**Check Point wykrywa kolejne zagrożenie w Google Play!**

**Firma Check Point Software Technologies wykryła za pomocą narzędzia Mobile Threat Prevention program typu malware w grze BrainTest. Aplikacja była opublikowana na Google Play dwukrotnie. Każda instancja miała od 100 000 do 500 000 pobrań według statystyk Google Play, zarażając w ten sposób od 200 000 do 1 miliona urządzeń. Check Point skontaktowało się z Google 10. września 2015, w wyniku czego aplikacja została usunięta ze sklepu 15. września 2015.**

Złośliwe oprogramowanie ukryte w grze na Androida zwanej BrainTest było opublikowane na Google Play dwukrotnie. Każda instancja miała od 100 000 do 500 000 pobrań według statystyk Google Play, zarażając w ten sposób od 200 000 do 1 miliona urządzeń. Check Point skontaktowało się z Google 10. września 2015, w wyniku czego aplikacja została usunięta ze sklepu 15. września 2015.

Oprogramowanie zostało pierwszy raz wykryte na smartfonie Nexus 5 i, pomimo że użytkownik próbował usunąć aplikację, pojawiła się ona ponownie na urządzeniu niedługo później. Nasza analiza tego złośliwego oprogramowania wskazuje na to, że korzysta ono z wielu zaawansowanych technik w celu uniknięcia wykrycia przez Google Play oraz pozostania na zainstalowanych urządzeniach.

Gdy tylko wykryto podejrzaną aplikację na urządzeniu, oprogramowanie Mobile Threat Prevention dostosowało strategie bezpieczeństwa w panelu zarządzania mobilnymi urządzeniami (MobileIron) zdalnie konfigurując zarażone urządzenia tak, aby nie miały one dostępu do służbowych danych.

Pomimo, że aplikacja jest w stanie wykonywać wiele czynności zlecanych przez cyberprzestępców, nasz zespół zaobserwował, że instaluje ona dodatkowe aplikacje na zainfekowanych urządzeniach. Co gorsza, złośliwe oprogramowanie instaluje rootkita, który pozwala na pobranie i uruchomienie dowolnego kodu na urządzeniu. Przykładowo może być to wykorzystane do wyświetlania niechcianych, irytujących reklam na urządzeniu albo pobrania programu, który przechwytuje loginy i hasła.

Najważniejsze informacje:

1. Próbki podejrzanego kodu znaleziono w aplikacji BrainTest na Google Play. Jego autor użył wielu sposobów aby uniknąć wykrycia przez Google, między innymi:

l Omijanie Google Bouncer poprzez wykrywanie, czy oprogramowanie jest uruchamiane z adresu IP należącego do zakresu używanego przez Google Bouncer i nie wykonywanie podejrzanych czynności w takim wypadku.

l Połączenie bomb czasowych, dynamicznego ładowania kodu oraz refleksji celem utrudnienia inżynierii wstecznej kodu

l Wykorzystanie najnowszego obfuskatora kodu (pakera) od Baidu, aby ponownie wprowadzić aplikację do Google Play po jej pierwszym usunięciu 24. Sierpnia

2. BrainTest wykorzystuje cztery exploity pozwalające na podniesienie poziomu uprawnień, co pozwala na zainstalowanie złośliwego oprogramowania jako aplikacji systemowej.

3. BrainTest korzysta ze strażnika anty-deinstalacyjnego, który wykorzystuje dwie aplikacje systemowe ponownie instalujące aplikację w przypadku jej usunięcia.

Po pierwszym wykryciu BrainTest, Google usunęło aplikację z Google Play. W ciągu kilku dni, zespół badaczy firmy Check Point wykrył kolejne wystąpienie pod inną nazwą pakietu, ale wykorzystujące ten sam kod. Autorzy złośliwego oprogramowania wykorzystali obfuskację w celu wrzucenia nowej wersji złośliwego oprogramowania na Google Play.

Szczegóły techniczne dostępne są pod adresem:

<http://blog.checkpoint.com/2015/09/21/braintest-a-new-level-of-sophistication-in-mobile-malware/>