Cyberdefence 24

aut. Szymon Palczewski 05.06.2020

SZTABY GŁÓWNYCH KANDYDATÓW NA PREZYDENTA W USA NĘKANE CYBERATAKAMI

Irańscy i chińscy hakerzy uderzyli w sztab obecnego prezydenta USA Donalda Trumpa oraz zespół jego kontrkandydata Joe Biden'a. Złośliwe kampanie były prowadzone przez znane w środowisku ugrupowania cyberprzestępcze. O cyberatakach poinformowane zostały organy ścigania. Scenariusz z 2016 roku staje się coraz bardziej realny?

Według Shane'a Huntley'a, specjalisty Google Threat Analysis Group, chińscy hakerzy powiązani z rządem prowadzą złośliwe działania wymierzone w przedstawicieli sztabu Joe Biden, a z kolei cyberprzestępcy na usługach Teheranu skupili się na kampanii Donalda Trumpa.

Główną metodą działania hakerów jest phishing. Obecnie nie wykryto śladów poważniejszych skutków złośliwych operacji. „Wysłaliśmy użytkownikom nasze ostrzeżenie przed atakiem na sektor rządowy i zgłosiliśmy sprawę organom ścigania" – czytamy na Twitterze eksperta Google.

Sytuacja pokazuje, że zagraniczni aktorzy są silnie zainteresowani zbliżającymi się wyborami prezydenckimi w Stanach Zjednoczonych. Zapewnienie ich bezpieczeństwa będzie kolejnym wyzwaniem dla Waszyngtonu w tym roku – po zawirowaniach gospodarczych, pandemii koronawirusa oraz masowych protestach wewnętrznych.

„Od początku naszej kampanii wiedzieliśmy, że będziemy podlegać takim atakom i jesteśmy na nie przygotowani" – stwierdził w oświadczeniu sztab Joe Bidena, którego słowa na Twitterze przytacza reporter Politico Martin Matishak. „Joe Biden poważnie traktuje cyberbezpieczeństwo, pozostaniemy czujni wobec tych zagrożeń i zapewnimy bezpieczeństwo zasobów kampanii" - czytamy w oświadczeniu.

Podobna retorykę wystosował obóz obecnego prezydenta Donalda Trumpa. „Zostaliśmy poinformowani, że zagraniczni aktorzy bezskutecznie próbowali naruszyć urządzenia naszych pracowników" – podkreślił sztab głowy państwa dla CyberScoop. – „Zachowujemy czujność w zakresie cyberbezpieczeństwa".

Kampania Joe Bidena jest atakowana przez znaną grupę hakerską APT31 lub inaczej Zirconium, która specjalizuje się w operacjach cyberszpiegowskich, przede wszystkim w branży telekomunikacyjnej. Jej cyberprzestępcy w przeszłości prowadzili również działania wymierzone w organizacje pozarządowe.

Z kolei sztab Donlada Trumpa jest nękany przez irańskich hakerów, którzy w środowisku są rozpoznawalni jako APT35 lub Charming Kitten. Grupa jest powszechnie znana z cyberataków wymierzonych w sektor energetyczny, rządowy i technologiczny.

„Na podstawie doświadczeń z przeszłości należy pamiętać, że możemy mieć do czynienia ze scenariuszem jak w 2016 roku, w którym dochodzi do incydentów" – zaznaczył w rozmowie z

CyberScoop specjalista FireEye John Hultquist. – „Większość z tych podmiotów jest przede wszystkim odpowiedzialna za gromadzenie informacji na temat polityki zagranicznej przecinków swoich krajów. Nie ma lepszego miejsca na tego typu działania niż kampania wyborcza”.