2025 Vol.6

PRIVACY REPORT

개인정보 이슈 심층분석

개인정보 유출

KISA 한국인터넷진흥원

PRIVACY REPORT

2025년
개인정보 이슈
심층분석

CONTENTS

1 **AI 기반 보이스피싱·스미싱 탐지 및 대응 정책** · · · · 3
윤해성 / 한국형사·법무정책연구원 / AI·미래정책연구실장

2 **보안 사고 사례와 개인정보 유출** · · · · · · · · · · 10
배상민 / 이스트시큐리티 개발혁신센터 / 실장

3 **다크웹과 개인정보 불법유통 현황 및 대응 전략** · · · · 16
김재기 / S2W 위협 인텔리전스 센터(TALON) / 센터장

AI 기반 보이스피싱·스미싱 탐지 및 대응 정책

윤해성
한국형사·법무정책연구원 I AI·미래정책연구실장

1. 들어가며

2006년 처음 발생한 보이스피싱 범죄는 서민경제를 위협하는 범죄로만 인식되어 왔다. 그러나 최근 보이스피싱, 스미싱 같은 피싱 범죄가 점점 진화되고 교묘화됨에 따라 전 국민을 상대로 범죄의 대상이 확대되고 있다. 보이스피싱 범죄의 경우, 대출 사기형과 기관 사칭형이 큰 비율을 차지하고 있으며, 2021년 이후에는 메신저, SNS 등 비대면 채널 이용이 증가하면서 가족이나 지인을 사칭하는 피싱 범죄 비중이 빠르게 증가하였다. 더구나 AI와 딥페이크와 같은 신종 수법의 등장으로 인하여 기존 피싱 범죄보다 그 수법이 발전되고 있다. 이와 같은 기술로 인하여 수사기관이 피싱 범죄자를 검거하는데 더욱 어렵게 되었고 국민 입장에서도 피싱 범죄에 대한 진위 여부를 파악하는데 혼란을 가중하고 있다.

이를 대비하기 위하여 금융 당국을 비롯하여 통신회사 등 범정부 차원에서 보이스피싱과 같은 피싱 범죄에 대응을 위하여 각종 법 제도를 마련하고 기술적 차원에서도 범죄 예방을 위한 조치를 취하고 있지만 신종 수법에 대응하는데 한계가 있다. 이하에서는 그동안 보이스피싱 및 스미싱과 같은 피싱 범죄의 유형별 특징과 진화 양상을 분석하고, 최근 부각된 AI 기반 음성합성 및 딥페이크를 이용한 신종 보이스피싱 수법 역시 간략하게 살펴보고자 한다. 그런 다음 피싱 범죄를 탐지하고 대응할 수 있는 정책과 법제도 개선 방향을 중심으로 제시하고자 한다.

2. 피싱 범죄 유형별 특징과 진화 양상 분석

1) 초기 피싱 범죄 유형별 특징과 양상

초기 피싱 범죄의 경우, 연금 관리 공단, 금융기관, 검찰, 경찰, 국세청 등의 기관 사칭형 유형으로 피해자를 현금인출기(ATM)까지 직접 가서 대포통장으로 이체하게 하는 수법을 주로 이용했다면, 이러한 사기 수법이 많이 알려진 이후에는 경품행사 당첨, 대학 등록금 환급 등 새로운 시나리오를 이용하거나, 사전에 입수한 개인정보를 활용한 대출을 빙자하는 수법, 카드론 대출 등과 같이 금품을 편취하는 수법이 이용되기도 했다.[1] 피싱 범죄의 사기 과정은 '사기 이용 계좌를 확보' →

‘전화, 문자메시지 시도’ → ‘피해자 기망 또는 공갈’ → ‘피해자의 계좌이체’ → ‘사기 이용 계좌에서 금원 인출 또는 송금’[2]의 수법이 대부분이었다.

2) 진화하는 피싱 범죄의 유형과 양상

정보통신의 발달과 새로운 기술과 결합하면서 피싱 범죄 역시 다양한 형태로 진화하였다. 가령, 피싱 범죄에서 피해자를 기망하는 시나리오를 사회 상황에 맞는 수법을 이용한다. 예를 들어, “VoIP를 이용하거나”, “공공기관, 금융회사 인터넷 홈페이지를 가장한 피싱 사이트를 개설하고 금융정보를 입력하도록 하는 수법”[3], “이용자의 컴퓨터에 악성코드를 감염시켜 미리 제작해 둔 사이트에 접속하도록 유도하여 금융정보를 탈취하는 파밍”, “문자메시지로 은행, 금융기관 등 관련 웹사이트 링크를 발송하여 휴대전화 이용자가 링크를 클릭하면 악성코드가 설치되고 설치된 악성코드를 이용하여 소액결제를 하여 금융정보를 탈취하는 스미싱”[4]이 대표적이다.

피싱 수법은 더욱더 진화하여 “메신저로 연결된 피싱 사이트를 통해 수집한 개인정보(계좌번호, 비밀번호, 금융 보안 카드번호 등)를 이용하여 예금을 불법으로 인출하는 2세대 피싱”, 최근 카카오톡(Kakao Talk) 또는 인스타그램(Instagram) DM(Direct Message)을 활용하는 메신저피싱으로 범죄 수법이 진화하였고, 경품 전달을 빙자한 사이트 접속을 유도하여 개인정보 등을 편취하는 수법이 속속 등장하고 있다. 이 밖에도 파밍이 변화된 수법인 악성 프로그램을 PC에 설치해서 피해자의 인터넷뱅킹 프로세스에 직접 개입하여 정상적인 최소한의 금융정보만 얻는 메모리해킹[5], 스카이프 또는 텔레그램 등의 SNS를 통해 음란 화상 채팅을 하자고 접근하여 상대방의 음란행위를 녹화 및 apk 파일 설치를 요구하여 해당 영상을 지인들에게 유포한다고 협박하면서 금전을 갈취하는 몸캠피싱[6] 등이 대표적인 유형이다.

한편, 보이스피싱 범죄의 경우 국내에 (이동식) 변작 중계기 및 SIM 박스를 설치하거나, 국내 이동통신 전화에 가입된 스마트폰의 ‘전화 및 문자메시지 연동’ 기능 등을 이용하여 외국에서 전화나 문자메시지를 발송했음에도 국내 이동통신을 이용한 것처럼 가장하는 수법[7]이 나타나고 있다. 또한 수사목적의 앱 설치를 요구하거나, 오픈뱅킹·간편송금을 이용한 피싱 등 수법이 점점 다양해지고 있다.

최근의 피해 유형은 개인정보를 탈취하는 수법과 연관되어 있다. 과거에는 가족이나 지인을 사칭하여 메신저 피싱을 통해 개인정보를 탈취하는 경우가 많았으나, 최근에는 문자나 카카오톡 등을

1) 윤해성 외, “보이스피싱 피해유형별 구체적 예방방안에 관한 연구”, 대검찰청 연구용역 보고서, 2017., p.3.
2) 김민정·김은미, “보이스피싱 피해 경험 및 영향요인 분석”, 소비자문제연구 제52권 제1호, 2021.04., p.4.
3) 윤해성 외, “보이스피싱 범행단계별 대응방안 연구”, 한국형사법무정책연구원, 2023.09.10., p.91.
4) 김동민, “접근매체를 이용하는 전자금융사기의 범위에 관한 소고“, 법학연구 제31권 제2호, 2020.05., p.63-64.
5) 윤해성 외, “보이스피싱 범행단계별 대응방안 연구”, 한국형사법무정책연구원, 2023.09.10., p.12.
6) 윤해성 외, “보이스피싱 범행단계별 대응방안 연구”, 한국형사법무정책연구원, 2023.09.10., p.14.
7) 발신번호 변작 중계기(SIM box)는 국제전화의 경우 발신번호를 010 또는 국내 지역번호로 변경하도록 하는 수법이다(부산지방법원, 2022고단4239 판결, 2023.03.13.)

