GRUDZIEŃ 2022

Raport ENISA 2022 Landscape Threat

część 2

EUROPEAN UNION AGENCY FOR CYBERSECURITY

fundacja instytut CYBERBEZPIECZEŃSTWA

AUTOR

Rafał Prabucki

MINISTERSTWO SPRAWIEDLIWOŚCI

www.ms.gov.pl

FUNDUSZ SPRAWIEDLIWOŚCI

SFINANSOWANO ZE ŚRODKÓW FUNDUSZU SPRAWIEDLIWOŚCI, KTÓREGO DYSPONENTEM JEST MINISTER SPRAWIEDLIWOŚCI

Wpływ wojny rosyjsko-ukraińskiej na cyberzagrożenia

Konflikt między Rosją a Ukrainą powoduje, że ENISA w swoich analizach zaczęła również uwzględniać nowe cyberzagrożenia. O ile w ENISA Threat Landscape 2022 wskazywano pewne czerwone flagi w kilku obszarach i bardzo mocno podkreślano powiązania pomiędzy różnymi zagrożeniami a wojną w Ukrainie, o tyle kolejny raport o dezinformacji – Foreign Information Manipulation Interference (FIMI) and Cybersecurity – Threat Landscape jest dogłębną analizą wcześniej opisanych problemów.

W kwestii wojny w Ukrainie ENISA wypunktowała kilka ważnych elementów:

1. Wpływ geopolityczny i związane z nim zmiany w zakresie:
   - wzrostu aktywności haktywistów;
   - pojawienia się działań w cyberprzestrzeni podejmowanych przez osoby skoordynowane z jednostkami prowadzącymi działania wojskowe;
   - mobilizacji haktywistów do inicjowania wspólnych działań;
   - cyberprzestępczości;
   - pomocy ze strony pewnych grup państw podczas tego konfliktu.
2. Uznanie geopolityki za wciąż niezwykle istotny element operacji odbywających się w cyberprzestrzeni.
3. Koordynacja działań podmiotów państwowych realizujących cele zarówno wojskowe, jak i cybernetyczne skutkowała działaniami destrukcyjnymi.
4. Nowa fala haktywizmu związana z wojną rosyjsko-ukraińską.
5. Umocnienie się pojmowania dezinformacji jako narzędzia prowadzenia wojny.
6. Wskazanie – jak w poprzedniej części tego tekstu – wpływu wojny w Ukrainie w zakresie phishingu (tj. metod związanych z budowaniem fałszywego zaufania na linii atakujący-użytkownik) co do opcji budowania przynęt.
7. Wypracowanie się pewnego modelu walki o charakterze destrukcyjnym. Destrukcyjność operacji w cyberprzestrzeni towarzysząca wojnie polegała na atakach typu Wiper (wymazanie/nadpisanie/usunięcie danych atakowanego). Ich celem było naruszenie ciągłości działania podmiotów publicznych i innych, których przerwa w funkcjonowaniu powodowałaby podważenie zaufania publicznego i osiągnięcie stanu FUD (ang. fear, uncertainty, and doubt, czyli strach, niepewność i wątpliwości). Wywołane w ten sposób nastroje pewnego społeczeństwa umożliwiały przeprowadzanie działań dezinformacyjnych.

Wojna pomiędzy Rosją a Ukrainą niewątpliwie bardzo mocno odcisnęła swoje piętno na sposobie postrzegania wojny informacyjnej w cyberprzestrzeni. W raporcie Threat Landscape za okres od lipca 2021 do lipca 2022 poświęcono jej podrozdział 9.1.1 w odniesieniu do trendów dotyczących dezinformacji. Dla odbiorców raportu był to wyraźny sygnał, że problem wojny informacyjnej staje się ważnym elementem trwającego konfliktu. Po tej publikacji pojawił się kolejny raport, Foreign Information Manipulation Interference (FIMI) and Cybersecurity – Threat Landscape, tym razem w kooperacji ENISA-EEAS (European Union External Action), w którym zagadnienie dezinformacji rozbudowano o nowe pojęcie – FIMI (Foreign Information Manipulation Interference).

