Anatomia ataków cybernetycznych

Grzegorz Data

Charakter zagrożeń cyfrowych bardzo się zmienił od początku upowszechnienia się informatyzacji. W pierwszych latach istnienia komputerów osobistych hakerzy tworzyli wirusy komputerowe i dokonywali włamań głownie dla zabawy lub sławy. Sporządzali złośliwe oprogramowanie i przełamywali zabezpieczenia komputerowe głównie po to, aby udowodnić, że potrafią to zrobić, albo przekazać jakiś komunikat. Dziś jest to duża gałąź nielegalnego biznesu lub narzędzie do prowadzania ataków na inne państwa. Już w 2011 r. w firma Norton w swym raporcie na temat cyberprzestępczości doniosła, iż we wrześniu 2011 dochód, osiągany z cyberprzestępczości przekroczył dochód osiągany z handlu narkotykami[1]. Jako pierwszy cyberatak na państwo uznaje się zmasowany atak hackerów na instytucje administracji rządowej, media i banki w Estonii. Nic więc dziwnego, że NATO, na szczycie w Warszawie w lipcu 2016 r postanowiło włączyć cyberprzestrzeń jako kolejny obszar działań operacyjnych ze wskazaniem kluczowego elementu cyberprzestrzeni przy prowadzeniu wojny hybrydowej[2]

Definicje

Atak cybernetyczny to wszelkiego rodzaju ofensywny manewr wykorzystywany przez państwa narodowe, jednostki, grupy, społeczeństwo lub organizacje, które atakują komputerowe systemy informacyjne, infrastrukturę, sieci komputerowe i/lub urządzenia komputerowe za pomocą różnych metod złośliwego działania, zwykle pochodzących z anonimowego źródła, który kradnie, zmienia lub niszczy określony cel poprzez włamanie się do systemu podatnego[3].

Z atakami typu **zero–day** mamy do czynienia, gdy informacja o błędach w oprogramowaniu nie jest publikowana, gdyż jej odkrywca sprzedaje ją cyberprzestępcom, a producent dowiaduje się o niej dopiero wtedy, gdy jest ona od pewnego czasu

[1] B. A. Parnell, Cyber crime now bigger than the drugs trade, http://www.theregister.co.uk/2011/09/07/cost_is_more_than_some_drug_trafficking, [6.9.2018]

[2] A. Kozłowski, Szczyt NATO w Warszawie – konsekwencje dla polityki cyberbezpieczeństwa. http://www.cyberdefence24.pl/406632,szczyt-nato-w-warszawie-konsekwencje-dla-polityki-cyberbezpieczenstwa [6.9.2018]

[3] S. D. Applegate, The Principle of Maneuver in Cyber Operations, 2012 4th International Conference on Cyber Conflict 2012, NATO CCD COE Publications, Tallinn

wykorzystywana do ataków. Niestety antywirusy głównie bazujące na różnorakich sygnaturach blokują złośliwy kod jedynie wtedy, gdy jest podobny do innego już znanego.

FUD oznacza całkowicie niewykrywalny/nieusuwalny malware, z jęz. ang. Fully Undetecdable lub Fully Unremovable. Całkowicie niewykrywalny nie odnosi się tylko do nowych i nieznanych wirusów – wystarczy kod wirusa zaszyfrować, a proces odkodowania powierzyć innej aplikacji lub procesowi. Z chwilą pierwszego ataku, który powoduje ujawnienie się malware`u, następuje wykorzystanie zero–day`a i rusza proces zdobycia próbki, analiza i zniesienie statusu FUD, następnie dystrybucja aktualizacji, która obejmuje nowy malware.

