Komunikat
FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP
z dnia 30 listopada 2021 r.
zagrożenia związane z instalacją zdalnego pulpitu

Zagrożenie - instalacja oprogramowania tzw. "zdalnego pulpitu" umożliwiającego przejęcie kontroli innej osoby nad urządzeniem, w którym to oprogramowanie zostało zainstalowane.

Co do zasady oprogramowania do zdalnego zarządzania np. komputerem są legalne i używane często przez administratorów sieci, jednak z takimi aplikacjami jest podobnie jak z nożem, może służyć do krojenia chleba, ale także może być wykorzystane jako narzędzie niebezpieczne - do popełnienia przestępstwa.

I tak się dzieje w tym przypadku, przestępcy używając zaawansowanej socjotechniki nakłaniają nieświadomych klientów (użytkowników usług płatniczych) do instalacji takiego oprogramowanie. FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP wraz z bankami identyfikuje sytuacje instalowania zdalnego pulpitu w incydentach Spoofing/Vishing oraz oszustwach inwestycyjnych na rynku FOREX i w kryptoaktywa.

W przypadku przestępstw Spoofing/Vishing przestępcy podszywając się pod instytucję zaufania publicznego np. bank informują o dokonaniu transakcji oszukańczej z konta osoby atakowanej. Prosząc o potwierdzenie mogą przekierować rozmowę do tzw. działu technicznego/wsparcia, który może poprosić o zainstalowanie takiego oprogramowania.

Natomiast przy przestępstwach związanych z inwestowaniem na rynku FOREX lub w kryptoaktywa, przestępcy wchodząc w rolę doradcy finansowego mogą sugerować potrzebę instalacji takiego oprogramowania w celu umożliwienia udzielenia klientowi zdalnej pomocy.

W związku z bardzo poważnym ryzykiem przejęcia kontroli nad komputerem, tabletem lub smartfonem pamiętajmy:

- nigdy nie instalujmy nieznanych aplikacji na czyjeś żądanie lub sugestię. Pamiętajmy, że przestępcy nigdy wprost nie powiedzą, że instalowana aplikacja może przejąć kontrolę nad urządzeniem klienta;
- bank nie poprosi Cię o instalację żadnej dodatkowej aplikacji oprócz mobilnej aplikacji bankowej, którą można pobrać z oficjalnej strony banku.

Jeśli niestety zainstalowałeś takie oprogramowanie to powinieneś podjąć w szczególności następujące działania w zalecanej kolejności:

1. natychmiast odinstaluj tę aplikacją;
2. jak najszybciej skontaktuj się z bankiem lub dostawcą internetowego serwisu i powiadom o ryzyku przejęcia Twojego konta przez osobę nieuprawnioną;
3. jeśli ujawniłeś dane do logowania do bankowości internetowej bezzwłocznie powinieneś zmienić hasło dostępowe do tego serwisu;

4. jeśli ujawniłeś dane karty płatniczej natychmiast powinieneś ją zastrzec za pośrednictwem bankowości internetowej lub dzwoniąc na telefoniczną linię międzybankową 828-828-828.
5. jeśli poniosłeś straty finansowe złóż zawiadomienie o popełnieniu przestępstwa na Policji lub w Prokuraturze.

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP
Centrum Wymiany i Analiz Informacji Sektora Finansowego

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP – jednostka operacyjna funkcjonująca w ramach Zespołu Bezpieczeństwa Banków Związku Banków Polskich, która gromadzi, analizuje oraz przekazuje w ramach sektora bankowego i we współpracy z organami ścigania oraz innymi instytucjami informacje dotyczące możliwych zagrożeń oraz o incydentach o charakterze przestępczym, godzących w bezpieczeństwo banków oraz ich klientów.