Special Report

심스와핑(SIM Swapping) 공격을 통한 가상 자산 탈취, 대응 방안은?

■ 개요

최근 국내에서 네 차례 연달아 심스와핑(SIM Swapping) 공격[1] 의심 사례가 발생했다. 피해자는 가상화폐거래소를 이용하던 개인이며 피해 규모는 2억 8000만 원에 달한다. 심스와핑 공격은 해외에서는 간혹 발생하던 공격이었지만 국내에서 2021년 12월경 최초로 발생했다. 이후 일부 가상화폐거래소에서 계정 해킹 및 출금을 시도한 정황을 포함해 심스와핑 의심 사례가 잇달아 발생하자 불안감이 커지고 있는 상황이다.

이번 Special Report에서는 심스와핑을 통한 가상 자산 탈취 시나리오를 유추하고 심스와핑이 가지는 파급력과 대응 방안에 대해 알아보고자 한다.

[1] 사용자를 식별하는 유심을 복제해 휴대전화를 이용한 본인 인증을 통과하는 방식으로 타인의 금융자산이나 가상 자산을 탈취하는 공격

■ 국내에서 발생한 심스와핑 의심 사례

심스와핑 공격으로 의심되는 4건의 국내 피해 사례를 살펴보면 공격자는 심스와핑을 통해 피해자의 SNS, 포털 비밀번호를 변경하고 2차 인증을 무력화했다. 최종적으로는 피해자의 가상화폐거래소 계정을 획득하여 해당 계정이 보유하고 있는 가상 자산을 노렸음을 알 수 있다.

infosec

분류	일자	증상 및 피해내용
사례 1	2021년 12월 23일 (IOS)	1. 스마트폰 통신 불가 증상(유심기변 기록) 2. SNS, 포털 비밀번호 타인에 의해 재설정 3. 다음날 동일 증상(유심 기변 기록) 4. 가상자산 타인 계좌로 무단전송(약 100만원 피해)
사례 2	2022년 1월 12일 (Android)	1. 스마트폰 통신 불가 증상(유심기변 기록) 2. 피해자가 재부팅 시도했으나 증상 반복 3. SNS, 포털 비밀번호 타인에 의해 재설정 4. 피해자가 해킹 의심되어 스마트폰 전원 종료 5. 가상자산 무단 유출 확인(약 2200만원 피해)
사례 3	2022년 1월 16일 (Android)	1. 스마트폰 통신 불가 증상(유심기변 기록) 2. SNS, 포털 비밀번호 타인에 의해 재설정 3. 당일 대리점 방문하여 유심정지 조치 4. 가상화폐거래소 자체 의심거래 차단(피해 없음)
사례 4	2022년 2월 12일 (알 수 없음)	1. 가상자산 무단 유출 확인(약 2억 6000천만원 피해) 2. 스마트폰 통신 불가 증상(유심기변 기록) 3. 유심변경 메시지 및 SNS 타 기기 로그인 내역 확인

■ 국내 심스와핑 의심 사례 분석

1. 복제된 유심에 의한 공격

언론의 보도에 따르면 국내에서 발생한 심스와핑 의심 사례는 복제된 유심에 의한 공격일 가능성이 높은 것으로 보인다. 공격자가 어떤 방식으로 유심을 복제했는지는 알려지지 않았지만, 해외에서 발생한 심스와핑 사례에서 유심 복제 방법은 크게 두가지로 분류할 수 있다.

첫 번째 방법은 다크웹에서 구매한 개인정보로 이동통신사를 속여 유심을 발급받는 것이다. 다크웹에서는 해킹을 통해 유출된 개인정보가 활발하게 유통되고 있기 때문에 이름, 연락처를 포함한 불특정 다수의 개인정보를 쉽게 획득할 수 있다. 이러한 정보를 이용하여 이동통신사에 유심 분실, 파손을 이유로 피해자를 가장해 재발급을 신청할 수 있으며, 발급과정에 적절한 본인확인 절차가 없는 경우 제3자의 유심 발급이 가능하다. 해외에서는 이동통신사의 허술한 보안 정책을 악용하여 유명인을 대상으로 심스와핑 공격이 이루어진 사례가 다수 존재한다. 또한 최근 스페인에서는 소셜 엔지니어링 기법[2]으로 통신사 직원들을 속여 심카드를 복제한 일당이 체포된 사례가 있다.

두 번째 방법은 이동통신사 내부 직원을 매수하여 유심을 복제하는 것이다. 2019년 미국에서 발생한 사례로, 이동통신사 직원이 대가를 받고 유심 발급에 필요한 개인정보를 공격자에게 제공했다. 공격자는 이를 이용하여 여러 피해자의 유심을 발급받아 공격에 악용하여 약 200만 달러 이상의 피해가 발생했다.

