MICROSOFT: WYKRYTO NOWĄ KAMPANIĘ PHISHINGOWĄ WYKORZYSTUJĄCĄ MOTYW KORONAWIRUSA

Nowa kampania phishingowa wykorzystująca motyw koronawirusa to zagrożenie, przed którym ostrzegają specjaliści Microsoftu. Hakerzy do swoich działań wykorzystują złośliwe makra w programie Excel i uzyskują w ten sposób zdalny dostęp do atakowanych komputerów.

Zespół ds. bezpieczeństwa Microsoftu poinformował o nowym zagrożeniu w serii wpisów w serwisie społecznościowym Twitter. Zdaniem ekspertów kampania cyberprzestępców rozpoczęła się 12 maja.

Spreparowane przez hakerów e-maile, które mają być przynętą dla ofiar, wyglądają tak, jakby wysłało je Centrum Johnsa Hopkinsa i są zatytułowane "RAPORT WHO O SYTUACJI COVID-19". Po otwarciu takiego listu automatycznie otwiera się plik programu Excel, w którym zawarty jest wykres rzekomo obrazujący sytuację epidemiczną w USA. Jedno z makr w arkuszu pobiera w tym czasie wirusa komputerowego pozwalającego na zdalny dostęp do komputera ofiary (oprogramowanie typu RAT).

Wykorzystanie makr do ataków hakerskich jest coraz częściej obserwowane przez ekspertów. Zdaniem Microsoftu liczba przypadków takich cyberataków od kilku miesięcy rosła w sposób stabilny, jednakże kwiecień - wraz z czasem izolacji społecznej celem ograniczania rozprzestrzeniania się pandemii przyniósł wzmożoną aktywność tego rodzaju. Cyberprzestępcy opierają swoje ataki na przynętach związanych z tematyką koronawirusa - ostrzega Microsoft.

Firma Google wcześniej w tym roku informowała, że dziennie blokuje nawet 240 mln złośliwych e-maili wykorzystujących do ataków na ofiary cyberprzestępców tematykę COVID-19 oraz 18 mln e-maili zawierających złośliwe oprogramowanie.

Specjaliści z branży cyberbezpieczeństwa oceniają, że głównym sposobem ochrony przed tego rodzaju zagrożeniami jest edukacja pracowników wykonujących swoje obowiązki zdalnie. "Phishing jest w gruncie rzeczy sposobem ataku na pracowników i to właśnie pracownicy pozostają najsilniejszą linią obrony przeciwko takim działaniom" - podkreśla badacz złośliwego oprogramowania związany z firmą DomainTools Tarik Saleh.