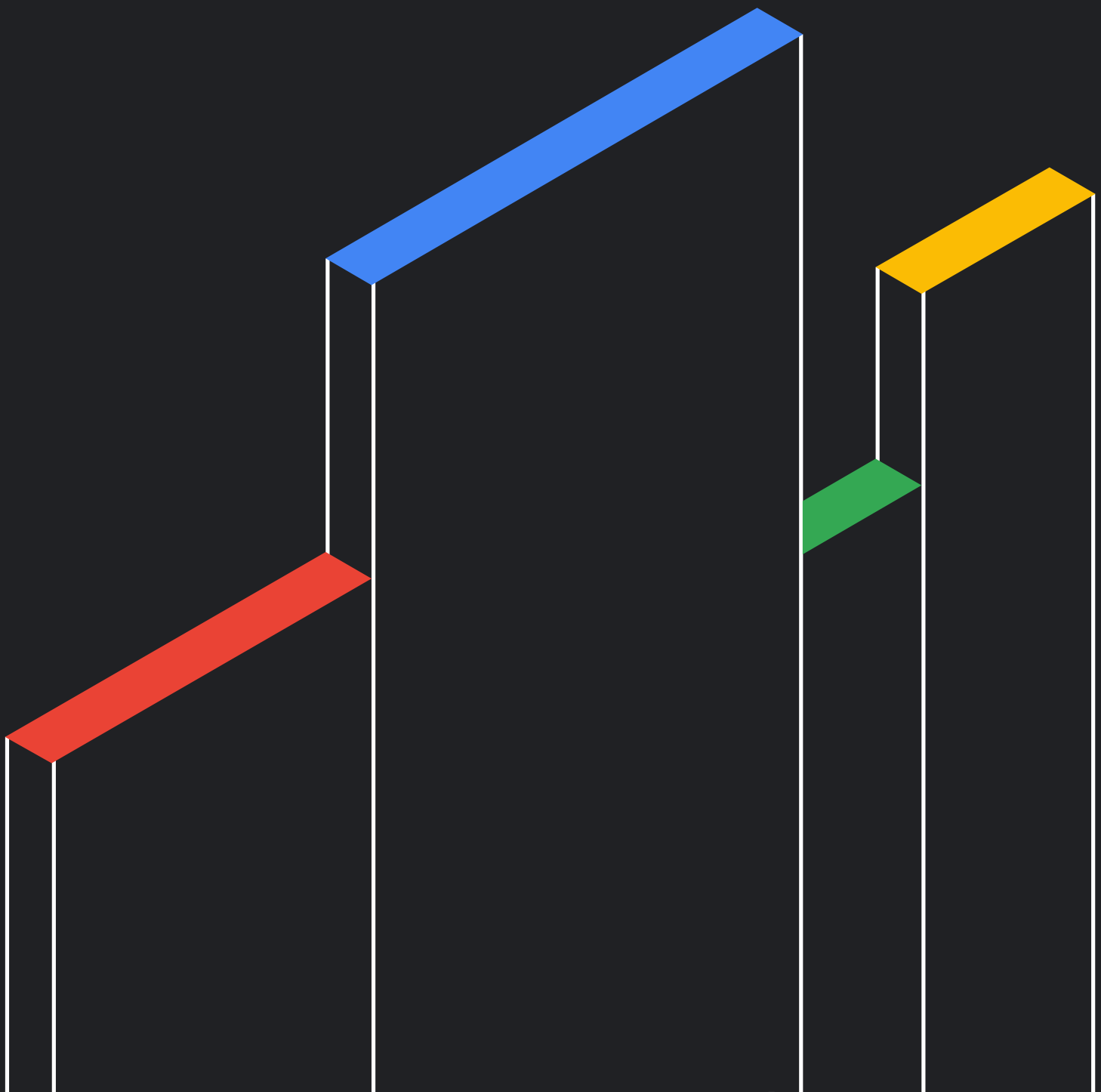
Mandiant

Google Cloud Security

M-Trends

2025 보고서

핵심 요약



숫자로 보는 M-Trends 데이터

M-Trends 2025에 포함된 지표는 2024년 1월 1일부터 2024년 12월 31일 사이에 실시한 표적 공격 활동에 대한 Mandiant 컨설팅의 조사를 바탕으로 합니다.