통해 지인으로 속여 개인정보 및 인증 정보를 요구하는 수법이 증가하고 있다. 또한 대출 문자를 보내 개인정보(신분증, 카드)를 송부하도록 하거나, 악성 앱을 설치하도록 하는 방식, 택배·정부지원금 등 관련 문자를 통해 출처가 불분명한 URL 클릭하도록 하는 방식도 빈번하다. 나아가 금융상품 거래 확인서 피싱처럼 투자성 금융상품 거래 내역을 조작하거나, 거래 관련 고객센터 전화번호로 전화를 유도하는 수법 등 피싱 범죄는 교묘해지고 대담해지고 있다.[8)]

3. AI 기반 음성합성·딥페이크를 이용한 신종 보이스피싱 수법 분석 및 피해 실태

2021년 아랍에미리트에서는 은행 임원의 전화를 받고 3,500만 달러를 송금했으나, 전화 상대방은 은행 임원이 아닌, 딥보이스로 만들어진 목소리였다.[9)] 캐나다에서도 손자의 목소리를 복제하여 교통사고로 유치장에 있고, 보석금이 필요하다고 기망하여 900만 원을 송금할 뻔한 사건이 발생한 것과 같이[10)] 해외에서는 이미 딥페이크를 활용한 피싱 범죄가 다수 발생하고 있다. 최근 우리나라도 AI를 이용한 보이스피싱 범죄가 증가하고 있으며, AI로 영상과 음성 위조로 2025년 상반기에만 6,421억 원의 피해가 발생하는 등[11)] AI를 기반으로 딥페이크와 딥보이스 기술까지 이용한 범죄 수법이 등장하고 있다.

이처럼 우리나라에서도 AI 기술을 통해 딥페이크와 같은 최신 기술을 활용하는 피싱 범죄가 심심찮게 발생하고 있는 것을 확인할 수 있다. 예컨대 특정인의 음성을 합성하여 그 음성을 특정 사실(예: 범죄나 금융거래 내역)과 결합함으로써 신뢰를 획득하거나 이를 빌미로 위협할 수 있다. 또한 딥페이크로 특정인의 얼굴과 음성을 결합해 화상통화를 가장하면서 사기행각을 벌이는 사례도 가능하다. AI는 기존 보이스피싱 수법을 고도화하고 피해를 확산시킬 우려가 있다. 즉, AI 기술을 이용하여 가족·친구의 음성을 단기간의 통화로도 분석해 음성 패턴을 도출하거나 유명인 등의 음성을 합성·딥페이크 음성을 생성하게 하고, AI 기반 음성인식 시스템이 대량의 전화를 자동으로 처리하거나 특정 패턴을 학습해 피해자와의 대화를 유도할 경우에는 적은 비용과 인원으로 다수의 피해자가 발생할 수 있다.[12)]

나아가 보이스피싱 범죄가 시대 상황에 맞게 맞춤형 시나리오를 통해 피해자를 속일 수 있다. 다시 말해서 AI를 통해 음성, 톤, 감정 상태, 언어 사용 패턴 등을 분석하여 정교한 보이스피싱 스크립트를 생성한다면 피해자는 쉽게 기망당할 수 있게 된다. 실제로 AI 음성합성 수법은 단 3초 분량의 음성으로도 특정인의 음성을 완벽하게 복제할 수 있으므로 기존 보이스피싱, 스미싱 등의 사기행각보다 더 신뢰성이 높아 피해자들이 쉽게 속을 수 있다. 더구나 얼굴과 음성까지 딥페이크

8) 윤해성, 보이스피싱 범행단계별 대응방안 연구, 한국형사법무정책연구원, 2023.09.10., p.93.
9) 머니투데이, “목소리 소름주의“...400억 가로챈 ‘딥보이스 범죄’ 檢도 나섰다.”, 2023.02.11.
10) 중앙일보, ““보증금 도와줘”영통까지 한 친구···‘딥보이스’피싱에 당했다”, 2023.06.18.
11) 조선일보, “보이스피싱 그놈 옆에 AI...한국 1조 낚였다”, 2025.07.16.
12) 이근우, AI 시대와 형사법의 대응, 가천법학 제18권 제1호, 2025.03., p.55.

화 한다면 현재의 보이스피싱보다 훨씬 더 많은 피해가 나타날 것은 자명한 일이다.

4. 탐지 및 대응 관련 정책 및 법제도 개선 방향

진화하는 피싱 범죄 대응에 있어서 정부는 통합신고·대응센터를 만들어 대응하고 있으나, 명실상부한 보이스피싱 예방 및 대응 기관으로 거듭나려면 신고접수에서 신속한 대응이 함께 이루어질 필요가 있다. 이에 부처 간 매우 긴밀한 협력이 필수적인 만큼 현재의 통합신고·대응센터의 인력과 규모를 확대하고, 더불어 AI 기반 피싱 범죄에 대응하기 위한 노력이 수반되어야 한다. 특히, 보이스피싱 범죄의 음성데이터의 경우 AI를 기반하여 특정 범죄자를 매칭할 수 있도록 하는 등 AI 기반의 탐지 시스템을 강화하여 보이스피싱 여부를 탐지하고 실시간 모니터링할 수 있는 시스템을 구축하는 것도 고려해야 한다.

최근 AI 기반 음성합성과 딥페이크를 이용한 신종 범죄가 나타남에 따라 법적으로는 개인정보의 범위에 음성을 포함해야 하는지에 대한 논의와 관련하여, 현행 개인정보 보호법에서는 개인정보를 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보로만 한정하고 있다. 물론 음성 정보 역시 개인정보 보호법 제2조 제1호에 따르면 다른 정보와 쉽게 결합하여 개인을 식별할 수 있다면 개인정보에 포함하게 된다. 그러나 개인정보 보호법상 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공해서는 안 된다고 규정하고 있어 음성이라는 개인정보를 어느 범위까지 활용할 수 있는지가 문제가 된다.

그러나 개인정보 보호법 제18조 제2항 제2호 다른 법률에 특별한 규정이 있거나, 제18조 제2항 제3호 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우, 제18조 제2항 제7호 범죄의 수사와 공소제기 및 유지를 위하여 필요한 경우 등이 예외 사유에 해당하게 되어 음성정보를 활용할 수 있게 된다. 또한 개인정보 보호법 제28조의2에서는 가명정보 처리와 관련된 규정이 있는데, 이에 대하여 헌법재판소는 통계 작성, 과학적 연구[13], 공익적 기록보존 등이라는 공익적 목적이 법익의 균형성 면에서 크기 때문에 정보주체의 동의 없이 처리할 수 있다고 판시하였다.[14] 그리고 동법 제28조의4에서는 개인정보처리자에 대하여 안전성 확보를 위한 각종 조치를 취하도록 규정하고 있다.

아울러 피싱 범죄 예방을 위한 음성 정보 활용에 대하여 개인정보보호위원회는 사전적정성 검토

13) 여기서 "과학적 연구"란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말하므로(제2조 제8호), 신설된 개인정보 조항은 데이터 관련 신산업 육성이 범국가적 과제로 대두되고 있는 현실을 고려하여 인공지능, 클라우드, 사물인터넷 등 신기술을 활용한 데이터 이용이 필요한 상황에서 데이터의 이용을 활성화하고자 하는데 그 입법취지가 있다고 헌법재판소가 밝히고 있다(헌법재판소, 선고 2020헌마1476 결정, 2023.10.26.)

14) 헌법재판소, 선고 2020헌마1476 결정, 2023.10.26.

