aut. Szymon Palczewski 29.10.2020

REKORDOWA LICZBA OPERACJI HAKERSKICH WYMIERZONYCH W INTERESY SZWAJCARII. ROSJA, CHINY I IRAN GŁÓWNYMI SPRAWCAMI

Cyberszpiegostwo będzie jednym z głównych wyzwań współczesnego świata – wskazuje szwajcarski wywiad. Jego zdaniem sytuacja geopolityczna przenosi się do cyberprzestrzeni i jest kreowana głównie przez rozwiązania siłowe, co widać na przykładzie działań kluczowych aktorów – USA, Chin, Rosji czy Iranu. Bardzo poważnym zagrożeniem jest również ransomware oraz cyberataki na wrażliwe dla państwa sektory, w tym służbę zdrowia.

Nie ulega wątpliwości, że szpiegostwo oraz międzynarodowa rywalizacja o władzę i strefy wpływów mają miejsce w cyberprzestrzeni. Infrastruktura krytyczna Szwajcarii nigdy jeszcze nie była bezpośrednią ofiarą cyberataków sponsorowanych przez państwo, lecz nie należy tego wykluczyć – wynika z raportu „Switzerland's Security 2020", opracowanego przez szwajcarską Federalną Służbę Wywiadowczą (ang. *Federal Intelligence Service*, FSI). Ponadto operacje hakerskie są często wymierzone w „szwajcarskich partnerów biznesowych i dostawców", w związku z czym naruszenie ich sieci oraz systemów może również uderzyć w interesy krajowych podmiotów.

„Ogólnie rzecz biorąc, motywy, cele i metody szpiegostwa pozostały niezmienne na przestrzeni lat" – wskazuje FIS. Współcześnie dochodzi jednak do bardziej agresywnych działań przy wykorzystaniu możliwości, jakie daje cyberprzestrzeń. Przykładem może być chociażby dezinformacja czy ukierunkowane cyberataki.

Co podkreślono w raporcie, w 2019 roku szwajcarski wywiad odkrył rekordową liczbę operacji hakerskich sponsorowanych przez państwo, które były wymierzone w „szwajcarskie interesy". Większość z nich pochodziła z Rosji, Korei Północnej, Chin i Iranu.

FIS uważa, że szpiegostwo pozostanie jednym z głównych wyzwań współczesnego świata. „Podobnie jak proliferacja, szpiegostwo jest zjawiskiem długotrwałym" – tłumaczy szwajcarski wywiad. Dlaczego? Wynika to z kliku powodów. Po pierwsze, obecna sytuacja geopolityczna jest kreowana przez rozwiązania siłowe, co widać na przykładzie działań między innymi Stanów Zjednoczonych, Rosji, Chin, Turcji, Iranu czy Izraela. Po drugie, ofensywne cybernarzędzia są stale udoskonalane, a cyfryzacja stwarza nowe możliwości pozyskiwania poufnych informacji lub niszczenia systemów informatycznych. Wreszcie „wyścig technologiczny" w zglobalizowanej gospodarce staje się coraz bardziej intensywny i agresywny, przez co postęp w dziedzinie innowacji jest warunkiem do dominacji na arenie międzynarodowej.

Czytaj też: „Dekada cyberszpiegostwa" w Europie Wschodniej. Rządowe tajemnice wykradano przez lata

Cyberataki. Ransomware liderem

FIS w ciągu ostatnich miesięcy zaobserwował znaczy wzrost liczby cyberataków, których celem były „szwajcarskie interesy w kraju oraz za granicą". Część z nich stanowiły kampanie wymierzone w lokalne instytucje finansowe. W tym przypadku główną motywacją wrogich podmiotów była chęć szybkiego zysku.

Ofiarą hakerów często padają również krajowe firmy, których sieci i systemy są penetrowane na rzecz realizacji operacji cyberszpiegowskich. Tego typu działania prowadzą głównie aktorzy państwowi lub grupy wspierane przez rząd danego kraju. „Cyberprzestępcy zazwyczaj wykradają tajemnice produkcyjne, patenty oraz informacje o planowanych fuzjach, przejęciach, penetracji rynku lub inwestycjach" – czytamy w raporcie FIS. W związku z tym środowisko wywiadowcze podkreśla, że szpiegostwo może mieć negatywny wpływ na Szwajcarię jako centrum finansowe świata i miejsce prowadzenia innowacyjnych badań.