알아두어야 할 사항은 무엇인가요?

- 2024년에도 지속적으로 금전적 이익을 노리는 위협 행위자가 다른 동기를 가진 행위자들보다 많았습니다. 위협 그룹의 55%가 금전적 이익을 목적으로 활동했으며, 이는 2022년 48%, 2023년 52%에서 꾸준히 증가한 수치입니다. 스파이 활동이 목적이었던 위협 그룹은 8%로, 2023년의 10%에서 소폭 감소했습니다.
- 가장 흔히 사용되는 초기 감염 벡터는 5년 연속으로 익스플로잇(33%)이었습니다. 도용된 사용자 인증 정보(16%)가 2024년에 처음으로 두 번째로 가장 흔히 사용되는 초기 감염 벡터로 확인되면서 사용도가 높아지고 있음을 보여주었습니다. 그 외의 상위 5개 벡터에는 이메일 피싱(14%), 웹 침해(9%), 사전 보안 침해(8%) 등이 포함되었습니다.
- 가장 빈번하게 표적이 된 업종은 금융(17.4%), 비즈니스 및 전문 서비스(11.1%), 첨단 기술(10.6%), 정부(9.5%), 의료(9.3%) 순이었습니다. 이러한 표적 트렌드는 지난 몇 년 동안의 트렌드와 거의 일치합니다.
- 조직이 악의적인 활동을 처음 인지한 경로는 외부 기관을 통한 경우가 57%, 내부에서 파악한 경우가 43%였습니다. 외부에서 악의적인 활동을 통보한 경우 해당 주체는 법 집행 기관, 사이버 보안 공급업체와 같은 기관이 43%, 공격자가 14%였으며, 공격자들은 주로 랜섬 노트를 사용해 악의적인 활동을 통보했습니다.
- 랜섬웨어는 공격자가 통보한 경우가 49%, 외부 기관이 통보한 경우가 21%, 내부적으로 파악한 경우가 30%였습니다.
- 전 세계 평균 드웰 타임(dwell time)은 11일로, 2023년 10일에서 증가했지만 2022년에 보고된 16일보다는 감소했습니다.
- 전 세계 평균 드웰 타임(dwell time)은 외부 기관이 통보한 경우 26일, 공격자가 통보한 경우 5일, 조직이 내부적으로 악의적인 활동을 파악한 경우 10일이었습니다.
- 조사에서 관찰된 205개의 멀웨어 패밀리 중 35%는 백도어, 14%는 랜섬웨어, 8%는 드로퍼, 7%는 다운로더, 6%는 터널러, 5%는 사용자 인증 정보 스틸러였습니다. 이러한 조사 결과는 지난 몇 년 동안의 결과와 비교적 일치합니다. 기존의 멀웨어를 사용한 공격이 아닌, 표적 시스템상의 합법적인 도구와 기능을 악용하는 LotL(living off the land) 유형의 공격 또한 지속적으로 발견되고 있습니다.

어떤 조치를 취해야 하나요?

