클릭픽스와 BPFDoor까지, 2025년 주요 사이버 위협 동향

기술이 빠르게 진화하면서 사이버 공격은 더욱 교묘하고 정밀해지고 있으며, 우리의 일상에도 점점 깊숙이 침투하고 있다. 2025년에도 사회공학적 기법과 최신 취약점을 악용한 해킹 공격이 활발하게 탐지되고 있으며, 실제 피해 사례도 빠르게 확산되고 있다.

이번 글에서는 2025년 상반기에 확인된 주요 사이버 위협 트렌드와 실제 사례 분석을 살펴본다.

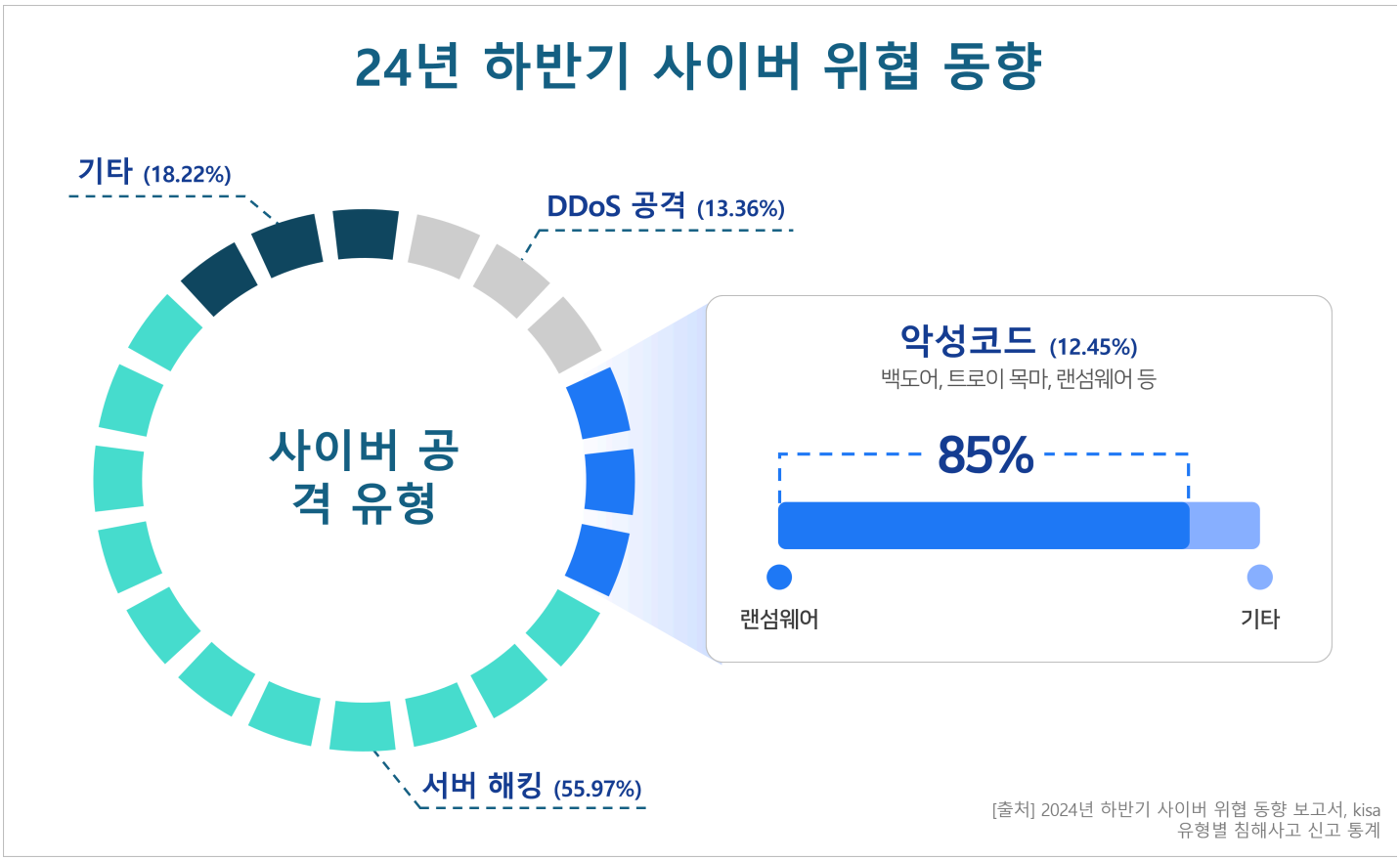
기술 발전과 사이버 위협의 가속화

오늘날 우리는 새로운 기술과 서비스가 출시된 지 며칠, 심지어 몇 시간 만에 수많은 사용자에게 확산되는 현상이 목격되고 있다. 디지털 시대에서 이러한 변화 속도는 상상을 초월하는 수준이다. 실제로 주요 온라인 서비스들이 100만 명의 사용자를 확보하는 데 걸린 시간은 불과 몇 년 사이에 극적으로 단축되었다. 예를 들어, 페이스북이 10개월, 트위터가 2년이 걸렸던 것과 달리, 최근 ChatGPT는 출시 단 5일 만에 100만 사용자를 확보하는 기록을 세웠다. 이처럼 불과 10여 년 만에 새로운 기술과 서비스가 일상에 스며드는 속도가 혁신적으로 가속화되고 있다.

신기술 확산의 가속화는 우리가 미처 준비하거나 대응할 틈도 없이 새로운 위험을 함께 가져오고 있다. 과거 해외에서 등장한 신종 랜섬웨어가 국내에 본격적으로 확산되기까지는 통상 약 2년 정도의 시간적 여유가 있었다. 하지만 최근에는 생성형 AI 악용, 신규 보안 취약점, 새로운 악성코드 유포 기법 등 해외에서 발견된 위협이 불과 몇 개월 또는 며칠 만에 국내에서도 사용되는 현상이 나타나고 있다. 이처럼 신기술 도입의 가속화는 사이버 위협이 우리의 삶을 더욱 짧은 시간 내에 파고들게 만들고 있다. 