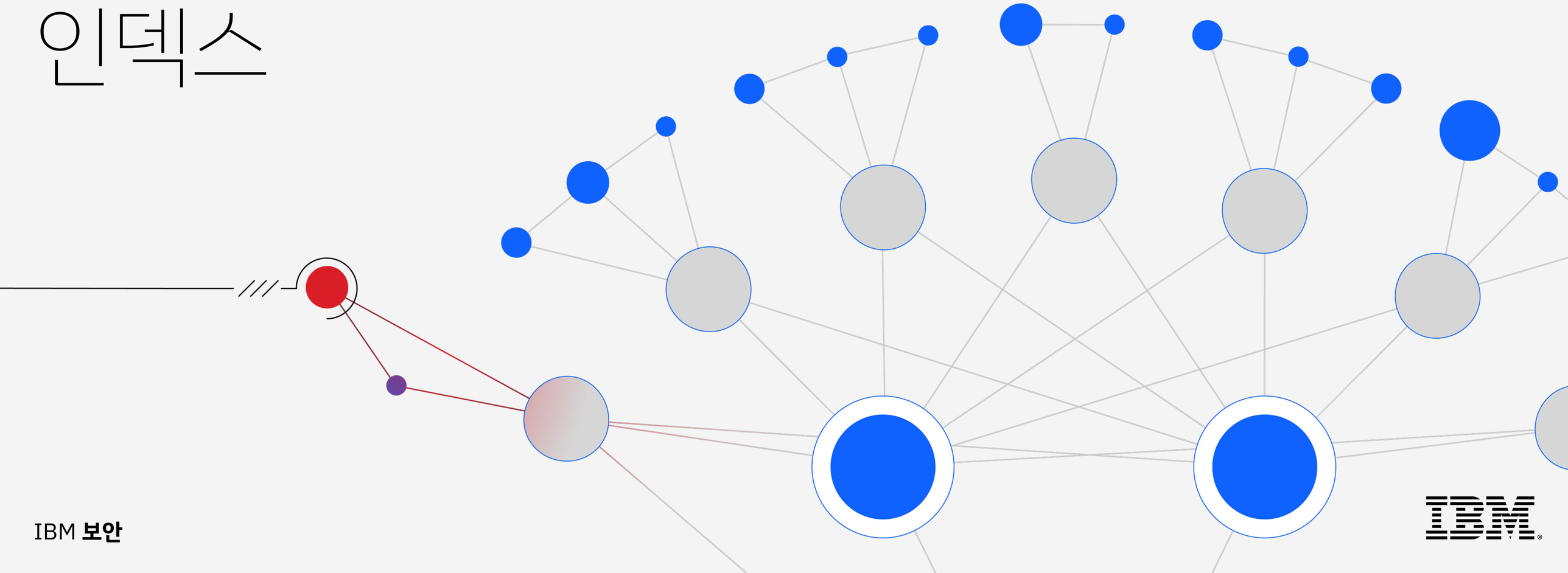
2023년 X-Force 위협 인텔리전스 인덱스

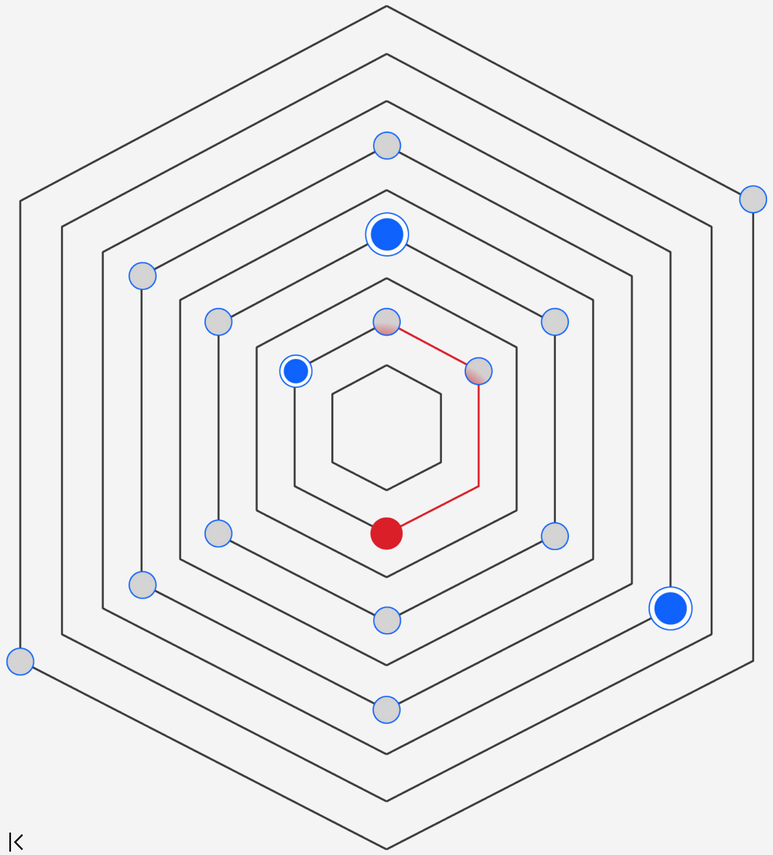


IBM 보안

목차

01

개요



2022년도 역시 사이버 보안 문제로 떠들썩한 한 해였습니다. 기존에 있던 문제들도 줄어들지 않았지만, 팬데믹의 영향이 계속되는 가운데 우크라이나에서 발발한 무력 충돌은 가장 큰 부분을 차지했습니다. 2022년에 발생한 가동 중단은 경제적, 지정학적, 인적 격변을 불러오고 비용을 초래했으며, 이러한 혼란은 사이버 범죄자들이 활동하기 좋은 환경입니다.

그리고 실제로 많은 활동이 있었습니다.

IBM Security® X-Force®는 기회를 엿보던 위협 행위자가 무질서한 환경을 활용하여 전 세계의 정부와 조직에 침투하는 것을 목격했습니다.

2023년 IBM Security X-Force 위협 인텔리전스 인덱스는 신규/기존 트렌드와 공격 패턴을 추적하며, 네트워크 및 엔드포인트 디바이스, 인시던트 응답(IR) 참여, 취약성, 악용 데이터베이스 등에 이르는 수십억 개의 데이터 요소를 포함하고 있습니다. 이 보고서는 2022년 1월부터 12월까지 수집한 포괄적인 연구 데이터입니다.

IBM은 이러한 발견을 통해 IBM 고객, 사이버보안 연구원, 정책 입안자, 미디어, 보안 업계 전문가, 리더로 이루어진 대규모 커뮤니티에 리소스를 제공합니다. 오늘날의 불안정한 환경에서는 악성 위협이 점점 정교해지고 있으며 기업과 일반 사용자를 보호하려면 협업을 통한 노력이 필요합니다. 그 어느 때보다 위협 인텔리전스와 보안 인사이트로 무장하여, 공격자보다 앞서고 중요 자산을 보호해야 할 때입니다.

또한 회사의 번영을 위해서도 필요합니다.

데이터 분석 변경 사항(2022년)

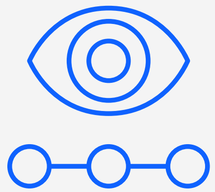
2022년 IBM은 일부 데이터 검사 방식을 변경했습니다. 이로써 더욱 통찰력 있는 분석이 가능해지고 업계 표준 프레임워크에 보다 근접하게 맞출 수 있게 되었습니다. 따라서 정보에 입각한 보안 의사 결정이 더 많아졌으며, 조직을 위협에서 효과적으로 보호할 수 있습니다.

2022년 IBM 분석에 대한 변경 사항은 다음과 같습니다.

- **초기 액세스 벡터:** MITRE ATT&CK 프레임워크를 채택하여 초기 액세스 벡터를 자세히 추적하면 광범위한 사이버보안 업계와 연구 결과에 보다 긴밀한 연관될 수 있고, 이를 통해 기술 수준에서 중요한 트렌드를 식별하게 됩니다.
- **악용 및 제로 데이 손상:** 거의 30년 동안의 데이터를 포함하고 있는 견고한 취약성 데이터베이스에서의 추론을 통해, 분석에 컨텍스트를 제공하고 취약성으로 인한 실제 위협을 식별하는 데 도움을 얻을 수 있습니다. 또한, 이 프로세스는 무기화 가능한 악용과 영향력 있는 제로 데이의 비율이 감소할 때 이에 컨텍스트를 부여합니다.
- **위협 행위자 방식과 그 영향력:** 공격 중 위협 행위자들이 취하는 조치를 인시던트의 실제 영향에서 분리함으로써 인시던트의 위험 단계를 식별할 수 있었습니다. 따라서 이 프로세스는 대응 담당자가 인시던트 발생 이후 처리하기 위해 준비할 부분을 알려줍니다.

02

보고서 하이라이트



관찰된 목표에 적용된 주요 조치: 2022년 목표에 대해 내렸던 최고의 조치는 21%의 백도어 배포였으며, 이는 해결된 모든 인시던트 중 1/4에 달합니다. 특히, 연초에 급증한 다목적 멀웨어 Emotet은 해마다 관찰되는 백도어 활동의 급증에 크게 기여했습니다. 이와 같은 백도어 활동의 급증에도 불구하고, 적어도 2020년 이후부터 계속 최상위 자리에 있던 랜섬웨어가 인시던트의 17%로 큰 부분을 차지하며 해당 멀웨어가 가하는 지속적인 위협을 강화했습니다.

조직에 영향을 미치는 가장 흔한 공격은 갈취입니다. 위협 행위자 공격 방식의 27%를 차지하는 갈취는 명백한 영향을 미칩니다. 사이버 범죄자들이 경직된 산업을 악용하는 추세가 계속되면서, 갈취로 이어지는 인시던트에서 제조업 부문 피해자가 30%를 차지했습니다.

주요 초기 액세스 벡터는 피싱이었습니다. 피싱은 인시던트의 41%에서 식별된 주요 감염 벡터로 남아 있으며 26%의 공용 애플리케이션 악용이 그 뒤를 이었습니다. 악성 매크로에 의한 감염은 Microsoft에서 매크로 차단을 기본값으로 하기로 결정하면서 그 발생률이 떨어졌습니다. 악성 ISO 및 LNK 파일은 에스컬레이션을 주요 수법으로 사용하여 2022년 스팸을 통해 멀웨어를 전달합니다.

핵티비즘 및 파괴적인 멀웨어의 증가: 우크라이나 러시아 전쟁은 많은 사이버보안 커뮤니티에서 볼 수 있을 것이라 기대했던, 현대 전쟁을 지원하는 사이버 방식에 길을 열어주었습니다. 이러한 상황 속에서 최악의 사이버공간 예견이 실현되지는 않았지만, 핵티비즘과 파괴적인 멀웨어는 눈에 띄게 다시 증가했습니다.

또한 X-Force는 사이버 범죄 그룹과 우크라이나 조직을 대상으로 하는 Trickbot 갱 사이의 협력을 비롯하여 사이버 범죄 세계의 전례 없는 변화를 목격했습니다.

03

주요 통계

27%

갈취 공격의 비율

위협 행위자는 2022년 X-Force가 응답한 전체 인시던트의 1/4이 넘는 사례에서 피해자의 금전을 노렸습니다. 이들이 사용한 수법은 지난 수십 년간 진화해왔으며, 이러한 트렌드는 위협 행위자가 더 공격적으로 이익을 추구함에 따라 지속될 것으로 예상됩니다.

21%

배포 백도어를 파악한 인시던트의 비율

백도어 배포는 지난해 목표 중 최고로 많이 사용된 조치였으며 전 세계적으로 보고된 인시던트 5건 중 1건 이상에서 발생했습니다. 방어자의 성공적인 개입이 랜섬웨어가 포함되었을지도 모르는 위협 행위자의 추가 목표를 달성하지 못하도록 막았을 가능성이 높습니다.

17%

랜섬웨어의 공격 점유율

수많은 랜섬웨어 신디케이트로 혼란스러운 한 해를 보냈음에도 불구하고, 랜섬웨어는 백도어 배포에 이어 두 번째로 흔한, 조직의 운영을 지속적으로 방해하는 조치였습니다. 인시던트에서 랜섬웨어의 점유율은 2021년 21%에서 2022년 17%로 감소했습니다.

41%

초기 액세스에 피싱이 포함된 인시던트 비율
피싱 작업은 2022년에도 가장 흔한 손상 경로였으며, 초기 액세스를 확보하는 이 기술을 사용한 X-Force를 통해 41%의 인시던트가 해결되었습니다.

100%

월별 스레드 하이재킹 횟수 증가
2021년 데이터에 비해 2022년의 월별 스레드 하이재킹 시도는 두 배 더 많았습니다. Emotet, Qakbot, IcedID로 이어지는 스팸 이메일은 스레드 하이재킹을 많이 사용했습니다.

52%

신용카드 데이터를 찾는 피싱 키트 보고 감소
데이터에서 분석된 거의 모든 피싱 키트는 98%의 이름, 73%의 이메일 주소, 66%의 집 주소, 58%의 비밀번호를 수집했습니다. 2021년 전체 시간 상 61%의 표적이 되었던 신용카드 정보는 위협 행위자의 관심을 얻지 못했습니다. 데이터를 보면 2022년 피싱 키트의 29%에서만 신용카드 정보를 찾았음을 알 수 있는데 이는 52%나 감소한 것입니다.

62%

스피어 피싱 첨부 파일을 사용한 피싱 공격 비율
공격자는 자체적으로 배포하거나, 서비스를 통해 링크 또는 스피어 피싱과 함께 배포되는 무기화된 첨부 파일을 선호했습니다.

26%

알려진 악용이 있는 2022년 취약성 점유율
2022년의 취약성 중 26%는 알려진 악용이었습니다. X-Force가 1990년대 초부터 추적한 데이터에 따르면 이 비율은 최근 몇 년 간 감소해왔으며, 이는 잘 유지된 패치 관리 프로세스의 이점을 보여줍니다.

31%

아시아 태평양 지역을 목표로 한 글로벌 공격 점유율
아시아 태평양 지역은 2022년 전체 인시던트의 31%를 차지하며 가장 많이 공격을 받은 지역 1위를 유지했습니다. 이 통계를 통해 X-Force가 2021년 해당 지역에서 대응한 공격의 총 점유율에서 5% 포인트 증가했음을 알 수 있습니다.

04

주요 초기 액세스 벡터

2022년 X-Force는 초기 액세스 벡터를 피싱 및 자격 증명 도난 등의 보다 넓은 범주로 추적하는 것에서, 엔터프라이즈용 MITRE ATT&CK Matrix 프레임워크에 나열된 초기 액세스 기술로 변경되었습니다. 이러한 변경을 통해 X-Force는 기술 수준에서 중요한 트렌드를 보다 세밀하게 추적할 수 있었습니다. 또한, 이를 통해 보다 쉽게 사용 가능하면서도 교차 비교가 가능한 데이터를 제공하고, 더 광범위한 업계의 표준화 노력에 맞출 수 있게 되었습니다.

2022년 주요 초기 액세스 벡터

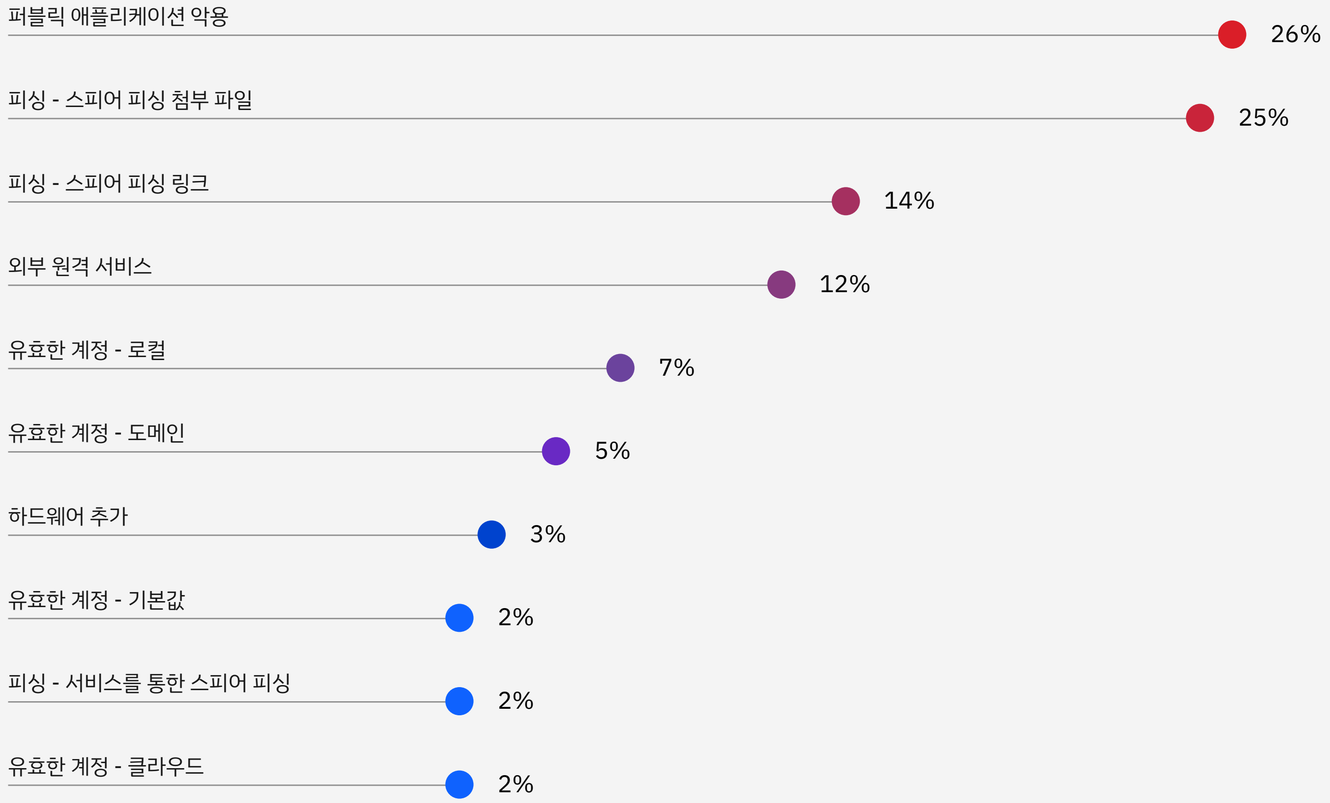


그림 1: 2022년에 가장 많이 관찰된 초기 액세스 벡터 X-Force. 출처: X-Force

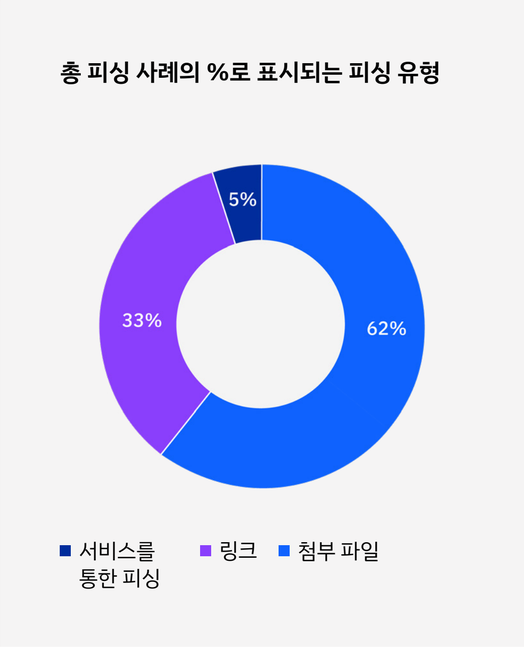


그림 2: 2022년에 X-Force에서 관찰된, 총 피싱 사례의 비율로 나타낸 피싱 하위 기술 유형. 출처: X-Force

피싱

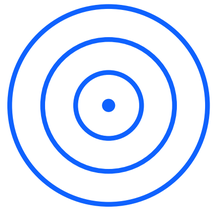
첨부 파일, 링크, 서비스로 유입되는 피싱(T1566)이 여전히 주된 감염 벡터이며, 이는 2022년에 X-Force로 해결된 모든 인시던트 중 41%를 손상했습니다. 이 비율은 2020년 33%에서 수치가 증가한 2021년부터 꾸준히 유지되고 있습니다. 모든 피싱 인시던트를 보면, 스피어 피싱 첨부 파일(T1566.001)이 해당 공격의 62%, 스피어 피싱 링크(T1566.002)가 33%, 서비스로서의 스피어 피싱(T1566.003)이 5%에서 사용되었습니다. 또한, X-Force는 위협 행위자가 일부 인스턴스에서 서비스 또는 링크로 피싱과 함께 첨부 파일을 사용하기도 하는 것을 목격했습니다.

