NOWE ZŁOŚLIWE OPROGRAMOWANIE NARZĘDZIEM DO ATAKÓW NA TWÓRCÓW GIER

Nowe złośliwe oprogramowanie wykryte przez specjalistów ze słowackiej firmy ESET jest narzędziem do ataków na twórców gier komputerowych - donosi serwis Infosecurity Magazine. Operatorem wirusa ma być grupa hakerska Winnti.

Złośliwe oprogramowanie znane pod nazwą PipeMon było dystrybuowane wśród firm w Korei Południowej i na Tajwanie. Gry produkowane w tych krajach są sprzedawane na całym świecie i dostępne na popularnych platformach gamingowych, a jednocześnie korzysta z nich nierzadko tysiące graczy - pisze Infosecurity Magazine.

Zdaniem specjalistów z firmy ESET złośliwe oprogramowanie PipeMon pozwala na umieszczenie tzw. tylnych drzwi w oprogramowaniu i jest sygnowane certyfikatem, który najprawdopodobniej został wykradziony podczas poprzedniej kampanii hakerskiej, przez co wykazuje podobieństwa do innego wirusa o podobnej funkcjonalności, znanego jako PortReuse.

W co najmniej jednym przypadku atak z użyciem PipeMona zakończył się powodzeniem i doprowadził do naruszenia bezpieczeństwa jednego z firmowych serwerów, pozwalając hakerom na przejęcie kontroli nad procesami automatycznej kompilacji kodu. Może to pozwolić np. na wbudowanie robaków internetowych typu trojan do popularnych gier wideo, a także manipulację wirtualnymi walutami często oferowanymi w ramach transakcji wewnątrzrozgrywkowych w celach zysku finansowego - ostrzega ESET.

"Wiele wskaźników analizowanych w przypadku tych ataków doprowadziło nas do przypisania ich grupie Winnti. Niektóre komendy i domeny kontrolne wykorzystywane przez złośliwe oprogramowanie PipeMon były wykorzystywane już przez Winnti w innych kampaniach" - powiedział serwisowi Infosecurity Magazine badacz złośliwego oprogramowania w firmie ESET Mathieu Tartare. "Dodatkowo, w 2019 roku w niektórych firmach, które stały się w tym roku ofiarami Winnti, znaleziono już złośliwe oprogramowanie dystrybuowane wcześniej przez tę grupę" - dodał.