

Przestępcy wysłał do ciebie fałszywy SMS

29 czerwca 2025

Policja w Wielkiej Brytanii ostrzega przed zbierającą żniwa metodą cyberoszustwa. Przestępcy zaczęli wykorzystywać urządzenie znane jako „SMS blaster”, które pozwala im wysyłać tysiące fałszywych wiadomości tekstowych w krótkim czasie. Co istotne, aby wysłać fałszywy SMS, nie potrzebują do tego nawet spisu z numerami ofiar.



Blaster działa jak mobilna, fałszywa stacja bazowa, podszywająca się pod sieć 2G. Telefony w pobliżu automatycznie się z nią łączą, co pozwala przestępcom ominąć zabezpieczenia operatorów sieci komórkowych, takie jak filtry antyspamowe.

To przenośne urządzenie wielkości walizki może być zamontowane np. w bagażniku samochodu i działać w ruchu. Jego skuteczność jest największa w gęsto zaludnionych miastach.

W marcu w Londynie doszło do głośnego zatrzymania. Student z Chin został skazany na ponad rok więzienia za korzystanie z „SMS blastera”. Mężczyzna krążył samochodem po Londynie, wysyłając fałszywe SMS-y do dziesiątek tysięcy osób. Jedna z

wiadomości, odebrana przez funkcjonariusza w chwili zatrzymania sprawcy, podszywała się pod brytyjski urząd skarbowy i prosiła o dane potrzebne do „przetworzenia zwrotu podatku”.

Podszywa się pod operatora i rozsyła fałszywe SMS-y w zasięgu kilku kilometrów

„SMS blaster” działa na zasadzie imitowania stacji bazowej telefonii komórkowej. Podszywa się pod legalną sieć 2G i zmusza telefony w pobliżu do automatycznego połączenia. W ten sposób przestępcy mogą przejąć kontrolę nad komunikacją i wysłać dowolny SMS bez wykrycia przez operatora. Fałszywe wiadomości wyglądają bardzo wiarygodnie.

Treść wiadomości naciągacze oczywiście starannie planują. SMS zawiera pilne wezwanie do działania, link do fałszywej strony i prośbę o podanie danych. Oszuści mogą również kopiować grafiki i język używany przez instytucje państwowe, by wzmocnić wrażenie autentyczności. Ponieważ urządzenie działa lokalnie, w obrębie kilku kilometrów, pozwala dotrzeć do co najmniej setek telefonów jednocześnie, a jego mobilność sprawia, że trudno go namierzyć.

W razie wątpliwości najlepiej samodzielnie wejść na stronę internetową danej instytucji lub zadzwonić pod oficjalny numer kontaktowy. Warto też zgłaszać podejrzane wiadomości do swojego operatora oraz lokalnej policji.

Autorstwo: Miłosz Magrzyk

Zdjęcie: [Fangirl](#) (CC0)

Źródło: PolishExpress.co.uk