MANDIANT
NOW PART OF Google Cloud

Cyber Snapshot Report
제 3 호

The Defender's Advantage Cyber Snapshot 보고서는 Mandiant 가 최일선에서 관찰한 사항과 실제 경험을 바탕으로 점점 중요해지는 사이버 방어 분야에 대한 인사이트를 제공합니다 . 이번 개정판에서는 다음과 같은 주제를 다룹니다 .

암호 없는 인증으로의 여정

과거에는 ID 인증을 위한 기본 메커니즘으로 단일 암호를 사용하는 시도 응답 인증 방식 (CRAM) 이 주로 사용되었습니다 . 하지만 추가적인 ID 검증 요건 없이 단일 트랜잭션의 인증 모델을 사용하는 것은 조직에 상당한 리스크를 초래할 수 있습니다 .

공격자들이 ID 침해에 보다 정교한 기법을 사용하면서 리스크 완화를 위한 새로운 보안 컨트롤과 방법론이 도입되었습니다 . 많은 조직에서 사용하고 있는 가장 일반적인 보안 컨트롤은 다중 인증 (MFA) 요건으로 , 두 가지 이상의 독립적인 방법을 결합하여 ID 를 검증하는 방식입니다 .

Mandiant 는 수많은 침해 사고 대응 조사를 통해 조직에서는 전통적인 다중 인증 (MFA) 방법을 도입하는 비율이 증가했지만 , 공격자들은 다음과 같은 기술을 악용하여 ID 를 침해할 수 있는 공격 기술을 계속 발전시키고 있다는 것을 확인했습니다 .

강제 MFA 우회

취약한 MFA 방식 악용 (예 : SMS, 푸시 알림 , 전화 통화)

MFA 검증 및 인증용으로 공격자가 제어하는 디바이스 등록

이렇게 진화한 위협으로 인해 숫자 매칭 , 상황별 텔레메트리 알림 , 시간 기반 일회성 암호 (TOTP) 입력 등 더욱 강력한 MFA 방식을 갖춘 새로운 툴을 도입하는 데 집중하고 있습니다 . 또한 공급업체와 조직은 FIDO2(Fast Identity Online 2) 키 / 토큰 , 소프트웨어 / 하드웨어 개방형 인증 (OATH) 토큰 또는 인증서 기반 인증을 활용하여 MFA 방식을 더욱 강화하고 있습니다 .

인증자

인증 보안을 더욱 강화하기 위해 ' 인증자 ' 라는 개념이 조직의 ID 및 액세스 권한 관리 방식의 일부로 통합되기 시작했습니다 . 인증자는 암호라는 단일 컨텍스트와는 달리 여러 구성 요소를 사용하여 ID 를 명확히 검증해야 합니다 . 강력한 MFA 방식 , 인증서 , 디바이스 상태 컨텍스트 , ID 리스크 계산 또는 암호 없는 인증 방법과 결합된 사용자 이름 / 암호의 다중 컨텍스트 등을 인증자의 예로 들 수 있습니다 .

' 인증자 ' 라는 개념에 따르면 이제 암호가 가진 하나의 특성이 인증의 유일한 방어선이 아니기 때문에 전반적으로 암호가 침해될 위험이 크게 줄어듭니다 .

암호 없는 인증이란 ?

많은 조직에서 강력한 MFA 방식을 구축하는 암호 없는 인증을 ' 인증자 ' 과정의 일부로 사용하기 시작했습니다 . 암호 없는 인증 방식은 본질적으로 지식 기반의 비밀을 요구하지 않고 ID 를 확인하는 방법입니다 . 대신 사용자가 소유한 것 (디바이스) 이나 신체 일부 (생체인식) 을 사용하여 ID 를 검증합니다 . 암호 없는 방식이라는 것을 전제로 , 사용자의 소유물이나 신체 기반의 요소를 요구하면 인증 과정에서 ' 사용자가 아는 것 '(암호) 이라는 요소가 필요 없기 때문에 보안이 강화됩니다 .

암호 없는 인증을 활용하는 실용적이고 확장 가능한 방법 :

- **모바일 인증자 애플리케이션** – 동기화 방식 알고리즘을 기반으로 하는 일회성 패스코드 (OTP) 를 생성하거나 사용자에게 표시되는 숫자 시퀀스를 승인 또는 매칭하는 데 사용할 수 있습니다 .
- **FIDO2 하드웨어 토큰 및 키** – 물리적인 연결 , 블루투스 또는 근거리 무선 통신 (NFC) 을 사용하여 디바이스와 인터페이스할 수 있습니다 . 특히 FIDO2 WebAuthn 방법을 이용하면 고유 암호화 키페어 (로밍 인증자 디바이스에 저장됨) 를 사용하여 디바이스 바인딩 하드웨어 토큰을 대상 애플리케이션에 인증하고 공개 키 암호화를 사용하여 교환할 수 있습니다 . FIDO2 Webauthn 은 피싱 , 스푸핑 및 중간 공격자 (AitM, Adversary-in-the-Middle) 공격에 대응하기 위해 암호 없는 인증을 활용하는 효과적인 방법입니다 .
- **패스키** – 암호화 키페어가 모바일 디바이스에 로컬로 생성 및 저장되는 FIDO2 토큰처럼 사용하며 , 인증 대상 (공개 키 보유) 애플리케이션과 공개 키 암호화를 사용하여 교환됩니다 . 설정된 패스키에 액세스하려면 생체인식 식별 또는 모바일 디바이스에서 일반적으로 사용하는 PIN/ 스와이프 패턴이 모바일 디바이스에 필요합니다 .
- **디지털 인증서** – 인증 요청에 응답하기 위해 공개 및 개인 키페어를 사용하여 유효한 디지털 'ID' 서명을 생성하는 데 사용할 수 있습니다 . 최신 디바이스의 보안 플랫폼 모듈 (TPM, Trusted Platform Module) 은 해당 공개 키를 사용하여 개인 암호화 키를 저장하는 내부 인증자로 사용할 수 있으며 , 이는 해당 공개 키를 사용하여 ' 암호 없는 ' 인증을 위해 유효성을 검증할 인증서에 서명하는 데 사용됩니다 .
- **생체인식** – 인간의 고유한 신체적 특징을 사용하여 ID 를 검증할 수 있습니다 . 가장 일반적인 생체인식 인증으로는 지문 (예 : Touch ID 및 Fingerprint Unlock) 및 안면 인식 방법 (예 : Face ID 및 Face Unlock) 이 있으며 이러한 기능은 대부분의 스마트폰 , 모바일 디바이스 , 최신 노트북에 기본적으로 탑재되어 있습니다 .

인증자로 사용하는 암호 없는 인증

강화된 인증 방법을 지원하는 기능이 없는 레거시 애플리케이션과 인프라는 인증자 개념을 적용하려는 조직의 속도를 늦출 수 있습니다 . 이제 조직에서는 각 개별 애플리케이션에 대한 인증 방식을 통합하는 데 집중하기 보다는 서드파티 싱글 사인온 (SSO, Single Sign-On) 솔루션을 주된 인증 방법으로 활용하여 백엔드 애플리케이션에 대한 인증된 액세스를 중개하는 것이 일반적입니다 .

인증자 방식의 일부로 암호 없는 인증을 계획하는 데는 시간이 소요될 수 있습니다 . 다음은 고려해야 할 사항에 대한 개괄적인 개요입니다 .