이제 사이버 공격은 매년 새로운 방식으로 등장하며 발생 건수 또한 지속적으로 최고 기록을 갱신하고 있다. 최신 통계를 살펴보면 사이버 위협 및 공격은 단순히 IT 관리의 이슈를 넘어 우리 일상 운영 전반에 직접적인 영향을 미치는 핵심적인 리스크로 부상하고 있음을 보여준다.

사이버 위협 동향

2024년 하반기 동안 국내 민간 분야에서 보고된 사이버 공격 통계를 살펴보면 다음과 같은 특징이 두드러진다.



[그림 1] 24년 하반기 사이버 위협 통계 (출처: KISA)

- **서버 해킹:**
  서버 해킹: 전체 사고의 약 56%로 과반이 넘는 수치를 차지하며 가장 큰 비중을 차지했다. 특히 기업의 웹사이트, 데이터베이스, 서버 인프라 등 주요 공격 표적이 되고 있다.
- **악성코드 감염:**
  전체 해킹 공격 중 약 12%를 차지했으며 악성코드 침해 유형 중 랜섬웨어가 85%로 가장 많이 발생했다. 이러한 랜섬웨어 공격은 기업, 병원, 공공기관 등 사회 전반을 표적으로 삼고 공격이 이루어지고 있다.

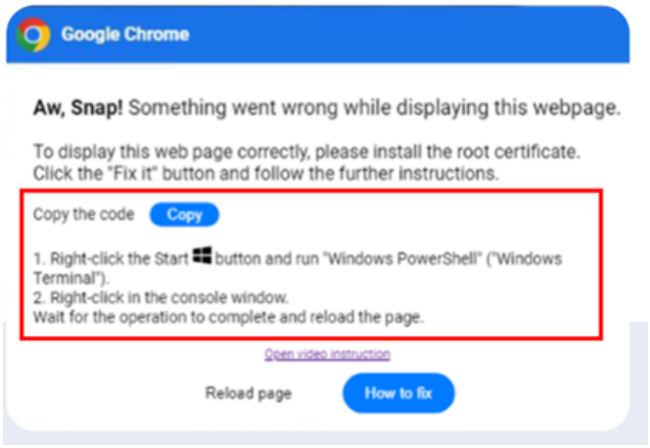
2025년 상반기에는 더욱 활발하게 해킹 공격이 발생하고 있으며 최근 금융권과 온라인 서점 해킹 사례를 살펴보면, 랜섬웨어 감염으로 인해 서비스가 수일간 지연되는 사태가 벌어졌으며, 수많은 고객이 직접적인 불편을 경험한 바 있다. 이 뿐만 아니라 공격 방법이 점점 정교해지고 있어 탐지하고 방어하는 것이 어려워지고 있다. 이와 같은 현실은 사이버 공격이 단순한 IT 문제를 넘어 사회 곳곳에 실질적인 위기와 혼란을 초래함을 보여준다. 그렇다면 상반기에 발생했던 실제 공격 사례와 그 대응 방법에 대해 알아보자.

