**Socjotechniczne sztuczki pozwalają na milionowe wyłudzenia. Groźne narzędzie na dostępne niemal dla każdego.**

**Socjotechniki, czyli wszelkiego rodzaju manipulacje ofiarami, są jednym z najważniejszych elementów ataków hakerskich. W ostatnich miesiącach ofiarami tego typu działań byli m.in. polscy użytkownicy bankowości internetowej. Eksperci Check Point Research ostrzegają przed kolejnymi, bardziej zaawansowanymi atakami, podobnymi do zaobserwowanej w Iranie potężnej kampanii SMS-owej, w której cybernapastnicy podszywali się pod instytucje rządowe w celu przejęcia danych płatniczych i informacji osobistych. Co ciekawe, narzędzia do przeprowadzenia takich ataków można zakupić na czarnym rynku za zaledwie 100 dolarów!**

W swoich przewidywaniach na rok 2022 eksperci bezpieczeństwa cybernetycznego z Check Point Software Technologies wskazywali, że phishing będzie jednym z najczęściej wykorzystywanych taktyk przez cyberprzestępców. Jak się okazuje, pod koniec 2021 roku trend ten się nasila m.in. w Polsce: pod koniec listopada media informowały o kampanii [phishingowej wymierzonej w klientów mBanku](https://finanse.wp.pl/niemal-perfekcyjne-oszustwo-uwazaj-ta-strona-podszywa-sie-pod-mbank-6710303007054432a), a zaledwie kilka dni wcześniej [sandomierska policja opisywała](https://sandomierz.policja.gov.pl/tsa/dzialania-policji/aktualnosci/53259%2CUwaga-na-oszustow-podszywajacych-sie-pod-pracownikow-banku.html) incydent w którym oszuści wyłudzili przeszło 30 tys. złotych od 37-letniej kobiety. Z kolei we wrześniu zeszłego roku cyberprzestępcy próbowali wykorzystać sytuację epidemiczną, podszywając się pod [Inspekcję Sanitarną](https://sekurak.pl/uwaga-na-smsy-perfekcyjnie-podszywajace-sie-pod-sanepid-sms-spoofing/).

Zdaniem ekspertów Check Point Research, tego typu działań będzie coraz więcej, a za przykład podają niedawną socjotechniczną kampanię SMS-ową skierowaną przeciwko obywatelom Iranu, w której cyberprzestępcy podszywający się pod irański rząd, rozsyłali wiadomości zachęcające do pobrania złośliwych aplikacji na Androida, które miały ułatwić przebieg spraw sądowych. W rzeczywistości aplikacja została stworzona by przejmować dane uwierzytelniające kart kredytowych oraz dwuskładnikowe kody uwierzytelniające. W momencie ich uzyskania cyberprzestępcy mieli już otwartą drogę do wykonywania nieautoryzowanych wypłat z kont swoich ofiar.

Jak wyjaśniają eksperci Check Point Research, w irańskiej kampanii wykorzystano technikę znaną jako botnet „smishing”, w której zhakowane urządzenia są wykorzystywane jako boty do rozprzestrzeniania podobnych wiadomości SMS phishingowych na inne potencjalne ofiary. Analitycy szacują, że cyberprzestępcy stojący za tymi atakami naruszyli i zainstalowali złośliwe oprogramowanie na dziesiątkach tysięcy urządzeń z Androidem, co doprowadziło do kradzieży miliardów irańskich rialów. Wg szacunków przeciętny łup z każdej ofiary mógł wynieść nawet 1000-2000 dolarów. Co więcej, dochodzenie przeprowadzone przez Check Point Research ujawniło, że dane skradzione z urządzeń ofiar są swobodnie dostępne online dla osób trzecich, ponieważ nie były należycie chronione.

**Jak przeprowadzono atak?**

1. Atak rozpoczynał się od phishingowej wiadomości SMS. W wielu przypadkach była to wiadomość z elektronicznego systemu powiadamiania sądowego, która powiadamia ofiarę o wniesieniu przeciwko niej nowej skargi. Wiadomość SMS zawiera łącze do strony internetowej umożliwiającej dalsze postępowanie w sprawie skargi.

2. Strona internetowa zachęca użytkownika do pobrania złośliwej aplikacji na Androida i wprowadzenia danych karty kredytowej pod pozorem niewielkiej opłaty za usługę.

3. Po zainstalowaniu złośliwa aplikacja kradła wszystkie wiadomości SMS z zainfekowanego urządzenia, umożliwiając atakującym korzystanie z karty kredytowej z dostępem do SMS z uwierzytelnianiem dwuskładnikowym wysyłanych przez firmy obsługujące karty kredytowe.

4. Złośliwa aplikacja okresowo sprawdzała kontrolowany przez atakującego serwer C&C w poszukiwaniu nowych poleceń do wykonania. Najbardziej godne uwagi jest polecenie rozsyłania dodatkowych wiadomości SMS phishingowych na listę nowych numerów telefonów.

Niestety, podobne ataki mogą w przyszłości dotyczyć również Polaków. Zdaniem ekspertów hakerzy wykorzystują m.in. kanały Telegram do promowania i sprzedaży narzędzi, wykorzystanych w irańskim ataku phishingowym. Za kwotę 50-150 dolarów cyberprzestępcy udostępniają pełny zestaw „Android Campaign Kit”, w tym złośliwą aplikację oraz podstawową infrastrukturę wraz z panelem sterowania, którym może łatwo zarządzać każdy niewykwalifikowany napastnik za pomocą prostego interfejsu bota Telegram! Oznacza to, że podobne sztuczki mogą być wykorzystywane w najbliższych miesiącach również przeciw kolejnym użytkownikom Androida i bankowości internetowej.