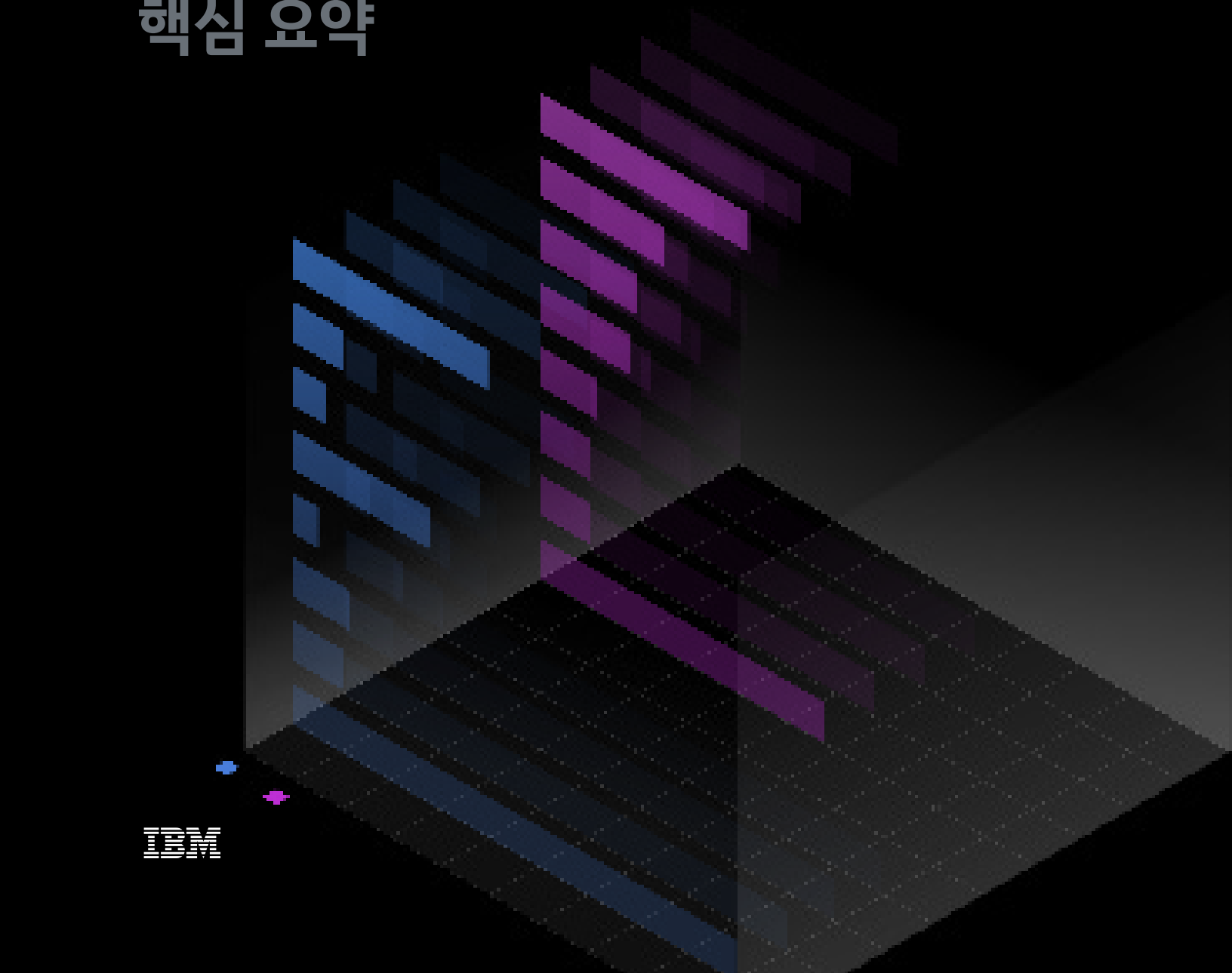
IBM Security

X-Force Threat Intelligence Index 2021

핵심 요약



IBM

소개

2020년은 의심할 여지 없이 최근 모습 중 가장 중요하고 변혁적인 해였습니다. 전세계적인 팬데믹, 수백만 명의 삶에 영향을 미치는 경제적 혼란과, 사회적 그리고 정치적 불안이 우리를 덮쳤습니다. 이러한 사건으로 인한 반향은 기업들이 분산된 환경, 원격 근무로의 전환을 포함하며 비즈니스에 깊은 영향을 미쳤습니다.

사이버 영역을 살펴보면 2020년의 비정상적인 상황은 사이버 공격자들에게 통신 네트워크의 필요성을 악용할 기회를 제공했고 공급망과 중요 인프라에 대한 풍부한 공격의 대상을 제공했습니다. 빠른 대응과 복원이 필요한 전세계적으로 중대한 위협이 발견되면서 한해가 마무리 되었습니다. 주로 단일 민족 활동가에 기인한 공격은 네트워크 모니터링 소프트웨어의 백도어를 활용하여 정부 및 민간 부문 조직을 공격했으며, 이로써 제3자 위험을 예상해야 하지만 예측할 수 없음이 입증되었습니다.