- 엔드포인트 탐지 및 대응, 고급 분석이 포함된 보안 정보 및 이벤트 관리(Security Information and Event Management, SIEM), 네트워크 트래픽 분석을 포함한 고급 위협 탐지 기술을 배포하고 최적화합니다.
- 정기적으로 취약점을 스캔하고, 위험 정도에 따라 패치를 적용할 우선순위를 정하고, 가능한 경우 패치 프로세스를 자동화하여 공격 표면을 최소화합니다.
- 최소 권한과 같은 탄탄한 기반을 마련하여 액세스 제어를 강화합니다. 사용자 및 애플리케이션 권한을 필수 권한으로 제한하고 가급적 FIDO2를 준수하는 다중 인증(Multi-Factor Authentication, MFA)을 시행하고 정기적으로 액세스 로그를 검토합니다.
- 사고 대응 및 복구 계획을 수립하고 정기적으로 테스트합니다. 랜섬웨어 및 조직과 가장 관련성이 높은 기타 위협에 대한 구체적인 플레이북을 계획에 포함합니다. 모의 훈련과 시뮬레이션을 실시하여 이러한 계획의 효과를 검증하고 대응 시간을 개선합니다.
- 레드팀을 통해 공격자 전술을 현실적으로 에뮬레이션하여 방어 체계를 테스트합니다. 보안팀이 탐지하고 대응하기까지 소요되는 시간을 측정하고, 기존 방어 체계의 취약점과 빈틈도 파악합니다.
- 지속적인 보안 인식 교육과 피싱 시뮬레이션에 투자합니다. 직원을 대상으로 피싱, 소셜 엔지니어링, 랜섬웨어 전술을 포함하여 가장 관련성 높은 최신 위협에 대해 교육합니다.

지속적으로 엔터프라이즈 시스템을 위협하는 인포스틸러 멀웨어

알아두어야 할 사항은 무엇인가요?

- 사용자 인증 정보, 브라우저 데이터와 같은 민감한 정보를 훔치는 인포스틸러 멀웨어가 증가하면서 조직이 침해 위험에 처하고 있습니다.
- 공격자는 시스템에 대한 초기 액세스를 확보하기 위해 인포스틸러 로그에서 훔친 사용자 인증 정보를 사용하며, 이는 데이터 도용, 갈취, 기타 악의적인 활동으로 이어집니다.
- UNC5537 그룹은 인포스틸러 멀웨어를 통해 훔친 사용자 인증 정보로 Snowflake 고객 데이터베이스 인스턴스를 표적으로 삼아 공격할 수 있었습니다. 이는 인포스틸러 마켓플레이스에서 유통되는 방대한 사용자 인증 정보가 초래하는 결과를 잘 보여줍니다.
- 업무용 개인 기기와 외주 시스템이 고유한 보안 문제점을 발생시키고 있습니다. 예를 들어 인포스틸러는 감염된 개인 시스템 또는 동기화된 브라우저에서 사용되는 기업 사용자 인증 정보를 침해할 수 있습니다.

어떤 조치를 취해야 하나요?

- 강력한 MFA를 구현하되, 특히 AiTM(Adversary-in-the-Middle) 공격을 방지하는 하드웨어 보안 키나 모바일 OTP 앱과 같은 MFA 방법을 사용합니다.
- 감염을 모니터링하고 방지하기 위한 엔드포인트 탐지 및 대응(Endpoint Detection and Response, EDR)과 침입 탐지 시스템(Intrusion Detection Systems, IDS)을 배포하여 엔드포인트 보안을 강화합니다.
- 개인 기기와 회사 기기 사용을 분리하기 위한 엄격한 정책을 수립하고, 서드 파티 공급업체 및 계약업체의 보안 제어를 검토합니다.
- 브라우저에 제어 기능을 적용하여 서드 파티 쿠키를 제한하고, 비밀번호 자동 완성을 끄고, 승인되지 않은 브라우저 확장 프로그램 사용을 중지합니다.
- 소프트웨어 사용 정책을 수립하고, 신뢰하지 않는 출처에서 파일을 다운로드하지 않도록 사용자를 교육하고, 검증된 애플리케이션만 이용 가능한 사내 전용 애플리케이션 스토어 구현을 고려합니다.

북한의 내부자 위협

알아두어야 할 사항은 무엇인가요?

