FLANKA WSCHODNIA POD ROSYJSKIM "OSTRZAŁEM" DEZINFORMACYJNYM. DEFENCE24 NA LIŚCIE CELÓW

Operacja dezinformacyjna wymierzona w obecność wojsk amerykańskich w regionie z którą zmierzyliśmy się w ostatnich dniach jest bliźniaczo podobna do tych, które przeprowadzono na terenie państw bałtyckich. Tego typu działania z pewnością będą się powtarzać, natomiast poziom ich zaawansowania będzie tylko rosnąć. Czy jesteśmy gotowi na wojnę informacyjną?

Jak informował portal CyberDefence24.pl, pracownik Grupy Defence24 padł ofiarą cyberprzestępców, którzy wykorzystując jego dane osobowe oraz specjalnie utworzoną w tym celu skrzynkę pocztową, rozsyłali wiadomości z prośbą o udzielenie komentarza do spreparowanej informacji o organizacji przez burmistrza Orzysza Zbigniewa Włodkowskiego marszu "Nie dla wojsk USA w Polsce!" oraz link do artykułu, który to mógł zawierać szkodliwe oprogramowanie.

Wspomiany link odsyłał do artykułu na portalu "Tygodnik Działdowski", na którym - jak ustalił portal CyberDefence24.pl - został on umieszczony w wyniku działań hakerskich. Obecnie portal zawiesił swoją działalność i skierował sprawę ataku do CERT-u. Wygląda jednak na to, że "Tygodnik" nie był jedyną ofiarą, a zaledwie jednym z ogniw, za pomocą którego cyberprzestępcy próbowali dotrzeć do szerszej publiki. Artykuł o tym samym tytule pojawił się również na innych lokalnych portalach - it.mragowo.pl, info.elblag.pl oraz elblag24.pl. Jednak prawdziwego rozgłosu informacji miała z pewnością przynieść prośba o komentarz do sprawy, wysłana od pracownika największego w Polsce i Europie portalu o bezpieczeństwie i obronności, jakim jest Defence24.pl, pod którego podszywali się cyberprzestępcy.

"Nie dla wojsk USA w Polsce!", czyli marsz, na którego zapomnieli przyjść "patrioci"…..

Jak informowaliśmy, burmistrz miasta Orzysz - Zbigniew Włodkowski - zaprzeczył informacjom, jakoby na stronie urzędu miasta pojawiła się informacja o zaproszeniu do udziału w marszu "NIE dla wojsk USA w Polsce!". Zgodnie z umieszczanymi na lokalnych portalach wiadomościami miał odbyć się on 20 stycznia 2020r., o godzinie 12:00 obok budynku Urzędu Miejskiego (ul. Rynek 3) w Orzyszu.
W artykułach, które pojawiły się na lokalnych portalach, a umieszczanych przez hakerów, reklamowany był on jako "marsz patriotów". Wygląda jednak na to, że informacja do przeciwnych obecności wojsk amerykańskich w Polsce "patriotów" nie dotarła.

Organizacja marszu, zgodnie z ustawą "Prawo o zgromadzeniach" wymaga przesłania do odpowiedniego urzędu gminy zawiadomienia o zamiarze zorganizowania zgromadzenia - w tym wypadku do Urzędu Miejskiego w Orzyszu. CyberDefence24.pl zapytał burmistrza Zbigniewa Włodkowskiego, czy w sposób formalny podjęto próby rejestracji takiego marszu, jednak zgodnie z przekazanymi informacjami - nikt takich działań nie podejmował. Urząd miasta potwierdził, że zaplanowane wydarzenie nie miało miejsca, nikt też nie zjawił się w terminie i miejscu wskazanym w

rozpowszechnianej informacji. Burmistrz miasta raz jeszcze podkreślił, że wiadomość o rzekomym opublikowaniu zaproszenia na stronie urzędu jest nieprawdziwa a informacje zawarte w artykułach na lokalnych portalach zostały spreparowane.

Również Policja nie odnotowała jakiejkolwiek informacji, aby takie zgromadzenie się odbyło. Rzecznik Policji wskazał także, że nie otrzymano żadnego zgłoszenia dotyczącego nawoływania do nienawiści na tle rasowym, czy narodowościowym w tym dniu.