다음 사항 식별 :

- 신뢰할 수 있는 ID 저장소 및 플랫폼 (IdP) 으로서의 기능을 가진 현재 기술 및 플랫폼
- 기본적으로 암호 없는 인증 방법을 지원하거나 서드파티 통합 및 브로커가 필요한 기존 ID 저장소
- 암호 없는 환경을 테스트하고 확인할 수 있는 ID 유형 등 조직 내에 존재하는 ID
- 암호 없는 인증 또는 강력한 인증 방법을 지원하지 않는 ID 유형 (예 : 프로그래밍 / 서비스 계정) 을 보완하는 컨트롤 및 향상된 탐지 기능
- 암호 없는 인증 통합을 지원하지 않는 게스트 / 서드파티 사용자에게 미치는 영향
- 사용자가 현재 인증과 액세스에 사용하는 디바이스 및 이러한 디바이스가 암호 없는 인증 방법을 지원하는지 확인
- 암호 없는 인증을 위해 직접 통합할 수 있는 애플리케이션 또는 암호 없는 인증을 지원하는 서드파티 플랫폼과의 SSO 통합을 지원하는 애플리케이션

다음 사항에 대한 계획 수립 :

- 암호 없는 인증을 지원하는 디바이스 조달 , 안전하게 제공 및 온보딩
- 사용자에게 암호 없는 인증 환경을 교육하는 교육 커리큘럼
- 암호 없는 인증 통합에 온보딩하도록 ID 저장소 및 디바이스 구성 수정
- 파일럿 사용자 및 범위가 지정된 애플리케이션과의 암호 없는 인증 통합 테스트 및 검증
- 초기 배포 및 온보딩은 물론 전사적으로 암호 없는 인증의 적용 범위 확장

암호 없는 인증에서 추가적으로 고려할 중요한 사항은 디바이스 또는 키를 분실하거나 도난당했을 때 복구 단계를 ID 인증 프로세스의 핵심 구성 요소로 포함시키는 것입니다 . 안전한 복구 단계를 계획하려면 조직의 리스크뿐만 아니라 전체 사용자 등록 및 셀프 서비스 환경에 대한 장단점을 고려해야 합니다 .

내부 인증자 (예 : 통합형 TPM 사용 디바이스) 는 디바이스 간에 개인 키를 내보내거나 동기화하는 기능을 갖추고 있지만 , 키가 적절히 보호되고 저장되지 않으면 리스크가 발생할 수 있습니다 . 서드파티 ID 공급자를 사용하는 경우 , 복구 키와 문구는 암호 없는 ID 를 새 디바이스에서 재구성하는 방법으로 고려할 수도 있습니다 . 암호 없는 인증에 로밍 인증자를 사용하는 경우 , ID 복구 옵션에는 모바일 디바이스 또는 이메일 주소로 전송된 메시지를 검증하는 방법이 포함됩니다 .

단일 암호 사용 방식에서 암호 없는 인증을 인증자로 사용하는 방식으로 마이그레이션하는 작업은 하나의 여정이라고 할 수 있습니다 . 인증자 개념을 사용하는 많은 조직에서는 강력한 다중 인증 (MFA) 이 암호 없는 인증 로드맵을 지원하는 기본 구성 요소임을 알게 되었습니다 . 이 여정에는 적절한 계획 , 실행 및 검증이 필요하지만 , 특히 오늘날의 하이브리드 운영 모델에서는 ID 가 새로운 보안 경계이기 때문에 암호 없는 인증은 상당한 보안 이점과 리스크 감소를 제공합니다 .

사이버 보험 가입에 대한 위험 최소화

미국 은행들은 2021 년 규제 당국에 보고된 1,489 건의 신고에서 12 억 달러 상당의 랜섬웨어 트랜잭션이 발생했음을 확인했으며 , 이는 전년도에 보고된 487 건의 신고에서 발생한 4 억 1,600 만 달러에서 급격히 증가한 수치입니다 .[4]

2020 년에서 2021 년 사이에 랜섬웨어 지급액이 2 배 이상 증가 [1] 하여 보험사들의 손실은 더욱 커졌으며 사이버 보안 보험 시장의 불안한 상황은 최근에야 안정을 찾기 시작했습니다 . 또한 2022 년 말 사이버 보험료 인상률이 80% 감소하며 2023 년 시장 전망이 개선 [2] 되었지만 , 대부분의 보험사들은 랜섬웨어를 여전히 가장 큰 위협으로 꼽으며 사이버 위험이 계속 증가할 것으로 생각합니다 .[3]. 따라서 조직은 보험 계약 심사를 받을 때 사이버 리스크와 관련된 보안 컨트롤 , 내부 프로세스 및 절차에 대한 검증이 더욱 엄격하게 진행될 것으로 예상합니다 . 또한 널리 알려진 취약점 (Log4j) 과 우크라이나 전쟁 또는 국가에서 후원하는 공격 그룹으로 추적되는 침해 사고 제외라는 골치 아픈 문제가 남아 있습니다 . 실제로 , 보험사들은 조직에서 랜섬웨어 관련 리스크를 완화하는 적절한 보안 컨트롤 역량을 입증하지 못할 경우 랜섬웨어 관련 보장 범위를 계속 축소하거나 심지어 제외하고 있습니다 .

Mandiant 는 지난 12 개월 동안 침해 사고 대응 업무 중 사이버 보험사의 개입이 증가한 것을 확인했습니다 . 보험 보장 범위 결정에서 정보보호 최고책임자 (CISO) 와 지속적으로 컨설팅을 하지는 않지만 , CISO 가 조직의 리스크 관리자 및 법률 자문위원과 협력하여 신청 프로세스의 정확성을 보장하고 보험 정책을 검토하여 침해 발생 시 불이익을 당하지 않도록 하는 것이 좋습니다 .

사이버 보험 101

2000 년대 중반 , 보험사들은 보장 범위를 확대하여 사업에 직접적인 피해를 준 사이버 공격에 대한 비용을 보상했습니다 [5]. 그 이후로 보장 범위가 확대되어 금융 리스크 관리자 및 사이버 보안 책임자들이 데이터 침해 또는 기타 보안 사고로 인한 리스크를 완화하고 비용을 상쇄하는 유용한 툴이 되었습니다 . 보험 상품은 일반적으로 회사에 대한 사이버 리스크 (피보험자 리스크) 와 소비자 또는 기업의 책임 (제 3 자 배상책임) 을 보장합니다 . 사이버 보험의 계약 심사는 초기에는 데이터 침해와 관련된 비용에 중점을 두었으며 , 조직은 처리한 레코드 유형 , 클라이언 데이터 및 규제 데이터에 대한 정보를 보험사에 제공하고 HIPAA 및 PCI DSS 와 같은 규제 표준을 준수하고 있음을 인증해야 했습니다 . 랜섬웨어 및 다각적 갈취는 비즈니스를 무력화시키고 상당한 비용을 발생시킬 수 있는 비즈니스 중단의 리스크를 내포하고 있습니다 .

1. Wall Street Journal, Reported Ransomware Incidents, Cost Soared in 2021, Treasury Says, 2022 년 11 월 4 일
2. Marsh, US Cyber Insurance Market Update Signs of improvement in third quarter of 2022, 2022 년 10 월 7 일
3. Woodruf Sawyer, 2023 Property & Casualty Looking Ahead Guide, 2023 년 1 월 10 일
4. Wall Street Journal, Reported Ransomware Incidents, Cost Soared in 2021, Treasury Says, 2022 년 11 월 4 일
5. The Federal Reserve Bank of Chicago, Chicago Fed Letter, No. 426, 2019 The Growth and Challenges of Cyber Insurance, 2019

표 1: 일반적인 사이버 보안 리스크 보장 범위

피보험자 보장 (First-Party Coverage)	제 3 자 배상책임 (Third-Party Liability)
침해 사고 대응 및 포렌식 비용	보안 및 개인정보보호 배상책임
통지 , 신용 및 ID 모니터링	멀티미디어 / 미디어 커뮤니케이션 배상책임
데이터 복구	규제 방어 및 페널티
비즈니스 중단	PCI DSS 배상책임
사이버 갈취 및 사이버 범죄	전화 소비자 보호법 방어
평판 악화	

* 출처 : Honigman LLP Attorneys and Counselors, Cyber Insurance 1012021 년 5 월 19 일

그 결과 , 보험사들은 비즈니스 중단 및 기타 비즈니스 관련 손실에 대비하여 조직의 기술적 컨트롤 및 완화 활동을 보다 심도 있게 검토해 왔습니다 . 그로 인해 리스크 및 보험 상품 가격을 결정하기 위한 계약 심사 프로세스가 더욱 엄격해졌습니다 . 현재 계약 심사 과정에는 추가 질문 , 인터뷰 및 고객의 환경에 대한 외부 심사 제출이 포함됩니다 .