- 북한(Democratic People's Republic of Korea, DPRK)은 수익을 창출하고 국가 자금을 조달하기 위해 자국민을 원격 IT 계약직으로 파견합니다.
- 북한의 IT 인력은 훔치거나 위조된 신분증, 가짜 채용 이력 및 증빙 서류를 사용하여 주로 미국 또는 유럽에 소재한 기술 회사의 고소득 직종에 취업합니다.
- 이들은 고용된 후에는 가상 사설망(Virtual Private Networks, VPN)과 현지 협력자를 통해 실제 위치를 마스킹하고 회사 시스템에 대한 액세스 권한을 유지하면서 합법적인 네트워크 트래픽에 섞여 들어 탐지를 피합니다.
- 한편 이들의 직접적인 악의적인 활동은 제한적이었으나, 회사 인프라에 액세스할 수 있다는 사실은 스파이 활동, 데이터 도용, 갈취 위험이 발생할 수 있음을 시사합니다. 또한 갈취의 경우 이미 몇 차례 발생한 바 있습니다.

어떤 조치를 취해야 하나요?

- 생체 인식 확인을 포함하여 직원에 대해 철저하게 신원 확인을 실시하고 독립적인 출처와 대조하여 교육 및 채용 이력을 검증합니다.
- 화상 면접을 실시하여 이를 꺼리는 지원자를 경계하고, 지원자가 제공한 인물 정보와 실제 외형적 특징 사이의 불일치를 확인함으로써 면접 절차를 개선합니다.
- 가능한 경우 직접 방문하여 신분증 확인 후 회사 노트북을 수령하도록 요구합니다. 채용 서류에 기재되지 않은 주소로 회사 리소스를 배송하는 경우 추가적인 검증을 위해 신원 조사를 실시합니다.
- EDR 도구를 설치하고, 원격 액세스 소프트웨어와 VPN 연결(특히 Astrill VPN)을 모니터링하고, 휴먼 인터페이스 장치(Human Interface Device, HID) 연결을 기록합니다.
- 최소 권한 액세스를 적용하여 각 직무에 필요한 데이터와 리소스로만 사용자 액세스를 제한합니다. 이를 통해 스파이 활동, 데이터 도용 또는 갈취 시도로 인한 잠재적 피해를 최소화할 수 있습니다.

2024년 이란의 위협 환경

알아두어야 할 사항은 무엇인가요?

- 2024년에는 이란 연계 공격자의 사이버 작전이 증가했습니다. 특히 이스라엘 기관을 표적으로 삼아 공격했으며 다양한 방법을 사용하여 침투 성공률을 높였습니다.
- 이란 연계 공격자에 의한 맞춤형 멀웨어가 2023년 대비 35% 급증했고 45개 이상의 새로운 멀웨어 패밀리가 발견되었습니다.
- 이스라엘에 소재한 표적을 공격할 때 주로 와이퍼 멀웨어를 이용한 파괴 및 교란 작전이 집중되었는데, 이러한 작전에는 이란과 연계 공격자와 관련된 다양한 온라인 페르소나의 해킹 및 유출 작전이 수반되는 경우가 많았습니다.
- 이란 연계 공격자는 탐지를 피하기 위해 공개 리소스, 클라우드 인프라, 원격 모니터링 및 관리(Remote Monitoring and Management, RMM) 소프트웨어와 같은 합법적인 도구를 활용했습니다.
- 그래픽 사용자 인터페이스(Graphical User Interface, GUI)를 도입해 멀웨어를 위장하고 최신 사건과 취업 관련 주제를 이용해 표적을 속이는 등 더욱 정교한 소셜 엔지니어링 기법을 사용했습니다.

어떤 조치를 취해야 하나요?