Czym jest FIMI

FIMI polega na wykorzystaniu informacji przez ingerencję w nią czy też manipulację przez obcy kraj (co do zasady wrogi). To integralna część działań wojennych. Raport Foreign Information Manipulation Interference (FIMI) and Cybersecurity – Threat Landscape podkreśla, że obronę przed tego typu zagrożeniem należy uznać za jedno z większych wyzwań w zakresie cyberbezpieczeństwa.

Nowy termin pojawił się w związku z wcześniejszymi obserwacjami, w których zwrócono uwagę, że często nie jakość, a ilość dezinformacji jest najważniejsza dla osiągnięcia celu przez atakującego. W sytuacji dużego natłoku wiadomości zanika u ludzi zdolność do odróżniania prawdziwych informacji od fałszywego przekazu. Taki nacisk na ilość położyła też Rosja przed rozpoczęciem działań zbrojnych w Ukrainie. Masowe rosyjskie kampanie dezinformacyjne miały na celu przedstawienie rzekomej słuszności inwazji. Zakładano, że zdezorientowane społeczeństwo nie będzie w stanie odróżnić prawdziwych informacji od tych, które zostały zmodyfikowane lub zmanipulowane.

Dlaczego jest to tak bardzo niebezpieczne?

Jak wskazuje się w raporcie, wykorzystanie informacji oraz zagraniczna ingerencja w nią stanowi rodzaj manipulacji i odnosi się do niepenalizowanego wzorca zachowania, który stanowi poważne zagrożenie i może negatywnie wpływać na system procedury i procesy polityczne. Taka działalność ma charakter manipulacyjny i jest prowadzona w sposób celowy oraz skoordynowany. Podmiotami takiej działalności mogą być jednostki zarówno państwowe, jak i niepaństwowe, w tym ich pełnomocnicy przebywający na własnym terytorium lub poza nim.
Ponadto oba raporty rozróżniają dezinformację intencjonalną (ang. disinformation) od tej nieintencjonalnej (ang. misinformation). Oznacza to, że w rozpowszechnianiu dezinformacji biorą też udział sami użytkownicy, którzy często udostępniają nieprawdziwy lub zmanipulowany przekaz. Mimo że w przekonaniu tych osób dany komunikat jest prawdziwy, to sama przekazywana przez nich informacja już nie. Trudności w obserwacji FIMI i wnioski W odniesieniu do FIMI podkreśla się, że chodzi o obserwację i zwalczanie dezinformacji intencjonalnej. Co więcej, istnieją trudności w jej ustandaryzowaniu w odniesieniu do parametrów takich jak czas i skutki. Wynika to z dwóch przyczyn:

- trudno precyzyjnie zmierzyć czas trwania zdarzenia związanego z FIMI/dezinformacją. Niektóre zdarzenia dotyczą incydentów bezpieczeństwa (jednorazowych, niepowtarzalnych działań), a inne operacji dezinformacyjnych;
- analiza wpływu wydarzeń związanych z FIMI/dezinformacją zależy przede wszystkim od ich zasięgu poza początkową „bańką informacyjną".

Powyższe przeszkody spowodowały, że ENISA i EEAS w raporcie poświęconym FIMI zdecydowały się na zastosowanie innych narzędzi pomocnych w analizie zagrożenia. Zdecydowano się na niezależne badanie czasu trwania incydentu oraz na podział skutków zdarzenia FIMI/dezinformacji na: dotkliwość działania (rozumianą jako zasięg tego zdarzenia) i wpływ działania (czyli dziedzinę, której dotyczy).
W odniesieniu do sektorów zaobserwowano, że ponad połowa zdarzeń miała bezpośredni wpływ na podmioty związane z różnymi aspektami funkcjonowania państwa, takimi jak:

- rząd i administracja;
- partie polityczne;
- obronność kraju;
- władza ustawodawcza.

