Gmina Mielec
ul. Głowackiego 5, 39-300 Mielec
Godziny pracy Urzędu: pon.: 7:30 - 17:00, Wt. - Czw.: 7:30 - 15:30, Pt.: 7:30 - 14:00
Telefon: 17 773 05 90 Fax: 17 773 05 91 Email: sekretariat@ug.mielec.pl

Ostrzeżenie CERT Polska o kampanii z trojanem bankowym Hydra

2023-01-18 13:21:32

Pełna treść ostrzeżenia dostępna w komunikacie "Trojan bankowy Hydra znowu w natarciu - nowa kampania" na stronie CERT.

- **Szczególnie narażeni użytkownicy: Klienci banków**
- **Wektor ataku: Wiadomości email**
- **Możliwe skutki: Zainfekowanie telefonu szkodliwym oprogramowaniem Hydra**
- **Atakowane platformy: Android**

Po ponad rocznej przerwie złośliwe oprogramowanie Hydra znowu jest wykorzystywane przez oszustów. Cel ataku jest wciąż taki sam - zainfekowanie telefonów z Androidem.

Schemat działania

Potencjalne ofiary otrzymują wiadomość mailową z domeny zbliżonej do domeny banku. W ostatnich odsłonach kampanii wykorzystywany jest logotyp banku Santander, warto jednak pamiętać, że oszuści mogą używać wizerunków innych podmiotów.

W wiadomości przestępcy informują o rzekomym braku instalacji aplikacji zabezpieczającej na urządzeniu mobilnym. Ma to być powodem zablokowania konta, które zostanie odblokowane dopiero po spełnieniu zalecanych kroków. Wiadomość zawiera link, który przenosi ofiarę na stronę podszywającą się pod bank.

Cyberprzestępcy w pierwszym etapie zachęcają ofiary do wpisania danych uwierzytelniających do bankowości internetowej.

Następnie strona oferuje pobranie wspomnianej aplikacji banku. Swoim wyglądem przypomina prawdziwą aplikację, jednak w rzeczywistości jest to złośliwe oprogramowanie.

Skutki oszustwa

Celem tego oszustwa jest zainfekowanie telefonów z Androidem szkodliwym oprogramowaniem Hydra, które po instalacji na urządzeniu mobilnym umożliwia m.in. kradzież danych uwierzytelniających do bankowości elektronicznej oraz danych kart płatniczych zapisanych na urządzeniu. Hydra, dzięki uzyskaniu specjalnych uprawnień, przejmuje kontrolę nad urządzeniem np. w momencie korzystania z aplikacji bankowej. Cyberprzestępcy zdobywają dane uwierzytelniające przez specjalne nakładki, które imitują prawdziwą stronę logowania do banku.

Co zrobić w przypadku, gdy wyłudzono dane logowania do bankowości internetowej?

W tym przypadku zalecamy podjąć następujące kroki:

- **jeśli doszło do kradzieży pieniędzy z konta, należy możliwie najszybciej skontaktować się ze swoim bankiem oraz zgłosić sprawę na najbliższym komisariacie policji,**
- **zmienić hasła do wszystkich kont, które były używane na telefonie,**
- **przywrócić telefon do ustawień fabrycznych.**

Samo wejście w link nie oznacza, że telefon zostanie zainfekowany. Hydra przejmie kontrolę nad urządzeniem, jeśli pobierze się szkodliwy plik i go zainstaluje.

Dziękujemy za odwiedziny i zapraszamy ponownie

bezpośredni link do strony www