이러한 시대의 과제를 해결하기 위해 IBM Security X-Force는 사이버 위협 환경을 평가하고 조직이 진화하는 위협, 관련 위험, 사이버 보안 노력의 우선 순위를 지정하는 방법을 이해하도록 지원합니다. 고객에게 제공하는 프리미엄 위협 인텔리전스 외에도 위협 지형도와 변화 방식에 대한 연례 점검 지표로서 X-Force 위협 인텔리전스 인덱스 (X-Force Threat Intelligence Index)를 생성하기 위해 수집한 풍부한 데이터를 분석합니다.

추적한 트렌드 중 랜섬웨어는 지속적으로 급증하여 2020년 X-Force가 대응한 보안 이벤트의 23%를 차지하는 1위 위협 유형이 되었습니다. 랜섬웨어 해커들은 데이터 암호화를 위협과 결합하여 공개 사이트에 데이터를 유출함으로써 금전을 강탈하려고 시도했습니다. X-Force 추정치에 따르면 이러한 공격으로 단하나의 랜섬웨어 갱단이 2020년 1억 2천3백만 달러 이상의 수익을 거두었습니다.

제조 업체는 2020년에 랜섬웨어 및 기타 공격의 맹습에 시달렸습니다. 전체적으로 제조업은 금융과 보험에 이어 두 번째 타겟이 되었으며, 이는 2019년에 8번째 타겟 산업이었던 점과 비교됩니다. X-Force는 제조업과 코로나19 백신 공급망과 관련된 NGO에 대한 공격에서 표적 스피어 피싱 캠페인을 사용한 정교한 해커들을 발견했습니다.

1. 이 보고서의 모든 통화는 미국 달러입니다.

위협 행위자들은 악성 코드, 특히 비즈니스에 중요한 클라우드 인프라와 데이터 스토리지를 지원하는 오픈 소스 코드, Linux를 표적으로 하는 악성 코드를 혁신적으로 개발했습니다. Intezer의 분석에 따르면 2020년에 다른 위협 유형에서 발견된 혁신 수준보다 훨씬 많은 56개의 새로운 Linux 맬웨어 제품군이 발견되었습니다.

우리는 2021년이 더 나은 해가 되기를 바라고 있습니다. 트렌드는 정말 예측하기 어렵지만 항상 의지할 수 있는 것은 변화입니다. 사이버 보안의 증가 및 감소 과제에 대응하는 복원성에는 실행 가능한 인텔리전스와 더 개방적이고 연결된 보안의 미래를 위한 전략적 비전이 필요합니다.

커뮤니티 파워의 중요성을 염두에 두고 있는 IBM Security는 2021 X-Force Threat Intelligence Index를 제공하게 된 것을 기쁘게 생각합니다. 이 보고서의 연구 내용은 보안팀, 위험 전문가, 의사 결정자, 연구자, 미디어 등이 작년에 위협이 어디에 존재했는지 이해하고 다음에 발생할 위험을 대비하도록 도움을줍니다.

개요

IBM Security X-Force는 2020년 1월에서 12월까지 고객과 공개 소스에서 수집한 수십억 개의 데이터 포인트를 활용하여 공격 유형, 감염 벡터, 글로벌 및 업종별 비교치를 분석했습니다. 다음은 X-Force 위협 인텔리전스 인덱스에 제시된 몇 가지 주요 결과입니다.

23%

랜섬웨어 공격 점유율

랜섬웨어는 2020년에 가장 인기 있는 공격 방법으로, IBM Security X-Force가 대응하고 해결하는 데 도움을 준 모든 사고의 23%를 차지했습니다.

$1억2천3백만 달러 이상

상위 랜섬웨어의 추정 수익

X-Force는 Sodinokibi (REvil이라고도 알려짐) 랜섬웨어 공격자만으로도 2020년에 최소 1억2천3백만달러의 수익을 올렸으며 약 21.6 테라바이트의 데이터를 훔친 것으로 보수적으로 추정합니다.

25%

2020년 1분기 공격을 가장 많이 받은 취약성

위협 행위자들은 경로 순회 Citrix 결함을 이용하여 첫 3개월 동안 전체 공격의 25%, 2020년 전체 공격의 8%에서 이 취약성을 악용했습니다.

35%

스캔 및 악용을 당한 상위 감염 벡터 점유율

취약성에 대한 스캔 및 악용은 2020년 최고 감염 벡터로 급증했으며 2019년 최고 벡터였던 피싱을 능가했습니다.

