

Duży wzrost cyberataków na urządzenia z systemem Android

Analitycy firmy G DATA zidentyfikowali około 3,2 miliona nowych złośliwych aplikacji do końca trzeciego kwartału 2018 roku, co stanowi wzrost o ponad 40 procent w porównaniu z analogicznym okresem w roku ubiegłym. Cyberprzestępcy coraz częściej atakują urządzenia przenośne, w szczególności te z systemami operacyjnymi Android. Powód: osiem na dziesięć osób na świecie korzysta ze smartphone'a wyposażonego w ten popularny system operacyjny. Dlatego też tak ważne jest korzystanie z aplikacji zabezpieczającej.

Prawie 12000 nowych przypadków złośliwego oprogramowania każdego dnia

Przewiduje się, że z końcem 2018 roku pobity zostanie nowy niechlubny rekord. Jedynie do końca trzeciego kwartału analitycy firmy G DATA odkryli prawie 3,2 miliona nowych próbek złośliwego oprogramowania atakującego system Android. Oznacza to, że badacze naliczyli dziennie około 11700 nowych złośliwych aplikacji na ten popularny system operacyjny. W porównaniu z analogicznym okresem w roku ubiegłym obserwujemy wzrost o ponad 40 procent. Aktualnie już osiągnięto wynik taki jak przez cały rok 2016. Poziom zagrożenia dla systemu Android osiągnął nowy rekordowo wysoki poziom. Jednak zagrożeniem nie jest jedynie złośliwe oprogramowanie – wciąż niebezpieczne jest pomijanie aktualizacji oprogramowania smartphone'ów.

Czy korzystanie z systemu Android jest niebezpieczne?

Gdy przyjrzymy się przedstawionym danym liczbowym nasuwa się pytanie: czy ogólnie rzecz biorąc Android jest niebezpieczny? Niełatwo odpowiedzieć na to pytanie. Warto najpierw przyjrzeć się udziałowi w rynku. Około 80 procent użytkowników smartphone'ów na całym świecie posiada urządzenie korzystające z systemu operacyjnego Android. Ma to oczywiście związek z niską ceną zakupu takiego smartphone'a. Dobre urządzenia z systemem Android można nabyć w stosunkowo niskich cenach.

Jednak Android wciąż musi stawić czoła problemowi przestarzałych urządzeń. Firma Google zajęła się tą kwestią w 2017 roku. W ramach projektu Treble stworzyła funkcję dla Android 8 i wyższych systemów umożliwiającą szybką dystrybucję aktualizacji. Mamy tu jednak do czynienia z pewnym haczykiem: zaledwie około jedno na pięć urządzeń posiada zainstalowany system Android 8, a od jego wypuszczenia na rynek w sierpniu 2017 minął już ponad rok. Najnowsza wersja Version 9 (Pie) wciąż zainstalowana jest na mniej niż 0,1 procent urządzeń.

Dostarczanie aktualizacji zabezpieczeń na czas

Kluczem do lepszej ochrony smartphone'ów i tabletów jest dostarczanie najnowszych aktualizacji zabezpieczeń na czas. Badacze zajmujący się tym zagadnieniem również podkreślają, że dostawcy urządzeń powinni reprezentować wyższe standardy.

Według raportu portalu technologicznego The Verge, od lata bieżącego roku firma Google zobowiązuje w oparciu o zapisy umowne producentów popularnych smartphone'ów z systemem Android do dostarczania aktualizacji zabezpieczeń co najmniej przez okres dwóch lat. Warunki umowy zakładają, że w pierwszym roku powinny zostać dostarczone co najmniej cztery aktualizacje zabezpieczeń od Google, a w drugim roku regularne dostarczanie aktualizacji również musi zostać utrzymane. Na koniec każdego miesiąca urządzenia muszą posiadać ochronę przed wszelkimi zagrożeniami wykrytymi ponad 90 dni wcześniej. Zapis ten podlega jednak pewnym ograniczeniom. Dotyczy wyłącznie smartphone'ów aktywowanych przez co najmniej 100000 użytkowników. Ponadto umowa zachowuje moc wyłącznie dla urządzeń wprowadzonych na rynek po 31 stycznia 2018 roku. Obszerne fragmenty rozporządzenia miały wejść w życie do 31 lipca tego roku, jednak w tym kontekście obowiązuje okres karencji do 31 stycznia 2019.

