E-ISSN 2544-9567
ISSN 1230-3801

Zeszyt 167 nr 5/2023, str. 97 - 106

PRZEGLĄD WSPÓŁCZESNYCH ZAGROŻEŃ W CYBERPRZESTRZENI

Grzegorz PILARSKI, *g.pilarski@pracownik.akademia.mil.pl*, ORCID: 0000-0001-9728-2611
Akademia Sztuki Wojennej

DOI 10.5604/01.3001.0054.2998

Streszczenie: Współczesny krajobraz zagrożeń w cyberprzestrzeni jest silnie związany z działalnością człowieka w tym obszarze. Ten rozdział prezentuje spektrum zagrożeń w cyberprzestrzeni oparty na dostępnych źródłach, takich jak raporty z obszaru cyberbezpieczeństwa z ostatnich kilku lat. Na tej podstawie identyfikuje się współczesne krytyczne zagrożenie, które według ekspertów ma największy negatywny wpływ finansowy na ofiary ataków. Używanie tego rodzaju ataków przez podmioty APT (Advanced Persistent Threat) może bezpośrednio wpływać na sytuację polityczną, ekonomiczną państwa lub określonych organizacji. Jednym z potencjalnych rozwiązań tego problemu jest nawiązanie relacji cyberkooperencyjnych w zakresie współpracy między różnymi podmiotami, firmami, instytucjami i państwami. Celem takiej współpracy byłoby zwiększenie efektywności oprogramowania antywirusowego, mechanizmów wykrywania i blokowania ataków ransomware oraz podnoszenie świadomości społeczeństwa na temat metod infekcji, działań prewencyjnych i postępowania w przypadku takich ataków. Wprowadzenie takich relacji cyberkooperencyjnych może przyczynić się do poprawy bezpieczeństwa cyberprzestrzeni oraz zwiększenia odporności na zagrożenia. Wymaga to zaangażowania różnych podmiotów, zarówno na poziomie krajowym, jak i międzynarodowym. Poprawa efektywności oprogramowania antywirusowego, wykrywanie i blokowanie ataków ransomware oraz edukacja cyberspołeczności są kluczowymi elementami skutecznej walki z zagrożeniami w cyberprzestrzeni.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, cybezagrożenia, cyberkooperencja

1. Wstęp

W rozdziale tym autor przyjmując problem badawczy w postaci pytania: które z zagrożeń identyfikowanych przez instytucje zajmujące się cyberbezpieczeństwem uznawane są za krytyczne zagrożenia (najczęstsze i o krytycznych skutkach) dla dowolnych podmiotów korzystających z cyberprzestrzeni w tym dla bezpieczeństwa państwa? zaprezentował wyniki badań związanych z analizą współczesnych zagrożeń w cyberprzestrzeni. Tematyka ta jest obecnie bardzo istotna i ważna dla nas wszystkich. Z uwagi na fakt, że od 2019 roku w wyniku postępującej pandemii COVID-19 aktywność ludzka bardzo zwiększyła się w cyberprzestrzeni co dało przyczynek do wzmożenia i ewolucji określonych zagrożeń w tym obszarze.

Celem niniejszej pracy w pierwszej kolejności jest zaprezentowanie spektrum zagrożeń w cyberprzestrzeni na podstawie dostępnych źródeł w postaci raportów z obszaru cyberbezpieczeństwa z kilku ostatnich lat. W dalszej kolejności bazując na kluczowym zagrożeniu, które w ocenie ekspertów urosło do miana krytycznego zagrożenia jakie nasiliło się w ostatnich kilku latach, przedstawić jego charakterystykę oraz wskazać prawdopodobne następstwa

jakie mogą być zauważalne w wyniku stosowania tego typu zagrożenia przez podmioty wykorzystujące tzw. TTPs (ang. *Tactics Techniques and Procedures*) w tej materii.

Materiał badawczy został opracowany na podstawie dostępnych źródeł, z których na szczególną uwagę zasługuje:

- raport Unii Europejskiej a w zasadzie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa ENISA przedstawiający listę 15 istotnych współcześnie zagrożeń w cyberprzestrzeni;
- raport Europolu – Internet Organised Crime Threat Assessment z 2020 r. przedstawiający ocenę zagrożeń cyberprzestępczości;
- raport M-Trends 2020 opracowany przez ekspertów z Madiant (amerykańskiej firmy zajmującej się bezpieczeństwem cybernetycznym);
- raport firmy F-Secure Attack Landscape 2020.