2위

격 대상 산업에서 제조업의 순위

제조업은 2020년에 두 번째로 많은 공격을 받은 산업으로 2019년 8위에서 금융 서비스에 이은 2위를 차지했습니다.

5시간

위협 그룹 서버에 존재한 공격 교육 비디오 시간

이란 국가 공격자들의 운영 오류로 인해 X-Force 연구원은 잘못 구성된 서버에서 약 5시간 분량의 비디오를 발견했으며 그들의 기술에 대한 통찰력을 얻을 수 있었습니다.

100명 이상

정밀 피싱 캠페인 대상 임원

2020년 중반, X-Force는 코로나19와의 전쟁에서 개인 보호 장비(PPE)를 확보하며 태스크 포스의 관리 및 조달 역할을 맡고 있는 100명 이상의 고위 임원에게 전송된 글로벌 피싱 캠페인을 발견했습니다.

49%

ICS 관련 취약성 증가율, 2019~2020

2020년에 발견된 산업 제어 시스템(ICS) 관련 취약성은 2019년에 비해 49% 증가했습니다.

56개

새로운 Linux 악성 코드 그룹의 수

2020년에 발견된 새로운 Linux 관련 악성 코드 그룹의 수는 56개로 역대 최고 수준입니다. 이는 2019년부터 2020년까지 전년 대비 40% 증가한 수치입니다.

31%

유럽의 공격 대상 점유율

유럽은 2020년에 가장 많은 공격을 받은 지역으로 X-Force가 관찰한 공격의 31%를 차지했으며 북미(27%)와 아시아(25%)가 그 뒤를 이었습니다.

향후 전망

기존 위협과 새로운 위협이 혼합되는 2021년에는 보안팀이 많은 위험을 동시에 고려해야 합니다. X-Force 분석에 따르면 다음 해의 우선 순위 핵심 사항은 하기와 같습니다.

- **2021년에도 위험이 계속 표면화할 것입니다.** 기존 및 신규 애플리케이션과 장치 모두에서 보고될 수 있는 새로운 취약성이 수천 개 존재합니다.
- **랜섬웨어에 대한 이중 갈취는 2021년까지 지속될 것입니다.** 비리자 공개 사이트에 데이터를 공개적으로 유출하는 해커들을 등에 업고 위협 행위자들은 랜섬웨어 감염에 대해 높은 가격을 요구하고 있습니다.
- **위협 행위자들은 계속해서 다른 공격 벡터로 수단을 바꿉니다.** Linux 시스템, 운영 기술(OT), IoT 장치 및 클라우드 환경은 계속 타겟일 될 것입니다. 이러한 시스템과 장치의 표적화가 더욱 발전함에 따라 위협 행위자들은 특히 중요한 사건 이후에 신속하게 수단을 전환할 수 있습니다.
- **모든 산업에는 위험이 존재합니다.** 산업별 타겟팅의 전년 대비 변화는 모든 산업 부문에 대한 위험이 존재하며 전반적인 사이버 보안 프로그램의 의미 있는 발전과 성숙이 필요함을 강조합니다.

회복 가능성(Resilience)을 높이기 위한 권고 사항

이 보고서의 IBM Security X-Force 조사 결과에 따르면 위협 인텔리전스를 유지하고 강력한 대응 능력을 구축하는 것은 어떤 산업 또는 국가에서 활동하는지에 관계없이 진화하는 환경에서 위협을 완화하는 효과적인 방법입니다.

X-Force는 조직이 2021년 사이버 위협에 더 잘 대비할 수 있는 다음 단계를 권장합니다.

위협에 대응하기 보다 앞서 나갑니다. 위협 인텔리전스를 활용하여 위협 행위자의 동기와 전술을 더 잘 이해함으로써 보안 리소스의 우선 순위를 지정합니다.

랜섬웨어 대응의 핵심은 준비입니다. 혼합된 랜섬웨어 및 데이터 절도 기술을 다루는 계획을 포함하여 랜섬웨어 공격을 방어하는 계획을 세우고 정기적으로 이러한 계획을 연습하면 중요한 순간에 조직이 대응하는 방식에서 큰 차이를 만들 수 있습니다.

조직의 패치 관리 구조를 다시 확인하십시오. 작년에 스캔 및 악용이 가장 일반적인 감염 벡터가 되면서 인프라를 강화하고 내부 탐지를 강화하여 자동화된 침입 시도를 빠르고 효과적으로 찾아 차단합니다.

내부자 위협으로부터 보호합니다. DLP(데이터 손실 방지)솔루션, 교육 및 모니터링을 사용하여 부주의하거나 악의적 인 내부자가 조직을 침해하는 것을 방지합니다.

조직 내에서 사고 대응팀을 구축하고 교육합니다. 또는, 효과적인 사고 대응 능력을 활용하여 영향력이 큰 사고에 신속하게 대응하십시오.

