KOMPONENT CYBER ROSYJSKIEJ AGRESJI NA UKRAINĘ JEST OGRANICZONY

Rosyjskie uderzenia rakietowe na terytorium Ukrainy 24 lutego, które rozpoczęły działania zbrojne były poprzedzone cyberatakami wymierzonymi w ukraińskie sieci komputerowe i strony internetowe. Jednak nie wszystkie z tych cyberataków (a w zasadzie mniejszość) miały charakter działań z wykorzystaniem cyberbroni we właściwym tego słowa znaczeniu. Są one także dalekie od wielu wizji cyberwojny przedstawianych przez ekspertów w ciągu ostatnich dekad. Najbardziej powszechne z nich - ataki DDoS na strony ukraińskich instytucji publicznych i organizacji – nie mają charakteru działań zbrojnych, choć mogą im towarzyszyć. W tym kontekście jednak ich celem jest sianie paniki i paraliż informacyjny wśród społeczeństwa, ale nie zniszczenie, które charakteryzuje efekty wykorzystania broni. Temu bliższe są ataki z wykorzystaniem złośliwego oprogramowania, które spełnia podstawowe charakterystyki cyberbroni, gdyż za cel ma trwałe wymazywanie danych na zainfekowanych maszynach (dopiero odkryte szczepy to FoxBlade i HermeticWiper). Takim oprogramowaniem między innymi 25 lutego zaatakowany został ukraiński posterunek na granicy z Rumunią. Jak dotąd, ofensywne działania Rosji przejawiają jednak stosunkowo ograniczony charakter, co jest szczególnie zaskakujące w kontekście faktu, że Rosja od lat rozwija swoje zdolności cyberofensywne i uznawana jest za jedną z najbardziej agresywnych potęg w tym kontekście. Innymi słowy, komponent cyber w rosyjskich działaniach wojennych odgrywa mniejszą rolę, niż dotychczas zakładano. Jedną z przyczyn takiego stanu rzeczy może być przekonanie rosyjskiego dowództwa o niskiej przydatności cyberbroni w sytuacji wojny konwencjonalnej.

„CROWDSOURCING" KONFLIKTU W CYBERPRZESTRZENI

Jednym z najciekawszych i najbardziej zaskakujących elementów konfliktu ukraińsko-rosyjskiego w cyberprzestrzeni było powołanie ochotniczej "Armii IT", której powstanie zainicjował na Twitterze wicepremier i Minister Cyfryzacji Ukrainy Mychajło Fedorow 26 lutego. Do wstąpienia w jej szeregi wezwał on globalną społeczność programistów, hakerów a nawet osoby bez zdolności technicznych, w tym influencerów. Działania są organizowane poprzez komunikator Telegram – grupa, do której dostęp jest otwarty dla wszystkich, liczy obecnie ponad 280 tysięcy osób. Celami „Armii IT" jest:

- dysrupcja rosyjskiej i białoruskiej przestrzeni informacyjnej poprzez przebicie się przez cenzurę, dotarcie do rosyjskich internautów oraz przerwanie działalności propagandowej rosyjskich mediów. Taktyka ta realizowana jest wielowektorowo: masowo zgłaszane są kanały rozpowszechniające rosyjskie narracje w mediach społecznościowych, tworzone są materiały wideo czy krótkie reklamy mające wyświetlać się rosyjskim Internautom, wezwano również do hakowania tradycyjnych mediów;
- zakłócenie działania stron internetowych i usług kluczowych podmiotów w cyberprzestrzeni – banków, dostawców energii, operatorów telekomunikacyjnych itp. Wśród wymienionych celów znajdują się m.in. Narodowy Bank Rosji, Gazprom, Łukoil, moskiewska giełda, rosyjskie i białoruskie Ministerstwa, a także witryny pozwalające Rosjanom zminimalizować efekt sankcji i chronić się przed atakami, np. internetowe kantory kryptowalutowe czy usługodawcy cyberbezpieczeństwa w Rosji;
- wywieranie presji na organizacje międzynarodowe, m.in. ONZ czy Human Rights Watch, oraz korporacje takie jak PayPal, poprzez zmasowany mailing dokumentujący rosyjskie zbrodnie popełniane w Ukrainie oraz wezwanie do zaprzestania świadczenia usług.

Trudno jest na ten moment oszacować skuteczność działań proukraińskich haktywistów, niemniej wiele stron wymienionych jako cele jest nieaktywnych dla internautów z Zachodu (co mogło jednak nastąpić na skutek odcięcia dostępu zachodnich serwerów). Działania zdają się jednak potwierdzać oficjalne przekazy rosyjskiego rządu, który donosi o zmasowanych atakach DDoS i utrudnieniach w ciągłości działania rządowych serwisów. Ochotnicza "Armia IT" to swoiste "pospolite ruszenie" w cyberkonflikcie toczonym pomiędzy Rosją a Ukrainą, zaś bardziej zaawansowane działania prowadzone są przez dedykowanych specjalistów IT, komunikujących się utajnionymi kanałami, których akcje spowite są mgłą wojny.