[2] 소셜 엔지니어링 기법 : 기술적인 해킹 기법을 사용하는 대신 사람의 심리를 악용해 시스템 또는 데이터, 건물에 대한 출입 권한을 확보하는 해킹 수법으로, 사회공학적 공격이라고도 함

2. 심스와핑 공격을 통한 가상 자산 탈취

국내에서 발생한 심스와핑 의심 사례에서 공격자의 최종 목표는 모두 피해자의 가상 자산이었다.

infosec

분류	증상 및 피해내용
사례 1	약 100만원의 자산이 무단으로 이더리움으로 환전 되고 타인의 가상 지갑으로 전송됐다.
사례 2	피해자가 휴대전화를 잠시 꺼둔 사이 가상화폐거래소에서 2,200만원가량의 가상자산이 탈취됐다.
사례 3	공격자가 피해자의 가상자산 계좌를 노렸으나, 거래소에서 자체적으로 크리덴셜 스터핑을 시도하는 계정으로 인지하고 출금 제한으로 전환되어 가상자산 출금에 실패했다.
사례 4	피해자의 약 2억 6000만원 상당의 가상자산이 무단으로 전량 매도한 후 클레이튼(KLAY)을 매수되어 다른 지갑으로 출금되었다.

위 사례들을 통해 공격자가 피해자의 가상화폐거래소 계정과 해당 계정이 보유하고 있는 가상 자산을 목표로 한다는 것을 알 수 있다. 가상 자산은 흔적이 남지 않고 추적이 어렵기 때문에 최근 공격자들이 선호하는 공격 목표다.

※ 가상 자산을 노리는 심스와핑 공격자 동향은 해외 사례로도 확인할 수 있다.

- 2018년 8월, 미국의 가상 자산 투자자가 통신사 직원의 정보 유출로 인해 2380만 달러 상당의 심스와핑 피해를 입었다고 주장하며 이동통신회사를 고소

- 2021년 4월, 메사추세츠에서 심스와핑을 통해 10명 이상의 SNS 계정을 탈취하고 가상 자산 53만 달러 이상을 탈취하려 시도했지만 검거

- 2021년 11월, 캐나다 온타리오 주에서 10대 청소년이 심스와핑을 통해 가상 자산 3650만 달러를 탈취하여 검거

- 2021년 한 해 동안 FBI가 접수한 심스와핑 공격은 1611건이며, 총 피해액은 6800만 달러에 달함

■ 심스와핑 공격 시나리오

공격자는 심스와핑을 시도할 수 있는 복제 유심과 피해자의 개인정보(이름, 전화번호, 생년월일)을 획득한 후, 가상화폐거래소에서 계정 인증수단으로 사용되는 주요 포털 또는 메신저의 '아이디 찾기', '비밀번호 재설정' 기능을 이용해 계정정보 탈취를 시도한다. 심스와핑 공격을 통해 본인인증 우회가 가능하여 피해자의 계정정보 획득이 가능하고, 이후 동일한 방법으로 피해자의 가상화폐거래소 계정에 접근할 수 있으며 가상 자산을 탈취할 수 있다.

[심스와핑 발생 시 가상 자산 탈취 시나리오]

1. 공격자는 공격에 필요한 복제 유심(심스와핑)과 공격 대상의 개인정보 일부를 획득

2. 가상화폐거래소에서 계정 인증수단으로 사용되는 A포털과 B메신저의 계정을 탈취 시도

- A 포털 심스와핑 통해 '계정찾기', '비밀번호재설정', '2차인증 해제'로 계정정보 탈취
- B 메신저 심스와핑 통해 '계정찾기', '비밀번호재설정'로 계정정보 탈취

3. C가상화폐거래소 계정 획득

- 심스와핑 통해 '비밀번호 찾기' 기능으로 1차 인증 획득
- 심스와핑 통해 'OTP 재발급' 통한 2차 인증 획득

4. 피해자의 가상화폐거래소 계정 접근 및 가상 자산 탈취

■ 심스와핑 공격 대응 방안

1. 유심(USIM) 비밀번호 설정

유심은 스마트폰 사용자를 인증하는 수단으로 사용될 수 있기 때문에 이를 악용한다면 금전적인 피해로 이어질 수 있다. 이러한 공격을 방지하는 방법은 유심에 비밀번호를 설정하는 것이다. 유심기변을 시도할 때마다 설정한 비밀번호를 입력해야 하기 때문에 타인이 무단으로 유심을 사용하는 것을 방지할 수 있다. 다만 공격자가 피해자의 개인정보를 훔쳐 별도의 유심을 발급한 경우 유심 비밀번호로는 공격을 막을 수 없다.