제 등을 통해 현행법 내 규제 리스크를 신속하게 해소하고 규제샌드박스 제도 등 강화된 안전조치를 전제로 특례를 마련해야한다는 입장이다. 기존에는 통신 3사를 대상으로 소형언어모델(sLM)을 활용해 '통화 문맥(시나리오)'을 분석하여 실시간 AI 보이스피싱 위험을 탐지하는 서비스와 더불어 보이스피싱 범인의 목소리와 통화 상대방 간 목소리 대조(화자 음성 인식)기술을 활용하여 보이스피싱 범인의 목소리와 일치하는 목소리를 탐지하는 다중 보이스피싱 탐지 서비스 출시 지원 등의 실증 특례를 허용하였다. 이때 서비스의 공익성 등을 고려하여 보이스피싱 범인의 음성 원본을 AI 학습에 활용할 수 있도록 통신사의 서비스 구조, 데이터 처리 흐름, 법 적용 관계 등을 검토하여 강화된 안전조치 등을 전제로 실증특례 이행점검을 완료하였다. 나아가 통신사-금융권과 연계하여 보이스피싱 통화 패턴 분석 기반의 AI 모델을 구축하고 이를 통해 보이스피싱 의심번호 추출 및 이상거래 탐지·차단에 활용하는 서비스에 대한 사전적정성 검토를 허용하였다. 그러나 이러한 규제샌드박스 제도는 임시방편적 해결책에 불과하며 안정적·장기적 데이터 활용과 국민의 권리 보호를 위해 개인정보 보호법 내 특례 제도를 마련할 필요가 있다. 이에 개인정보보호위원회는 보이스피싱 예방과 같이 공익 · 사회적 이익을 위한 경우로서 정보주체의 이익 침해 가능성이 낮을 경우 보이스피싱 범인의 음성 원본을 AI 학습에 활용하는 것을 허용하는 등의 내용을 내포한 'AI 특례'를 신설하기 위한 개인정보 보호법 개정을 추진하고 있다.

한편, 현재 금융기관에서는 '이상금융거래탐지시스템(Fraud Detection System, FDS)'[15]을 구축하여 시행하고 있는 만큼 AI를 기반으로 한 음성합성이나 딥페이크의 경우에도 진위 여부를 판명할 수 있는 AI 탐지 시스템을 마련하여 피싱 범죄를 방지해야 한다. 가령, AI를 활용하여 발신자의 음성데이터를 분석하거나, 딥러닝 기술을 이용하여 피싱 범죄 위치 정보를 분석하여 범죄 여부를 판별한다면 상당한 피싱 범죄를 예방할 수 있게 된다. 아울러 통신회사의 경우 보이스피싱 범인과의 통화 시 AI로 하여금 범죄자의 음성을 분석하도록 하여 이용자에게 경고 알림을 주거나 수사기관에 연결시키는 방법도 고려될 수 있는데, 통신회사가 자체적으로 통화 중 AI 탐지 서비스를 활용한다거나 AI 앱을 활용하는 것을 고려해 볼 수 있다.

또한, AI 기반 탐지 시스템을 마련하기 위한 전제조건으로 많은 양의 음성데이터를 빅데이터화하거나 음성데이터를 텍스트화하여 이를 분석한 다음 수사기관과 통신회사, 금융기관과 협조하는 시스템도 마련해야 한다. 특히, 음성데이터의 경우 실제 음성으로 개인을 특정할 수 있을 뿐만 아니라 딥러닝 기술을 활용하여 패턴 분석을 통하여 피싱 범죄 여부 또한 확인할 수 있다. 실제로 경찰청은 '전화사기 수사 지원 시스템'을 개발하여 보이스피싱 음성분석 기술과 수사기법에 적용하고 있다. 이처럼 보이스피싱 범죄자와 의심되는 용의자의 음성을 AI로 하여금 분석한다면 시간과 인력은 줄이면서 효과적인 대응이 가능하다. 따라서 피싱 범죄에 대응하기 위해서는 AI를 활용한 탐지기술이 수반되어야 하며 이를 위해선 기술개발과 함께 관련 법제도 마련은 필연적이다.

15) 금융권에서 보이스피싱 범죄 대응과 관련해서 의심 거래를 탐지하여 금융회사의 이상금융거래 담당자에게 알림을 보내는 방식으로 2022년 모든 은행에서 시행하고 있다.

5. 나가며

보이스피싱은 전화로 피해자를 기망하여 금전을 편취하는 범죄 수법이다. 최초 발생한 이후, 파밍, 스미싱, 메신저 피싱 등 범죄 수법이 등장한 이후에도 피싱사이트를 이용한 범죄, 팝업창에 접속하게 하는 등 수법이 조금씩 변화하고 있다. 최근 문제된 대출 사기형의 경우 범행 대상이 미끼 문자 등을 발송하여 불특정 다수의 개인정보 탈취 후 송금을 유도하였다. 또한 피해자에게 대출 신청서 앱을 설치하도록 하고 카카오톡 친구를 맺은 다음 악성 앱을 설치하도록 하여 스마트폰 상의 모든 개인정보가 범죄자에게 넘어가는 등 기술의 발전에 따라 보이스피싱 범죄 수법도 계속적으로 진화하고 있다. 그동안 정부는 피싱 범죄 예방과 대응을 위해 범정부 차원에서 관련 정책과 법제도를 마련하여 해결해 왔었다.

그러나 최근 AI 기반 음성합성과 딥페이크를 활용한 피싱 범죄가 등장함에 따라 법률상의 허점과 정책상의 사각지대가 나타나게 되었다. AI 기반 음성합성과 딥페이크 피싱 범죄는 기존 보이스피싱과는 다른 또 다른 형태의 정밀하고 정교한 범죄 수법이다. 이에 따라 범정부 차원에서 전문가와의 협력을 통해, 진화하는 피싱 범죄에 대응할 수 있도록 AI 기반 탐지 시스템 구축과 관련 법제도 및 정책을 조속히 마련할 필요가 있다.

참고 문헌 |

1. 윤해성 외, “보이스피싱 피해유형별 구체적 예방방안에 관한 연구”, 대검찰청 연구용역 보고서, 2017.
2. 김민정·김은미, “보이스피싱 피해 경험 및 영향요인 분석”, 소비자문제연구 제52권 제1호, 2021.04.
3. 윤해성 외, “보이스피싱 범행단계별 대응방안 연구”, 한국형사법무정책연구원, 2023.09.10.
4. 김동민, “접근매체를 이용하는 전자금융사기의 범위에 관한 소고“, 법학연구 제31권 제2호, 2020.05.
5. 부산지방법원, 2022고단4239 판결, 2023.03.13.
6. 머니투데이, “목소리 소름주의“...400억 가로챈 ‘딥보이스 범죄’ 檢도 나섰다.”, 2023.02.11.
7. 중앙일보, ““보증금 도와줘”영통까지 한 친구···‘딥보이스’피싱에 당했다”, 2023.06.18.
8. 조선일보, “보이스피싱 그놈 옆에 AI...한국 1조 낚였다”, 2025.07.16.
9. 이근우, AI 시대와 형사법의 대응, 가천법학 제18권 제1호, 2025.03.
10. 헌법재판소, 선고 2020헌마1476 결정, 2023.10.26.

보안 사고 사례와 개인정보 유출

배상민
이스트시큐리티 시큐리티 대응센터 I 실장

1. 들어가며

사이버 공격은 시대의 기술적·사회적 흐름을 반영하며 끊임없이 변화해 온 진화적 현상이다. 오늘날 공격자들의 전술은 상상을 초월하는 수준으로 고도화되었으며, 시스템 내의 사소한 취약점이나 보안 통제의 작은 간극조차 대규모 사회적 파장과 직결되는 사고를 초래하고 있다. 금전적 이익, 핵심 정보 수집, 서비스 마비, 정치적 영향력 행사 등 복합적인 목적성을 가진 이들의 공격 방법론은 끊임없이 진화해 왔으며, 이제는 인공지능(AI)을 활용한 지능형 공격이 주류로 포착되는 시점에 이르렀다.