W większości sytuacji obywatele nie zostali dotknięci atakiem bezpośrednio. W ponad połowie przypadków stanowią oni jedynie cel drugorzędny. W dokumencie ENISA i EEAS zauważono też, że pewne aktywności w zakresie budowania cyberbezpieczeństwa koncentrują się obecnie na sektorach krytycznych (np. energetyce lub transporcie), których zakłócenie z definicji jest szczególnie groźne dla społeczeństwa. W odniesieniu do tych sektorów stosuje się liczne regulacje, wyznaczające pewne podstawowe ramy działań podejmowanych w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa. Sektor, który obecnie pozostaje poza regulacjami, to sektor mediów i produkcji audiowizualnych. Należy jednak szczególnie zwrócić na niego uwagę w zakresie działań i aktywności typu FIMI.

Równie ciekawym elementem analizy fenomenu FIMI jest motywacja atakujących. Wskazuje się, że rzadko kiedy kierują się oni motywem finansowym. Częściej są to pobudki ideologiczne lub geopolityczne oraz chęć destabilizacji pewnych funkcjonujących już struktur.

Rekomendacje w sprawie FIMI

W ramach opracowania ENISA i EEAS przygotowała szereg rekomendacji dotyczących zjawiska FIMI. Ze względu na to, że obejmują one wiele wątków, warto podkreślić te, które zostały wypunktowane jako swoiste podsumowanie raportu w zakresie FIMI/dezinformacji:

1. Ważne jest rozróżnianie incydentów informacyjnych/cybernetycznych od operacji. Inaczej niż w przypadku podstawowych zagadnień z zakresu cyberbezpieczeństwa, dane typu open source na temat incydentów FIMI/dezinformacji często dotyczą całych operacji, na które składa się kilka incydentów. Jak zauważa ENISA i EEAS, nie stanowi to nic niezwykłego, ponieważ zdarzenia FIMI/dezinformacyjne często definiowane są jako takie dopiero po tak zwanym „połączeniu kropek" (ang. connecting the dots) pojedynczych incydentów.
2. W związku ze specyfiką FIMI rekomenduje się wspieranie odpowiednich mechanizmów wymiany informacji na zasadzie dobrowolności, na przykład opierając się na istniejących lub nowych Centrach Analizy i Wymiany Informacji (ang. Information Sharing and Analysis Center, ISAC). Można również wziąć pod uwagę wprowadzenie obowiązkowości zgłaszania FIMI za sprawą rozwiązań prawnych, które mogłyby się pojawić w NIS2.

3. Oprócz zgłaszania operacji ENISA i EEAS proponują oficjalnie rozróżnić incydent bezpieczeństwa od operacji dezinformacyjnych, jakimi są działania FIMI. Wpływ trwającego kilka dni incydentu w zakresie bezpieczeństwa cybernetycznego na środowisko informacyjne może znacznie przekraczać dane ramy czasowe. Ponadto nie zawsze może być jasne dla odbiorcy, co stanowi „koniec" operacji, w przeciwieństwie do bardziej zrozumiałego „tymczasowego wstrzymania operacji".
4. W rekomendacjach znajdziemy też wnioski dotyczące stosowania taktyk DISARM i MITRE. Przyjęcie taktyki DISARM według ENISA i EEAS najlepiej sprawdza się w opisywaniu zestawów incydentów, które mają wspólny cel i są częścią tej samej operacji, jak to ma miejsce w FIMI/dezinformacji. Inaczej to wygląda w przypadku taktyki MITRE, bardzo przydatnej w charakteryzowaniu pojedynczych incydentów, niezależnie od tego, czy mają one ten sam cel lub są elementem tej samej operacji.
5. Ponadto w rekomendacjach zwraca się też uwagę na nieoczywistość celu. Krajobraz zagrożeń przedstawiany w kolejnych cyklicznych raportach ENISA identyfikuje sektory dotknięte incydentem, bez potrzeby określania, czy stanowią one cel główny czy drugorzędny. W przypadku zdarzeń wynikających z FIMI/dezinformacji ważna okazuje się ocena, czy bezpośrednio dotknięta ofiara/sektor/obszar (pierwotna/pierwotny) jest rzeczywista, czy też jedynie wykorzystywana jako środek do osiągnięcia innego celu (wtórna/wtórny).
6. Zdarzenia związane z FIMI/dezinformacją często dotyczą sektorów, które niekoniecznie są uznawane za krytyczne (np. media), i mogą mieć katastrofalne skutki niezależnie od krytyczności danego sektora. Według ENISA i EEAS otwarta Platforma CTI jest uważana za bardziej odpowiednie narzędzie dla zdarzeń dezinformacyjnych.