Ideą autora niniejszej publikacji nie jest straszenie o zagrożeniach jakie możemy zidentyfikować w cyberprzestrzeni, chociaż po części celem artykułu jest ich identyfikacja, tylko uświadomienie o kluczowych zagrożeniach na jakie możemy być narażeni korzystając z cyberprzestrzeni. Jest to w ocenie autora bardzo ważny aspekt ponieważ współcześnie bardzo istotnym zadaniem w zakresie cyberbezpieczeństwa, a może inaczej w zakresie przeciwdziałania cyberprzestępczości, jest podnoszenie świadomości nas wszystkich korzystających na co dzień z cyberprzestrzeni.

2. Przegląd zagrożeń

Analiza przeglądu zagrożeń ukazała, że w czasie trwania pandemii nastąpiło wzmocnienie wszystkich wcześniej znanych problemów dotyczących aktywności w cyberprzestrzeni. Atmosfera niepewności połączona z nagłym przejściem na pracę zdalną była i obecnie w dalszej perspektywie czasowej sprzyja cyberprzestępcom. Złośliwe oprogramowanie, ataki hakerskie i wyłudzanie informacji to najważniejsze cyberzagrożenia według raportu przygotowanego przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ang. European Union Agency for Cybersecurity - ENISA). Zgodnie z przedstawionym raportem wskazano na 15 najważniejszych zagrożeń takich jak[1]:

1. Złośliwe oprogramowanie – to cyberatak polegający na wykorzystaniu szkodliwego oprogramowania. Istnieje wiele różnych rodzajów złośliwego oprogramowania, takich jak oprogramowanie do wydobywania kryptowalut, wirusy, oprogramowanie ransomware, robaki i programy szpiegujące. Główne cele tych rodzajów oprogramowania to kradzież informacji lub tożsamości, szpiegostwo oraz dezorganizacja usług.
2. Ataki przez strony internetowe – stanowią atrakcyjną metodę dla sprawców szkodliwych działań, którzy wykorzystują systemy i usługi online jako wektor ataku. Ten rodzaj ataku obejmuje szeroką powierzchnię, w tym tworzenie szkodliwych adresów URL lub złośliwych skryptów, które mają na celu zwiedzenie użytkownika lub ofiary i przekierowanie ich do niepożądanej witryny lub pobranie złośliwej zawartości. Ataki obejmują również wstrzykiwanie złośliwego kodu do prawdziwych, ale niewystarczająco zabezpieczonych witryn internetowych w celu kradzie-

[1] Zob. szerz. List of top 15 threats ENISA Threat Landscape, ENISA 2020.

ży danych, osiągnięcia zysków finansowych, wykradzenia informacji lub nawet wymuszenia okupu za pomocą oprogramowania typu ransomware.

