NOWA FALA CYBERATAKÓW NA AMERYKAŃSKI SERWIS PŁATNOŚCI

Zaobserwowano nową falę cyberataków na serwis płatności administracyjnych Click2Gov wykorzystywany do pobierania opłat przez władze wielu miast w USA. W ubiegłych latach hakerzy włamujący się do systemu tej usługi wykradli 300 tys. numerów kart płatniczych.

Jak poinformowali specjaliści z firmy Gemini Advisory, wykryta przez nich nowa fala ataków rozpoczęła się w sierpniu br. i do chwili obecnej objęła systemy Click2Gov w ośmiu miastach w pięciu amerykańskich stanach. Sześć spośród tych miejscowości ucierpiało również w wyniku poprzednich cyberataków na tę usługę.

W wyniku najnowszych ataków na internetowym czarnym rynku znalazło się już ponad 20 tys. rekordów z baz danych zawierających informacje finansowe Amerykanów. Specjaliści zwracają uwagę, że problem dotyczyć może mieszkańców wszystkich 50 stanów, którzy korzystali z Click2Gov np. podczas podróży. Click2Gov używany jest nie tylko przez władze miast, ale również przez firmy świadczące usługi komunalne, a także organizacje społeczne pobierające płatności np. za usługi parkingowe dla mieszkańców osiedli.

Serwis Ars Technica zwraca uwagę, że wiele zhakowanych portali samorządowych, które stały się furtką dla cyberprzestępców, działało w oparciu o zaktualizowane, najnowsze oprogramowanie. Nie jest zatem jasne, jak głęboko zdołali włamać się hakerzy.

Gemini Advisory podkreśla, że pomimo aktualizacji oprogramowania w usłudze Click2Gov wciąż pozostaje ona podatna na cyberataki. Odpowiedzialność za ochronę przed działaniami przestępców spoczywać ma zatem po stronie podmiotów korzystających z tego systemu obsługi płatności, które powinny regularnie monitorować własne systemy oraz stosować wszystkie łatki aktualizujące dla oprogramowania.

W 2018 roku firma FireEye oceniała, że nie wiadomo do końca, jak hakerzy zdołali dostać się na serwery Click2Gov. Przypuszczano jednak, że prawdopodobnie cyberprzestępcy skorzystali z podatności logicznych, które pozwoliły im uzyskać zdalny dostęp do sterowania serwerami bądź wpłynąć na ustawienia poziomów uprawnień dostępowych.