침해 사고 대응 자문위원으로서의 업무 외에도 고객을 위해 사이버 보험을 검토하고 협상하는 데 상당한 시간을 할애하고 있는 Woods Rogers 의 사이버 보안 및 개인정보 보호 업무 책임자인 Beth Burgin Waller 는 고객에게 리스크 관리 팀과 협력하여 보험 계약 심사 프로세스를 준비할 것을 권고합니다 .

계약 심사 질문서에는 현재의 복잡한 멀티 클라우드 , 멀티 네트워크 기업 인프라에 적용되지 않는 예 , 아니요의 이분형 질문이 포함되어 있는 경우가 많습니다 . 예를 들어 , 기업 전반에서 다중 인증 (MFA) 을 사용하고 있는지 대한 질문에 답변하는 경우 , 보험 심사원은 백업부터 클라우드 비즈니스 애플리케이션과 VPN 에 이르기까지 기업의 모든 부분에 MFA 가 존재한다는 증거를 요청할 수 있습니다 . 고객의 자문위원과 리스크 관리팀은 신청서에 작성된 포괄적인 진술을 지원하고 보완 응답을 통해 현재의 실제 환경 컨트롤 및 개선 계획을 명확히 설명하도록 지원할 수 있습니다 .

IR 보장의 미묘한 차이 이해

Burgin Waller 는 표본 (샘플) 보험 증서를 검토할 것을 강력히 권고합니다 . " 시장이 안정됨에 따라 사이버 보험 증서의 언어가 다른 보험 증서와 유사하게 표준화되고 있습니다 " 라고 Burgin Waller 는 말합니다 . 샘플 보험 증서에는 비즈니스 중단의 보장 범위에 일정 부분 제한이 있다고 명시될 수 있습니다 . 따라서 표본 보험 증서를 주의 깊게 검토하지 않으면 , 레거시 소프트웨어 , Log4j 와 같은 광범위한 이벤트 , 국가 차원의 공격자로 인한 침해 사고를 비롯한 전쟁 행위까지 보험 증서에 예외 사항으로 규정된 것을 모르고 지나칠 수 있습니다 . Burgin Waller 는 특히 2 차보상한도를 주의해서 검토해야 한다고 권고합니다 . 한 예로 , 기본 수준의 사이버 보험 증서에는 피싱을 통해 시작된 침해 사고에 대한 2 차보상한도가 포함되어 있으며 조직이 랜섬웨어에 대한 추가 보장에 가입할 것으로 예상했습니다 . " 표본 보험 증서를 주의 깊게 읽는 것 만으로도 침해 사고 발생 전에 조직이 보장받을 수 있는 범위를 명확히 알 수 있어 침해 사고 중에 골치 아픈 일을 상당 부분 줄일 수 있습니다 " 라고 Burgin Waller 는 말합니다 .

침해 사고 대응 (IR) 제공업체 및 관련 비용이 지원될 것으로 예상하십니까 ? Mandiant 침해 사고 대응 담당자가 경험하는 세 가지 일반적인 시나리오는 다음과 같습니다 .

1) IR 제공업체가 승인된 벤더이며 , 요율이 사전에 협상되어 있습니다 . 따라서 효율적으로 대응을 시작할 수 있으며 고객은 클레임을 더 쉽게 제출할 수 있습니다 .

2) IR 제공업체가 사전 승인되지 않았으며 , 보험사에서 시간당 x 달러를 보상합니다 . 고객은 IR 비용이 보장 금액을 넘는 경우에 차액을 감수해야 합니다 .

3) IR 제공업체는 사전 승인되지 않았으며 , 해당 IR 제공업체를 사용할 경우 보험사에서 어떤 보장도 제공하지 않습니다 . 이 시나리오에 해당될 경우 침해 발생 시 가장 큰 혼란을 초래할 수 있습니다 .

표본 보험 증서에서 전체 침해 사고 대응 프로세스의 보장 범위를 검토하는 것이 중요합니다 . 일부 보험 정책은 보험이 조사에만 적용되며 랜섬웨어 지급 , 일반 자문 비용 또는 복구 및 장기적인 문제 해결 작업과 관련된 비용은 제외됩니다 . 또한 보험 회사에서는 공격자의 침입 경로를 정확히 파악하고 재감염에 취약하게 만드는 백도어를 남기지 않았는지 여부 확인을 위한 전체 조사 비용을 보장하지 않을 수도 있습니다 . 이때 기업은 향후 리스크를 줄이기 위한 심층 조사를 진행할 것인지 결정해야 합니다 .

새로운 접근 방식

전체적으로 사이버 보험 시장은 매우 성숙되어 가고 있으며 공급업체는 고객과 협력하여 전반적인 사이버 복원력을 강화하고 있습니다 . 보험 업계는 조직을 보다 안전하게 만들기 위해 적용되는 매우 발전된 리스크 모델링 프로그램을 갖추고 있습니다 .

많은 보험 파트너사에서 고객이 사이버 보안 시장을 탐색하고 , 효율성이 입증된 기술을 통해 리스크를 낮출 수 있도록 다양한 공급업체와 솔루션을 제공합니다 .

보험 파트너사들은 조직의 사이버 리스크 및 관련 보험 비용에 긍정적인 영향을 미칠 수 있는 보안 컨트롤 기능도 검증하고 있습니다 [6]. Mandiant 는 보험 업계의 권고 사항을 받아들이며 , 적절히 시행할 경우 일반적인 공격의 영향을 완화하거나 공격 자체를 예방할 수 있는 다음의 5 가지 과정에 주목합니다 .

1. **다중 인증 (MFA, Multi-factor authentication):** MFA 나 이중 인증 (2FA, Two-Factor Authentication) 은 두 개 이상의 개별적인 크리덴셜 (예 : 암호 , 보안 토큰 , 안면 또는 지문 인식) 을 결합하여 사용자에게 액세스 권한을 제공하는 기술입니다 . Mandiant 는 수많은 침해 사고 대응 조사를 통해 조직에서는 전통적인 다중 인증 (MFA) 방법을 도입하는 비율이 증가했지만 , 공격자들은 ID 를 침해할 수 있는 공격 기술을 계속 발전시키고 있다는 것을 확인했습니다 . 외부에서 액세스할 수 있는 모든 로그인 포털과 및 중요한 내부 애플리케이션 전반에 걸쳐 숫자 매칭 , 상황별 텔레메트리 알림 , 시간 기반 일회성 암호 (TOTP) 입력 등 강력한 MFA 툴 및 방법을 구현하면 공격자들이 일반적인 초기 액세스 기법에 노출될 리스크를 줄일 수 있습니다 .
2. **ID 및 권한 있는 액세스 관리 :** 오늘날의 하이브리드 운영 모델에서 ID 는 새로운 보안 경계입니다 . Mandiant 는 많은 침해 사고 대응 과정에서 디렉터리 및 액세스 관리 시스템이 침해된 것을 확인했습니다 . 공격자들은 권한을 에스컬레이션하는 데 이러한 시스템을 이용하는 경우가 많습니다 . 조직은 사용자와 시스템이 적절한 액세스 권한을 보유하고 있으며 승인되지 않은 액세스 권한 에스컬레이션을 방지하도록 디렉터리 및 액세스 관리 시스템이 적절하게 구성되어 있는지 확인해야 합니다 .
3. **백업의 보안 , 암호화 및 테스트 :** Mandiant 는 사이버 공격이 발생할 경우 시스템과 데이터를 쉽게 복원할 수 있도록 백업을 보호하고 암호화하기 위한 계획을 수립하고 테스트를 완료할 것을 권고합니다 . 백업 및 외부 스토리지 솔루션을 사용하면 IP 손실 가능성을 줄이고 중요한 레코드가 손실되는 것을 방지하는 데 도움이 됩니다 . 비즈니스 중단으로 이어질 수 있는 사이버 공격이 발생할 경우를 대비하여 회사의 클라우드나 하이브리드 네트워크의 사본을 유지 관리하는 방법으로 클라우드 서비스 솔루션을 사용하는 기업이 증가하고 있습니다 .

