**Pierwszy trojan mobilny rozprzestrzeniany za pośrednictwem „obcych” botnetów**

**W ciągu ostatnich trzech miesięcy analitycy z Kaspersky Lab badali, w jaki sposób rozprzestrzenia się trojan Obad – najbardziej zaawansowany wykryty dotychczas szkodliwy program dla Androida.**

Okazuje się, że stojący za tym trojanem przestępcy zastosowali nową technikę - po raz pierwszy w historii cyberprzestępczości mobilnej trojan jest rozprzestrzeniany przy użyciu botnetów kontrolowanych przez inne grupy przestępcze. Stwierdzono również, że Obad jest głównie wykrywany w krajach Wspólnoty Niepodległych Państw. Łącznie 83% prób infekcji odnotowano w Rosji, poza tym wykryto je również na urządzeniach mobilnych na Ukrainie, Białorusi, w Uzbekistanie i Kazachstanie.

W najbardziej interesującym modelu dystrybucji Obad był rozprzestrzeniany wraz z trojanem Opfake. Ta próba podwójnej infekcji rozpoczyna się od SMS-ów nakłaniających użytkowników do pobrania otrzymanej niedawno wiadomości tekstowej. Jeżeli ofiara kliknie odsyłacz, na smartfon lub tablet zostanie automatycznie pobrany plik zawierający szkodnika Opfake.

Szkodliwy plik może zostać zainstalowany tylko wtedy, gdy zostanie uruchomiony przez użytkownika; jeżeli tak się stanie, trojan wyśle dalsze wiadomości do wszystkich kontaktów na nowo zainfekowanym urządzeniu. Kliknięcie odsyłacza w tych wiadomościach spowoduje pobranie programu Obad. Jest to dobrze zorganizowany system: jeden z rosyjskich dostawców usług komórkowych zarejestrował ponad 600 SMS-ów zawierających takie odsyłacze w ciągu zaledwie pięciu godzin, co wskazuje na masową dystrybucję. W większości przypadków szkodnik był rozprzestrzeniany przy pomocy zainfekowanych wcześniej urządzeń.

Oprócz wykorzystywania botnetów mobilnych ten wysoce złożony trojan jest również rozprzestrzeniany przy użyciu wiadomości spamowych. Jest to główny nośnik Obada. W celu nakłonienia ofiary do kliknięcia odsyłacza, który automatycznie pobiera na urządzenie mobilne szkodliwą aplikację, najczęściej wykorzystywana jest wiadomość zawierająca ostrzeżenie o niezapłaconych „długach”. Jednak i w tym przypadku, w celu zainstalowania trojana użytkownicy muszą uruchomić pobrany plik.

Obad jest również rozprzestrzeniany za pośrednictwem fałszywych sklepów z aplikacjami. Oszuści kopiują zawartość strony Google Play, zastępując legalne odsyłacze szkodliwymi. Warto zaznaczyć, że Obad.a atakuje wyłącznie użytkowników mobilnych. Gdy potencjalna ofiara odwiedzi taką szkodliwą stronę na komputerze domowym, nic się nie stanie. Inaczej sprawa się ma ze smartfonami i tabletami z dowolnym systemem operacyjnym – użytkownik zostanie przekierowany na wspomniane fałszywe strony (jednak na infekcję narażeni są tylko użytkownicy systemu Android).

*„W ciągu trzech miesięcy wykryliśmy 12 wersji trojana Obad. Wszystkie z nich posiadały ten sam zestaw funkcji oraz stosowały wysoki poziom zaciemniania kodu w celu utrudnienia analizy. Ponadto, każda wykorzystywała lukę w systemie Android, która nadaje szkodliwemu oprogramowaniu prawa administratora urządzenia i znacznie utrudnia jego usunięcie. Natychmiast poinformowaliśmy Google o naszym odkryciu, co zaowocowało usunięciem wspomnianej luki w wersji 4.3 Androida. Warto jednak podkreślić, że wersja ta jest wykorzystywana jedynie w przypadku kilku nowych smartfonów i tabletów: starsze urządzenia działające pod kontrolą wcześniejszych wersji systemu mobilnego Google’a nadal są zagrożone. Obad, który wykorzystuje dużą liczbę nieznanych luk, bardziej przypomina szkodliwe oprogramowanie dla systemu Windows niż inne trojany dla Androida”* – powiedział Roman Unuchek, ekspert ds. zwalczania szkodliwych programów, Kaspersky Lab.

Szczegóły techniczne dotyczące trojana Obad są dostępne w serwisie SecureList.pl prowadzonym przez Kaspersky Lab: <http://securelist.pl/blog/7225,najbardziej_zaawansowany_trojan_dla_androida.html>.

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/news>.