**Nowe zagrożenie na horyzoncie! Agent Smith zainfekował już 25 mln urządzeń**

**W trylogii Wachowskich “Agent Smith” opisuje ludzi jako gatunek rozmnażający się aż do czasu wyczerpania wszystkich zapasów. W rzeczywistości prawdziwym wirusem, rozprzestrzeniającym się z niepokojącą prędkością, jest “Agent Smith” - złośliwe oprogramowanie atakujące urządzenia mobilne, wskazuje firma Check Point Software Technologies.**

Dział Check Point Researchers niedawno odkrył nowy wariant złośliwego oprogramowania atakującego urządzenia mobilne, który w sposób niezauważalny zainfekował około 25 milionów urządzeń, o czym ich użytkownicy nie mieli najmniejszego pojęcia. Główna część tego programu, ukrywającego się pod postacią aplikacji Google, wykorzystuje różne luki systemu Android i automatycznie zastępuje aplikacje zainstalowane na urządzeniu ich złośliwymi wersjami bez jakiegokolwiek udziału użytkownika.

Jak do tej pory największa grupa ofiar to mieszkańcy Indii, chociaż są wśród nich również mieszkańcy innych krajów Azji, takich jak Pakistan i Bangladesz, a nawet znaczna liczba mieszkańców Wielkiej Brytanii, Australii i USA.

Malware ten, określany jako “Agent Smith”, obecnie wykorzystuje szeroki dostęp do zasobów urządzenia do wyświetlania fałszywych reklam w celu osiągnięcia korzyści finansowych. Jego działanie przypomina działanie występujących w przeszłości złośliwych programów, np. [Gooligan](https://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/), [Hummingbad](http://blog.checkpoint.com/2016/07/01/from-hummingbad-to-worse-new-in-depth-details-and-analysis-of-the-hummingbad-andriod-malware-campaign/) oraz [CopyCat](https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world/) i może infekować wszystkie smartfony, nawet te z wersjami programu Android 7.0.

“Agent Smith” służy do osiągania zysków finansowych poprzez wyświetlanie złośliwych reklam. Jednak może on być z łatwością wykorzystywany do działań o większym stopniu ingerencji i szkodliwości, np. kradzieży danych umożliwiających dostęp do kont bankowych, a także podsłuchów. Co więcej, ze względu na zdolność do ukrywania ikon tak, że nie są widoczne oraz do udawania istniejących popularnych aplikacji cieszących się zaufaniem użytkownika, złośliwe oprogramowanie może spowodować wiele szkód na urządzeniu użytkownika.

**Co robi “Agent Smith”?**

Atak oprogramowania “Agent Smith” odbywa się w ramach trzech zasadniczych etapów.

Na pierwszym z nich użytkownik urządzenia mobilnego jest nakłaniany do pobrania aplikacji wprowadzającej ze sklepu z aplikacjami, takiego jak 9Apps. Aplikacje te zazwyczaj mają formę bezpłatnych gier, aplikacji użytkowych lub aplikacji rozrywkowych dla osób dorosłych, jednak zawierają zaszyfrowane złośliwe oprogramowanie. Następnie aplikacja inicjująca sprawdza, czy na urządzeniu zainstalowane są popularne aplikacje, np. WhatsApp, MXplayer, ShareIt i inne aplikacje znajdujące się na liście atakującego. Jeśli jakakolwiek z tych aplikacji znajduje się na zainfekowanym urządzeniu, “Agent Smith” na kolejnym etapie atakuje oryginalne aplikacje.

W drugim etapie, po pobraniu aplikacji wprowadzającej na urządzenie ofiary, aplikacja automatycznie odszyfrowuje złośliwe oprogramowanie do formy pierwotnej, tzn. pliku APK (plik instalacyjny systemu Android), który stanowi zasadniczą część ataku “Agenta Smitha”. Następnie aplikacja inicjująca wykorzystuje kilka znanych luk oprogramowania do zainstalowania właściwego programu złośliwego bez jakiejkolwiek interakcji z użytkownikiem.

Na trzecim etapie, złośliwy program prowadzi atak na każdą zainstalowaną aplikację znajdującą się na jego liście. Złośliwy program w sposób niezauważalny pobiera plik APK danej aplikacji, uzupełnia go o dodatkowe złośliwe moduły, a następnie wykorzystuje kolejny zestaw luk systemu do niezauważalnego zastąpienia oryginalnej wersji aplikacji wersją złośliwą.

Ponieważ “Agent Smith” został pierwotnie pobrany z popularnego niezależnego sklepu z aplikacjami 9Apps, przeznaczonego głównie dla klientów mówiących w języku hinduskim, arabskim, rosyjskim i indonezyjskim, nic dziwnego, że liczba zainfekowanych urządzeń jest tak duża. Jak wiadomo niezależne sklepy z aplikacjami często nie posiadają zabezpieczeń niezbędnych do blokowania aplikacji z oprogramowaniem adware.

Ze względu na tak przebiegłą metodę infekcji, jaką jest zastępowanie aplikacji zainstalowanych na urządzeniu ich złośliwymi wersjami, użytkownicy muszą pamiętać o konieczności pobierania aplikacji wyłącznie z zaufanych sklepów z aplikacjami, w celu ograniczenia ryzyka infekcji.

Jeśli Twoje urządzenie zostało zainfekowane przez aplikacje podobne do “Agenta Smitha” lub inne, wykonaj następujące działania w celu usunięcia złośliwych aplikacji.