W przypadku infrastruktury krytycznej największe obawy budzą możliwe konsekwencje „cybersabotażu", ponieważ takie ataki mogą spowodować ogromne szkody fizyczne i mieć poważne konsekwencje dla społeczeństwa. FIS do tej pory nie wykrył żadnego tego typu incydentu, lecz nie można ich wykluczać z katalogu realnych zagrożeń. Wynika to z faktu, że miały one miejsce w innych krajach i większość z nich została przeprowadzona przez agencje rządowe. Szwajcarski wywiad wyróżnił między innymi na operacje prowadzone na Bliskim Wschodzie oraz w Europie Wschodniej, nie wskazując jednak na konkretne działania.

FIS jednoznacznie stwierdził, że obecnie największym zagrożeniem dla infrastruktury krytycznej w Szwajcarii jest ransomware. Incydent z udziałem oprogramowania szyfrującego może mieć „poważne konsekwencje", zwłaszcza dla krajowych firm. Zgodnie z raportem kampanie tego typu były wykorzystywane głównie do celów finansowych.

Ransomware jest jednym z głównych cyberzagrożeń w skali globalnej. Szwajcarski wywiad wskazuje, że zaobserwowano globalny wzrost liczby tego typu operacji, a kwoty okupu żądane przez hakerów są coraz wyższe. W wymiarze międzynarodowym atrakcyjnym celem są nie tylko firmy, ale także podmioty z sektora administracji oraz opieki zdrowotnej. Skalę zjawiska potęguje fakt, że bardzo często trudno jest odzyskać lub odtworzyć naruszone podczas cybeataku dane, co prowadzi do ich trwałego utracenia.

Zdaniem szwajcarskiego wywiadu płacenie okupu w przypadku ataku ransomware jest błędem, ponieważ potęguje to jedynie skalę zjawiska. Hakerzy widząc, że ofiary decydują się na przekazanie środków finansowych, prowadzą więcej operacji ze względu na odnoszone korzyści materialne. „Płacenie okupu wspiera zatem ich dalsze cyberataki" – czytamy w raporcie FIS.

Poza oprogramowaniem szyfrującym szwajcarski wywiad podkreśla ryzyko płynące również z innych rodzajów złośliwego oprogramowania. FIS wskazuje na masowe cyberataki na sektor przemysłu, administracji, ochrony zdrowia oraz pozostałe branże, które regularnie muszą odpierać kampanie phishingowe. W raporcie wyróżniono przykład fałszywej wiadomości rozsyłanej do obywateli, rzekomo pochodzącej od Federalnego Urzędu Zdrowia Publicznego. W rzeczywistości w korespondencji zamieszczony był zainfekowany plik. Incydent miał miejsce w momencie wybuchu pandemii.

Szwajcarski wywiad podkreślił w raporcie, że od 2018 roku rośnie tendencja do przeprowadzania cyberataków etapami. Zazwyczaj zaczynają się one od „początkowej infekcji", a gdy ofiara okaże się dla hakerów „wystarczająco atrakcyjna", operacja kończy się zainstalowaniem złośliwego oprogramowania na danym urządzeniu. Kampanie są więc ukierunkowane tylko do pewnego stopnia.

„W szczególności infekcja wirusem Ryuk przeprowadzana jest na podstawie dwu- lub trzystopniowego ataku, który rozpoczyna się od infekcji złośliwym oprogramowaniem Emotet" – czytamy w raporcie. Bardzo często jeden z największych botnetów na świecie Trickbot służy jako pośrednik do rozprzestrzeniania w sieci wrogiego ładunku.

Czytaj też: Pierwsza ofiara śmiertelna ataku ransomware. Zarzut nieumyślnego spowodowania śmierci

Inne zagrożenia

Zagrożenie dla infrastruktury krytycznej nie ogranicza się do cyberprzestrzeni. Szwajcarski wywiad wskazał między innymi na ataki na maszty 5G, które miały miejsce w tym kraju oraz innych europejskich miastach. Rzekome rozprzestrzenianie się koronawirusa za pomocą promieniowanie 5G często stanowi podstawę do aktów wandalizmu wymierzonych w infrastrukturę telekomunikacyjną.