과거 사이버 공격의 주요 표적이었던 개인 사용자(Individual Users) 중심의 공격 흐름을 되짚어 보면, 초기의 애드웨어(Adware)[16]나 온라인 게임 계정을 노린 정보 탈취형 악성코드들이 주를 이루었으며 랜섬웨어(Ransomware)[17]가 처음 등장했을 시기에도 주요 타겟은 개인 디바이스였다. 물론 이 시기에도 기업 및 국가 기관에 대해 크고 작은 보안 사고가 발생했으나, 근래의 공격 양상을 분석하면 그 양상이 확연히 달라졌음을 알 수 있다.

최근 몇 년간의 사이버 공격을 분석해 보면, 주요 기업과 국가 핵심 기반 시설을 향한 공격으로 전략적 전환되었으며 개인 이용자를 대상으로 하는 공격은 이러한 대규모 공격을 위한 시작점이 될 수 있는 주요 인물 혹은 그 대상을 향한 공격으로 변환되었다. 이는 공격의 목적성을 미루어 볼 때, 개인 이용자 중심의 공격보다 훨씬 높은 경제적 가치와 전략적 정보력을 내포하고 있는 조직의 자산을 노리는 것이 효율성이 높다고 판단하기 때문이다.

최근 언론 보도를 통해 확인되는 주요 보안 사고 사례에서 알 수 있듯이, 이제 대부분의 사이버 공격은 개인이 아닌 조직을 표적으로 하는 '대규모 위협'으로 자리매김했다. 더욱 중요한 점은 이 피해가 단순히 특정 기업에 국한되지 않는다는 사실이며 해당 기업의 서비스를 이용하는 수많은 일반 이용자 또한 개인정보 유출, 서비스 중단 등의 간접적인 피해를 보게 된다는 것이다. 이는 사이버 공격이 개별 조직의 문제를 넘어 사회 전체의 신뢰 시스템과 안정성을 위협하는 수준에 도달했음을 의미하며, 사이버 보안에 대한 사회적 경각심이 최고조에 달하는 시대적 배경이 되고 있다.

16) 사용자 컴퓨터나 모바일 장치에 설치되어 원치 않는 광고를 자동으로 표시하거나 다운로드하도록 설계된 소프트웨어
17) '몸값(Ransom)'과' 소프트웨어(Software)'의 합성어로 이는 사용자의 컴퓨터 시스템 접근을 막거나, 내부 파일을 암호화하여 이용할 수 없게 만든 뒤, 이를 복구하는 대가로 금전을 요구하는 악성코드의 한 종류였으나, 코인을 통한 몸값 지불과 함께 맞물려 폭발적으로 증가하고 고도화되어 오늘날에 보안 위협의 한 축으로 자리 잡게 되었다.

이 글은 최근 발생한 대형 사건들 속에서 우리가 간과하고 있는 핵심 교훈이 무엇인지, 그리고 우리의 방어 체계에 어떤 관점을 도입해야 하는지 논하고자 한다.

2. 최근 주요 보안 사고 사례

매년 발생하는 보안 사고 사례들을 분석하는 것은 해당 기간의 공격 동향과 산업별 취약점 노출 영역을 명확히 파악하는 핵심적인 방법론이다. 최근 수년간의 공격 기록을 살펴보면, 금융, 제조, 유통 등 핵심 산업군 전반에서 새로운 공격 방법론이 동원된 것처럼 보인다.

그러나 이러한 현상을 본질적 관점에서 해체하여 분석하면, 공격자들의 전술은 '고도화'되었을 뿐, 실제로 활용된 핵심 기법들은 기존에 이미 알려진 공격 메커니즘을 재활용하거나 복합적으로 결합한 경우가 대다수이다. 이의 가장 대표적인 사례로 랜섬웨어 공격을 들 수 있으며 랜섬웨어는 감염경로와 암호화 방법을 혁신하며 진화하여, 최종적으로는 '데이터 암호화를 통한 금전 요구'에 이어 데이터 유출이라는 행위 구조로 발전되었다. 국내에서 랜섬웨어 공격이 본격적으로 확산되던 시기, 다양한 감염 방식이 관찰되었으나 대부분 스피어피싱(Spear phishing)[18]을 통한 개인 PC 감염이 주를 이루었다. 공격은 주로 개인 문서나 사진 파일 등을 암호화하고 몸값(Ransom)을 요구하는 형태로 이루어졌으며, 그 피해자 수는 상당했다. 그러나 이후 서비스형 랜섬웨어(Ransomware as a Service, RaaS) 모델의 등장과 암호화 기능의 고도화가 맞물리면서 공격의 전략적 목표가 전환되었다고 볼 수 있다. 공격자들은 더 높은 경제적 가치 실현과 더불어 핵심 정보 탈취라는 두 가지 목적을 달성하기 위해 개인보다는 기업을 표적으로 하는 공격으로 그 전술을 집중적으로 변화시켰다. 이로써 랜섬웨어는 단순히 금전을 요구하는 위협을 넘어, 데이터 유출 및 기업 운영 마비를 초래하는 고도화된 침해 행위로 진화한 것이다.

2025년에도 국내에서 랜섬웨어 공격 사례는 끊이지 않았으며, 특히 예스24(YES24), SGI서울보증보험, 그리고 자산관리업계를 겨냥한 대형 침해 사고들이 발생했다. 이는 랜섬웨어가 여전히 기업 보안의 최대 위협임을 방증한다. YES24 사례에서는 6월과 8월 사이 두 차례에 걸친 연속적인 공격으로 각각 5일과 7시간의 서비스 중단이 초래되어, 일반 이용자들이 해당 서비스를 이용하지 못했으며, 수십억 원의 매출 손실이 보도되었다. SGI서울보증보험 공격에는 Gunra 랜섬웨어가 사용되었는데, 이는 기존에 발견된 Conti 랜섬웨어의 소스코드를 기반(약 25%의 구조적 유사성)으로 제작된 것으로 파악되었다. 해당 랜섬웨어는 이중 암호화 구조(ChaCha20 + RSA-2048)를 특징으로 하며, SSL-VPN[19] 장비에 대한 SSH Service[20] 무차별 대입 공격(Brute-force Attack)이

18) 특정 개인, 그룹, 또는 조직을 표적으로 삼아 이메일(E-mail)을 전달하여 정보 탈취 및 악성코드를 유포하는 사회공학적 방법의 한 종류
19) 웹 브라우저를 이용해 회사 내부망에 안전하게 접속할 수 있도록 데이터를 암호화하는 기술

병행되어 시스템 마비와 함께 약 13TB의 데이터 유출이 발생했다.

자산관리업계 침해 사례 역시 그 양상이 복합적이었다. 공통 IT 서비스 제공업체를 통해 다수의 자산운용사를 동시에 침해했을 것으로 유추하고 있으며, 1.024TB의 데이터 유출이라는 막대한 피해를 입혔다. 공격에는 AES-256, ChaCha20 등의 고급 암호화 기법이 동원되어 중소 사모펀드의 핵심 자료가 암호화되었고, 클라우드 서버 해킹까지 연속적으로 이어졌다. 이러한 사례들은 원격 접속 서비스 악용, 사회 공학적 기법, 공급망을 통한 다중 표적 공격 등 복합적인 침투 및 확산 전술이 채택되었음을 보여준다. 공격의 전술적 부분은 다양하지만, 금전적 요구, 기업 자산 탈취 및 서비스 마비라는 궁극적인 목적은 동일하며, 랜섬웨어가 기업 입장에서 가장 경계해야 할 사이버 공격 1순위임을 명확히 시사한다.