6. Marsh, Cyber Insurance Market Overview: 2021 년 4 분기 , 2021 년 12 월 7 일

4. **사이버 침해 사고 대응 계획 및 테스트 :** Mandiant 는 사이버 침해 사고 대응 계획 및 테스트가 기존의 기술적 컨트롤 , 네트워크 아키텍처 및 최초 대응 능력을 검토할 수 있는 중요한 활동이라고 생각합니다 . Mandiant 는 일반적인 대응 시나리오에 대한 계획을 개발하고 , 침해 사고 발생 시 격리 조치를 신속히 시행할 수 있는 사이버 방어 태세 역량을 지속적으로 검증할 것을 권고합니다 .
5. **법률 및 침해 사고 대응 파트너 보유 :** 법적 리스크로부터 회사를 보호하고 침해 사고 대응에 대한 전문성을 갖춘 외부 지원을 받을 수 있도록 준비하는 것은 사이버 침해 사고 대응 계획의 중요한 부분입니다 . 법률 자문위원 (특히 사이버 문제 전문가) 은 공격 발생 시 포렌식 대응 담당자와 원활하게 협력하여 침해 사고에서 발생할 수 있는 법적 책임과 리스크를 평가할 수 있어야 합니다 . 침해 사고 대응에 대한 외부 지원을 받으면 대응 시간이 크게 감소하여 침해 피해를 줄일 수 있습니다 . 침해 사고 대응 자문 서비스 (IRR) 를 통해 기업은 사이버 보안 침해 사고 정황이 의심되기 전에 침해 사고 대응 서비스에 대한 약관에 동의할 수 있습니다 .

또한 보험 파트너는 신청 프로세스를 확인하는 데 도움이 되는 보안 컨설팅 및 서비스도 제공합니다 . 많은 브로커와 보험사들이 효과적인 방어 역량을 개발하는 데 필요한 평가 , 사이버 위생 및 프로세스로 컨설팅을 확장함으로써 서비스를 차별화하고 있습니다 .

사이버 보험을 살펴보는 데 더 많은 도움이 필요한 경우 , Mandiant 파트너 , 팟캐스트 , 웨비나 및 Google Cyber Risk 서비스를 이용하시기 바랍니다 .

보안 분석 사례 연구 : 소프트웨어 공급망 침해 확인 및 차단

탐지 및 대응 기능을 활성화하면 갖게 되는 이점

지난해 , Mandiant 는 공급망 침해가 크게 증가 (공급망에서 시작된 침입이 2020 년 1% 미만에서 2021 년 17% 로 급증) 했다고 발표했습니다 [7]. 이러한 증가는 Mandiant 가 추적한 침입의 86% 가 SolarWinds 침해 및 SUNBURST 와 관련되어 있다는 사실에서 일부 설명됩니다 [8]. 하지만 이는 조직들이 평균 244 개의 공급업체와 기술 관계를 유지하고 있다는 사실과도 관련이 있습니다 [9].

소프트웨어 공급망 공격은 새로운 문제가 아닙니다 . 2017 년 , NotPetya 라는 공격에 의해 전 세계가 타격을 받았습니다 . 랜섬웨어로 위장한 이 악성 코드는 NSA 에서 유출된 EternalBlue 의 취약점을 악용하여 네트워크에 침투한 뒤 체계적으로 데이터를 파괴했습니다 . NotPetya 배후의 공격자들은 우크라이나 정부에 금융 서비스 소프트웨어 공급하는 업체를 침해했습니다 .

같은 해 , 유틸리티 CCleaner[10] 는 침해 피해를 입었고 해커들은 정상 버전의 소프트웨어를 악성 소프트웨어로 대체하였으며 이로 인해 2 백만 개 이상의 호스트가 손상되었습니다 .

2020 년에는 앞서 언급한 SolarWinds 제품을 악용한 광범위한 공격은 러시아와 전략적인 이해 관계가 일치한다고 평가되는 공격자인 APT29(이전의 UNC2452) 에 의해 자행되었습니다 [11]. 정부 조직과 포춘 500 대 기업을 비롯한 다양한 피해자들이 APT29 의 영향을 받았습니다 . 다시 한번 , 공격자들은 소프트웨어 구성 요소인 Orion 에 백도어 코드를 삽입하여 소프트웨어 공급망을 표적으로 삼았기 때문에 피해자들의 내부 환경에 대한 액세스 권한을 받은 공격자들은 정상적인 프로세스를 통해 업데이트된 코드를 배포한 후 SUNBURST 멀웨어를 배포할 수 있었습니다 .

공격자들은 디지털 엔터프라이즈의 구성 요소를 침해할 수 있는 방법을 찾아냈습니다 . 소프트웨어 개발자들이 사용하는 인기 패키지를 표적으로 삼고 침해에 성공하면 악성 코드를 대규모로 쉽게 피해자에게 직접 배포할 수 있습니다 . 이러한 접근 방식은 기업의 방어 태세가 충분한가에 대한 의문을 갖게 합니다 . 전 세계의 조직들은 자사의 공격 표면에 대한 가시성을 유지하고 탐지 및 대응 기능에 대한 확신을 얻기 위해 노력하고 있습니다 . 그러나 소프트웨어 공급망 내에서 사이버 공격을 신속하게 확인하고 차단하는 능력을 확신하지 못하는 경우가 너무 많습니다 . 적절하게 교육을 받은 담당자가 부족하고 교육과 지식을 세부적으로 조정할 수 있을 만큼 자주 활성화하거나 대응할 기회가 없기 때문입니다 .

7. Mandiant, M Trends 2022
8. Mandiant, M Trends 2022
9. Mandiant, The Defender's Advantage Cyber Snapshot 제 2 호 , 2022 년
10. Mandiant Threat Intelligence, "CCleaner Supply-Chain Compromise Possibly Linked to Chinese Cyber Espionage Operators, 2017 년 9 월
11. Mandiant,"Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor", 2020 년 12 월

소프트웨어 공급망 침해는 서드파티 제공업체에 대한 신뢰를 악용하여 피해자의 환경에 간접적으로 액세스할 수 있도록 설계되어 탐지가 어려울 수 있습니다 . 결국 훈련 받은 보안 분석가의 안목과 조사 프로세스가 지능형 공격을 파악하고 막을 수 있는 결정적인 요소입니다 .

공급망 공격의 경우 , 사전에 신뢰가 구축되어 있기 때문에 악성 코드 이식을 직접 탐지하기가 매우 어렵습니다 . 동일한 공격 라이프사이클의 후반에 탐지된 의심스러운 이벤트에 대한 조사를 통해 분석가는 공격자의 행동을 역으로 추측하여 이식 항목을 간접적으로 발견할 수 있기 때문에 활성화된 효과적인 탐지 및 대응 능력은 더욱 중요해집니다 .

