Cyberdefence 24

03.07.2020

NOWE ZŁOŚLIWE OPROGRAMOWANIE NA MAC OS UKRYTE W PIRACKICH APLIKACJACH

Nowe złośliwe oprogramowanie szyfrujące dla okupu (ransomware) na Mac OS dystrybuowane jest z użyciem pirackich aplikacji, które można pobrać z nielegalnej dystrybucji m.in. poprzez torrenty - ostrzegają eksperci z firmy Malwarebytes.

Pełniący funkcję dyrektora w Malwarebytes Thomas Reed w rozmowie z serwisem Infosecurity Magazine zaznaczył, że nowy wirus nazywa się OSX.ThiefQuest, stanowi jednak pochodną robaka internetowego EvilQuest już wcześniej znanego badaczom.

Po raz pierwszy złośliwe oprogramowanie odkryto w wyglądającej wiarygodnie, nielegalnej kopii oprogramowania obsługującego usługę firewalla Little Snitch na Mac OS. Pobrano ją z rosyjskiej strony z torrentami pozwalającymi na instalowanie pirackich wersji popularnego oprogramowania na komputery Apple'a. OSX.ThiefQuest znaleziono również w instalatorze aplikacji do tworzenia muzyki elektronicznej Mixed In Key 8. Według firmy Malwarebytes, wirus z pewnością rezyduje również w innych nielegalnych kopiach oprogramowania bądź ich plikach instalacyjnych.

Reed zwrócił uwagę, że złośliwe oprogramowanie dystrybuowane w ten sposób nie zaprezentowało do tej pory szczególnie wyszukanego działania. Wirus szyfruje szereg plików zawierających ustawienia systemowe oraz np. pliki zawierające dane z pęku kluczy (rejestru haseł) na Mac OS. Skutkiem działania robaka po stronie użytkownika jest wyświetlenie błędu na ekranie komputera - dodał Reed.

Inni eksperci wskazują, że nowy wirus może zawierać również kod tzw. keyloggera pozwalającego na rejestrowanie wszystkiego, co użytkownik zainfekowanego komputera wpisuje z użyciem swojej klawiatury. OSX.ThiefQuest może również wykradać informacje o portfelach kryptowalutowych, jeśli znajdzie na atakowanym komputerze powiązane z nimi pliki. Wirus wyposażony jest również w kod umożliwiający mu zwrotną komunikację z serwerem kontrolowanym przez operatorów.

Po zaszyfrowaniu plików OSX.ThiefQuest domaga się od ofiar okupu w wysokości 50 dolarów za odblokowanie dostępu do plików. Firma Malwarebytes twierdzi jednak, że obecnie nie ma informacji o istnieniu klucza deszyfrującego - eksperci prowadzą badania nad tym, jak skonstruowany jest szyfr wykorzystywany przez wirusa i jak można go złamać.