Cyberdefence 24

aut. Sylwia Gliwa 29.04.2021

„GHOSTWRITER" POWRACA. OPERACJE INFORMACYJNE ROSJI UDERZAJĄCE W WIZERUNEK NATO I STOSUNKI Z LITWĄ

- W lipcu ubiegłego roku FireEye opublikowała raport opisujący działania prowadzone w ramach operacji Ghostwriter.
- Firma przenalizowała wykorzystanie nieistniejących w rzeczywistości autorów treści, którzy mieli „udawać" lokalnych dziennikarzy do publikowania materiałów opartych na sfabrykowanych materiałach jako źródłach informacji.
- Większość z przebadanych przez ekspertów działań, było narracjami wymierzonymi w NATO w ramach, których wykorzystywano włamania na strony internetowe lub fałszywe konta e-mail do rozpowszechniania sfabrykowanych treści, w tym sfałszowanej korespondencji od przedstawicieli wojska.

Operacja Ghostwriter, czyli kampania wpływu wymierzona w obszar informacyjny Polski, Litwy i Łotwy, została ujawniona w lipcu ubiegłego roku. Z najnowszego raportu Madiant (FireEye) wynika niepokojący wniosek – działania przeprowadzane w jej ramach wykorzystywały również przejęte konta polskich urzędników w mediach społecznościowych w celu rozpowszechniania narracji, mających zdyskredytować polski rząd i poszerzyć istniejące wewnętrzne podziały polityczne.

Firma FireEye opublikowała kolejny raport odnośnie działań informacyjnych w ramach operacji określonej mianem Ghostwriter. Jej kolejnym przejawem były wykryte kampanie, w których ofiarami padli m.in. politycy Zjednoczonej Prawicy. Jak wskazują eksperci odpowiedzialni za analizę wykrytych działań, narracje, które były promowane poprzez te działania miały na celu zdyskredytowanie rządzącej koalicji politycznej, poszerzenie istniejących wewnętrznych podziałów politycznych i stworzenie obrazu rozłamu koalicyjnego w Polsce.

Atak na media społecznościowe polityków elementem operacji informacyjnych

W każdym z wykrytych incydentów treści były rozpowszechniane za pośrednictwem Twittera, Facebooka lub Instagrama. Dobrze znane opinii publicznej incydenty dotyczyły: rozpowszechniania kompromitujących zdjęć urzędników i osób, z którymi są powiązani, fałszywego oskarżenia o krytykę aktywistek oraz fikcyjnych oświadczeń o zrzeczeniu się przynależności do partii rządzącej.

Omawiane przez specjalistów FireEye przykłady dotyczyły posłanki Joanny Borowiak, posła Marcina Duszka, minister rodziny i polityki społecznej Marleny Maląg, posłanki Iwony Michałek oraz posła Marka Suskiego.

W grudniu 2020 roku na oficjalnym profilu Facebookowym minister Maląg pojawił się wpis na temat Strajku Kobiet, w którym znalazły się treści obraźliwe i rasistowskie. Chwilę później szefowa MRiPS za pośrednictwem Twittera poinformowała, że jej konto na Facebooku zostało zhakowane. W styczniu

natomiast informowaliśmy o sprawie Marka Suskiego. Za pośrednictwem jego twitterowego konta opublikowano kompromitujące zdjęcia jednej z radnych.

Działania, do realizacji których wykorzystano przejęte konta na portalach społecznościowych znanych polityków miały na celu głównie uderzenie w wizerunek zarówno ich jak i partii rządzącej. Jednocześnie, co należy podkreślić, działania te ukierunkowane były na rzecz podburzania nastrojów społecznych - jak przy okazji strajków kobiet i krytyki, która została wymierzona w aktywistki poprzez konto minister Maląg.

Nie tylko budowanie podziałów w społeczeństwie… NATO jako stały cel ataków

W październiku 2020 roku, jak czytamy w raporcie, doszło również do operacji mającej wpłynąć na postrzeganie NATO oraz podkreślenie agresywnych zamiarów Sojuszu względem Rosji. Działania te wskazywały, że wojska NATO przygotowują się do ataku na Rosję oraz prowadzenia działań zbrojnych na terenie Polski, Litwy i Łotwy. Miały one bez wątpienia wpłynąć na postrzeganie organizacji przez obywateli tych trzech państw.