—Steve Ledzian, Mandiant, VP, CTO-APAC,

소프트웨어 공급망 침해에 대한 분석가 탐지 및 조사

2021 년 10 월 중순부터 Mandiant 관리형 탐지 및 대응 서비스의 보안 분석가들은 오픈 소스 리포지토리 중독으로 보이는 여러 이벤트를 확인했습니다 . 다음 사례에서는 Node.js JavaScript 플랫폼의 패키지 관리자인 NPM(Node Package Manager) 에 호스팅된 패키지와 관련된 탐지 및 조사 프로세스와 보안 분석가들이 답변하고자 하는 질문에 대해 설명합니다 .

처음에는 Mandiant 보안 분석가로 구성된 소규모팀에서 기본 Windows 유틸리티 **CERTUTIL.EXE** 가 공통 URL **(hxxps://citationsherbe[.]at/sdd.dll) 에서 페이로드를 다운로드하는 데 사용되고 있음을 보여주는 다수의 경고를 확인했습니다** . 보안 운영 센터 (SOC) 의 더 많은 분석가들이 비슷한 경고를 받기 시작하면서 , 당사 보안 분석가팀은 조사의 질문에 대한 답을 찾기 위해 협력하기 시작했습니다 .

이 페이로드는 무엇이며 , 어떻게 시스템에 다운로드되었는가 ?

가장 먼저 대답해야 할 조사 질문은 ' 어떤 멀웨어가 존재하며 그 기능은 무엇인가 ?' 그리고 ' 어떻게 시스템에 들어왔는가 ?' 입니다 . 분석가들은 초기 호스트에서 페이로드를 받아 의심스러운 바이너리의 기능과 역량을 확인했습니다 . 분류 분석에 따르면 해당 바이너리는 공격자 제어형 커맨드 및 컨트롤 (C2) 서버와의 통신을 통해 크리덴셜 도용을 표적으로 하는 DANABOT 멀웨어의 변형이었습니다 . 분석가들은 멀웨어의 C2 주소를 사용하여 공격자의 인프라와 통신하는 다른 시스템을 파악하고 조사 범위를 더욱 확장하기 시작했습니다 . 이러한 프로세스를 통해 동일하거나 유사한 멀웨어가 해당 경고 없이 다른 시스템에 배포되었는지 판단할 수 있습니다 . 페이로드가 멀웨어로 확인된 후 분석가 팀은 침해된 호스트를 원격으로 격리하거나 침해 사고 대응팀을 가동하여 조치를 취했습니다 .

DANABOT 은 Delphi 로 작성된 백도어로 , TCP 를 통해 사용자 지정 바이너리 프로토콜을 사용하여 통신합니다 . 이 백도어는 다운로드한 플러그인을 통해 기능을 추가할 수 있는 플러그인 프레임워크를 실행합니다 . DANABOT 에는 VNC 또는 RDP 플러그인을 사용한 전체 시스템 컨트롤 , 비디오 및 스크린샷 캡처 , 키로깅 , 임의 셸 명령 실행 , 파일 전송 등의 기능이 있습니다 . DANABOT 의 프록시 플러그인을 사용하면 표적이 된 웹 사이트와 연결된 네트워크 트래픽을 리디렉션하거나 조작할 수 있습니다 . 이 기능은 크리덴셜 또는 결제 데이터를 캡처하는 데 사용되는 경우가 많습니다 . 또한 DANABOT 을 통해 웹 브라우저 및 FTP 클라이언트와 연결된 저장된 크리덴셜을 추출할 수도 있습니다 .

'ua-parser-js' 는 웹 애플리케이션 또는 서버 측 애플리케이션 내에 배포되는 경량의 소형 패키지로 , 사용자 에이전트 문자열 (즉 , 브라우저 , 엔진 , OS, CPU, 디바이스) 을 구문 분석하는 데 필요한 관련 데이터를 추출하고 필터링합니다 .

어떻게 침입했는가 ?

일반적으로 분석가들은 멀웨어가 배포된 방법을 파악하기 위해 엔드포인트 탐지 및 대응 (EDR, Endpoint Detection and Response) 기술을 통해 수집한 데이터를 활용합니다 . 분석가들은 EDR 텔레메트리를 검토하여 NPM 패키지를 업데이트하기 위해 사용자가 실행한 정상적인 명령에 대한 활동을 추적했습니다 .

철저한 조사를 통해 영향을 받은 각 호스트의 **UA-PARSER-JS PACKAGE** 디렉터리에 유사한 파일이 삽입되어 있는 것이 밝혀졌으며 , 분석가들은 이 파일이 침해되어 멀웨어를 배포하고 있다고 판단했습니다 . JS Package 디렉터리에 대한 악의적 변경으로 인해 패키지 설치 프로세스에 사전 설치 단계가 추가되어 멀웨어가 다운로드되었습니다 . 분석가들은 침해된 스크립트를 검토하면서 CoinMiner(암호화폐 채굴기라고도 함) 를 다운로드하여 호스트에 배포했다는 사실도 확인했습니다 . 분석가들은 GitHub Issues 에서 해당 패키지 리포지토리를 살펴보았고 누군가가 패키지가 아주 최근에 침해되었는지 여부를 물었던 것을 발견했습니다 . 2021 년 10 월 22 일 12 시 15 분 (UTC) 에 GitHub Issues 에 게시된 내용에 따르면 , 매주 700 만 건 이상 다운로드되고 있는 인기 있는 Node.js 라이브러리인 NPM 패키지 '**ua-parser-js**' 가 침해되어 악성코드를 전달했습니다 . 공격자는 작성자의 NPM 계정을 하이재킹하여 세 가지 악성 버전의 패키지를 게시했습니다 . 리포지토리의 Git 로그에 따르면 10 월 22 일 , 오후 4 시 14 분 ~4 시 25 분 (UTC) 사이에 패키지 작성자가 악성 패키지의 삭제 버전을 커밋하여 추가적인 침해를 막았습니다 .

이 공격자는 어떤 다른 활동을 수행했는가 ?

호스트를 격리한 후 , 분석가들은 공격의 근본 원인을 판단하기 위한 조사를 계속했습니다 . 해당 패키지 리포지토리의 Git 로그를 검토한 결과 , 악성 변경 사항이 푸시된 시점과 몇 시간 후 수정이 적용된 시점의 타임스탬프를 발견했습니다 . 공격자 TTP 에 대한 추가 분석을 통해 동일한 공격자가 침해한 다른 NPM 패키지를 발견하고 공격자가 수행한 활동 범위를 파악할 수 있었습니다 . 분석 팀에서는 해당 활동이 UNC3379 에 의해 수행되었음을 확신할 수 있었으며 멀웨어를 분석하고 , 공격자 행동을 문서화하여 향후 활동을 저지하기 위한 탐지 기술을 개발할 수 있었습니다 .

이 소프트웨어 공급망 침해에 대한 자세한 내용은 , 연구 블로그인 No Unaccompanied Miners: Supply Chain Compromises Through Node.js Packages 를 참고하십시오 .

신뢰할 수 있는 분석가의 직감 , 비판적인 사고 및 경험

조사의 규모가 어느 정도든 시간이 관건입니다 . Mandiant 는 조사와 대응에서 우리 분석가들의 지식 , 훈련 , 비판적인 사고를 충분히 활용합니다 . 분석가 팀은 형사처럼 단서 , 증거 및 포렌식 아티팩트를 활용하여 각 침해 사고 뒤에 숨겨진 사실을 밝혀냅니다 . 조사 프로세스의 목표는 다음과 같은 사항을 판단하기 위해 공격에 대한 주요 질문의 답을 찾는 것입니다 .