3. Phishing – to oszukańcza próba kradzieży danych użytkownika, takich jak dane logowania, informacje kredytowe i pieniądze, za pomocą technik inżynierii społecznej. Atak ten najczęściej jest przeprowadzany za pośrednictwem wiadomości e-mail, które wyglądają na pochodzące od zaufanego źródła. Celem jest skłonienie użytkownika do otwarcia złośliwego załącznika lub kliknięcia fałszywego adresu URL.
4. Ataki oparte na aplikacjach sieciowych – złożoność aplikacji internetowych i ich powszechne zastosowanie stwarzają wyzwania związane z zabezpieczaniem ich przed różnymi zagrożeniami. Ataki na usługi i aplikacje sieciowe obejmują m.in. ataki SQL lub ataki cross-site scripting, gdzie sprawcy wykorzystują słabe punkty formularzy lub innych funkcji wejściowych aplikacji internetowych. Pozwala to na przeprowadzanie szkodliwych działań, takich jak przekierowywanie do złośliwych witryn.
5. Spam – to masowe wysyłanie niechcianych wiadomości, które stanowi zagrożenie dla bezpieczeństwa cybernetycznego. Często jest wykorzystywany jako wektor ataku do rozpowszechniania innych zagrożeń lub kradzieży danych osobowych. Otrzymanie spamu umożliwia sprawcom podejmowanie działań mających na celu kradzież danych lub instalację złośliwego oprogramowania.
6. Atak typu DoS (ang. *Denial of Service*) – to celowa blokada komputera poprzez wysyłanie takiej ilości informacji, że nie jest on w stanie ich przetworzyć. Ataki typu DDoS (ang. *Distributed Denial of Service*) są rozproszonymi atakami DoS, które wykorzystują wiele kontrolowanych komputerów do przeciążenia celu.
7. Kradzież tożsamości – polega na nielegalnym wykorzystaniu danych osobowych ofiary w celu podszywania się pod tę osobę i osiągania różnych korzyści m. in. finansowych. Do najczęściej kradzionych danych należą konta, karty kredytowe, adresy, imię i nazwisko, hasła oraz adresy e-mail.
8. Naruszenie bezpieczeństwa danych – to incydent związany z cyberbezpieczeństwem, który polega na nieuprawnionym uzyskaniu dostępu do danych lub części systemu informatycznego, zazwyczaj w celach przestępczych. Tego rodzaju naruszenia mają potencjalnie skutki w postaci utraty lub nieodpowiedniego wykorzystania danych. Często naruszenia bezpieczeństwa danych wynikają również z "błędów ludzkich", które mogą wystąpić podczas konfiguracji i wdrażania usług oraz systemów, powodując niezamierzone narażenie bezpieczeństwa danych.
9. Zagrożenie wewnętrzne – jest to działanie przeprowadzane przez osobę lub grupę osób związane z potencjalną ofiarą lub pracującą dla niej, które może prowadzić do incydentu. Zagrożenia wewnętrzne przyjmują różne formy. Przykładem dobrze znanego zagrożenia wewnętrznego jest współpraca osób z zewnątrz z podmiotami wewnętrznymi w celu uzyskania nieuprawnionego dostępu do zasobów. Osoby z wewnątrz mogą wyrządzić szkody nieumyślnie lub z powodu braku wiedzy. Często mają one zaufanie i posiadają uprawnienia, a także są zaznajomione z zasadami, procesami i procedurami obowiązującymi w organizacji, co utrudnia odróżnienie, czy uzyskanie dostępu do aplikacji, danych i systemów było uprawnione, miało na celu działania przestępcze czy też było wynikiem pomyłki.
10. Botnety – są to zbiory urządzeń podłączonych do Internetu, takich jak komputery, serwery, urządzenia mobilne i urządzenia Internetu rzeczy IoT (ang. *Internet of*

things), które zostały zainfekowane i kontrolowane przez złośliwe oprogramowanie. Użytkownicy często nie są świadomi, że ich systemy zostały zainfekowane przez botnety.

11. Ingerencja fizyczna, uszkodzenie, kradzież i utrata – integralność urządzeń jest niezwykle ważna dla zapewnienia bezpieczeństwa i mobilności technologii, zwłaszcza w przypadku Internetu rzeczy. IoT może poprawiać bezpieczeństwo fizyczne poprzez zastosowanie zaawansowanych i kompleksowych rozwiązań. Jednak wszelka ingerencja fizyczna, uszkodzenie, kradzież lub utrata danych może stanowić poważne zagrożenie dla tych technologii.
12. Zagrożenie wycieku informacji – odnosi się do sytuacji, w której poufne lub chronione informacje są udostępniane osobom nieuprawnionym lub organizacjom zewnętrznym. Może to mieć poważne konsekwencje, takie jak utrata zaufania klientów, naruszenie prywatności, szkody finansowe lub reputacyjne np. w przypadku: niezabezpieczonych sieci komputerowych; działań socjotechnicznych czy też wewnętrznych zagrożeń w organizacji. W celu zabezpieczenia się przed zagrożeniami związanymi z wyciekiem informacji, organizacje powinny wdrożyć odpowiednie środki ochronne, takie jak szyfrowanie danych, zabezpieczanie sieci, zarządzanie uprawnieniami, regularne szkolenia pracowników w zakresie świadomości bezpieczeństwa, monitorowanie działań na sieciach i systemach, oraz reagowanie na incydenty bezpieczeństwa w czasie rzeczywistym.
13. Oprogramowanie typu ransomware – ransomware to złośliwe oprogramowanie, które stało się popularnym narzędziem wykorzystywanym przez przestępców, którzy codziennie dążą do naruszania bezpieczeństwa rządów, firm i osób fizycznych. Atak ransomware polega na zablokowaniu dostępu do danych lub systemu ofiary, a następnie żądaniu okupu za ich przywrócenie. Ofiara ransomware może ponieść poważne straty finansowe oraz utracić cenne dane. Skuteczna walka z ransomware obejmuje konieczność implementacji różnych środków ochronnych, takich jak wzmocnienie zabezpieczeń, edukacja użytkowników oraz współpraca między sektorem publicznym i prywatnym w celu szybkiego reagowania i przeciwdziałania temu zagrożeniu.
14. Szpiegostwo w sieci – jest to zagrożenie i motyw przestępstw, które polega na nielegalnym uzyskiwaniu dostępu do poufnych informacji, zwykle znajdujących się w posiadaniu rządowych organizacji lub innych podmiotów. Celem szpiegostwa w sieci jest m. in. kradzież tajemnic państwowych i handlowych, informacji chronionych prawem własności intelektualnej oraz danych kluczowych dla sektorów strategicznych.
15. Złośliwe wydobywanie kryptowalut (cryptojacking) – to forma cyberataków, w której cyberprzestępcy wykorzystują zasoby komputera lub urządzenia ofiary do nielegalnego wydobywania kryptowalut. Zamiast bezpośrednio atakować dane lub systemy ofiary, cryptojacking koncentruje się na wykorzystaniu mocy obliczeniowej urządzenia w celu wydobywania kryptowalut, takich jak m. in. Bitcoin.