2022년의 IBM X-Force Red 데이터는 피싱 및 위협 행위자에 대한 피싱과 잘못 처리된 자격 증명의 가치를 더 강조합니다. 2022년 클라이언트에 대한 침투 테스트에서 X-Force Red는 테스트의 약 54%가 부적절한 인증 또는 자격 증명 처리를 드러냈다고 밝혔습니다. X-Force Red Adversary Simulation 팀은 다중 인증(MFA) 토큰을 대상으로 하는 QR 코드를 사용해 주기적으로 스피어 피싱을 수행했습니다. ID 액세스 관리 및 Okta와 같은 SSO(Single Sign-On) 포털을 통해 노출되는 애플리케이션과 엔드포인트에 대한 가시성이 부족한 조직이 많이 있습니다.

두 번째로, X-Force가 대응한 인시던트의 26%에서 퍼블릭 애플리케이션(T1190)의 악용이 확인되었습니다. 이는 인터넷 연결 컴퓨터 또는 프로그램의 약점을 악용하는 공격자로 정의됩니다. 이는 과거 위협 인텔리전스 인덱스 보고서에서 '취약성 악용'이라고 언급했던 것과 상관이 있으며, 2021년의 34%에서 감소한 수치입니다.

세 번째로, 관찰된 인시던트의 16%에서 유효한 계정(T1078)의 남용이 식별되었습니다. 이는 공격자가 액세스 권한을 얻기 위해 기존 계정의 자격 증명을 획득하고 악용한 사례입니다. 이러한 인시던트는 클라우드 계정(T1078.004)과 기본 계정(T1078.001)이 각각 2%, 도메인 계정(T1078.002)이 5%, 로컬 계정(T1078.003)이 7%였습니다.

신용카드 정보는 2021년 61%의 시간 동안 목표 대상이 되었지만 2022년에는 피싱 키트의 29%로 크게 감소했습니다.



신용카드 데이터를 통해 PII를 표적으로 하며, 오래 지속되는 피싱 키트

IBM Security는 2년 연속으로 전 세계에서 수천 개의 피싱 키트를 분석하여 키트 배포가 더 오래 작동하고 더 많은 사용자에게 도달한다는 것을 발견했습니다. 이 데이터는 관찰된 피싱 키트의 수명이 매년 두 배 이상으로 증가했음을 보여주며, 데이터 세트 전반에서 배포 중앙값은 3.7일로 상대적으로 낮았습니다.

전반적으로, 가장 짧은 배포는 몇 분 동안 지속되었으며 2022년에 발견된 가장 긴 배포는 3년 이상 지속되었습니다. IBM에서 조사를 시행해 다음의 사실을 발견했습니다.

- 배포된 키트 중 1/3은 지난 해 약 2.3 일 동안 지속되었으며, 이는 같은 비율로 따졌을 때 하루를 넘지 않았던 전년도의 두 배 이상입니다.
- 보고된 모든 키트의 절반 가량이 93명의 사용자에게 영향을 미쳤지만, 2021년에는 각 배포에서 잠재적 피해자가 평균 75명을 넘지 않았습니다.
- 한 건의 보고된 피싱 공격에서 최대 총 피해자는 예외적인 수치이긴 하나 4,000명을 살짝 웃돌았습니다.
- 분석 및 보고된 피싱 키트는 거의 모두 98%로 이름을 수집하려고 했습니다. 이에 이메일 주소가 73%, 집 주소가 66%, 비밀번호가 58%로 그 뒤를 이었습니다.
- 신용 카드 정보는 2021년 61%의 시간 동안 목표 대상이 되었지만, 2022년에는 피싱 키트의 29%로 크게 감소했습니다.
- 신용카드 데이터를 찾는 피싱 키트의 인스턴스가 낮다는 것은 피셔가 개인 식별 정보(PII)를 우선으로 여긴다는 것이며, 이로써 더 광범위하고 악질적인 옵션을 허용하게 됩니다. PII는 다크 웹이나 그 외 포럼에서 수집 또는 판매될 수도 있고, 대상에 대한 추가 작업을 수행하는 데 사용될 수도 있습니다.

가장 많이 스푸핑된 브랜드

스푸핑이 가장 많이 관찰된 브랜드는 대부분 기술 분야의 유명 브랜드들이었습니다. X-Force는 좀 더 다양했던 2021년의 목록에서 이러한 변화가 생긴 것은 기본값으로 목표 삼은 브랜드 외에도 그 후 키트를 따로 설정하여 스푸핑하는 브랜드를 식별하는 능력이 향상되었기 때문이라고 생각합니다. 많은 피싱 키트는 다목적용이며, 간단한 매개 변수를 바꾸면 스푸핑할 브랜드를 변경할 수 있습니다. 예를 들어, 어떤 키트는 Gmail을 기본값으로 스푸핑하지만 한 줄 업데이트를 통해 공격 스푸핑 Microsoft로 바꿀 수 있습니다.

이러한 서비스에서 도난된 자격 증명은 가치가 있습니다. 피해자가 온라인 상태의 전체 부분을 관리할 때 사용하는 계정에 액세스를 얻게 되면, 다른 계정에 액세스하는 문이 열릴 수도 있습니다. 공격자가 중점적으로 다루는 이러한 형태의 초기 액세스는 2022년 클라우드 위협 환경 보고서에 뚜렷하게 밝혀져 있으며, 다크 웹에서 광고되는 판매용 클라우드 계정 수가 2021년에 관찰된 바의 200%로 3배 이상 증가한 것으로 나타났습니다.

연도별 가장 많이 스푸핑된 브랜드

	2022	2021
1	Microsoft	Microsoft
2	Google	Apple
3	Yahoo	Google
4	Facebook	BMO Harris Bank
5	Outlook	Chase
6	Apple	Amazon
7	Adobe	Dropbox
8	AOL	DHL
9	PayPal	CNN
10	Office365	Hotmail

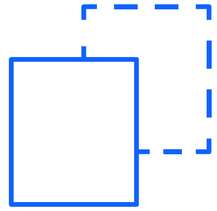
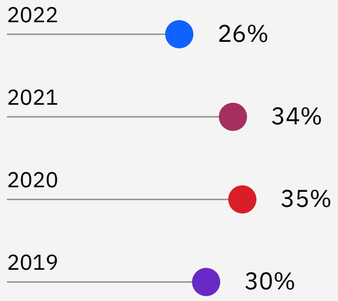


그림 3: 이 차트는 2021년과 2022년에 가장 많이 스푸핑된 브랜드를 식별하여 위협 행위자가 점점 더 대규모 기술 브랜드를 중점적으로 목표하고 있음을 보여줍니다.
출처: IBM 피싱 키트 데이터

지난 4년 간 취약성 악용으로 인해 발생한 인시던트 비율



취약성

2022년 퍼블릭 애플리케이션(T1190)의 악용으로 포착된 취약성 악용은 상위 감염 벡터 중 2위를 차지했고, 2019년부터 공격자가 선호하는 손상 방식이었습니다. 취약성은 X-Force가 2022년에 해결했던 공격의 26%에서, 2021년의 경우는 34%에서, 2020년은 35%, 2019년은 30% 에서 악용되었습니다.

위협 행위자가 악용한 모든 취약성이 사이버 인시던트로 이어지는 것은 아닙니다. 2022 년 취약성 악용으로 인해 발생한 인시던트 수는 2020년에 34% 증가한 이후로, 2021년에 비해 19%가 감소했습니다. X-Force는 2021년 말 널리 확산된 Log4J 취약성이 이러한 변화를 이끌어냈다고 평가했습니다.

액세스를 위한 악용은 X-Force Red Adversary Simulation Services 팀에서 고급 위협을 계속 시뮬레이션하기 위해 추구하는 핵심 연구 영역입니다. 팀은 액세스를 확장하고 권한 에스컬레이션을 수행하기 위해 운영체제(OS) 및 애플리케이션 악용에 대한 취약성 연구에 중점을 두었습니다. 해당 영역에 중점을 둔 이유는, 주로 기존 Active Directory 공격 경로를 강화하고 새로운 공격 경로를 추구해야 하는 오랜 고객과 함께한 과거 연습 때문이었습니다.

취약성은 일반적인 초기 액세스 벡터이고 업계는 특정 해에 몇 가지 주요 벡터에 대응하지만, 모든 취약성이 동일한 것은 아닙니다. 의사 결정권자가 취약성 환경을 전체적으로 파악하고, 주어진 취약성이 네트워크에 가하는 실제 위협을 이해하는 데 필요한 컨텍스트를 갖추는 것이 중요합니다.

약 30년 전에 일반적인 취약성 및 노출(CVE) 시스템이 등장하기 전부터 X-Force는 강력한 취약성 데이터베이스를 구축하기 시작했습니다. 이 데이터베이스는 현재 사이버 보안 업계에서 가장 포괄적인 데이터베이스 중 하나입니다. 취약성은 보안에서 주요 위험 요소이지만, 무기화되고 알려진 악용보다 보고된 취약성이 훨씬 더 많습니다. 또한, 제로 데이에 대한 관심이 높음에도 불구하고 알려진 제로 데이의 실제 수가 알려진 취약성의 총 수에 비해 작습니다.

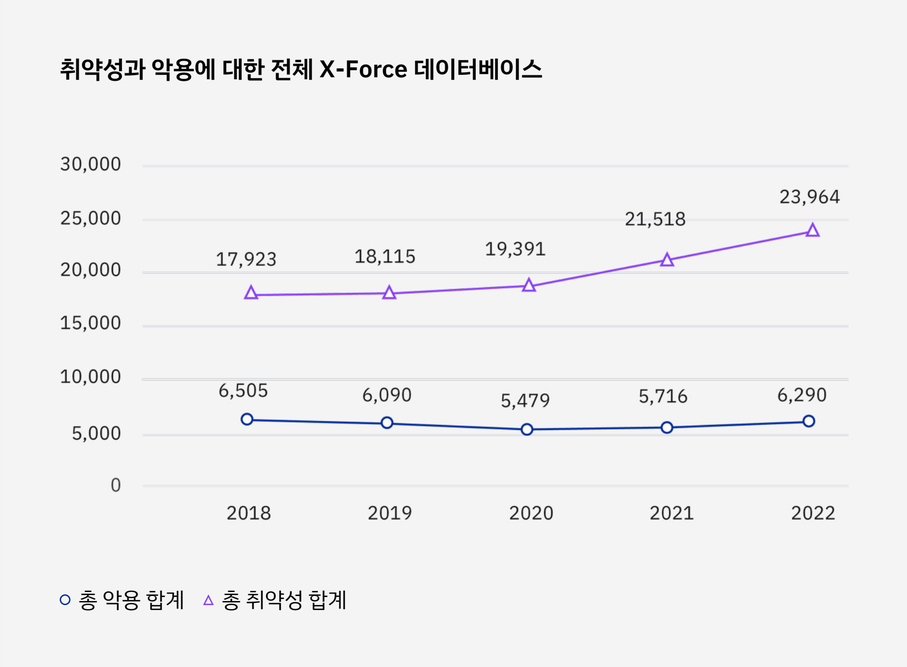


그림 4: 지난 5년 간의 취약성과 악용을 보여주는 X-Force 취약성 데이터베이스 뷰. 출처: X-Force

매년 새롭게 기록적인 수의 취약성이 발견됩니다. 2022년에 추적한 총 취약성의 수는 23,964개로, 2021년 21,518개와 비교됩니다. 매년 증가한 취약성 추세는 지난 10년 동안 지속되었습니다. 방어자의 입장에서 시행한 취약성 데이터베이스 분석은 보고된 취약성에 대한 알려진 실행 가능한 악용의 비율이 최근 몇 년간 감소했음을 보여줍니다. 2018년에는 36%, 2019년에는 34%, 2020년에는 28%, 2021년에는 27%, 2022에는 26%였습니다.

이 수치는 제로 데이의 노출과 오래된 취약성의 악용(때로는 식별된 지 몇 년 후에 발생)에 따라 바뀔 수 있으며, 이러한 감소에는 몇 가지 잠재적인 이유가 있습니다. 첫째, 공식적인 버그 바운티 프로그램을 구축하여 애플리케이션의 취약성을 사전에 발견하도록 했습니다. 이와 함께 이미 널리 알려지고 잘 구축한 취약성이 몇 가지 존재하는데 이는 공격자들의 시스템 악용 수단으로 사용되고 있으며, 이 때문에 위협 행위자는 새로운 악용 수단을 개발할 필요가 줄어 듭니다. 여러 요인으로 인해 감소했을 수 있지만, 취약성의 악용이 위협적이지 않다는 뜻은 아닙니다.

취약성 악용의 비율은 감소했지만 지난 5년 동안 X-Force가 추적한 해당 악용의 심각성은 증가했습니다. 2018년에는 취약성의 58%가 일반적인 취약성 점수 시스템(CVSS)에서 중간 점수를 기록했습니다.

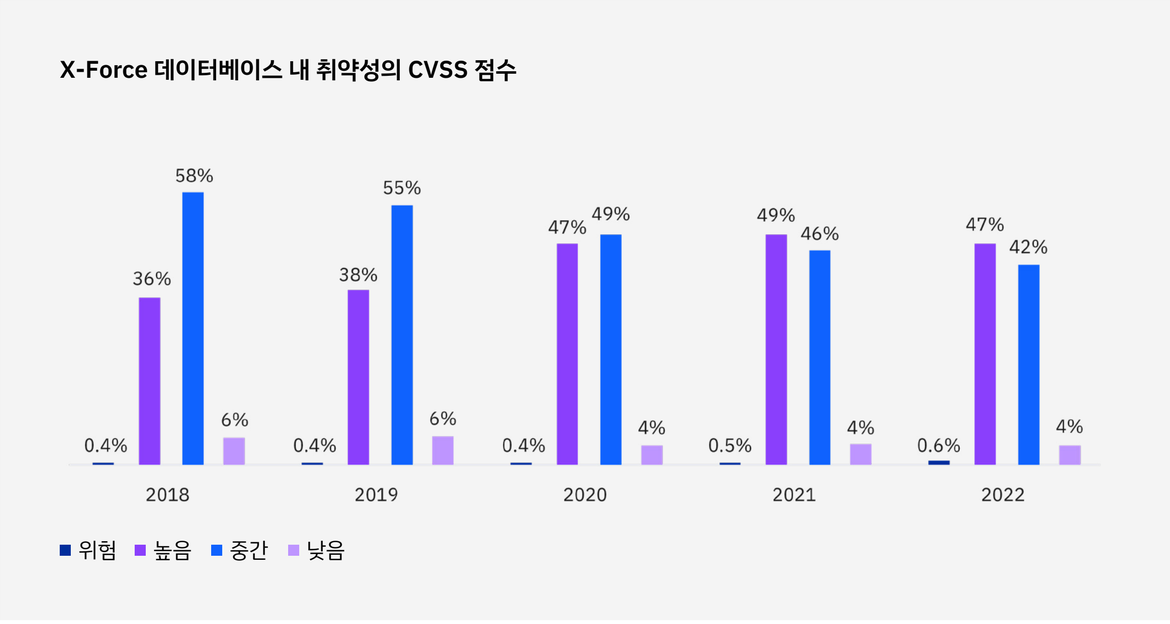


그림 5: 시스템에서 추적한 취약성의 심각도를 보여주는 X-Force 취약성 데이터베이스. 출처: X-Force

10점 만점에 4.0~6.9로 중간이었고, 36%가 조금 안 되는 7.0~9.9였습니다. 2021년에 역전된 이 두 점수의 차이와 높은 심각도의 취약성은 이제 중간 점수를 받은 취약성보다 5% 포인트 더 많습니다.

하지만 X-Force가 1988년 이후 추적한 모든 취약성 중 38%가 높은 순위를 차지했으며, 그 중 1%만이 임계 점수 10점을 받았습니다. 추적한 취약성에서 절반은 중간 등급이고 나머지 11%는 3.9 이하로 낮습니다. 악용 방법이나 악용 존재 여부를 설명하지 않기 때문에, 이러한 점수만으로는 특정 CVE의 실제 심각성과 상관관계를 찾을 수 없습니다. 하지만 해당 점수는 방어자가 취약성을 비교하고, 해결의 우선순위를 정하도록 도와줍니다. 다음 페이지의 그림 6에 나온 표는 사이버 보안 업계가 직면한 취약성 문제에서 진정한 본질을 이해하는 데 도움이 됩니다.

운영 기술(OT) 취약성

2022년에 발견된 산업용 제어 시스템(ICS) 취약성은 2021년 715개, 2020년 472개에서 2022년 457개로, 2년 만에 처음으로 감소했습니다. 이에 대한 한 가지 설명은 ICS 수명 주기와 일반적으로 관리 및 패치되는 방식에서 찾아볼 수 있습니다. 공격자는 다운타임 최소화에 대한 요구, 긴 장비 수명 주기, 지원이 잘 되지 않는 오래된 소프트웨어 로 인해 많은 ICS 구성 요소 및 OT 네트워크가 여전히 오래된 취약성의 위험에 노출되어 있음을 알고 있습니다. 인프라는 일반적으로 표준 사무실 워크스테이션보다 몇 년 더 오래 유지되므로 IT가 악용될 수 있는 취약성 이상으로 ICS 관련 취약성의 수명이 연장됩니다.

