MANDIANT
NOW PART OF Google Cloud

M-Trends 2023 스페셜 리포트

개요

14 번째 에디션인 M-Trends 2023 보고서는 www.mandiant.kr/m-trends 에서 확인하실 수 있습니다 .

숫자로 보는 M-Trends 데이터

제공되는 정보는 2022 년 1 월 1 일부터 12 월 31 일 사이에 실시한 Mandiant 컨설팅 조사를 기반으로 합니다 .

주요 내용

- 전 세계적으로 보면 공격이 빠르게 탐지되고 있는 가운데 , 미주와 EMEA 지역에서는 개선되는 모습이 보이지만 , APAC 지역에서는 아직 그렇지 못했습니다 .
- 침해 상황을 알게 되는 경로로는 조직의 내부 보안팀보다 보안 벤더와 기타 외부 소스가 더 높지만 , 공격 탐지 속도는 내부 팀이 외부 조직보다 더 빠릅니다 .
- 공격자들은 조직에 대한 액세스 권한을 얻기 위해 미주 지역에서는 익스플로잇 , EMEA 지역에서는 피싱 , APAC 지역에서는 계정 도용 등 지역별로 가장 효과적인 방법을 활용하고 있습니다 .

CISO 에게 질문할 사항

- 우리 조직의 탐지 및 대응 시간은 어떻게 측정하며 , 탐지부터 대응 및 복구까지 평균 얼마나 걸립니까 ?
- 우리 조직은 가장 보편적인 멀웨어 , 익스플로잇 , 피싱과 같은 초기 감염 벡터를 탐지하고 이에 대응할 대비가 되어 있습니까 ?
- 침해를 당했을 가능성이 있다는 서드파티의 알림을 받았을 때 우리는 어떤 프로토콜을 따릅니까 ?
- 우리는 시스템의 알려진 취약점이 악용되는 것을 완화할 수 있는 기반을 갖추고 있습니까 ?

우크라이나 침공

주요 내용

- Mandiant 는 2022 년 2 월 24 일 러시아의 우크라이나 침공과 그 이후로 이어진 광범위한 사이버 스파이 활동 , 조직의 와해를 조장하는 파괴적인 사이버 공격 , 정보 작전을 확인했습니다 .
- 러시아의 작전은 산업 제어 시스템과 핵심 인프라에 영향을 주었고 , 일부는 침공 전 이루어진 캠페인과 확보한 액세스 권한 덕분에 수행할 수 있었습니다 .
- 러시아의 우크라이나 침공은 사이버 작전과 전통적 전쟁 양상의 결합이 새로운 표준이 되었음을 보여 주었습니다 .

CISO 에게 질문할 사항

- 우리 조직은 파괴적 와해성 공격에 대비하여 시스템을 강화하기 위한 조치를 취했습니까 ?
- 가장 최근에 백업 및 운영 연속성 계획을 테스트한 결과는 어떻게 나왔습니까 ?
- 정보 작전에 맞서 싸우기 위해 위협 인텔리전스를 이용해야 합니까 ?

북한의 금융 관련 공격

주요 내용

- 전통적인 정보 수집 임무나 파괴적 공격도 하지만 , 북한의 작전 요원들은 2022 년에 암호화폐 절도와 사용에 더 많은 관심을 보였습니다 .
- 암호화폐로 높은 수익을 냈기 때문에 암호화폐의 절도와 사용은 2023 년 내내 계속될 가능성이 높습니다 .

CISO 에게 질문할 사항

- 우리는 우리 조직을 대상으로 할 가능성이 높은 금융 위협에 얼마나 대비되어 있습니까 ?

핵심 요소의 변화와 특수 기법

주요 내용

- 기술적 역량이 부족한 공격자들도 조직에 엄청난 영향을 끼치고 있습니다 .
- 이들의 작전으로도 데이터 절도 , 지적 재산 도용 , 조직의 치명적 평판 손상이라는 결과를 불러옵니다 .
- 이러한 공격자들은 금전이나 스파이 활동보다 악명을 얻는 것이 동기인 것으로 보이며 , 많은 자원으로 무장했음을 증명해 왔고 , 자신의 목표를 달성하기 위해 뇌물 , 심지어는 괴롭힘과 협박을 시도합니다 .

