Cyberdefence 24

aut. Sylwia Gliwa 29.10.2020

SPOSÓB NA "UDZIAŁ W KONFERENCJI". CYBERKAMPANIA WYWIADOWCZA WYMIERZONA W POLITYKÓW

Dwie międzynarodowe konferencje stały się elementem przestępczej działalności hakerów. Cyberprzestępcy chcąc uderzyć w decydentów politycznych podszywali się m.in. pod Monachijską Konferencję Bezpieczeństwa - celem było gromadzenie informacji wywiadowczych – informuje Microsoft.

Wykryliśmy i podjęliśmy pracę na rzecz powstrzymania serii cyberataków ze strony grupy określonej jako „Phosphorous" podszywającej się pod organizatorów znanych konferencji. Wiadomości rozsyłane przez cyberprzestepców, zostały skierowanego do ponad 100 znanych osób – informuje Microsoft.

Działania zostały wymierzone w osoby, które potencjalnie byłyby zainteresowane największymi konferencjami - Monachijską Konferencją Bezpieczeństwa oraz konferencją The Think 20 (T20) Summit odbywającą się w Arabii Saudyjskiej.

Cyberprzestępcy drogą mailową wysyłali potencjalnym uczestnikom zaproszenia do udziału w tych wydarzeniach. Na co zwracają uwagę eksperci Microsoftu, w przygotowanych wiadomościach posługiwano się niemal perfekcyjnym językiem angielskim. Wiadomości zostały skierowane do byłych urzędników rządowych, ekspertów politycznych, naukowców i liderów organizacji pozarządowych. Cyberprzestępcy wykazywali się dużą empatią i z uwagi na pandemię koronawirusa oferowali możliwość uczestnictwa w wydarzeniu online. Po zdobyciu zaufania ofiary poprzez wymianę maili, celem działań phishingowych przestępców, było przejęcie danych logowania do skrzynek mailowych.

W opinii amerykańskiego giganta technologicznego, grupa Phosphorus, zaangażowała się w te ataki w celu gromadzenia informacji wywiadowczych. Jak informuje Microsoft, zakończyły się one sukcesem i skutecznie zagroziły bezpieczeństwu danych kilku z zaatakowanych osób - w tym byłym ambasadorom oraz ekspertom którzy pomagają kształtować globalne agendy i politykę zagraniczną w swoich krajach.

Jak wskazuje Microsoft, o całej sytuacji zostali poinformowani organizatorzy konferencji, którzy jak sygnalizuje firma, podjęli działania informacyjne. Jednocześnie co podkreślono w oświadczeniu nie dostrzeżono, aby w działania te miały jakiekolwiek powiązanie z wyborami prezydenckimi w Stanach Zjednoczonych.

Grupa Phosphorous została zidentyfikowana jako zespół hakerów z Iranu. Wcześniej grupie zostały przypisane ataki na amerykańskich weteranów. Jak informowaliśmy w zeszłym roku, hakerzy wykorzystywali fałszywą stronę o nazwie „Hire Military Heroes" zawierająca oferty pracy skierowane do weteranów chcących powrócić do aktywnego życia cywilnego. Witryna zachęcała do pobrania aplikacji infekującej używany sprzęt. Jak ustalili urzędnicy z Departamentu Obrony, działania

ukierunkowane były na osoby, które już niebawem miały opuścić struktury wojskowe i były zainteresowane poszukaniem pracy w sektorze cywilnym. W ich opinii, działania miały na celu pozyskanie dostępu do systemów informatycznych Pentagonu.

Czytaj też: Północnokoreańscy hakerzy z globalną misją wywiadowczą. Grupa Kimsuky rozpracowana