Ataki typu **APT** (ang. Advanced Persistent Threats) to złożone, długotrwałe i wielostopniowe działania kierowane przeciwko konkretnym osobom, firmom lub instytucjom.
Advanced (zaawansowane) – ponieważ atakujący wykorzystują różne techniki i metody skutecznego przełamania zabezpieczeń, wykorzystując znane podatności, ale także wynajdując nowe, specjalnie do przeprowadzenia danego ataku,
Persistent (przedłużone, trwałe, uporczywe) – ze względu na formalne zadanie przeprowadzenia skutecznego ataku. Ma on być wykonany tak, aby nie zwrócić niczyjej uwagi, a po uzyskaniu dostępu do jednego systemu ofiary poszerzyć kontrolę o kolejne, w sposób umożliwiający długotrwałą i stałą obecność oraz dozór.
Threat (zagrożenie) – bowiem atakujący to zorganizowana grupa z odpowiednim zapleczem technicznym oraz budżetem. Zagrożenie jest stałe, dopóki atakujący posiada motywację (polityczną, ekonomiczną) do wykradania informacji ofiary. To nie użyte oprogramowanie jest niebezpieczne, a ludzie stojący za nim[4].

Najczęściej opisuje się je jako prowadzone przez atakujących, tygodniami lub miesiącami zbierają dane o pracownikach danej firmy lub organizacji, by po jakimś czasie przystąpić do planowanego ataku. Wykorzystywane przez nich aplikacje i narzędzia są tworzone i użytkowane w sposób ukrywający wykrycie złośliwej aktywności przez ofiarę. Z tego powodu mogą bez przeszkód wykradać informacje przez długi czas. Ataki typu APT różnią się od najczęściej obserwowanych szybkich ataków na instytucje trudnością w wykryciu oraz szerokim zasięgiem. Przeprowadzają je zazwyczaj zorganizowane grupy lub państwa dysponujące znacznymi budżetami oraz czasem pozwalającym na zinfiltrowanie konkretnego celu – firmy bądź instytucji – a następnie precyzyjnego przeprowadzenia ataku, którego celem

[4] R. Bejtlich, What Is APT and What Does It Want? https://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html [6.9.2018]

najczęściej jest kradzież wrażliwych danych lub rzadziej uszkodzenie systemu komputerowego.

Najczęstsze źródła ataków

- Złośliwe oprogramowanie (malware) pobierane na komputer docelowy, które może zrobić prawie wszystko, od kradzieży danych do szyfrowania plików i żądania okupu
- Phishing - tworzony w celu oszukiwania ofiar, aby wyłudzić hasła, informacje z haseł lub podjęcia innych szkodliwych działań. Ukierunkowany na daną osobę lub instytucję nazywany jest spearphisingiem.
- Denial of Service, wyłączają serwery generując fałszywy ruch.
- Man In the Middle, który oszukuje komputer docelowy i łączy się z zagrożoną siecią podsłuchując transmisję bądź zmieniając przesyłane dane (sniffing, spoofing).

Najczęściej występujące problemy z bezpieczeństwem informatycznym ułatwiające atak

- Proste, rzadko zmieniane hasła.
- Otwarte punkty zdalnego dostępu do sieci lub systemu.
- Brak aktualizacji.
- Bannery z informacja o usłudze i wersji.
- Dziurawe skrypty aplikacji webowych (XSS, SQLiniection).
- Uruchomione niepotrzebne usługi.
- Brak monitoringu sieci.
- Niewłaściwe prawa dostępu do zasobów.
- Brak standardów i procedur bezpieczeństwa.
- Błędne zasady na zaporach.

Historia

Za pierwszy „atak hackerski” tygodnik New Science uznaje przejęcie pasma radiowego przez brytyjskiego magika Nevila Maskelynego, podczas pokazu telegrafu radiowego Gugliemo Marconiego w sali The Royal Institution w roku 1903. Marconi chciał zaprezentować swój wynalazek przesyłający bezpieczne i bezprzewodowo wiadomości na długie dystanse. W tym celu ustawił swoje urządzenie nadające w Kornwalii, zaś odbiornik zainstalowano w londyńskim teatrze około 480 km dalej. Zgromadzona publiczność z niecierpliwieniem oczekiwała na pokaz. Jednak przed rozpoczęciem transmisji brytyjski fizyk John Fleming -

współpracownik Marconiego zauważył, że odbiornik zarejestrował pewne wiadomości przesłane alfabetem Morse'a: „szczury, szczury, szczury". Później kilka wersów z Szekspira i parę obelg skierowanych przeciw Marconiemu. Maskelyne chciał udowodnić, iż przesyłanie informacji telegrafem nie jest bezpieczne, można przejąć informację i nadać zmodyfikowaną[5].