무의식적 기억(muslce memory)으로 체화하기 위해 위해 조직내 사고 대응 계획에 대한 스트레스 테스트를 수행합니다. 테이블탑 연습 또는 다양한 사이버 경험은 대응팀에 중요한 경험을 제공하여 대응 시간을 개선하고 다운 타임을 줄이며 궁극적으로 침해 발생시 비용을 절감할 수 있습니다.

다단계 인증(MFA)을 구현합니다. 계정에 보호 계층을 추가하는 것은 조직을 위한 가장 효율적인 보안 우선 순위 중 하나입니다.

백업을 하고, 백업을 테스트하고, 백업을 오프라인으로 저장합니다. 백업 자체를 보장할 뿐만 아니라 실제 테스트를 통한 효율성은 특히 랜섬웨어 활동의 부활을 보여주는 2020년 데이터를 감안할 때 조직 보안에서 중요한 차이를 만듭니다.

IBM Security X-Force 정보

IBM Security X-Force는 고객이 보안 태세를 개선하도록 통찰력, 탐지 및 대응 기능을 제공합니다.

IBM Security X-Force Threat Intelligence는 IBM 보안 운영 원격 측정, 연구, 사고 대응 조사, 상용 데이터 및 오픈 소스를 결합하여 고객이 새로운 위협을 이해하고 정보에 입각한 보안 결정을 신속하게 내리도록 지원합니다.

또한 고도로 훈련된 X-Force 사고 대응팀은 조직이 보안 사고 및 위반을 더 잘 제어하도록 지원하는 전략적 복원 수단을 제공합니다.

IBM Security Command Center의 다양한 사이버 경험을 결합한 X-Force는 고객이 오늘날 실제 위협에 대비하도록 교육합니다.

IBM X-Force 연구원은 연중 블로그, 백서, 웨비나, 팟 캐스트의 형태로 연구 및 분석 자료를 지속적으로 제공하여 지능형 위협 행위자, 새로운 악성 코드 및 새로운 공격 방법에 대한 인사이트를 제공합니다. 또한 프리미어 위협 인텔리전스 플랫폼 구독 고객에게 가장 최신 분석 결과를 제공합니다.

다음 단계

IBM Security를 통한 사고 대응에 대해 알아보기 >

IBM Security에 대해

IBM Security는 AI가 구현된 고급 일체형 엔터프라이즈 보안 제품 및 서비스 포트폴리오와 제로 트러스트 원칙에 기반하여 보안 전략에 대한 현대적인 접근 방식을 통해 비즈니스를 보호하고 불확실성에 대처하도록 지원합니다. 보안 전략을 비즈니스에 연계하고, 디지털 사용자, 자산 및 데이터를 보호하도록 설계된 통합 솔루션을 사용하고, 증가하는 위협에 대한 방어 수단을 관리하는 기술을 배포하여 오늘날의 하이브리드 클라우드 환경을 지원하는 위험 관리 및 통제 수단을 제공합니다.

새로운 현대적이고 개방적인 접근 방식인 IBM Cloud Pak for Security 플랫폼은 RedHat Open Shift를 기반으로 구축되었으며 광범위한 파트너 에코 시스템을 통해 차세대 하이브리드 멀티 클라우드 환경을 지원합니다. Cloud Pak for Security는 기존 보안 도구를 신속하게 통합하여 하이브리드 클라우드 환경 전반에 걸쳐 위협에 대한 심층적인 통찰력을 제공함으로써 데이터 및 애플리케이션의 보안을 관리할 수 있는 엔터프라이즈급 컨테이너 소프트웨어 솔루션입니다. 이를 통해 보안 대응을 쉽게 조율하고 자동화할 수 있습니다.

자세한 내용은 www.ibm.com/security을 참조하시거나, Twitter @IBMSecurity를 팔로우하시거나 IBM Security Intelligence 블로그를 방문하십시오.

도움을 주신 분들

대표 저자:
Camille Singleton

기여자:
Allison Wikoff
Ari Eitan (Intezer)
Charles DeBeck
Charlotte Hammond
Chenta Lee
Chris Sperry
Christopher Kiefer
Claire Zaboeva
David McMillen
David Moulton
Dirk Hartz
Georgia Prassinos
Ian Gallagher (Intezer)
John Zorabedian
Joshua Chung
Kelly Kane
Lauren Jensen
Limor Kessem
Mark Usher
Martin Steigemann
Matthew De Fir
Megan Radogna
Melissa Frydrych
Michelle Alvarez
Mitch Mayne
Nick Rossman
Patty Cahill-Ingraham
Randall Rossi
Richard Emerson
Salina Wuttke
Scott Craig
Scott Moore

(07326) 서울시 영등포구 국제금융로10
국제금융로 10
TEL: (02)3781-7114

:NONE.
2021년 2월