NOZOMI NETWORKS

중요 인프라 공격의 동향 및 대책

OT/IoT 환경에서 사이버 방어를 강화하는 방법

핵심 요약

OT/IoT 보안 보고서

2021년 하반기 검토

랜섬웨어 공격에 의한 운영 중단

Nozomi Networks 연구소에서는 2021년 하반기에 대한 이 반기 보고서를 통해 업계 동향과 자체 연구를 지속적으로 종합하고 있습니다. 사이버 범죄는 올해 하반기인 6개월 동안 계속 증가했습니다. 랜섬웨어와 공급망 공격으로 피해와 운영 중단이 뉴스 헤드라인을 장식했습니다. 법 집행 기관, 정부 기관 및 업계의 새로운 관심에도 불구하고 조직에 대한 공격 기술 및 위험의 정교함은 계속해서 악화되어 가는 추세입니다.

OT/IoT 환경의 보안 팀과 연구원을 지원하기 위해, 이 보고서에서는 공격 동향, 취약성 연구, 개선 노력 및 기술의 모범 사례라는 세 가지 주요 영역을 주로 다룹니다. 일부 영역에 랜섬웨어 공격에 대한 심층 분석과 보안 카메라 및 소프트웨어 공급망의 취약성에 대한 Nozomi Networks 자체 연구가 포함됩니다. 또한 공격 표면 감소, 최신 OT/IoT 네트워크에서 제로 트러스트의 역할, 취약성에 대해 장치 펌웨어를 분석하는 기술도 다룹니다.

지속적으로 운영 중단을 일으키는 랜섬웨어 공격

2021년 상반기와 마찬가지로 하반기도 랜섬웨어 뉴스와 운영 중단 소식으로 가득 차 있었습니다. Conti 랜섬웨어 그룹이 이번 한 해 동안 1억 5천만 달러 이상을 갈취한 것으로 보고되었습니다. 많은 사람들이 REvil의 후계자로 생각하는 IT 솔루션 제공업체 Kaseya와 BlackMatter의 소프트웨어 공급망을 목표로 하는 REvil을 통해 미국 농민 협동조합에 590만 달러의 몸값을 요구하는 등 다양한 랜섬웨어 그룹이 활동했습니다.

주요 인프라 부문, 특히 교통, 의료 및 식품 부분은 주요 타겟이 되고 있습니다. 이 모든 부문이 이제 랜섬웨어 그룹과 지정학적 동기를 가진 국가 행위자에 의해 고가치 표적으로 간주되는 상황입니다. 법 집행 기관(LEO)은 또한 랜섬웨어 조직 및 협력자들에 대해 중대한 조치들을 취했는데, 여러 국가의 협력이 필요한 장기적인 작업인 경우가 많았습니다.

모든 랜섬웨어 뉴스가 나쁜 것은 아닙니다. Conti 그룹 협력자들로부터 유출된 문서를 통해 연구원들은 랜섬웨어 집단이 사용하는 도구와 전술을 더 잘 파악하게 되었으며 이들 그룹을 잠시 묶어 두는데 도움이 되었습니다. 그럼에도 불구하고 협력자들은 일반적으로 법 집행 기관에 의해 차단되면 다른 랜섬웨어 그룹으로 이전합니다. Conti의 경우 협력자들이 2021년 하반기에도 핵심 산업에 대한 공격을 계속할 수 있었기 때문입니다.

2021년 하반기 타게팅된 주요 핵심 인프라 산업


교통


의료


식품

공급망 공격으로 빠르게 피해 확산

가장 주목할 만한 취약성 - 2021년 하반기

Apache Log4j (CVE-2021-44228)

피해

많은 플랫폼과 산업에서 광범위한 피해가 발생했습니다. 랜섬웨어 그룹은 취약성을 악용하여 파일을 암호화하고 지불을 탈취하는 완전한 프로세스를 통해 반복 가능한 공격을 재빨리 만들어 냈습니다. 이제 조직은 취약한 시스템을 보다 신속하게 파악하고 개선할 수 있도록 소프트웨어 애플리케이션에 대한 소프트웨어 BOM(Bill of Material)을 유지 관리하는 것의 중요성을 인식하고 있습니다.

Log4j 라이브러리를 신속하게 개선하지 않는 조직의 경우 그 여파는 향후 몇 달 또는 몇 년 동안 이어질 수 있습니다.

공급망 공격은 피해를 빠르게 확산시킬 수 있는 공격입니다.

공통 소프트웨어 구성 요소가 얼마나 널리 사용되고 있으며 취약성이 악용될 수 있는지에 따라 공급망 공격으로 수백 또는 수천 개의 조직이 혼란에 빠질 수 있습니다.