Przedstawiony wykaz zagrożeń jest określonym zbiorem przygotowanym przez ekspertów współpracujących z ENISA, jednakże należy mieć świadomość o tym, że jest to ogólna klasyfikacja nie uwzględniająca różnorodnych metod i technik ataku.

3. Atak ransomware – współczesne krytyczne zagrożenie

W dzisiejszych czasach rozwój technologii i globalnej sieci komputerowej przynosi wiele korzyści, ale niesie również ze sobą liczne krytyczne zagrożenia, które stanowią poważne wyzwania dla naszego społeczeństwa. Zdaniem ekspertów Europolu ransomware[2] jest ciągle czołowym zagrożeniem wśród tych przedstawionych w raporcie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, które powodują duże straty finansowe. Obecnie zauważana jest tendencja świadcząca, że cyberprzestępcy mocniej naciskają na płacenie okupów. Przykładem może być Szkocka Agencja Ochrony Środowiska (ang. Scottish Environment Protection Agency - SEPA), która odmówiła zapłacenia okupu cyberprzestępcom, a w odpowiedzi hakerzy opublikowali 4 tyś. skradzionych plików w postaci umów, dokumentów strategicznych czy też baz danych. Także eksperci Mandriant potwierdzają w swoim raporcie M-Trends 2021 wskazują tendencję rozwojową ataków typu ransomware. Zgodnie z barometrem cyberbezpieczeństwa KPMG International w 2020 roku największe ryzyko dla organizacji stanowiły kampanie ransomwarowe oraz zaawansowane ukierunkowane ataki APT. Państwa, w których najwięcej zidentyfikowano ofiar tego typu ataków to Stany Zjednoczone, Kanada, Europa zachodnia. W raporcie firmy ESSET z 2019 r. nawet Polska znalazła się na trzeciej pozycji jako państwo, w którym organizacje poniosły straty finansowe w wyniku ataków ransomware przy wykorzystaniu trojana Ryuk. Ransomware jest jednym z najbardziej kosztownych zagrożeń dla biznesu i bezpieczeństwa podmiotów państwowych. Tylko w 2019 r. wygenerował globalne straty w wysokości 11,5 miliarda dolarów. Aktualnie ataki ukierunkowane są głównie na przedsiębiorstwa i instytucje publiczne.

Charakterystyka

Pojęcie ransomware to połączenie dwóch słów *ransom* – czyli okup oraz *ware* – software czyli oprogramowanie. Jest to oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych, a następnie żąda od ofiary okup za przywrócenie stanu pierwotnego. Jednym z interesujących aspektów jest fakt, że ataki ransomware mają długą historię sięgającą ponad 30 lat. Po raz pierwszy został zrealizowany w 1989 r. przez dr. Josepha L. Popp'a co ciekawe, który był z wykształcenia biologiem ewolucyjnym. Zastosował on trojan PC Cyborg znany również pod nazwą AIDS[3]. Wirus zliczał liczbę uruchomienia komputera, a gdy ta liczba osiągnęła 90 to ukrywał katalogi i szyfrował lub blokował nazwy plików na dysku C. Podobnie jak jego następcy żądał od ofiary na wydruku komputerowym okupu w celu rozwiązania problemu (koszt 189 USD). Początkowo ransomware koncentrował się na atakach kierowanych na urządzenia konsumenckie poprzez techniki typu scareware[4]. Ponieważ okazało się, że ataki ransomware mogą przynieść duże zyski, powstawały kolejne wersje oprogramowania. Niegdyś cyberprzestępcom wystarczyło

[2] Zob. szerz. 1. Internet Organised Crime Threat Assessment (IOCTA) 2020, Europol 2020.

