Cyberdefence 24

aut. Szymon Palczewski 05.03.2021

ROSJA WYKORZYSTAŁA INFRASTRUKTURĘ LITWY DO CYBERSZPIEGOSTWA

Służby rosyjskiego wywiadu wykorzystywały infrastrukturę IT na Litwie do cyberataków na cele w innych krajach, w tym podmioty pracujące nad szczepionką przeciwko COVID-19. Wrogie działania były skierowane również wobec wysokich rangą litewskich urzędników, a także instytucji państwowych zajmujących się bezpieczeństwem, polityką zagraniczną, energetyką oraz edukacją. Poza cyberszpiegostwem Moskwa miała prowadzić także szereg innych kampanii, takich jak operacje wpływu. Jednym z głównych źródeł zagrożenia jest grupa hakerska Cozy Bear (APT29) powiązana z rosyjskim wywiadem.

Przeniesienie codziennych działań do sieci w czasie pandemii COVID-19, w tym przejście na tryb pracy zdalnej, przyczyniło się do wzrostu ryzyka związanego z wrogimi operacjami prowadzonymi w cyberprzestrzeni. Dotyczy to m.in. działań realizowanych przez zewnętrzne służby wywiadowcze, które poszukują nowych sposobów na zwiększenie skuteczności realizowanych zadań. Zagrożenie dotyczy nie tylko Litwy, ale także innych państw w skali globalnej – wskazuje Departament Bezpieczeństwa Państwowego Litwy w „National Threat Assessment 2021".

W dokumencie litewski wywiad skupił się przede wszystkim na operacjach prowadzonych przez Rosję jako naczelnego przeciwnika dla państwa oraz NATO. Służby jednoznacznie oceniły, że „grupy szpiegowskie koordynowane przez rosyjski wywiad stanowią poważne zagrożenie dla litewskich instytucji". Jednak ze względu na pandemię ich sposób działania został zdecydowanie ukierunkowany na prowadzenie operacji w cyberprzestrzeni – to ona stała się głównym wymiarem gromadzenia informacji zarówno przez wschodniego sąsiada, jak i inne wrogie państwa.

> *Ograniczenia dotyczące podróży i spotkań utrudniają operacje zbierania informacji przez służby przy użyciu tradycyjnych metod. Niemniej jednak wysiłki mające na celu walkę z pandemią nie zapobiegają operacjom szpiegowskim.*
>
> Departament Bezpieczeństwa Państwowego Litwy

Służby wywiadu Litwy wyraźnie podkreśliły, że w 2020 roku grupy hakerskie powiązane z rosyjskim wywiadem odpowiadają za cyberataki wymierzone w wysokich rangą decydentów, a także instytucje publiczne zajmujące się sprawami bezpieczeństwa narodowego, polityki zagranicznej, energią oraz edukacją. Co więcej, w raporcie stwierdzono, że Moskwa wykorzystywała infrastrukturę IT na Litwie do prowadzenia wrogich kampanii, których celem były inne kraje. Jako przykład podano operacje

realizowane przez grupę Cozy Bear (powiązana z wywiadem Rosji) wymierzone w podmioty pracujące nad szczepionką przeciwko COVID-19.

Pandemia koronowirusa ułatwiła zagranicznym służbom prowadzenie działań cyberszpiegowskich, co wynika z braku odpowiedniej dbałości o cyberbezpieczeństwo przez użytkowników czy np. pracodawców, którzy pod presją czasu starali się dostosować swoje firmy do trybu pracy zdalnej. Tworzono m.in. kanały komunikacyjne, organizowano spotkania online oraz wdrażano nowe rozwiązania i narzędzia, zapominając często o zapewnieniu odpowiedniej jakości zabezpieczeń. Podatności wynikały nie tylko z presji czasu, ale także braku doświadczenia czy używaniu programów, które wcześniej nie były popularne, a przez to nie stanowiły głównego obiektu zainteresowania hakerów.

Dezinformacja siłą Kremla?

Darius Jauniskis, szef Departamentu Bezpieczeństwa Państwowego Litwy, podkreślił podczas przedstawienia raportu w parlamencie, że Rosja posługuje się militarnymi i gospodarczymi środkami, a także operacjami wpływu „dla realizacji swoich celów politycznych" w tym kraju.

> *Rosyjskie operacje wywiadowcze stanowią poważne zagrożenie dla bezpieczeństwa narodowego Litwy.*
>
> Darius Jauniskis, szef Departamentu Bezpieczeństwa Państwowego Litwy

Szef Departamentu oskarżył Moskwę o próby wykorzystania pandemii jako sposobu na wywołanie chaosu na Litwie. Jak zaznaczył, w ostatnim czasie miały miejsce dziesiątki tego typu operacji, które ostatecznie okazały się nieskuteczne. „Działania te były dobrze skoordynowane i napędzane antyzachodnią propagandą wychodzącą z Kremla" – zwrócił uwagę Darius Jauniskis.

W raporcie litewskie służby jednoznacznie wskazały, że w ubiegłym roku obywatele tego kraju stanęli w obliczu „ogromnego strumienia wrogich narracji", których źródło miało miejsce w Rosji. Było to szerokie spektrum fake newsów – od drobnych fikcyjnych wiadomości po zorganizowane kampanie odnoszące się do II wojny światowej. W tym obszarze głównym celem wrogich podmiotów było „zdyskredytowanie Litwy i sojuszników oraz zwiększenie nieufności społecznej do rządu i sił zbrojnych". W dokumencie wskazano, że część operacji dezinformacyjnych była prowadzona równocześnie na Litwie i… w Polsce.