Schemat działań jest już znany z wcześniejszych operacji opisywanych na naszym portalu. Sfabrykowany artykuł pojawiał się na polskich portalach, a następie linki do tych treści były rozpowszechniane za pośrednictwem mediów społecznościowych, w tym przez przejęte konta polskich obecnych i byłych posłów.

Spreparowany artykuł opierał się częściowo na prawdziwej informacji o spotkaniu ministrów obrony w ramach NATO i był de facto przekopiowaniem tekstu informacyjnego, w którym zmieniono tytuł i dodano dodatkowy komentarz, że Polska ma stać się de facto epicentrum przyszłych zmagań wojennych. Artykuł ten pojawił się na Prawy.pl i Obserwatorze Nadodrzańskim oraz na stronie starostwa powiatowego (wschowa.info). Analitycy FireEye wskazują, że nie byli wstanie ustalić, czy teksty pojawiły się w wyniku włamania na serwisy czy w efekcie celowego działania.

Podobny schemat działań mogliśmy zaobserwować np. podczas ataku na Akademię Sztuki Wojennej, której przypadek opisywaliśmy w naszej analizie Akademia Sztuki Wojennej obiektem działań dezinformacyjnych. Próba osłabienia relacji z USA. W ramach ataku, na stronie głównej serwisu uczelni, 22 kwietnia ubiegłego roku został umieszczony sfabrykowany list rektora-komendanta Ryszarda Parafianowicza, skierowany do wojskowych, w którym generał zarzuca partii rządzącej nieodpowiedzialną politykę względem Stanów Zjednoczonych. W jego treści uderzono również w amerykańską obecność na flance wschodniej, gdzie dochodzi do prób „demonstrowania swojej siły wojskowej", a także zarzut o budowaniu niesprawiedliwych oskarżeń względem Rosji. Jak wynikało z analizy przeprowadzonej przez naszą redakcje, sfabrykowany list okazał się być jedynie elementem w szerszej operacji dezinformacyjnej. Kampania miała na celu pogorszenie relacji pomiędzy sojusznikami, a przede wszystkim uderzanie w stacjonujące w Polsce wojska NATO.

Prostytucja w Wojsku Polskim?

W lutym br. zidentyfikowano również działania uderzające w dobre imię naszej armii. Operacja skierowana do odbiorców z Litwy i Polski została przeprowadzona w dniach 25-26 lutego i promowała narrację o udziale amerykańskich, polskich oraz litewskich urzędników w skandalu związanym z prostytucją w Siłach Zbrojnych RP.

W ramach tej operacji promowano narrację, według której polskie Ministerstwo Obrony Narodowej wykorzystuje kobiety oficerów wojska do „eskortowania" ważnych polskich i zagranicznych funkcjonariuszy. W celu realizacji zadań posłużono się co najmniej jednym serwisem informacyjnym oraz stroną internetową Elżbiety Witek.

Jak wskazano w raporcie, działania te miały być bez wątpienia elementem budowania napięć na linii Polska-Litwa. Do jej przeprowadzenia wykorzystano sfabrykowany artykuł rozpowszechniany zarówno poprzez serwisy informacyjne jak i media społecznościowe.

Do sprawy odniósł się m.in.rzecznik ministra koordynatora służb specjalnych Stanisław Żaryn za pośrednictwem Twittera.

> Further information activities aimed at hitting the credibility of the Polish Armed Forces, as well as ridiculing the most important officials in Poland and creating tensions between PL and LT. The actions of the info-aggressor follow a scenario known from previous attempts. 1/5 pic.twitter.com/5fSuJRMt1c
>
> — Stanisław Żaryn (@StZaryn) February 26, 2021

Kto jest za to odpowiedzialny?

Analiza wykrytych działań pozwoliła na ustalenie jednego z podmiotów prawdopodobnie współodpowiedzialnego za prowadzenie operacji – UNC1151 – grupę prawdopodobnie sponsorowaną przez państwo. Jak wskazuje FireEye, jak dotychczas podmiot ten nie był znany ekspertom. Jak wskazują wyniki przeprowadzonych badań grupa od początku 2021 roku rozszerzyła swoją działalność w zakresie kradzieży danych uwierzytelniających na użytkowników z Niemiec, ze szczególnym uwzględnieniem polityków.

Według ekspertów FireEye UNC1151 prowadzi działania wymierzone w odbiorców z Polski, Litwy, Estonii, Ukrainy, Irlandii, Kolumbii, Szwajcarii i Niemiec.