Ministerstwo Cyfryzacji
Departament Cyberbezpieczeństwa

AGENCJA WYWIADU
Służba w cieniu dla Polski

TLP:CLEAR

Analiza zagrożeń dla cyberbezpieczeństwa placówek dyplomatycznych RP oraz innych państw NATO w kontekście wybranych ataków hakerskich

Ministerstwo Cyfryzacji:

Agencja Wywiadu:

Wstęp

Niniejsza publikacja ma służyć przybliżeniu tematyki zagrożeń dla cyberbezpieczeństwa placówek dyplomatycznych Rzeczypospolitej Polskiej oraz innych państw NATO w kontekście ostatnich ataków hakerskich.

Po agresji Rosji na Ukrainę Polska oraz reprezentujące ją instytucje coraz częściej padają ofiarą cyberataków. Odpowiedzialność za wiele z nich jest przypisywana grupom hakerskim działającym w bliskim, często wręcz bezpośrednim, powiązaniu z Federacją Rosyjską i stanowią one konsekwencję zaangażowania RP w pomoc Ukraińcom. Szczególnie zagrożonym obszarem jest infrastruktura krytyczna, zwłaszcza sektor transportowy, z uwagi na biegnące przez terytorium RP szlaki służące przekazywaniu międzynarodowego wsparcia dla Ukrainy.

Grupy hakerskie realizujące cyberataki mają różne cele, w tym wykradanie wrażliwych informacji, zakłócanie dostępu do usług oraz szerzenie dezinformacji. Działania te negatywnie wpływają na interesy osób i instytucji nimi dotkniętych. Ich celem są zarówno instytucje rządowe, jak i przedsiębiorstwa, organizacje pozarządowe oraz pojedyncze osoby.

Warto mieć świadomość, jakie są sposoby postępowania tego typu grup działających na różnych kierunkach, dlatego też w niniejszej publikacji przedstawimy przykłady ataków wymierzonych w istotne dla bezpieczeństwa państwowego instytucje rządowe krajów UE i NATO, którymi są placówki dyplomatyczne. Nawiążemy również do ostatnio rozpoznanych operacji ukierunkowanych bezpośrednio na przedstawicielstwa dyplomatyczne Rzeczypospolitej Polskiej. Mamy nadzieję, że publikacja ta dostarczy Państwu wartościowych informacji na temat cyberzagrożeń związanych z działalnością grup hakerskich przeciwko ww. instytucjom.

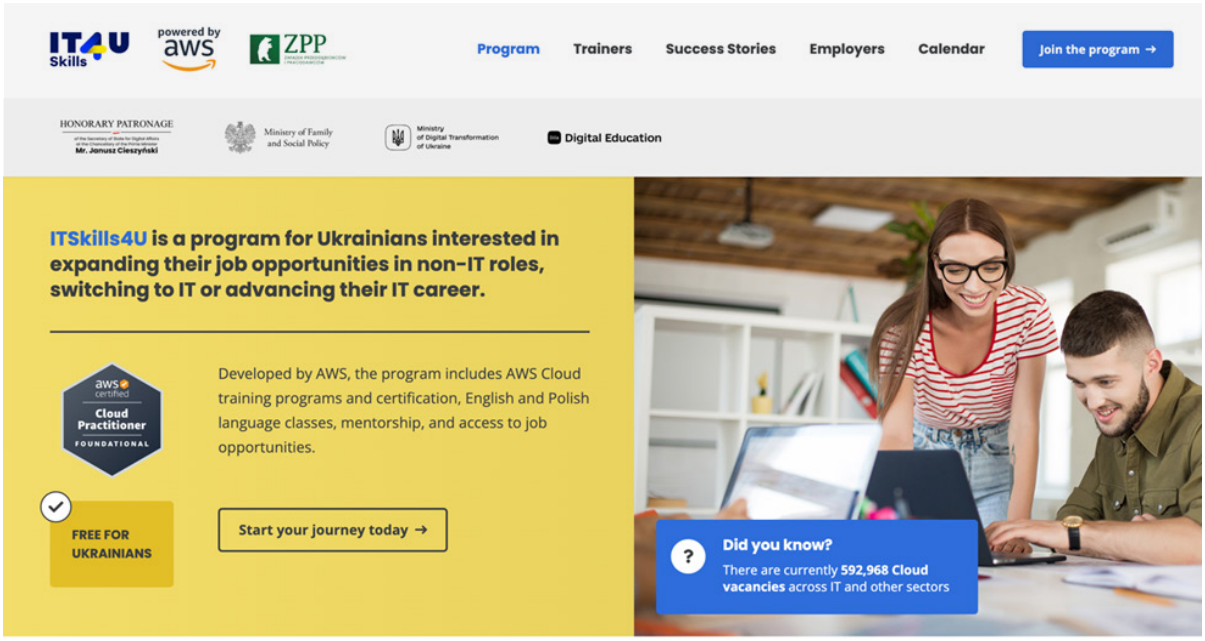
Zapraszamy do lektury!

Trwająca cyberwojna i jej skutki dla państw NATO

Agresja Rosji na Ukrainę na pełną skalę rozpoczęła się 24 lutego 2022 r. wraz z wkroczeniem rosyjskich oddziałów wojskowych na ukraińskie terytorium. Konfrontacja w cyberprzestrzeni trwa jednak co najmniej od 2014 r., tj. nielegalnego zajęcia Krymu oraz wschodnich terenów Ukrainy. W tym czasie powiązani z Moskwą hakerzy zrealizowali wiele operacji wymierzonych we wszystkie obszary funkcjonowania tego państwa, w tym jego system energetyczny czy bankowy. Skala zniszczeń spowodowanych tymi działaniami wielokrotnie szokowała międzynarodową społeczność oraz skutecznie zakłócała życie zwykłych Ukraińców. W 2022 r. cyberataki stanowiły również zapowiedź rosyjskiej agresji, gdyż miały na celu przygotowanie przedpola i paraliż ukraińskiej przestrzeni informacyjnej w najważniejszych, pierwszych godzinach konfliktu.

Wojna za wschodnią granicą RP niezmiennie dowodzi tego, że cyberprzestrzeń jest płaszczyzną strategicznej rywalizacji, wykorzystywaną do realizacji interesów przez nieprzychylne Zachodowi państwa. Jej instrumentalizacja następuje w warunkach zarówno pokoju (jako narzędzie walki hybrydowej), jak i wojny. Obserwacje trwającego konfliktu wskazują na obszary szczególnie narażone na niebezpieczeństwo. Rosyjscy hakerzy dążą do niszczenia ukraińskich sieci wojskowych, cywilnych oraz rządowych i zakłócania w nich przekazu, głównie poprzez ataki destrukcyjne na systemy i bazy danych. Obok tego typu działań operacje hakerskie służą Rosjanom do pozyskiwania informacji wspierających wysiłek wojenny (cyberszpiegostwo).

To, że jak dotąd cyberataki wymierzone w Ukrainę nie doprowadziły do całkowitego paraliżu infrastruktury państwa i sił zbrojnych, nie powinno umniejszać znaczenia ciągłej potrzeby zwiększania bezpieczeństwa w cyberprzestrzeni. Wręcz przeciwnie – to właśnie między innymi dzięki organizacji sił cyberdefensywy oraz międzynarodowej kooperacji w tym obszarze ukraińskie sieci IT okazały się odporne na agresję. Podmioty komercyjne specjalizujące się w usługach chmurowych umożliwiły wyniesienie danych poza obszar działań wojennych i jednocześnie zapewniły ich redundancję z wykorzystaniem globalnej infrastruktury. Istotne było również szybkie nabywanie przez Ukraińców kompetencji potrzebnych do pracy z technologią chmurową. Przykładem pomocy Polski w tym zakresie może być inicjatywa IT Skills 4U jako darmowy program szkoleń i rozwoju kariery dla obywateli Ukrainy.



