CYBERSZPIEGOSTWO W KOREI POŁUDNIOWEJ. PÓŁNOCNOKOREAŃSCY HAKERZY POWRACAJĄ

Północnokoreańscy hakerzy prowadzili złośliwą kampanię cyberszpiegowską, wymierzoną w obywateli Korei Południowej. Cyberprzestępcy jako „wabik" wykorzystali problematyczną kwestię dotyczącą uchodźców pochodzących z północy. Hakerzy zmienili dotychczasową taktykę działania w celu zmniejszenia ryzyka wykrycia.

Specjaliści południowokoreańskiej firmy ESTsecurity Security Response Center (ESRC) wykryli złośliwą kampanię hakerską pochodzącą z Korei Północnej – informuje serwis CyberScoop. Cyberprzestępcy odpowiedzialni za incydent prawdopodobnie są członkami ugrupowania cyberszpiegowskiego Geumseong121.

W ramach kampanii hakerzy zachęcają swoje ofiary do klikania w linki, które poruszają tematykę uchodźców z Korei Północnej. W rzeczywistości zamiast dostarczania informacji, załącznik pobiera na urządzenie użytkownika złośliwe oprogramowanie – informuje CyberScoop, powołując się na ESRC.

Operacja hakerska została nazwana przez specjalistów „Operation Spy Cloud", ponieważ opiera się na usługach w chmurze. Incydent pokazuje, że grupa Geumseong121 powraca do działania po licznych niepowodzeniach, które miały miejsce pod koniec ubiegłego roku. Jak przypomina CyberScoop, wówczas Microsoft przejął 50 stron internetowych używanych przez jej hakerów do prowadzenia kampanii spearphishingowych.

Według ESRC od momentu wykrycia cyberprzestępcy starają się ukryć swoje działania, stosując nową taktykę infekowania urządzeń. „Takie podejście pozwala hakerom modyfikować lub usuwać pliki w razie potrzeby, aby uniknąć wykrycia i zminimalizować ślad działania" – wskazują specjaliści ESRC, cytowani przez CyberScoop.

Eksperci tłumaczą, że po kliknięciu w link dane urządzenie jest infekowane złośliwym oprogramowaniem. Następnie wirus łączy się z serwerem kontrolowanym przez hakerów, Dyskiem Google oraz próbuje udostępnić informacje systemowe PickCloud.

Kampania, która rozpoczęła się na początku marca br. jest najnowszą operacją szpiegowską prowadzoną przez Geumseong121. Obejmuje ona zarówno urządzenia obsługiwane przez system Windows, jak i Android.

Specjaliści ESRC powiązali złośliwą kampanię z grupą Geumseong121, ponieważ taktyka, techniki, procedury oraz sposób działania są dokładnie takie same jak zastosowane w innej niedawnej operacji cyberszpiegowskiej przeprowadzonej przez tą grupę.

AK/SZP