- 피싱 방지(phishing-resistant) MFA, 특히 권한이 있는 계정에 인증서 기반 인증(Certificate-Based Authentication, CBA) 및 FIDO2 보안 키를 시행하여 자격 증명 수집 및 MFA 우회 시도에 대응합니다.
- 보안 제어를 정의하고 모든 클라우드 기반 활동에 대한 가시성을 확보하며 위협 헌팅, 사고 대응, 지속적인 모니터링을 위한 데이터를 제공하는 등 클라우드 기술 도입을 위한 보안 우선 설계를 구현합니다.
- 조직 보안 경계 밖의 개인을 표적으로 한 공격 등 점점 더 복잡해지는 소셜 엔지니어링 공격 캠페인을 인식하고 대응하는 데 중점을 두고 포괄적인 사용자 인식 교육을 실시합니다.
- 공격자가 기존의 탐지 방법을 우회할 수 있는 RMM 소프트웨어와 같은 합법적인 도구를 사용한다는 점에 경각심을 가져야 합니다. 비정상적인 RMM 활동에 대한 모니터링 및 감사를 구현하고, 필요시 정상적인 도구 사용은 허용하도록 탐지 기능을 조정합니다.
- 공동 방어가 중요하므로 여러 업종 및 분야에 걸쳐 협업하여 이란 연계 공격자에 맞서 방어하기 위한 위협 정보와 권장사항을 공유합니다.

클라우드 및 Software as a Service 환경에서 데이터 도용의 진화

알아두어야 할 사항은 무엇인가요?

- 공격자는 온프레미스 네트워크를 표적으로 삼던 방식에서 싱글 사인온(Single Sign-On, SSO) 포털과 같은 클라우드 기반의 중앙 집중식 인증 저장소를 표적으로 삼는 방식으로 전환하여 광범위한 액세스 권한을 확보하려 하고 있습니다.
- 소셜 엔지니어링은 기존 네트워크 제어를 우회하여 Software as a Service(SaaS) 환경에 대한 권한이 있는 사용자를 표적으로 삼아 공격하는 용도로 점점 더 많이 사용되고 있습니다.
- 공격자는 하이브리드 접근 방식을 사용하여 온프레미스와 클라우드 리소스를 결합하고 합법적인 트래픽에 악의적인 활동을 혼합해 탐지를 회피하고 있습니다.
- 클라우드 환경에서 로깅 및 모니터링이 충분히 이뤄지지 않을 경우 사각지대가 발생하여 공격자 활동을 탐지하기가 어려워지고 조사가 늦어집니다.
- 공격자는 클라우드의 책임 공유 모델에 대한 이해가 부족한 조직에서 발생하는 관리되지 않는 위험을 악용하고 있습니다.

어떤 조치를 취해야 하나요?

- 모든 클라우드 서비스에 걸쳐 네트워크 트래픽 로그, 방화벽 로그, 스토리지 액세스 로그, 컴퓨팅 및 리소스 모니터링, 감사 로그, 데이터베이스 로그, ID 및 액세스 관리(Identity and Access Management, IAM) 로그를 포함한 포괄적인 로깅을 사용하도록 설정해야 합니다.
- MFA를 포함한 강력한 IAM 방식을 구현하고 SSO 포털과 권한이 있는 계정에서 의심스러운 활동이 일어나는지 면밀히 모니터링합니다.
- 클라우드 및 SaaS 제공업체와 정기적으로 구독 수준을 검토하고 검증하여 필수 로깅 및 보안 가시성 요구사항을 충족하는지 확인합니다.
- 클라우드와 SaaS 환경을 표적으로 삼아 공격하는 소셜 엔지니어링 전술에 대해 사용자에게 교육하고 비밀번호 재설정, MFA 등록과 관련된 요청을 검증하기 위한 명확한 절차를 수립합니다.
- 클라우드 보안의 책임 공유 모델을 완전히 이해하고, 조직과 클라우드 제공업체 간의 보안 책임을 명확하게 구분합니다.
- 하이브리드 환경을 고려한 사고 대응 계획을 수립하되, 통합 온프레미스 및 클라우드 시스템에 대한 탐지, 격리, 근절, 복구 절차에 중점을 둡니다.

클라우드 침해 조사의 공통적인 주제

알아두어야 할 사항은 무엇인가요?

