Do zaangażowania cyberprzestrzeni w działania wojenne na Ukrainie po 24 lutego 2022 roku ostatnim wydarzeniom na Biskim Wschodzie również towarzyszy wzmożona aktywność w tym obszarze. Przypomnijmy, że od początku działań zbrojnych podjętych na Ukrainie cyberprzestrzeń stała się istotną domeną działań wojennych. Zgodnie z informacjami przekazanymi przez izraelską firmę Checkpoint w okresie 24-27 lutego 2022 roku liczba cyberataków wymierzonych w ukraińskie instytucje polityczne i wojskowe wzrosło o 196 procent.

Ataki cybernetyczne na Izrael i Ukrainę

Podobnie liczba ataków cybernetycznych wymierzonych w Izrael wyraźnie wzrosła po 7 października 2023 roku, tj. po ataku organizacji terrorystycznej Hamas na terytorium izraelskie. Zorganizowane grupy hakerów, również te, związane z Federacją Rosyjską (chociaż oficjalnie nie udowodniono rosyjskich powiazań z działaniami Hamasu podejmowanymi w cybersferze), blokują izraelskie strony rządowe. Scenariusz podejmowanych działań pozostaje analogiczny do tego zastosowanego na Ukrainie w przededniu 24 lutego 2022 roku. Zgodnie z danymi zawartymi w raporcie Microsoft Digital Defense Raport 2023 od lipca 2022 roku do czerwca 2023 roku miało miejsce nasilenie ataków kierowanych przez Liban, sojusznika Hamasu, na izraelską infrastrukturę rządową i sektor prywatny. Zgodnie z informacjami pozyskanymi z platformy CyberKnow, bezpośrednio po 7 października w atakach w cyberprzestrzeni uczestniczyło 58 grup: 10 popierających Izrael, 48 – Palestynę. Cyberprzestępcy winią Izrael o eskalację konfliktu palestyńsko-izraelskiego i oskarżają o udzielanie poparcia dla Ukrainy i NATO.

Należy zauważyć, że techniki wykorzystane przez Federację Rosyjską przeciwko Ukrainie bezpośrednio poprzedzające i towarzyszące pierwszym tygodniom wojny po 24 lutego 2022 roku w wojnie na Bliskim Wschodzie są mniej skuteczne, nauczeni bowiem doświadczeniem Ukrainy eksperci z zakresu cyberbezpieczeństwa przygotowani byli na potencjalne zagrożenia w tej sferze, skutecznie im przeciwdziałając. W wojnie izraelsko-palestyńskiej, porównując wachlarz instrumentów stosowanych na Ukrainie w 2022 roku, użytkowane są podstawowe metody cyberataków o zdecydowanie mniejszym spektrum oddziaływania, tj. DoS/DDos[1], propaganda i dezinformacja oraz cyberszpiegostwo.

DoS/DDoS

Podobnie jak w przypadku operacji podjętych wobec Ukrainy, w pierwszych dniach konfrontacji palestyńsko-izraelskiej zaatakowano strony rządowe Izraela, portale serwisów informacyjnych, instytucji finansowych, infrastrukturę telekomunikacyjną i energetyczną. Podjęte ataki miały przede wszystkim na celu manipulację opinią publiczną oraz szerzenie

dezinformacji. W grupie organizacji otwarcie ogłaszających zaangażowanie w konflikt na Bliskim Wschodzie wymienić należy takie grupy hakerskie, jak Anonymous Sudan, KillNet, AnonGhost. Co ciekawe, grupa Killnet grupująca hakerów o prorosyjskich sympatiach, zaangażowana była w cyberataki (DoS/DDoS, dezinformacja) przeprowadzane na instytucje rządowe w kilku państwach podczas inwazji Federacji Rosyjskiej na Ukrainę w 2022 roku. Kolejna grupa o konotacjach prorosyjskich to Anonymous Sudan, deklarująca wsparcie dla Palestyńczyków. Grupa ta była autorem m.in. ataku na stronę dziennika Jerusalem Post.