[3] Trojan PC Cyborg, znany również jako "AIDS Info Disk Trojan" lub po prostu "PC Cyborg", to jeden z pierwszych znanych trojanów, który pojawił się w latach 80. XX wieku. Był to złośliwy program komputerowy rozprzestrzeniany za pomocą dyskietek. Trojan PC Cyborg maskował się jako program oferujący informacje na temat AIDS, które w tamtym czasie było tematem szerokiej dyskusji i zainteresowania społecznego.

[4] Techniki typu scareware są wykorzystywane przez cyberprzestępców w celu zastraszenia użytkowników i nakłonienia ich do podejmowania niepożądanych działań. Obejmują one różnego rodzaju manipulacje i sztuczki, które mają na celu wprowadzenie użytkowników w stan paniki lub niepokoju, aby skłonić ich do podjęcia określonych działań lub zakupu fałszywych produktów, np. poprzez wyświetlanie: fałszywych komunikatów o wirusach; fałszywych reklam antywirusowych, fałszywych komunikatów o blokadzie, fałszywych skanerów systemowych, fałszywych powiadomień o wygranych lub konkursach.

szyfrowanie danych i oczekiwanie na okup. Celem ataków było skierowanie masowych kampanii ransomware wobec pojedynczych konsumentów, dążących do ich infekcji i wymuszenia okupu. Tendencja ta zmieniła się w 2018 r. gdzie można odnotować ataki ransomware w kierunku biznesu. Co było powodem tej zmiany? Z pewnością poprawa wykrywalności tego rodzaju złośliwego oprogramowania przez systemy antywirusowe oraz wysokie koszty realizacji kampanii masowych. Ostatnio ataki ransomware są już bardziej wyrafinowane i wykorzystują techniki, taktyki i procedury znane jako Advanced Persisten Threat - APT. Kiedyś, wystarczyło zaszyfrować dane i czekać na okup, aby poradzić sobie z atakami ransomware. Jednak wraz z rozwojem zagrożeń cybernetycznych, nowym trendem stało się grożenie ujawnieniem skradzionych danych, co można zaobserwować w przypadku SEPA, o czym autor wspomniał wcześniej. Obecnie zdarzają się przypadki jednoczesnego ataku ransomware oraz ataku DDoS strony internetowej lub zasobów informatycznych ofiary. Wydaje się, że to może być nowy kierunek rozwoju tzw. „modelu biznesowego" ransomware. Jednocześnie na podziemnym rynku pojawiły się oferty usługowe pozwalające na wykorzystanie kodów ransomware nawet przez osoby nie mające wiedzy i umiejętności programistycznych. Obecnie można teraz mówić, że ransomware jest usługą, którą można sobie wykupić czyli *ransomware as a service*.

Tendencje rozwojowe

Ten kierunek rozwoju modelu biznesowego ransomware daje duże możliwości dla grup cyberprzestępczych, które poprzez ich specyfikę działania określa się jako zaawansowane trwałe zagrożenie (ang. Advanced Persistent Threat – APT). Grupy te stosują zaawansowane technicznie ataki teleinformatyczne na cele polityczne, ekonomiczne, gospodarcze, techniczne i wojskowe. Niejednokrotnie grupy APT utożsamiane są z określonymi państwami, ponieważ istnieją przesłanki ku temu aby stwierdzić, że określone grupy cyberprzestępcze działają na zlecenie określonych państw realizując z góry zaplanowane działania. Przykładami mogą być grupy określane akronimami APT1 utożsamiane z Chinami czy też APT28 czy APT29 utożsamiane z Rosją[5]. Oczywiście wskazanie przynależności do określonych podmiotów atrybucji nie jest proste i wymaga zaawansowanych działań dochodzeniowo-śledczych w cyberprzestrzeni. Sposób działania tychże podmiotów jest zróżnicowany ale można przyjąć uogólnienie i wyróżnić cztery główne fazy cyklu życia ataku realizowanego przez te wyspecjalizowane grupy cyberprzestępcze: rozpoznanie, wstępna infekcja, przejęcie kontroli oraz infiltracja. Przykładowa charakterystyka podmiotu APT może obejmować następujące informacje:

