Cyberdefence 24

aut. Szymon Palczewski 29.04.2020

„PRZEPRASZAMY WSZYSTKICH POSZKODOWANYCH". CYBERPRZESTĘPCY ZAWIESZAJĄ DZIAŁALNOŚĆ

Twórcy złośliwego oprogramowania ransomware przepraszają ofiary i udostępniają instrukcję oraz elementy niezbędne do zneutralizowania wirusa. Opublikowane klucze deszyfrujące są prawdziwe i rzeczywiście pozwalają zlikwidować złośliwe oprogramowanie zainstalowane na danym urządzeniu. Grupa hakerska publicznie oświadczyła, że zaprzestała swojej działalności.

Operatorzy oprogramowania ransomware Shade, znanego również jako Troldesh, zamknęli swoje operacje, wydali ponad 750 000 kluczy deszyfrujących, a także przeprosili za wszystkie szkody, jakie ich narzędzie wyrządziło ofiarom. „Wszystkie dane związane z naszą działalnością zostały nieodwracalnie zniszczone" – czytamy w oświadczeniu udostępnionym w serwisie GitHub. W ten sposób grupa poinformowała o zaprzestaniu swojej działalności.

Wirus Shade działa od 2014 roku. W przeciwieństwie do innych rodzajów złośliwego oprogramowania, których celem są między innymi państwa zachodnie, Troldesh był przeznaczony do cyberataków wymierzonych w Rosję oraz Ukrainę – donosi Bleeping Computer.

W 2019 roku intensywność działań hakerskich z użyciem Shade uległa znacznemu osłabieniu. Wynika to z faktu, że w tamtym okresie operatorzy wirusa przestali dystrybuować oprogramowanie ransomware. Teraz jego twórcy przepraszają wszystkie ofiary i udostępniają wszelkie niezbędne instrukcje oraz elementy potrzebne do skutecznego zlikwidowania Troldesh.

„Podjęliśmy decyzję o (…) opublikowaniu wszystkich posiadanych kluczy deszyfrujących (w sumie ponad 750 000). Udostępniamy również nasze oprogramowanie do deszyfrowania" – czytamy w oświadczeniu. Twórcy wirusa wyrazili nadzieję, że posiadając wspomniane elementy firmy antywirusowe opracują i wydadzą własne, bardziej dopracowane narzędzia deszyfrujące. Zwieńczeniem oświadczenia były słowa: „przepraszamy wszystkie ofiary trojana i mamy nadzieję, że klucze, które opublikowaliśmy, pomogą im odzyskać swoje dane".

Sergei Golowanow, specjalista Kaspersky Lab, powiedział w wywiadzie dla Bleeping Computer, że udostępnione przez hakerów klucze są prawidłowe. Ekspert wykorzystał opublikowane elementy do odszyfrowania testowego urządzenia. Wszystko odbyło się bez przeszkód.