널리 보고된 최초의 공급망 공격은 1년 전 SolarWinds 취약성으로 인해 산업 및 연방 정부 전반에 걸쳐 수십 개의 중요한 네트워크 운영이 손상된 시기였습니다. 그 이후로 오픈 소스 코드의 실제 취약성과 악용에 대한 우려가 증가하는 것이 확인되었습니다.

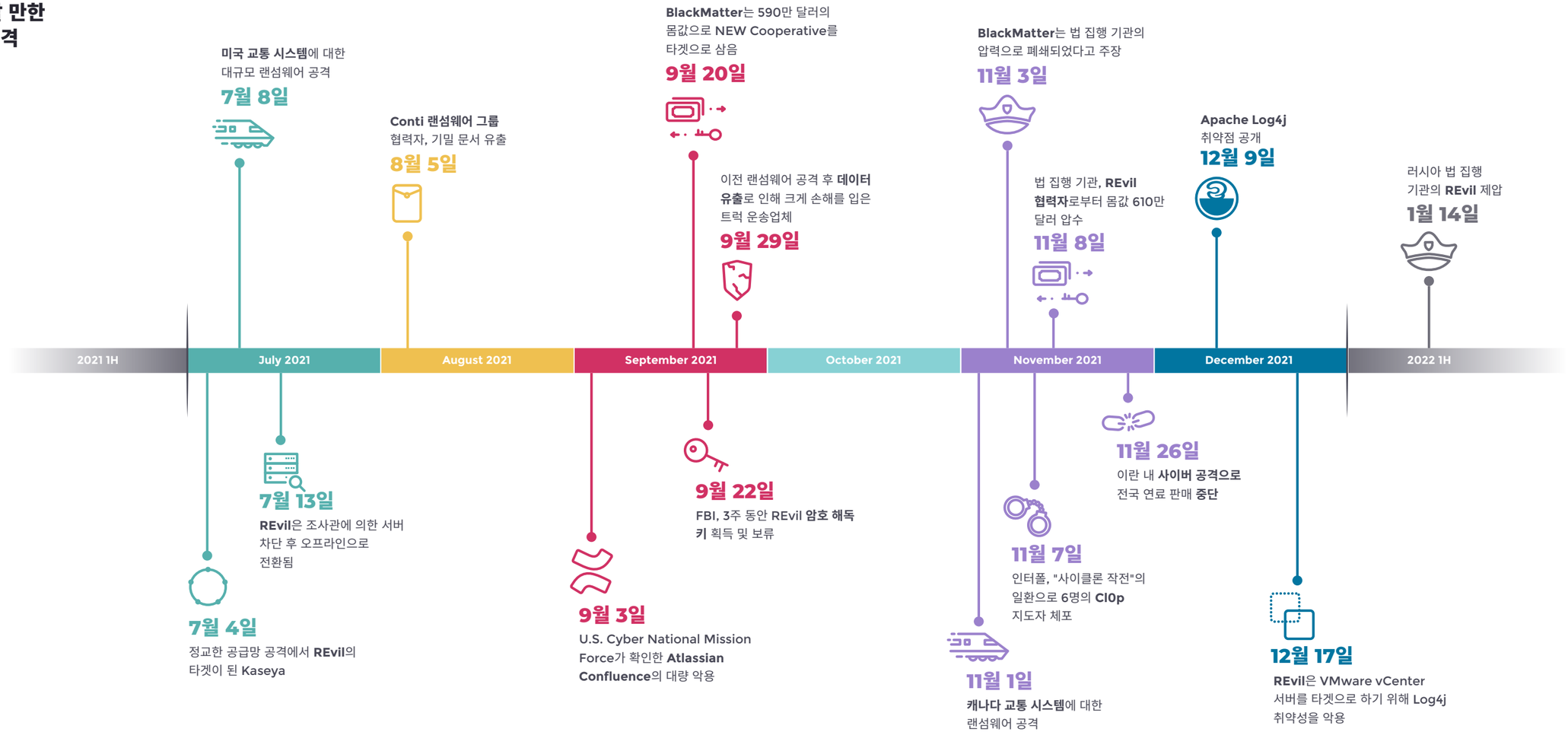
많은 애플리케이션에서 사용할 수 있는 오픈 소스 소프트웨어에서 취약성이 발표되면 단일 공급업체 소프트웨어 수준 또는 그 이상으로 피해가 커질 수 있습니다. 이는 라이브러리 구성 요소가 얼마나 널리 사용되는지에 따라 다릅니다.

Log4Shell 취약성이 12월에 공개된 경우도 마찬가지였습니다. Log4Shell은 상용 애플리케이션 및 대규모 온라인 플랫폼에서 널리 사용되는 Apache Log4j(log-forge로 발음) 오픈 소스 로깅 라이브러리에서 발견되었습니다.