최신 해킹 공격 사례와 대응 방법

사이버 공격은 사용자 행위 유도, 정상 기능 악용, 위장 사이트 제작 등의 방법으로 더욱 다양한 형태로 진화하고 있다. 공격자들은 사회공학 기법과 보안 취약점을 정교하게 조합해 피해자에게 직접적인 실행을 유도하고 있으며, 실제 국내에서도 그 영향을 받은 사례가 지속적으로 보고되고 있다. 2025년 상반기에 확인된 주요 공격 사례와 대응 방법은 다음과 같다.

1. 클릭픽스 (Clickfix)

클릭픽스는 2024년 중반에 처음 보고된 신종 사회공학적 악성코드 유포 방식이다. 공격 방법은 다음과 같다.



[그림 2] 클릭픽스 공격 화면

1. **사용자 유인:** 공격자는 사용자가 이메일이나 메시지를 통해 웹사이트로 접근하도록 유도
2. **악성 스크립트 복사 유도 :** 보안 문제 해결을 빙자한 안내 메시지와 사용자가 버튼을 클릭하도록 유도해 사용자 PC 클립보드에 악성 명령어가 복사되도록 웹사이트를 구축 (대표적으로 '여기를 클릭하고 문제 해결을 위해 복사된 코드를 실행하세요'와 같은 유도 메시지 활용).
3. **악성 스크립트 실행 및 추가 감염:** 사용자가 안내에 따라 악성 명령어를 직접 입력하여 실행하도록 하며 이 과정에서 추가적인 악성코드 감염

공격자는 로봇 확인 캡차 버튼처럼 보이는 화면으로 사용자의 클릭을 유도한다. 이 때 공격자는 클릭 시에만 클립보드 접근을 허용하는 자바스크립트 기능을 악용하며 사용자가 해당 버튼을 클릭하는 순간, 악성 명령어가 PC 클립보드에 자동으로 복사되도록 한다.

이후 공격자는 사회공학적 기법으로 사용자에게 클립보드의 명령어를 직접 실행하도록 안내하며 이를 따른다면 악성코드가 활성화된다. 이처럼 평범한 사용자 동작을 통해 공격을 완성하는 것이 클릭픽스의 주요 특징이다.

클릭픽스 앞서 언급한 것과 같이 2024년 중반에 최초 발견되었으며 불과 6개월 만인 2025년 초에 국내에서도 실제 피해 사례가 보고되고 있다. 초기에는 웹사이트를 통한 감염이 주로 이루어졌지만, 최근 국내에서 발견된 사례에서는 정교한 스피어 피싱 방식으로 변형되었다.

1. **메일 첨부파일을 이용한 공격:** 이메일 보안 솔루션 같은 보안 제품에서 텍스트 파일에 적힌 악성코드를 단순 문자열로 인식하는 허점을 노린 공격 방식이다. 이메일을 통해 악성 명령어가 담긴 텍스트 파일과 실제 안내문처럼 정교하게 제작된 PDF 매뉴얼을 첨부하여 사용자가 이를 따라 직접 악성코드를 복사하고 실행하도록 유도한다.
2. **웹사이트를 이용한 공격**: 정기 채용 공고나 직무 기술서 게시글이 있는 실제 게시판처럼 위장 웹사이트를 제작한 후 게시글 클릭할 때 팝업을 통해 악성코드를 복사하고 실행하도록 유도한다.

