NukeBot: Nowa gotowa do ataku wersja niebezpiecznego trojana

ID artykułu: 51272 / 2264

URL: http://www.publikuj.org/51272

Badacze z Kaspersky Lab wykryli nowe szkodliwe oprogramowanie NukeBot, które zostało stworzone w celu kradzieży danych uwierzytelniających klientów bankowości online.

Wcześniejsze wersje tego trojana znane były w branży bezpieczeństwa pod nazwą TinyNuke, ale nie zawierały funkcji niezbędnych do przeprowadzania ataków. Natomiast najnowsze wersje są w pełni funkcjonalne i zawierają kod umożliwiający atakowanie użytkowników określonych banków.

Chociaż pojawienie się rodziny szkodliwego oprogramowania na wolności nie jest niczym niezwykłym, posiadanie przez przestępców gotowej do ataków wersji trojana oznacza, że wkrótce mogą oni przeprowadzić szkodliwą kampanię na szeroką skalę, infekując wielu użytkowników. W ramach wczesnego ostrzeżenia swoich klientów i innych użytkowników Kaspersky Lab opublikował krótką analizę tego szkodliwego oprogramowania.

NukeBot to trojan bankowy. Po infekcji szkodnik wstrzykuje szkodliwy kod do strony internetowej serwisu bankowości online wyświetlanego w przeglądarce ofiary, a następnie kradnie dane użytkownika, fałszuje jego dane uwierzytelniające i inne informacje. Według badaczy z Kaspersky Lab, kilka skompilowanych próbek tego trojana istnieje już na wolności i jest udostępnianych na podziemnych forach cyberprzestępczych. Większość z nich to robocze wersje szkodliwego oprogramowania, które nie są w pełni funkcjonalne, jednak eksperci z firmy zidentyfikowali również kilka próbek, które stanowią realne zagrożenie.

Około 5% próbek znalezionych przez Kaspersky Lab stanowiły nowe gotowe do ataku wersje NukeBota, które posiadają udoskonalony kod źródłowy oraz możliwości infekowania ofiar. Wersje te zawierają między innymi funkcje podszywania się pod elementy interfejsów istniejących serwisów bankowości online. Na podstawie analizy eksperci z Kaspersky Lab uważają, że głównym celem nowej wersji NukeBota są użytkownicy kilku banków francuskich i amerykańskich.

Ponadto badacze z Kaspersky Lab zdołali wykryć kilka modyfikacji NukeBota, które nie posiadały funkcjonalności wstrzykiwania sieciowego, a ich celem była kradzież haseł do klienta pocztowego i przeglądarki. To oznacza, że być może twórcy nowych wersji próbują rozszerzyć funkcjonalność tej rodziny szkodliwego oprogramowania.

Wprawdzie przestępcy stojący za najnowszymi wersjami omawianego szkodliwego oprogramowania jeszcze nie rozprzestrzeniają aktywnie NukeBota, wkrótce prawdopodobnie się to zmieni. Taki mechanizm obserwowaliśmy już wcześniej w przypadku kilku innych rodzin szkodliwego oprogramowania: po krótkim okresie testowym kodu gotowego do ataku cyberprzestępcy zaczynają rozprzestrzeniać go szeroko za pośrednictwem zainfekowanych stron internetowych, spamu i phishingu. Jak dotąd zidentyfikowaliśmy wersje NukeBota, które mogą zaatakować klientów co najmniej sześciu banków zlokalizowanych we Francji i Stanach Zjednoczonych, jednak wydaje się, że ta lista celów to dopiero początek. Celem naszego krótkiego badania jest ostrzeżenie środowiska bankowego oraz klientów bankowości online przed potencjalnym nowym zagrożeniem. Zachęcamy zainteresowane strony, aby wykorzystały wyniki naszego badania do zapewnienia sobie ochrony przed tym zagrożeniem, zanim dojdzie do ataku powiedział Siergiej Junakowski, ekspert ds. cyberbezpieczeństwa, Kaspersky Lab.

W celu zapewnienia sobie i swoim klientom ochrony przed atakami NukeBot eksperci ds. bezpieczeństwa z Kaspersky Lab zalecają następujące działania:

Dla organizacji finansowych świadczących usługi bankowości online:

Stosuj skuteczne rozwiązanie do zapobiegania oszustwom, które umożliwia szybkie i precyzyjne zidentyfikowanie nieautoryzowanego korzystania z kont klientów oraz podejrzanej aktywności finansowej.

Dla klientów serwisów bankowości online:

Stosuj rozwiązanie bezpieczeństwa zawierające wyspecjalizowane technologie do ochrony transakcji finansowych, np. moduł Bezpieczne pieniądze wbudowany w produkty Kaspersky Lab.

Regularnie skanuj system w celu wykrycia potencjalnych infekcji.

Produkty firmy Kaspersky Lab wykrywają omawiane szkodliwe oprogramowanie jako Trojan-Banker.Win32.TinyNuke.

Więcej informacji na temat gotowych do ataku wersji NukeBota znajduje się na stronie http://r.kaspersky.pl/nukebot.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie http://www.kaspersky.pl/nowosci.

Piotr Kupczyk
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska
E-mail: piotr.kup czyk@kaspersky.pl
Tel. 34 390 94 00

Aktywacja: 19/07/17 11:55, odsłony: 653