Cyberdefence 24

aut. Szymon Palczewski 16.04.2019

NOWA KAMPANIA HAKERSKA. KOLEJNA GRUPA WYSPECJALIZOWANA W SZPIEGOSTWIE

Specjaliści ds. cyberbezpieczeństwa wykryli nową kampanię cyberprzestępczą. Według ekspertów hakerzy, działając przez co najmniej 5 lat, wykorzystywali szereg narzędzi oraz innowacyjnych rozwiązań dla celów szpiegowskich.

Kampania została przez specjalistów nazwana „TajMahal". W jej ramach hakerzy wykorzystywali backdoory w systemach oraz oprogramowaniu, a także luki w zabezpieczeniach rejestratorów dźwięku, kamerkach internetowych czy narzędziach przeznaczonych do przechwytywania ekranu. Według analiz opublikowanych przez Kaspersky Lab, celem cyberprzestępców była kradzież danych i informacji w ramach szerszej operacji szpiegowskiej.

Sposób działania TajMahal opiera się na zupełnie nowych technikach oraz metodach hakerskich. Taki stan rzeczy sprawia, że grupa odpowiedzialna za kampanię nie wykazuje żadnych podobieństw do innych, znanych powszechnie podmiotów cyberprzestępczych, potocznie zwanych „APT", co znacznie utrudnia wykrycie oraz lokalizację jej członków.

Jak wskazują specjaliści Kaspersky Lab, hakerzy TajMahal są w stanie wykraść dane znajdujące się na „wypalonej" płycie CD lub we wbudowanej pamięci drukarki. „Mogą również wykraść informacje znajdujące się w konkretnym pliku na dowolnym nośniku USB" – tłumaczą eksperci. – „Ich działanie jest proste. Zwyczajnie przy podłączeniu urządzenia USB do danego komputera, do którego mają dostęp hakerzy, jego zawartość zostanie skradziona".

Kampania opiera się na dwóch szkodliwych oprogramowaniach – Tokio i Yokohama. Pierwsze z nich służy do początkowego zainfekowania urządzenia i zainstalowania drugiego, które odpowiada za tworzenie kopii zapasowych, a tym samym kradzież danych.

Według ekspertów Yokohama, to „w pełni funkcjonalny pakiet złośliwego oprogramowania". Wraz z kradzieżą informacji z płyt CD, drukarek, nośników USB oraz innych urządzeń, to innowacyjne narzędzie hakerskie dodatkowo wykonuje zrzuty ekranu, nagrywa dźwięk czy gromadzi dane z kopii zapasowych z urządzeń mobilnych. Co więcej, jest to oprogramowanie, które pomimo że zostanie usunięte może ponownie pojawić się na danym nośniku.

Specjaliści wykryli działalność hakerów w regionie Azji Środkowej. Jednak, jak sami wskazują, obszar ich działania jest prawdopodobnie znacznie większy.