또한 국내 주요 이동통신사에서 연이어 발생한 대규모 보안 사고는 단순한 기업의 문제가 아니라, 국가 기간망의 안정성과 국민 생활의 근간을 위협하는 중대한 사안임을 시사한다. 외부 소프트웨어의 관리적 미흡, 내부적인 보안 구조의 취약점이 복합적으로 작용하여 특정 악성코드를 설치한 고도화된 지능형 지속위협(Advanced Persistent Threat, APT) 공격으로 확인된다. 이동통신사의 보안 사고는 단순히 데이터 유출을 넘어, 국가적 재난으로 이어질 수 있는 체인 리스크를 내포한다. 특히 유심 인증키(Ki) 관리 부실 등에서 드러나듯이 보안의 기본 원칙마저 훼손된 현실은 심각한 경고음을 울린다. 따라서 이제는 보안을 비용이 아닌 국가 인프라의 핵심 투자로 인식하고, 전면적인 방어 체계 재정립에 착수해야 할 시점이다.

3. AI를 활용한 공격의 지능화

AI의 등장으로 사이버 보안 생태계는 근본적인 패러다임 전환(Paradigm Shift)이 이루어지고 있다. 사이버 공격과 AI의 융합은 공격적 전술의 고도화가 이루어졌으며 공격의 속도, 규모, 정교함 등의 큰 발전을 이루게 되었고 과거 고도의 전문 지식이 필요했던 맞춤형 악성코드 제작이나 제로데이(Zero-day)[21] 취약점 분석이 이제 대규모 언어모델(Large Language Model, LLM)[22] 기반의 도구를 통해 비전문가 수준에서도 대규모로 자동화되어 공격자들에게 AI는 강력한 무기가 되어 보안 기술의 변화와 패러다임의 전환이 필요한 시기가 되었다.

AI 기반 사이버 위협 중 특히 주목해야 할 것은 생성형 AI를 이용한 사회공학적 공격 방법의

20) Secure Shell (보안 셸) 프로토콜을 사용하여 네트워크상의 다른 컴퓨터에 안전하게 원격으로 접속하고 명령을 실행하거나 파일을 전송할 수 있도록 하는 서비스
21) 소프트웨어 또는 하드웨어의 개발자나 공급업체에게 아직 알려지지 않았거나, 알려졌더라도 공식적인 보안 패치가 나오지 않은 상태의 보안 취약점
22) 방대한 양의 텍스트 데이터와 수십억 개의 매개변수를 사용하여 학습된 딥러닝 기반의 인공지능 모델

고도화라고 볼 수 있다. 최근 사례들을 보면, 해커들은 AI 이미지 생성 기술을 활용한 딥페이크 스캠 영상 혹은 공격 대상의 관심사나 직무와 관련된 매우 정교하고 그럴듯한 이미지를 첨부하여 피싱 메일을 발송하는 스피어 피싱 공격이 자주 목격되고 있다. 이러한 스피어 피싱 공격은 일반적인 피싱 메일과 달리 공격 대상이 경계를 풀도록 유도하며, 특히 특정 산업 분야의 연구원이나 임원 등을 겨냥하는 타겟형 공격(Targeted Attack)에서 그 성공률을 높이고 있다. AI가 만든 이 '미끼'는 시각적 신뢰도를 확보함으로써, 악성 링크 클릭이나 중요 정보 유출을 유도하는 데 치명적인 효율성을 발휘한다. 스피어 피싱은 기술적 취약점이 아닌 인간 요소, 즉 심리적 및 인지적 취약성을 핵심 공격 경로로 삼는다. 특히 AI에 의해 개인화된 스피어 피싱 공격은 공격 대상자의 신뢰를 조작하고 긴급성, 권위, 호기심 등의 심리적 원리를 악용하여 보안 통제를 우회한다. 이러한 공격은 기술적 탐지 난이도가 높을 뿐만 아니라, 최종적으로 조직 내 가장 취약한 고리(임직원·협력업체·이용자 등)를 통해 침투함으로써 정보 유출 및 시스템 장악의 성공률을 극대화한다.

AI를 활용한 사이버 공격은 단순한 기술적 진화를 넘어 인간의 심리적 취약성까지 공격 경로로 활용하며 보안 위협의 근본을 변화시키고 있다. 이에 대한 대응 역시 AI를 활용한 선제적 위협 예측과 적응형 방어 체계의 전환이 필요한 시점으로 판단되며 기술 혁신과 함께 조직 내 임직원의 지속적인 보안 인식 재고만이 유일한 생존 전략이 될 것이다.

4. 보안 사고와 개인정보 유출에 대한 방어 전략 및 개선 방안

사이버 공격에 대한 효과적인 개인정보 유출을 방지하기 위한 방어 전략은 기술적, 관리적, 인적 요소라는 세 가지 핵심 구성 요소로 이루어져야 한다.

첫째, 기술적 방어 전략과 시스템 개선이 필수적이다. 단순한 시그니처 기반의 정적 방어에서 벗어나, 인공지능과 머신러닝(Machine Learning, ML)을 활용하여 선제적 탐지 및 대응이 가능한 위협 인텔리전스 솔루션을 도입해야 한다. 이와 함께, 제로 트러스트 아키텍처(Zero Trust Architecture)를 적용하여 모든 접근을 엄격하게 검증하는 체계를 확립해야 한다. 또한, 최근 문제가 되는 공급망 공격(Supply Chain Attack)[23]에 대비하여 지속적인 취약점 관리 및 보안 패치 평가를 의무화하고, 민감 정보에 대한 강력한 데이터 보호(암호화 및 비식별화)를 필연적으로 적용해야 한다.

둘째, 관리적 및 정책적 개선 방안이 병행되어야 한다. 서비스형 소프트웨어(Software as a Service, SaaS)나 외부 협력사 등 공급망 전체에 대한 보안 실사(Due Diligence)를 의무화하고, 계약 단계에서 명확한 보안 요구사항(Service Level Agreements, SLAs)을 명시하여 외부 리스

23) 공격할 특정 대상이 신뢰할 수 있는 외부 협력업체나 소프트웨어를 침투 경로로 악용하는 사이버 공격 방식

크를 체계적으로 통제해야 한다. 침해 사고 발생 시에는 신속하고 체계적인 대응을 위한 위협 대응 체계(Computer Security Incident Response Team, CSIRT)를 확립하는 것이 핵심이다. 아울러, 개인정보보호책임자(Chief Privacy Officer, CPO) 및 담당 부서의 독립적인 감사 권한과 예산 집행 권한을 보장하고, 법규 준수를 최우선 과제로 설정하는 조직 문화의 정착이 필요하다.

마지막으로, 보안 문화 개선이 수반되어야 한다. 매뉴얼 위주의 형식적인 교육 대신, AI 기반 스피어 피싱 등 최신 공격 기법을 모방한 모의 훈련(Phishing Simulation)을 정기적으로 실시하는 등의 보안 인식 제고 교육이 필수적이다. 또한, 내부 위협 통제 시스템을 운영함과 동시에, 보안 규정 준수나 위협 보고에 대해 보상 및 긍정적인 피드백을 제공함으로써, 보안을 '규제'가 아닌 '모두의 책임이자 업무의 일부'로 인식하는 문화를 조성하는 것이 가장 중요하다고 판단된다.

모든 기업과 이용자의 입장에서 보안 사고의 여파는 더 이상 먼 뉴스 속 이야기가 아닌, 나의 개인정보 또는 기업 기밀과 핵심 시스템에 직접적인 영향을 미치는 실질적인 위협으로 자리매김하였다. 이러한 고도화된 공격에 대비하기 위한 새로운 전략과 개선 방안을 필두로, 보안을 단순한 관리 영역이 아닌 기업 경영의 핵심 축으로 재편하는 근본적인 전략 전환이 절실한 시기로 판단된다.

