trends는 침해 사고에서 사용되는 위협과 전술을 심층적으로 조망하는 보고서로, 2025년 한 해 동안 Mandiant에서 실시한 50만 시간 이상의 현장 사고 조사 결과를 기반으로 작성되었습니다. Mandiant는 Google Threat Intelligence Group(GTIG)과 함께 현재 위협 환경뿐만 아니라 향후 공격을 주도할 수 있는 신종 위협에 대한 포괄적인 관점을 갖추고 있습니다.

최근 GTIG 보고에 따르면 공격자들이 AI 기술을 도입하고 있는 것으로 확인되었습니다. 공격자들은 초개인화된 소셜 엔지니어링, 탐지를 회피하기 위해 실행 도중 LLM에 쿼리하는 멀웨어, 독자적인 머신러닝 로직을 겨냥한 '증류 공격'에 대규모 언어 모델(LLM)을 활용하고 있습니다. Mandiant 레드팀도 이처럼 새롭게 부상하는 위협에 대한 대비책으로 AI 기반 기술을 활용하고 있습니다. 그러나 M-Trends 2026의 분석 결과에 따르면 보안 침해를 가능하게 하는 인적, 시스템적 오류를 완화하는 것이 무엇보다 시급한 과제인 것으로 드러났습니다.

2025년 사고 대응 사례에서 발견한 중요한 특징은 일부 공격자가 주로 표준 원격 분석이 부족한 에지 기기에 지속성을 확보해 네트워크에서 탐지되지 않고 활동하는 기간이 늘었다는 점입니다. 2025년 Mandiant에서 실제로 이러한 유형의 사고에 수차례 대응한 바 있으며 해당 사례를 분석한 결과, 전 세계 드웰 타임(dwell time) 중앙값이 이전 보고서에 보고된 11일에서 14일로 증가했습니다. 이는 주로 장기적인 스파이 활동과 북한 IT 인력이 수행한 작전에 영향을 받은 결과입니다.

한편, 일부 위협 그룹은 속도전에 집중합니다. 초기 액세스 파트너가 액세스 권한을 불법 거래 시장에서 판매하는 대신 2차 공격 그룹과 직접 협업하는 사례가 늘고 있습니다. 이로 인해 30초도 채 안 되어 '권한 이전'이 이루어지기도 합니다. 이렇게 되면 '사소한' 경보가 순식간에 심각한 침해로 이어질 수 있습니다.

동시에 공격자들은 복구를 방해하기 위해 백업, ID 서비스, 가상화 계층 같은 인프라를 표적으로 삼아 체계적인 공격을 가하고 있습니다. 이로 인해 조직은 금전을 요구하는 랜섬 요구에 응하거나 복구 능력을 상실할 위험을 감수해야 하는 엄청난 압박에 직면하게 됩니다.

진정한 운영 복원력을 갖추기 위해서는 조직도 공격자와 동일한 속도로 움직여야 합니다. 이때 공격자의 성공 전략을 이해하는 것이 매우 중요합니다. M-Trends 2026에서 제시하는 방어 체계를 도입하고 치명적인 가시성 부족을 해소한다면, 기업은 사소한 경보가 심각한 침해로 확대되기 전에 사후 대응 복구 방식에서 벗어나 선제 대응 체계로 전환할 수 있습니다.

숫자로 보는 현황

M-Trends 2026 보고서에 포함된 지표는 Mandiant 컨설팅에서 2025년 1월 1일부터 2025년 12월 31일 사이에 표적 공격 활동에 대해 실시한 조사를 바탕으로 합니다.

핵심 요점

공격자들이 초기 액세스 전략을 바꾸고 있습니다. 익스플로잇은 여전히 가장 일반적인 방식이지만 그다음으로 대화형 음성 기반 소셜 엔지니어링 공격이 빠르게 늘어나고 있습니다. 동시에 정교한 스파이 활동 그룹과 내부자 위협이 은밀하고 장기적인 액세스를 선호하면서 전 세계 드웰 타임 중앙값이 증가했습니다. AI를 공격 무기로 활용하고, 에지 기기의 제로데이 취약점을 악용하며, 초기 액세스 파트너와 사이버 범죄 그룹 간에 권한을 이전할 기회를 노리는 공격자에게 맞서기 위해 조직은 기존의 정적인 방어 수준을 넘어서야 합니다. 특히 EDR 등 기존 보안 도구의 관찰 범위에서 벗어나 있던 가상화 같은 인프라와 ID 행동을 지속적으로 모니터링하는 방향으로 보안 전략을 발전시켜야 합니다.