- podejrzewana atrybucja – z reguły grupy tego rodzaju działają na zlecenie różnych organizacji niejednokrotnie utożsamianych z określonym państwem np. APT 1 (Chińska Republika Ludową); APT 28 (Rosja);
- sektor docelowy – uściślenie grupy prawdopodobnych ofiar jest niejednokrotnie pomocne w identyfikacji kto stoi za cyberatakiem np. APT 40 chociaż mają zasięg globalny to koncentrują się na branży turystycznej i firmach informatycznych; APT 38 koncentrują się na instytucjach finansowych na całym świecie;
- opis podmiotu – ta cześć analizy obejmuje opis tzw. TTP, czyli w jaki sposób dany podmiot do tej pory funkcjonował i jak przeprowadzał cyberataki;

[5] Zob. szerz. G. Pilarski, Cyberprzestrzeń : relacje w wojnie hybrydowej, ASzWoj, Warszawa 2020, str. 69.

- powiązane złośliwe oprogramowanie – identyfikacja zbioru złośliwego oprogramowania jest również pomocna w atrybucji, wskazując z dużym prawdopodobieństwem z jakim podmiotem utożsamiany jest analizowany cyberatak;
- wektor ataku – wskazuje najczęściej wybierany środek przeprowadzenia cyberataku np. luka systemu operacyjnego Microsoft Office opisana zgodnie z CVE-2017-11882 przy wykorzystaniu oprogramowania o nazwie POWRUNER – APT 34.

Czym zatem jest APT? Akronim ten według CERT Polska nadawany jest zaawansowanym technicznie grupom, które specjalizują się w przeprowadzaniu ataków teleinformatycznych na cele polityczne, ekonomiczne, techniczne i wojskowe. Głównym zadaniem takich ataków jest wykradanie informacji. Analizując poszczególne elementy tej nazwy można stwierdzić, że nazwa jest adekwatna do zagrożeń jakie mieliśmy, mamy i będziemy mieli w przyszłości. Należy mieć świadomość, że grupy te czasami charakteryzowane są poprzez tzw. TTP czyli taktyki, techniki i procedury działania. Wprowadzając do swojego „portfolio" wykorzystanie modelu biznesowego ransomware as a service, bez wątpienia staną się współcześnie jednym z najpoważniejszych zagrożeń z jakim możemy się spotkać w piątej domenie walki[6], jaką jest cyberprzestrzeń.

Prewencja

Współcześnie ataki ransomware są skoncentrowane na sektorach o szczególnym znaczeniu, takich jak infrastruktura krytyczna, opieka zdrowotna, sektor edukacyjny, dostawcy usług IT oraz instytucje samorządowe. Każda z tych grup jest narażona na zagrożenia. Jak to jest możliwe? Mechanizm jest stosunkowo prosty i może być związany, między innymi, ze zjawiskiem społecznym znanym jako *cyberslacking*. Zjawisko to jest powszechną praktyką, gdzie większość osób codziennie sprawdza prywatną pocztę i korzysta z mediów społecznościowych na swoim komputerze służbowym. Kliknięcie w odpowiednio spreparowany link może spowodować uruchomienie procesu, który będzie skutkował zainfekowaniem infrastruktury teleinformatycznej pracodawcy. Taka sytuacja jest bardzo realna. Jak można temu trendowi przeciwdziałać? Oczywiście, działania prewencyjne w zakresie cyberbezpieczeństwa są ważne, ale czy są wystarczające? Czy poszczególne podmioty są w stanie samodzielnie sobie poradzić? Według autora, należy poprawić relacje cyberkooperencyjne[7] między różnymi podmiotami, firmami, instytucjami i państwami, szczególnie w kontekście ulepszania oprogramowania antywirusowego w celu wykrywania i blokowania ataków ransomware. Takie działania mogą przyczynić się do zmniejszenia tempa tego trendu, przynajmniej w przypadku masowych kampanii ransomware.

