Popularny serwis Apple, z którego korzystają miliony użytkowników i przesyłają każdego dnia na platformę swoje dane bankowe, stał się obiektem ataku hakerów szukających poufnych danych bankowych. Rozsyłany e-mail to fałszywy rachunek za zakup, którego użytkownik nie dokonał.

Użytkownicy, którzy klikną w link podany w wiadomości, są proszeni o pobranie fałszywego czytnika plików PDF. Jeśli zgodzą się na pobranie, zostaną przekierowani na strony internetowe, które uruchamiają pobieranie innych złośliwych kodów, m.in. trojanów bankowych.

Popularna platforma Apple, iTunes, padła ofiarą ataków hakerów, których celem były miliony potencjalnych ofiar, wprowadzających każdego dnia dane swoich kart kredytowych do aplikacji. Celem ataków była kradzież danych i infekowanie komputerów – informuje PandaLabs, laboratorium systemów zabezpieczających firmy Panda Security.

Klienci serwisu iTunes otrzymują zręcznie przygotowany e-mail informujący o dokonaniu drogiego zakupu. Zaniepokojony e-mailem użytkownik, który nie dokonał takiego zakupu, chce jak najszybciej rozwiązać problem, klikając w link podany w wiadomości.

Jednak po kliknięciu w link, internauta proszony jest o pobranie fałszywego czytnika plików PDF. Po instalacji program przekierowuje na zainfekowane strony (głównie rosyjskie), zawierające m.in. trojany bankowe i inne złośliwe kody kradnące osobiste dane użytkownika.

„Phishing to nic nowego” - mówi Luis Corrons, dyrektor techniczny PandaLabs, „To, co nas nie przestaje zaskakiwać, to fakt, że techniki oszukiwania ofiar są wciąż tak proste. Choć muszę przyznać, iż wygląd i zawartość wiadomości są często bardzo dobrze przygotowane i pewnie dlatego tak łatwo wpaść w pułapkę. Kiedy korzystamy z takich platform jak iTunes i otrzymujemy tego rodzaju powiadomienia, absolutnie nie powinniśmy wchodzić na stronę przez e-mail, tylko przez samą platformę. Stan konta możemy sprawdzić w czasie rzeczywistym z samego konta. W ten sposób przekonalibyśmy się, że jest to próba ataku phishingowego”.

Technikę zgłoszono zespołowi ds. zwalczania phishingu (http://www.apwg.com/), który zaczął blokować niektóre adresy internetowe, do których odnośniki pojawiały się w fałszywym e-mailu.

Zalecamy wszystkim użytkownikom traktowanie takich e-maili z ostrożnością bez względu na to, jak autentycznie wyglądają. Jeśli sądzisz, że mogłeś paść ofiarą ataku, radzimy dokładnie przeskanować komputer w celu wyszukania ewentualnych aktywnych zagrożeń. Jeśli na twoim komputerze nie ma oprogramowania antywirusowego, możesz skorzystać z bezpłatnego programu Panda Cloud Antivirus, dostępnego do pobrania ze strony: http://www.cloudantivirus.com/pl/

Więcej informacji na można znaleźć na blogu PandaLabs.

Panda Security Polska