- 침입의 범위
- 아직도 진행 중인지 여부
- 첫 침해 날짜 및 침입 원인
- 노출된 데이터의 유형 및 범위
- 공격자의 신원 및 동기

침입과 관련된 이러한 사실을 파악하면 격리 , 제거 및 복구에 도움이 됩니다 . Mandiant 는 최일선 경험 , 시뮬레이션 및 교육을 통해 , 조사를 주도하고 격리 및 제거 타이밍과 실행에 관한 주요 결정을 내릴 수 있는 권한을 분석가에게 부여할 것을 권고합니다 . " 조직이 자체적으로 침해 사고의 조사와 대응을 수행하고 복구에 너무 성급하게 착수하는 것을 흔히 볼 수 있습니다 . 공격에 관한 더 많은 사항을 파악하면 , 제거와 복구를 훨씬 더 성공적으로 수행할 수 있습니다 " 라고 Mandiant 의 VP 인 Eric Scales 가 말합니다 .

여기에 제시된 사례에서 Mandiant MDR 의 분석가 주도 조사는 공격 활동과 관련된 핵심 지표를 개발하고 , 배포된 멀웨어를 분류하여 적절한 복구 조치를 결정했으며 , 위협 그룹에 대한 Mandiant 의 심도 있는 지식과 연구를 활용하여 범위에 포함된 고객의 환경을 성공적으로 조사하여 EDR 제품에서 발견하지 못한 이 캠페인과 관련된 위협 활동을 탐지했습니다 .

CISA 의 크로스섹터 사이버 보안 성과 목표에 대한 사이버 방어 태세 활성화

국가 차원의 공격자들은 계속해서 중요한 인프라 기술을 표적으로 삼고 있습니다 . 지난 해 , Mandiant 는 공격자가 운영기술 (OT, Operational Technology) 네트워크의 액세스 권한을 획득하면 특정 산업 제어 시스템 (ICS, industrial control systems) 또는 감시 제어 및 데이터 획득 (SCADA, supervisory control and data acquisition) 장치를 스캔하고 침해하여 제어할 수 있는 특정 목표 맞춤형 툴을 발견했다고 보고했습니다 [12]. 네트워크에 연결되는 산업용 인프라와 중요 인프라가 점점 더 많아지면서 이러한 공격이 고도화되고 있어 중요 인프라에 대한 사이버 보안 지침을 업데이트해야 할 필요성이 커지고 있습니다 . 미국 사이버 보안 및 인프라 보안국 (CISA, Cybersecurity and Infrastructure Agency), 미국 국립 표준 기술 연구소 (NIST, National Institutes of Standards and Technology) 및 기관 간 커뮤니티에서 모든 중요 인프라 분야에 걸쳐 일관된 사이버 보안 목표를 수립했습니다 .

2022 년 10 월 , CISA 는 조직이 가장 중요한 사이버 보안 업무를 파악하고 우선순위를 정하는 지침으로 사용할 수 있는 크로스섹터 사이버 보안 성과 목표 (CPG, Cross-Sector Cybersecurity Performance Goals)[13] 를 발표했습니다 . CISA CPG 는 조직이 매일 겪고 있는 사이버 보안 문제를 해결하기 위한 기준이 되어야 합니다 . 병원 , 에너지 공급업체 , 운송 시스템 , 주요 제조업체 등 국가 핵심 인프라의 방어 태세를 강화하기 위해 사이버 리스크를 줄이는 공동의 목표를 달성하는 것이 목적입니다 .

Mandiant 는 리스크를 줄이는 출발점으로 삼기 위해 CISA CPG 지침을 채택했습니다 . CPG 는 ' 국가 안보 각서 (NSM-5, National Security Memorandum): 핵심 인프라 제어 시스템에 대한 사이버 보안 개선 ' 을 위한 목표의 첫 번째 기준 역할을 합니다 . 이러한 목표는 모든 것을 포괄하는 사이버 보안 프로그램이 아닌 보다 강력한 사이버 보안 관행을 만들기 시작하는 중요한 단계입니다 .

12. Mandiant, INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems, 2022 년 4 월 13 일
13. Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022

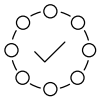
CPG 는 사이버 리스크를 줄이기 위한 상한선이 아니라 기본으로 활용되어야 합니다 . 강조되는 주요 특징은 다음과 같습니다 .

사이버 보안 관행에 매핑된 하위 집합

IT 및 OT 에 대한 특별 지침

우선순위가 지정된 리스크 축소 방식

CISA, 해당 정부 및 업계 파트너가 관찰한 위협에 따라 정보 제공



모든 핵심 인프라 (CI) 섹터에 적용 가능

CPG 는 이러한 조직이 핵심 인프라를 더 잘 보호할 수 있도록 OT 및 ICS 와 관련된 구체적인 조치와 항목을 요구합니다 .

조직의 규모에 관계없이 , 핵심 인프라를 보호하려면 관련 사이버 위협에 대한 이해 , 엄격한 보안 테스트 , 위협 탐지와 대응이 전사적으로 수행되어야 합니다 . CPG 를 통해 조직은 예산 , 인력 및 전문 지식을 고려하면서 가장 파급력이 큰 보안 작업에 투자를 집중하는 방법을 생각해 볼 수 있습니다 . CPG 를 구현하는 데 투자하면 " 미국 국민의 안전 , 건강 , 생계를 해치는 심각한 위협을 유의미하게 해결할 수 있을 것입니다 [14]."

14. Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022.

관련 사이버 위협에 대한 이해

CPG 는 조직이 지속적으로 관련 위협을 인지하고 공격자의 전술 , 기술 및 절차 (TTP) 를 활용하여 진행 중인 공격을 탐지할 수 있도록 지침을 제시합니다 . 관련 사이버 위협에 대한 이해는 Mandiant 가 OT 보안에 접근하는 방식의 핵심이며 , 이를 통해 고객은 상황을 완전히 인식하여 IT 및 OT 네트워크의 위협 탐지 기능을 강화할 수 있습니다 [15]. Mandiant 는 기업과 침해 사고 대응 담당자가 공격 라이프사이클 전반에 걸쳐 침입 방법 또는 TTP 에 훨씬 더 많은 관심을 기울여야 한다고 생각합니다 . 이 중 대부분은 IT 와 OT 의 네트워크 경계를 넘나드는 시스템 또는 IT 에서 사용하는 것과 비슷하거나 동일한 운영 체제 및 프로토콜을 사용하는 OT 네트워크 내의 네트워크 연결 워크스테이션 및 서버 등 이른바 ' 중개 시스템 ' 에 존재합니다 . 대다수의 정교한 OT 공격에서 이러한 중개 시스템을 최종 표적으로 향하는 발판으로 사용하기 때문에 침입 방법에 집중하는 것이 효과적입니다 .