Firma Group IB specjalizująca się w cyberbezpieczeństwie poinformowała, że grupa hakerów o nazwie AnonGhost shakowała mobilną aplikację wykorzystywaną do wysyłania Izraelczykom ostrzeżeń o atakach rakietowych. Aplikacja, pobrana około milion razów z Google Play Store, wysyła fałszywe komunikaty („śmierć dla Izraela", „nadchodzi bomba atomowa"). Działaniami w cyberprzestrzeni wykazują się również ugrupowania proizraelskie, przeprowadzające własne ataki. Wśród nich największą aktywność uzyskały: Indian Cyber Force, która doprowadziła do shakowania portalu Palestinian National Bank i strony Hamasu.

Regularne ataki przeprowadzane są na połączenia internetowe w Stefie Gazy: według danych przekazanych przez organizację NetBlocks dwa dni po ataku Hamasu nie działały usługi ośmiu głównych dostawców internetu. Informacje o zrywaniu połączeń internetowych opublikowała firma Fusion, jeden z ważniejszych dostawców usług łączności dla Palestyny. Częścią działań hakerskich było odcięcie w Strefie Gazy dostaw energii elektrycznej.

Ataki hakerskie typu DoS/DDos zastosowano wobec organizacji dostarczających pomoc humanitarną dla Izraela i Palestyny. Zgodnie z danymi agencji Reuters skierowano je przeciwko stronie internetowej organizacji medycznej United Hatzalah z Jerozolimy oraz Medical Aid for Palestinians (MAP, Pomoc Medyczna dla Palestyny) działającej w Wielkiej Brytanii.

Propaganda i dezinformacja w Internecie

Propaganda definiowana jako *celowe oddziaływanie na zbiorowości i jednostki zmierzające do pozyskania zwolenników i sojuszników, wpojenia pożądanych przekonań i wywołania określonych dążeń i zachowań*[2] oraz dezinformacja rozumiana jako celowa forma przekazywania informacji w sposób zmanipulowany, wprowadzający w błąd i wywołujący określone konsekwencje w postaci podejmowania przez odbiorcę błędnych decyzji stanowią najprostsze metody cyberataków[3]. Stosowanie tych instrumentów ułatwia powszechny dostęp do social mediów i łatwość publikowania tam materiałów. Zgodnie ze wspomnianym już raportem Microsoft Digital Defense Raport 2023 w samym X (Twitter) w 2022 roku

działało około 16,5 miliona botów, generujących treści w social mediach. Szacuje się, że około 20% wiadomości publikowanych przez boty docierało do prawie 14,4 mln użytkowników. Działania te są obecnie kontynuowane również na terenie Izraela. Unia Europejska zwróciła się do Elona Muska i Marka Zuckerburga w związku z rzekomą dezinformacją dotyczącą ataku Hamasu na Izrael, domagając się zastosowania środków zaradczych przeciwko zagrożeniom dla bezpieczeństwa publicznego wynikającym z zastosowania dezinformacji i propagandy. Strony internetowe, konta w mediach społecznościowych i platformy cyfrowe powiązane z podmiotami izraelskimi i palestyńskimi stały się również celem zniesławiania.

Cyberszpiegostwo

Metoda ta stosowana jest zarówno przez Palestynę, jak i Izrael. Szczególnie aktywna na tym polu jest grupa hakerska Storm-1133 z siedzibą w Gazie, atakująca firmy telekomunikacyjne i energetyczne w Izraelu. Ataki dokonywane są za pośrednictwem social mediów i przeglądarek internetowych. Omijają tradycyjne metody bezpieczeństwa poprzez zastosowanie tzw. Backdoorów[4], wykorzystywanie zaatakowanych systemów i danych. Zgodnie z raportem Microsoft Digital Defense Raport 2023 grupa Storm-1133 tworzy fałszywe profile izraelskich deweloperów i grup HR na LinkedIn. Za ich pośrednictwem rozsyłany jest malware do sektora związanego z obronnością, energetyką i kosmosem (tzw. spear-phishing).

Wnioski

W konflikcie palestyńsko-izraelskim, z którego nową odsłoną mamy do czynienia po 7 października 2023 roku, cyberwojna toczy się równolegle z wojną fizyczną. Należy jednak zauważyć, że cyberataki na tym etapie działań palestyńsko-izraelskich mają minimalny wpływ na ich wynik. Konsekwencjami prowadzonych przez obie strony operacji w cyberprzestrzeni, w odróżnieniu od sytuacji na Ukrainie w 2022 roku, są raczej niewielkie zakłócenia, należy jednak przypuszczać, że w miarę rozwoju wydarzeń zagrożenia cyberbezpieczeństwa będą rosły, co stanowi przyczynek do wydania rekomendacji dla bezpieczeństwa w cybersferze. Eskalacja działań w cyberprzestrzeni, towarzysząca konfliktowi palestyńsko-izraelskiemu, w pierwszej kolejności będzie miała na celu polaryzację nastrojów społecznych, a cybersfera stanowi najefektywniejszy instrumentem w osiągnieciu tego celu. Ze wzrostem nastrojów antyizraelskich mamy już do czynienia, ataki o charakterze antysemickim w Dagestanie, Niemczech, Francji są tego najlepszym przykładem i świadczą o globalizacji zjawiska.

