aut. Andrzej Kozłowski 08.08.2019

„OPERACJA INFEKCJA 2.0”. NOWE DZIAŁANIA DEZINFORMACYJNE ROSJI

Rosjanie stale rozwijają operacje dezinformacyjne w cyberprzestrzeni. Ich ostatnie działania pokazują, że odpowiedzialne za nie są prawdopodobnie profesjonalne służby zaopatrzone w duże zasoby – zauważają analitycy DFRLab. Dodają oni, że coraz częściej Rosjanom zależy na ukryciu propagandowej działalności w sieci. Nawet za cenę jej popularności.

DFRLab z Atlantic Council zajmujący się badaniem rosyjskiej dezinformacji wykryło nową kampanię, za którą prawdopodobnie stoi rosyjski wywiad. Jej początek datuje się na rok 2014. Eksperci wpadli na trop tej operacji, kiedy w maju 2019 roku Facebook usunął 16 kont, 4 fanpage i jedno konto na Instagramie. Początkowo wydawało się, że to działania dezinformacyjne na małą skalę jednak wykorzystując te konta DFRLab było w stanie odkryć o wiele większą operację, która wykorzystywała szerokie spektrum manipulacji: wykorzystanie fałszywych profili, podszywanie się pod prawdziwe konta oraz fałszowanie dokumentów.

Eksperci opisując główne cele dezinformacji wymieniają wśród nich: wykorzystanie podziałów w Irlandii, podsycanie nastrojów antyimigranckich w Niemczech, kampanie skierowane przeciwko Ukrainie i ostatnim wyborom w państwach europejskich, ataki typu „fałszywej flagi” w Wenezueli oraz wzmacnianie narracji pro-kremlowskiej we wszystkich regionach światach. Pomimo iż, obiekty działania rosyjskiej dezinformacji były różne, to cel był ten sam, czyli podważenie stabilności Zachodu, podsycanie napięć społecznych oraz pogłębianie różnic między sojusznikami.

Kreml używał dobrze znanych narracji, próbując wykorzystywać napięcia w relacjach pomiędzy Stanami Zjednoczonymi a krajami europejskimi do pogłębienia problemów politycznych w Irlandii Północnej czy zwiększyć strach przed imigrantami w Niemczech. Starał się również przedstawić wydarzenia rozgrywające się w sąsiedztwie Rosji oraz takich państwach jak Ukraina, Wenezuela czy Syria zgodnie ze swoimi celami polityki zagranicznej. Eksperci DFRLab stwierdzili, że kampania dezinformacyjna miała bardzo ambitne cele, ale jej skutek określili jako stosunkowo mały. Większość przedstawianych historii i narracji nie zyskała popularności w Internecie. Kampania ta jednak pokazuje w jaki sposób, Kreml dostosowuje swoje środki manipulacji w sieci do kroków podejmowanych przez platformy mediów społecznościowych ukierunkowanych na usuwanie fałszywych informacji i botów. Sytuacja ta możne zostać określona jako cyfrowy wyścig zbrojeń do tego stopnia, że eksperci DFRLab porównali dezinformację do wirusa, który ciągle mutuje i się zmienia, stając się odpornym na obecne metody jego zwalczania.

Nowo odkryta operacja dezinformacyjna została nazwa przez DFRLab „Secondary Infektion”. Nazwa nawiązuje do sowieckich działań dezinformacyjnych z okresu zimnej wojny. Ich celem było rozpowszechnienie fałszywych informacji, że to Amerykanie stworzyli wirus HIV.

„Secondary Infektion” opierała się na takich samych zasadach, ale jej zakres tematyczny był o wiele szerszy – twierdzą eksperci DFRLab. Fałszywe historie publikowane przez Rosjan były oparte na

podrobionych dokumentach i materiałach, które zostały zmanipulowane z użyciem Photoshopha (jak np. fałszywe posty znanych polityków). Następnie były rozpowszechniane przez fałszywe konta, które istniałby bardzo krótko i były przeznaczone do publikowania jednej historii, a potem były określane jako „spalone". Przed publikacją historii były praktycznie nieaktywne, aby uniknąć wykrycia. W wielu przypadkach również te same artykuły były tłumaczone i rozpowszechniane w innych krajach.

