aut. Szymon Palczewski 21.05.2020

CYBERSZPIEGOSTWO PRIORYTETEM TEHERANU

Irańscy cyberszpiedzy zostali zdemaskowani podczas kampanii wymierzonej w firmy telekomunikacyjne znajdujące się w Azji Południowej. Zadaniem hakerów było uzyskanie dostępu do systemów z danymi, a następnie ich potajemna infiltracja. Cyberszpiegostwo to wysoki priorytet Teheranu – wskazują eksperci.

Specjaliści Symantec wskazują, że grupa cyberszpiegowska Greenbug prowadziła kampanię wymierzoną w firmy telekomunikacyjne z regionu Azji Południowej. „Istnieją przesłanki, że jedno z przedsiębiorstw było już celem cyberataków w kwietniu ubiegłego roku" – czytamy w raporcie.

Eksperci podkreślają, że podstawą złośliwych działań były fałszywe e-maile, które „wydają się być początkowym wektorem infekcji". Głównym celem hakerów stanowiło uzyskanie dostępu do systemów baz danych.

Greenbug jest grupą działającą na zlecenie Iranu. Analiza kampanii wykazała, że techniki i narzędzia działania są charakterystyczne dla cyberprzestępców tego ugrupowania. Wśród nich można wskazać na korzystanie z publicznie dostępnego oprogramowania hakerskiego, takiego jak Mimikatz i Plink, a także koncentracja na kradzieży danych przy minimalizacji ryzyka wykrycia.

W ramach kampanii Greenbug ukierunkowała swoje działania na cele znajdujące się między innymi w Pakistanie. Cyberprzestępcy byli bardzo zdeterminowani, aby uzyskać dostęp do sieci wielu firm. „Zamykając jedne drzwi, próbowali wejść przez kolejne" – posłużył się porównaniem Jon DiMaggio, specjalista Symantec.

Kampania wskazuje, przed jakimi wyzwaniami stoją obecnie dostawcy usług telekomunikacyjnych. Utrzymanie bezpieczeństwa sieci i zasobów stanowi kluczowy element działalności przedsiębiorstwa w tej branży. Według Symantec 18 różnych grup hakerskich powiązanych z państwami prowadziło zaawansowane kampanie wymierzone w sektor telekomunikacyjny. W jednym przypadku chińscy cyberszpiedzy naruszyli systemy około 10 operatorów komórkowych w Afryce, Europie, na Bliskim Wschodzie i Azji.

„Nie wszyscy operatorzy na całym świecie mają takie same zasoby. Niektórzy są odpowiednio przeszkoleni i mają środki, aby odpierać ataki, podczas gdy inni są łatwiejszymi celami" – podkreślił specjalista CrowdStrike Adam Meyers, cytowany przez CyberScoop. Dodał, że jeśli hakerzy uzyskają dostęp do sieci telekomunikacyjnej mogą infiltrować wiele różnych celów.

Irańscy hakerzy nie raz prowadzili operacje cyberszpiegowskie wymierzone w ten sektor. „Prawdopodobnie jest to wysoki priorytet dla Teheranu (...) biorąc pod uwagę wartość tych danych i cele bezpieczeństwa narodowego" – wyjaśnił na łamach CyberScoop ekspert w BAE Systems Saher Naumaan.

Czytaj też: Zidentyfikowano grupę irańskich hakerów. Posiadali "cyberbroń" od NSA