필수 확인 사항

- 2025년에 관찰된 위협 클러스터 중 금전적 이득을 노리는 그룹은 41%로 감소했으며(2024년: 55%) 사이버 스파이 활동 그룹은 16%로 증가했습니다(2024년: 8%).
- 가장 일반적인 초기 감염 벡터는 6년 연속으로 익스플로잇(32%)이었으며, 보이스 피싱은 11%로 급증해 두 번째로 많이 관찰되는 벡터였습니다. 반면 이메일 피싱은 2024년 14%에서 2025년 6%로 지속적인 감소세를 보였습니다. 이메일 피싱과 보이스 피싱은 모두 넓은 의미에서 소셜 엔지니어링 공격에 해당하지만 방어 측면에서는 이 둘을 구분하는 것이 매우 중요합니다. 대화형 공격은 자동화된 기술 제어에 대한 내성이 높아 별도의 탐지 전략이 필요하기 때문입니다.
- 랜섬웨어 관련 사고에서는 사전 침해가 30%로 가장 빈번한 초기 감염 벡터인 것으로 나타났습니다. 일부 위협 클러스터는 대량의 기회형 감염 벡터를 통해 여러 조직에서 초기 거점을 확보한 뒤 해당 액세스 권한을 다른 위협 클러스터에 판매하거나 넘겨 후속 익스플로잇에 활용하도록 합니다.
- 가장 빈번하게 표적이 된 산업은 첨단 기술, 금융, 비즈니스, 전문 서비스, 헬스케어였으며, 전체적으로 16개 이상의 산업군이 사고의 영향을 받았습니다. 특히 주목할 부분은 첨단 기술 분야에서 조사된 건수가 2023년과 2024년에 가장 높은 비중을 차지했던 금융 분야를 넘어섰다는 점입니다.
- 2025년 전체 조사 사례에서 조직이 악성 활동을 최초로 탐지한 경우는 내부 탐지가 52%(2024년 43%에서 증가), 외부 기관의 통보에 의한 경우는 34%(2024년 43%에서 감소)였습니다. 공격자가 직접 침해 사실을 알린 경우도 14%에 달했습니다.
- 랜섬웨어 사례에서는 공격자가 직접 피해 조직에 통보한 비율이 44%로 가장 높았고, 내부 탐지는 41%, 외부 기관 통보는 15%였습니다. 공격자 통보 비율이 훨씬 높은 이유는 랜섬웨어의 비즈니스 모델 특성에 따른 것입니다.
- 전 세계 드웰 타임 중앙값은 2024년 11일에서 2025년 14일로 증가했습니다. 2024년 분포율과 비교했을 때 2025년에 일주일 이내에 탐지된 사고는 소폭 감소했으며 드웰 타임이 1주에서 6개월 사이로 길어지는 경향이 나타났습니다. 이는 은밀하고 장기적인 액세스 상태를 유지하는 것을 중시하는 사이버 스파이 활동과 북한 IT 인력 관련 사고가 늘어난 영향으로 보입니다. 두 유형의 드웰 타임 중앙값은 122일에 달했습니다.
- 2025년 조사로 확인된 멀웨어 패밀리 중 36%는 백도어, 11%는 다운로더, 10%는 랜섬웨어, 10%는 드로퍼, 9%는 사용자 인증 정보 스틸러였습니다.
- Mandiant 조사에서 5년 연속으로 가장 많이 관찰된 멀웨어 패밀리였던 Cobalt Strike BEACON은 4위로 내려갔습니다. 그다음으로 가장 많이 관찰된 멀웨어 패밀리는 GOLDVEIN.JAVA 다운로더였으며, 그다음은 REDBIKE(Akira) 랜섬웨어였습니다.
- 위협 클러스터는 EDR을 지원하지 않는 어플라이언스에서 BRICKSTORM 백도어와 같은 경량 멀웨어와 은밀한 전술을 활용하고 있습니다. 금전적 이득을 노리는 그룹과 사이버 스파이 그룹 모두 온프레미스 환경과 클라우드 환경의 기본 기능과 합법적인 도구를 악용하여 탐지 가능성을 낮추고 있습니다.

- 위협 클러스터는 정찰, 소셜 엔지니어링, 멀웨어 개발의 생산성을 높이기 위해 AI 도구를 점점 더 적극적으로 활용하고 있습니다. 더 나아가 공격자들은 침해된 환경 내 AI를 공격에 활용하고 있습니다. 예를 들어 QUIETVAULT 사용자 인증 정보 스틸러의 경우 대상 머신에 AI CLI 도구가 설치되어 있는지 확인한 후 사전 정의된 프롬프트를 실행해 구성 파일을 검색하는 사례가 관찰되었습니다.

