Microsoft zaatakował północnokoreańskich hakerów

4 stycznia 2020

Grupa Thallium od miesięcy była na celowniku specjalistów z microsoftowych Digital Crimes Unit i Threat Intelligencje Center. W końcu 18 grudnia koncern z Redmond złożył do sądu wniosek przeciwko grupie. Tydzień później sąd wydał zgodę na przejęcie przez firmę ponad 50 domen wykorzystywanych przez hakerów.

Thallium to cyberprzestępca grupa powiązana z rządem Korei Północnej, która wykorzystywała wspomniane domeny do przeprowadzania ataków. Wyspecjalizowała się w przeprowadzaniu precyzyjnych ataków phishingowych za pomocą e-maili. Przestępcy najpierw zbierali o ofierze jak najwięcej informacji, a następnie wysyłali do niej wiarygodnie wyglądający e-mail, którego zadaniem bylo skłonienie odbiorcy do wizyty na złośliwej witrynie.

Jak poinformowali przedstawiciele Microsoftu, grupa brała na cel „pracowników administracji rządowej, think-tanków, uczelni wyższych, członków organizacji działających na rzecz praw człowieka i pokoju oraz osoby pracujące nad problemami związanymi z rozprzestrzenianiem broni jądrowej”. Jej ofiarami padali mieszkańcy USA, Japonii i Korei Południowej.

Microsoft nie po raz pierwszy stosuje podobną taktykę do zwalczania grup cyberprzestępczych. Wcześniej przejmował domeny rosyjskich, chińskich i irańskich hakerów.

Oczywiście przejęcie domen nie rozbija grupy hakerskiej. Jednak na jakiś czas zmniejsza lub paraliżuje jej aktywność, a specjaliści ds. bezpieczeństwa, analizując dane znalezione w przejętych domenach, mogą lepiej poznać taktykę cyberprzestępców.

Autorstwo: Mariusz Błoński
Na podstawie: TechReport.com
Źródło: KopalniaWiedzy.pl