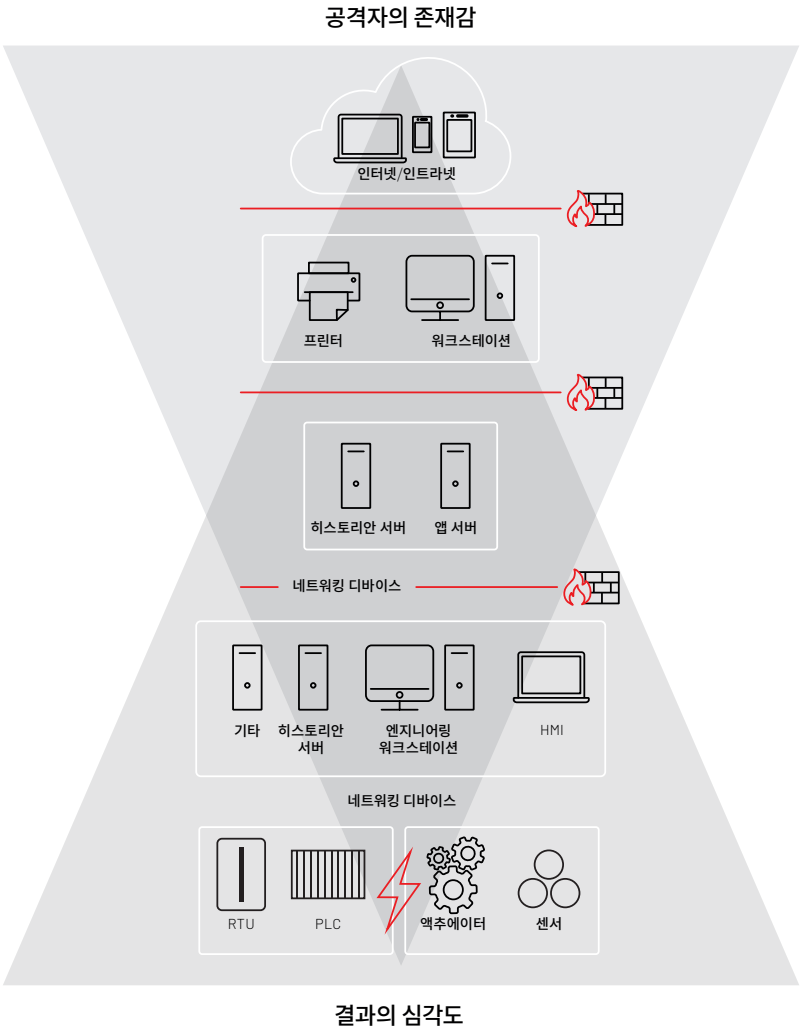


그림 1. OT 위협 탐지 기회

15.Mandiant, The Mandiant Approach to Operational Technology Security, 2019 년 12 월

OT 를 표적으로 하는 공격자를 탐지하는 가장 큰 기회는 그림 1 에서 두 삼각형의 교차점에 있습니다 [16]. 바로 여기에서 공격자의 존재와 침입으로 인한 운영적 결과 사이의 균형을 통해 보안 조직은 위협 활동을 보다 쉽고 의미 있게 파악할 수 있습니다 . 조직은 공격자의 침입 방법을 이해하고 해당 지식을 활용하여 지능형 위협을 헌팅하고 탐지해야 합니다 . 탐지 가능한 침입의 특징은 여전히 존재하며 침입으로 인해 예상되는 피해의 심각도가 높지만 치명적이지는 않기 때문에 OT DMZ 및 분산 제어 시스템 (DCS, Distributed Control System) 에 근접한 위협 헌팅이 가장 효율적일 수 있습니다 .

16. Mandiant, The Mandiant Approach to Operational Technology Security, 2019 년 12 월

2022 년

2022 년 , Mandiant 는 랜섬웨어 갈취 공격으로 중요한 OT 와 네트워크 문서가 노출되었음을 보고했습니다 [17]. 랜섬웨어 관련 유출 또는 다양한 유형의 데이터 유출로 인해 민감한 OT 데이터가 노출되면 정교한 공격자에게 표적에 대한 정보 , 특히 피해자의 인프라 , 자산 , 보안 취약점 및 프로세스에 대한 정보를 제공하게 됩니다 . 공격자는 이러한 종류의 정찰 데이터를 사용하여 보다 심각하고 정밀한 공격을 수행합니다 .

표 2: 랜섬웨어 갈취 공격으로 노출된 문서

피해 기업 (기업명 삭제)	유출 내용
화물 및 여객 열차 제조업체	OEM 용 암호 관리 크리덴셜 , 유럽 트램 차량에 대한 제어 아키텍처 및 통신 채널 요건 , Siemens TIA Portal PLC 프로젝트 파일 백업 등
석유 및 가스 기업 2 곳	다이어그램 , HMI, 스프레드 시트 등 상세한 네트워크 및 프로세스 문서
제어 시스템 통합업체	고객 프로젝트의 엔지니어링 문서 (일부 파일은 암호로 보호되어 있어 우회를 시도하지 않음)
수력발전소	재무 및 회계와 관련된 데이터가 대부분이었지만 IT, 플랜트 유지보수 및 운영 직원의 이름 , 이메일 , 사용자 권한 및 일부 암호 목록 유출 확인
위성 차량 추적 서비스 제공업체	글로벌 위치 추적 시스템 (GPS) 를 통해 차량을 추적하는 데 사용되는 독점 플랫폼의 제품 다이어그램 , 시각화 자료 및 소스 코드
재생 에너지 생산 기업	재생 에너지 인프라에 대한 유지 보수 및 공급 조건을 명시한 피해 기업과 고객 간의 법적 계약서 . 계약서에는 서비스 제공자가 퍼블릭 인터넷 IP 주소를 통해 서드파티의 SCADA 시스템에 대한 완전한 액세스 권한을 가진다고 명시되어 있었음

- 네트워크의 모든 세그먼트에서 데이터를 사용하는 직원 및 협력업체에 대해 강력한 데이터 처리 정책을 시행하여 내부 문서를 보호합니다 .
- 보안이 약한 네트워크에 중요도가 매우 높은 운영 데이터를 저장하지 않습니다 .
- 운영 데이터를 보호하기 위해 포괄적인 보안 프로그램을 구현하는 협력업체 선택 시 각별한 주의를 기울입니다 .
- 랜섬웨어 침입의 피해를 입은 기업은 유출된 모든 데이터의 가치를 평가하여 어떤 대체 컨트롤이 추가 침입의 리스크를 줄이는 데 도움이 될지 판단해야 합니다 .
- 유출된 모든 크리덴셜 및 API 키는 변경합니다 . 핵심 시스템 및 OT 점프 서버의 IP 주소가 노출된 경우 변경하는 것이 좋습니다 .
- 정기적으로 레드팀 모의 연습을 시행하여 외부에 노출되고 안전하지 않은 내부 정보를 파악합니다 .

17. Mandiant, 1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information, 2022 년 1 월

엄격한 보안 테스트

OT 네트워크의 보안 태세를 확실히 향상시킬 수 있는 한 가지 핵심 방법은 중요 자산을 표적으로 하는 가장 일반적인 공격 및 멀웨어 패밀리에 대해 OT 네트워크의 각 계층에서 보안 컨트롤을 안전하게 테스트하는 것입니다 . CISA CPG 는 서드파티를 활용하여 조직의 사이버 방어 태세의 효과와 적용 범위를 정기적으로 검증할 것을 권고합니다 .

Mandiant 는 조직의 평가 요구에 맞게 맞춤형으로 제작된 프로그램을 제시합니다 . OT 에 대한 포괄적인 테스트 프로그램은 공격자의 관점에서 수행하고 , 시뮬레이션과 에뮬레이션을 활용하여 실시간 운영에 미치는 영향을 줄이고 , 레드 팀 , 퍼플 팀 , 침투 테스트 , 네트워크 및 구성 요소 보안 테스트를 적절히 조합하여 수행할 때 가장 효과적입니다 . 실제 OT 환경의 가동 시간 요구 사항으로 인해 사전 예방적 테스트를 시행할 수 없는 경우 , Mandiant 는 네트워크 세분화 , 액세스 컨트롤 , 네트워크 모니터링 시스템 , 임시 디바이스 정책 및 침해 사고 대응 역량의 효과를 기술적으로 평가할 것을 권장합니다 . 지속적인 테스트를 수행하면 특정 시점에서 보안 컨트롤의 효과를 평가할 수 있을 뿐만 아니라 공격자가 네트워크를 악용하기 전에 통합 네트워크 (IT-OT) 에서 복잡한 보안 문제를 식별하는 데 도움이 됩니다 . 또한 지속적인 검증을 통해 조직의 팀이 사이버 침해 사고를 모니터링 , 탐지 및 대응하도록 준비할 수 있습니다 . 조직은 이러한 프로그램을 통해 심각한 문제의 완화를 위한 전술적 권고 , 장기적 개선을 위한 전략적 권고 , OT 침해 사고를 모니터링하고 대응하는 직원의 능력 격차 파악 등을 기대할 수 있습니다 .