향후 실행 과제

- **기존 엔드포인트를 초월한 가시성 확장:** 전체 생태계에 고급 위협 탐지 기능을 배포해야 합니다. 특히 EDR이 적용되지 않는 에지 어플라이언스에 대해서는 네트워크 트래픽 분석 기능을 도입하고, 가상화 인프라에 대해서는 엄격한 원격 분석을 적용해야 합니다.
- **인터넷 노출 공격 표면의 적극적인 관리:** 익스플로잇이 6년 연속 가장 빈번한 초기 감염 벡터로 확인되는 만큼, 조직은 신속한 패치 적용과 취약점 스캔을 최우선 과제로 삼아야 합니다. 또한 제로데이 및 n-day 취약점 공격의 주요 표적이 되는 외부 노출 웹 애플리케이션 서버에 대해서도 엄격한 격리 조치가 이루어져야 합니다.
- **이메일 중심에서 벗어나 다양한 공격 벡터로 보안 인식 교육의 범위를 확장:** 이메일 피싱은 여전히 주된 공격 방식이지만 Mandiant에서 파악한 바에 따르면 공격자들은 대화형 보이스 피싱, 사용자 인증 정보 도용, ClickFix와 같은 전술 등 점점 더 다양한 초기 감염 벡터를 사용하고 있습니다. 따라서 직원들과 IT 헬프 데스크팀은 실시간 음성 기반 소셜 엔지니어링 공격, 메시징 앱을 통한 유인 시도, 승인되지 않은 MFA 재설정 요청을 식별할 수 있도록 교육받아야 합니다.
- **반복적인 본인 인증 체계로 전환:** 대화형 소셜 엔지니어링 공격은 기존 MFA를 우회하는 경우가 많으며 북한 IT 인력을 비롯한 다양한 공격자가 장기적인 액세스 권한을 확보하려고 시도하고 있습니다. 그러므로 조직은 최소 권한 원칙을 엄격히 적용하고, SaaS/클라우드 통합 환경을 정기적으로 점검하며, 직원과 원격 계약 인력 모두의 ID 관련 이상 징후를 선제적으로 헌팅해야 합니다.
- **최신 랜섬웨어 및 정보 유출 협박 대응 가이드:** 사고 대응 및 복구 계획은 암호화 기반 랜섬웨어뿐만 아니라 데이터 도용 갈취까지 모두 대응할 수 있도록 설계되어야 합니다. 기회형 초기 감염을 조기에 탐지하여 대응 시간을 단축하고 초기 액세스 파트너로부터 2차 공격 그룹으로 권한이 이전되지 않도록 차단하는 데 초점을 맞춘 모의 훈련을 실시해야 합니다.
- **개발 환경 및 AI 도구 모음 보호:** 위협 클러스터가 침해된 환경 내의 AI를 공격에 활용하는 사례가 확인되고 있습니다. 실제로 멀웨어가 합법적인 로컬 AI 명령줄 도구를 악용해 GitHub 및 NPM 토큰을 탐색하고 탈취하는 사례가 관찰된 만큼 조직은 Google의 안전한 AI 프레임워크(SAIF) 원칙을 적용해야 합니다. 구체적으로는, 위협 모델에 AI 도구를 포함하도록 '탐지 및 대응 범위를 확장'하는 방식을 사용하면 보안팀에서 정상적인 동작 기준을 설정하고 이러한 유틸리티에서 발생하는 비정상적인 프롬프트 실행이나 무단 데이터 도용 시도를 모니터링할 수 있습니다.
- **실전형 위협 시나리오 기반의 레드팀 수행:** 최신 공격 전술을 반영한 현실적인 에뮬레이션을 통해 방어 체계를 지속적으로 테스트해야 합니다. 특히 자급자족식 기법, 에지 기기 익스플로잇, 대화형 소셜 엔지니어링에 대한 보안팀의 탐지 및 대응 시간을 측정해야 합니다.

오늘의 사소한 감염이 내일의 랜섬웨어가 된다

핵심 요점

사이버 범죄 파트너 간 협업이 더욱 긴밀해지면서 방어할 수 있는 시간적 여유가 사실상 사라졌습니다. 한 공격 그룹이 기회형 초기 액세스 권한을 확보한 시점부터 2차 위협 그룹이 해당 액세스 권한을 넘겨받아 사용하기까지 걸리는 평균 시간이 과거 약 8시간에서 이제 단 22초로 크게 감소했습니다. 이러한 변화는 조직이 저위험 경보조차도 중요한 침해 지표로 간주해야 함을 의미합니다. 고위험 공격자가 해당 액세스 권한을 악용하기 전에 즉각적인 해결 조치를 취해야 합니다.

필수 확인 사항

- **공격 전이 시간(Time to Hand-Off) 단축에 따른 대응 한계:** 초기 침투가 발생한 시점부터 2차 위협 그룹으로 액세스 권한이 넘어가기까지 평균적으로 걸리는 시간이 2022년 8시간 이상에서 2025년 22초로 급격히 감소했습니다. 이는 초기 액세스 파트너가 액세스 권한을 나중에 불법 거래 시장에서 판매하는 대신, 2차 공격 그룹이 즉시 활용할 수 있도록 직접 협업하는 방식으로 전환되고 있음을 시사합니다.
- **저위험 침해 사고와 고위험 공격의 상관관계:** 역할 분담 모델을 활용하는 공격자의 경우 전문 그룹이 악성 광고(멀버타이징)나 가짜 브라우저 업데이트와 같이 영향력이 크지 않아 보이는 기법을 사용하여 거점을 확보합니다. 이러한 초기 벡터는 겉보기에는 저위험 멀웨어처럼 보이기 때문에 고위험 전술만을 헌팅하는 조직은 이를 놓치는 경우가 많습니다.
- **공격 전이 단계(Pre-Staging) 분석:** 초기 액세스 파트너는 불법 거래 시장에서 액세스 권한만 판매하는 것이 아니라, 초기 감염 단계에서 2차 공격 그룹이 선호하는 멀웨어, 터널, 백도어 등을 미리 배치해 둡니다. 이처럼 불법 거래 시장을 거치지 않고 환경을 사전 구성해 두면, 후속 공격자가 원하는 시점에 해당 거점을 즉시 활용할 수 있으며 네트워크와 처음 상호작용하는 순간부터 고위험 공격을 실시할 만반의 준비를 갖추게 됩니다.