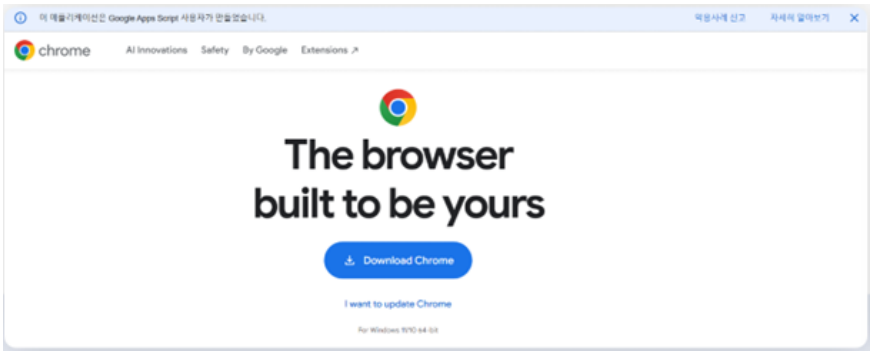
클릭픽스 유형의 공격은 사용자의 행동을 유도하는 사회 공학적인 공격 기법이기 때문에 공격 방식에 대해 미리 이해해야 방지할 수 있으며 보안에 대한 교육이 병행되어야 한다.

2. 정상 소프트웨어 위장 공격 (가짜 소프트웨어 다운로드 페이지)

최신 사이버 위협 두 번째 사례는 정상 소프트웨어로 위장한 공격 방식이다. 공격자는 악성코드를 정상적인 소프트웨어 다운로드 페이지로 위장한 가짜 사이트를 제작하여 이를 통해 사용자가 악성코드를 다운로드받도록 속인다.

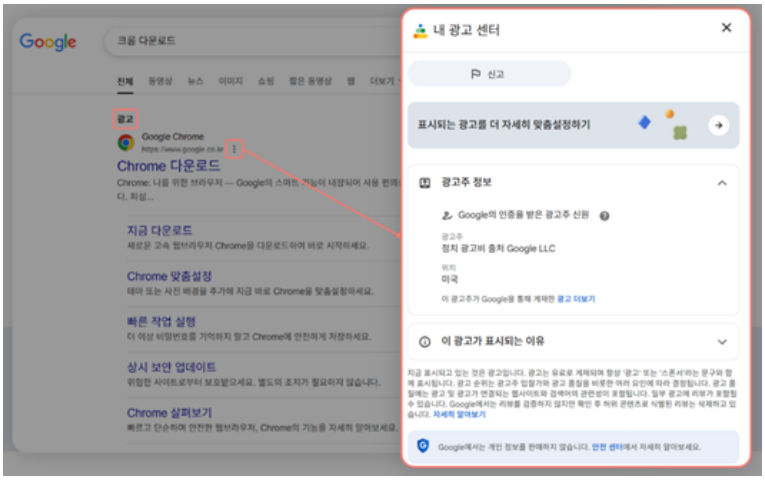
정상 소프트웨어 위장 공격 과정은 다음과 같다.

1. **가짜 페이지 제작**: 가짜 소프트웨어 다운로드 페이지를 제작한 후, 구글 광고 영역에 등록하여 노출
2. **검색 엔진 최상단 노출**: 검색 엔진 최적화 기능을 악용하여 제작한 가짜 페이지를 검색 결과 최상단에 노출
3. **악성코드 감염**: 사용자가 소프트웨어 다운로드해 실행하면 악성코드에 감염



[그림 3] 크롬 다운로드 사이트로 위장한 가짜 웹페이지

대표적인 사례는 구글 크롬 다운로드로 위장한 악성코드다. 공격자는 실제 소프트웨어 다운로드 페이지인 것처럼 속이기 위해 실제 로고를 사용하며 비슷한 디자인을 활용하여 사용자를 속인다. 또한 Google Apps Script 플랫폼을 활용한다면, 실제 구글 도메인이 주소창에 출력되지만 내부적으로는 iframe 태그를 이용해 구글 도메인과 무관한 공격자가 제작한 가짜 크롬 웹사이트를 출력시킬 수 있다. 결국 이 페이지는 구글 크롬 다운로드로 위장되어 있지만 실제로는 악성코드가 다운로드되는 최종 목적지로 연결되는 웹사이트이다.



