SAMSUNG I OXFORD WYKORZYSTANE W NOWEJ KAMPANII PHISINGOWEJ

Nowa kampania phishingowa wycelowana w użytkowników Microsoft Office 365 wykorzystuje znane marki, takie jak Samsung, Adobe czy Uniwersytet Oksfordzki - ostrzegają eksperci z izraelskiej firmy Check Point Research.

Cyberprzestępcy rozsyłają do użytkowników pakietu Office 365 e-maile z wiarygodnych domen, kierując ofiary na kontrolowane przez siebie fałszywe witryny podszywające się pod strony Microsoftu. Celem ataków jest pozyskanie danych do logowania w usługach cyfrowych tej firmy - uważają specjaliści.

Atakujący w swoich działaniach wykorzystywali serwery poczty wychodzącej (SMTP) np. Uniwersytetu w Oksfordzie, uwiarygadniając tym korespondencję, która przekierowywała ofiary do fałszywych stron wyłudzających dane. Zdaniem firmy Check Point Research ataki były bardzo dobrze przygotowane. Wykorzystanie znanych marek ze świata elektroniki i edukacji miało posłużyć uśpieniu czujności zarówno użytkowników usług internetowych, jak i programów antywirusowych, które nie reagowały na złośliwe e-maile wysyłane z użyciem przekierowania prowadzącego przez prawdziwe serwery SMTP.

Pierwsze ataki realizowane w ramach tej kampanii wykryto w kwietniu tego roku. 43 proc. z nich wymierzonych było w europejskie firmy, reszta zaś obierała za cele ofiary w Azji i na Bliskim Wschodzie.

Serwis Tech Republic zwraca uwagę, że Microsoft to popularna marka wykorzystywana w atakach hakerskich, ponieważ z jej produktów korzysta bardzo wiele osób - zarówno do celów osobistych, jak i służbowych. Dane do logowania w usługach tej firmy mogą stać się dla cyberprzestępców bramą prowadzącą do innych, powiązanych witryn i informacji na temat ofiar.