W przypadku Linux a mamy do czynienia z poważnymi zaległościami. Według Grega Kroah-Hartmana z Linux Foundation, znikomy odsetek smartphonów z systemem operacyjnym Android korzysta z najnowszego systemu Linux. Specjalista podaje, że aktualny system odkryto wyłącznie w opracowanej wewnątrz firmy Google linii urządzeń przenośnych Pixel. Dodaje, iż narażone na atak są w zasadzie wszystkie smartphone'y z systemem Android, poza tymi z serii Pixel. Wynika to z faktu, iż wszelkie zmiany w oprogramowaniu open source są publicznie dostępne i wystarczy, że atakujący sprawdzą, czego dotyczą łaty stworzone przez deweloperów.

Sprawdź oferty abonamentów komórkowych na portalu TaniAbonament.pl

Oprogramowanie szpiegujące źródłem niepokoju

Najnowsze doniesienia w zakresie oprogramowania szpiegującego atakującego smartphonę y z systemem Android to kolejne źródło niepewności. Złośliwe oprogramowanie jest w stanie skopiować prywatne dane z hosta oraz odczytać wiadomości z aplikacji WhatsApp. Rozwiązanie zabezpieczające G DATA Internet Security na system Android rozpoznaje to zagrożenie pod nazwą Android.Trojan-Spy.Buhsam.A. Smartphonę y to urządzenia, na których przechowuje się dużą ilość ważnych prywatnych danych. Przykład ten pokazuje, że zastosowanie rozwiązania zabezpieczającego na urządzeniu przenośnym dostarcza niezbędnej ochrony.

Virus Bulletin: Google poważnie traktuje zabezpieczenia IT dla systemu Android

Niebezpieczeństwo kryjące się za złośliwym oprogramowaniem jest teraz ważnym tematem również dla firmy Google. Eksperci branży zabezpieczeń IT spotykają się co roku na konferencji Virus Bulletin. W tym roku w jej ramach badacze z firmy Google wygłosili dwie prezentacje dotyczące złośliwych aplikacji atakujących system Android. W swoim wystąpieniu analityczka Maddie Stone przedstawiła wyjątkowo wyrafinowaną odmianę złośliwego oprogramowania podejmującą bardzo dużo działań, by uchronić się przed wykryciem przez zautomatyzowane systemy.

Drugą prezentację przedstawił Łukasz Siewierski, ekspert w zakresie zabezpieczeń, który opowiedział o kampanii opartej na złośliwym oprogramowaniu pre-instalowanym na smartphonę ach z systemem Android. Przeprowadzone przez niego analizy pokazały, że złośliwe oprogramowanie zostaje zainstalowane na etapie tworzenia systemu. Firma G DATA przedstawiała podobne doniesienia na konferencji Virus Bulletin 2015, a przede wszystkim także na blogu, i to już w roku 2014.

Pewna ochrona: po raz dziewiąty z rzędu najwyższe noty w teście instytutu AV-TEST

By ustrzec się przed niebezpieczeństwem, warto zaufać zweryfikowanym producentom oprogramowania. Rozwiązanie G DATA Internet Security na system Android osiągnęło maksymalne noty w najnowszym teście porównawczym AV-TEST. Po raz szósty z rzędu inteligentna aplikacja zabezpieczająca wykryła 100 procent złośliwego oprogramowania, a najwyższe noty otrzymała już dziewiąty raz z rzędu.

Instytut AV-TEST przeanalizował tym razem łącznie 20 produktów z zakresu zabezpieczeń na system Android. Wszystkie rozwiązania zabezpieczające musiały wykazać się skutecznością wszystkich swoich funkcjonalności oraz poziomem ochrony. Rozwiązanie G DATA Internet Security na system Android osiągnęło imponujący wynik we wszystkich kategoriach, w tym 100-procentową skuteczność wykrywania złośliwego oprogramowania. W ten sposób firma G DATA, niemiecki dostawca rozwiązań zabezpieczających, uzyskała prestiżowy certyfikat AV-TEST.

Dane testowe:

Testowane rozwiązania bezpieczeństwa: 20, w tym G DATA Internet Security

Platforma: Android

Okres: wrzesień 2018