향후 실행 과제

- **사소한 경고를 위협의 전조로 대응:** 초기 감염은 중요도가 낮아 보일 수 있지만, 이후 고위험 공격으로 이어질 가능성이 매우 높기 때문에 대응 플레이북을 재정비해야 합니다. 보안팀은 일반적인 멀웨어 경보도 2차 공격 그룹으로 권한 이전이 이루어질 수 있는 고우선순위 지표로 간주해야 합니다.
- **표준 소프트웨어 베이스라인 준수 시스템 구축:** IT팀과 보안팀은 사용자에게 제공할 사전 승인된 도구 모음을 결정하고 중앙에서 배포해야 합니다. 이렇게 하면 사용자가 임의로 설치하는 도구로 인한 노이즈를 줄이고, 기준선에서 벗어난 이상 징후를 신속하게 식별하고 대응할 수 있습니다.
- **이벤트 상관관계 분석 및 맥락 가시성 최적화:** 방어 워크플로는 개별 경보를 하나하나 검토하는 방식에서 벗어나 이벤트 간 상관관계를 분석하는 방향으로 전환되어야 합니다. 경보에 컨텍스트 데이터를 결합하면 고위험 침입으로 이어질 수 있는 특정 동작 패턴을 더 쉽게 식별할 수 있습니다.
- **본격적 위협 확산 전 즉각적 대응 체계 구축:** 방어자의 목표는 2차 공격 그룹이 본격적인 활동에 들어가기 전, 대개 비대화형 이벤트로 발생하는 초기 액세스 단계에서 침입을 차단하는 것입니다. 공격이 아직 단일 시스템 안에 머물러 있을 때 이를 차단하는 것이 이후 고위험 공격 단계에서 복구를 시도하는 것보다 훨씬 더 효과적입니다.

랜섬웨어, 이제는 '방어'를 넘어 '회복 탄력성'의 문제

핵심 요점

랜섬웨어 그룹은 더 이상 데이터를 암호화하는 데 그치지 않고 복구 자체를 불가능하게 만드는 방향으로 공격을 전개하고 있습니다. 이들은 핵심 시스템을 표적으로 삼아 조직이 결국 금전적인 요구를 들어줄지, 아니면 인프라를 재구축할지 선택하도록 압박합니다. 이제 진정한 복원력을 갖추려면 복구 도구를 분리하여 별도로 보호할 수 있도록 네트워크를 설계해야 합니다. 핵심 시스템을 철저히 보호하고 공격자가 네트워크를 활보하지 못하게 만드는 것이 오늘날 랜섬웨어 위협에 맞서 보안팀이 우위를 점할 수 있는 중요한 전략입니다.

필수 확인 사항

- **'복구 거부' 공격으로 진화한 랜섬웨어:** 단순한 데이터 도용 정도였던 랜섬웨어 운영자의 주요 목표가 이제 복구 자체를 불가능하게 만드는 것으로 전환되었습니다. 공격자는 특히 ID 서비스, 가상화 관리 계층, 백업 인프라와 같은 시스템 및 관리 경로를 표적으로 삼아 조직의 복구 능력을 약화시키고 금전 지불 압박을 극대화하고 있습니다.

- **새로운 보안 경계로 부상한 ID:** 정교한 위협 그룹은 ID 컨트롤 플레인을 조작하여 표적 환경 전체를 장악하고 있습니다. 실제로 공격자들이 잘못된 설정을 악용해 인증서를 발급하거나 관리자 계정을 생성하여 다중 인증(MFA) 및 비밀번호 순환 정책을 우회하는 사례가 관찰되었습니다. 어떤 경우에는 전체 데이터베이스를 탈취하거나 클라우드 테넌트를 침해하여 인프라 백엔드를 파괴함으로써 위기 상황에서 보안 담당자가 비상 계정에 액세스하지 못하도록 차단하기도 합니다.

- **기존 안전망의 무력화:** 백업에 의존하는 기존 전략은 점점 효과를 잃고 있습니다. 공격자가 백업 아키텍처를 적극적으로 헌팅해 파괴하고 있기 때문입니다. 공격자는 정찰 활동을 통해 저장 위치를 파악하고 암호화 구성을 확보한 뒤 클라우드 스토리지와 로컬 시스템에서 백업 객체를 체계적으로 삭제합니다. 온프레미스 환경에서는 가상화 환경을 백업 플랫폼과 분리하거나, 로컬 복구 지점을 암호화하는 사례도 확인되었습니다. 이로 인해 기존 사고 대응 플레이북은 무력화되며 복구에 필요한 도구 자체를 사용할 수 없는 상황이 발생합니다.