Ilustracja 1. Inicjatywa ITSkills4U[1]

Jednym z warunków gwarantujących stabilność Sojuszu Północnoatlantyckiego, jego państw członkowskich oraz obywateli zachodniej wspólnoty jest neutralizacja zagrożenia płynącego z wrogich operacji realizowanych w cyberprzestrzeni. Zagwarantowanie tego stanu wymaga stałego monitorowania aktywności grup hakerskich, poznawania ich sposobów działania oraz wykorzystywanych narzędzi. Jest to proces złożony i ciągły w swojej naturze. Agresorzy wciąż rozwijają swoje metody działalności równolegle do postępu technologicznego, który skutkuje cyfryzacją życia – zarówno publicznego, jak i prywatnego – oraz zwiększa tym samym potencjalną płaszczyznę ataku.

Z uwagi na znaczenie niezakłóconego dostępu do zasobów teleinformatycznych problematyka ta powinna stanowić jeden z priorytetów NATO i jego państw członkowskich. Znajduje to odzwierciedlenie w licznych inicjatywach Sojuszu dotyczących budowania potencjału sektora cyberbezpieczeństwa – od umiejętności poszczególnych ekspertów (programy szkoleniowe i edukacyjne), przez ich grupy (ćwiczenia i gry wojenne) do całego bloku. Zwieńczeniem tych zabiegów są wspólne doktryna i strategia, w tym *Cyber Defence Pledge (Zobowiązanie do Obrony Cybernetycznej)*[2]. Dokument został przyjęty w lipcu 2016 r. podczas szczytu NATO w Warszawie. Cyberprzestrzeń uznano wówczas za kolejną – piątą – domenę operacyjną (obok lądu, morza, powietrza i przestrzeni kosmicznej).

[1] Źródło:https://itskills4u.com.ua/ (dostęp: 31.08.2023 r.)
[2] Źródło:https://www.nato.int/cps/en/natohq/official_texts_133177.htm (dostęp: 31.08.2023 r.)

Ilustracja 2. Ćwiczenia Locked Shields 2023[3]

W czasie pokoju państwa sojusznicze NATO skupiają się na odstraszaniu i odpieraniu ataków w cyberprzestrzeni. Istnieje wiele inicjatyw wspierających te działania takich jak chociażby „EU Cyber Diplomacy Toolbox", czyli zestaw narzędzi do dyplomacji dotyczącej działań w cyberprzestrzeni. Inicjatywa ta została stworzona jako wspólna odpowiedź dyplomatyczna UE na szkodliwe działania w cyberprzestrzeni, w tym liczne ataki hakerskie. Wpisuje się to w podejście UE do dyplomacji związanej z działaniami w obszarze cyberbezpieczeństwa w ramach Wspólnej Polityki Zagranicznej i Bezpieczeństwa. Działalność w tym zakresie przyczynia się do zapobiegania konfliktom, redukcji zagrożeń związanych z cyberbezpieczeństwem oraz zwiększenia stabilności w stosunkach międzynarodowych. Reakcja dyplomatyczna UE na złośliwe działania w cyberprzestrzeni jest adekwatna do zakresu, skali, czasu trwania, intensywności, złożoności, wyrafinowania i wpływu każdego cyberataku. Wszystkie wysiłki dyplomatyczne promują bezpieczeństwo i stabilność w cyberprzestrzeni poprzez zacieśnienie współpracy międzynarodowej oraz zmniejszają ryzyko błędnego postrzegania, eskalacji i konfliktów, które mogą wynikać z incydentów ICT"[4].

[3] Źródło:https://news.err.ee/1608955571/sweden-iceland-team-triumphs-at-locked-shields-2023-cyber-defense-exercise (dostęp: 31.08.2023 r.)
[4] Źródło:https://www.cyber-diplomacy-toolbox.com/ (dostęp: 31.08.2023 r.)

To, że wojna toczy się na terytorium Ukrainy, nie oznacza, że zachodnie systemy IT są bezpieczne. Wrogie Zachodowi państwa i organizacje wciąż dążą do wiązania i rozpraszania jego potencjału. Szkodliwe działania w cyberprzestrzeni wymierzone w kraje sojusznicze obejmują m.in. kradzież wrażliwych informacji (uzyskiwanie niepowołanego dostępu do chronionych zasobów sieci), operacje wykorzystujące oprogramowanie szyfrujące (*ransomware*), niszczące (*wiper*) oraz ataki *distributed denial of service* (DDoS)[5] . Często pierwszym podejmowanym działaniem jest wysyłanie niepozornych e-maili phishingowych wyłudzających dane do logowania, które następnie mogą służyć do ustanowienia dostępu do infrastruktury teleinformatycznej. Instytucje i rządy państw sojuszniczych zareagowały na te zagrożenia hybrydowe, organizując liczne inicjatywy mające na celu zwiększanie odporności na tego typu ataki. Z tego względu można uznać, że kluczem wspólnego bezpieczeństwa jest NATO.

Na zakres reakcji państw zachodnich wpływa kwestia atrybucji. Kraje posługujące się narzędziami hakerskimi wykorzystują to, że ustalenie osób i instytucji odpowiedzialnych za daną operację generuje duże trudności. Wielokrotnie nie da się dowieść, że atak hakerski został zrealizowany na polecenie władz konkretnego państwa. Sami winowajcy natomiast nie mają zamiaru odpowiadać za swoje czyny, dlatego też rządy krajów zlecających ataki oficjalnie odcinają się od nich, opierając się na doktrynie wypierania odpowiedzialności *(plausible deniability)*.

Pomimo tego, śledztwa teleinformatyczne potrafią określić pewne elementy dotyczące ataków, np. udowodnić, jaka infrastruktura została wykorzystana do przeprowadzenia operacji, jakich użyto narzędzi, metod działania itp. Na podstawie uzyskanych śladów można zrekonstruować przebieg wydarzeń, w tym wytropić rzeczywistych napastników. Ich działania są prowadzone co do zasady w zorganizowany sposób oraz wykorzystują powtarzające się cechy *(TTPs – Tactics, Techniques, Procedures)* pozwalające na łączenie ich w tzw. klastry aktywności. Następnie podmioty rządowe lub prywatne na podstawie posiadanej wiedzy oraz danych przypisują ww. zbiory cech do konkretnej grupy, która z kolei może zostać powiązana ze strukturami rządowymi obcego państwa lub potraktowana jako organizacja cyberprzestępcza. Zazwyczaj działania hakerów finansowanych przez rządy skupiają się na realizacji strategicznych celów mocodawców, natomiast grupy haktywistyczne zajmują się osiąganiem zysku lub promowaniem swojej ideologii.

[5] Atak polegający na zakłóceniu dostępności usługi poprzez jej przeciążenie

Powyższe ustalenia mogą wywołać reakcję geopolityczną. Należy bowiem zauważyć, że w 2016 r. wojna w cyberprzestrzeni została uznana przez NATO za kolejną domenę operacyjną, a **przeprowadzane ataki hybrydowe oraz cyberataki mogą stanowić podstawę do podjęcia kolektywnej obrony w ramach art. 5 Traktatu północnoatlantyckiego.** W przypadkach czynów mniejszej wagi **sojusznicy dysponują również art. 4 Traktatu, który pozwala na konsultacje, ilekroć któryś z nich uważa, że „integralność terytorialna, niezależność polityczna lub bezpieczeństwo" sojusznika są zagrożone.**

Kraje NATO muszą się skoncentrować na wzmacnianiu swojej cyberodporności i zdolności obronnych. Ich działania obejmują inwestowanie w cyberbezpieczeństwo, rozwijanie możliwości wykrywania ataków i reagowania na nie, wzmacnianie infrastruktury krytycznej oraz współpracę międzynarodową w celu wymiany informacji i wspólnych działań przeciwko cyberzagrożeniom.