참고 문헌 |

1. GENIANS Inc. Blog, Gunra 랜섬웨어 분석 보고서, 2025.07.25.
2. AhnLab Security Emergency Response Center, 2025년 9월 국내외 금융권 관련 보안 이슈, 2025.10.17.
3. GENIANS Inc. Blog, Qilin Ransomware 분석, 2025.10.28.
4. 매일경제, Companies preyed on hackers, individuals suffering from terrorist threats…, 2025.08.11.
5. 보안뉴스, [SGI서울보증 랜섬웨어] 공격 배후 추정 '건라', 어떤 조직이길래?, 2025.07.16.
6. 보안뉴스, [SGI서울보증 랜섬웨어] 13.2T 규모 SGI 데이터 '매물'로 나왔다…"후폭풍 심각", 2025.08.05.

다크웹과 개인정보 불법유통 현황 및 대응 전략

김재기
S2W 위협 인텔리전스 센터(TALON) I 센터장

1. 서론: 개인정보 불법유통의 전략적 위협 재정의

1) 배경 및 목적

2025년 최근 사이버 위협 환경에 대응하기 위해서는 과거처럼 침해 사고를 단발적인 이슈로 바라보는 것이 아닌, 전문화된 지하 경제 생태계를 통해 유기적으로 결합된 형태로 진화하고 있다는 점을 이해할 필요가 있다. 이 생태계의 핵심에는 언더그라운드 포럼 및 히든 마켓을 통해 유출되는 데이터의 불법유통 및 상업화가 자리 잡고 있다.

이러한 위협은 단순히 개인의 피해를 초래하는 것을 넘어, 전 세계적으로 2025년까지 12조 $(USD)에[24] 달하는 천문학적인 경제적 손실을 야기할 것으로 전망되며,[25] 이는 개인정보 유출을 국가 안보 및 경제 시스템에 대한 전략적 위협으로 재정의할 필요가 있다.

본 보고서는 개인정보 관련 정책 담당자 및 기업 내 개인정보 담당자를 대상으로, 개인정보 불법유통 생태계의 복잡성, 유출 정보의 악용을 통한 2차 피해의 심각성, 그리고 이러한 위협을 선제적으로 방어하기 위한 다층적 정책 및 기술 전략을 제시함으로써, 전략적 의사결정을 지원하는 데 목적이 있다.

2) 2025년 다크웹 환경: 복원력과 전문화 현황

다크웹은 전체 인터넷상 작은 비중 대비, 그 영향력은 기하급수적으로 증가하고 있다. 2025년 초 기준으로 일일 Tor(The Onion Router) 네트워크 이용자가 200만 명에서 300만 명 이상으로 증가하는 등 이용자 기반이 지속적으로 확장되고 있다. Tor 네트워크와 다크웹 이용이 모두 사이버 범죄에만 국한되는 것은 아니지만, 이러한 성장은 사이버 범죄 활동의 규모 확대를 의미하며, 지하 경제 내에서 특히 데이터 거래 시장이 주류를 이루고 있다. 특히 탈취당한 자격 증명(Credentials)은 히든 마켓 거래의 약 2/3를 차지할 정도의 핵심 상품이다.

주목할 점 중 하나는 다크웹 시장의 높은 복원력(Resilience)이라는 특성이다. 법 집행기관에

24) Help Net Security, Ransomware groups are multiplying, raising the stakes for defenders, 2025.08.26.
25) DeepStrike, Dark Web Statistics 2025: Trends, Usage, and Security Insights, 2025.10.19.

의한 국제 공조 및 수사의 결과, 2022년 Hydra 마켓 단속[26]이나 2025년 Operation Rap Tor와[27] 같은 국제적인 법 집행 활동에도 불구하고, Abacus Market처럼 새로운 대형 마켓이나 특화된 포럼이 단속의 공백을 빠르게 커버하며 활동을 재개하는 현상이 관찰되고 있다.[28] 이러한 음성적인 시장들은 Tor, 가상자산, 에스크로(Escrow) 시스템을 활용하여 높은 익명성과 거래의 신뢰를 유지함으로써 지속성을 확보한다. 대표적인 예로, 각종 공격 도구 및 서비스형 랜섬웨어(Ransomware-as-a-Service, RaaS) 모델의 확산은 사이버 범죄의 진입 장벽을 낮추고, 유출된 개인정보를 활용한 대규모 공격을 용이하게 하고 있다.

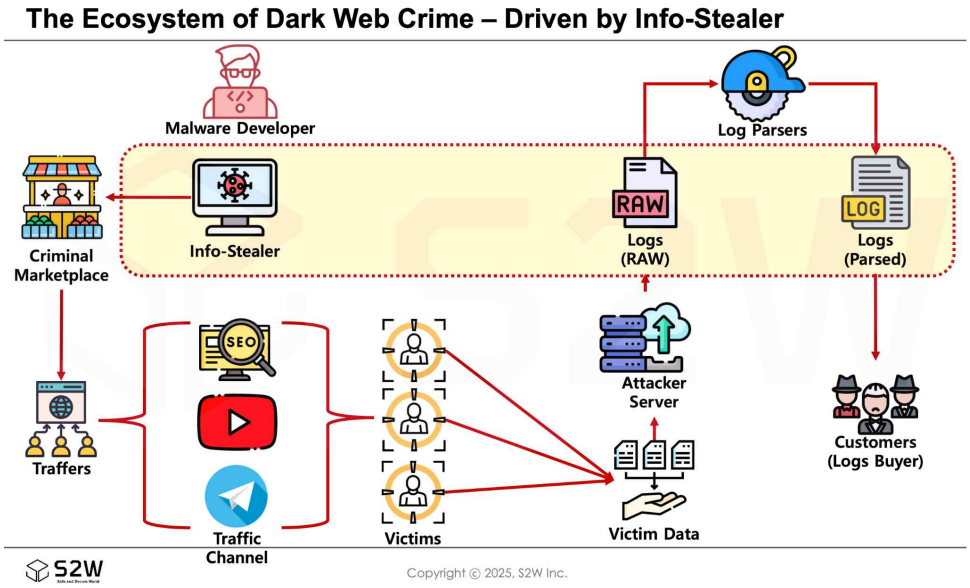
2. 개인정보 불법유통 생태계 분석

1) 데이터 유출 출처 및 영향도 파악

① 정보탈취형 악성코드(Info-stealer) 생태계와 데이터 탈취

유출된 개인정보의 가장 광범위하고 위험도가 높은 출처는 정보탈취형 악성코드(Info-stealer, 이하 인포스틸러) 생태계이다. 이 악성코드는 개인 이용자의 PC나 단말에 설치되어 검색 이력, 캐시 파일, 가상자산 지갑 정보, 쿠키 파일 등과 같은 이용자의 민감 데이터를 훔친다.

그림1 인포스틸러가 주도하는 다크웹 범죄 생태계



26) U.S. Department of Justice (DOJ), Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace, 2022.04.05.
27) European Union Agency for Law Enforcement Cooperation, 270 arrested in global dark web crackdown targeting online drug and criminal networks, 2023.05.02.
28) DeepStrike, Top 7 Dark Web Marketplaces of 2025: Inside the Underground Economy, 2025.10.07.

해당 생태계는 고도로 분업화되어 있다. 인포스틸러 개발자는 악성코드를 제작하고, 많은 감염자가 생길 수 있게 개발된 스틸러를 각종 채널로 유포하는 트래퍼(Traffer)팀이 존재한다.[29] 이후 피해자의 데이터를 훔쳐 오는 조직이 훔친 데이터를 정제·가공하여 히든 마켓 내 고객에게 판매한다.[30] 이는 단순한 해킹이 아닌, 개인정보를 상품화하고 재판매하는 '개인정보 가공 산업'이 하나의 비즈니스로 형성되었음을 의미한다.