취약성 문제

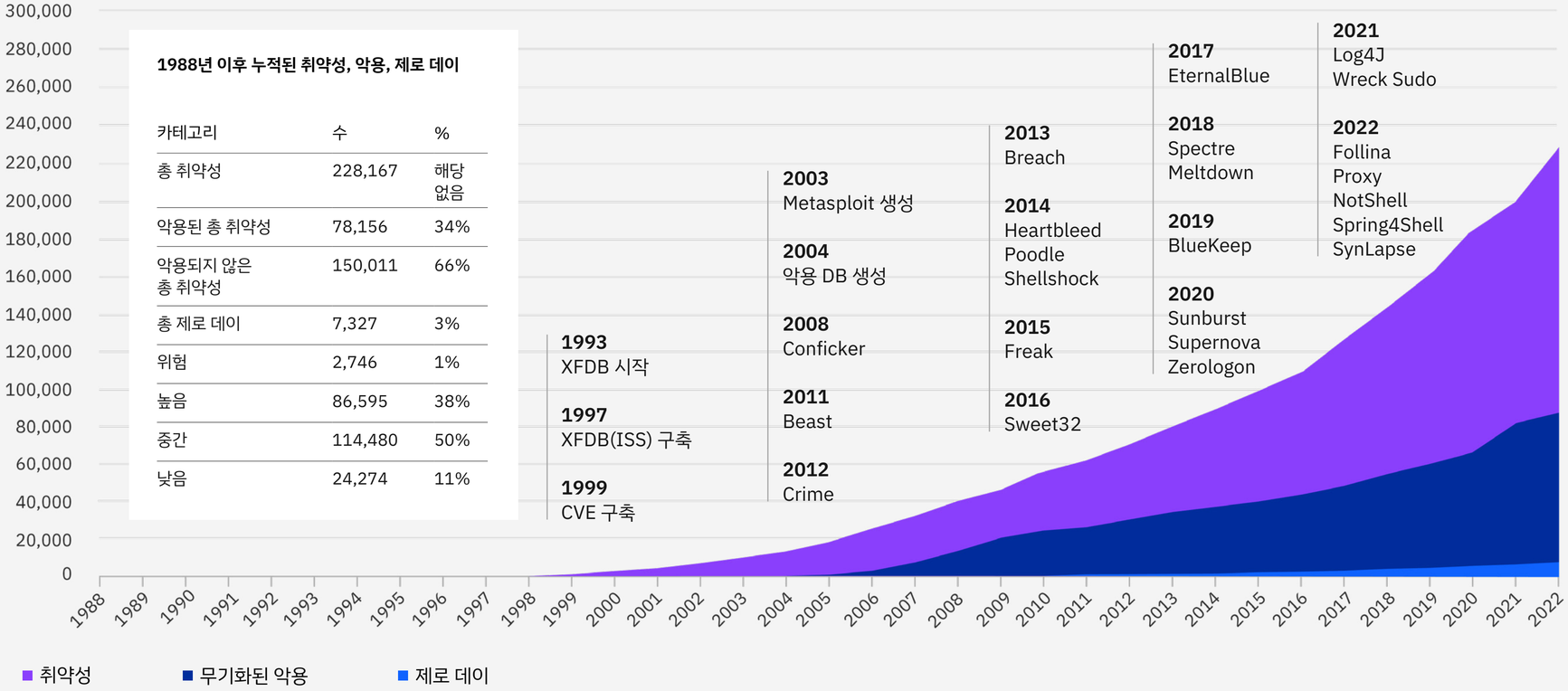


그림 6: 1988년 이후 취약성, 악용, 제로 데이의 증가를 보여주는 표입니다. 1933년 이후 취약성과 관련된 주요 이벤트의 타임라인도 포함되어 있습니다. XFDB는 X-Force 데이터베이스 및 악용을 의미하며 DB는 악용 데이터베이스를 의미합니다. 출처: X-Force

목표에 대한 주요 조치

이전에는 X-Force 위협 인텔리전스 인덱스에서 가장 많았던 공격 범주를 광범위하게 조사했습니다. 2022년에 X-Force는 이 분류를 다음의 두 가지 범주로 분석했습니다. 위협 행위자가 피해자 네트워크에서 취한 특정 조치 또는 목표를 갖고 행한 악의적 조치, 그리고 해당 조치가 피해자 또는 영향에 대해 의도하거나 실현한 효과입니다.

X-Force Incident Response 데이터에 따르면 백도어 배포는 목표에 적용된 가장 일반적인 조치였으며 보고된 모든 인시던트 중 21%에서 발생했습니다. 랜섬웨어가 17%, 비즈니스 이메일 손상(BEC)이 6%로 그 뒤를 이었습니다. 악성 문서(maldocs), 스팸 캠페인, 원격 액세스 툴 , 서버 액세스가 각 사례의 5%에서 발견되었습니다.

2022년 목표에 가장 많이 적용된 조치

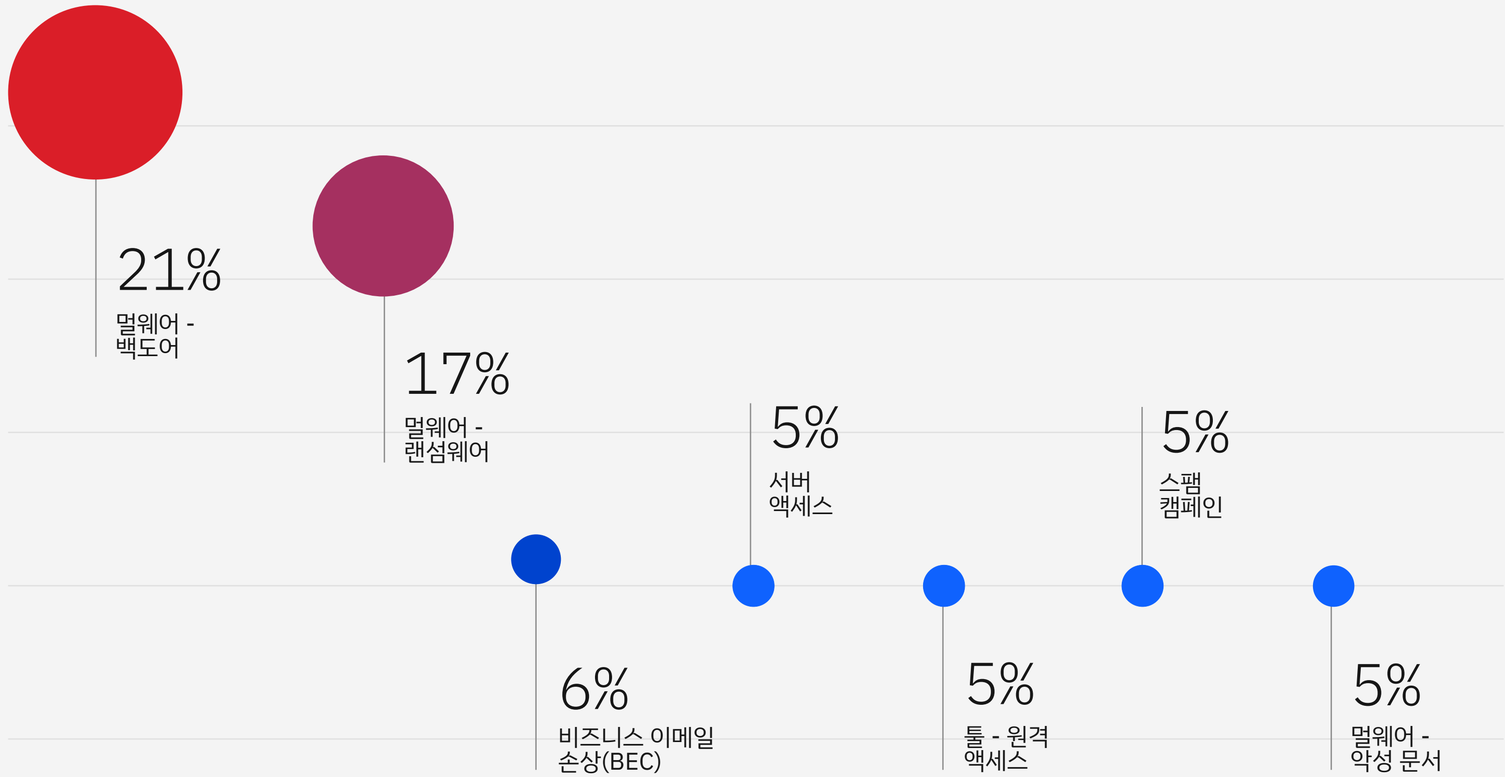


그림 7: 2022년 X-Force에서 관찰된, 목표에 가장 많이 적용된 조치. 출처: X-Force

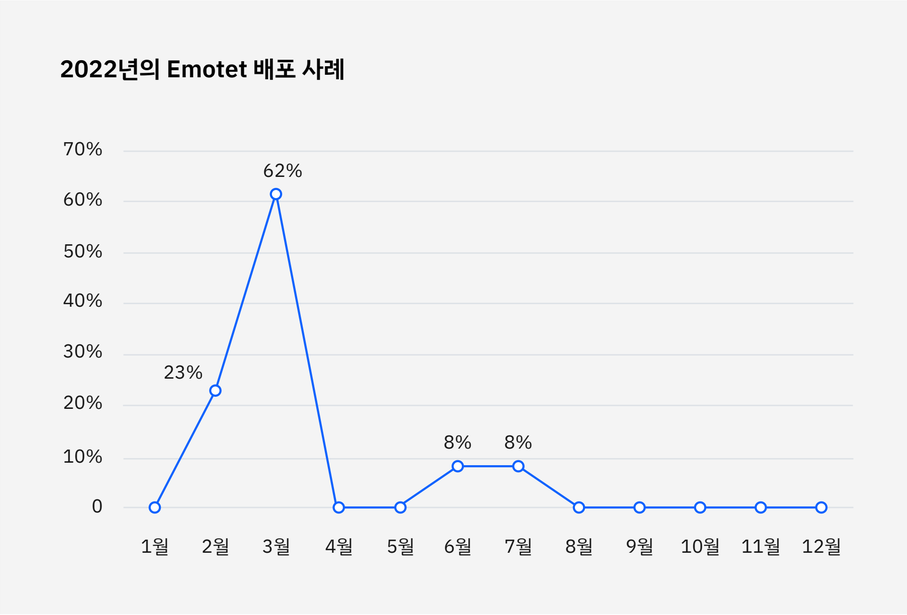


그림 8: 2022년 초의 Emotet 사례 증가를 보여주는 그래프. 출처: X-Force

백도어 배포가 목표에 따른 조치로 분류된 경우, 백도어가 운영될 때 위협 행위자가 추가 계획을 세웠을 가능성이 있습니다. 보안 팀이나 인시던트 대응 담당자가 성공적으로 개입하면 위협 행위자가 추가 목표를 달성하지 못할 수 있습니다. 이처럼 악의적인 추가 활동에는 랜섬웨어가 포함되었을 가능성이 높습니다. 해당 백도어 사례의 약 2/3에 랜섬웨어 공격 흔적이 있었기 때문입니다.

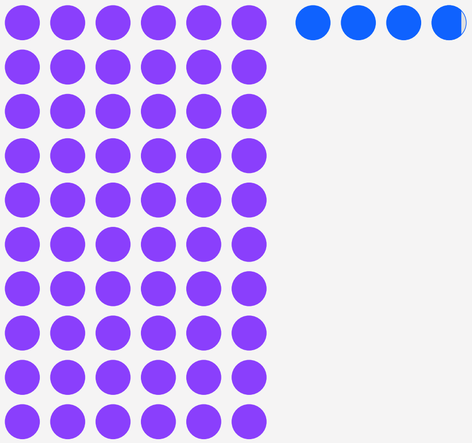
백도어 배포가 증가함에 따라 이러한 종류의 액세스로 다크 웹에서 창출할 수 있는 수익이 발생할 수도 있습니다. 초기 액세스 브로커의 손상된 기업 네트워크 액세스는 일반적으로 수천 달러를 벌어 들입니다. 우회적으로 이동하고 고가치 데이터를 유출하는 동시에 액세스를 유지하는 문제를 피함으로써 신속하게 이익을 창출하고자 하는 악의적인 행위자는 이러한 유형의 액세스를 찾아 나설 수도 있습니다. 이러한 악의적인 행위자는 액세스 권한을 설정하기 위해 필요한 멀웨어에 액세스 권한이 없다면 백도어를 찾아 나설 수도 있습니다.

초기 액세스 브로커는 일반적으로 액세스 경매를 시도합니다. X-Force가 확인한 바에 따르면 5천~1만 달러였으며 최종 가격은 이보다 적을 수도 있습니다. 2천~4천 달러에 판매되는 액세스가 보고되기도 했으며, 그 중 하나는 5만 달러까지도 도달하기도 했습니다. 이러한 금액은 미화 10달러 이하로 제공되는 단일 신용카드와 같은 조건의 훨씬 낮은 가격과 비교됩니다.

백도어로 인해 2~3월에 Emotet 사례가 눈에 띄게 급증했습니다. 이 때문에 백도어 사례의 순위가 과도하게 부풀려졌습니다. 이 기간에 배포된 사례가 2022년에 전 세계적으로 확인된 모든 백도어의 47%를 차지하기 때문입니다. 7월부터 11월까지 Emotet의 활동이 중단된 후, 거의 2주 동안 훨씬 낮은 양으로만 조금씩 증가하면서 백도어 사례 수는 크게 감소했습니다.

랜섬웨어 공격 평균 지속 기간

2019	2021
2개월 이상	3일 이상



랜섬웨어

수많은 랜섬웨어 신디케이트로 혼란스러운 한 해를 보냈음에도 불구하고, 랜섬웨어는 백도어 배포에 이어 두 번째로 흔한, 조직의 운영을 지속적으로 방해하는 조치였습니다. 인시던트에서 랜섬웨어의 점유율은 2021년 21%에서 2022년 17%로 감소했습니다.

IBM Security X-Force 연구에 따르면 2019~2021년 랜섬웨어 공격의 평균 지속 시간이 2개월 이상에서 4일 미만으로, 94.34% 감소했습니다. 그럼에도 불구하고 랜섬웨어는 명확히 존재하는 위험으로써, 계속 증가하고 있는 것으로 보입니다.

특히 랜섬웨어 운영자가 페이로드를 배포하여 피해를 줄 수 있는 한 가지 방법은 도메인 컨트롤러를 손상시키는 것입니다. X-Force Red의 네트워크 침투 테스트 결과를 통해, 4%의 적은 비율에 해당하긴 하지만 Active Directory에서 오류 구성을 지닌 엔티티가 나타나 권한 상승 또는 전체 도메인 테이크오버에 개방될 수 있음이 밝혀졌습니다. 2022년에 X-Force는 ESXi 및 Hyper-V 등 기본 인프라에 대한 더욱 공격적인 랜섬웨어 공격도 발견했습니다. 이러한 공격 방법이 잠재적으로 갖고 있는 큰 영향은 도메인 컨트롤러 및 하이퍼바이저를 적절하게 보호하는 것의 중요성을 강조합니다.

랜섬웨어 변종

랜섬웨어 그룹 및 관련 액세스 브로커가 등장하고 사라짐에 따라, X-Force는 이 공간에서 활동하는 상위 그룹에서 이탈이 주기적으로 발생하는 것을 목격했습니다. X-Force는 2022년 랜섬웨어 변종을 19개 발견했으며, 이는 2021년 16개와 비교됩니다. LockBit 변종은 관찰된 총 랜섬웨어 인시던트의 17%를 차지했으며, 이는 2021년의 7%에서 증가한 것입니다. Phobos는 11%로 WannaCry와 공동으로 2위를 했습니다. 2022년의 상위 그룹은 2021년의 1위 REvil(또는 Sodinokibi)을 대체하며 2021년 사례의 37%와, 13%였던 2위 Ryuk을 각각 3%로 줄였습니다.

LockBit 3.0은 LockBit 랜섬웨어 제품군의 최신 변종이며 이는 LockerGoga 및 MegaCortex와 관련된 서비스형 랜섬웨어(RaaS) 작업의 일부입니다. LockBit은 2019년 9월부터 운영 중이며 LockBit 3.0은 2022년에 출시되었습니다. LockBit 3.0 소스 코드의 상당 부분이 BlackMatter 랜섬웨어에서 차용된 것으로 보입니다.

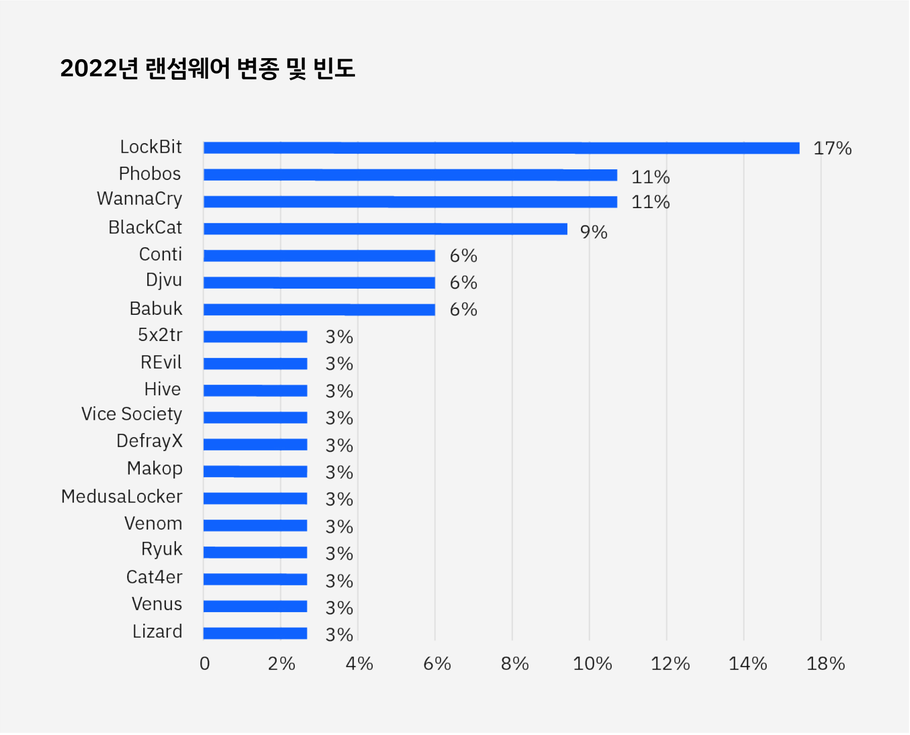


그림 9: 랜섬웨어 변종과, 랜섬웨어 변종이 2022년 X-Force Incident Response와관련하여 관찰된 빈도입니다. 출처: X-Force

연구원들은 2019년 초에 처음으로 Phobos 랜섬웨어를 발견했습니다. Phobos는 코드, 전달 메커니즘, 악용 기술 및 랜섬 노트의 유사성을 기반으로 이전에 알려진 랜섬웨어 계열인 Crysis 및 Dharma의 분기로 식별되었습니다. Phobos는 일반적으로 랜섬 요구가 낮은 소규모 공격에 사용되었습니다. 이메일 피싱 캠페인과 취약한 원격 데스크톱 프로토콜(RDP) 포트의 악용은 Phobos에서 관찰되는 주요 배포 방식입니다.

2017년 처음 발견된 WannaCry는 EternalBlue를 사용하여 Microsoft SMBv1(Server Message Block 1.0) 서버 (MS17-010)의 취약성을 악용하여 자체 확산됩니다. X-Force가 2022년에 발견한 WannaCry 또는 Ryuk의 몇 가지 사례는 3~5년 전 감염의 결과였으며 패치되지 않은 오래된 장비에서 발생했고, 따라서 이벤트 이후 적절한 정리의 중요성을 일깨웠습니다.

비즈니스 이메일 손상(BEC)

BEC는 X-Force에서 대응한 인시던트의 6%를 차지하며 2022년 3위에 올랐습니다. 이는 2021년의 공격 8%, 2020년의 5위에 해당하던 9%보다 약간 낮은 수치입니다. 서버 액세스 공격이었던 2021년 2위 공격을 대체했습니다. 이러한 유형의 공격은 공격자가 알 수 없는 최종 목표를 위해 서버에 대한 액세스 권한을 얻을 때 발생하며, 이는 2022년에 해당 행위자가 달성한 액세스 유형에 따라 더 세분화되었습니다. X-Force가 대응한 BEC 사례 중 절반에서 스피어 피싱 링크가 사용되었습니다. 악의적인 첨부 파일 및 유효한 계정의 남용을 사용해 각각 25%의 사례에서 BEC 시도를 가능하게 했습니다.