Postawa Sojuszu w zakresie odstraszania i obrony opiera się na odpowiednim połączeniu zdolności obrony nuklearnej, konwencjonalnej i przeciwrakietowej, uzupełnionych możliwościami kosmicznymi i cybernetycznymi, co zostało stwierdzone podczas szczytu na Litwie, który odbył się w lipcu 2023 r. „Zgodziliśmy się kontynuować nasze prace nad operacjami wielodomenowymi, możliwymi dzięki transformacji cyfrowej NATO, która dodatkowo zwiększa naszą przewagę wojskową i technologiczną, wzmacniając zdolność Sojuszu do zdecydowanego działania w obszarach lądowych, powietrznych, morskich, cyberprzestrzeni i przestrzeni kosmicznej"[6]

[6] Źródło:https://www.nato.int/cps/en/natohq/official_texts_217320.htm (dostęp: 31.08.2023 r.)

Ilustracja 3. Szczyt NATO w Wilnie[7]

Wroga cyberaktywność rosyjskich grup APT jako rosnące zagrożenie dla sektora rządowego państw NATO

Rosja wykorzystuje operacje w cyberprzestrzeni jako narzędzie walki hybrydowej do osiągnięcia swoich celów strategicznych. Jakkolwiek powiązani z nią hakerzy są zdolni do niszczenia infrastruktury, w tym krytycznej lub zakłócania jej funkcjonowania, tak ich istotnym zadaniem jest wykradanie wrażliwych danych. Nowoczesne technologie oraz właściwie nieograniczony zasięg działania w cyberprzestrzeni sprawiają, że ta forma aktywności może zastępować tradycyjne operacje szpiegowskie. Poszukiwane są wszelkiego rodzaju informacje mogące wesprzeć państwo w doborze celów własnej polityki (zagranicznej, wewnętrznej, wojskowej, gospodarczej) oraz środków do ich realizacji. Wbrew pozorom nie tylko ściśle tajne sieci łączności rządowej mogą stanowić źródło cennych danych. Wiele przydatnych materiałów jest przetwarzanych w sposób zdecentralizowany przez mniejsze, także prywatne, instytucje nieposiadające aż tak wymagających standardów bezpieczeństwa teleinformatycznego. Są to w szczególności wszelkiego rodzaju podwykonawcy, uczestnicy, obserwatorzy czy opiniodawcy. Nawet jeżeli nie przetwarzają informacji, na których najbardziej zależy napastnikowi, ich wiedza może służyć do rekonstrukcji pożądanych danych – a to wszystko przy mniejszym ryzyku operacyjnym i większych szansach powodzenia.

[7] Źródło:https://www.act.nato.int/article/nato-summit-vilnius-2023-day-one/ (dostęp: 31.08.2023 r.)

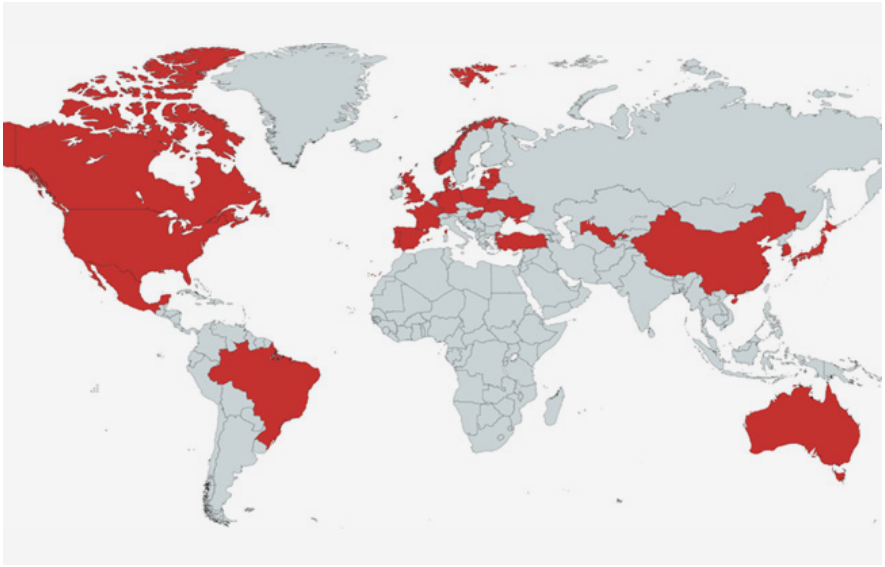
W związku z trwającą w Ukrainie wojną Rosja dąży do pozyskiwania wszelkiego rodzaju informacji nt. skali międzynarodowej pomocy dla broniących się Ukraińców. Szczególnie cenne są dane dotyczące wsparcia materiałowego, w tym defensywnego sprzętu wojskowego. W proces koordynowania organizacji tego typu transportów zaangażowany jest szereg podmiotów. Poza przywódcami państw i rządami udział biorą w nim m.in. struktury odpowiedzialne za utrzymanie sieci telekomunikacyjnych, infrastruktury drogowej i kolejowej, węzłów komunikacyjnych (dworce, lotniska, porty morskie) czy wreszcie poszczególni operatorzy floty pojazdów ciężarowych przewożących towary na wschód. Wszystkie elementy łańcucha dostaw mogą paść ofiarą ataku hakerskiego, zaś napastnicy – pozyskać wartościowe dane. W obliczu tego zagrożenia podstawowym zadaniem instytucji odpowiedzialnych za bezpieczeństwo państwa, w tym w cyberprzestrzeni, jest ochrona kanałów logistycznych oraz infrastruktury krytycznej.

Ataki na placówki dyplomatyczne przypisywane rosyjskim grupom APT

W tak zarysowanym kontekście sytuacyjnym placówki dyplomatyczne stanowią niezwykle ważne ogniwo. Poza dostępem do wrażliwych informacji nt. polityki zagranicznej poszczególnych państw, w tym kooperacji z sojusznikami, wiele z nich bierze udział w pozyskiwaniu środków pomocowych oraz koordynowaniu ich transportu do Ukrainy. Z tego względu stanowią one istotny cel ataków hakerskich. Zdobywane dane mają wartość w zasadzie wyłącznie dla rządów innych, rywalizujących państw, stąd to właśnie powiązane z nimi grupy są najbardziej aktywne w tym zakresie. Skupiają się one głównie na pozyskiwaniu danych oraz infiltracji zainfekowanego środowiska, aby zdobyć możliwie dużą ilość informacji, które mogą okazać się przydatne w planowaniu kolejnych operacji i realizacji interesów.

Ilustracja 4. Przynależność grupy APT29 do rosyjskich służb specjalnych i powiązane nazwy – opracowanie własne na podstawie dostępnych danych

Analitycy Agencji Wywiadu współpracujący z podmiotami w ramach Krajowego Systemu Cyberbezpieczeństwa obserwują liczne próby ataków na placówki dyplomatyczne RP. Jedną z najaktywniejszych, a jednocześnie najbardziej niebezpiecznych organizacji próbujących przełamać ich zabezpieczenia jest grupa określana jako APT29 (inaczej: NOBELIUM, The Dukes, Cozy Bear, BlueBravo).