Pierwszym opisanym kinetycznym[6] efektem działania komputerowego konia trojańskiego była potężna eksplozja w ZSRR gazociągu transsyberyjskiego. Za eksplozję odpowiedzialne miało być CIA, które do przeprowadzenia sabotażu użyło zmodyfikowanego oprogramowania komputerowego. Stojący na czele Departamentu Sił Powietrznych w administracji Ronalda Reagana Thomas Reed w swoich wspomnieniach – w książce „*At the Abyss: An Insider's History of the Cold War*" opisał akcję, którą, jak twierdził, przeprowadziła CIA. Na podstawie informacji przekazanych przez Władimira Wetrowa, pracownika I Zarządu Głównego KGB, francuskiemu wywiadowi, CIA ustaliła, że Sowieci chcą wykraść oprogramowanie niezbędne do obsługi gazociągu z jednej z kanadyjskich firm. Amerykańscy agenci skłonili więc firmę, która znalazła się na celowniku KGB, do przygotowania zmodyfikowanej wersji oprogramowania, zawierającej tak zwaną logiczną bombę, czyli lukę w kodzie, dzięki której pozornie poprawnie działający program, po określonym czasie miał doprowadzić do katastrofy. Z książki Reeda wynika, że plan udało się w pełni zrealizować. Sowieci wykradli wadliwe oprogramowanie, które następnie zostało użyte do obsługi turbin, zaworów bezpieczeństwa oraz pomp w gazociągu. W momencie uaktywnienia się logicznej bomby oprogramowanie ustawiło pompy, turbiny i zawory tak aby ciśnienie gazu przekroczyło dopuszczalne parametry łączeń i spawów, co doprowadziło do gwałtownego wzrostu ciśnienia, którego efektem była potężna eksplozja. Zarejestrowały ją nawet amerykańskie satelity, a Dowództwo Obrony Północnoamerykańskiej Przestrzeni Powietrznej i Kosmicznej początkowo było przekonane, że w rejonie gazociągu doszło do zdetonowania bomby atomowej, jednakże nie zanotowano impulsu elektromagnetycznego, który by świadczył o wybuchu nuklearnym. Nie było ofiar w ludziach, gdyż gazociąg przebiegał przez niezamieszkaną część Syberii, ale straty spowodowane całą akcją uderzyły w radziecką gospodarkę, dla której bardzo ważne były dewizy uzyskiwane ze sprzedaży gazu do Europy Zachodniej. Po ujawnieniu w 2004 roku przez Reeda szczegółów operacji pojawiły się wątpliwości, czy faktycznie miała ona miejsce. Rosyjskie media dotarły między innymi do

[5] Marks, P., 2011. "Dot-dash-diss: The gentleman hacker's 1903 lulz". New Scientist, 24 12, https://www.newscientist.co

[6] Cyberatak kinetyczny to atak powodujący rzeczywiste fizyczne zniszczenia w infrastrukturze lub narażający życie ludzi.

oficera KGB w stanie spoczynku, który twierdził, że w 1982 roku faktycznie doszło do eksplozji gazociągu na Syberii, ale z powodu błędów konstrukcyjnych[7].