오픈 플랫폼 통신 서버를 사용하면 산업 환경 내에서 기계 , 장치 및 시스템 간에 특정 제조업체에 종속되지 않고 데이터 교환이 가능합니다 .

대응 및 복구

섹션 7 에서 CISA CPG 는 조직이 관련 위협 시나리오에 대한 사이버 보안 침해 사고 대응 계획을 유지 , 실행 및 업데이트해야 하는 필요성에 대해 설명합니다 . Mandiant 는 TRITON 및 INCONTROLLER 와 같이 중대한 OT 침해 사고를 최일선에서 대응한 경험을 바탕으로 IT 및 OT 사고 대응 간의 차이와 OT 대응을 수행하는 데 필요한 툴 및 절차에 대해 보다 깊이 이해할 수 있었습니다 .

복구 및 방지 목표 (환경에서 위협을 제거하고 시스템을 정상적인 운영 상태로 복원) 는 IT 및 OT 환경에서 동일하지만 툴은 상당히 다를 수 있습니다 . IT 대응 담당자는 정기적으로 엔드포인트 탐지 및 대응 기술을 사용하여 조사 , 격리 및 복구 / 개선을 지원합니다 . 이러한 툴은 일반적으로 OT 네트워크의 서버나 구성 요소에 설치되지 않습니다 .

IT 에서의 격리는 복잡한 OT 환경에서 수행할 때보다 상대적으로 간단하고 영향을 적게 받는 경우가 많습니다 . 예를 들어 , 특정 기능을 중단하고 시작하거나 심지어 IT 네트워크에서 전체 시스템을 제거하는 작업도 일반적입니다 . OT 구성 요소에 이러한 조치를 사용하는 경우 더 큰 영향을 받을 수 있습니다 . 심각한 가동 중단 또는 생명 안전에 위험을 미칠 가능성이 있는 작업에 영향을 주지 않고 프로세스를 시작 또는 중단하거나 구성 요소를 오프라인으로 전환하려면 기본 프로세스에 대한 포괄적인 이해가 선행되어야 합니다 . 예를 들어 , 오픈 플랫폼 통신 (OPC, Open Platform Communication) 서버가 예기치 못하게 오프라인으로 전환될 경우 몇 주 동안 전체 제조 라인에 영향을 미칠 수 있습니다 . 계획을 세부적으로 수립 (진행 중인 침해 사고 대응 제외) 하면 시스템 담당자는 잠재적 가동 중단 , 생산 피해 또는 생명 안전 위험을 바탕으로 리스크에 기반한 의사 결정을 내릴 수 있습니다 . 잠재적 공격자의 목표와 대상을 파악할 수 있도록 조직의 능력을 개발하면 시스템 담당자가 보다 안전하고 리스크가 낮은 결정을 내리도록 지원할 수 있습니다 .

마지막으로 , OT 네트워크는 벤더가 운영하는 여러 서브 네트워크로 구성되며 조직은 여기에 직접 액세스할 수 없습니다 . Mandiant 는 서드파티 시스템을 포함한 대응 계획과 플레이북을 개발하고 해당 공급업체와 함께 테스트할 것을 권장합니다 . 사이버 보안 침해 사고를 대규모로 신속하고 효과적으로 해결하기 위해 계획을 수립하고 이를 연습하는 것의 중요성은 아무리 강조해도 지나치지 않습니다 .

Mandiant 는 OT 보안 제품을 NIST 사이버 보안 프레임워크의 5 가지 기능 [18] 에 매핑하고 CISA CPG 를 통해 이를 보완하여 서비스를 조직의 사이버 보안 리스크 관리 라이프사이클에 매칭시킵니다 .

18. NIST, Cybersecurity Framework, The Five Functions, 2021 년 5 월

		파악	보호	탐지	대응	복구
인텔리전스	인텔리전스 구독	■	■	■		
	전담 인텔리전스 분석가	■	■	■		
	취약점 평가 서비스	■	■			
	맞춤형 분석 및 블랙박스 평가	■				
컨설팅	상태 점검	■	■	■		
	보안 프로그램 평가	■	■			
	공격 및 침투 테스트	■	■	■		
	침해 사고 대응 계획 수립	■			■	■
	침해 사고 대응				■	■
	보안 교육	■	■			
	전담 컨설턴트	■	■	■	■	■
OT 를 위한 관리형 방어	점프스타트	■	■			
	지속적인 모니터링		■	■	■	
서드파티 기술	OT 네트워크 프로토콜 모니터링	■		■		

그림 2. Mandiant OT 관련 제품 및 서비스

Mandiant 는 ICS 및 OT 환경에서 수십 년 간의 실무를 통해 축적된 산업 제어 시스템에 대한 심도 있는 기능적 지식을 활용하여 최일선의 사이버 보안 인사이트를 제공합니다 . Mandiant 의 OT 전문가는 산업 조직이 OT 네트워크의 전체에 걸쳐 완화 및 탐지 기능을 개선할 수 있도록 고급 보안 테스트를 수행합니다 . OT 환경의 보안 강화와 사이버 보안 태세 개선을 위해 CISA CPG 를 활용할 수 있도록 Mandiant 가 도와드리겠습니다 .

마치는 말

The Defender's Advantage Cyber Snapshot 의 이번 호는 기존의 암호 및 다중 인증 (MFA) 에서 벗어나 암호 없는 인증을 구현하여 강력한 MFA 방식을 구축하고 모든 디바이스 및 애플리케이션에 대한 브로커 백엔드 인증을 지원하기 위한 서드파티 싱글 사인온을 적용하려는 여정을 계획하고 있는 기업에 유용한 지침을 제시합니다 . Mandiant 는 변동성이 심한 사이버 보험 시장을 탐색하는 분들에게는 보험 심사 신청 준비 과정에 자문 및 리스크 관리를 포함하고 표본 보험 증서를 신중하게 검토하며 보험사를 전반적인 리스크 관리 파트너로 생각하라는 팁을 제공합니다 .

또한 The Defender's Advantage 에서 설명하는 사이버 방어의 6 가지 핵심 기능이 미국 사이버 보안 및 인프라 보안국 (CISA) 이 최근 발표한 크로스섹터 사이버 보안 성과 목표 (CPG, Cross-Sector Cyber Security Performance Goals) 에서 제공한 지침과 같은 선상에 있음을 보여줍니다 . 이는 핵심 인프라 소유자와 운영자가 리스크를 유의미하게 줄이기 위해 구현할 수 있는 사이버 보안 방식을 설명하고 있습니다 . 또한 분석가가 관련 경고에 대한 조사에 집중하고 분석가의 교육 , 경험 및 비판적 사고를 활용하여 공급망 공격을 조사하는 최적화된 SOC 에서 배포한 전술의 예를 보여주는 사례 연구를 조명합니다 .

지식은 사이버 공격에 맞서 대응하는 우리의 가장 큰 장점 중 하나입니다 . The Defender's Advantage Cyber Snapshot 은 보안팀에게 정보를 제공하고 리더가 현명한 결정을 내리는 데 도움이 되는 인사이트와 인텔리전스를 제공하기 위해 고안되었습니다 . 사이버 보안 업계는 대응 담당자들이 계속해서 맞서 방어할 수 있도록 정보를 공유하고 협력해야 합니다 . The Defender's Advantage Cyber Snapshot 은 Mandiant 가 이를 지원하는 방법 중 하나일 뿐입니다 .

자세한 정보 : www.mandiant.kr

Mandiant

서울특별시 강남구 테헤란로 518
섬유센터빌딩 13 층 101 호

02-2138-3191
Korea@Mandiant.com

Mandiant 소개

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

MANDIANT
NOW PART OF Google Cloud