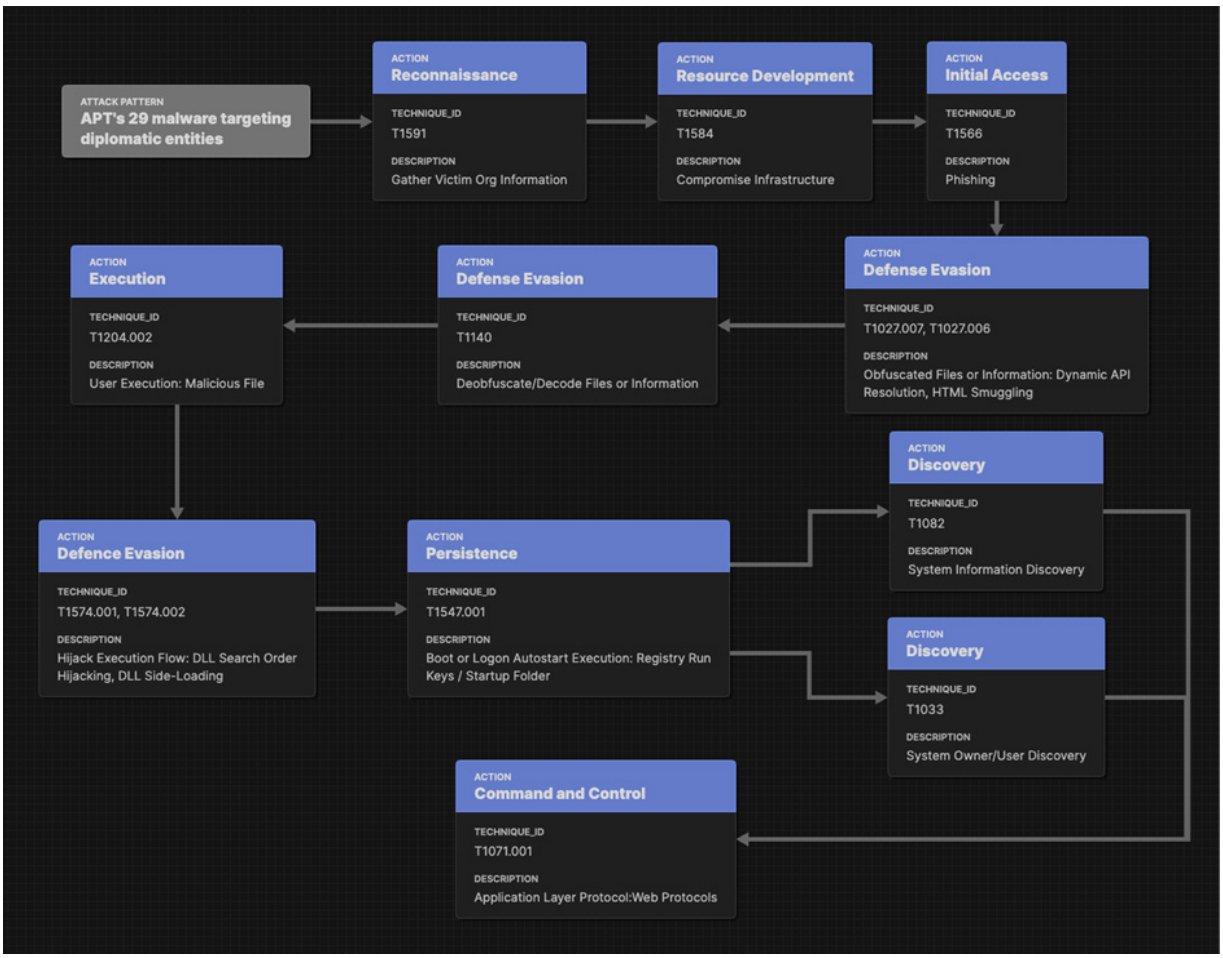


Ilustracja 5. Kraje dotknięte atakami grupy APT29 – opracowanie własne na podstawie dostępnych danych

Jest ona powiązana ze Służbą Wywiadu Zagranicznego Federacji Rosyjskiej (zgodnie z ustaleniami m.in. rządów Stanów Zjednoczonych[8] i Wielkiej Brytanii[9]). Powiązania APT29 z rosyjskim wywiadem świadczą o ukierunkowaniu działań przeciwko krajom NATO – zgodnie z ogólnie przyjętymi praktykami Rosjan.

Operacje prowadzone przez grupę APT29 w dużej mierze rozpoczyna masowa wysyłka e-maili, które mają zachęcić pracowników ambasady do otwarcia załącznika lub hiperłącza prowadzącego do podstawionej strony internetowej. W tym celu hakerzy posługują się różnorodnymi metodami, w tym spoofingiem (ukrywaniem rzeczywistych adresów e-mailowych pod budzącymi zaufanie nazwami). Wykorzystują także uprzednio przejęte skrzynki pocztowe (również należące do przypadkowych osób niezwiązanych z dyplomacją). W treści dystrybuowanych wiadomości pojawiają się natomiast wątki mogące zainteresować osoby pracujące w przedstawicielstwie dyplomatycznym. Są to między innymi zaproszenia na rauty, prośby o umówienie spotkania z ambasadorem lub oferty sprzedaży różnego rodzaju towarów ze zniżką dla dyplomatów.

[8] Źródło: https://www.cisa.gov/news-events/alerts/2021/04/26/fbi-dhs-cisa/join-advisory-russian-foreign-intelligence-service (dostęp: 31.08.2023 r.)
[9] Źródło: https://www.nscs.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf (dostęp: 31.08.2023 r.)



Ilustracja 6. Schemat przedstawiający modus operandi w ostatnich operacjach grupy APT29 – opracowanie własne na podstawie dostępnych danych

Jedna z takich kampanii, która została zidentyfikowana przez analityków ds. cyberbezpieczeństwa, była związana z wykorzystaniem zmodyfikowanego rzeczywistego ogłoszenia sprzedaży samochodu wysłanego przez rzekomego pracownika placówki dyplomatycznej. To, że atakujący przygotował fałszywą ofertę (ilustracja 7.), łudząco podobną do oryginalnej, może sugerować, że miał on dostęp do skrzynki jednego z odbiorców autentycznej wiadomości.

CAR FOR SALE IN KYIV
THE PRICE IS REDUCED!!!

BMW 5 (F10) 2.0 TDI, 7,500 Euros!!

Very good condition, low fuel consumption

More high quality photos are here: [redacted]

Model	**BMW 5, 2.0 TDI (184 HP)**
Year	April 2011
Mileage	266,000 km
Engine	2.0 Diesel
Transmission	Mechanic
Colour	Black, black leather interior
Package	A/C, set of summer and winter tires, ABS/ESP, led lights, cruise control, multifunction steering wheel, CD, electric seats, electric windows, engine control, rain sensor, electrical hand brake, airbags, start-stop system.
Price	7,500 Euros
Custom	NOT CLEARED
Contact	[redacted]

Ilustracja 7. Fałszywa oferta sprzedaży samochodu bazująca na podobnej wysłanej kilka dni wcześniej – opracowanie własne na podstawie dostępnych danych

W ofercie znalazł się link prowadzący do przejętej strony internetowej, która po sprawdzeniu parametrów przeglądarki wywoływała pobieranie szkodliwego pliku. W przypadku niespełnienia warunków założonych przez atakującego (weryfikacja parametru User-Agent) przeglądarka ofiary pobierała nieszkodliwe zdjęcie samochodu. Weryfikacja odwiedzającego stronę ma na celu zablokowanie mechanizmów skanujących takich jak sandbox, pozwalających na automatyczne zabezpieczenie oraz weryfikowanie plików. Ciekawy jest również mechanizm logowania adresów IP przy użyciu dodatkowego pliku PHP umieszczonego na serwerze – prawdopodobnie służy on do rejestrowania skuteczności kampanii oraz ewentualnych analiz pod kątem wykrywania i oznaczania w przyszłości adresacji należących do ekspertów zajmujących się cyberbezpieczeństwem (ilustracja 8.). Analogiczny mechanizm był już obserwowany w przypadku poprzednich kampanii przypisywanych APT29.