CISO 에게 질문할 사항

- 우리 조직은 직원들에게 손을 뻗칠 수 있는 소셜 엔지니어링이나 다른 유사한 공격 리스크를 어떻게 최소화하고 있습니까 ?
- 이러한 유형의 공격으로부터 우리 직원들 , 특히 임원과 외부에 많이 알려진 직원들을 보호하기 위해 어떤 프로그램을 운영하고 있습니까 ?
- 독점 정보 또는 고객 개인정보가 도용되어 우리를 대상으로 한 갈취 공격에 사용된다면 어떻게 대응해야 합니까 ?
- 갈취 공격에 대응하여 신속하게 암호화폐를 회수할 수 있는 절차가 마련되어 있습니까 ?

클라우드 중심 – 레드팀 사례 연구

주요 내용

- 레드팀은 실제 공격 시나리오에 대응하는 조직의 보안 프로그램 역량을 평가하여 보안 태세를 개선하는 데 도움을 줍니다 .
- Mandiant 는 공격자가 주요 클라우드 및 운영기술 (OT, Operational Technology) 환경에 어떻게 침투하는 지 한 인프라 기업에 보여주었습니다 .

CISO 에게 질문할 사항

- 조직의 클라우드 사용 현황을 정확히 파악할 수 있습니까 ?
- 공격자들이 악용할 수 있는 구성 오류 유무를 정기적으로 점검하고 있습니까 ?
- 클라우드 아키텍처 배포를 테스트하고 있습니까 ?

캠페인 및 글로벌 이벤트

주요 내용

- Mandiant 의 캠페인 및 글로벌 이벤트팀은 더 효과적인 고객 보호를 위해 2022 년 한 해 동안 러시아 스파이 활동 , 랜섬웨어 , 주요 취약점 (Log4Shell 등) 을 조사했습니다 .
- Mandiant 는 고객과 커뮤니티가 이러한 캠페인으로부터 스스로를 보호하는 데 도움이 되도록 유용한 인텔리전스와 지표를 공유합니다 .

CISO 에게 질문할 사항

- 네트워크의 취약점을 추적하고 패치하기 위해 어떤 조치를 취하고 있습니까 ?
- 현재 위협 인텔리전스를 어떻게 사용하여 의사 결정에 필요한 정보를 얻고 있습니까 ?

APT42 – 주목할 만한 분류 사례

주요 내용

- APT42 는 이란을 배후로 둔 위협 그룹으로 , 정교한 피싱과 소셜 엔지니어링 공격을 바탕으로 스파이 활동을 수행하고 있습니다 .
- APT42 의 활동은 이란 관련 프로젝트에 참여하고 있는 외교 정책 관계자 , 평론가 , 언론인 , 특히 미국 , 영국 , 이스라엘의 관계자들에게 위협이 되고 있습니다 .

CISO 에게 질문할 사항

- 우리 조직의 보안 , IT, 비즈니스 팀에서 전체 직원을 보호하기 위해 무엇을 해야 합니까 ?
- 우리 조직은 직원들에게 손을 뻗칠 수 있는 소셜 엔지니어링 공격 리스크를 어떻게 최소화하고 있습니까 ?
- 직원들이 피싱 및 기타 소셜 엔지니어링 시도를 인지하도록 하려면 어떻게 해야 합니까 ?

자세한 정보 : www.mandiant.kr/m-trends

Mandiant

서울특별시 강남구 테헤란로 152
강남파이낸스센터 22 층

02-6959-4017
korea-mandiant@google.com

Mandiant 소개

Mandiant 는 역동적 사이버 방어 , 위협 인텔리전스 및 침해 사고 대응 서비스 분야에서 인정 받는 리더로서 , 수십 년간 사이버 보안의 최일선에서 쌓아온 경험을 확장하여 조직이 사이버 위협에 맞서 대응 태세를 갖출 수 있도록 지원합니다 . Mandiant 는 이제 Google Cloud 가 되었습니다 .

MANDIANT
NOW PART OF Google Cloud

©2023 Mandiant, Inc. All rights reserved. Mandiant 와 M-Trends 는 Mandiant, Inc. 의 등록상표입니다 .
다른 모든 브랜드 , 제품 또는 서비스 명칭은 각 소유자의 상표 또는 서비스 마크입니다 . M-EXT-BF-KO-KR-000494-01