향후 실행 과제

- **최소한의 실행 가능한 보안 기준 강화:** 조직은 ID를 주요 경계로 간주해야 합니다. 이를 위해서는 '권한 기반 ID 관리'와 '조건부 액세스'를 적용하여 관리자 권한에 시간 제한을 두고 지속적으로 모니터링하는 등 고위험 액세스 경로의 보안을 강화해야 합니다. 보안팀은 모든 액세스에 대해 MFA를 적용하고, 강화된 '권한 기반 액세스 워크스테이션'을 사용하며, '서비스 보안 주체 이름'을 감사해야 합니다. 또한 원격 분석을 조정하여 '자급자족식' 동작을 탐지함으로써 관리 권한 탈취의 영향이 환경 전반으로 확산되기 전에 이를 식별해야 합니다.
- **핵심 Tier-0 컨트롤 플레인 격리:** 가상화 및 관리 플랫폼은 'Tier-0' 애셋으로 간주하고 가장 엄격한 액세스 제약을 적용해야 합니다. 조직에서 제로 트러스트 기반의 세분화를 적용하여 이러한 시스템을 공식적인 서버 Active Directory(AD) 통합으로부터 완전히 격리함으로써 단일 ID 침해가 전체 환경에 대한 암호화 공격으로 이어지는 상황을 방지해야 합니다. MFA로 보호되는 로컬 계정과 함께 별도의 전용 관리 채널을 활용하면 시스템을 구조적으로 확실하게 분리할 수 있으며 프로덕션 환경과 복구 기능이 동시에 침해되는 상황을 방지할 수 있습니다.
- **복구 경로 신뢰성 강화:** 프로덕션 환경이 침해되더라도 복구 역량은 그대로 유지할 수 있어야 합니다. 이를 위해 조직은 팀에서 시스템을 정리하고, 검증하고, 시스템 복원을 준비할 수 있는 별도의 격리된 복구 환경을 구축해야 합니다. 이렇게 해야 재감염 루프를 방지할 수 있습니다. 또한 Tier-0 애셋, 특히 ID 및 백업 카탈로그는 프로덕션 네트워크와 동일한 위험을 공유하지 않도록 오프라인 상태또는 또는 변경 불가능한 버전을 유지해야 합니다. 재해 복구 계획은 기본 ID 인프라가 완전히 손실되는 최악의 상황까지 철저하게 고려하여 수립해야 합니다.

초장기 지속 침투 분석

핵심 요점

예방이 가장 이상적이지만 대비는 필수입니다. 정교한 공격자는 사각지대와 관리 권한에 대한 신뢰를 악용하여 수년에 걸쳐 액세스 권한을 유지합니다. 로그 공백으로 인해 침해 범위를 입증할 수 없는 조직은 최악의 데이터 도용 시나리오를 가정하여 발표해야 하는 상황에 놓여 결국 고객 신뢰를 잃게 될 위험이 있습니다. 가시성을 확보하기 위해서는 지속적인 감사가 필요하며, 이를 통해 이러한 위협이 통제 불가능한 위기로 확대되기 전에 탐지하고 해결할 수 있어야 합니다.

알아두어야 할 사항

- **만연한 잠복성과 지속성:** 일부 공격자의 경우 커스텀 멀웨어보다는 합법적인 사용자 인증 정보를 우선적으로 활용하는 전략을 통해 1년 이상의 드웰 타임을 기록하기도 합니다. 이들은 가상화 인프라와 관리되지 않는 에지 기기를 표적으로 삼고, 기본 제공 도구를 사용해 정상적인 관리 활동처럼 위장함으로써 탐지를 회피합니다.
- **위협 가시성 공백:** 지금의 로깅 전략으로는 이러한 침해의 전체 범위를 포착하기 어렵습니다. 예를 들어 은밀한 백도어인 BRICKSTORM이 사용된 사례에서는 평균 드웰 타임이 393일에 달했습니다. 즉, 기존의 90일 표준 로그 보관 정책으로는 초기 액세스 벡터를 파악할 수 없습니다. 또한 EDR에 대한 의존은 또 다른 사각지대를 만듭니다. 공격자가 엔드포인트 에이전트의 적용 범위를 벗어나는 네트워크 에지 어플라이언스와 인증 프로토콜을 표적으로 삼기 때문입니다.
- **사고 대응을 가로막는 안티 포렌식:** 정교한 공격자는 사고 범위를 파악하는 데 필요한 증거를 의도적으로 제거하는 것으로 관찰되었습니다. 파일 변경사항을 마스킹 처리하거나 시스템 로그를 삭제하는 기법으로 데이터 도용의 전체 타임라인을 재구성하는 것을 거의 불가능하게 만듭니다. 명확한 포렌식 증거가 없는 경우 조직은 최악의 침해 상황을 가정하여 발표해야 할 수 있으며, 이는 규제 및 평판 측면에서 심각한 피해로 이어질 수 있습니다.