Ilustracja 8. Wyciąg kodu strony internetowej wykorzystywanej w trakcie ataku – opracowanie własne

Identyczne mechanizmy wykorzystano w kolejnej kampanii. Atakujący dystrybuował e-maile zawierające spreparowany dokument, który wyglądał na wysłany przez Ministerstwo Spraw Zagranicznych Turcji. Otwarcie linku powodowało przekierowywanie na stronę internetową, która po zweryfikowaniu parametrów przeglądarki oraz zapisaniu adresu IP rozpoczynała pobieranie szkodliwego oprogramowania lub niegroźnego pliku PDF – w zależności od wyników weryfikacji. Sam mechanizm nie jest zaawansowany i jego obejście nie stanowi problemu. Atakujący w poprzednich kampaniach stosował bardziej zaawansowane metody, czyli weryfikację parametrów przeglądarki w sposób niejawny – przy użyciu odpowiednich funkcji w pliku PHP, który następnie zwracał plik szkodliwy lub nie, w zależności od wyniku weryfikacji. W następnych kampaniach napastnik zdecydował się na wykorzystanie techniki *HTML smuggling* (ilustracja 8. i 9. – oznaczenie, gdzie punkt 3. przedstawia funkcję składającą docelowy plik) polegającej na umieszczaniu plików w postaci binarnej bezpośrednio w kodzie strony z wykorzystaniem języka JavaScript. Zabieg ten ma za zadanie obchodzić skanery antywirusowe oraz inne zabezpieczenia, tj. *web proxy*.

Ilustracja 9. Zawartość pliku HTML wykorzystywanego w następnej kampanii – opracowanie własne

Z obserwacji analityków Agencji Wywiadu wynika, że do dystrybuowania szkodliwego oprogramowania wykorzystywane są przejęte strony internetowe. Grupa APT29 nie tworzy tymczasowych domen prawdopodobnie ze względu na to, że tego typu zabieg jest łatwy do wykrycia oraz zablokowania.

Analiza przeprowadzona przez Agencję Wywiadu wykazała, że skompromitowane strony w większości są utrzymywane w ramach infrastruktury jednej firmy świadczącej usługi hostingowe lub powiązanych z nią spółek. W tym przypadku cechą wspólną jest panel zarządzania serwerami (cPanel), który można zaobserwować na każdym serwerze biorącym udział w ataku – jest on instalowany automatycznie przez firmę hostingową na każdym urządzeniu. Prawidłowość ta prowadzi do wniosku sugerującego, że atakujący dysponuje narzędziem umożliwiającym wykorzystanie podatności w usłudze cPanel pozwalającej uzyskać uprzywilejowany dostęp do zasobów.

Domena	cPanel	WordPress	Technologia
totalmassasje.no	❌	✅	HTML+PHP
infomegaware.com.br	✅	?	PHP
cgw.ge	✅	✅	PHP
signitivelogics.com	✅	✅	HTML
literaturaelsalvador.com	✅	✅	HTML
simplesalsamix.com	✅	✅	PHP->HTML
remcolours.com	✅	✅	PHP
resetlocations.com	✅	✅	HTM
Suma:	7	7	

Ilustracja 10. Technologie oraz usługodawcy pojawiający się w trakcie ataków – opracowanie własne

Należy również zauważyć inną cechę łączącą skompromitowane witryny. Większość stron wykorzystywanych w atakach oparta jest na otwartoźródłowych rozwiązaniach CMS *(Content Management System)* – system zarządzania treścią WordPress. W tym miejscu należy pamiętać, że oprócz bazowego kodu silnika WordPress ma bardzo dobrze rozwiniętą funkcjonalność instalowania różnorodnych dodatków lub szablonów. Analiza opublikowanych podatności w silniku WordPress wykazała, że istnieje małe prawdopodobieństwo wykorzystania jej do przejęcia kontroli nad stroną. W przypadku modułów dodatkowych sytuacja wygląda zupełnie inaczej. W związku z otwartością rozwiązania WordPress *(open-source)* oraz tym, że każdy może stworzyć dodatek, należy mieć na uwadze, że ich jakość pozostaje zróżnicowana. Ze względu na powyższe fakty – w przypadku założenia, że wektorem wejściowym dla atakującego jest WordPress – należy przyjąć, że atakowane są podatności w dodatkach (pluginach), a nie sam silnik rozwiązania.

W momencie powstawania publikacji Agencja Wywiadu nie dysponowała zadowalającymi dowodami, mogącymi jednoznacznie wskazać wektor ataku, który jest wykorzystywany do przejmowania stron internetowych służących następnie do dystrybucji szkodliwego oprogramowania.

Więcej informacji na temat narzędzi oraz innych kampanii realizowanych przez grupę APT29 można znaleźć w publikacji przygotowanej przez analityków Służby Kontrwywiadu Wojskowego oraz CERT Polska (CSIRT NASK) pt. Kampania szpiegowska wiązana z rosyjskimi służbami specjalnymi - Baza wiedzy - Portal Gov.pl (www.gov.pl)[10]

Chińskie grupy APT źródłem ataków wymierzonych w państwa NATO

Drugim obok Rosji źródłem zagrożenia dla zachodnich sieci IT są Chiny. Pomimo oficjalnie deklarowanej neutralności w związku z konfliktem w Ukrainie, Pekin jest bardzo zainteresowany osłabieniem Zachodu. Razem z Moskwą dąży on bowiem do zmiany międzynarodowego ładu, który według obu stolic faworyzuje Stany Zjednoczone oraz Europę. W narodzinach tzw. wielobiegunowego świata Rosja i Chiny upatrują możliwości własnego rozwoju. Dodatkowo wielu badaczy wskazuje na to, że zainteresowanie Pekinu reakcją Zachodu na rosyjską inwazję w Ukrainie może być spowodowane próbą przełożenia przez Chińczyków tej sytuacji na potencjalny atak wymierzony w Tajwan[11]. Oprócz walki o wpływy strona chińska dąży do zniwelowania przewagi naukowej i technologicznej krajów zachodnich na wielu polach, w szczególności w zakresie przemysłu oraz nowoczesnych technologii.

Według Pekinu powyższe priorytety mogą być zaspokajane również przy użyciu środków oddziaływania w cyberprzestrzeni. Hakerzy sponsorowani przez państwo mają za zadanie pozyskiwanie informacji – zarówno politycznych, jak i obejmujących tajemnice przedsiębiorstw, patenty i innego rodzaju własność intelektualną lub przemysłową. Dane te mają wesprzeć Chiny w rywalizacji na wielu płaszczyznach, zwłaszcza ze Stanami Zjednoczonymi – ale również z Europą – zapewniając im przewagę polityczno-gospodarczą.

[10] https://www.gov.pl/web/baza-wiedzy/kampania-szpiegowska-wiazana-z-rosyjskimi-sluzbami-specjalnymi (dostęp: 31.08.2023 r.)
[11] Źródło: https://www.japantimes.co.jp/news/2023/02/19/asia-pacific/ukraine-war-anniversary-taiwan-comparison/ (dostęp: 31.08.2023 r.)

W publikacji wydanej przez European Union Agency For Cybersecurity (ENISA) oraz CERT-EU w lutym 2023 r.[12] umieszczono ostrzeżenie o wzmożonej aktywności chińskich grup hakerskich APT27, APT30, APT31, Ke3chang, Gallium oraz Mustang Panda. Instytucje wezwały wszystkie europejskie podmioty z sektora publicznego i prywatnego do podjęcia działań w celu zmniejszenia ryzyka narażenia ich na potencjalne ataki w cyberprzestrzeni. Działania grup koncentrują się na kradzieży wrażliwych informacji m.in. poprzez przeprowadzanie kampanii spearphishingowych, w których jest wykorzystywany motyw wojny Rosji z Ukrainą.

Ilustracja 11. Grupa Mustang Panda i powiązane nazwy – opracowanie własne na podstawie dostępnych danych

Mustang Panda (inaczej: EarthPreta, BronzePresident, CamaroDragon) to grupa hakerska, która działa od co najmniej 2017 r. Zajmuje się przede wszystkim kradzieżą danych i szpiegowaniem państw oraz firm z sektora prywatnego. Stosuje zaawansowane narzędzia i techniki takie jak spearphishing lub wykorzystuje podatności w oprogramowaniu. Jej cele obejmują głównie sektory energetyczny, przemysłowy i związany z obronnością. Grupa jest uważana za jedną z bardziej aktywnych i zaawansowanych technicznie w Chinach.