최근 3년(2023년~2025년 10월 말 기준) 국내 관련 정보만 해도 460만 건 이상이 다크웹에서 판매된 것으로 추정되며, 이는 국내 이용자들이 지속적으로 이러한 위협에 노출이 되고 있음을 보여준다.

② 유출 데이터의 구조 및 영향도 파악

다크웹에서 유통되는 대규모 유출 데이터는 보통 분할 zip 압축이나 tar.gz 파일 형태로 유통이 되며, 내부에는 sql, .csv, .txt 등의 형식으로 정리된 계정 정보(이메일, 비밀번호, 이름, 전화번호 등)가 포함되는 경우가 있다.

단, 다크웹 상에서 유통되는 데이터에 대한 진위 여부 파악이 필요하기에 유출된 데이터 실제 유무 파악 및 구조에 대한 분석이 되어야 한다. 회사나 기관의 자산(도메인, IP 주소 등)포함 여부, 사내 메일 포맷과의 일치 여부, 그리고 이용된 비밀번호 해시 패턴이 자사 정책과 일치 여부 등은 유출 정보의 진위성 및 즉각적인 악용 가능성을 결정하는 핵심 지표이다. 정책 담당자나 기업 보안팀은 이러한 기술적 분석을 통해 유출의 심각성을 정확히 측정하고, 우선순위를 정하여 유출된 계정의 무효화 및 대응 조치를 취해야 한다.

2) 불법 유통의 핵심: 초기 접근 브로커(Initial Access Broker, IAB)

사이버 범죄 생태계에서 가장 중추적이며 위험한 역할을 수행하는 것은 IAB다.[31] IAB는 기업 자산의 특수 접근 권한(Remote Desktop Protocol, RDP) 접근권, 관리자 패널 로그인, 도메인 관리자 액세스 권한)을 확보하는 데 집중하며, 이를 전문화된 다크웹 포럼에서 거래 및 경매에 부친다.

이러한 기업 액세스 권한은 평균 1,000$(USD)에서 3,000$ (특이값 제외) 수준에서 거래되는데,[32] 이는 랜섬웨어 공격으로 예상되는 피해 규모에 비해 극히 저렴한 비용이다. IAB 시장의 활성화는 대규모 사이버 공격의 일반화를 의미한다. 즉, 제로데이와 같이 발굴 난이도가 높은 취약점이 확보되지 않은 범죄자의 경우, IAB로부터 저렴하게 초기 접근 권한을 구매한 후 LockBit, Clop, Qilin과 서비스형 랜섬웨어(Ransomware-as-a-Service, RaaS)을 통해서 랜섬웨어 공격을 즉시 시작할 수 있게 된 것이다.

---

29) S2W Blog (Medium), Detailed Analysis of the Stealer-Traffer Ecosystem, 2025.08.18.
30) Forum of Incident Response and Security Teams, Info-stealer: Most bang for the buck malware, 2023.06.
31) 매일경제, “女잠옷, 물건은 현관앞”…여자 혼자 사는지·언제 집 비우는지, 민감정보 다 넘어갔다., 2024.07.03.
32) Flare, Report – Stealer Logs & Corporate Access, 2023.07.25.

특히 IAB 판매량과 RaaS 확산은 2024년 상반기 대비 2025년 상반기 기준 랜섬웨어 공격 증가와 직접적으로 연결되는 지표로 해석될 수 있다.[33]

3. 유통된 개인정보를 이용한 2차 피해 심층 분석

1) 협력사 계정정보를 통한 공급망 공격(Supply Chain Attack)

사이버범죄 조직은 금전적 이득 극대화를 위해 개인 표적 공격보다는 기업 환경을 대상으로 하는 공격을 주로 수행하고 있다. 특히 랜섬웨어 협상 시 피해 기업의 매출액을 기준으로 몸값을 산정하는 방식이 존재한다.

그러나 대기업 및 주요 기관이 사이버 보안에 대한 투자를 강화함에 따라, 공격자들은 상대적으로 보안이 취약한 '약한 연결고리'를 찾고 있다. 이 약한 고리는 바로 주요 기업과 업무를 수행하는 1차 협력사, 외주 개발사 등 공급망 내의 파트너사들이다.

이러한 협력업체들은 상대적으로 보안 역량이 미흡함에도 불구하고, 업무 특성상 타겟 대기업의 민감한 자료와 핵심 프로젝트 정보를 취급하는 경우가 많다. 공격자가 이들 협력업체의 계정 정보나 네트워크 접근 권한을 탈취하는 경우, 궁극적인 표적 대기업이나 정부 기관의 핵심 정보까지 확보할 수 있게 된다.[34]

대표적인 2차 피해 사례

○ 글로벌 사례: 과거 2021년 리빌(REvil) 랜섬웨어 조직이 애플(Apple)의 직접적인 공격 대신, 애플의 제조 협력업체인 대만의 콴타컴퓨터(Quanta Computer)를 공격하여 애플 신형 제품의 도면을 유출시킨 바 있다. 이는 협력업체 침해를 통해 최종 타겟이 피해를 입은 대표적인 공급망 공격 사례이다.[35]

○ 국내 사례: 2025년 4월 국내 보험 대리점(General Agency, GA) 침해사고의 경우에도 보험영업 지원 IT 서비스를 제공하는 협력사의 보안 문제가 전체 GA로 확산되어 직접적인 피해가 발생한 사례가 확인되었다.[36]

---

33) S2W Blog (Medium), Ransomware Landscape in H1 2025: Statistics and Key Issues, 2025.08.12.
34) PASCON 2024 Conference (Dailysecu), Partnering Up, Lo cking Down: The Partnership Paradox in Cyber Threat Intelligence, 2024.
35) BBC, Taiwan authorities look into Apple supplier hack, 2021,04.23.
36) 금융감독원, GA 개인정보 침해사고(해킹) 발생 경과 및 향후 계획, 2025.05.20.

이러한 협력업체의 유출된 계정 정보 및 접근 권한은 공격자가 타겟팅할 수 있는 범위와 잠재적 피해 규모를 특정 대기업 또는 정부 기관까지 확장시킨다는 점에서, 계정 정보 유출 관리가 공급망 보안의 핵심으로 인식되어야 한다.

2) 랜섬웨어 공격과의 유기적 결합

① IAB 접근 권한을 활용한 서비스형 랜섬웨어(RaaS) 모델 확산

IAB로부터 구매한 특정 기업의 계정 정보 초기 접근 권한(Initial Access)은 LockBit, Qilin, ALPHV/BlackCat, 과 같은 주요 RaaS 그룹의 공격 기반이 된다. IAB 시장의 팽창은 RaaS 모델의 확산 가속화로 이어지며, 이는 2025년 상반기에만 91개 랜섬웨어 그룹이 3,624건의 피해 조직을 공개하는 등 활동이 기록적인 수준에 도달한 주된 원인이다.

② 데이터 유출 협박(Double Extortion)과 다크웹 활용

랜섬웨어 조직은 단순히 데이터를 암호화하는 것을 넘어, 탈취한 데이터를 다크웹 유출 사이트(Leak Site)에 공개하겠다고 협박하는 이중 갈취 전략을 이용한다. Underground와 같은 랜섬웨어 그룹은 피해자에게 법률 위반 가능성을 포함한 협박성 랜섬노트를 제공하며, 이 노트에 다크웹 채팅 사이트 주소와 로그인 정보를 제공하여 피해자가 직접 협상 테이블로 오도록 유도한다. 유출된 개인정보는 이때 공격의 금전적 레버리지를 극대화하는 수단으로 기능한다.

3) 생성형 AI 및 딥페이크 악용한 신규 위협

2025년 사이버 위협 전망에서 가장 중요한 변화는 공격자의 생성형 AI 활용 본격화이다. AI는 유출된 개인정보의 악용 효율을 극대화하는 역할을 수행할 수 있다.

