**Rafel RAT atakuje Androida. Aktualizujcie systemy!**

**Użytkownicy Androida powinni mieć się na baczności! Tym razem najpopularniejszy mobilny system operacyjny atakowany jest przez trojana Rafel, posiadającego szerokie spektrum zastosowań – od spyware’u, infiltrującego użytkownika, aż po ransomware szyfrujące całe urządzenie.**

Android jest obecnie najpopularniejszym systemem na urządzenia mobilne, z którego korzysta ponad [3,9 miliarda aktywnych użytkowników w ponad 190 krajach](https://www.bankmycell.com/blog/how-many-android-users-are-there). Oznacza to, że trzy czwarte wszystkich urządzeń mobilnych działa właśnie na nim. To właśnie ogromna popularność tego systemu i jego otwarty charakter powoduje, że staje się coraz częstszym celem hakerów. Tym razem użytkowników Androida atakuje trojan zdalnego dostępu Rafel, który wykorzystany został przede wszystkim przeciwko użytkownikom w USA i Chinach, choć również w kilku krajach europejskich.

W jednej ze swoich [publikacji](https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/) eksperci Check Pointa zidentyfikowali **zespół APT-C-35 / DoNo, jako czołowego użytkownika Rafela**. Jego funkcje, takie jak zdalny dostęp, inwigilacja, eksfiltracja danych i mechanizmy utrwalania, czynią go potężnym narzędziem do prowadzenia tajnych operacji i infiltrowania celów o dużej wartości. Analitycy zebrali wiele próbek złośliwego oprogramowania i odkryli około 120 serwerów dowodzenia i kontroli. Dokonując analizy ofiar i odkryli, że najczęściej atakowanymi krajami były Stany Zjednoczone, Chiny i Indonezja.

*Zainfekowane urządzenia według kraju*

Większość ofiar posiadała telefony Samsung, a drugą co do wielkości grupę wśród docelowych ofiar stanowili użytkownicy Xiaomi, Vivo i Huawei. Nie stoją jednak za tym żadne większe teorie spiskowe, wynik ten odpowiada po prostu popularności urządzeń na różnych rynkach.

Intrygujące jest za to rozkład wersji Androida wśród dotkniętych ofiar. Najpopularniejszy jest Android 11, a następnie wersje 8 i 5. Pomimo różnorodności wersji Androida, złośliwe oprogramowanie może zwykle działać na nich wszystkich. Eksperci Check Pointa zwracają jednak uwagę, że nowsze wersje systemu operacyjnego zazwyczaj stwarzają większe wyzwania dla złośliwego oprogramowania w wykonywaniu swoich funkcji lub wymagają większej liczby działań ze strony ofiary, aby były skuteczne.

*Wersje Androida*

Jedną z rzeczy, którą stale się obserwuje w przypadku botów systemu Windows, jest niezmiennie wysoka liczba infekcji Windows XP, mimo że „koniec życia” tej wersji systemu nastąpił w 2014 roku. Ten sam scenariusz zaobserwowano w przypadku zainfekowanych urządzeń z systemem Android. **Ponad 87% dotkniętych ofiar korzysta z wersji Androida, które nie są już obsługiwane** i w związku z tym nie otrzymują poprawek bezpieczeństwa.

Check Point postanowił szczegółowo przeanalizować trzy konkretne przypadki ataków. Pierwszym była operacja oprogramowania ransomware dla systemu Android, podczas której ugrupowanie zagrażające szyfrowało pliki urządzenia. Drugim był wyciek wiadomości dwuskładnikowego uwierzytelniania (2FA), który prawdopodobnie mógł prowadzić do obejścia 2FA, natomiast ostatnim przypadkiem było zainstalowanie narzędzia Rafel na zhakowanej rządowej stronie internetowej.

Rafel RAT okazał się doskonałym przykładem ewoluującego krajobrazu szkodliwego oprogramowania dla systemu Android, charakteryzującym się otwartym kodem źródłowym, obszernym zestawem funkcji i powszechnym wykorzystaniem w różnych nielegalnych działaniach. Występowanie Rafela RAT uwydatnia potrzebę ciągłej czujności i proaktywnych środków bezpieczeństwa w celu ochrony urządzeń z Androidem przed złośliwym wykorzystaniem. Cyberprzestępcy w dalszym ciągu wykorzystują techniki i narzędzia, takie jak Rafel RAT, do naruszania prywatności użytkowników, kradzieży wrażliwych danych i popełniania oszustw finansowych, stąd niezbędne jest wielowarstwowe podejście do bezpieczeństwa urządzeń mobilnych.

**Oto rekomendowane przez Check Point Research kroki, które użytkownicy Androida muszą podjąć, aby zachować bezpieczeństwo:**

l

Instaluj aplikacje z zaufanych źródeł: pobieraj i instaluj aplikacje wyłącznie z renomowanych źródeł, takich jak Sklep Google Play. Unikaj zewnętrznych sklepów z aplikacjami i zachowaj ostrożność w przypadku aplikacji, które mają niewiele pobrań lub mają słabe recenzje. Przed instalacją zawsze sprawdzaj uprawnienia i recenzje aplikacji.

l

Aktualizuj swoje oprogramowanie: regularnie aktualizuj swój system operacyjny Android i aplikacje. Aktualizacje często zawierają poprawki zabezpieczeń, które chronią przed nowo wykrytymi lukami w zabezpieczeniach. Włącz automatyczne aktualizacje, aby mieć pewność, że bezzwłocznie otrzymasz najnowsze zabezpieczenia.

l

Użyj niezawodnej aplikacji zabezpieczającej urządzenia mobilne: zainstaluj renomowaną aplikację zabezpieczającą, która zapewnia ochronę w czasie rzeczywistym przed złośliwym oprogramowaniem. Aplikacje te potrafią skanować w poszukiwaniu złośliwego oprogramowania, wykrywać podejrzaną aktywność i zapewniać dodatkowe funkcje bezpieczeństwa, takie jak zabezpieczenia przed kradzieżą i bezpieczne przeglądanie.

Wykonując powyższe kroki, użytkownicy Androida mogą znacznie zmniejszyć ryzyko napotkania złośliwego oprogramowania i zwiększyć bezpieczeństwo swojego urządzenia.