[12] Źródło:https://www.enisa.europa.eu/publications/sustained-activity-by-specific-threat-actors-joint-publication (dostęp: 31.08.2023 r.)

Ilustracja 12. Kraje dotknięte atakami grupy APT Mustang Panda – opracowanie własne na podstawie dostępnych danych

W styczniu 2023 r. specjaliści z firmy ESET wykryli nowy backdoor, którym prawdopodobnie posługuje się grupa Mustang Panda, i nazwali go MQsTTang. Pozwala on na zdalne wykonywanie poleceń na urządzeniu oraz wykradanie wprowadzanych danych *(keylogger)*. Jest wykorzystywany w ramach kampanii spearphishingowej wymierzonej w podmioty z Europy, Azji (w tym z Tajwanu) i Australii. Znamienne jest to, że w przypadku Tajwanu wrogie działania zostały skierowane przeciwko jednej z instytucji rządowych, co pozwala sądzić, że – biorąc pod uwagę napięte stosunki z Chinami – to właśnie hakerzy z tego kraju są odpowiedzialni za kampanię grupy APT[13].

Ataki na placówki dyplomatyczne przypisywane chińskim grupom APT

Pomimo zaawansowanych możliwości technicznych prezentowanych przez grupę Mustang Panda wydaje się, że jej aktywność przeciwko Polsce pozostaje na niskim poziomie. Kampanie phishingowe wymierzone w przedstawicielstwa RP są przeprowadzane sporadycznie i zazwyczaj są częścią operacji na większą skalę – przeciw wielu krajom należącym do NATO. Ten stan rzeczy jest prawdopodobnie spowodowany tym, że omawiana grupa APT skupia się na realizowaniu innych, ważniejszych zadań.

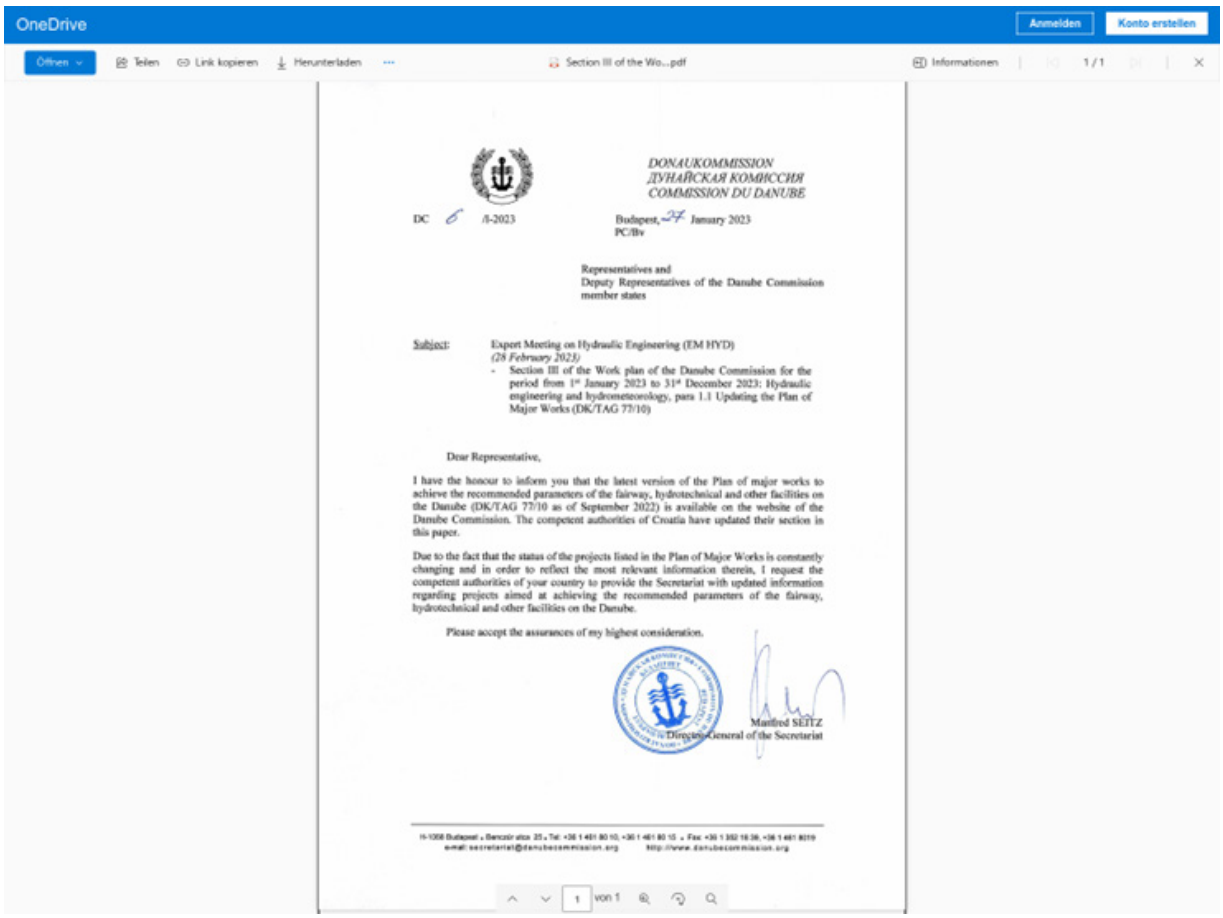
[13] Źródła: securityweek.com, cyberdefence24.pl, enisa.europa.eu, blogs.blackberry.com (dostęp: 31.08.2023 r.)

Jedna z kampanii przypisywanych Mustang Pandzie, której celem były również polskie przedstawicielstwa zagraniczne, miała miejsce w lutym 2023 r. Grupa, wykorzystując konta pocztowe założone w usłudze Outlook.com, dystrybuowała wiadomość mającą zachęcić ofiarę do kliknięcia w link oraz pobrania szkodliwego oprogramowania. Jej treść dotyczyła prośby o udzielenie informacji na potrzeby międzynarodowego projektu. Interesujący pozostaje mechanizm użyty do umieszczenia linku w wiadomości – w tym celu napastnik wykorzystał technikę polegającą na ukryciu faktycznego linku pod tekstem. W przypadku tego zabiegu ofiara spotyka się zazwyczaj z informacją „Kliknij TUTAJ", gdzie pod słowem „TUTAJ" znajduje się szkodliwy link.

```
<ahref=3D"https://www.midasconsilium.com/Section III of the Work plan of the
Danube Commission for the period from lS January 2023 to 31st December
2023.zip">https://1drv.ms/b/s!AlnWqYjBbeyVaUey24BS5iYzVmM?e=3DfP4TL5</a>
```

Ilustracja 13. Tag HTML wykorzystany do wstawienia linku – opracowanie własne na podstawie dostępnych danych

W tej kampanii atakujący postanowił wygenerować dwa linki. Pierwszy inicjował pobieranie szkodliwego oprogramowania, natomiast drugi prowadził do nieszkodliwego dokumentu umieszczonego w serwisie świadczącym usługę hostowania plików OneDrive. Zabieg ten został wykorzystany do zabezpieczenia szkodliwego oprogramowania przed zbyt szybkim zdemaskowaniem. Być może przeciwnik liczył na to, że w przypadku przekazywania odnośnika do weryfikacji mniej doświadczony użytkownik zamiast docelowego linku skopiuje wyświetlany tekst prowadzący do nieszkodliwego pliku.

