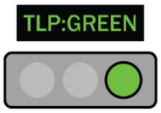
SIM swap csalás

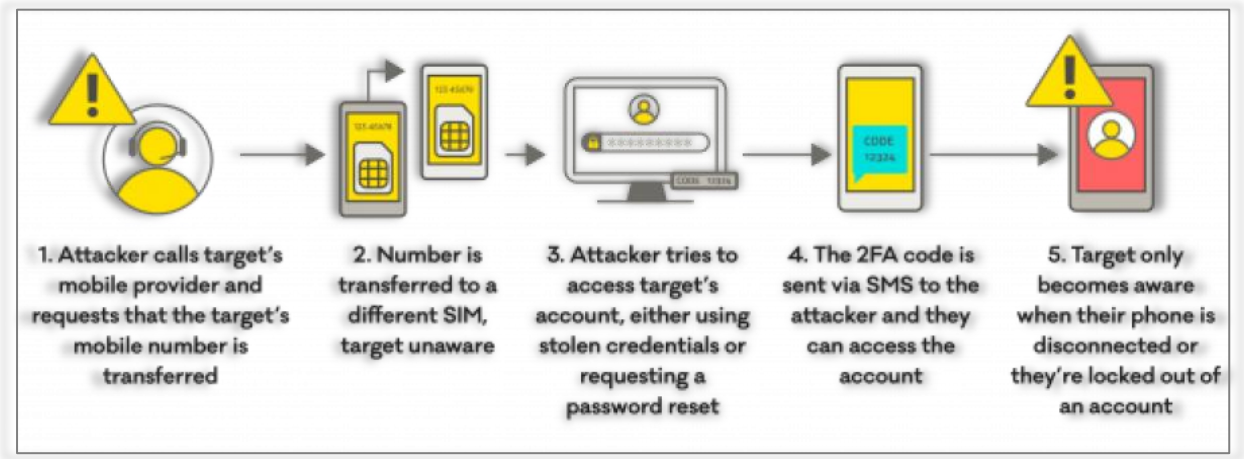


SIM swap csalás

Az elmúlt években megnövekedett a SIM swap módszerrel elkövetetett csalások száma az egész világon. A kiberbűnözők olyan komplex módszert használnak, amellyel a felhasználóktól célzott adathalászattal szereznek meg érzékeny adatokat, melyek felhasználásával további csalásokat hajtanak végre, elsősorban anyagi haszonszerzés céljából.

A SIM swapping bemutatása

A komplex módszer első eleme, hogy a csalók illegális kémprogram telepítésével vagy adathalász eszközökkel megszerzik többek között az áldozat jelszavát, felhasználóneveit, számlavezető bankjának nevét, a folyószámláját, a lakcímét, illetve a személyazonosító okmányainak számát.



1. ábra SIM swapping folyamata

A SIM swap (SIM csere) csalásnál a mobiltelefon eltulajdonítása nem szükséges, sőt az elkövetővel sem kell találkoznunk. A csaló a korábban megszerzett személyes adatok segítségével megszemélyesíti a mobil valódi tulajdonosát, majd az áldozat telefonszolgáltatójánál valamilyen ürüggyel igényel egy „új" SIM kártyát (leggyakoribb indok: kisebb kártyára van szüksége készülékcsere miatt). Ezt követően az áldozatnál lévő SIM kártya inaktiválódik, a telefonszám pedig aktívvá válik a csaló tulajdonában lévő SIM kártyán.

2. ábra Az áldozat és a csaló telefonja támadás után

Ez a csalási módszer nagy problémát jelent, hiszen számos szolgáltató még mindig SMS-t használ a többfaktoros hitelesítésnél használt biztonsági kódok kiküldésére. A telefonszámunkra érkező sms-ben lévő kódok, második autentikációként szolgálnak az egyéb azonosítóink és jelszavaink mellett. Arra használjuk, hogy belépjünk a netbankukba, közösségi média fiókunkba vagy akár jelszó visszaállításra is. A SIM swap visszaélés erre a funkcióra épül, hiszen a csalónál lévő SIM kártyára érkeznek majd a biztonsági kódot tartalmazó sms-ek például a bankunktól. Így a már első lépében megszerzett belépési adatok mellé megkapott sms-el, banki tranzakciót is indíthatnak.

Eszközök, Technikák és Eljárások

A SIM swap csalás általában az illetékes személyek meggyőzésével jár, a támadó valamilyen legenda segítségével rábírja az ügyfélszolgálatot, hogy helyezze át a telefonszám irányítását hozzájuk. A támadók a SIM swapping elkövetéséhez **többféle módszert és technikát** alkalmaznak, amelyek közül az alábbiak a legjellemzőbbek:

- ***Adathalászat (phishing):*** Hamis e-maileken, sms-eken és weboldalakon keresztül a támadó megszerzi a személyes adatokat, amelyekkel később hitelesíti magát a szolgáltatónál.
- ***Pszichológiai manipuláció (social engineering):*** A támadó félrevezeti a távközlési szolgáltató ügyfélszolgálatát, és az áldozat nevében kér egy új SIM kártyát.
- ***Belső alkalmazottak bevonása:*** A támadók megpróbálják megvesztegetni a szolgáltató munkatársait, hogy azok közvetlenül hajtsák végre a szám áthelyezését.
- ***Technikai visszaélések:*** Automatizált eszközök vagy rendszerek sérülékenységeinek kihasználása a SIM swap végrehajtásához.