Redakcja CyberDefence24.pl podjęła również próby skontaktowania się z wydawcami portali, na których ukazał się sfabrykowany artykuł. Zgodnie z informacjami, które udało się pozyskać, cyberprzestępcy podjeli wiele starań, aby wiadomość o marszu została rozpowszechniona. "Tygodnik Działdowski" zmagał się z atakami hakerów przez dwa dni, podobnie jak inne redakcje. Gdy spreparowane artykuły były usuwane, cyberprzestępcy publikowali je ponownie na eksponowanych miejscach. Z informacji do których dotarł CyberDefence24.pl wynika również, że na różnych portalach "wisiała ona" od godziny do nawet kilkunastu - na jednym z nich została ona umieszczona w niedzielę i została usunięta dopiero następnego dnia.

W jednym przypadku nie doszło do zhakowania strony, a artykuł ukazał się na serwisie dziennikarstwa obywatelskiego orzysz.wm.pl, należącego do grupy WM Sp. z. o. Autorem artykułu, jak i innych tekstów był bloger, który - jak dowiedział się portal CyberDefence24.pl - nie jest w żaden sposób związany z grupą WM. Jego działalność miała stanowić przykład wspomnianego "dziennikarstwa obywatelskiego". Publikował on artykuły pod imieniem i nazwiskiem, pod którym umieszczał również liczne komentarze na innych portalach. Jego poprzednie wpisy na blogu miały również wydźwięk antyamerykański i skierowane były przeciwko NATO. Pomimo, że aktywny był na portalu orzysz.wm.pl od 2017 roku, to wczoraj (tj. 21 stycznia 2020 roku) zarówno jego artykuły jak i blog zostały ze strony skasowane. Osoba o tym nazwisku jest również autorem petycji sprzeciwiającej się stacjonowaniu obcych wojsk oraz twórcą postów na ten temat. Z uwagi na fakt, że artykuły umieszczano na serwisie "dziennikarstwa obywatelskiego", zasadne jest postawienie pytania, czy istnieje mechanizm weryfikacji treści przez takie media. Na przykładzie tego blogera widzimy, że umieszczane przez niego treści mogły odegrać istotną rolę w kampanii dezinformacyjnej. Artykuł z zaproszeniem na marsz został tam opublikowany w piątek, tj. 17 stycznia 2020 roku o 13:30 i aktywny był aż do wtorku (21 stycznia 2020 roku) rano.

Idealny czas, idealne okoliczności …. modus operandi ten sam

Czas rozpoczęcia działań dezinformacyjnych, podobnie jak dzień organizacji marszu przeciwko obecności wojsk USA w naszym kraju, nie został wybrany przypadkowo. 20 stycznia br. w Bemowie Piskim doszło do uroczystego przekazania dowodzenia Batalionową Grupą Bojową NATO. Dowództwo nad batalionem objął 3 szwadron The Wolfpack z 2 Pułku Kawalerii z Vilseck w Niemczech, który zmienił 3 szwadron "Pacesetter" z 278 Pułku Kawalerii Pancernej z Pensylwanii.

Mondus operandi tej operacji podobny jest do tego znanego już z rozpowszechniania fake newsa o ewakuacji ludności z obszarów zagrożonych działaniami militarnymi. Nieprawdziwą informację umieszczono w nocy m.in. na portalach niezależna.pl, epoznan.pl, powiatlomzynski.pl, kalinowo.pl. Hakerzy przełamali zabezpieczenia tych portali i publikowali fałszywe wiadomości za ich pośrednictwem. Z perspektywy czasu można stwierdzić, że cyberprzestępcy mieli ku temu możliwość z uwagi na "dziury" w ich CMS-ach (narzędzie do administrowania stroną).

Czytaj też: Litwa i Polska celem ataku informacyjnego. W tle ćwiczenia wojskowe [KOMENTARZ]

Podobna sytuacja miała również miejsce w przypadku fake newsa o amerykańskim żołnierzu, który

miał zamordować Polaka. Artykuł pod tytułem "UWAGA! Policja poszukuje żołnierza USA. Jest podejrzany o ZABÓJSTWO" był widoczny przez około trzy godziny w godzinach nocnych na portalach epoznan.pl, podlasie24.pl, leszno.pl, jaworzyna.net, radiopodlasie.pl, powiatchoszczno.pl, miedzyrzecz.pl czy wschowa.info - informowała wtedy Zaufana Trzecia Strona. Portale prawdopodobnie zostały zhakowane. W tym wypadku publikacja w godzinach nocnych gwarantowała, że redakcje zauważą fałszywą treść dopiero następnego dnia po przyjściu do pracy. W wypadku podszywania się pod pracownika Grupy Defence24, akcja została przeprowadzona w weekend, kiedy istniało mniejsze prawdopodobieństwo telefonicznej weryfikacji treści.