- 공격자가 클라우드 환경에 액세스하기 위해 클라우드 경계를 넘어 확장되어 있는 잘못된 구성을 악용하는 경우가 증가하고 있습니다. 이는 성숙한 클라우드 보안을 갖춘 조직에서도 마찬가지입니다.
- 성공한 클라우드 침해에 자주 등장하는 세 가지 주제는 1) 보안 정책이 충분히 발전되지 않은 ID 솔루션, 2) 적절히 보호되지 않는 온프레미스 통합, 3) 확장된 클라우드 공격 표면에 대한 가시성 부족입니다.
- ID 침해가 자주 발생하는 경로는 MFA와 같은 보안 제어 수단이 없는 ID 아키텍처와 관행, 쉽게 우회가 가능한 비밀번호 재설정 포털, 부적절한 서드 파티 액세스 제어입니다.
- 온프레미스와 클라우드 인프라 간의 통합이 제대로 보호되지 않으면 공격자는 여러 환경 사이를 수직적으로 이동하면서 클라우드 보안 제어를 우회할 수 있습니다.
- 클라우드 공격 표면에는 네트워크 노출뿐만 아니라 열거된 데이터, 무분별하게 확산된 사용자 인증 정보, 공개적으로 노출된 리소스도 포함되므로 조직은 이 확장된 공격 표면을 선제적으로 식별하고 줄여야 합니다.

어떤 조치를 취해야 하나요?

- 강력한 피싱 방지 MFA를 구현하여 ID 보안을 강화하고 안전한 비밀번호 재설정 프로세스를 확보하고 서드 파티 액세스를 엄격히 제어합니다. 권한이 있는 ID 관리(Privileged Identity Management, PIM)를 사용하고 외부 인력을 위한 별도의 ID 저장소를 마련합니다.
- 신뢰할 수 있는 서비스 인프라, 온프레미스와 클라우드 환경 간의 컴퓨팅 및 네트워크 통합을 감사하고 보호하여 온프레미스 통합을 보호합니다. 관리 인터페이스에 대한 액세스를 정기적으로 검토하고 제한하며, 네트워크 연결이 적절하게 세분화되었는지 확인합니다.
- 데이터 열거를 관리하고 사용자 인증 정보의 무분별한 확산에 대처하고 공개적으로 노출된 리소스를 보호하여 클라우드 공격 표면을 선제적으로 파악해 줄입니다. 포괄적인 가시성과 규정 준수 모니터링을 위한 클라우드 보안 태세 관리 플랫폼을 사용합니다.
- ID, 리소스, 네트워크, 엔드포인트를 포함한 모든 계층에 걸쳐 액세스 제한, 강화 조치, 지속적인 탐지 전략, 선제 대응 조치를 포함하는 포괄적인 다층 보안 접근 방식을 도입합니다.

Web3와 암호화폐에 대한 위협

알아두어야 할 사항은 무엇인가요?

- 암호화폐와 블록체인을 포함한 Web3 기술이 절도와 자금 세탁, 불법 활동 자금 조달을 위해 공격을 받는 경우가 증가하고 있습니다.
- 북한과 연계된 세력을 포함한 공격자는 정교한 소셜 엔지니어링 전술을 사용하고 취약점을 악용하여 지금까지 상당한 양의 디지털 애셋을 훔쳤습니다.
- 암호화폐 거래는 난독화된 자금 흐름과 스마트 계약의 불변성으로 인해 추적하고 규제하기가 어려우며, 악성 인프라를 호스팅하는 데 악용될 가능성도 있습니다.
- '드레이너'와 악성 스마트 계약은 사용자 지갑에서 암호화폐를 훔치는 데 사용되며, 이러한 공격을 부추기는 '서비스형 드레이너(Drainer-as-a-Service, DaaS)' 시장도 등장했습니다.
- Web3 기술을 도입하는 조직은 빠른 통합과 견고한 보안 사이에서 균형을 유지하는 데 어려움을 겪고 있으며, 표준 보안 제어를 소홀히 하여 기술 부채가 발생하고 공격 범위가 확대되는 결과를 초래하는 경우가 많습니다.

어떤 조치를 취해야 하나요?