[그림 4] 광고주 정보 확인 방법

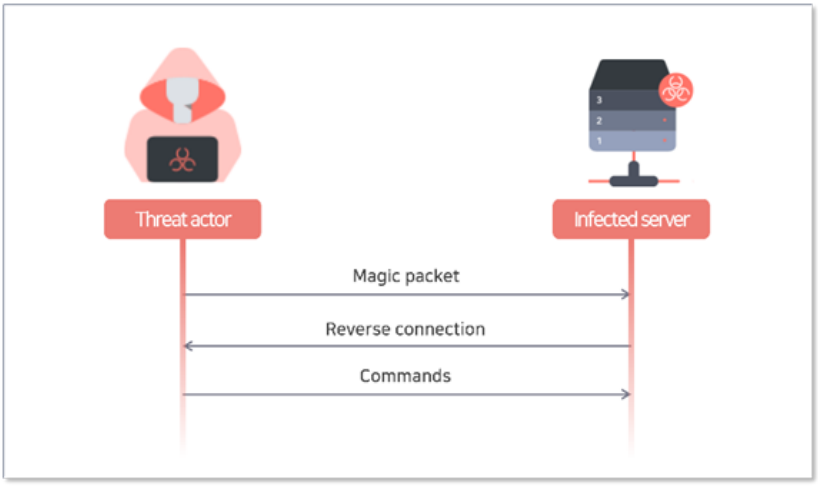
이와 같은 공격을 방지하는 것이 어렵지는 않다. 검색 결과에 표시되는 옆의 아이콘을 클릭하여 광고주 정보를 확인하여 정상적인 페이지인지 확인할 수 있다. 하지만 기업의 경우 매번 광고주 정보를 확인해 정당한 사이트인지 검증하는 것은 매우 번거로운 일이기 때문에 업무에 자주 사용하는 소프트웨어를 한 곳에서 통합하여 다운로드할 수 있는 다운로드 센터를 운영하는 방안도 매우 효과적이다.

3. BPFDoor

BPFDoor는 리눅스 시스템을 주요 타깃으로 삼는 백도어 악성코드다. 이는 장기 은닉 및 재침투 목적으로 설계되었으며, 시스템 침투 후 오랫동안 탐지되지 않고 은밀하게 활동할 수 있다는 점이 가장 큰 특징이다.

BPF는 원래 비효율적인 네트워크 패킷 분석 문제를 해결하기 위해 개발된 기술로 성능 저하 없이 네트워크 트래픽만을 분석할 수 있도록 돕는다. 기존 방식의 네트워크 분석 방식은 커널의 모든 네트워크 패킷을 유저 영역으로 복사한 후 필요한 패킷을 골라내는 데 반해, BPF는 커널 영역에서 미리 필터링을 적용하여 필요한 패킷만 유저 영역에 전달한다. 이를 통해 불필요한 데이터 이동이 최소화되며 성능 저하 없이 네트워크 트래픽을 빠르게 분석할 수 있다.

BPFDoor 악성코드는 이러한 BPF 기술을 악용하여 다음과 같은 방식으로 동작한다.



[그림 5] BPFDoor 공격 흐름

1. **BPF 필터 등록:** 공격자에 의해 시스템이 BPFDoor에 감염되면, 악성코드는 커널 영역에 BPF 필터를 등록하여 공격자가 미리 지정한 매직 넘버가 포함된 특정 네트워크 패킷을 계속해서 감시
2. **명령 제어용 공격자 인식:** 네트워크 패킷을 감시하다가 매직 넘버가 포함된 패킷을 발견하면, 해당 패킷의 출발지 IP주소를 공격자의 명령 제어 서버로 인식
3. **리버스 커넥션 시도:** BPFDoor는 공격자의 명령에 따라 리버스 커넥션 방식을 활용하여 감염된 시스템에서 공격자의 명령 제어 서버로 직접 연결
4. **원격 명령 실행:** 연결에 성공하면 공격자로부터 원격 명령을 받아 시스템에서 실행

BPFDoor는 커널 영역에서 네트워크 패킷을 감시할 수 있기 때문에 특정 포트를 열지 않아도 네트워크 상을 오가는 모든 패킷에서 미리 지정한 매직 넘버를 찾아낼 수 있다. 즉, 기존 방화벽이나 네트워크 보안 솔루션이 고정 포트를 기반으로 탐지하는 외부 접속 방식 없이도 정상적인 시스템처럼 조용히

명령을 주고받을 수 있다. 더불어, 리버스 커넥션 방식을 활용하여 공격자 서버와 통신하기 때문에 인바운드 연결을 차단하는 일반적인 방화벽 규칙도 쉽게 우회할 수 있다.