Operacje informacyjne wymierzone w żołnierzy NATO prowadzone są na całej flance wschodniej. Podobne przypadki, jak ten z którym mamy do czynienia obecnie, zdarzały się już wcześniej w państwach bałtyckich. Przykładowo, na Łotwie pojawiła się fałszywa informacja, że stacjonujący tam niemieccy żołnierze zgwałcili miejscową kobietę. Inny przypadek, również dotyczący żołnierzy kontyngentu z Niemiec, miał miejsce w Kownie, gdzie mieli się oni dopuścić zbezczeszczenia cmentarza żydowskiego. Czas wypuszczenia fake newsa również nie był przypadkowy. Trwało wtedy w Wilnie spotkanie pomiędzy prezydentem Litwy a przedstawicielami społeczności żydowskiej ze Stanów Zjednoczonych. Fałszywą historię wysłano także do międzynarodowych redakcji jak The Jewish Press, Jewish National News i Infos Israel News. Cyberprzestępcy podszyli się również pod znanego litewskiego dziennikarza i posługując się jego danymi wysłali pytania do biura prasowego prezydenta (podobnie jak miało to w przypadku przedstawiciela Grupy Defence24). Wreszcie zhakowali także portal kasvyksta.lt, publikując tę samą fałszywą historię. Schemat zastosowany na Litwie jest więc bliźniaczo podobny do tego z którego skorzystano obecnie w Polsce.

Druga znacząca operacja informacyjna na tym terenie, która nie umknęła uwadze zachodnich mediów, związana była z fałszywymi doniesieniami o przeniesieniu broni jądrowej z Turcji na Litwę. Pojawiła się ona w czasie napięć między Waszyngtonem i Ankarą. Na początku hakerzy włamali się na portal kasvyksta.lt, na którym umieścili fake newsa o przeniesieniu broni jądrowej na Litwę. Następnie podszywając się pod znanych dziennikarzy wysłano prośby o komentarz w tej sprawie do biura prasowego litewskiego prezydenta i innych przedstawicieli administracji rządowej. Na tym jednak operacja się nie zakończyła. Kolejnym celem byli dziennikarze litewskich mediów, którzy otrzymali maile od cyberprzestępców podszywających się pod urzędników litewskiej administracji z fałszywymi informacjami w tej sprawie. Przykłady te pokazują, że problem dezinformacyjny jest ponadnarodowy i wymaga ścisłej koordynacji pomiędzy członkami NATO.

Czytaj też: Amerykańska broń nuklearna na Litwie - fake news rosyjskim sposobem na osłabienie NATO?

Czy jesteśmy gotowi na wojnę informacyjną?

Podobne operacje będą się powtarzać, a ich poziom zaawansowania z pewnością będzie tylko rosnąć. Kampania, której elementem było wysyłanie fałszywych wiadomości podszywając się pod pracownika Grupy Defence24, tylko to potwierdza. W wypadku tego typu operacji konieczne jest nie tylko zwiększenie kontroli mediów nad publikowanymi za ich pośrednictwem informacjami, ale również - jak pokazują liczne przykłady - zwiększenie zabezpieczeń nawet lokalnych portali informacyjnych. Także władze nie mogą pozostać bierne w oczekiwaniu na rozwój wypadków. Wygląda na to, że szczególnym obszarem zainteresowania akcji dezinformacyjnych przeprowadzanych w Polsce i państwach bałtyckich jest kwestia amerykańskiego zaangażowania w regionie i stacjonowania wojsk USA. Niezbędne wydaje się przeprowadzenie kampanii informacyjnych, za pomocą których nie tylko obala się opublikowane już fake newsy, ale również objaśnia się cel amerykańskiej obecności, czy wyczula obywateli na możliwość pojawiania się spreparowanych wiadomości. Konieczne jest również

wsparcie dla lokalnych mediów w zabezpieczeniu ich stron internetowych. Wygląda na to, że zadanie to leży w gestii Ministerstwa Cyfryzacji i NASK-u, które powinny zaangażować środki w poprawę cyberbezpieczeństwa, nie tylko na poziomie krajowym.

Andrzej Kozłowski/Sylwia Gliwa