향후 실행 과제

- **로그 보관 기간 및 범위 확대:** 일부 정교한 공격자의 긴 드웰 타임을 고려할 때 기존의 90일 표준 로그 보관 정책만으로는 침해 범위를 파악하기에 충분하지 않습니다. 조직은 중앙의 장기 스토리지로 로그를 전송하는 것을 우선시해야 하며, 특히 표준 EDR 도구로는 포착하기 어려운 네트워크 에지 기기, 하이퍼바이저, 인증 프로토콜 같은 사각지대의 데이터를 포함해야 합니다.
- **로그 무결성 강화:** 로컬 로그 삭제와 타임 스톰핑 같은 안티 포렌식 기법에 대응하기 위해 로그를 즉시 중앙 저장소로 전송하는 체계를 우선적으로 구축해야 합니다. 이렇게 조치하면 호스트가 침해되더라도 증거를 보존할 수 있습니다. 또한 로그가 비정상적으로 종료될 경우 경보가 발생하도록 저장소를 구성하면 공격자가 자신의 흔적을 숨기기 위해 보안 제어 체계를 의도적으로 비활성화하는 상황을 운영팀에서 탐지할 수 있습니다.
- **선제적 위협 헌팅으로 전환:** 보안팀은 단순히 경보에 대응하는 수준을 넘어 정기적이고 선제적인 위협 헌팅 루틴을 구현해야 합니다. 이를 위해 스택 순위 데이터와 같은 고급 분석 기법을 활용하여 정상적인 행동에서 벗어난 이상 징후를 식별해야 합니다. 최신 위협 인텔리전스를 통합하면 정상적인 관리 활동과 은밀하게 기본 도구를 악용하는 공격자 행동을 구분할 수 있습니다.
- **애셋 및 가정 검증:** 리더는 보안팀과 인프라팀 간의 협업을 강화해 환경 전반에 대한 감사를 수행해야 합니다. 중요한 애셋이 예상한 대로 원격 분석을 실제로 생성하고 있는지 확인하기 위해 기존의 가정을 정기적으로 검증해야 합니다. 또한 이 과정을 통해 사용되지 않는 기술과 시스템을 식별하고 삭제하여 관리 부담을 줄이고 공격 표면을 축소해야 합니다.

인프라 장악의 지름길, 가상화 플랫폼 타깃 공격

핵심 요점

가상화 플랫폼은 이제 단순한 백엔드 인프라가 아닌 주요 공격 표적이 되었습니다. 공격자는 하이퍼바이저의 'Tier-0' 특성을 악용하여 게스트 수준의 보안 방어를 우회하고, 일반적인 해결 조치로는 제거되지 않는 강력한 지속성을 확보하며, 기존 복구 방식으로는 대응이 불가능한 수준으로 랜섬웨어를 배포하고 있습니다. 이 스택을 보호하기 위해서는 관리 계층을 격리된 핵심 애셋으로 취급하고 심각한 로깅 사각지대를 해소하여 전체 환경에 대한 가시성을 확보해야 합니다.

필수 확인 사항

- **방치된 중추, 하이퍼바이저 보안의 맹점:** 하이퍼바이저는 일반적으로 표준 EDR 도구와 호환되지 않는 독자적인 운영체제에서 실행됩니다. 이로 인해 가시성 부족 문제가 발생하는데, 공격자는 이를 악용하여 EDR 또는 SIEM 경보를 발생시키지 않고 멀웨어를 배포하거나 관리되지 않는 가상 머신을 생성해 공격을 준비할 수 있습니다.
- **게스트 방어 체계 무력화:** 정교한 공격자는 데이터 탈취를 위해 더 이상 표적 시스템에 직접 로그인할 필요가 없습니다. 가상화 스토리지 계층을 직접 표적으로 삼아 가상 디스크를 클론하고, 게스트 운영체제나 보안 제어 체계와 상호작용하지 않고도 민감한 Active Directory 데이터베이스를 탈취할 수 있습니다.
- **데이터 저장소(Datastore)를 정조준하는 랜섬웨어:** 최신 랜섬웨어 공격은 스택 하위 계층으로 이동하여 개별 머신이 아닌 하이퍼바이저 데이터 스토어를 암호화합니다. 이 방식은 단일 호스트의 모든 서버를 동시에 중단시키고 잠금 상태로 만들어 관련 가상 머신 전체를 운영 불가능하고 복구 불가능한 상태로 만듭니다.
- **탐지 회피를 위한 시스템 하위 계층 잠복 위협 분석:** 공격자들이 하이퍼바이저의 기본 셸을 표적으로 삼아 숨겨진 백도어와 비인가 가상 머신을 배포하는 사례가 늘고 있습니다. 이러한 메커니즘은 일반적인 서버 환경의 하위 계층에서 작동하기 때문에, 표준 사고 해결 절차와 시스템 재부팅 이후에도 제거되지 않고 지속적으로 남아 공격자에게 영구적인 액세스 경로를 제공합니다.