06

주요 영향

또한, X-Force는 X-Force가 대응했던, 피해 조직에 대한 인시던트의 효과를 면밀히 조사하여 위협 행위자가 얻고자 했던 영향을 잘 이해하고자 했습니다. 조직은 이 정보를 통해 가장 일반적인 영향을 더 잘 이해하여 잠재적인 향후 인시던트에 대한 대응을 보다 효과적으로 계획할 수 있습니다.

분석을 통해 4건 중 1건 이상의 인시던트가 피해 조직을 갈취하려고 했으며, 갈취는 X-Force가 해결한 인시던트에서 관찰된 가장 큰 영향입니다. 관찰된 갈취 사례는 랜섬웨어 또는 BEC를 통해 가장 빈번하게 발생했으며, 원격 액세스 도구, 크립토마이너, 백도어, 다운로더 및 웹 셸의 사용을 포함하는 경우가 많았습니다.

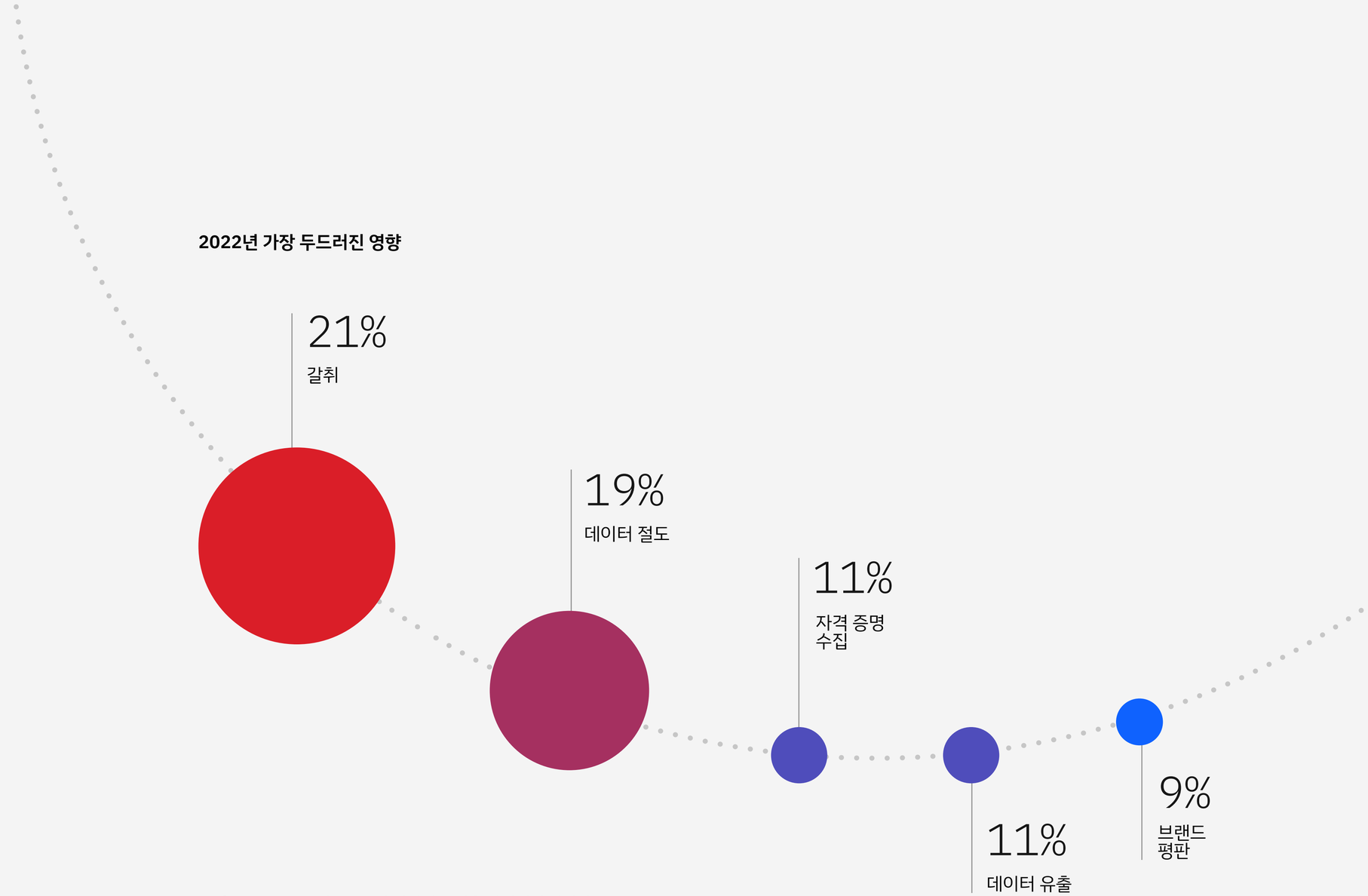


그림 10: X-Force가 2022년 인시던트 대응 참여에서 관찰한 가장 두드러진 영향입니다. 출처: X-Force

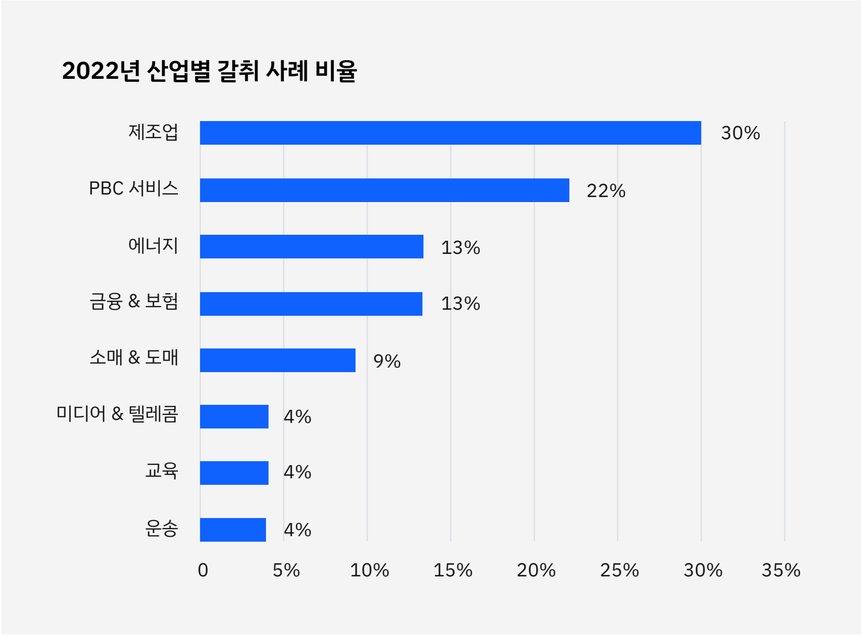


그림 11: 2022년 인시던트 대응 참여에서 X-Force가 관찰한 산업별 갈취 사례의 비율입니다. 반올림을 하더라도 100%가 넘지는 않습니다. 출처: X-Force

데이터 절도는 2위로 X-Force가 해결한 모든 인시던트 중 19%를 차지했습니다. 사용자 이름과 암호를 도용하고 해당 완화 조치가 필요했던 자격 증명 수집은 11%를 차지했습니다. X-Force가 도난당한 후 실제로 유출된 목표 정보를 식별할 수 있는 인시던트는 11%의 데이터 도난에 비해 흔치 않았습니다. 클라이언트가 고객에게 제공하는 서비스 중단과 같은 브랜드 평판에 대한 영향은 인시던트의 9%를 차지했습니다. X-Force가 추적한 영향의 전체 목록은 부록을 참조하세요. 피해 브랜드 평판에 영향을 준 인시던트는 주로 배포된 서비스 거부 (DDoS) 공격이었으며, 이는 또한 피해자가 돈을 지불해 공격을 멈추게 하도록 갈취하는 데 자주 사용됩니다.

주목할 만한 온라인 갈취의 전개[1-9]

연도	사건	전략
2013	Cryptolocker—최초의 주요 랜섬웨어 발생 중 하나	데이터 암호화
2014	DDoS 4 Bitcoin, Armada Collective	랜섬 DDoS
2015	Chimera 랜섬웨어로 인한 도난 데이터 온라인 유출 위협 증가	이중 갈취
2017~2018	BitPaymer 및 SamSam	빅 게임 헌팅
2020	Vastaamo 랜섬웨어 사례	삼중 갈취

갈취

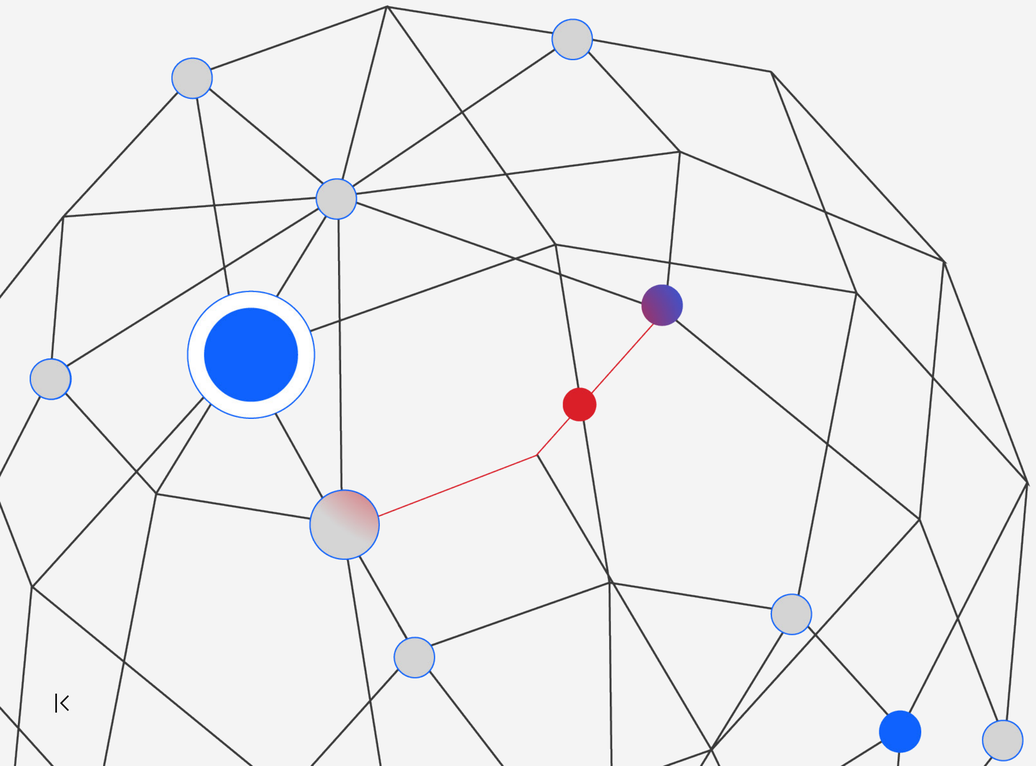
갈취는 오늘날 랜섬웨어와 가장 일반적으로 연관되어 있지만 갈취 캠페인에는 목표물에 압력을 가하는 다양한 방법이 포함되었습니다. 여기에는 DDoS 위협, 데이터 암호화, 그리고 보다 최근에는 이전에 보았던 여러 요소를 결합한 이중 및 삼중 갈취 위협이 포함됩니다.

적어도 하나의 랜섬웨어 그룹이 2022년부터 실험한 또 다른 전략은, 그들이 훔친 데이터에 하위 피해자가 더 쉽게 접근할 수 있도록 하는 것이었습니다. 운영자는 간접적인 피해자가 데이터 유출 중에 자신의 데이터를 쉽게 식별하도록 함으로써 애초에 랜섬웨어 그룹이나 계열사가 표적으로 삼은 조직에 대한 후속 압력을 늘리려고 합니다. 2023년에 X-Force는 침입에 대한 잠재적인 법적 비용 및 평판 비용을 증가시키기 위해 강화되거나 새로운 다운스트림 피해자 알림을 실험하는 위협 행위자를 볼 것으로 예상합니다.

사이버 공격의 방어자와 피해자 모두 위협 행위자가 조직에 미치는 영향을 관찰하는 데 중점을 두는 경우가 많습니다. 그러나 위협 행위자의 의도, 이들의 능력, 시간에 따른 진화 방식을 고려하는 것이 중요합니다. 이 접근 방식을 통해 차세대 기능 진화가 무엇인지를 더 잘 알아볼 수 있습니다. 계속 확장되는 갈취 옵션 메뉴와 금전적 이익이라는 랜섬웨어 행위자의 주요 목표를 고려할 때 X-Force 팀은 위협 행위자가 계속해서 진화하고 갈취 방법을 확장하여 피해자에게 돈을 지불하도록 압력을 가할 새로운 방법을 찾을 것이라고 평가합니다.

07

우크라이나의 러시아 전쟁에서 사용된 사이버 관련 개발



이 문서 발행 시점을 기준으로, 러시아가 우크라이나를 침공한 이후 러시아 정부가 후원하는 사이버 활동은 원래 서방 정부 기관들이 두려워했던 광범위하고 영향력이 큰 공격으로 이어지지 않았습니다. 그러나 러시아는 우크라이나의 목표물에 전례 없던 개수의 와이퍼를 배치하여 파괴적인 멀웨어 기능에 지속된 투자를 강조했습니다. 또한 이번 침공으로 인해 양측에 동조하는 그룹이 수행하는 핵티비스트 활동이 다시 떠오르고, 동유럽 사이버 범죄 환경이 재편되었습니다.

2015년 이후 중요 인프라 사이버 공격에 대해 입증된 러시아의 고급 기능을 고려하여, 국제 사이버 보안 기관에서 2022년 4월 경고를 발표했습니다. 이 경고는 잠재적으로 중요한 사이버 작업과 우크라이나 및 기타 지역의 관련 중단을 언급했습니다. X-Force는 핵티비즘과 와이퍼 멀웨어의 부활, 사이버 범죄 세계의 중대한 변화 등 가장 중요하게 떠오르는 위협을 평가했습니다. 이러한 작업의 대부분은 우크라이나, 러시아 및 주변 국가를 중심으로 하는 기관을 희생시켰지만 일부는 다른 지역으로도 퍼졌습니다.

한편, 방어자는 지난 몇 년에 걸쳐 개발된 탐지, 대응 및 정보 공유의 진보를 능숙하게 활용하고 있습니다. 초기에 시도된 많은 와이퍼 공격이 신속하게 식별, 분석, 공개되었습니다. 이러한 공격에는 최소 8개의 확인된 와이퍼와 2022년 4월 우크라이나의 전력망에 대해 러시아가 계획한 사이버 공격 발견 및 중단이 포함됩니다.

사이버 공간에서 가장 널리 느껴지는 현 전쟁의 영향력은 우크라이나 또는 러시아의 국익을 지원하기 위해 활동하는 자칭 핵티비스트 그룹이 제공하고 있습니다. 러시아 침공 이후 많은 그룹이 형성되어 정치적 주장을 펼치기 위해 러시아와 우크라이나 네트워크에 모두 맞서 활동하고 있지만, Killnet은 가장 왕성한 러시아 동조 그룹 중 하나입니다. 북대서양 조약기구(NATO) 회원국, 유럽의 동맹국, 일본, 미국에 기반을 둔 공공 서비스, 정부 부처, 공항, 은행, 에너지 회사에 대한 디도스(DDoS) 공격을 주장했습니다. Killnet의 대상 프로필에 맞는 기관은 디도스 완화 외부 제공업체의 서비스 참여 등 디도스 완화 조치가 준비되어 있는지 확인해야 합니다.

2022년 선별된 핵티비스트 이벤트 타임라인

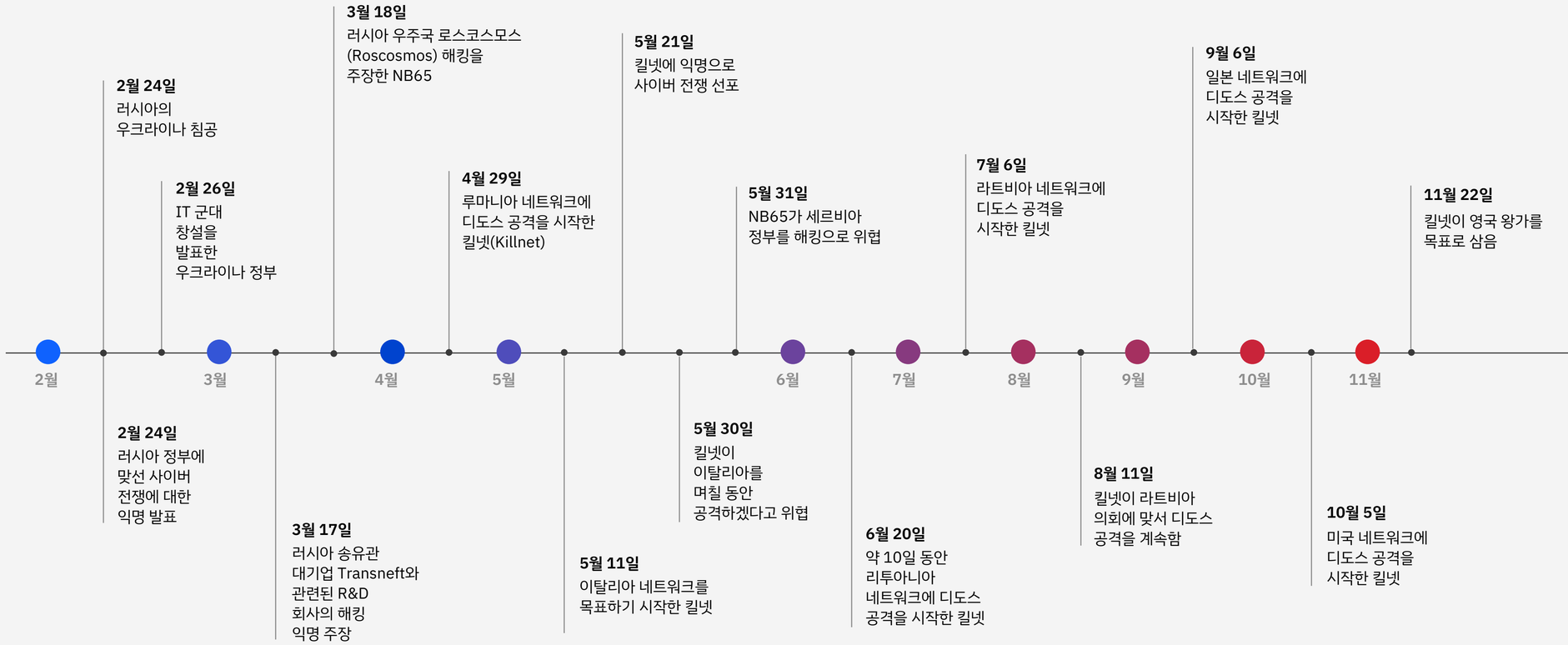


그림 12: 우크라이나 분쟁 중에 현재까지 관찰된 핵티비스트 사건을 보여주는 이미지입니다.
출처: 오픈 소스 보고에 대한 X-Force 분석

우크라이나 러시아 전쟁에서 사용된 와이퍼

러시아의 우크라이나 전쟁은 이전에는 볼 수 없었던 규모로 여러 대상에 대해 여러 와이퍼 제품군을 빠르게 연속으로 사용하고, 역동적인 군사 작전과 함께 멀웨어를 사용한다는 점이 두드러집니다.