Przykłady rosyjskich działań obejmują np. fałszywe tweety i memy mówiące o tym, że brytyjski wywiad wykorzysta technologie Deep Fake do pomocy Partii Demokratycznej w czasie wyborów do Kongresu w 2018 roku. Informacja ta pojawiła się pierwszy raz na stronie funnyjunk.com, a później została przekazana przez konto na Twitterze, które zostało stworzone tego samego dnia. W 2018 roku miała miejsce również inna operacja. Sfałszowano list Josepa Borrella - ministra spraw zagranicznych Hiszpanii, który już niebawem obejmie stanowisko Przedstawiciela Unii Europejskiej ds. Polityki Zagranicznej i Bezpieczeństwa, w którym ostrzega przed próbą zabójstwa nowego premiera Borisa Johnsona. Ta fałszywka została najpierw opublikowana na Facebooku przez konto zarządzane przez Rosjanina, a później na jej podstawie stworzono i opublikowano artykuły po hiszpańsku, które zostały przetłumaczone na angielski.

W Irlandii przygotowano jeszcze inną operację dezinformującą, składających się z trzech fikcyjnych historii, których sposób dystrybucji opierał się na tej samej strategii. Pierwszy krok zakładał umieszczenie fałszywej informacji w Internecie, następnie jej popularyzację poprzez przetłumaczenie na różne języki i promowanie za pomocą licznych kont w mediach społecznościowych.

W Niemczech głównym celem operacji dezinformacyjnych było zwiększenie niechęci do imigrantów, co ma znaczenie z uwagi na wyniesienie problemu imigracji do rangi jednego z najważniejszych. Narracja antyimigrancka przewijała się również w trakcie ostatnich wyborów do Europarlamentu. Innym przykładem antyeuropejskiej kampanii było podkreślanie, że liberałowie dążą do wywołania wojny przeciwko prawicy. W celu uwiarygodnienia przekazu kolejny raz sfabrykowano źródła. Tym razem wykorzystano fałszywy listy od szwedzkiego eurodeputowanego, który wzywał do sojuszu środowisk liberalnych przeciwko prawicy.

Według DFRLab rosyjskie operacje mają kilka celi. Są one oczywiście związane z osłabieniem jedności i integralności Zachodu, ale nie tylko. Promują również pro-kremolwski punkt widzenia na wydarzenia na arenie międzynarodowej. W szczególności istotne było to na początku konfliktu na Ukrainie. Następnie kampania została rozszerzona na Syrię i obecnie Wenezuelę. We wszystkich tych miejscach ma ona wydźwięk mocno antyzachodni. Jak podkreślają analitycy DFRLab, działania dezinformacyjne Kremla pokrywają się z rosyjskimi celami geopolitycznymi.

Operacje prowadzone przez Rosję nie są dziełem amatorów. Ich zasięg, poziom zaawansowania i koordynacji oraz zaangażowanie dużych zasobów wskazują na autorstwo służb wywiadowczych. Autorzy DFRLab podkreślają również, że ostatnia wykryta przez nich operacja była przez długi okres czasu utrzymywana w tajemnicy a jej autorom bardziej zależało na niewykryciu niż olbrzymiej popularności fałszywych narracji.

Niewielki skutek takiej operacji jest powodem do zadowolenia. Należy jednak pamiętać o kilku ważnych kwestiach. Po pierwsze, istnieją państwa takie jak Rosja, które inwestują swoje środki i zasoby w celu usprawnienia operacji manipulujących ludźmi w środowisku online. Ostatnio nacisk kładziony jest na kwestie związane z ukrywaniem takich operacji, co stanowi różnice w porównaniu do działań z przeszłości, kiedy Rosjanie specjalnie nie starali się ukryć własnych działań. Analitycy DFRLab ostrzegają, że Rosjanie uczą się na swoich błędach i to, że obecna ich kampania została wykryta nie oznacza, że z kolejnymi pójdzie równie łatwo. Niestety Internet i platformy mediów społecznościowych są bardzo podatne na wszelkiego rodzaju dezinformację, dlatego też wszystkie podmioty będą szukały coraz to nowych i bardziej wyszukanych sposobów ominięcia środków

bezpieczeństwa. Administracja państwowa, sektor prywatny oraz społeczeństwo obywatelskie powinny obserwować rozwój tego rodzaju zagrożeń i odpowiednio się do nich przygotować.

Autorzy DFRLab porównują problem walki z dezinformacją do cyberbezpieczeństwa. Wystarczy jedna luka w systemie aby dokonać skutecznego ataku. Podobnie jest w przypadku propagandy. Jedna udana kampania może doprowadzić do negatywnych zmian i wpłynąć na wynik wyborów, doprowadzić do kryzysu w służbie zdrowia czy wywołać zamieszki.