Pierwszy publiczny i motywowany politycznie atak DDoS przeprowadzono już 1994 roku, gdy grupa określająca się jako Zippies postanowiła zaprotestować 5 listopada (na ten dzień przypada angielskie święto zwane dniem Guya Fawkesa) przeciwko nowemu prawu zakazującemu organizacji imprez z mocną muzyką elektroniczną. Zaatakowane rządowe witryny zostały wyłączona na niemal tydzień. Nikt wówczas nie wiedział, w jaki sposób obronić się przed nowym zagrożeniem[8].

Drugiego października 1988 r. Robert Morris student Uniwersytetu w Cornell stworzył program składający się z 99 linii, który miał, w założeniu autora „zmierzyć rozmiar Internetu". Wykorzystywał on 3 luki w oprogramowaniu, hasła dostępowe do serwerów łamał metodą siłowa dysponując słownikiem składającym się jedynie z 400 słów. Po pomyślnym wniknięciu do systemu robak m.in. sprawdzał czy jego kopia jest już uruchomiona w systemie, losowo (algorytm rzutu kostką) wybierał, która z nich ma pozostać w systemie, a która miała ulec samozniszczeniu. Jedna na siedem kopii Morrisa rezygnowała z „rzucania kostką" i działała dalej, niezależnie od innych obecnych wersji. Nie wiadomo, czy był to błąd w kodzie, czy próba zwiększenia szans na przeżycie robaka w systemie, jednak właśnie takie działanie prowadziło do „zatkania" zainfekowanej maszyny, co jest wczesnym atakiem DoS – na wielu komputerach jednocześnie działy dziesiątki kopii Morrisa. W efekcie zainfekowane zostało 6000 komputerów, czyli 10 % z wszystkich podłączonych wówczas do Internetu. Straty szacowano na kwotę pomiędzy 100 tysięcy a 10 milionów dolarów, autor po przyznaniu się do winy został skazany na 3 lata w zawieszeniu, 10 000 dolarów grzywny oraz 400 godzin prac społecznych. Morris obecnie jest profesorem MIT[9].

Najbardziej spektakularne ataki cybernetyczne

Jednym z najpoważniejszych skoordynowanych ataków prowadzonych przez stronę rządowa był atak Moonlight Maze, który rozpoczął się w marcu 1998 r. i trwał ponad dwa lata. W tym okresie rosyjscy hakerzy dokonali serii skoordynowanych ataków w cyberprzestrzeni

[7] The New York Times, William Safire, 2004. "The Farewall Dosier". http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?_r=1

[8] G Świechowski. „Hacktywizm, czyli bunt internautów" http://www.pcworld.pl/news/Hacktywizm-czyli-bunt-internautow,368875.html [6.9.2018]

[9] Kaspersky, Lab, 2013. Kaspersky Daily blog: https://plblog.kaspersky.com/robak-morris-konczy-25-lat/669/ [6.9.2018]

na serwery wielu amerykańskich instytucji rządowych i prywatnych, w tym m.in. Pentagonu, NASA, Departamentu Energii, uniwersytetów oraz instytutów badawczych. Atak ten umożliwił zapoznanie się z informacjami dotyczącymi systemów kierowania rakietami USA. (Niezwykłe jest to, że kod ten jest nadal wykorzystywany w atakach. Zauważono go na wolności w 2011 r., gdy został wykryty w ataku przeprowadzonym na wykonawcę z branży zbrojeniowej, firmę Ruag w Szwajcarii, który został przypisany ugrupowaniu Turla. Następnie, w marcu 2017 r., badacze z Kaspersky Lab wykryli nową próbkę trojana Penquin Turla dostarczoną z systemu w Niemczech[10]) Wydarzenia te częściowo otworzyły oczy amerykańskiej opinii publicznej na zagrożenia płynące z cyberprzestrzeni, dzięki czemu pojawiły się pierwsze projekty legislacji regulującej ten wymiar bezpieczeństwa.