Destrukcja w kosmosie i działania odwetowe

Kraj „agresor", zanim przystąpi do FIMI, zaczyna od działań destabilizacyjnych. W tym celu głównie będą wykorzystywane znane w cyberbepieczeństwie rozwiązania, takie jak złośliwe oprogramowania. Biorąc pod uwagę źródła medialne, które chętnie wskazują na znaczenie łączności, jaką Ukrainie zapewniają satelity komunikacyjne, warto przyjrzeć się przytoczonemu przez ENISA studium przypadku dotyczącego cyberbezpieczeństwa z perspektywy kosmosu. Komercyjne przedsiębiorstwo zajmujące się komunikacją satelitarną Viasat zostało zaatakowane złośliwym oprogramowaniem AcidRain. Skutki tego ataku były szczególnie widoczne na Ukrainie, ponieważ przestały działać modemy satelitarne Viasat. Ponadto atak dotknął urządzenia w Europie Środkowej. Doszło do zakłóceń w funkcjonowaniu farm wiatrowych i łączności satelitarnej z Internetem.

ENISA zwraca uwagę, że nierzadko ataki cybernetyczne kierowane w Ukrainę będą też dotykać inne kraje. Uznaje też za całkiem naturalne prawdopodobieństwo, że Rosja skoordynuje grupy cyberprzestępcze zajmujące się atakami z wykorzystaniem ransomware. Te grupy miałyby przeprowadzić destrukcyjne operacje w ramach odwetu za sankcje nałożone na Rosję i wsparcie udzielone Ukrainie. ENISA podkreśla, że wykorzystywanie grup przestępczych w cyberprzestrzeni przez różne kraje jest istotnym problemem, z którym trzeba walczyć.

Fenomen IT Army of Ukraine

Przy analizie rozbudowanego zagadnienia wpływu agresji rosyjskiej na Ukrainę warto też zwrócić uwagę na grupę IT Army of Ukraine. Trudno określić, czym obecnie ta jednostka jest. Sama ENISA pozostawia ten fenomen badaczom do prześledzenia. W dniu 26 lutego 2022 roku wicepremier Ukrainy i minister ds. transformacji cyfrowej ogłosił utworzenie Ukraińskiej Armii Informatycznej, jednocześnie zapraszając ochotników do wstępowania do niej. Kanał na komunikatorze Telegram zgromadził ponad 300 tys. subskrybentów z całego świata. Ukraińska Armia Informatyczna zdołała obrać za cel różne podmioty i przeprowadzała głównie skoordynowane ataki typu Distributed Denial of Services (DDoS). ENISA ze względu na hybrydowość tego podmiotu uznała, że nie jest najważniejsze opracowanie dokładnej definicji, a jedynie wskazanie trendu, który prawdopodobnie będzie się nasilał. Nie można bowiem wykluczyć, że wypracowany na Ukrainie wzorzec będzie w przyszłości realizowany przez inne kraje.

Polska w raporcie ENISA

W raporcie pojawił się również fragment poświęcony Polsce jako potencjalnemu państwu, na którym Rosja będzie dokonywać odwetu, chociażby za wsparcie udzielone Ukrainie. O ile wydaje się, że tego typu sprawy w Polsce w miarę możliwości traktuje się poważnie, o tyle należy zastanowić się, czy w kontekście zjawiska FIMI/dezinformacji jesteśmy dość odporni, aby nie dać się zmanipulować jako społeczeństwo. Szczególnie że ENISA podkreśla, że machina dezinformacyjna korzysta z takich wynalazków jak systemy sztucznej inteligencji czy też deepfake.

Rafał Prabucki

MINISTERSTWO SPRAWIEDLIWOŚCI
www.ms.gov.pl
FUNDUSZ SPRAWIEDLIWOŚCI
SFINANSOWANO ZE ŚRODKÓW FUNDUSZU SPRAWIEDLIWOŚCI, KTÓREGO DYSPONENTEM JEST MINISTER SPRAWIEDLIWOŚCI

fundacja@instytutcyber.pl
www.instytutcyber.pl