이러한 배포에는 최소 9개의 새로운 와이퍼가 포함됩니다(AcidRain, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, AwfulShred, OrcShred and SoloShred). 이러한 와이퍼는 주로 초기 침공 이전부터 전쟁 초기 단계까지, 특히 2022년 1월부터 3월까지 우크라이나 네트워크에 사용되었습니다. 와이퍼는 과거부터 사용되었지만 대부분 제한된 대상 세트에 대한 독립 실행형 캠페인이었습니다. 그러나 WannaCry 및 NotPetya의 주목할 만한 예외는 초기 피해자에게 영향을 미친 후 무차별적으로 확산되었으며, 이러한 와이퍼가 더 광범위하게 확산되거나 다른 곳에서 악의적인 작업을 하는 데 쓰일 수 있다는 우려를 불러 일으킵니다.

X-Force는 계속해서 러시아 정부가 후원하는 사이버 위협 행위자가 여전히 전 세계의 컴퓨터 네트워크와 중요 인프라에 심각한 위협을 가하고 있다고 평가합니다. 이러한 판단은 러시아가 우크라이나, 유럽, NATO 및 미국 네트워크를 대상으로 오랫동안 유지해온 사이버 작전과 2015년 이후 러시아 위협 그룹이 수행한 공격 작전을 기반으로 합니다.

우크라이나 러시아 전쟁에서 사용된 사이버 관련 전개

러시아 사이버 범죄 그룹의 격변

2022년은 ITG23에게 격동의 한 해였습니다. ITG23은 가장 유명한 러시아 사이버 범죄 신디케이트 중 하나이며, 주로 Trickbot 뱅킹 트로이 목마 및 Conti 랜섬웨어를 개발한 것으로 알려져 있습니다. 이 그룹은 러시아의 전쟁 개입을 공개적으로 지지한 후, 2022년에 일련의 중요 정보 유출을 겪었습니다. ContiLeaks 및 TrickLeaks는 수천 개의 채팅 메시지와 수많은 그룹 구성원의 신상을 공개했습니다. X-Force는 ITG23이 2022년 4월 중순부터 적어도 6월 중순까지 체계적인 공격을 시작했음을 나타내는 증거를 발견했습니다. 이 그룹은 이전에 우크라이나를 표적으로 둔 적이 없었기 때문에 전례 없는 변화였습니다.

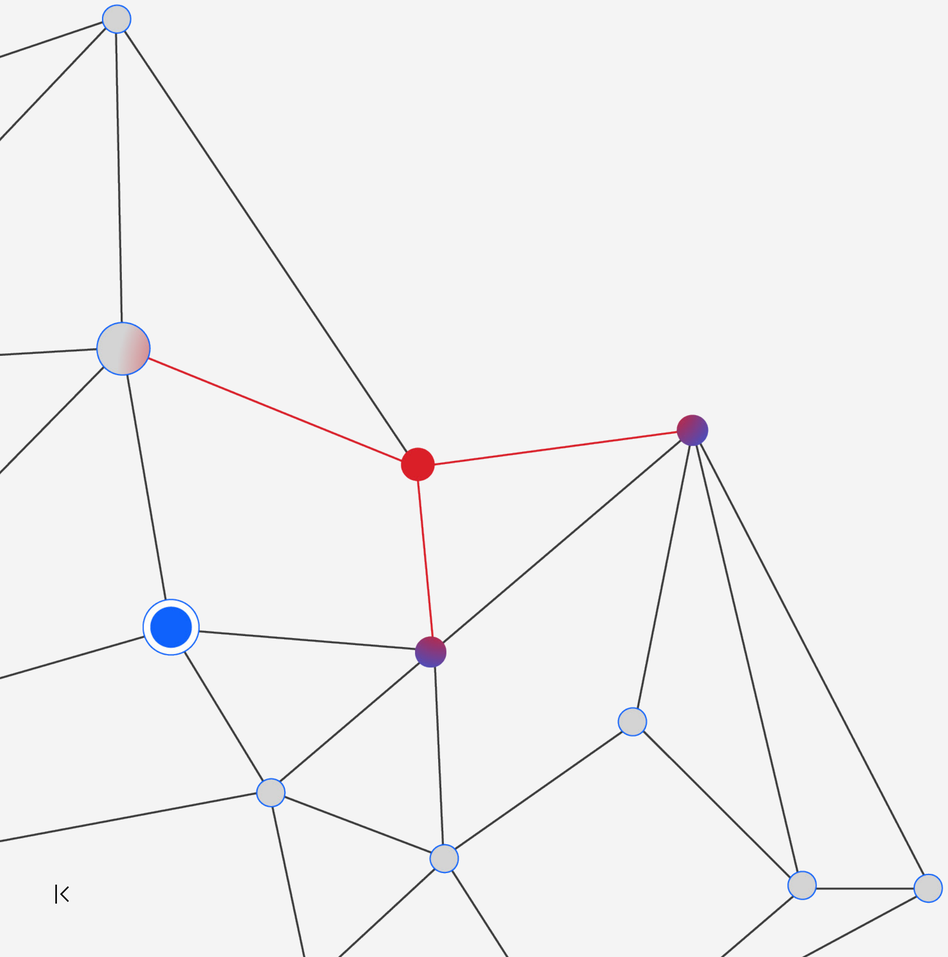
또한, 이 그룹은 가장 유명한 멀웨어 제품군 2가지, Trickbot과 Bazar를 폐기하고 Conti 랜섬웨어 작업을 종료한 것으로 보입니다. 여러 보고서에서 그룹이 여러 부분으로 나뉘고, 일부 구성원이 완전히 이동하는 등 상당한 인력 개편이 발생할 수 있다고 제시했습니다.

2021년 상당한 수의 감염을 일으킨 Trickbot 및 Bazar가 종료되면서 생긴 공백은 Emotet, IcedID, Qakbot, Bumblebee와 같은 멀웨어 제품군으로 빠르게 채워졌습니다. ITG23은 종료되기 전에 여전히 Conti 랜섬웨어를 대량으로 배포하고 있었으며 2022년 1분기에 X-Force가 대응한 모든 랜섬웨어 참여에서 3분의 1을 차지했습니다.

이 그룹은 기존에 중요 대상에 배포했던 은밀한 백도어인 Anchor 멀웨어의 새 버전을 출시하기도 했습니다. X-Force에서 발견한 AnchorMail이라는 업그레이드 버전에는 새로운 이메일 기반 명령 및 제어(C2) 통신 메커니즘이 있습니다. C2 서버는 SMTPS(Simple Mail Transfer Protocol Secure) 및 IMPS(Internet Message Access Protocol Secure) 프로토콜을 사용하며, 멀웨어는 특수하게 조작된 이메일 메시지를 주고받으며 서버와 통신합니다.

08

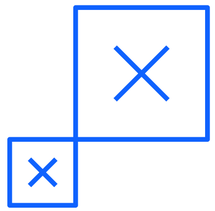
멀웨어 환경



USB 확산 웜 증가

X-Force가 2022년 5월 중순 조직에 영향을 미치는 Raspberry Robin 감염 시도를 관찰한 후, 범용 직렬 버스(USB) 장치를 공유하는 사용자로부터 수수께끼 웜이 피해자의 네트워크에서 빠르게 확산되기 시작했습니다. 6월 초에 감염이 급증했고, 8월 초에는 Raspberry Robin이 X-Force가 관찰한 감염 시도의 17%에 이르며 최고조에 달했습니다. 이러한 최고 수치는 석유 및 가스, 제조, 운송 업계에서 확인되었습니다. 이러한 업계에서 17%의 감염 시도율은 중요합니다. 전체X-Force 클라이언트에서 동일한 멀웨어 유형을 본 것은 1% 미만이기 때문입니다. 또한, X-Force는 2022년 9월부터 11월까지 Raspberry Robin 활동을 더 많이 관찰했습니다.

USB 기반 웜은 소셜 엔지니어링을 통해 확산할 수 있으며, 합법적인 사용자 또는 다른 수단을 통해 성공적으로 감염시키려면 네트워크 또는 엔드포인트에 대한 물리적 액세스가 필요합니다. X-Force는 보안 툴을 통해 알려진 USB 기반 멀웨어를 차단하고 보안 인식 교육을 구현하며 모든 이동식 미디어에 대한 자동 실행 기능을 비활성화할 것을 권장합니다. OT처럼 특히 민감한 환경이나 에어 갭이 존재하는 환경에서는 단지 USB 플래시 드라이브의 사용을 아예 금지하는 것이 가장 안전합니다. 이를 허용해야 하는 경우, 이전의 제안 사항을 구현하는 것 외에도 환경에서 사용이 승인된 휴대용 장치의 수를 엄격하게 제어해야 합니다.



떠오르는 Rust

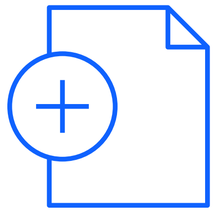
Rust 프로그래밍 언어는 교차 플랫폼 지원과, 보다 흔한 다른 언어에 비해 낮은 바이러스 백신 탐지율 덕분에 2022년 멀웨어 개발자들 사이에서 꾸준히 인기가 늘었습니다. Go 언어와 유사하게, 더 복잡한 컴파일 프로세스에서 얻는 이점도 있습니다. 이 프로세스의 경우 리버스 엔지니어가 멀웨어를 분석하는 데 더 시간이 많이 걸릴 수 있습니다. 일부 랜섬웨어 개발자는 BlackCat, Hive, Zeon 및 가장 최근의 RansomExx를 비롯한 Rust 버전의 멀웨어를 출시했습니다. 또한, X-Force는 Rust로 작성된 ITG23 크립터와 CargoBay 백도어 및 다운로더 제품군을 분석했습니다. Rust의 인기가 높아지면서 랜섬웨어 에코시스템 전반에서 탐지를 피하기 위한 혁신에 지속적으로 집중하고 있다는 사실이 드러났습니다.

Vidar InfoStealer

X-Force는 2022년 6월에 시작되어 2023년 초까지 지속된 Vidar InfoStealer 멀웨어의 갑작스러운 유입을 주목했습니다. 2018년에 처음 관찰된 Vidar는 서비스로서의 멀웨어(MaaS)로 배포되는 악성 정보 탈취 트로이 목마입니다. 트로이 목마는 주로 사용자가 악성 스팸(malspam) 링크나 첨부 파일을 클릭할 때 실행됩니다. Vidar의 광범위한 기능 세트 덕분에 신용카드 정보, 사용자 이름, 암호, 파일 등 다양한 장치 정보를 검색하고, 사용자 데스크탑의 스크린샷을 찍을 수 있습니다. 또한, Vidar는 비트코인 및 이더리움 암호화폐 지갑을 훔칠 수 있습니다.

일반적으로 정보 도용자를 통해 공격할 때는 금전적 동기가 있습니다. 절도 데이터를 분석하고 중요한 정보는 수집하여 데이터베이스에 정리합니다. 이 데이터베이스는 다크 웹이나 개인 메시징 앱인 Telegram에서 판매할 수 있습니다. 위협 행위자는 이 정보를 사용하여 은행 대출 또는 신용카드 신청, 온라인으로 상품 구매 또는 사기성 건강 보험 청구와 같은 다양한 유형의 사기를 행할 수 있습니다.

위협 행위자는 손상된 로그인 자격 증명을 사용하여 회사 계정 및 원격 서비스에 액세스 권한을 확보할 수 있습니다. 정보 도용자를 사용하려면 월 평균 약 250달러의 비용이 들며, 사용자가 원하는 대로 멀웨어를 선택해 배포할 수 있습니다. X-Force는 주기적으로 마켓플레이스를 확인하며 정보 도용 멀웨어가 캡처한 액세스 권한을 미화 10~75달러에 판매하고자 시도합니다. 액세스 권한을 확보하면 위협 행위자가 손쉽게 해킹된 계정의 권한을 시작점으로 사용하여 더 많은 악성 활동을 시작할 수 있습니다.



멀웨어 전달 메커니즘의 진화

피싱 이메일에 첨부된 악성 Microsoft Office 문서를 통해 멀웨어가 전달되는 일이 점점 일반화되고 있습니다. 멀웨어 개발자는 문서가 열릴 때 멀웨어를 실행하도록 설계된 악성 매크로가 포함된 문서를 만들었습니다. 이러한 목적으로 매크로를 사용하는 것이 널리 퍼지자 Microsoft Office 제품에서는 매크로 사용 문서를 열 때 보안 경고를 표시하기 시작했습니다. 2022년 7월부터 Microsoft는 이메일 또는 인터넷을 통해 받은 문서에서 매크로 실행을 기본으로 차단하기 시작했습니다.

방어자가 탐지 및 방지 기능을 강화하자, 공격자는 VBA(Visual Basic Application)에서 매크로 4.0으로 알려진 Microsoft Excel 내 기존 매크로 형식으로 이동하기 시작했습니다. 한동안 악성 Excel 문서가 사용되었습니다. 하지만 Excel 문서 내 VBA 매크로를 중심으로 대부분의 보안 메커니즘이 구축되었습니다. 한동안 Excel Macro 4.0 매크로는 탐지를 회피하는 좋은 수단을 제공했습니다. 같은 시기에 일부 공격자는 악성 문서를 이메일 첨부 파일로 보내는 대신, 이메일 안에 링크를 보내 피해자를 드로퍼 사이트로 유도하여 악성 문서를 다운로드하게 했습니다. Microsoft가 설정을 변경하여 관리자가 Macro 4.0을 비활성화하고 인터넷에서 다운로드한 매크로의 실행을 차단할 수 있게 되면서 공격자는 전략을 다시 바꿔야 했습니다.

Microsoft의 변경 사항 이후에도 많은 멀웨어 작성자는 계속 매크로가 활성화되어 있는 Microsoft Office 문서를 사용하지만, 정교한 그룹은 더 섬세하고 복잡한 감염 체인을 채택했습니다. 이러한 최신 전략에는 바이너리가 포함된 HTML 파일이나 암호로 보호된 압축 파일의 조합이 포함됩니다. 이러한 파일에는 ISO 이미지도 포함되어 있으며 여기에는 LNK 파일, CMD 파일 또는 이메일 수신자에게 보내거나 인터넷에서 다운로드할 가능성이 없는 기타 파일 유형이 포함될 수 있습니다.

그 외로는 원격 템플릿 주입 또는 취약성 악용이 포함됩니다. Microsoft HTML(MSHTML)의 원격 코드 실행 취약성인 CVE-2021-40444는 매크로에 의존하지 않고 소프트웨어 구성 요소를 사용하여 Microsoft Windows에서 웹 페이지를 렌더링하여 멀웨어를 실행하는 한 가지 예입니다.

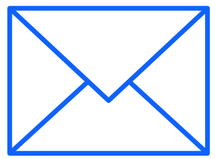
스팸 데이터는 랜섬웨어 위협을 강조하고 매크로 트렌드를 더 보여줍니다.

X-Force는 피싱 및 스팸 이메일 트렌드를 분석하여 그것의 전반적인 효율성과 위협 행위자의 사용 방식을 보다 효과적으로 파악했습니다. 조사를 통해 스팸 이메일이 Emotet, Qakbot, IcedID, Bumblebee 등의 멀웨어를 전달하기 위해 1년 내내 주기적으로 사용되었으며 종종 랜섬웨어 감염으로 이어졌다는 사실을 알 수 있었습니다.

멀웨어[10-18]	**랜섬웨어**
Trickbot	*Conti*
Bazarloader	*Conti*, Diavol
IcedID	*Conti*, Quantum
Bumblebee	*Conti*, Diavol, Quantum
Emotet	*Conti*, BlackCat, Quantum
Qakbot	*REvil*, *Conti*, Black Basta
SocGholish	LockBit

이 표의 데이터는 2021년 말부터 이 보고서가 게시될 때까지의 기간을 다루고 있습니다. 이탤릭체는 멀웨어 또는 랜섬웨어가 2022년에 발견되었지만 적어도 2022년 10월 현재는 X-Force에서 관찰되지 않았음을 의미합니다.

X-Force는 2022년 9월 HTML 밀수(smuggling)를 사용하여 피해자를 손상시킨 Qakbot 활동이 급증한 것을 확인했습니다. 이러한 감염은 정찰, 정보 수집, 추가 페이로드 배포를 포함해 광범위한 손상 후 활동과 연결됩니다. 2022년에 확인되지 않은 Qakbot 감염은 여러 Black Basta 감염으로 이어졌습니다. X-Force는 2022년 여름 Qakbot의 피싱 활동이 중단되는 동안 Black Basta 랜섬웨어 그룹의 유출 사이트에서 랜섬웨어 공격이 현저하게 감소한 것을 확인했습니다. X-Force는 Qakbot 활동이 재개되면 더 많은 랜섬웨어 피해자와 유사한 상관 관계를 갖게 될 것으로 예상합니다.



매크로 우회

ISO 및 LNK 파일 사용은 2021년 10월부터 시작된 Microsoft의 매크로 변경에 대응하여 피해자 조직을 감염시키는 중요한 전략으로 등장했습니다. 이 전략은 해당 컨테이너 파일을 통해 페이로드를 직접 전달하는 것과 그 안에 있는 매크로 사용 파일을 난독화하는 것을 모두 포함합니다.

- ISO 파일과 압축 파일은 대상이 악성 매크로를 활성화하도록 Microsoft가 사용하는 웹 표식(MOTW) 속성을 우회하는 데 사용되고 있습니다. ISO 또는 압축 파일이 인터넷에서 다운로드된 것처럼 보이지만 그 안에 포함된 매크로 지원 첨부 파일은 그렇지 않으므로 위협 행위자가 이 공격을 계속할 수 있습니다.
- 매크로 제한을 우회하는 또 다른 방법은 LNK 파일에 직접 페이로드를 포함하는 것입니다. 이 파일을 클릭하면 주로 다음 단계를 다운로드하거나 로드하는 데 사용되는 임의의 명령이 실행됩니다. 2022년 초 이전에는 2021년 2월에 이 전략을 사용한 캠페인이 하나뿐이었습니다. X-Force는 2022년 2월 말~3월에 처음으로 이것이 반복되는 것을 보았고 지금은 주기적으로 보고 있습니다.

X-Force가 위협 행위자의 스팸 캠페인에서 감지한 추가 트렌드에는 여기에 설명된 대로, 첨부 파일 및 스레드 하이재킹으로 암호화된 압축 아카이브의 사용 증가가 포함됩니다.

- 암호화된 압축 확장 프로그램은 바이러스 백신 소프트웨어가 탐지하고 악성으로 플래그하기 더 어려우며, 2022년에 더 자주 발견되었습니다. 이러한 첨부 파일이 포함된 스팸 이메일의 주당 평균 개수는 2022년 4월 이후 2021년 데이터에 비해 9배 증가했습니다.
- 스레드 하이재킹은 위협 행위자가 자신을 기존 이메일 스레드에 삽입하는 것으로, 스팸 합법성을 높이고 피해자가 더 효과적으로 참여하도록 유도하는 데 사용되는 오랜 전략입니다. 이 전략은 2021년 대부분의 시간과 비교해 2022년에 눈에 띄게 증가했으며 봄에 잦아들었습니다. X-Force가 평가하는 트렌드가 대부분 Emotet 스팸에 의해 주도되는 시기이기 때문입니다.

