MICROSOFT OSTRZEGA PRZED "NIEWYKRYWALNYM" ZŁOŚLIWYM OPROGRAMOWANIEM

Microsoft ostrzega przed atakami z użyciem złośliwego oprogramowania Astaroth, które do swojego działania nie potrzebuje plików, przez co jest w praktyce niewykrywalne. Celem hakerów wykorzystujących Astaroth jest wykradanie poufnych informacji.

Jak donosi serwis Infosecurity Magazine, pierwsze ataki z użyciem tego złośliwego oprogramowania wykryto na przełomie maja i czerwca tego roku. Astaroth służy hakerom do wykorzystania wbudowanego w system Windows narzędzia do uruchamiania skryptów (funkcja systemowa WMIC), dzięki czemu zyskują możliwość wykradzenia z systemu poufnych informacji.

Astaroth rozpowszechniany jest przez cyberprzestępców z wykorzystaniem techniki spear-phishingu, czyli ukierunkowanego na konkretną ofiarę ataku, który ma skłonić cel do kliknięcia w złośliwy odnośnik. Czynność ta uruchamia funkcję WMIC, która z kolei pozwala na zdalne wykonanie spreparowanego przez hakerów kodu JavaScript wykorzystującego w swoim działaniu pliki systemowe Windowsa, a Astaroth jest wstrzykiwany w końcowym etapie całego procesu i w praktyce niewykrywalny dla tradycyjnych narzędzi cyberbezpieczeństwa.

Jak wskazuje inżynier działu badań Microsoft Defendera Andrea Lelli, kluczowe w wykrywaniu tego rodzaju zagrożeń są metody heurystyczne i monitoring behawioralny ukierunkowany na anomalie w wykonywanych przez daną infrastrukturę czynnościach.

Według firmy Malwarebytes z kolei ataki z użyciem złośliwego oprogramowania, które w działaniu nie potrzebuje plików, w 2018 r. stanowiły 35 proc. wszystkich zagrożeń. Mogą one być nawet 10 razy bardziej skuteczne, niż inne metody działania hakerów.

Specjaliści z innej firmy z branży cyberbezpieczeństwa - Trend Micro - podają z kolei, iż liczba wykrytych zagrożeń tego rodzaju od sierpnia 2017 do grudnia 2018 roku wzrosła o 819 proc.

Źródło: AK/PAP