이 악용은 매우 단순하여 공격자들은 전 세계적인 개선 및 패치 작업보다 빠르게 공격을 시작할 수 있었습니다.

가장 큰 랜섬웨어 그룹 중 한 그룹은 일주일 만에 Log4j 익스플로잇을 이용하여 VMware vCenter 배포에 대한 공격을 시작했습니다.

2021년 하반기 주목할 만한 랜섬웨어 및 공급망 공격 타임라인



Nozomi Networks OT/IoT 취약성 연구

Nozomi Networks 연구소 취약성 연구, OT/IoT 장치 및 네트워크 중심

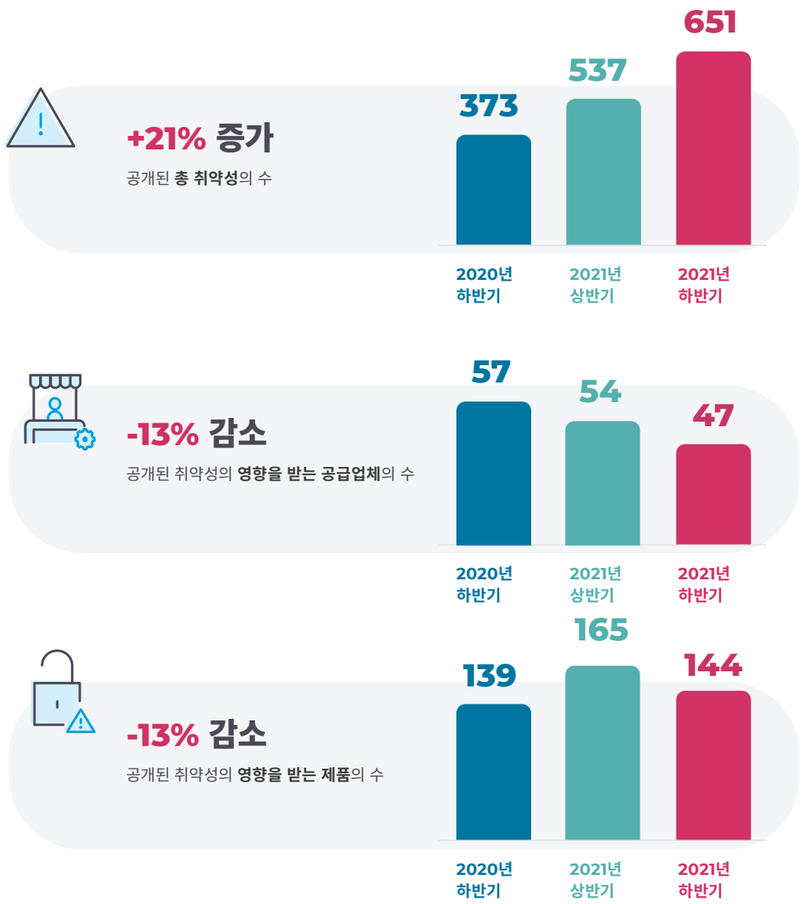
OT 및 IoT 장치는 Nozomi Networks 연구소의 주요 연구 분야입니다. 지난 몇 년 동안 IoT 장치는 전체 네트워크에 대한 공통적인 진입점이 되었으며 널리 배포된 IT 플랫폼 및 운영 체제에 비해 간과되는 경우가 매우 많습니다.

IoT 장치는 종종 전력 및 비용 제약에 따라 보안 기능이 제거된 단순한 운영 체제를 실행합니다.

SCADA 및 ICS 장비와 같은 OT 시스템은 한때 Wi-Fi, 인터넷 및 대규모 IT 클라우드 네트워크 간의 에어 갭에 의존할 수 있었지만 이제는 그렇지 않습니다. 이에 따라 보안 방어가 강화되어야 합니다.

이 반기 보고서에서 Nozomi Networks 연구소는 공급망, 클라우드 플랫폼, 특정 엔터프라이즈 소프트웨어 플랫폼의 취약성을 포함하여 당사의 주요 연구 영역 중 일부를 강조합니다. 2021년 하반기에 연구소 팀에서 가장 영향력 있는 취약성 공개 몇 가지를 검토하는 것 외에도 우리는 감시 시스템의 공격 표면과 자산 소유자가 네트워크에 배포하기 전에 염두에 두어야 할 사항에 대한 연구에 대해 다룹니다.