범죄자를 위한 생성형 AI 서비스(WormGPT, FraudGPT, XanthroxAI 등)는 다크웹에서 지속적으로 나오고 있으며, 이를 통해 자연스럽고 맞춤화된 피싱 및 스피어피싱 메일을 자동으로 생성할 수 있다. 이는 기존의 대량 스팸성 피싱을 넘어, 저렴한 가격에 대규모로 유통되는 계정 정보를 활용하여 표적 공격의 성공률을 높일 수 있다.

나아가 딥페이크 기술의 발전은 유출된 신원 정보(여권, 신분증 스캔 자료 등)와 결합하여 심각한 수준의 신원 도용 및 협박 범죄로 이어질 수 있다. 딥페이크 기술이 가짜 메시지를 식별하기 어렵게 만드는 수준으로 개선됨에 따라, 금융 거래 및 신원 인증 과정에서 딥페이크 탐지 및 방지 기

술의 도입이 시급해지고 있다.

4. 다크웹 개인정보 불법 유통 대응 전략

개인정보 불법 유통에 효과적으로 대응하기 위해서는 사후 대응이 아닌 선제적 위협 가시성 확보 및 유통 채널 차단으로 패러다임을 전환해야 한다.

1) 기술적 방어 및 선제적 위협 인텔리전스 활용

① 지속적 다크웹 모니터링 및 유출된 계정 정보에 대한 가시성 확보

다크웹 모니터링은 유출된 계정 정보를 사전에 확보하여 조직에 대한 위협을 선제적으로 파악하는 가장 효과적인 방어 수단이다. 대규모DB 덤프는 수작업 분석이 불가능하므로, 조직 도메인 포함 여부, 해시 패턴 등을 자동으로 분석하여 위협 우선순위를 결정하고 대응 시간을 단축하는 자동 분석 CTI(Cyber Threat Intelligence) 플랫폼 도입이 필요하다.

CTI를 통해 확보된 전술적 위협 인텔리전스(Tactics, Techniques, and Procedures, TTPs)를 MITRE ATT&CK(MITRE Adversarial Tactics, Techniques, and Common Knowledge) 프레임워크 기반하여 분석하고 보안 관제(Security Operation Center, SOC)에 활용함으로써, 보안팀은 알려지지 않은 위협에 대해서도 선제적으로 탐지 및 대응할 수 있다.

② 데이터 유출 모니터링 및 제로 트러스트 체계 구축

내부 시스템에서 외부 C&C(Command and Control) 서버로의 암호화된 통신 시도나 지속적인 은닉 송신 패턴(Beaconing)을 탐지하고 차단하는 데이터 유출 모니터링 시스템을 강화해야 한다. 이는 정보탈취형 악성코드(Info-stealer)에 의한 데이터 탈취를 막는 데 필수적이다.

2차 피해를 근본적으로 차단하기 위한 가장 효과적인 기술적 방안은 강력한 신원/접근 통제 시스템이다. 유출된 자격 증명으로 인한 계정 탈취(Account Takeover, ATO)를 무력화하기 위해 강력한 고유 비밀번호 사용을 의무화하고, 모든 주요 서비스에 대해 2단계 인증(Two-Factor Authentication, 2FA)을 활성화하는 것은 기본 방어 전략이다. 특히 기업 환경에서는 IAB가 거래하는 초기 접근 권한이 무력화되도록 강력한 다중 인증 및 제로 트러스트 시스템을 구축해야 한다.

2) 정책 및 제도 개선 방인

① 불법 유통 상습 매매자 단속 및 국제 수사 공조 강화

다크웹 범죄는 국경을 초월하므로, 신속한 사법 대응을 위해 국제 공조 체계를 강화해야 한다. EU의 전자증거 규정(Electronic Evidence Regulation, e-Evidence)이나 미국의 합법적 해외 데이터 이용 명확화법(Clarifying Lawful Overseas Use of Data Act, CLOUD Act), 그리고 사이버범죄에 관한 부다페스트 협약(Budapest Convention on Cybercrime)과 같은 국제적인 전자 증거 교환 프레임워크에 대한 이해를 높이고 이를 활용하여, 해외에 위치한 서버나 범죄자 정보를 신속히 확보할 수 있는 법적 및 기술적 인프라 구축을 가속화해야 한다.

② 국경간 불법 자금 추적 역량 강화

다크웹 거래는 주로 가상자산을 통해 이루어지므로, 불법 자금의 흐름을 추적하는 기술적 역량이 범죄 수익 차단의 핵심이 된다. 피싱이나 랜섬웨어 공격으로 탈취된 가상자산 자금 회수를 위해서는 국경을 초월한 가상자산 추적 기술의 도입과 사법 기관 간의 협력이 필수적이다. 이러한 기술 도입은 범죄 수익 환수율을 높여 다크웹 기반 범죄의 경제적 동기를 약화시키는 데 기여한다.

5. 결론: 위협의 핵심 인식 및 패러다임 전환

2025년 다크웹 환경은 개인정보 유출을 통한 2차 피해를 산업화된 수준으로 고도화하고 있다. 핵심적인 위험은 초기 접근 브로커(IAB)를 통한 랜섬웨어 공격의 대중화와 생성형AI를 이용한 타겟팅 된 피싱의 지능화 및 자동화로 요약된다. 이 두 요소는 유출 정보의 공격 효용성을 극대화하여 2차 피해의 규모와 속도를 예측 불가능한 수준으로 증가시키고 있다. 따라서 개인정보 정책은 '피해 발생 후 사후 처리'에서 '위협의 공급망을 선제적으로 감시하고 무력화'하는 방향으로 패러다임을 전환해야 할 필요가 있다.

참고 문헌 |

1. Help Net Security, Ransomware groups are multiplying, raising the stakes for defenders, 2025.08.26.
2. DeepStrike, Dark Web Statistics 2025: Trends, Usage, and Security Insights, 2025.10.19.
3. U.S. Department of Justice (DOJ), Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace, 2022.04.05.
4. European Union Agency for Law Enforcement Cooperation, 270 arrested in global dark web crackdown targeting online drug and criminal networks, 2023.05.02.
5. DeepStrike, Top 7 Dark Web Marketplaces of 2025: Inside the Underground Economy, 2025.10.07.
6. S2W Blog (Medium), Detailed Analysis of the Stealer-Traffer Ecosystem, 2025.08.18.
7. Forum of Incident Response and Security Teams, Info-stealer: Most bang for the buck malware, 2023.06.
8. 매일경제, “女잠옷, 물건은 현관앞”…여자 혼자 사는지·언제 집 비우는지, 민감정보 다 넘어갔다., 2024.07.03.
9. Flare, Report – Stealer Logs & Corporate Access, 2023.07.25.
10. S2W Blog (Medium), Ransomware Landscape in H1 2025: Statistics and Key Issues, 2025.08.12.
11. PASCON 2024 Conference (Dailysecu), Partnering Up, Lo cking Down: The Partnership Paradox in Cyber Threat Intelligence, 2024.
12. BBC, Taiwan authorities look into Apple supplier hack, 2021,04.23.
13. 금융감독원, GA 개인정보 침해사고(해킹) 발생 경과 및 향후 계획, 2025.05.20.

PRIVACY REPORT

개인정보 이슈 심층분석

「2025 개인정보 이슈 심층분석 보고서」는
개인정보보호위원회의 출연금으로 수행한 사업의 결과물입니다.

한국인터넷진흥원의 승인 없이 본 보고서의 무단전재나 복제를 금하며,
인용 출처 「2025 개인정보 이슈 심층분석 보고서」를 밝혀주시기 바랍니다.

본 보고서의 내용은
한국인터넷진흥원의 공식 견해가 아님을 알려드립니다.

발행일 2025년 11월
발행처 한국인터넷진흥원 개인정보제도팀
전라남도 나주시 진흥길 9

KISA 한국인터넷진흥원