[6] NATO uznało cyberprzestrzeń jako piątą domenę walki podczas szczytu w Warszawie, który odbył się w lipcu 2016 roku. W ramach deklaracji z tego szczytu, cyberprzestrzeń została formalnie uznana za obszar operacyjny, obok domen lądowej, morskiej, powietrznej i kosmicznej. Decyzja o uznaniu cyberprzestrzeni jako piątej domeny walki wynikała z narastającego znaczenia zagrożeń związanych z cyberatakami oraz ich potencjalnego wpływu na bezpieczeństwo państw członkowskich NATO. Uznając cyberprzestrzeń za oddzielną domenę, sojusz chciał podkreślić konieczność podjęcia działań zarówno w celu ochrony własnych systemów informatycznych, jak i zdolności do prowadzenia operacji cybernetycznych w obronie i odstraszaniu. Uznanie cyberprzestrzeni za piątą domenę walki było ważnym krokiem dla NATO w dostosowaniu się do współczesnych zagrożeń i rozwijaniu odpowiednich polityk i strategii w obszarze cyberbezpieczeństwa.

[7] Zob. szerzej. G. Pilarski, Cyberprzestrzeń : relacje w wojnie hybrydowej, ASzWoj, Warszawa 2020, str. 36.

Czym zatem jest cyberkooperencja[8]? W związku z tym, że w cyberprzestrzeni odbywa się ciągła walka pozwalająca na osiąganie różnych celów, m. in. takich, jak bycie lepszym, wiodącym czy innowacyjnym. Podmioty w cyberprzestrzeni mają swoje odrębne, rozbieżne cele, w wyniku czego kooperacja nie jest możliwa do osiągnięcia. Decydując się na otwarte określenie swoich celów, podmioty te mają szansę, iż mimo działań konkurencyjnych będą mogły znaleźć sferę wzajemnej współpracy, gdzie platformą bazową będzie cyberprzestrzeń. Takim obszarem z pewnością jest obronność i bezpieczeństwo państwa. Namacalnym przykładem cyberkooperencji jest funkcjonowanie Sojuszu Północnoatlantyckiego w domenie cyberprzestrzeni, gdzie obserwujemy długofalowe działanie z jednej strony kooperacji pomiędzy poszczególnymi państwami w jednych obszarach, zaś z drugiej konkurencji w innych. Kooperacja przeplata się z konkurencją, dlatego autor proponuje posługiwać się pojęciem opisującym różne zależności w cyberprzestrzeni przez użycie pojęcia cyberkooperencji (ang. *cybercoopetition*). Cyberkooperencja to prowadzenie lub przygotowanie aktywności w cyberprzestrzeni przy udziale podmiotów (aktorów), pozostających w jednoczesnych i współzależnych relacjach konkurencji i kooperacji w określonym horyzoncie czasowym. Autor proponuje, przyjmując za podstawowe kryterium skutek oddziaływania w wyniku funkcjonowania cyberkooperencji, posługiwać się następującym podziałem:

- cyberkooperencja pozytywna;
- cyberkooperencja negatywna.

Przyjmując za aksjomat, że funkcjonowanie w cyberprzestrzeni bez znamion cyberprzestępstwa, tj. działanie etyczne, które nie powoduje żadnego negatywnego wpływu na funkcjonowanie innych podmiotów w cyberprzestrzeni, z poszanowaniem życia prywatnego i komunikowania się, należy do rodzaju aktywności, którą można zaliczyć do typu pozytywnego. Natomiast działania zgoła odmienne, nieetyczne i prowadzące do negatywnych efektów będą zakwalifikowywane do aktywności negatywnych.

Przykładem cyberkooperencji pozytywnej może być realizacja cyberedukacji np. w RON. Dzięki edukacji jesteśmy w stanie wpływać na postrzeganie cyberprzestrzeni, jej zalet, ale i zagrożeń z nią związanych chociażby analizowanych w tym artykule ataków ransomware. Istotne w cyberedukacji jest zwiększenia świadomości społeczeństwa na temat zagrożeń związanych z atakami ransomware, metod infekcji, prewencji oraz postępowania po wystąpieniu takiego ataku.

Kolejnym aspektem w zakresie prewencji w stosunku do ataków typu ransomware jest inwestycja w zaawansowane systemy tworzenia kopii zapasowych, które umożliwią względnie szybkie przywracanie sparaliżowanych przez ataki ransomware systemów do działania.