- 거래 데이터 분석을 엔드포인트 및 보안 원격 분석과 결합하여 Web3와 암호화폐 플랫폼을 표적으로 삼아 공격하는 악의적인 활동을 더 효과적으로 탐지합니다.
- 핵심 지갑 인프라와 암호화 제어에만 집중하는 것을 넘어 표준 보안 제어를 구현하고 유지 관리하여 기술 부채를 방지하고 공격 표면을 줄여야 합니다.
- 직원을 대상으로 소셜 엔지니어링 전술에 대한 교육을 실시합니다. 공격자는 초기 액세스 권한을 얻기 위해 피싱, 가짜 채용 정보와 같은 소셜 엔지니어링 수법을 자주 사용하므로 직원을 교육하여 이러한 전술을 인지하고 피하도록 하는 것이 중요합니다.
- 공격자는 거래 또는 암호화폐 소프트웨어를 트로이 목마로 만들어 소프트웨어 공급망을 침해할 수 있으므로, 조직은 모든 서드 파티 소프트웨어를 배포에 앞서 철저히 심사하고 확인해야 합니다.
- 디지털 애셋을 훔치려고 하는 악성 스마트 계약과 '드레이너'를 경계해야 합니다. 암호화폐 지갑에 대한 무단 액세스를 탐지하고 차단하기 위해 모니터링을 구현합니다.

보호되지 않는 데이터 저장소

알아두어야 할 사항은 무엇인가요?

- 조직에서 파일 공유, SharePoint 사이트와 같은 내부 데이터 저장소에 대한 보안을 간과하는 경우가 많습니다.
- 이러한 저장소는 일반적으로 표준 권한이 있는 직원이 액세스할 수 있으며 사용자 인증 정보, 재무 데이터, 지식 재산을 비롯한 민감한 정보를 포함할 수 있습니다.
- 금전적 이익을 노리는 공격자는 갈취를 위해, 지능형 지속 공격(Advanced Persistent Threat, APT) 그룹은 스파이 활동을 위해 보호되지 않는 데이터 저장소를 표적으로 삼아 공격합니다.
- 보호되지 않은 데이터 저장소는 공격자가 더 적은 노력으로 목표를 달성할 수 있게 합니다. 멀웨어 또는 제로데이 익스플로잇과 같은 고급 방법을 사용하지 않고도 목표(권한 상승 등)를 달성할 수 있기 때문입니다.

어떤 조치를 취해야 하나요?

- 데이터 저장소에 대해 인벤토리와 감사를 수행합니다. 민감한 정보가 저장된 위치를 파악하고 콘텐츠를 정기적으로 검토하고 불필요하거나 오래된 데이터를 제거합니다.
- 사용자에게 직무상 필요한 액세스 권한만 부여하며, 읽기 액세스 권한과 읽기/쓰기 액세스 권한을 구분하고 포괄적인 권한 부여를 자제합니다.
- 직원을 대상으로 데이터 보안 권장사항, 민감한 정보 보호의 중요성, 노출된 데이터 사례를 보고하는 방법에 대한 교육을 실시합니다.
- 전송 중인 데이터와 저장 중인 데이터를 모두 암호화하여 노출을 제한합니다.
- 자동화된 도구를 사용하여 노출된 사용자 인증 정보와 보안 비밀을 파악하고, 정기적인 보안 평가를 수행하여 제어 수단의 효과를 평가합니다.
- 중요한 데이터 스토어를 대상으로 한 모든 액세스 시도에 대해 FIDO2를 준수하는 MFA를 필수 보안 조치로 구현합니다.
- 데이터 손실 방지(Data Loss Prevention, DLP) 기술을 구현하여 이메일 및 파일 공유를 통해 민감한 데이터가 보안 환경을 벗어나지 않도록 효과적으로 방지합니다.

전체 보고서를 다운로드해 보세요.

조직에 사이버 이슈가 의심되거나 보안 침해를 겪고 있다면 사고 대응 지원을 받을 수 있도록 Mandiant에 문의하시기 바랍니다.

Google Cloud

자세한 내용은 **cloud.google.com**을 참조하세요.