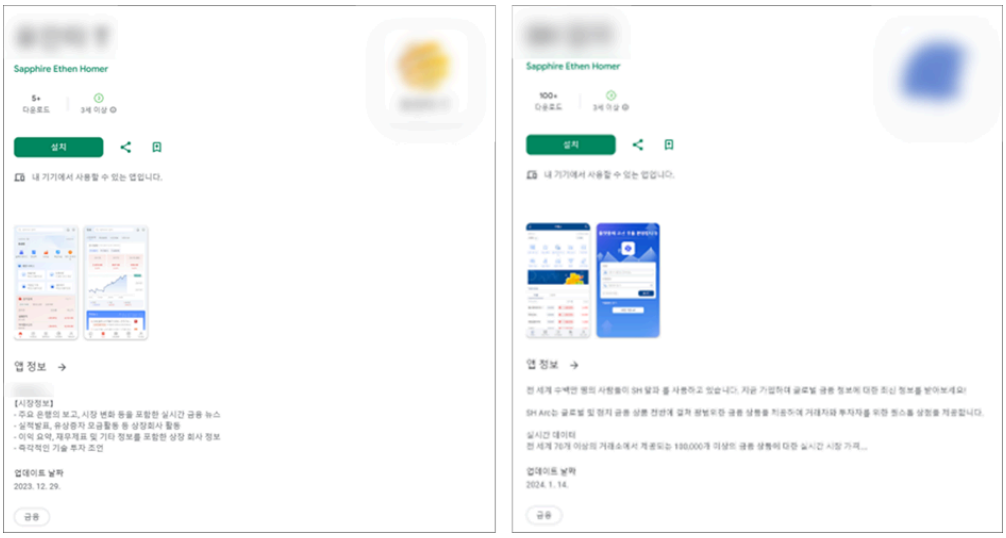
BPFDoor의 이러한 특징으로 인해 탐지하기에 어려운 경우가 많아 리눅스 전용 보안 솔루션을 활용하여 지속적으로 모니터링하고 방지해야 한다.

4. 스캠 (Scam)

스캠은 일상에서 우리가 흔히 마주치는 사기와 방식이 비슷하고 그 종류와 범위가 굉장히 다양하다. 국내에서는 특히 악명 높은 두 가지 스캠이 있는데, 바로 로맨스 스캠과 투자 사기 스캠이다.

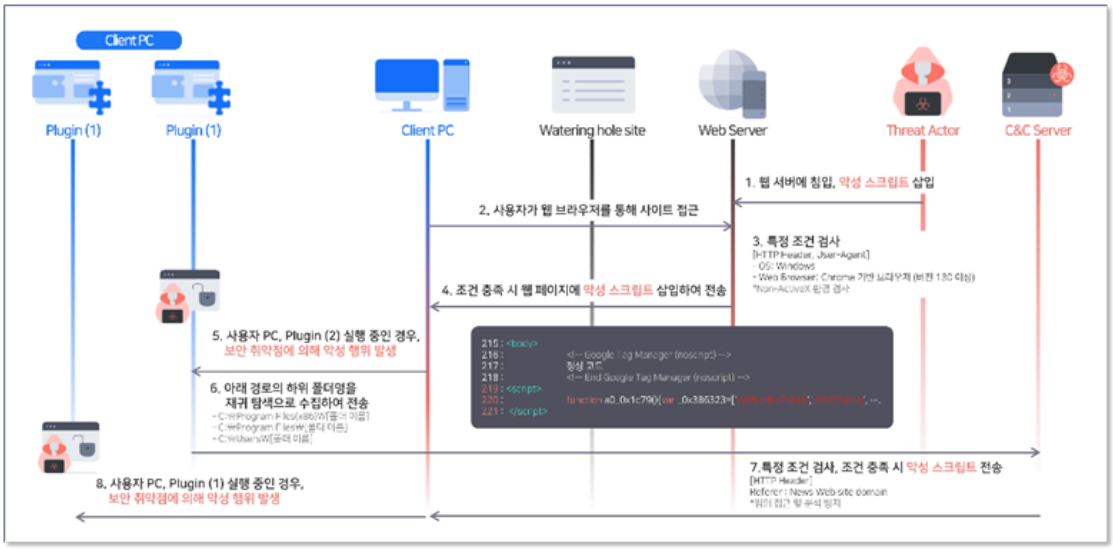
- **로맨스 스캠:** 연애 감정에 편승해 사용자의 돈을 빼내는 수법
- **투자 사기 스캠:** 가짜 주식 거래소와 같은 가짜 투자 플랫폼을 활용하여 사용자가 자발적으로 송금하도록 유도