향후 실행 과제

- **ID체계와 인프라 관리 권한의 분리:** 하이퍼바이저와 백업 인프라를 기업 Active Directory 도메인에서 분리해야 합니다. 운영 업무와 인프라 관리 모두에 동일한 ID 제공자(IdP)를 사용하는 것은 치명적인 단일 장애점(을 생성하는 것과 같습니다. 인프라 전용 인증 프로바이더를 별도로 구축하거나, 적시 권한 부여(Just-in-Time, JIT) 접근 제어를 강제해야 합니다.
- **관리 영역 격리:** 가상화 인터페이스를 최상위 보안 등급인 'Tier-0' 자산으로 취급해야 합니다. 관리 트래픽은 전용 방화벽으로 격리된 전용 네트워크 세그먼트로 엄격히 제한하고, 보안이 강화된 특권 접근 워크스테이션을 통해서만 접속 가능하도록 구성해야 합니다. 또한 피싱 공격에 강한 MFA를 적용해야 합니다.
- **불변의 회복 탄력성:** 복구 기능이 파괴되는 상황에 대비해 백업 환경을 격리해야 하며 변경 불가능한 스토리지를 사용해야 합니다. 또한 에어 갭이 적용된 사본을 기반으로 정기적인 복구 테스트를 수행하여 긴급 복구 상황에서도 의도한 대로 백업이 가능한지 검증해야 합니다.
- **중앙 집중형 인프라 분석:** 가상화 관리 로그와 하이퍼바이저 수준 로그를 중앙 SIEM으로 전송하도록 의무화해야 합니다. 공격자가 게스트 운영체제를 우회하는 상황에서는 하이퍼바이저 원격 분석이 무단 액세스, 스냅샷 조작, 비인가 가상 머신 생성을 탐지할 수 있는 유일한 수단이기 때문입니다.

에지 및 핵심 네트워크 기기]에 대한 대상의 조직적 취약점 악용 분석

핵심 요점

공격자는 최신 보안 도구를 우회하기 위해 에지 및 핵심 네트워크 기기를 공격 무기로 활용하고, 패치가 배포되기 전에 취약점을 공격하며, 기기의 기본 기능을 악용해 은밀하게 데이터를 탈취하고 있습니다. 이러한 핵심 게이트웨이 기기는 카탈로그에 포함되지 않거나 모니터링되지 않는 경우가 많아 공격자가 장기간 은밀하게 액세스할 수 있게 됩니다. 그러므로 조직은 포괄적인 애셋 파악, 엄격한 패치 관리, 중앙 집중식 로깅을 최우선 과제로 삼아 네트워크 경계를 확실하게 제어해야 합니다.

필수 확인 사항

- **제로데이 취약점 공격의 가속화:** 취약점 공격의 평균 소요 시간이 급격히 줄어들었습니다. 즉, 공급업체가 패치를 배포하기도 전에 공격자가 에지 및 핵심 네트워크 기기를 포함한 여러 시스템을 점점 더 빠르게 침해하고 있습니다.
- **보안 사각지대에 있는 네트워크 기기:** 에지 어플라이언스는 기존 EDR 소프트웨어를 실행할 수 없기 때문에 공격자는 이를 안전한 은신처로 활용합니다. 공격자는 인메모리 기반 커스텀 멀웨어를 배포하여 탐지를 회피하고 원격 분석이 부족한 환경에서 장기간 활동을 지속합니다.
- **엔드포인트 보안 무력화:** 정교한 공격자는 정찰부터 데이터 도용에 이르는 전체 공격 수명 주기의 거의 모든 단계를 네트워크 인프라에서 직접 수행하며, 모니터링이 철저하게 이루어지는 워크스테이션과 서버를 완전히 우회합니다.
- **사고 대응 체계의 마비:** 에지 기기는 저장용량이 매우 작고 업타임 요구사항을 엄격하게 지켜야 하므로, 침해가 발생하더라도 일반적인 파일 시스템 포렌식 분석이 불가능한 경우가 많습니다. 이로 인해 증거가 소실되기 전에 공격자의 존재를 확인하기 어려운 상황이 발생합니다.
- **기본 기능을 공격에 악용하는 공격자:** 공격자가 내장된 관리용 서브셸과 기본적인 패킷 캡처 기능을 사용하여 기기를 통과하는 실시간 트래픽 사본을 수집하는 경우가 늘고 있습니다. 이 방법으로 일반 텍스트 네트워크 프로토콜에서 비밀번호를 추출할 수 있으며 탐지 가능한 멀웨어를 배포하지 않고도 레이더망을 피할 수 있습니다.

향후 실행 과제

- **네트워크 로그의 중앙 집중화 및 관리 체계 구축:** 엔드포인트 데이터에만 의존해서는 안 됩니다. 특히 애플리케이션 로그와 관리 로그를 포함한 핵심 네트워크 기기 로그를 중앙 SIEM으로 전송하고, 관리 로그는 조사 과정에서 가시성을 확보할 수 있도록 최소 1년 이상 보관해야 합니다.
- **엄격한 취약점 관리 체계 구축:** 네트워크 기기를 전체 취약점 스캔 및 애셋 관리 프로그램에 포함해야 합니다. 명확한 관리 책임을 정의하고 비즈니스 운영에 지장을 주지 않는 범위 내에서 단계별 패치 적용 일정을 수립해 공격자가 악용하기 전에 취약점을 신속하게 해결해야 합니다.
- **네트워크 전용 사고 대응 플레이북 개발:** 보안팀은 상세한 아키텍처 다이어그램과 사고 대응 플레이북을 마련해야 합니다. 또한 일반적인 재부팅이나 전원을 껐다 켰다 하는 과정에서 중요한 휘발성 증거가 삭제되지 않도록 포렌식 수집 절차를 미리 계획해 두어야 합니다.
- **미등록 네트워크 자산의 전수 조사 및 식별:** 에지 어플라이언스는 배포된 후 잊혀지는 경우가 많기 때문에 보안팀은 포괄적인 검색 스캔을 통해 카탈로그 목록에 없는 시스템을 식별해야 합니다. 존재 여부조차 모르는 애셋은 조직에서 보호하거나, 패치를 적용하거나, 모니터링할 수 없기 때문입니다.