Konkludując, działania podejmowane w tym zakresie na poziomie krajowym nie są wystarczające do skutecznego zwalczania międzynarodowej cyberprzestępczości. Niemniej jednak, świadomość coraz częstszych ataków ransomware rośnie, a postęp mentalny w tym obszarze jest zauważalny zarówno wśród aktorów międzynarodowych, jak i w społeczeństwie. Wkrótce może to doprowadzić do zmiany obecnego stanu rzeczy i próby bycia o krok przed cyberprzestępcami.

[8] Cyberkooperencja jest kontaminacją słów „cyber" – jako obszaru związanego z cyberprzestrzenią oraz „kooperencji", czyli zjawiska, w którym wyróżniamy jednoczesną współpracę (kooperację) połączoną ze współzawodnictwem (konkurencją). Pojęcie to zostało wprowadzone przez G. Pilarskiego w monografii pt. Cyberkooperencja, MP Know-How, Warszawa 2019.

4. Podsumowanie

W niniejszym artykule autor dokonał przeglądu współczesnych zagrożeń w cyberprzestrzeni, gdzie w opinii ekspertów obecnie krytycznym rodzajem zagrożenia dla dowolnych podmiotów korzystających z cyberprzestrzeni w tym dla bezpieczeństwa państwa są ataki typu ransomware. Ataki te są o tyle niebezpieczne, że ich działanie ukierunkowane głównie na przedsiębiorstwa i instytucje publiczne powodują niejednokrotnie ich paraliż i są źródłem bardzo dużych strat finansowych i wizerunkowych. Na przełomie lat tego typu zagrożenie przybierało różne formy począwszy od kampanii ransomware skończywszy na spersonalizowanych wektorach ataku, czy też jako usługa, którą można wykupić w cyberprzestrzeni. Ten ostatni model może być wykorzystywany przez grupy cyberprzestępcze, które poprzez swoją specyfikę działania określa się jako zaawansowane trwałe zagrożenie APT. Jednym z kierunków prewencji w zakresie ataków ransomware jest budowanie relacji cyberkooperencyjnych między różnymi podmiotami, firmami, instytucjami i państwami w zakresie współpracy w działaniach w cyberprzestrzeni. Efektem tych relacji powinno być zwiększenie efektywności oprogramowania antywirusowego, mechanizmów wykrywania i blokowania ataków ransomware oraz podnoszenie świadomości społeczeństwa na temat metod infekcji, działań prewencyjnych i postępowania w przypadku tego typu zagrożeń w cyberprzestrzeni.

Bibliografia

[1] Annual Report 2022, F-Secure 2022.

[2] Attack Landscape H1 2020, F-Secure 2022.

[3] Attack Landscape update, Ransomware 2.0, automated recon, supply chain attacks, and other trending threats, F-Secure 2021.

[4] ENISA Threat Landscape 2021, ENISA 2021.

[5] ENISA Threat Landscape 2022, ENISA 2022.

[6] ENISA Threat Landscape for ransomware attacks, ENISA 2022.

[7] ENISA Threat Landscape for supply chain attacks, ENISA 2021.

[8] ENISA Threat Landscape: transport sector, ENISA 2023.

[9] Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – threat Landscape, ENISA 2022.

[10] G. Pilarski, Cyberprzestrzeń : relacje w wojnie hybrydowej, ASzWoj, Warszawa 2020.

[11] Global Threat Landscape Report A Semiannual Report by FortiGuard Labs, Fortinet 2022.

[12] Internet Organised Crime Threat Assessment (IOCTA) 2019, Europol 2019.

[13] Internet Organised Crime Threat Assessment (IOCTA) 2020, Europol 2020.

[14] Internet Organised Crime Threat Assessment (IOCTA) 2021, Europol 2021.

[15] Krajobraz cyberzagrożeń w 2022 r. oraz prognozy na 2023 r., Tehtris 2022.

[16] List of top 15 threats ENISA Threat Landscape, ENISA 2020.

[17] Main incidents in the EU and worldwide ENISA Threat Landscape, ENISA 2020.

[18] Malware ENISA Threat Landscape, ENISA 2020.

[19] Ransomware Defense Assessment, FireEye Mandiant 2020.

[20] Special report M-TRENDS 2020, FireEye Mandiant 2020.

[21] Special report M-TRENDS 2021, FireEye Mandiant 2021.