Przesłanie raportu w kontekście operacji wpływu jest jednoznaczne: w 2021 roku pojawią się nowe kampanie, których tematyka będzie dotyczyła regionalnych ćwiczeń wojskowych prowadzonych przez NATO i/lub Rosję. Co więcej, jest wysoce prawdopodobne, że liczba operacji wykorzystujących fake newsy w regionie Morza Bałtyckiego pozostanie wysoka w „dającej się przewidzieć przyszłości".

Chiny. Chronić infrastrukturę krytyczną!

W raporcie odniesiono się również do zagrożenia płynącego ze strony Chin. Podkreślono w nim, że w 2020 roku jedna z litewskich firm zajmujących się infrastrukturą krytyczną ogłosiła przetarg na rozwój inteligentnych rozwiązań IT. Cieszył się on dużym zainteresowaniem ze strony przedsiębiorstw, pochodzących z Państwa Środka. „Jeden z nich zaproponował nawet bezpłatną instalację sprzętu w zamian za usprawnienie zarządzania systemem" – czytamy w dokumencie.

Jak wskazują litewskie służby, wśród potencjalnych dostawców biorących udział w przetargu było 5 chińskich firm, przy czym dwie z nich były spółkami powiązanymi z rządem w Pekinie. Zdaniem wywiadu planowały one nie tylko rozwijać „więzi biznesowe", lecz także „zdobywać wiedze o infrastrukturze IT w krytycznych dziedzinach dla bezpieczeństwa narodowego".

> *Próby uzyskania dostępu do infrastruktury krytycznej odzwierciedlają ogólny cel Chin, jakim jest utrzymanie długoterminowego wpływu na strategiczne sektory w skali globalnej i umocnienie pozycji krajowych przedsiębiorstw na światowym rynku.*
>
> Departament Bezpieczeństwa Państwowego Litwy

Państwo Środka dąży do zwiększenia zależności od jego technologii w skali globalnej – wynika z raportu litewskiego wywiadu. Co więcej, Pekin jest zainteresowany prowadzeniem „inwazyjnych cyberoperacji, w tym kradzieży danych wywiadowczych i know-how".

Wróg czyha w sieci

Litewskie służby w opracowaniu zwróciły uwagę także na szersze spektrum zagrożeń występujących w cyberprzestrzeni, wskazując na ransomware. W dokumencie podkreślono, że hakerzy chętniej używają oprogramowania szyfrującego, ponieważ pozwala im to na czerpanie zysków finansowych pochodzących z okupów. Co jest szczególnie niepokojące, jednym z podstawowych celów tego typu kampanii są placówki opieki zdrowotnej. Logika działania hakerów jest prosta: instytucje te muszą działać w oparciu o w pełni sprawną infrastrukturę, dlatego z pewnością zdecydują się zapłacić żądaną kwotę w zamian z odblokowanie systemów lub danych.

W raporcie podkreślono również, że atrakcyjnym celem w obecnych czasach są także podmioty odpowiedzialne za prace nad szczepionką przeciwko COVID-19. W tego typu przypadków główną motywacją jest kradzież danych i informacji na temat metod walki z pandemią, zarządzaniem sytuacją kryzysową czy szczegółów dotyczących obecnego stanu badań nad lekarstwem na koronawirusa.

Katalog zagrożeń na tym się jednak nie kończy. Litewski wywiad wskazuje, że okres pandemii to również czas wzrostu operacji phishingowych prowadzonych przez „wrogie służby wywiadowcze". Często w złośliwych wiadomościach e-mail wykorzystywano tematykę koronawirusa, aby zachęcić ofiary do otwarcia zainfekowanego pliku lub odnośnika. Wynika to z faktu, że COVID-19 przykuwa uwagę i budzi zainteresowanie, a także lęk, niepokój oraz inne silne emocje, które zmniejszą czujność użytkowników.

Oczywiście w raporcie nie pominięto także kwestii dezinformacyjnych. Zgodnie z opracowaniem służb, na Litwie prowadzone są operacje wpływu wykorzystujące fake newsy na temat pandemii COVID-19. Jak podkreślono, mają one charakter cykliczny. Oczywiście należy mieć na uwadze, że tego typu zagrożenie występuje również w innych państwach, w tym Polsce, a walka z nim jest bardzo trudna i aby była skuteczna, wymaga zaangażowania najlepiej wszystkich użytkowników sieci.

Litewski wywiad ostrzega, że aktywność hakerów w najbliższym czasie nie zmaleje. Jednak należy oczekiwać, że z czasem administratorzy sieci, w tym m.in. pracodawcy, nabędą odpowiednie doświadczenie w kwestii cyberbezpieczeństwa, a także zostaną wprowadzone aktualizacje do produktów zyskujących popularność w czasie pandemii, co znacząco utrudni działanie hakerom.

Niemniej jednak zapobieganie cyberzagrożeniom w dalszej perspektywie pozostanie priorytetem dla sektora publicznego i prywatnego, ze względu na rosnące wykorzystanie technologii w czasie pandemii.

Czytaj też: „Hashtag poisoning": zakłócanie protestów poparcia dla Nawalnego