서드 파티 SaaS 침해)의 연쇄적 파급 효과

핵심 요점

클라우드 중심 인프라로 전환되면서 SaaS 애플리케이션이 대규모 공급망 공격의 통로가 되고 있습니다. 공격자는 통합 토큰을 탈취하고 검증되지 않은 서드 파티 앱을 악용하는 방식으로 기존 방어선을 우회하여 단일 공급업체 침해를 기업 전반의 연쇄적 위기로 만들고 있습니다. 이에 대응하기 위해 조직은 반복적인 본인 인증 체계로 전환하고, 최종 사용자 애플리케이션 승인에 대한 거버넌스를 강화하고, 조달 이전 단계에서부터 엄격한 서드 파티 위험 관리를 시행해야 합니다.

필수 확인 사항

- **MFA의 무력화:**공격자는 단순히 비밀번호를 탈취하는 데 그치지 않고 장기간에 걸쳐 OAuth 토큰과 세션 쿠키를 수집하고 있습니다. 이러한 토큰은 로그아웃 후에도 유효한 경우가 많기 때문에 공격자는 MFA 경보를 발생시키지 않고 세션을 탈취할 수 있습니다.
- **시스템 연동으로 인한 새로운 보안 경계:** 공격자는 서드 파티 SaaS 공급업체를 침해하여 하드코딩된 키와 개인 액세스 토큰을 탈취하고, 훔친 보안 비밀을 활용해 다운스트림 고객 환경으로 원활하게 전환한 뒤 대규모로 데이터를 도용합니다.
- **고도화되고 있는 소셜 엔지니어링:** 금전적 이득을 노리는 공격 그룹이 IT 헬프 데스크를 표적으로 삼아 보이스 피싱을 통해 적극적으로 공격하고 있습니다. 공격자는 직원으로 가장하여 보안 제어를 우회하고 초기 SaaS 액세스 권한을 확보한 뒤 표적 환경 내에서 더 높은 권한이 필요한 키를 채굴합니다.

향후 실행 과제

- **SaaS 자산 식별 및 거버넌스 구현:** 기존 애셋 관리 방식으로는 클라우드 앱을 충분히 파악하기 어렵습니다. SaaS 보안 상황 관리(SSPM) 도구를 배포하여 모든 애플리케이션, 통합, 숨겨진 보안 비밀(예: API 키)을 적극적으로 인벤토리화하여 사각지대를 없애야 합니다.
- **ID 제어 강화:** 모든 SaaS 애플리케이션이 중앙 ID 공급업체(IdP)를 통해 인증되도록 의무화해야 합니다. 서드 파티 API 키에는 최소 권한의 원칙을 엄격하게 적용하고, 와일드 카드 권한을 제거하며, 적시(JIT) 액세스 방식을 활용해 상시 권한을 최소화해야 합니다.
- **라이프사이클 자동화 전략:** 모든 보안 비밀과 서비스 계정 사용자 인증 정보에 대해 자동 순환을 구현해야 합니다. 또한 탈취된 쿠키가 다크 웹에서 거래되더라도 즉시 가치가 떨어지도록 액세스 토큰과 브라우저 세션의 유효 기간을 최대한 짧게 설정해야 합니다.
- **최종 사용자 앱 승인 권한 제한:** 관리자는 최종 사용자가 검증되지 않은 서드 파티 애플리케이션을 승인하지 못하도록 제한해야 합니다. 이렇게 하면 검증된 애플리케이션만 지속적으로 토큰을 획득하도록 할 수 있으며, 결과적으로 악성 OAuth 애플리케이션이 환경에 액세스할 수 있는 경로를 효과적으로 차단할 수 있습니다.
- **외부 공급업체 보안 리스크 관리 체계의 강제화:** 서드 파티 애플리케이션에서 비롯된 위험은 곧 프로덕션 환경의 위험이기도 합니다. 조직은 공급업체 온보딩 전에 검증을 수행하는 강력한 서드 파티 위험 관리 프로그램을 도입해야 하며, 조달 과정에서 싱글 사인온(SSO), 세분화된 감사 로그, 안전한 개발 프로세스 같은 요건을 필수로 포함해야 합니다.

전체 보고서를 다운로드하세요.

조직에서 사이버 사고가 의심되거나 보안 침해를 겪고 있다면 Mandiant에 문의하여 사고 대응 지원을 받아보세요.

Google Cloud

자세한 내용은 cloud.google.com을 참조하세요.