aut. Szymon Palczewski 13.02.2020

IRAŃSCY HAKERZY UDERZYLI W AMERYKAŃSKIE FIRMY? FBI OSTRZEGA

Specjaliści FBI alarmują o nowej złośliwej kampanii wymierzonej w amerykańskie firmy sektora prywatnego. Złośliwe oprogramowanie wykorzystywane przez hakerów jest podobne do wirusa, którym posługują się irańscy hakerzy.

Według informacji zdobytych przez serwis ZDNet, FBI wydało ostrzeżenie dotyczące trwającej kampanii hakerskiej wymierzonej w dostawców oprogramowania wykorzystywanego w łańcuchu dostaw. Bezpieczeństwo amerykańskiego sektora prywatnego jest zagrożone – ostrzegają specjaliści.

FBI wskazuje, że hakerzy próbują zainfekować prywatne firmy złośliwym oprogramowaniem Kwampirs, czyli trojanem zdalnego dostępu (RAT). „Firmy zajmujące się łańcuchem dostaw są celem cyberprzestępców. Koncentrują się na uzyskaniu dostępu do strategicznych partnerów ofiary i/lub klientów, w tym podmiotów wspierających systemy kontroli przemysłowej (ICS) w zakresie globalnego wytwarzania, przesyłu i dystrybucji energii" – tłumaczą eksperci FBI na łamach ZDNet.

Jak donosi serwis, to samo złośliwe oprogramowanie zostało również zastosowane w atakach na podmioty z sektora finansowego oraz służby zdrowia. Służby nie podają informacji na temat potencjalnego źródła incydentu.

Wirus Kwampirs po raz pierwszy został zidentyfikowany w kwietniu 2018 roku przez specjalistów Symantec. Wówczas eksperci firmy odkryli, że grupa o kryptonimie Orangeworm wykorzystała szkodliwe oprogramowanie w podobny sposób atakując podmioty, wchodzące w skład łańcucha dostaw w branży medycznej – informuje ZDNet.

Ostrzeżenie o nowej kampanii wydane przez FBI wskazuje, że cyberataki prowadzone przez hakerów znacznie ewoluowały. Co więcej, analiza operacji z wykorzystaniem trojana Kwampirs uwidacznia liczne podobieństwa z Shamoon, czyli złośliwym oprogramowaniem, którym posługiwali się irańscy cyberprzestępcy. „Analiza wykazała, że Kwampirs ma liczne podobieństwa z destrukcyjnym szkodliwym oprogramowaniem Shamoon" – wyjaśnia FBI na łamach ZDNet.

Firmy wchodzące w skład łańcucha dostaw są atrakcyjnym celem hakerów. Skuteczny cyberatak na jeden podmiot daje możliwość wtargnięcia do sieci i systemów innego. W ten sposób działalność cyberprzestępców może sparaliżować większą grupę przedsiębiorstw lub instytucji, dlatego też jakość zabezpieczeń całego procesu jest kluczowa. FBI zaleca, aby amerykańskie firmy zachowały czujność, a wszelkie incydenty natychmiast zgłaszały odpowiednim służbom.

Czytaj też: Zakłócenie irańskiej sieci. Cyberatak czy celowe działanie władz?