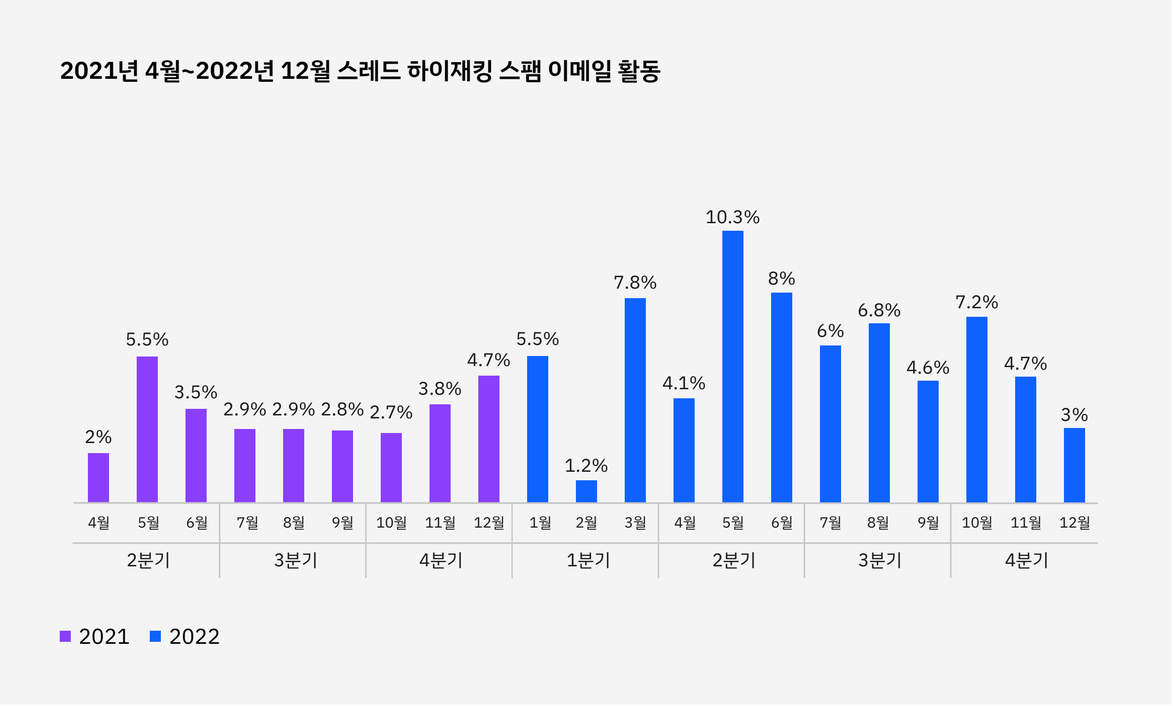


그림 13: 수치는 2021년 4월 이후 X-Force 데이터에서 탐지된 총 스레드 하이재킹 시도의 월별 백분율을 보여줍니다.
출처: X-Force

– Emotet은 2021년 1월 봇넷이 중단된 후 2021년 11월에 돌아왔습니다. 2022년까지 활동을 계속했고, 7월 중순부터 거의 4개월을 쉬었다가 2022년 11월 2주 가까이 복귀했습니다.

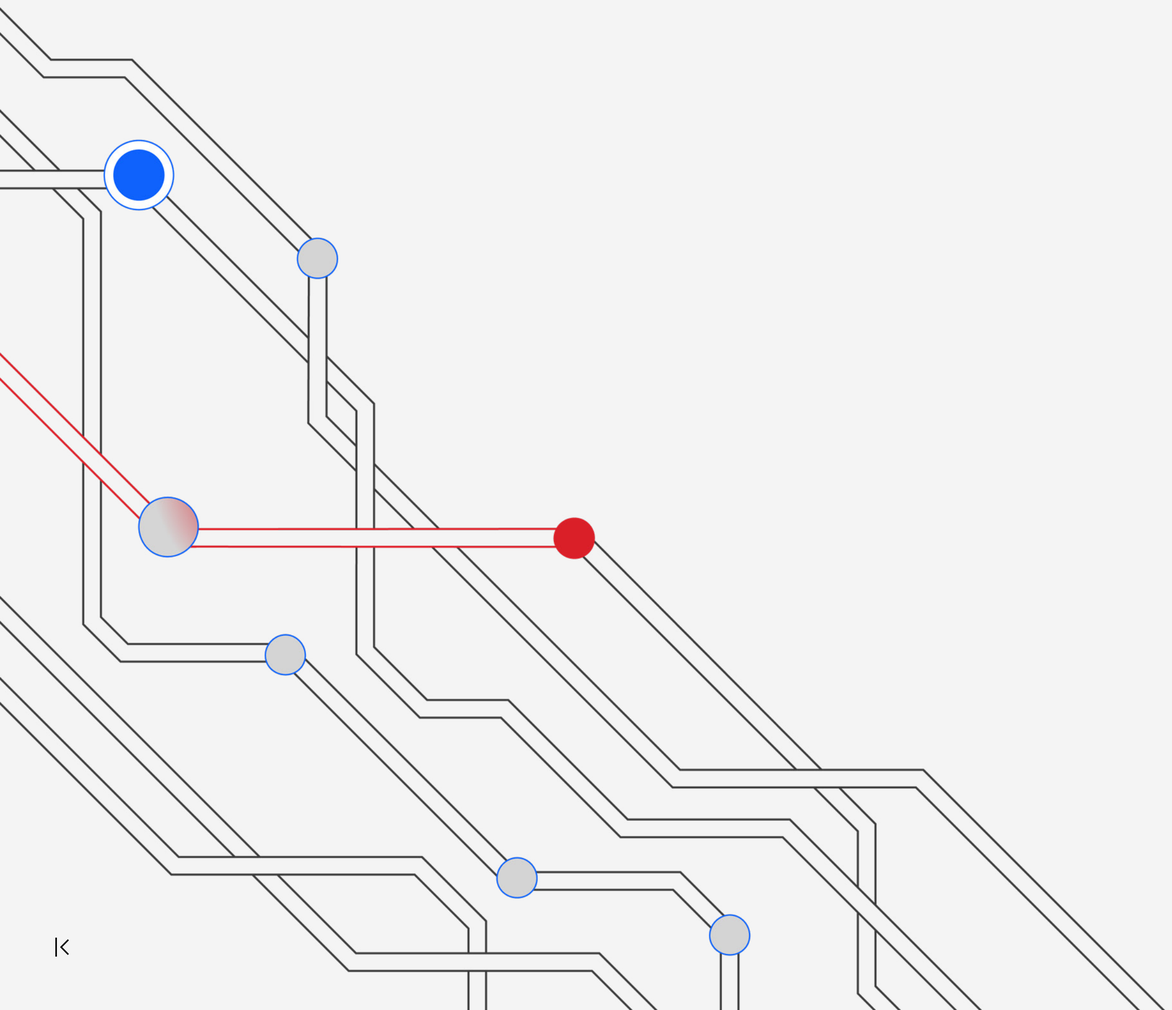
– 이 데이터는 2021년 4월 이후 사용 가능한 데이터와 비교하여 2022년에 정기적으로 있었던 월별 시도가 약 2배에 불과함을 보여줍니다. 스레드 하이재킹은 2022년 5월까지 불안정하게 상승했고, 하반기에는 감소했으며 이는 대략 Emotet의 비활동성과 일치합니다.

– Emotet, Qakbot, IcedID로 이어지는 스팸 이메일은 스레드 하이재킹을 많이 사용했습니다. 2021년 11월 Emotet이 복귀하여 2022년 5월까지 불안정한 증가에 기여했습니다. 하반기의 전반적인 감소는 Emotet이 2022년 7월부터 10월까지 중단되었다가 11월에 잠시 복귀했던 것에 기인합니다.

– 스레드 하이재킹을 추적하고, 이를 단순히 스팸 이메일에 답장 제목 줄 헤더를 추가하는 행위자의 인스턴스와 정확하게 구별하기는 어려우며 더 어려워질 가능성이 높습니다. 예를 들어 ‘Re:’ 제목 줄 헤더를 지우기 시작한 위협 행위자들도 있는데, 이러한 헤더를 사용해 자신의 활동이 추적될 수 있음을 알고 있어서 그럴 가능성이 높습니다.

09

OT 및 산업 제어 시스템에 대한 위협



운영 기술에 대한 위협

2022년에는 Industroyer2 및 INCONTROLLER(또는 PIPEDREAM)라는 새로운 OT 관련 멀웨어가 두 가지 발견되었고, OT:ICEFALL이라 불리는 OT 취약성이 많이 드러났습니다 OT 사이버 위협 환경은 극적으로 확장되고 있기 때문에 OT 자산 소유자와 운영자는 변화하는 환경을 예리하게 인지하고 있어야 합니다.

X-Force는 OT 관련 네트워크 공격과 IR 데이터를 자세히 조사하여 위협 행위자가 OT 관련 업계에서 클라이언트를 손상시키는 방법에 관한 인사이트를 도출하도록 도움을 주었습니다. 네트워크 공격 데이터는 무차별 암호 대입 공격, 취약하고 오래된 암호화 표준 사용, 취약한 암호나 기본 암호가 이러한 업계의 IT 및 OT 환경에서 흔히 발생하는 경고임을 보여줍니다.

무차별 암호 대입 시도 가능성을 나타내는 경고는 인시던트 명령 시스템(ICS), 특정 네트워크 공격 데이터에서 가장 흔했고 약한 암호화 경고가 그 뒤를 이었습니다. 취약한 암호화에 대한 가장 일반적인 경고는 2021년 3월부터 사용되지 않는, 안전하지 않고 위험한 암호화 방법인 전송 계층 보안(TLS) 1.0을 지속적으로 사용하는 것과 관련이 있습니다. 미국 정부는 재구성을 통해 TLS 1.2 또는 1.3을 사용하도록 권장하지만 미국 국립표준기술원(NIST) 지침은 일반적인 현실을 보다 심층적으로 다루고 있습니다. 여기서 일반적인 현실이란, 오래된 시스템이 계속 기능하려면 더 약한 버전의 암호화를 쭉 사용해야 할 수도 있다는 것입니다. 취약하거나 기본 암호 경고도 눈에 띄었는데, 특히 이러한 경고가 기본적이라는 점을 고려할 때 그렇습니다.

OT 및 산업 제어 시스템에 대한 위협

특히 공격자가 무차별 암호 대입 공격을 더 쉽게 하도록 만드는 기본적인 취약성이라는 점을 감안하면 더욱 그렇습니다. 광범위하고 무차별적인 내부 및 외부 취약성 스캐닝은 OT 관련 산업에 대한 가장 일반적인 공격 시도였습니다. 데이터에 따르면 오래된 취약성과 위협은 현재도 여전히 관련이 있습니다. 2021년 Cisco Talos가 발견한 Advantech R-SeeNet 모니터링 소프트웨어의 취약성 그룹은 2022년 OT 산업 전반에 걸쳐 취약성 스캐닝 경고에서 거의 대부분을 트리거했습니다. 이러한 취약성으로 인해 공격자가 임의 코드나 명령을 실행할 수 있게 됩니다.

그러나 두 번째로 흔한 취약점은 2016년으로 거슬러 올라갑니다. Trihedral VTScada 애플리케이션의 필터 우회 취약성인 CVE-2016-4510은 인증되지 않은 사용자가 파일에 액세스하기 위해 HTTP 요청을 보내도록 허용할 수 있습니다. WannaCry 및 Conficker와 같은 공격 유형은 오래된 위협의 위험을 더욱 강조하며, OT에 계속 심각한 위협을 가하고 있습니다.

계속 가장 많은 표적이 되는 OT 산업인 제조업

데이터에 따르면, OT 관련 산업에서 발생하는 인시던트의 하위 집합에서 제조업이 2022년에 가장 많은 공격을 받았습니다. 이 업계는 X-Force가 해결을 도운 인시던트의 58%에서 피해를 입었습니다. 백도어 배포는 목표에 가장 많이 적용된 조치로, 제조 부문 사례의 28%에서 확인되었습니다. 특히 랜섬웨어 행위자는 이 업계를 매력적인 대상으로 여기는데, 이는 이러한 조직이 가동 휴지시간에 대한 내성이 낮기 때문일 수 있습니다.

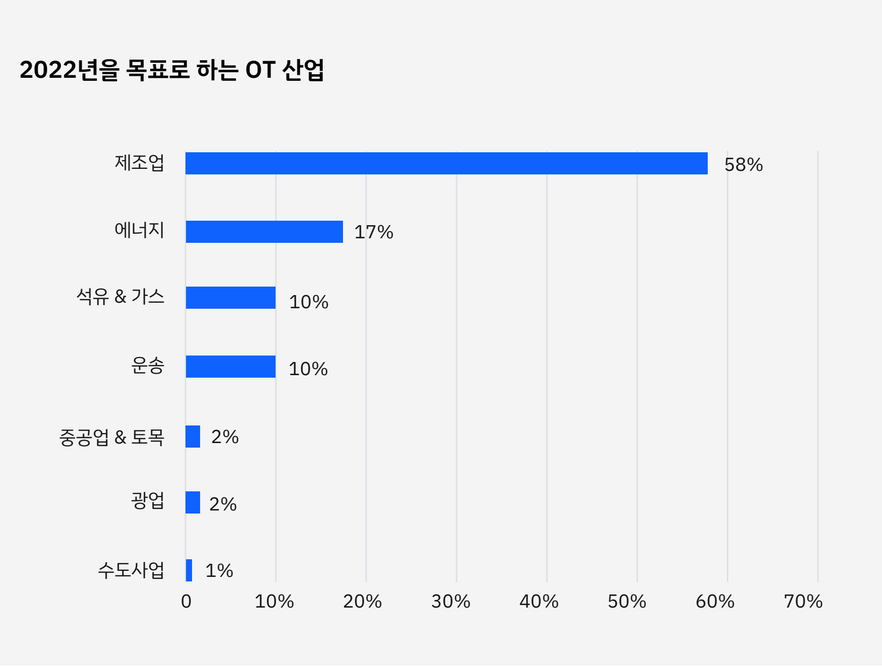


그림 14: 2022년에 X-Force가 응답한 OT 관련 산업별 IR 사례의 비율입니다. 출처: X-Force

OT 관련 산업 사례의 초기 액세스 벡터를 살펴보면 스피어 피싱이 38%였으며, 그 중 첨부 파일 사용이 22%, 링크 사용이 14%, 서비스로서의 스피어 피싱이 2%였습니다. 퍼블릭 애플리케이션 악용은 24%로, 광범위한 산업 추세 다음으로 2위를 차지했습니다. 또한 백도어 탐지가 20%의 사례에서 이러한 업계의 인시던트를 주도했고 랜섬웨어가 19%로 그 뒤를 이었습니다. 갈취는 29%로 1위 영향 요소의 자리를 유지했으며, 데이터 절도는 24%의 사례에서 그 뒤를 바로 따르고 있습니다.

OT에서 악용되는 또 다른 주요 취약성은 OT와 IT 네트워크 간에 적절한 세분화가 부족하다는 것입니다. X-Force Red Adversary Simulation Services 팀은 격리된 OT 환경에 대한 액세스 권한을 얻기 위해 약한 세분화를 주기적으로 할 것을 목표로 합니다. 이러한 환경에는 대상 점프 서버, 이중 홈 운영자 워크스테이션, 보고 서버(예: OT에서 기업 IT 네트워크로 웹 및 SQL 서비스를 노출하는 데이터 히스토리언)가 포함됩니다. 네트워크의 이러한 부분을 적절하게 세분화하고 전체적인 통신을 세심하게 모니터링하면 자산을 안전하게 지킬 수 있습니다.

10

지정학적 트렌드

아시아 태평양 지역은 2022년에 2년 연속 가장 공격을 많이 받은 지역으로 1위를 차지했으며 X-Force IR이 대응한 인시던트에서 31%를 차지했습니다. 유럽이 28%의 공격으로 바로 그 뒤를 이었고, 북미는 25%의 인시던트를 확인했습니다. 아시아 태평양과 유럽은 2021년의 수치에서 각각 5% 포인트와 4% 포인트가 증가하여 사례의 비율이 더 높아졌고, 중동에서는 14%에서 4%로 크게 감소했습니다.

2020~2022년 지역별 인시던트

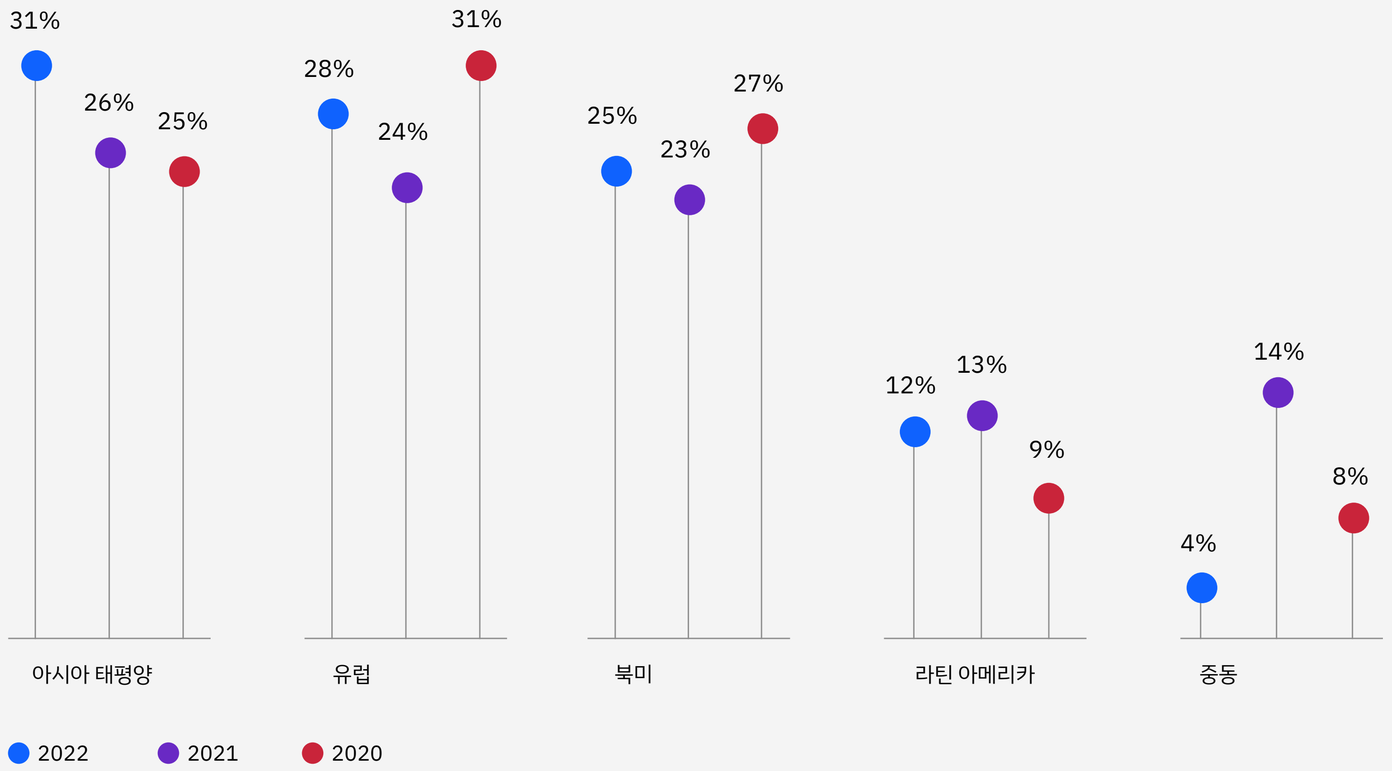


그림 15: 2020~2022년에 X-Force가 대응했던 지역별 IR 사례의 비율입니다. 출처: X-Force

#1 | 아시아 태평양

아시아 태평양 지역, 특히 일본은 2022년 Emotet이 급증한 진원지였습니다. 유럽의 전쟁과 직접적인 관련은 없지만 러시아의 우크라이나 침공과 더불어 일본에서도 Emotet 사례가 급증했으며, 사이버 보안 커뮤니티의 다른 연구원들의 말에 따르면 당시 이것이 Emotet 활동에 상당히 도움이 되었다고 합니다. 스팸 캠페인은 여러 산업에서 확인되었으며 대부분의 사례는 제조업, 금융, 보험 분야에서 발생했습니다. Emotet은 주로 눈길을 끄는 헤드라인을 사용하는 스팸 캠페인을 통해 전달됩니다.