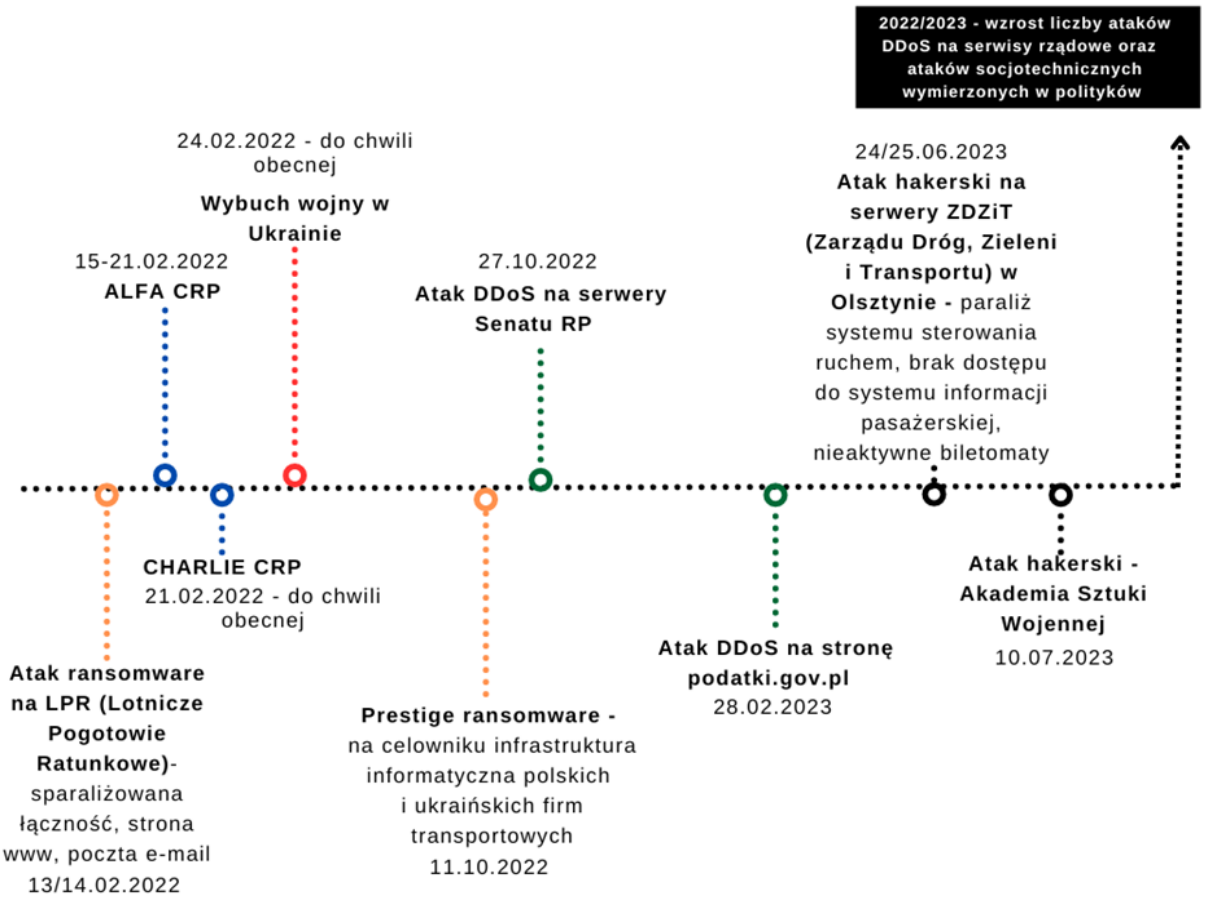


Ilustracja 14. Strona OneDrive zawierająca nieszkodliwy dokument, wyświetlana w przypadku skopiowania linku – opracowanie własne na podstawie dostępnych danych

W przypadku gdy użytkownik kliknął w link, rozpoczynało się pobieranie pliku o nazwie „Section III of the Work plan of the Danube Commission for the period from IS January 2023 to 31st December 2023.zip". Po rozpakowaniu okazywał się on kolejną odsłoną znanego i wykorzystywanego wcześniej szkodliwego oprogramowania o nazwie PlugX. Narzędzie to kwalifikowane jest jako RAT (Remote Access Trojan), tj. oprogramowanie wykorzystywane do przejęcia kontroli nad zainfekowanym komputerem oraz wykradania danych. PlugX stosowany jest również w innych kampaniach Mustang Pandy. Może to sugerować, że jednym z jego głównych celów jest wykradanie danych, które mogą się okazać cennym źródłem informacji na temat relacji biznesowych drugiego państwa lub wykorzystywanych technologii.

Proaktywne działania w celu zapobiegania skutkom ataków na polskie instytucje rządowe, w tym placówki dyplomatyczne

Polska prawdopodobnie pozostanie celem ataków grup sponsorowanych przez obce rządy, w szczególności Rosji. Są one symptomem działań hybrydowych przeciwko państwom wspierającym Ukrainę, wśród których RP odgrywa szczególną rolę. Aktywność tych organizacji może być szczególnie niebezpieczna z uwagi na zbliżające się wybory parlamentarne w Polsce (jesień 2023 r.). Wprowadzenie stopnia alarmowego Charlie CRP i jego utrzymywanie od lutego 2022 r. było odpowiedzią na rosnącą skalę ataków hakerskich i pozwoliło sprawniej reagować na zagrożenia w cyberprzestrzeni.



Ilustracja 15. Wybrane zdarzenia powiązane z wprowadzeniem stopni alarmowych w kraju – opracowanie własne na podstawie dostępnych danych

Aktualnie najistotniejsze jest dalsze zabezpieczanie najważniejszych usług i infrastruktury krytycznej państwa oraz łańcucha dostaw (o czym świadczy przypadek ransomware Prestige z października 2022 r.)[14], również pod kątem oceny praktyk bezpieczeństwa stosowanych przez dostawców oprogramowania. W celu zapewnienia odpowiedniego poziomu zabezpieczenia infrastruktury teleinformatycznej kraju konieczne jest stosowanie odpowiednich standardów takich jak Zero Trust, Security by Design oraz Defense in Depth.

Ministerstwo Cyfryzacji prowadzi liczne działania w zakresie przeciwdziałania zagrożeniom dla cyberbezpieczeństwa RP, m.in.:

- Program Współpracy w Cyberbezpieczeństwie (PWCyber) – kooperacja sektora publicznego i prywatnego. Uczestniczy w nim ponad 30 firm z sektora technologicznego i sukcesywnie dołączają kolejne. W jego ramach organizowane są szkolenia i warsztaty oraz następuje wymiana wiedzy[15];
- przygotowywanie cyklicznych opracowań nt. zagrożeń w cyberprzestrzeni oraz organizowanie szkoleń dot. *security awareness;*
- koordynacja działań na poziomie krajowym, m.in. poprzez dostarczanie narzędzi służących bezpiecznej komunikacji jawnej oraz niejawnej, w tym również organizowanie cyklicznych spotkań nt. stanu bezpieczeństwa;
- udział w licznych inicjatywach międzynarodowych dot. bezpieczeństwa w cyberprzestrzeni takich jak Counter Ransomware Initiative.

Dzięki zdolnościom posiadanym przez CSIRT-y na poziomie krajowych komórek bezpieczeństwa w instytucjach rządowych, wiedzy i doświadczeniu pracujących tam ekspertów oraz narzędziom, którymi dysponują te struktury, jesteśmy w stanie zapewniać bezpieczeństwo infrastrukturze teleinformatycznej oraz natychmiast reagować na nowe zagrożenia. Osłona placówek dyplomatycznych przed incydentami naruszającymi integralność, dostęp do danych i poufność polega na wyposażaniu tych instytucji w narzędzia ochrony systemów teleinformatycznych. Na podstawie analiz dot. funkcjonowania Krajowego Systemu Cyberbezpieczeństwa została zauważona potrzeba utworzenia podmiotu zajmującego się ochroną jednostek podległych lub nadzorowanych przez Ministra Spraw Zagranicznych, jak również samego resortu. Katalog instytucji, nad których cyberbezpieczeństwem mógłby czuwać obejmowałby m.in. polskie przedstawicielstwa na całym świecie, a także podmioty takie jak PISM (Polski Instytut Spraw Międzynarodowych) lub PLSZ (Przychodnia Lekarska

[14] Źródło: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/ (dostęp: 31.08.2023 r.)
[15] Źródło: https://www.gov.pl/web/cyfryzacja/program-wspolpracy-w-cyberbezpieczenstwie-pwcyber--partnerstwo-publiczno-prywatne-na-rzecz-krajowego-systemu-cyberbezpieczenstwa (dostęp: 31.08.2023 r.)

