aut. Szymon Palczewski 14.12.2020

POPULARNY PRODUKT IT POSŁUŻYŁ W ATAKU NA RZĄD USA. POLSKA STOI W OBLICZU ZAGROŻENIA?

Oprogramowanie dostarczone przez firmę SolarWinds, które posłużyło hakerom do cyberataku na Departament Skarbu oraz Departament Handlu USA jest wykorzystywane przez polski rząd. Problem dotyczy jednak nie tylko naszego kraju, ale także pozostałych, ponieważ produkt amerykańskiego koncernu zyskał popularność w skali świata. Czy rosyjski wywiad infiltruje polskie sieci pozostając w ukryciu?

Specjaliści Microsoft Security Response Center zaangażowali się w działania mające na celu zbadanie cyberataku na Departament Skarbu oraz Departament Handlu USA. Przeprowadzone do tej pory analizy pozwoliły im stwierdzić, że włamanie do rządowych sieci odbyło się za pomocą oprogramowania do zarządzania IT „Orion", którego producentem jest SolarWinds. W ten sposób hakerzy stworzyli sobie doskonały „przyczółek" do dalszych działań.

Jak tłumaczą specjaliści, cyberszpiedzy, będąc już w sieci, wykorzystali uprawnienia administracyjne uzyskane w wyniku włamania do lokalnych systemów, aby następnie pozyskać dostęp do kont administratora poszkodowanych organizacji. W ten sposób hakerzy podszyli się pod „uprzywilejowane profile", tym samym swobodnie operując w sieci departamentów.

Specjaliści Microsftu wskazali, że grupa cyberprzestępców wykorzystała backdoora w oprogramowaniu „Orion". Jest on rozpowszechniany za pośrednictwem platform lub systemów automatycznej aktualizacji w docelowych sieciach, które trafiły na rynek w marcu 2020 roku. Eksperci nie są jednak w stanie wyjaśnić, w jaki sposób hakerom udało się uzyskać dostęp do pakietów aktualizacyjnych.

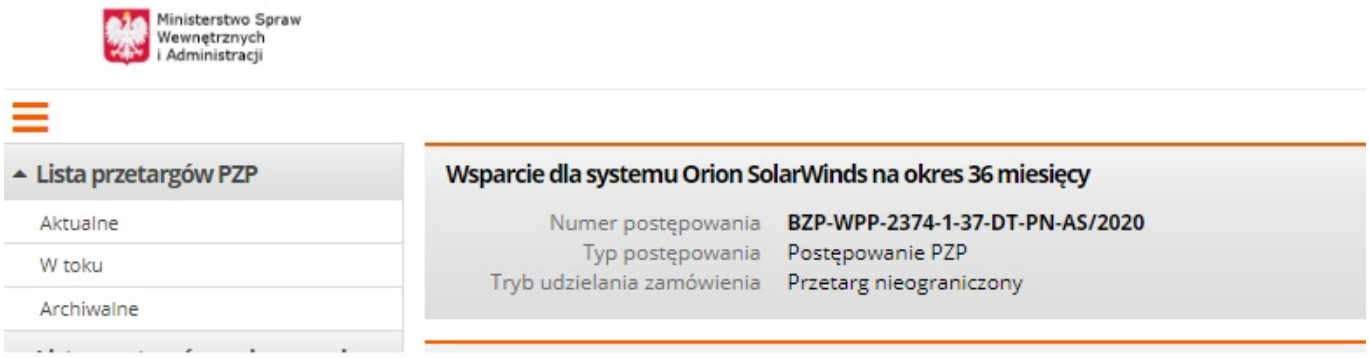
Polska w sidłach Rosjan?

SolarWinds, to firma informatyczna, która obsługuje klientów rządowych, wojsko i służby wywiadowcze, w tym m.in.: wszystkie największe w USA firmy telekomunikacyjne (jest ich dziesięć), Pentagon, NASA, Departament Stanu, Departament Sprawiedliwości oraz Biuro Prezydenta Stanów Zjednoczonych. Koncern świadczy nie tylko usługi dla amerykańskich podmiotów, ale również zagranicznych.

Z rozwiązań SolarWinds korzysta m.in. Wielka Brytania (np. Narodowa Służba Zdrowia), Turcja (np. Ministerstwo Zdrowia Turcji), Parlament Europejski czy nawet NATO (np. Agencja Wsparcia NATO). To sprawia, że cyberatak zyskuje rangę incydentu międzynarodowego, ponieważ produkty amerykańskiej firmy są wykorzystywane globalnie przez podmioty rządowe oraz prywatne powiązane z kluczowymi sektorami dla państwa.

Nie inaczej jest w przypadku Polski. Wynika to z faktu, że oprogramowanie dostarczane przez

SolarWinds jest stosowane w systemach rządowych w naszym kraju. Przykładem może być MSWiA i niedawny przetarg na usługę „Wsparcie dla systemu Orion SolarWinds na okres 36 miesięcy z 25 listopada br., której wartość zamówienia wyniosła 270 000 zł bez VAT (unieważniono postępowanie na podstawie art. 93 ust. 1 pkt 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych).



Fot. Przetarg na usługę „Wsparcie dla systemu Orion SolarWinds na okres 36 miesięcy z 25 listopada br. / zamowienia-mswia.ezamawiajacy.pl

Cyberatak na Departament Skarbu oraz Departament Handlu USA przy użyciu powszechnie wykorzystywanego przez rządu oprogramowania IT „Orion" pokazuje, że rosyjski wywiad może posiadać dostęp do kluczowych zasobów również innych państw, w tym Polski. Obecnie ujawniono jedynie incydent w amerykańskich sieciach, lecz rzeczywista skala kampanii pozostaje tajemnicą.

Czytaj też: Największa operacja w roku? Rosyjski szturm na sieci Departamentu Skarbu oraz Handlu USA