제조업은 사례의 48%에서 이 지역에서 공격을 받는 산업 분야 중 1위를 차지했으며 금융과 보험 업계가 18%로 2위를 차지했습니다.

첨부 파일을 통한 스피어 피싱은 이 지역 전체에서 40%로 가장 높은 감염 벡터였으며, 공용 애플리케이션 악용이 22%로 그 뒤를 이었습니다. 외부 원격 서비스 및 스피어 피싱 링크 사례는 12%로 공동 3위를 차지했습니다.

백도어 배포는 해당 지역 사례의 31%에서 목표에 가장 일반적으로 적용된 조치였습니다. 랜섬웨어는 13%로 2위, maldocs는 10%로 3위를 차지했습니다. 갈취는 사례의 28%에서 관찰된 가장 일반적인 영향이었습니다. 브랜드 평판에 미치는 영향은 22%로 2위, 데이터 절도는 19%로 3위를 차지했습니다.

일본은 아시아 태평양 사례의 91%를 차지했으며 필리핀이 5%, 호주, 인도, 베트남이 각각 1.5%였습니다.

아시아 태평양 지역은 사례의 48%에서 가장 많이 공격을 받은 업계가 제조업임이 확인되었습니다.

#2 | 유럽

유럽에서는 러시아가 우크라이나를 침공한 직후인 2022년 3월부터 백도어 배포가 크게 증가했습니다. 백도어 배포는 해당 지역 사례의 21%를, 랜섬웨어는 11%를 차지했습니다. X-Force가 대응한 인시던트의 10%에서 원격 액세스 툴이 확인되었습니다. 클라이언트에 대한 영향 중 유럽에서 관찰된 X-Force 사례의 38%는 갈취와 관련이 있었고, 17%는 데이터 절도로 이어졌으며 14%는 자격 증명 수집이었습니다. 유럽은 갈취 피해가 가장 큰 지역이며, 관찰된 전체 갈취 인시던트의 44%를 차지했습니다.

퍼블릭 애플리케이션 악용은 유럽 조직에 대해 가장 많이 사용된 감염 벡터였으며 X-Force가 해당 지역에서 해결한 모든 인시던트의 32%를 차지했고 그 중 일부는 랜섬웨어 감염으로 이어졌습니다. 유효한 로컬 계정의 남용이 18%로 2위를 차지했으며 스피어 피싱 링크는 14%로 2021년 42%에 비해 특히 많이 감소했습니다.

이러한 스피어 피싱 링크의 감소는 개선된 사용자 인식, 더 강력한 이메일 보안 방어, 또는 설치 후 멀웨어를 잡기에 더 효과적인 방어의 결과일 수 있습니다.

가장 공격을 많이 받은 업계에서는 금융 및 보험과 관련된 전문가, 기업, 소비자 서비스가 각각 X-Force 대응 사례의 25%를 차지했습니다. 제조업은 사례의 12%로 2위를 차지했으며, 에너지 및 의료 분야는 10%로 공동 3위를 차지했습니다.

영국은 유럽에서 가장 많은 공격을 받은 국가로 사례의 43%를 차지했습니다. 독일은 14%, 포르투갈은 9%, 이탈리아는 8%, 프랑스는 7%를 차지했습니다. X-Force는 노르웨이, 덴마크, 스위스, 오스트리아, 그리스, 그린란드, 스페인, 세르비아에서 발생한 소수의 사례에도 대응했습니다.

영국은 유럽에서 가장 많은 공격을 받은 국가이며 사례의 43%를 차지했습니다.

#3 | 북미

X-Force의 관찰에 따르면 북미 지역의 인시던트 수는 2021년 전체 사례의 23%에서 2022년 25%로 소폭 증가했습니다.

에너지 기업들은 2022년에 북미에서 가장 많은 피해를 입었으며, X-Force가 대응한 모든 공격 중 20%를 차지했습니다. 제조업과 소매/도매 부문은 각각 14%의 사례로 공동 2위를 차지했습니다. 소매/도매 부문는 2021년에 비슷한 위치를 유지했지만 제조업 수치는 2021년에 비해 50% 감소했습니다. 랜섬웨어 및 기타 멀웨어 관련 사례가 증가하는 가운데, 2022년에는 전문가, 기업, 소비자 서비스가 12%로 3위를 차지했습니다.

가장 많이 확인된 감염 벡터는 35%의 공용 애플리케이션 악용과 20%의 스피어 피싱 첨부 파일이었습니다. 랜섬웨어 인시던트는 사례의 23%를 차지했으며, 그 중 일부는 2018년 또는 2019년으로 거슬러 올라가는 WannaCry 또는 Ryuk의 지속적인 감염 탐지의 결과였고, 이러한 사건 이후 적절한 정리 작업의 중요성이 강조되었습니다. 이 지역에서는 사례의 12%가 봇넷이었으며 백도어와 BEC가 각각 10%로 공동 3위를 차지했습니다.

위협 행위자가 가장 크게 미친 영향을 살펴보면, 자격 증명 수집이 X-Force가 북미에서 해결한 인시던트의 25%로 가장 높은 위치를 차지했습니다. 데이터 유출과 데이터 절도는 각각 17%로 공동 2위를 차지했으며, 갈취가 13%를 차지했습니다.

미국은 이 지역 공격에서 80%를 차지했고 캐나다는 20%를 차지했습니다.

북미에서 가장 일반적으로 공격된 조직은 에너지 기업으로, 사례의 20%를 차지했습니다.

#4 | 라틴 아메리카

IBM은 보고 목적으로 라틴 아메리카에 멕시코, 중미, 남미가 포함되는 것으로 간주합니다.

라틴 아메리카의 인시던트는 글로벌 트렌드를 거스르며, X-Force가 해결한 사례의 28%에서 가장 공격을 많이 받은 산업으로 소매업이 다시 그 자리를 차지했고 2021년의 2위에서도 올라갔습니다. 금융 및 보험 산업은 사례의 24%를 차지하며 2위 표적이 되었고, 에너지 부문이 20%로 그 뒤를 이었습니다.

랜섬웨어는 라틴 아메리카에서 X-Force가 대응한 사례의 32%를 차지하면서 그 외 다른 공격을 제쳤습니다. 백도어 배포는 16%를 차지하면서 두 번째로 많이 확인된 목표에 적용된 조치였으며, BEC 및 이메일 스레드 하이재킹은 각각 11%로 공동 3위를 차지했습니다. 갈취 및 데이터 절도는 이 지역에서 가장 흔히 볼 수 있는 영향으로 사례의 27%를 차지했으며, 금전적 손실은 20%였습니다. 데이터 파괴 및 유출은 각각 사례의 13%를 차지하며 공동 3위였습니다.

가장 많았던 초기 액세스 벡터로는 외부 원격 서비스 30%, 공용 애플리케이션 악용 20%가 포함되었습니다. 드라이브 바이 손상, 하드웨어 추가, 유효한 도메인 계정, 유효한 로컬 계정 및 스피어 피싱 첨부 파일이 각각 10%를 차지했습니다.

라틴 아메리카에서 X-Force가 대응한 모든 사례 중에서 브라질이 67%, 콜롬비아가 17%, 멕시코가 8%를 차지했습니다. 페루와 칠레는 나머지 8%를 나눠 차지했습니다.

라틴 아메리카의 X-Force 대응 사례에서 브라질이 67%를 차지했습니다.

#5 | 중동 및 아프리카

IBM은 보고 목적으로 중동과 아프리카에 레반트, 아라비아 반도, 이집트, 이란, 이라크 및 아프리카 대륙 전체가 포함되는 것으로 간주합니다.

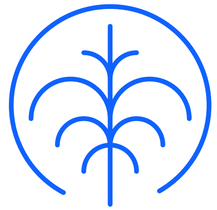
2022년에 이 지역에서 X-Force가 대응한 사례 중 27%에서 백도어 배포가 탐지되었습니다. 랜섬웨어와 웜은 각각 18%를 차지하며 두 번째로 흔한 공격 유형이었습니다. 갈취와 재정적 손실은 각각 2021년 지역 전체에서 발생한 인시던트에서 확인된 영향의 절반씩을 차지했습니다.

스피어 피싱 링크는 사례의 2/3에서 초기 액세스에 사용되었으며, 이동식 미디어는 X-Force가 중동 및 아프리카에서 해결한 인시던트 중 나머지 3분의 1을 차지했습니다.

금융 및 보험 업계는 2022년 중동과 아프리카에서 가장 많이 표적이 된 산업으로, 인시던트의 44%를 차지했으며 2021년의 48%에 비하면 약간 감소했습니다. 전문가, 기업, 소비자 서비스가 공격의 22%를 차지했으며 제조업 및 에너지 부문이 11%로 3위를 차지했습니다.

사우디아라비아는 X-Force가 대응한 지역 내 사례 중 2/3를 차지했습니다. 나머지 사례들은 카타르, 아랍 에미레이트, 남아프리카가 차지합니다.

이 지역에서 가장 일반적인 공격은 백도어 배포였으며 사례의 27%를 차지했습니다.



11

업계 트렌드

X-Force 인시던트 대응 데이터에 따르면 제조업은 2년 연속으로 가장 공격을 많이 받은 업계가 되었습니다. 금융 및 보험은 5년 연속 타이틀을 유지하다가 2021년에 단 1% 포인트 차이로 1위 자리를 잃었고, 2022년에는 6% 포인트에 달하는 큰 차이로 다시 2위를 차지했습니다.

2018~2022년 업계별 공격 비율

산업	2022	2021	2020	2019	2018
제조업	24.8%	23.2	17.7	8	10
재무 및 보험	18.9%	22.4	23	17	19
전문가, 비즈니스 및 소비자 서비스	14.6%	12.7	8.7	10	12
에너지	10.7%	8.2	11.1	6	6
소매업 및 도매업	8.7%	7.3	10.2	16	11
교육	7.3%	2.8	4	8	6
의료	5.8%	5.1	6.6	3	6
정부	4.8%	2.8	7.9	8	8
운송	3.9%	4	5.1	13	13
미디어 및 텔레콤	0.5%	2.5	5.7	10	8

24.8%

X-Force 인시던트 대응 사례가 제조업 부문에서 발생했습니다.

#1 | 제조업

제조업은 가장 공격을 많이 받은 산업으로 2021년에 비해 비율이 약간 늘었습니다. 2022년에는 인시던트의 28%에서 백도어가 배포되어 X-Force에서 해결한 인시던트의 23%으로 나타난 랜섬웨어를 제쳤습니다. 백도어 배포의 비율은 Emotet 감염 급증에서 영향을 받은 것이기도 합니다. 이러한 사례 중 일부는 랜섬웨어 공격을 비롯해 악의적인 다른 활동으로 이어질 수도 있었지만 다행히 일찍 식별하여 해결할 수 있었습니다.

스피어 피싱 첨부 파일과 공용 애플리케이션 악용은 감염 벡터 공동 2위로 각각 28%를 차지했습니다. 외부 원격 서비스는 14%로 2위를 차지했으며 스피어 피싱 링크 및 유효한 기본 계정은 10%의 사례에서 초기 액세스로 공동 3위를 차지했습니다.

갈취는 제조업 조직에 가장 주요한 영향이었으며 사례의 32%에서 확인되었습니다. 제조업체는 다운타임을 거의 또는 전혀 허용하지 않는 것으로 유명하기에, 이러한 점 때문에 갈취는 공격자에게 유리한 전략이 됩니다. 데이터 절도는 두 번째로 가장 일반적이었으며 인시던트의 19%를 차지하고 데이터 유출이 16%로 그 뒤를 이었습니다. 아시아 태평양 지역에서는 제조업 인시던트가 사례의 약 61%를 차지하며 가장 많았습니다. 유럽, 북미 지역은 각각 14%로 공동 2위를 차지했고, 라틴 아메리카 지역은 8%, 중동과 아프리카는 4%였습니다.

18.9%

X-Force 인시던트 대응 사례가 재무 및 보험 부문에서 발생했습니다.

#2 | 금융 및 보험

금융 및 보험 조직은 2022년에 X-Force가 대응한 공격 5건 중 1건 미만을 차지하며 2위에 올랐습니다. 이 비율은 다른 산업, 특히 제조업이 공격자에게 주목을 받기 시작하면서 지난 몇 년 동안 약간 감소했음을 보여줍니다.

금융 및 보험 회사는 다른 산업에 비해 디지털 혁신 및 클라우드 채택 여정에서 더 앞서가는 경향이 있습니다. 그 결과, 공격자는 이러한 조직을 공격하려면 더 애를 써야 하게 되었습니다.

백도어 공격은 가장 일반적으로 목격되는, 목표에 적용된 작업이었으며 랜섬웨어 및 악성 문서가 각각 11%로 그 뒤를 따랐습니다. 가장 많았던 감염 벡터는 스피어 피싱 첨부 파일로, 이 분야에 대한 공격의 53%에서 사용되었습니다. 퍼블릭 애플리케이션 악용은 공격의 18%로 2위를 차지했고, 사례의 12%에서 초기 액세스 벡터는 스피어 피싱 링크였습니다.

유럽은 금융 및 보험 조직에서 전체 공격의 약 33%에 해당하는 가장 많은 공격을 받았으며, 아시아 태평양은 약 31%로 근소한 차이를 만들며 2위를 차지했습니다. 라틴 아메리카는 X-Force가 대응한 인시던트에서 약 15%를 경험했으며 북미와 중동, 아프리카는 각각 약 10%를 경험했습니다.

14.6%

X-Force 인시던트 대응 사례가 전문가, 기업, 소비자 서비스 부문에서 발생했습니다.

#3 | 전문가, 기업, 소비자 서비스

전문 서비스 업계에는 컨설팅 회사, 관리 회사, 법률 회사가 포함됩니다. 이러한 서비스는 해당 부문 피해 사례에서 52%를 차지합니다. 반면 비즈니스 서비스에는 IT 및 기술 서비스, 홍보, 광고, 커뮤니케이션 등의 회사가 포함됩니다. 이러한 서비스는 피해 사례의 37%를 차지합니다. 주택 건설, 부동산, 예술, 엔터테인먼트, 레크리에이션을 포함한 소비자 서비스는 11%를 차지했습니다. 이들은 함께 2023 X-Force Threat Intelligence Index 의 전문가, 기업, 소비자 서비스 범주를 이루게 됩니다. 전문가, 기업, 소비자 서비스는 랜섬웨어 및 백도어 공격을 가장 자주 경험했으며 이는 각각 사례의 18%에 해당합니다. 상위 2개의 감염 벡터는 공용 애플리케이션과 외부 원격 서비스의 악용이었으며, 각각 23%를 차지했습니다. 스피어 피싱 첨부 파일과 유효한 계정은 각각 사례의 15%를 차지했습니다.

갈취는 사례의 28%에서 가장 일반적인 영향이었으며 데이터 절도, 자격 증명 수집, 데이터 유출은 각각 17%를 차지했습니다. X-Force는 유럽에서 47%, 북미에서 33%, 아시아 태평양에서 10%, 중동과 아프리카에서 7%, 라틴 아메리카에서 3%의 사례에 대응했습니다.

10.7%

X-Force 인시던트 대응 사례가 에너지 부문에서 발생했습니다.

#4 | 에너지

에너지 유틸리티, 석유 및 가스 회사 등의 에너지 기업은 2021년과 마찬가지로 공격의 10.7%를 차지하며 네 번째로 가장 많은 공격을 받은 산업이었습니다. 퍼블릭 애플리케이션의 악용은 가장 흔한 감염 벡터로 40%를 차지했습니다. 스피어 피싱 링크와 외부 원격 서비스는 각 사례의 20%를 차지했습니다. 봇넷은 19%의 사례에서 가장 빈번하게 행한 목표에 적용된 조치였으며, 랜섬웨어와 BEC가 15%로 2위를 차지했습니다.

데이터 절도 및 갈취는 23%의 사례로 나타났고, 자격 증명 수집 및 봇넷 감염이 각각 15%로 나타났습니다. X-Force가 전 세계적으로 대응한 모든 사례에서 북미 조직이 가장 일반적인 피해자로 46%를 차지했으며, 유럽과 라틴 아메리카는 각각 23%, 아시아 태평양, 중동, 아프리카에서는 5% 미만이었습니다.

에너지 산업은 다양한 글로벌 세력, 특히 러시아 우크라이나 전쟁으로 악화된 세력과 이미 격동 중인 글로벌 에너지 무역에 미친 영향으로 인해 압박을 받고 있습니다.

8.7%

X-Force 인시던트 대응 사례가 소매 및 도매 부문에서 발생했습니다.

#5 | 소매 및 도매

소매업체는 소비자와 도매업체에게 상품을 판매할 책임이 있습니다. 도매업체는 일반적으로 제조업체에서 소매업체로 직접, 또는 소비자에게 직접 이러한 상품을 운송하고 유통합니다. 2021년 순위와 동일한 X-Force IR 데이터에 따르면, 소매 및 도매 산업은 다섯 번째로 표적이 된 산업이었습니다.

소매업 및 도매업 공격에서 가장 일반적인 초기 액세스 벡터는 악성 링크가 포함된 스피어 피싱 이메일이었으며 33%를 차지했습니다. 손상된 외부 원격 서비스, 악성 첨부 파일이 포함된 스피어 피싱, 하드웨어 추가가 각각 17%를 차지했습니다.

랜섬웨어, 백도어, BEC는 공격자가 취한 가장 일반적인 조치였으며 각각 활동의 19%를 차지했습니다. 웜은 사례의 10%에서 확인되었습니다. 피해자는 사례의 50%에서 갈취를 경험했으며, 자격 증명 수집 및 재정적 손실은 각각 25%를 차지했습니다. 북미 및 라틴 아메리카는 사례의 각각 39%로 가장 많은 사례를 경험했으며 이는 22%를 차지한 유럽과 비교됩니다.

7.3%

X-Force 인시던트 대응 사례가 교육 부문에서 발생했습니다.

#6 | 교육

교육 부문 인시던트는 X-Force가 대응한 공격의 20%에서 백도어 사례와 관련이 있었습니다. 랜섬웨어, 애드웨어, 스팸이 각각 13%를 차지했습니다. 사례의 42%에서 가장 일반적으로 관찰된 초기 액세스는 퍼블릭 애플리케이션 악용이었으며, 스피어 피싱 첨부 파일이 25%로 그 뒤를 이었습니다. 서비스, 링크, 유효한 클라우드, 로컬 계정 남용을 통한 피싱은 각각 초기 액세스 벡터의 8%를 차지했습니다. 데이터 절도, 데이터 유출, 갈취, 정찰은 각각 25%의 영향을 미쳤습니다. 아시아 태평양은 사례의 67%를 차지했으며, 북미는 27%, 라틴 아메리카는 6%였습니다.

5.8%

X-Force 인시던트 대응 사례가 의료 부문에서 발생했습니다.