ICS 취약성 동향 - 2021년 상반기 대비 2021년 하반기



오늘날의 위협에 대처하기 위해 알아야 할 사항

결론 및 권고

OT 및 IoT 환경에서 사이버 방어를 강화하려면 보완 기술, 잘 정의된 감독 및 프로세스, 필요한 보안 위생 등 다각적인 접근 방식이 필요합니다. 보안 팀이 너무 자주 과부하되면 인적 오류가 발생하여 약한 암호, 잘못 구성된 네트워크 및 장치, 사회 공학 등으로 인해 가장 진보된 방어 수단에도 문제가 발생할 수 있습니다. 대부분의 랜섬웨어 공격은 순진한 사용자가 방어가 잘 된 네트워크에서 악성 이메일 링크를 클릭하는 것으로 시작됩니다.

네트워크 세분화는 중요한 애플리케이션 및 OT 프로세스로의 맬웨어 확산을 방지하기 위한 사이버 방어 전략의 또 다른 기본 구성 요소입니다. 환경 및 정책 요구 사항에 따라 VLAN 및 방화벽과 같은 네트워크를 분할하는 데 다양한 기술을 사용할 수 있습니다. OT 네트워크에서 Purdue 모델은 프로세스 요소 및 시스템 기능에 맞는 네트워크 영역을 만드는 한 가지 방법입니다. 그러나 미션 크리티컬 애플리케이션 및 프로세스가 있으며 쉽게 손상되는 시스템에서 격리가 거의 또는 전혀 없는 완전히 평평한 네트워크(최소 분할)를 가진 조직이 너무 많습니다.

이 보고서에서는 제로 트러스트 모델에 이르기까지 네트워크 세분화를 늘리는 방법을 제안합니다. 마이크로 세분화라고도 하는 제로 트러스트는 명시적으로 허용되는 연결을 제외하고 개별 엔드포인트 간의 모든 네트워크 연결이 거부됨을 의미합니다. 제로 트러스트 모델로 마이그레이션할 때 방해를 피하기 위해 명시적으로 승인된 연결을 지정하기 전에 트래픽 패턴을 모니터링하여 조직내 합법적인 트래픽 흐름을 이해하는 것이 중요합니다.

네트워크 흐름과 OT 프로세스 모두에서 잠재적인 보안 위협, 위반 및 기타 이상을 감지하기 위해 트래픽 모니터링의 중요성에 대해 더 논의합니다. 마지막으로 공격 표면 감소와 합리적인 노력으로 효과적으로 달성할 수 있는 것에 대해 설명합니다.

즉시 취해야 할 4가지 개선 조치

- 펌웨어 접근성
- 네트워크 모니터링
- 네트워크 세분화
- 공격 표면 감소

이 보고서는 위협 및 취약성 환경의 주요 영역에 대한 통찰력을 제공하여 조직이 보안 태세를 평가하고 강화하는 데 도움이 되는 것을 목표로 합니다.

우리는 기업이 OT/IoT 가시성, 보안 및 모니터링을 개선하여 앞으로 발전해 나갈 것을 권장합니다. 오늘날의 공격자들의 교묘함과 무자비함 속에 침해 후 사고방식의 채택도 중요합니다.

IT/OT 보안 태세의 지속적인 발전이 운영 시스템의 가용성, 안전성, 무결성, 기밀성을 보장하는 가장 좋은 방법입니다.

Nozomi Networks 연구소의 추가 OT/IoT 사이버 보안 연구

연구 보고서

OT/IoT 보안 보고서: 중요 인프라 공격의 동향 및 대책

다음의 전체 보고서 다운로드:

- 2021년 하반기 랜섬웨어 및 소프트웨어 공급망 공격에 대한 통찰력
- OT/IoT 취약성 연구 및 악용 동향
- 제안된 개선 전략

다운로드

백서

S3CUREC4M 프로젝트: 최신 IP 영상 감시 기술의 취약성 연구

다음의 백서 다운로드:

- 하드웨어 분석 및 펌웨어 추출 기술
- 감시 시스템의 소프트웨어 공격 표면에 대한 통찰력
- 최신 IP 비디오 감시 기술의 보안 평가

다운로드

전체 연구 보고서의 목차

NOZOMI NETWORKS

Nozomi Networks

OT, IoT 보안과 가시성을 위한 최상의 솔루션

Nozomi Networks는 전 세계의 중요 인프라, 산업, 정부 조직을 사이버 위협으로부터 보호하여 디지털 트랜스포메이션 속도를 높입니다. 당사 솔루션은 OT 및 IoT 환경에 대한 탁월한 네트워크 및 자산 가시성, 위협 탐지, 통찰력을 제공합니다. 고객들은 당사 서비스를 이용하여 운영 회복력을 극대화하면서 위험과 복잡성을 최소화하고 있습니다.

NN-SEC-RP-ES-KO-2021-2H-001

nozominetworks.com