Ciekawym wykorzystaniem cyberprzestrzeni w ramach konfliktu zbrojnego były ataki informatyków sojuszu NATO w marcu 1999 r., podczas operacji w Kosowie, informatycy Sojuszu dokonali wielu ataków w cyberprzestrzeni, których celem było zablokowanie infrastruktury teleinformatycznej Serbii. Co prawda, operacja ta nazwana „Matrix" nie miała większego znaczenia dla operacji NATO, jednak stanowiła historycznie pierwszy przykład wykorzystania cyberprzestrzeni, równolegle z konfliktem zbrojnym[11].

Wiosną 2007 roku po raz pierwszy w historii doszło do zmasowanego cyberataku przeciw suwerennemu państwu. Agresja, która miała wspomóc działania prowadzone przez Rosję w "realu", zapoczątkowała nowy wyścig zbrojeń. Zmasowany atak rozpoczął się po ostrym sporze Tallina z Moskwą wokół usunięcia radzieckiego pomnika z centrum stolicy. Podczas gdy na ulicach estońscy Rosjanie walczyli z policją, polem bitwy elektronicznej stał się estoński Internet. 27 kwietnia o godzinie 22.30 serwis rządu zaczęły bombardować tzw. ataki denial of services (DoS). Dziś wiadomo, że te cyberataki, prowadzone przez wielu niezależnych hakerów, rozpoczęła rosyjska organizacja „Nasi", podporządkowana Kremlowi Od tamtego wieczora fala cyberataków na infrastrukturę informatyczną nasilała się, unieruchamiając strony internetowe parlamentu, ministerstw obrony i sprawiedliwości, partii politycznych, policji, a nawet szkół publicznych. Cyberataki osiągnęły apogeum 9 maja (rosyjski Dzień Zwycięstwa), gdy ich celem stał się też sektor prywatny. dwa największe banki, Hansapank i SEB Ühispank, musiały zawiesić usługi on-line i wstrzymać transakcje zagraniczne. Zamarła też strona największego dziennika „Postimees" Cel został jednak

[10] Kaspersky LAB. Cyberpaleontologia: 20-letni zaawansowany atak, który nadal jest istotny https://www.kaspersky.pl/o-nas/informacje-prasowe/2767/cyberpaleontologia-20-letni-zaawansowany-atak-ktory-nadal-jest-istotny [6.9.2018]

[11] Lakowmy M. „Cyberwojna jako rzeczywistość XXI wieku", Stosunki Międzynarodowe – International Relations • nr 3–4 (t.44) 2011.

spełniony: pokazano, jak bezbronne wobec cyberterroryzmu jest społeczeństwo małego kraju. Prezydent Toomas Hendrik Ilves powiedział potem: „*W obecnych czasach nie potrzeba pocisków, żeby zniszczyć infrastrukturę. Można to zrobić on-line*". Jeszcze bardziej ponuro zabrzmiał komentarz Gadi Evrona, izraelskiego eksperta ds. bezpieczeństwa, który był w tym czasie w Estonii: „*Za pomocą cyberbomby Estonia została niemal zepchnięta do epoki kamiennej*"[12]. Rosja oczywiście zaprzeczyła jakiemukolwiek udziałowi w blokadzie serwerów Estonii[13].