※ 초기 유심 카드 비밀번호는 0000(4개) 또는 00000000(8개)이며 제품과 제조사에 따라 상이할 수 있다. 또한 비밀번호 3회 이상 틀릴 경우 유심이 잠기므로 무리하게 시도하지 말아야 한다.

2. 엠세이퍼(M-Safer) - 이동전화 가입 제한 서비스 이용

한국정보통신진흥협회(KAIT)에서 운영 중인 엠세이퍼(www.msafer.or.kr)를 이용하면 개인정보 유출에 의한 유심 발급을 방지할 수 있다. 엠세이퍼에서는 '이동전화 가입제한 서비스', 'SMS 및 이메일 안내 서비스'를 제공하고 있다. 이동전화 가입제한 서비스는 통신사 별로 신청해야 하는 가입제한을 일괄적으로 처리해 주는 서비스이며 명의 도용에 의한 이동전화 신규 가입 및 명의변경을 사전에 차단할 수 있다. 또한 SMS 및 이메일 안내 서비스는 본인의 명의로 이동전화가 개통되는 경우 SMS 또는 이메일로 알람을 받을 수 있어 무단 개통이 발생하는 경우 빠르게 조치할 수 있다.

3. 심스와핑 의심 시 가상화폐거래소 계정 잠금 요청 및 유심 이용정지 신청

아침 시간에 스마트폰이 갑자기 먹통이 되거나, 메신저 또는 메일에 타인에 의한 계정 상태 변경 기록이 남아 있다면 심스와핑 공격을 의심할 수 있다.

심스와핑 공격은 주로 이른 새벽 시간대에 발생하며, 복제 유심이 타 기기에 삽입되어 인증되는 경우 피해자가 기존에 사용하던 스마트폰은 정상적인 통신이 불가한 상태가 된다. 만일 메일 또는 메신저에 제3자에 의한 계정 탈취를 시도한 흔적이 남아 있다면 즉시 가상화폐거래소의 계정 잠금 기능을 이용하여 로그인과 출금을 막아야 한다. 국내 사례에서 확인할 수 있듯 공격자는 최종적으로 피해자의 가상 자산을 노리고 있다. 공격자의 목표가 가상 자산인 만큼 자신이 사용하는 가상화폐거래소의 계정 잠금 설정 방법을 숙지하고 있는 것이 좋다.

또한 심스와핑을 인지한 즉시 이동통신사 고객센터를 통해 이용정지를 신청하는 것이 추가적인 피해를 막을 수 있는 방안이다. 다만 개인정보를 탈취하여 명의를 도용한 경우 피해자가 기존에 사용하던 통신사가 아닌 다른 통신사에서 개통될 가능성도 존재한다. 따라서 엠세이퍼(www.msafer.or.kr)에서 '가입사실 현황조회 서비스'를 이용하여 개통된 유심을 확인하고 아래 도표의 통신사별 고객센터에 문의하여 유심 이용정지를 신청해야 한다.

infosec

분류	SKT	KT	LGU+	LG헬로비전	KCT	세종텔레콤	알뜰폰
무료	114, 080-011-6000 (유선)	114, 080-000-1618	114, 080-019-7000	070-7373-1002~3 (LG헬로비전 이용자)	080-1300-114	080-880-9300	각 통신사별 문의
유료	1599-0011	1588-0010	1544-0010	1855-1144	1877-9115	1688-9300	-

■ 참고 URL

https://m.boannews.com/html/detail.html?mtype=1&idx=104183
https://m.boannews.com/html/detail.html?mtype=1&idx=104097
https://m.boannews.com/html/detail.html?mtype=1&idx=103915
https://www.hankookilbo.com/News/Read/A2022021515400003908
https://cointelegraph.com/news/sim-swapping-how-hackers-stole-millions-worth-of-crypto-via-victims-telecoms-operator
https://www.justice.gov/opa/pr/massachusetts-man-pleads-guilty-operating-nationwide-scheme-steal-social-media-accounts-and
https://www.abcactionnews.com/money/consumer/taking-action-for-you/cybercriminals-cleanout-cryptocurrency-using-sim-card-swap-scam
https://www.pcmag.com/news/canadian-teen-arrested-for-sim-swap-attack-that-looted-36-million
https://post.naver.com/viewer/postView.naver?volumeNo=33149073&memberNo=36310338&vType=VERTICAL
https://www.forbes.com/sites/jeanbaptiste/2019/08/31/why-twitter-blames-att-for-ceo-jack-dorsey-account-hack-sending-shocking-racist-tweets/
https://www.vice.com/en/article/d3n3am/att-and-verizon-employees-charged-sim-swapping-criminal-ring
https://www.vice.com/en/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-scam
https://www.boannews.com/media/view.asp?idx=104785
https://abcnews.go.com/Politics/sim-swap-scams-netted-68-million-2021-fbi/story?id=82900169