Służby Zagranicznej)[16]. **Podmiot taki jak CSIRT INT mógłby wspierać ww. instytucje w procesie obsługi incydentów, a jego powołanie odegrałoby istotną rolę w podniesieniu cyberbezpieczeństwa RP.**

Planowane jest dalsze rozwijanie krajowej odporności na cyberataki, ze szczególnym uwzględnieniem zabezpieczenia sektora rządowego, w tym placówek dyplomatycznych. Jednymi z głównych celów są wzmacnianie zespołów Cyber Threat Intelligence na poziomie krajowym (w kontekście realizowania działań wyprzedzających) oraz dalszy rozwój kanału wymiany informacji nt. nowych zagrożeń między poszczególnymi instytucjami w ramach Krajowego Systemu Cyberbezpieczeństwa. Dbanie o cyberbezpieczeństwo to działanie zespołowe, dlatego konieczna jest pogłębiona współpraca sektora publicznego i prywatnego, w tym komórek bezpieczeństwa SOC oraz CSIRT na poziomie krajowym, a także dzielenie się posiadanymi informacjami. Realizowany jest bowiem wspólny cel, którym jest zapewnienie bezpieczeństwa RP i jej obywatelom.

Z uwagi na dużą dynamikę działań podejmowanych w cyberprzestrzeni informacje szybko się dezaktualizują. W konsekwencji liczy się szybkie, ale jednocześnie przemyślane podejmowanie działań w odpowiedzi na dany incydent (zwłaszcza przy utrudnionej atrybucji). Istotne jest budowanie zespołów łączonych (modułowo), co w przypadku szczególnie złożonego incydentu pozwoli na współpracę specjalistów z różnych instytucji. Przykładem takich działań są ćwiczenia Locked Shields – w edycji 2023 polski zespół po raz kolejny zajął miejsce na podium, m.in. dzięki kooperacji specjalistów z poszczególnych instytucji sektora rządowego i prywatnego.

Mając na uwadze obecną niestabilną sytuację na Wschodzie oraz liczne ataki hakerskie wymierzone w Polskę, należy wykorzystywać możliwie jak najkrótsze ścieżki decyzyjne, które pozwolą na szybkie działanie w obliczu zagrożenia. Wskazane jest również wzmacnianie aktywnej cyberobrony jako działań odstraszających przez instytucje do tego uprawnione.

[16] Na podstawie danych ze strony: https://www.gov.pl/web/dyplomacja/jednostki-podlegle-nadzorowane (dostęp: 31.08.2023 r.)

Podsumowanie

„My, Szefowie Państw i Rządów Sojuszu Północnoatlantyckiego, związani wspólnymi wartościami wolności jednostki, praw człowieka, demokracji i rządów prawa, zebraliśmy się w Wilnie w związku z toczącą się wojną na kontynencie europejskim, aby potwierdzić naszą trwałą transatlantycką więź, jedność, spójność i solidarność w krytycznym momencie dla naszego bezpieczeństwa oraz międzynarodowego pokoju i stabilności. NATO jest sojuszem obronnym. Jest to jedyne i niezbędne transatlantyckie forum do konsultowania, koordynowania i działania we wszystkich sprawach związanych z naszym indywidualnym i zbiorowym bezpieczeństwem. Potwierdzamy nasze żelazne zobowiązanie do obrony siebie nawzajem i każdego centymetra terytorium Sojuszu przez cały czas, ochrony miliarda naszych obywateli oraz ochrony naszej wolności i demokracji, zgodnie z artykułem 5 traktatu waszyngtońskiego. Będziemy nadal zapewniać naszą zbiorową obronę przed wszystkimi zagrożeniami, bez względu na to, skąd one pochodzą, w oparciu o kompleksowe podejście, aby wypełnić trzy podstawowe zadania NATO: odstraszanie i obronę, zapobieganie kryzysom i zarządzanie kryzysowe oraz wspólne bezpieczeństwo".

Szczyt NATO w Wilnie, 11-12 lipca 2023 r. [17]

Niniejsza publikacja pokrótce charakteryzuje zagrożenia dla placówek dyplomatycznych państw NATO ze strony wrogich grup hakerskich. Nie są to pojedyncze incydenty, lecz działanie ciągłe, wymierzone w różne kraje Sojuszu. Z danych Ministerstwa Cyfryzacji wynika, że w 2022 r. w Polsce liczba zgłoszonych incydentów w porównaniu z 2021 r. wzrosła w sektorze rządowym o ok. 62%, a w sektorze cywilnym o ok. 178%. Liczba ataków typu phishing wzrosła o 61% w 2022 r. Kolejnym wyzwaniem są ataki typu DDoS, które stanowią w ostatnim czasie stałe zagrożenie dla państw NATO, w tym dla Polski. Ataki mają na celu zaburzanie dostępności stron internetowych, usług online i serwerów zarówno w sektorze rządowym jak i prywatnym. W tym aspekcie kluczowe jest dalsze wzmacnianie infrastruktury teleinformatycznej poszczególnych instytucji oraz inwestowanie w narzędzia ochrony anty-DDoS. Znamienne jest także to, że tylko przez pierwsze siedem miesięcy 2023 r. CSIRT NASK obsłużył więcej incydentów niż przez cały 2022 r. Obserwowany jest również wzrost popularności narzędzi typu cybercrime i usług cybercrime-as-a-service (na przykład możliwość kupna gotowego złośliwego oprogramowania, czy też usługi ransomware przez Internet). W tym kontekście prognozowane jest utrzymanie wysokiej presji w cyberprzestrzeni pod kątem realizowanych ataków. Obecnie nie da się stwierdzić, czy nastąpi eskalacja działań.

[17] Źródło: https://www.nato.int/cps/en/natohq/official_texts_217320.htm (dostęp: 31.08.2023 r.)

Możliwe jest jednak, iż w razie spadku zainteresowania Ukrainą jako głównym celem ataków nastąpi przekierowanie większej niż dotychczas części sił i środków na Zachód.

W tym kontekście konieczne jest dalsze podejmowanie działań prewencyjnych w celu zabezpieczenia infrastruktury teleinformatycznej, wzmacnianie współpracy między państwami członkowskimi oraz stosowanie nowoczesnych technologii w zwalczaniu tego typu zagrożeń. Obecnie jednym z głównych zadań jest utrzymanie zdolności obronnej NATO i wzmocnienie współpracy w dziedzinie cyberbezpieczeństwa, aby zapewnić skuteczną ochronę przed atakami hakerskimi, które mogą zagrażać jedności, stabilności i bezpieczeństwu Sojuszu oraz wartościom przyświecającym jego istnieniu.

Jako zaangażowany członek Sojuszu Północnoatlantyckiego RP odgrywa ważną rolę we wspieraniu jedności, spójności i solidarności w regionie. Jej strategiczne położenie geograficzne sprawia, że pełni ona istotną funkcję w obronie wschodniej flanki NATO. Polska uczestniczy w działaniach mających na celu wspieranie stabilności w regionie i przeciwdziałanie zagrożeniom hybrydowym, w tym atakom hakerskim. Skuteczna obrona cyberprzestrzeni wymaga zintegrowanego podejścia i współdziałania zarówno poszczególnych krajów ze sobą, jak i organów rządowych oraz firm prywatnych, tak aby „żelazne zobowiązanie do obrony siebie nawzajem i każdego centymetra terytorium Sojuszu” pozostało naszym wspólnym, nadrzędnym celem.

Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

AGENCJA WYWIADU

Służba w cieniu dla Polski