HAKTYWIZM WOJENNY

Oczy społeczności międzynarodowej są również skierowane w stronę grup haktywistycznych takich jak Anonymous, Network Batalion 65 czy Belarusian Cyber-Partisants, które wypowiedziały "cyberwojnę" Federacji Rosyjskiej

w odpowiedzi na jej agresję na Ukrainę. Najsłynniejsza z tych grup, Anonymous, to zdecentralizowany kolektyw osób zjednoczonych ideologicznie wokół danej sprawy, które dążą do tymczasowego wspólnego celu. W jej ramach funkcjonuje wiele komórek, które mają ze sobą ograniczony kontakt - bądź nie mają go wcale. Nie wiemy jednak, kto kryje się pod cyfrowymi maskami Guya Fawkesa. Wielu analityków podejrzewa, że szyld Anonymous jest obecnie wykorzystywany w ramach operacji fałszywej flagi przez grupy sponsorowane przez państwa Zachodu, na co wskazywałby poziom skomplikowania hacków przeprowadzonych w ostatnich dniach. Nie można jednak z całkowitą pewnością wykluczyć, że za tymi działaniami nie stoją ochotnicy o specjalistycznej wiedzy IT. W następnych dniach możemy spodziewać się nawet bardziej spektakularnych operacji niż te dotychczas przeprowadzone, które i tak odbiły się głośnym echem – jak np. zhakowanie rosyjskich stron rządowych przez Anonymous, włamanie do systemów Moskiewskiego Instytutu Bezpieczeństwa Jądrowego przeprowadzone przez NB65, czy naruszenie systemów działania białoruskiej kolei, będące sabotażem białoruskich cyber-partyzantów. Możemy jednak również spodziewać się odwrócenia operacji fałszywej flagi i wykorzystania szyldu Anonymous przez antyzachodnich hakerów. W czwartek rano przeprowadzono atak na serwis money[.]pl, który skutkował przekierowaniem użytkowników mobilnej wersji serwisu na podstawioną stronę z wiadomością “Ukraina musi przegrać”, podpisaną właśnie jako “Anonymous”.

NIE MAMY JESZCZE DO CZYNIENIA Z CYBERWOJNĄ - ALE GROŹBA ESKALACJI CYBERKONFLIKTU JEST REALNA

Pomimo narastającego konfliktu w cyberprzestrzeni w związku z rosyjską inwazją na Ukrainę, nie możemy jednak stwierdzić, że doszło do wybuchu cyberwojny we właściwym tego słowa znaczeniu. Istotne jest rozróżnienie pojęć cyberkonfliktu od cyberwojny. Cyberkonflikt rozumieć można jako wrogie działania w cyberprzestrzeni i takie znamiona mają choćby działania grupy Annonymous przeciwko Rosji, skupiające się głównie na wykorzystaniu środków cyfrowych do prowadzenia sabotażu i dywersji (zadeklarowany atak na rosyjską agencję kosmiczną, zhakowanie kanałów rosyjskiej telewizji). Cyberwojna zaś, to w pełni ofensywne działania toczone przez państwa w cyberprzestrzeni, które spełniają kluczowy warunek: mają niszczycielski charakter i są prowadzone za pomocą cyberbroni na dużą skalę. W tym kontekście, cyberataki przeprowadzane przez Rosję są nadal ograniczone ilościowo oraz jakościowo. Jednak ryzyko dalszej eskalacji cyberkonfliktu – a nawet jego przeistoczenia się w cyberwojnę - jest jak najbardziej możliwe. Intensyfikacja cyberkonfliktu, którą w ostatnich dniach obserwujemy, związana m.in. wzrostem liczby zaangażowanych podmiotów i wrogich działań, może rozlać się angażując bezpośrednio aktorów państwowych. Nie jest też jasne, którzy z operujących aktorów pozapaństwowych działają jako tzw. proxy – a więc na zlecenie aktorów państwowych. W ostatnich dniach doszło m.in. do skompromitowania grupy cyberprzestępczej Conti podejrzewanej o związki z rosyjskim wywiadem, po tym, jak jej członkowie opowiedzieli się w konflikcie po stronie Rosji. Działania takich podmiotów mogą łatwo przekroczyć próg tego, co uznawane jest za działanie o charakterze wojennym i sprowokować zdecydowaną reakcję ze strony państwa.