이러한 사칭형 앱은 피해자가 스스로 자발적으로 금전을 송금하도록 유도하기 때문에 애플리케이션 자체는 실제 단순히 웹페이지를 보여주는 역할만 수행한다. 이로 인해 구글이나 애플의 앱 마켓에서는 이러한 앱을 악성 앱으로 탐지되지 않는 사례가 많다. 사용자의 설치를 유도하는 사기 앱들은 실제로 애플 앱스토어나 구글 플레이 스토어에도 업로드 되어 있는 것을 확인할 수 있다. 겉으로는 국내 기업이나 금융사와 비슷한 아이콘을 사용하고 있었으며, 실제로는 모두 스팸용으로 제작된 가짜 앱임을 주의해야 한다.



[그림 6] 플레이스토어에 게시된 스캠 애플리케이션 예시

5. 워터링 홀 (Watering Hole)



[그림 7] 워터링 홀 공격 흐름

워터링 홀은 사용자가 평소 자주 방문하는 합법적인 웹사이트를 공격자가 먼저 감염시킨 뒤, 이 웹사이트를 찾는 방문자 PC에 악성코드를 유포하는 APT형 공격 기법이다.

공격 방식은 다음과 같이 전개된다.

1. **악성 스크립트 삽입**: 공격 대상이 자주 사용하는 웹 서버에 침입해 악성스크립트 삽입
2. **공격 대상 검증**: 웹 사이트에 접근한 사용자가 공격 대상인지 확인
3. **악성 스크립트 전달**: 공격 대상에 해당할 경우, 웹 사이트에서 추가 악성 스크립트를 전달
4. **정보 수집 및 탈취**: 보안 취약점을 악용하여 시스템의 각종 정보를 수집하고 이를 외부 서버로 탈취
5. **연쇄적 취약점 악용**: 추가로 다른 악성 스크립트도 실행해 연쇄적으로 악성코드 다운로드 및 실행

워터링 홀에 대한 피해를 방지하기 위해서는 웹사이트 보안 조치도 중요하지만 사용자도 이러한 해킹방식에 대해 인지하고 보안 소프트웨어를 최신상태로 유지하여 공격에 대해 대비해야 한다.

결론

앞서 살펴본 다섯 가지 사이버 공격 사례는 모두 형태나 침투 경로는 다르지만, 공통적으로 사람의 심리를 이용하는 사회공학 기법과 기술적인 취약점을 교묘하게 결합하고 있다는 특징이 있다. 사용자의 클릭, 복사, 다운로드와 같은 평범한 행동을 통해 공격이 실행되고, 기업 내부의 작은 방심 하나가 전체 시스템을 마비시키는 결과로 이어진다.

특히 최근의 사이버 위협은 이전보다 훨씬 빠른 속도로 등장하고, 더 짧은 시간 내에 실제 공격하는데 활용한다. 클릭픽스처럼 기존 보안 탐지 체계를 우회하는 신종 기법이나, 정상 소프트웨어를 가장한 악성코드 배포 방식은 기술적 방어만으로는 막기 어렵다. 공격자들이 진화하고 있는 만큼, 우리 역시 보안 전략의 방식도 함께 바뀌어야 한다.

이제 사이버 보안은 단순히 시스템을 ‘지키는 것’이 아니라, 위험을 ‘예측하고 방지’하는 선제적 대응이 핵심이 되어야 한다. 이를 위해서는 보안 솔루션의 최신화뿐 아니라, 임직원 대상의 보안 교육, 사용자 습관 점검, 취약점에 대한 빠른 패치와 내부 프로세스 정비 등 복합적인 노력이 병행되어야 한다. 지속적으로 진화하는 사이버 공격 앞에서 완벽한 보안은 존재하지 않지만, 위협을 정확히 이해하고 선제적으로 대응하는 자세가 무엇보다 중요하다.

안랩은 이러한 흐름에 맞춰 TIP 서비스를 통한 위협 정보 제공, 실시간 취약점 공지, 국내외 기관과의 협력을 강화해 나가고 있으며, 앞으로도 기업과 사용자들이 더욱 안전한 디지털 환경을 구축할 수 있도록 기술과 인프라를 지속적으로 발전시켜 나갈 것이다.

AhnLab
분석대응팀 이선호 팀장