W tym zakresie w kontekście międzynarodowym rekomendacje dotyczą ściślejszej

współpracy w obrębie organizacji, które przeciwdziałają zagrożeniom w cyberprzestrzeni, tj. NATO Cyber Defence Management Authority; Cooperative Cyber Defence Centre of Excellence (CCDCoE), funkcjonujących w ramach Sojuszu Północnoatlantyckiego; European Network and Information Security Agency (ENISA), działających w ramach Unii Europejskiej; Forum of Incident Response and Security Teams (FIRST), organizacji grupujących zespoły CERT (Computer Emergency Response Team) z całego świata. Zacieśnienie współpracy instytucjonalnej umożliwi szybką wymianę potrzebnych informacji pomiędzy państwami, a w dalszej kolejności efektywne reagowanie na kolejne zagrożenia. Współpraca z organizacjami na poziomie międzynarodowym umożliwi również transfer doświadczeń i rozwiązań. Przyczyni się do powstawania ujednoliconego systemu zabezpieczeń, który może gwarantować wysoki poziom ochrony we wszystkich krajach należących do danej organizacji.

Na poziomie krajowym rekomendacje dotyczą efektywnej współpracy organizacji odpowiedzialnych za bezpieczeństwo informatyczne, tj. Ministerstwo Spraw Wewnętrznych i Administracji; Agencji Bezpieczeństwa Wewnętrznego; Ministerstwa Obrony Narodowej; Służby Kontrwywiadu Wojskowego. Wskazane jest również rozszerzenie kompetencji organizacji dedykowanych bezpieczeństwu systemów teleinformatycznych, tj. CERT.GOV.PL, Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe Ministerstwa Obrony Narodowej; CERT-y, działające w ramach operatorów telekomunikacyjnych, chociażby poprzez podjęcie działań przez te organizacje w obszarze całego kraju.

Działania podejmowane w ramach zalecanych rekomendacji miałaby na celu uszczelnienie systemu obiegu informacji, szybką reakcję na zagrożenia zidentyfikowane w cyberprzestrzeni, wzmocnienie bezpieczeństwa sieci lokalnych, podjęcie prewencyjnych rozwiązań odseparowujących, np. ruch DDoS, monitorowanie infrastruktury oraz budowę dobrych praktyk w zakresie współpracy na poziomie międzynarodowym.

---

[1] Ataki z użyciem DoS polegają na atakowaniu ofiary z wielu komputerów jednocześnie. DoS wykorzystuje określone limity przepustowości zasobów sieciowych, takich jak np. infrastruktura umożliwiająca działanie firmowej strony internetowej; atak DDoS zalewa atakowaną stronę żądaniami tak długo, aż nie będzie ona w stanie ich obsłużyć i zawiesi się. Wzmocniony atak łączy metodę zalewania żądaniami synchronizacji ataku DoS i rozproszonego ataku DDoS. Polega na zwiększeniu przepustowości ataku bez znacznego zwiększania zasobów atakującego. Szerzej: Atak DoS;

https://instytutcyber.pl/artykuly/atak-dos/, dostęp: 6.11.2023 r.

[2] https://encyklopedia.pwn.pl/encyklopedia/propaganda.html, dostęp: 9.11.2023 r.

[3] M.J. Manning; H. Romerstein, "Disinformation", Historical Dictionary of American Propaganda, Greenwood, 2004, pp. 82–83.

[4] Backdoor to niewidoczny na pierwszy rzut oka punkt dostępu do programu komputerowego. Ta luka w budowie systemu operacyjnego osłabia mechanizm bezpieczeństwa. Szerzej: Backdoor; https://instytutcyber.pl/encyklopedia/backdoor/, dostęp: 9.11.2023 r.

Grafika: obraz autorstwa Freepik