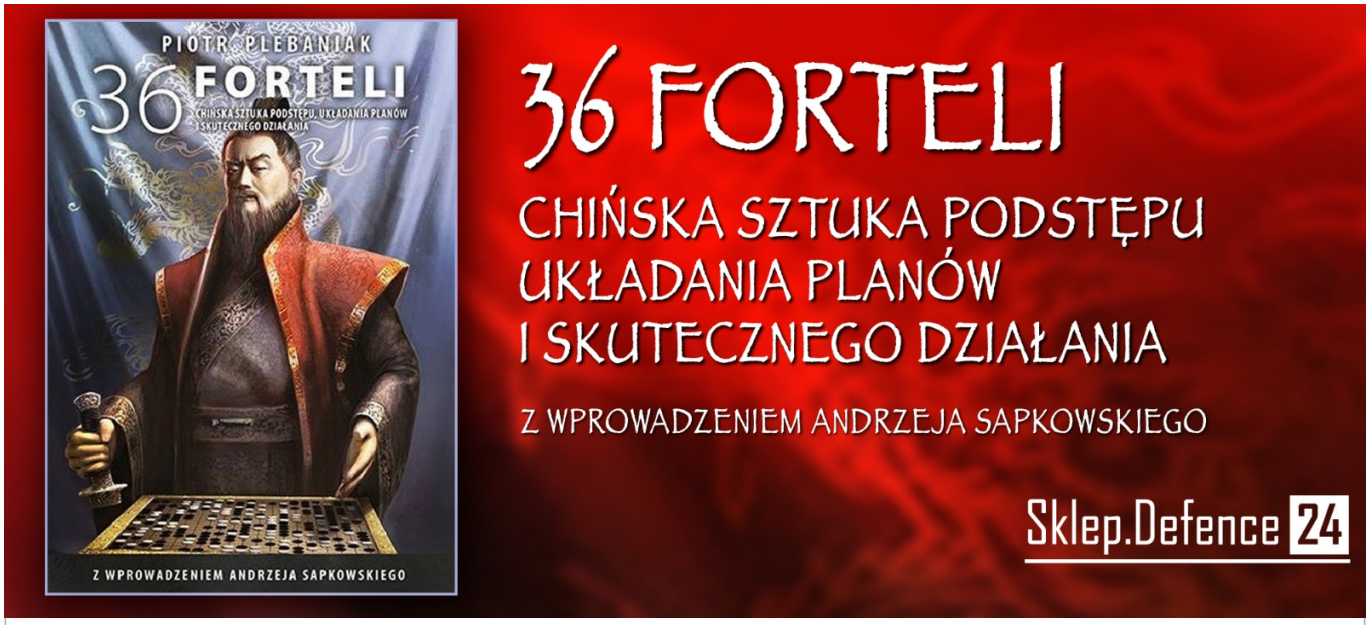
Szwajcarska infrastruktura krytyczna jest relatywnie bezpieczna i nie zagraża jej obecne większe ryzyko – uważa tamtejszy wywiad. Wynika to z faktu, że zaawansowane operacje hakerskie są narzędziem w rękach wrogo nastawionych wobec siebie państw, a Szwajcaria jest państwem neutralnym. Zdaniem FIS cyberataki to forma wzajemnego odstraszania, szczególnie w sytuacjach konfliktowych.

Hakerzy bardzo często wykorzystują globalne wydarzenia, aby podnieść skuteczność swoich operacji. Jednym z nich jest obecna pandemia COVID-19, która stała się „wabikiem" podczas wielu operacji, w tym ransomware. „Należy spodziewać się dalszego wzrostu liczby tego typu cyberataków na podmioty prywatne" – czytamy w raporcie.

W perspektywie krótko- i średnioterminowej spodziewane są dalsze bezpośrednie kampanie ugrupowań oraz pojedynczych cyberprzestępców na szwajcarskie podmioty z szeroko rozumianego biznesu, gospodarki, a także polityki. Nie można również definitywnie wykluczać zaangażowania ze strony aktorów państwowych, których celem będą podmioty wojskowe, administracja oraz organizacje międzynarodowe mające siedzibę w Szwajcarii. Ryzyko cyberszpiegostwa dotyczy również branży technologicznej, edukacji, sportu i sektora finansowego.

Bezpieczniej już było, czyli raport szwajcarskiego wywiadu

Czytaj też: Covid-19 wzmacnia cyberprzestępczość. Globalna „pandemia cyberatków"



[Fot. Do kupienia w Sklepie Defence24.pl]