Nemzetközi vonatkozás

Kanadában egy torontói házaspár összesen 140 000 USD-t vesztett a SIM swap támadás miatt. A támadók kisajátították a számukat és hozzáfértek a kriptotárcájukhoz – az eset nagy médiavisszhangot kapott.

SEC[1] (USA) X fiók támadás: A támadók átírták az SEC hivatalos X bejegyzését kripto-ETF jóváhagyásról, aminek hatására a Bitcoin ára rövid időre 10%-kal emelkedett.

Egyesült királyság: 2025. áprilisában történt kibertámadás következtében a Marks & Spencer online webáruháza leállt és a boltok működésében is zavar keletkezett. A cég szerint az online üzlet működése júliusig is akadozhat, és akár 300 millió fontnyi profitkiesést is jelenthet. A támadást SIM swapping módszerrel hajtották végre, amely lehetővé tette a támadók számára, hogy hozzáférjenek a kétfaktoros hitelesítési kódokhoz és érzékeny fiókokhoz.

2025-ben a **Közel-Kelet régiójában** nagymértékben megnőtt a SIM swap csalások száma. A támadók jellemzően **phishing weboldalakat** és **social engineering** technikákat használnak arra, hogy megszerezzék az áldozatok személyes adatait.

SIM swapping elleni védelem

A SIM swapping támadások elleni védekezés két szinten is megvalósulhat: felhasználói és szolgáltatói oldalon is. Mindkét oldalon szükséges különböző intézkedéseket bevezetni a kockázatok csökkentése érdekében.

1. ***Felhasználói szintű védelem***

Az sms alapú kétlépcsős azonosítás sérülékeny a SIM cserével szemben. Ezért ajánlott az autentikációs applikációk (pl. Google Hitelesítő vagy az Authy) használata SMS helyett, a kétfaktoros hitelesítéshez. Az említett alkalmazások a telefonkészüléken generálnak kódokat, így a csalók nehezebben férnek hozzá. Fontos, hogy ne osszunk meg nyilvánosan e-mail címet, telefonszámot és lakcímet. Továbbá PIN- vagy jelszavas védelem beállítása a szolgáltatói fiókokhoz, illetve értesítések bekapcsolása a fiókmódosításokról és az új eszközökről.

2. ***Szolgáltatói szintű védelem***

Számhordozás előtti erősebb ügyfél azonosítás (pl. fényképes azonosítás). Emellett számzáras funkciók bevezetése, mint a „Number Lock” vagy a „Wireless Lock”. A „Number Lock” funkciót, a Verizon amerikai telekommunikációs vállalat, a „Wireless Lock” funkciót pedig az AT&T telekommunikációs vállalat vezette be, a SIM swapping támadások ellen. A számzáras funkciók segítségével az ügyfelek be tudnak jelentkezni az adott vállalat mobilalkalmazásába vagy weboldalára, ahol lezárhatják a telefonszámukat. Ez megakadályozza, hogy bárki más

[1] **SEC** - U.S. Securities and Exchange Commission, vagyis az Amerikai Értékpapír- és Tőzsdefelügyelet, az Egyesült Államok szövetségi kormányának egyik független ügynöksége, amely az értékpapírpiacok felügyeletéért és szabályozásáért felel.

átvigye a számot egy másik SIM kártyára vagy szolgáltatóhoz. Emellett más típusú információk módosítását is védi, mint például a számlázási adatok, illetve a jogosult felhasználók megváltoztatása.

Következtetések

A SIM swapping egyre elterjedtebb és kifinomultabb formája a digitális csalásoknak, amely súlyos anyagi és adatbiztonsági következményekkel járhat mind az egyének, mind a szervezetek számára. A támadók személyes adatainkat felhasználva könnyedén megszerezhetik az irányítást a telefonszámunk felett, ezzel hozzáférhetnek pénzügyi fiókjainkhoz, közösségi profiljainkhoz vagy akár a kriptotárcáinkhoz is. A támadók célja sokszor a pénzszerzés, és ehhez nemcsak technikai eszközöket, hanem megtévesztést és társadalmi manipulációt is bevetnek. Fontos a megelőzés, mind a felhasználói, mind a szolgáltatói oldalon. Felhasználói oldalon az sms alapú hitelesítés helyett, biztonságosabb, ha autentikációs alkalmazásokat használunk. Szolgálati oldalon pedig nélkülözhetetlen a szigorúbb ügyfélazonosítás mellett olyan technikai megoldások bevezetése, mint a számzáras funkciók (pl. „Number Lock” vagy „Wireless Lock”), amelyek megakadályozzák a telefonszám jogosulatlan áthelyezését.

Források:

https://www.bleepingcomputer.com/news/security/atandt-rolls-out-wireless-lock-feature-to-block-sim-swap-attacks/

https://cointelegraph.com/learn/articles/what-is-a-sim-swap-attack

https://www.ownyouronline.govt.nz/personal/know-the-risks/common-risks-and-threats/sim-swapping-attacks/

https://raketa.hu/hogyan-vedekezhetunk-a-sim-csere-atveres-ellen

https://www.telekom.hu/rolunk/telekom_vilaga/biztonsagi_tartalmak/csalas/sim-swap-csalas

https://www.the-sun.com/news/10861078/cell-phone-sos-mode-customer-panics-140k-scam-canada/

https://www.yubico.com/resources/glossary/sim-swap/

https://yohomobile.com/hu-HU/how-to-tell-if-youve-been-sim-swapped