#7 | 의료

의료 분야는 상위 10개 산업 중 7위로 다시 떨어졌으며, 2021년 순위였던 6위에서 더 하락했습니다. X-Force가 대응한 의료 사례의 비율은 지난 3년 동안 약 5~6%를 유지했습니다. 백도어 공격은 사례의 27%에서 발생했으며 웹 셸은 18%를 차지했습니다. 애드웨어, BEC, 크립토마이너, 로더, 정찰, 스캐닝 툴, 원격 액세스 툴은 각각 9%를 차지했습니다. 관찰된 영향의 대부분을 구성한 정찰은 50%였으며 데이터 절도와 디지털 통화 마이닝은 각각 25%로 확인되었습니다.

유럽 기반 표적은 인시던트의 58%를 차지했으며, 북미의 사례가 나머지 42%를 차지했습니다.

4.8%

X-Force 인시던트 대응 사례가 정부 부문에서 발생했습니다.

#8 | 정부 기관

또 한 가지 백도어의 가장 주요한 표적으로는 정부 표적이 있었으며 이는 X-Force IR 사례의 25%를 차지했습니다. 사례의 1/4를 차지한 이 비율은 디도스 공격의 비율과도 동일합니다. 공공 부문 네트워크의 풍부하고 민감한 정보는 사이버 스파이 캠페인의 일반적인 목표입니다. 이 정보에는 방대한 PII 데이터베이스 및 기타 정보가 포함될 수 있으며 이는 국가 후원 그룹이 사용하거나 사이버 범죄자가 이익을 위해 판매할 수 있습니다. 악성 문서는 사례의 17%에서 식별되었으며 크립토마이너, 자격 증명 획득 툴, 랜섬웨어 및 웹 셸은 나머지 83% 사례를 분할하여 차지했습니다.

이 부문의 사례에서 X-Force는 인시던트를 사이버 범죄자, 데이터 파괴로 이어진 내부자 위협, 핵티비스트, 스파이 활동을 수행하는 국가 지원 위협 그룹과 각각 동일한 비율로 식별했습니다.

공용 애플리케이션 악용과 스피어 피싱 첨부 파일은 각각 40%를 차지하는 주요 감염 벡터였으며, 유효한 기본 계정의 남용이 20%를 차지했습니다. 아시아 태평양 지역의 정부 기관은 사례의 50%를 가장 주요한 표적으로 삼았으며 유럽은 30%, 북미는 20%였습니다.

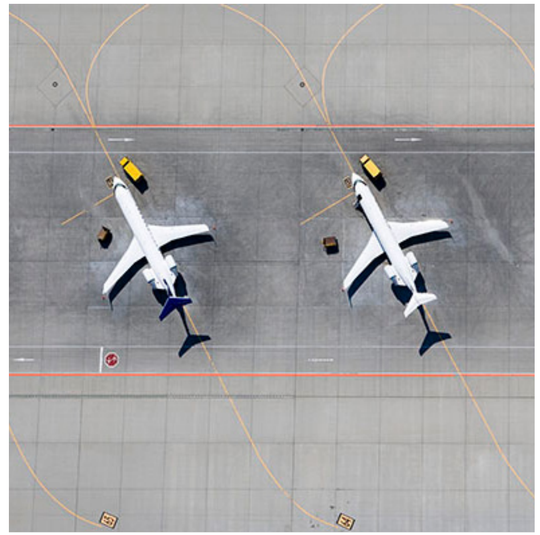
3 . 9%

X-Force 인시던트 대응 사례가
대중교통 부문에서 발생했습니다.

#9 | 교통

2020년 9위였던 대중교통은 2021년 7위로 다시 올라왔습니다. 그러나 업계는 여전히 X-Force가 대응한 인시던트의 비율과 거의 동일한 비율을 구성했습니다. 피싱은 사례의 51%에서 가장 일반적인 초기 액세스 벡터였으며 링크, 첨부 파일 및 서비스형 스피어 피싱 간에 고르게 나뉘어 있습니다. 유효한 로컬 계정의 남용이 초기 액세스 벡터의 33%를 차지했고, 유효한 클라우드 계정이 17%의 사례에서 시작점 역할을 했습니다. 목표에 따라 가장 많이 행해진 조치는 서버 액세스 및 원격 액세스 툴 배포로 각각 25%를 차지했으며, 스팸 캠페인, 랜섬웨어, 백도어, 손상이 각각 사례의 13%을 차지하며 뒤를 이었습니다.

데이터 절도는 사례의 50%를 차지하며 가장 흔했고, 갈취 및 브랜드 평판에 대한 영향은 각각 25%였습니다. 유럽의 대중교통 기관은 가장 주요한 표적 그룹이었으며 사례의 62%를 구성했습니다. 아시아 태평양 지역이 2위를 차지했으며 37%를 조금 웃도는 수준이었습니다.



0.5%

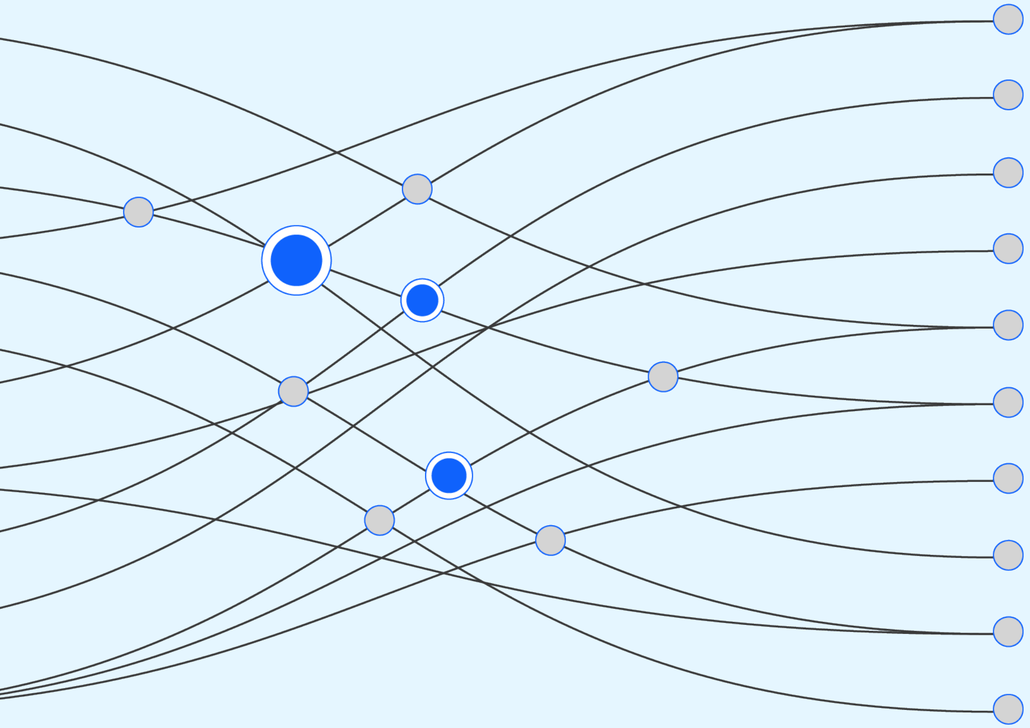
X-Force 인시던트 대응 사례가 미디어 및 텔레콤 부문에서 발생했습니다.

#10 | 미디어 및 텔레콤

미디어와 텔레콤 분야는 X-Force가 대응한 인시던트에서 작은 부분을 차지하며 2년 연속 최하위를 기록했습니다. 관찰된 감염 벡터로는 VPN 및 기타 액세스 메커니즘과 같은 외부 원격 서비스의 남용 및 유효한 도메인 계정이 있었습니다. 이러한 벡터는 랜섬웨어 공격으로 이어졌습니다. 해당 사례에서 관찰된 조치로는 랜섬웨어 배포, 데이터 유출 툴이 포함되었습니다. 이러한 조치는 데이터 절도, 유출, 파괴, 갈취로 이어졌습니다.

12

권장 사항



다음의 권장 사항은 이 보고서에 제시된 것을 포함하여 악의적인 위협으로부터 조직을 보호하기 위해 취해야 하는 조치입니다.

자산 관리: “무엇을 갖고 있는가? 무엇을 보호하고 있는가? 어떤 데이터가 비즈니스에 중요한가?” 보안 팀은 먼저 이 질문들에 대답할 수 있어야 성공적인 방어를 구축할 수 있습니다. 경계에서 자산 검색의 우선 순위를 지정하고 피싱 공격에 대한 노출을 이해하여 이러한 공격 표면을 줄이면, 전체적인 보안에 더 기여하게 됩니다. 마지막으로, 조직은 인터넷이나 다크 웹에 이미 존재할 수 있는 소스 코드, 자격 증명 및 기타 데이터를 포함하도록 자산 관리 프로그램을 확장해야 합니다.

공격자에 대해 알기: 많은 조직이 위협 환경에 대해 폭넓은 관점을 가지고 있는데, X-Force는 조직이 산업, 조직, 지역을 표적으로 삼을 가능성이 가장 높은 특정 위협 행위자를 특별히 강조하는 관점을 채택하기를 권장합니다. 이러한 관점에는 위협 행위자의 작동 방식을 이해하는 것, 이들의 정교함 수준을 식별하는 것, 공격자가 가장 선택할 가능성이 높은 전략과 기술, 절차를 아는 것이 포함됩니다.

가시성 관리: 조직은 공격할 가능성이 가장 높은 적에 대해 더 많이 파악한 다음 공격자의 존재를 나타내는 데이터 소스에 적절한 가시성이 있는지 확인해야 합니다. 공격자가 혼란을 일으키기 전에 이를 사전 예방하려면 기업 전반의 주요 지점에서 가시성을 유지하고 적시에 경고를 생성하며 조치를 취하는 것이 중요합니다.

문제점 가정하기: 조직은 이미 손상된 상황을 가정해봐야 합니다. 그렇게 하면 팀이 계속 다음을 재검토할 수 있습니다.

- 공격자가 시스템에 침투하는 방법
- 공격자의 탐지 및 대응 능력이 새로운 전술, 기술, 절차에 얼마나 잘 대처하는지 여부
- 공격자가 가장 중요한 데이터 및 시스템을 손상시키기 어려운 정도

가장 성공적인 보안 팀은 위협 사냥, 침투 테스트 및 목표 기반 레드 팀 구성 등 주기적으로 공격 테스트를 수행하여 환경을 엿보는 공격 경로를 감지하거나 검증합니다.

인텔리전스에 따라 조치: 모든 곳에 위협 인텔리전스를 적용합니다. 위협 인텔리전스를 효과적으로 적용하면 일반적인 공격 경로를 분석하고 일반적인 공격을 완화하기 위한 주요 기회를 식별할 수 있을 뿐만 아니라 신뢰도 높은 탐지 기회를 개발할 수 있습니다. 위협 인텔리전스를 적용할 때는 공격자 및 공격자의 작동 방식에 대한 이해가 함께 해야 합니다.

준비하기: 공격은 피할 수 없지만, 실패는 피할 수 있습니다. 조직은 환경에 맞춤화된 인시던트 대응 계획을 개발해야 합니다. 이러한 계획은 응답, 해결, 복구 시간을 개선하는 데 중점을 두고 조직이 변화에 맞춰 주기적으로 연습해보고 수정해야 합니다.

평판이 좋은 IR 공급업체를 보유하면, 숙련된 대응 담당자가 공격 완화에 집중하는 데 걸리는 시간을 줄일 수 있습니다. 또한 응답 계획 개발 및 테스트에 IR 공급업체를 포함하는 것이 중요하며, 이렇게 하면 보다 효과적이고 효율적으로 대응하는 데 도움이 됩니다. 최상의 IR 계획에는 조직 간 대응, IT 외부 이해 관계자 포함, 기술 팀과 고위 경영진 간의 커뮤니케이션 라인 테스트가 포함됩니다. 마지막으로, 몰입형 고압 사이버 범위 연습(high-pressure cyber range exercise)에서 계획을 테스트하면 공격에 대응하는 능력을 크게 향상할 수 있습니다.

다음의 조치를 통해 보안 강화하기:

- [ ] 자산 관리
- [ ] 공격자에 대해 알기
- [ ] 가시성 관리
- [ ] 과제 가정하기
- [ ] 인텔리전스에 따라 조치
- [ ] 준비하기

소개

IBM Security X-Force

IBM Security X-Force는 해커, 대응 담당자, 연구원, 분석가로 구성된 위협 중심 담당 팀입니다. X-Force 포트폴리오에는 위협에 대한 360도 분석을 기반으로 하는 공격 및 방어 제품과 서비스가 포함되어 있습니다.

끊임없는 사이버 공격, 광범위한 연결성, 증가하는 규제 요구 사항을 겪는 시대에 조직에는 집중적인 보안 접근 방식이 필요합니다. X-Force는 그 중심에 위협이 있다고 믿습니다. X-Force Red 해커 팀은 침투 테스트, 취약점 관리, 상대 시뮬레이션 서비스를 통해 공격자의 역할을 상정하고, 가장 중요한 자산을 노출하는 보안 취약성을 찾아냅니다. X-Force 인시던트 대응 팀은 인시던트 대비, 탐지, 대응, 위기 관리 서비스를 통해 위협이 잠복해 있을 만한 위치와 이를 차단하는 방법을 파악합니다. X-Force 연구진은 위협을 탐지 및 방지하기 위한 공격 기술을 개발하고, 분석가는 X-Force를 통해 위협 데이터를 수집하고 실행 가능한 정보로 변환하여 위험을 줄입니다.

X-Force는 공격자의 사고, 전략 수립, 공격 방법에 대한 심도 있는 이해를 바탕으로 인시던트를 예방하고, 탐지하고, 대응하고 복구할 뿐 아니라 비즈니스 우선순위에 집중하는 데 도움을 드립니다.

보안 태세를 강화하는 데 지원이 필요하다면 IBM Security X-Force 전문가와 일대일 상담을 예약하세요.

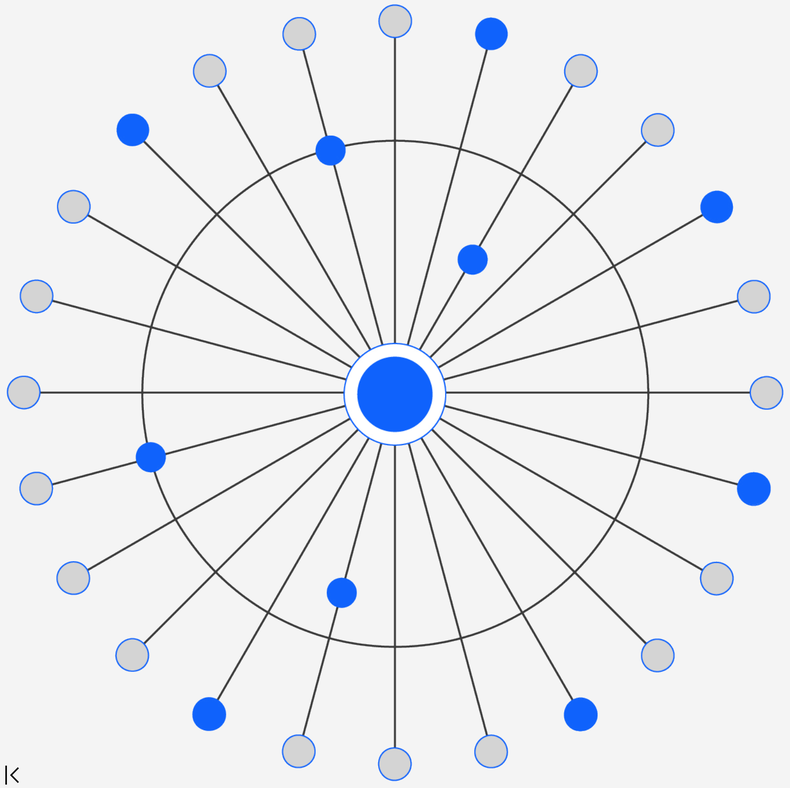
상담 예약 →

IBM Security

IBM Security는 지속적으로 확장되는 공간에 맞춰 적응하고 올바른 방향으로 나아가기 위해 협력합니다. 동적 AI 및 자동화 기능을 통해 더 빠르고 더 정확하게 항상 한 발 앞서 나가도록 지원합니다. 신뢰할 수 있는 업계 최고의 전문가 팀을 통해 인사이트를 확보하여 확신을 갖고 현재와 미래를 위한 올바른 조치를 취할 수 있습니다. 위협 예측에서 보호 데이터 지원까지 공급업체 전반 또는 전 세계에서 업무가 가능하며, IBM Security는 비즈니스의 방향성과 무관하게 중요한 신기술을 탐색하고 예상치 못한 위협을 최소화하며, 비즈니스 목표를 달성하도록 지원합니다.

더 알아보기 →

기고자



Michael Worley
Christopher Caridi
Michelle Alvarez
Karlina Bakken
Yannick Bedard
Michele Brancati
Christopher Bedell
Joshua Chung
Scott Craig
Joseph DiRe
John Dwyer
Emmy Ebanks
Richard Emerson
Charlotte Hammond
Kevin Henson
Guy-Vincent Jourdan
Vio Onut
Mitch Mayne
Dave McMillen
Kat Metrick
Scott Moore
Golo Mühr
Andy Piazza
Benjamin Shipley
Christopher Thompson
Ole Villadsen
Reginald Wong
John Zorabedian

15

부록

영향 목록

영향	영향
봇넷	디지털 통화 마이닝
브랜드 평판	스파이 활동
자격 증명 수집	갈취
데이터 파괴	재정 손실
데이터 유출	생산 중단(OT)
데이터 절도	정찰

1. “A timeline of the biggest ransomware attacks,” CNET, 2021년 11월 15일
2. “International action against DD4BC cybercriminal group,” Europol, 2016 년 1월 12일
3. “DD4BC, Armada Collective, and the Rise of Cyber Extortion,” Recorded Future, 2015 년 12월 7일
4. “A Brief History of Ransomware.” Varonis, 2015년 11월 10일
5. “Inside Chimera Ransomware - the first ‘doxingware’ in wild,” MalwardBytes Labs, 2015년 12월 8일
6. “Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware,” Crowdstrike, 2018년 11월 14일
7. “Operators of SamSam Continue to Receive Significant Ransom Payments,” Crowdstrike, 2018년 4월 11일
8. “Triple Extortion Ransomware: The DDoS Flavour,” PacketLabs, 2022년 5월 12일
9. “They Told Their Therapists Everything. Hackers Leaked It All,” Wired, 2021년 5월 4일
10. “BazarCall to Conti Ransomware via Trickbot and Cobalt Strike,” The DFIR Report, 2021년 8월 1일
11. “Diavol Ransomware,” The DFIR Report, 2021년 12월 13일
12. “Quantum Ransomware,” The DFIR Report, 2022년 4월 25일
13. “Bumblebee Loader Linked to Conti and Used In Quantum Locker Attacks,” Kroll, 2022년 6월 6일
14. “This isn’t Optimus Prime’s Bumblebee but it’s Still Transforming,” Proofpoint, 2022년 4월 28일,
15. “Understanding REvil: REvil Threat Actors May Have Returned (Updated),” Unit 42, 2022년 6월 3일
16. “AdvIntel’s State of Emotet aka “SpmTools” Displays Over Million Compromised Machines Through 2022,” AdvIntel, 2022년 9월 13일
17. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack,” NCC Group, 2022 년 8월 19일
18. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack,” NCC Group, 2022년 8월 19일

(07326) 서울특별시 영등포구 국제금융로 10
서울국제금융센터(3IFC)

미국에서 제작됨
2023년 2월