Od roku 2003 do 2007 prowadzona była operacja zmasowanego ataku oraz wykradania danych z serwerów w Stanach Zjednoczonych. W 2004 roku amerykańskie agencje federalne zauważyły serię ataków na sieci departamentów obrony, stanu, energii i bezpieczeństwa wewnętrznego. Atakowane były także serwery firm produkujących na potrzeby departamentu obrony - hakerzy ściągnęli całe terabajty danych. Śledztwo wykazało, że ataki zostały przeprowadzone z terenu Chin, z prowincji Guangdong. Grupie, która je przeprowadziła, nadano kryptonim Titan Rain. O skali ataków świadczy wypowiedź Jima Lewisa, dyrektora Center for Strategic and International Studies, który w 2007 roku stwierdził: „*To katastrofa. To elektroniczne Pearl Harbor*". Skala problemu była tak duża, że doszło do bezprecedensowego kilkudniowego wyłączenia sieci kilku amerykańskich instytucji, w tym. m.in. Departamentu Energetyki. Jednocześnie podjęto próbę uszczelnienia sieci wojskowych. W ramach operacji Buckshot Yankee amerykańscy informatycy rozpoczęli operację usuwania malware'u z wojskowych komputerów. Ich wyczyszczenie zajęło 14 miesięcy. Lista wykradzionych projektów obejmuje kilkadziesiąt systemów m.in. myśliwiec piątej generacji F-35, samolot wielozadaniowy V-22 Osprey, obrona przeciwrakietowa THAAD, obrona przeciwrakietowa Patriot, pocisk kierowany średniego zasięgu powietrze-powietrze AIM-120, dron do prowadzenia rozpoznania Global Hawk. Hakerzy uzyskiwali także dostęp do informacji umożliwiających identyfikację osób, większości wojskowych, adresów e-mail, numerów SSN, numerów kart kredytowych i haseł. "*To jest miliard dolarów przewagi bojowej dla Chin, a oni właśnie uratowali 25 lat badań i rozwoju. To szalone*" - powiedział wysoki urzędnik[14]. Choć powszechnie uważa się, że za całą akcją stała chińska armia, Pekin konsekwentnie temu zaprzecza i nie przyjmuje na siebie odpowiedzialności. W 2007 roku

[12] J. Jalonen „Dni, które wstrząsnęły Estonią" https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html
[13] I. Traynor The Guardian, 2007. Russia accused of unleashing cyberwar to disable Estonia. https://www.theguardian.com/world/2007/may/17/topstories3.russia [6.9.2018]
[14] T. Phillips, The Telegraph, 28 maj 2013, https://www.telegraph.co.uk/news/worldnews/asia/china/10083296/Chinese-hackers-access-sensitive-US-weapons-systems.html [6.9.2018]

kolejne ataki przeprowadzone przez tę samą grupę wzięły za cel między innymi serwery brytyjskiego ministerstwa spraw zagranicznych.[15] [16] [17]

W maju 2013 roku rząd Stanów Zjednoczonych oskarżył Chiny o dokonanie serii ataków hakerskich na najważniejsze amerykańskie systemy obronne i rządowe. Zgodnie z raportem FBI Chiny w sekrecie powołały do życia armię 180 tysięcy cyberszpiegów i cyberwojowników, którzy w ciągu roku przeprowadzają około 90 tysięcy ataków na sieci samego tylko Departamentu Obrony USA.[18]

Wrzesień 2010, pierwszy znany prawdziwy wirus bojowy Stuxnet niszczy około 1000 z 5000 wirówek wzbogacających uran w irańskim zakładzie w Natanz. To jeden z pierwszych odnotowanych cybersabotaży przy użyciu profesjonalnie stworzonego wirusa komputerowego. Badacze stwierdzili: *Siły zbrojne i inne podobne organizacje korzystają z izolowanych sieci wewnętrznych. Stuxnet został stworzony, żeby przeniknąć do takiej sieci*[19]*. To był wyjątkowy wirus.* Stuxnet jest wyjątkowo duży jak na wirusa miał prawie pół megabajta (kilkukrotnie większy od standardowego). Stuxnet atakował komputery z Windowsem, ale jego rzeczywistym celem były programowalne sterowniki przemysłowe firmy Siemens. Wirus pozostawał w uśpieniu, jeżeli nie znalazł takiego sterownika w systemie. Jego zadaniem było doprowadzenie do zmian obrotów wirówek a w rezultacie do przeciążeń i zmęczeniowych zniszczeń w mechanizmach wirówek, mechanizmy kontrolne przy tym były oszukiwane – operator na ekranie był informowany o poprawnej pracy systemu. Najprawdopodobniej z powodu błędu Stuxnet rozprzestrzenił się poza komputery zakładów Natanz i z czasem został wykryty. Przyczynił się także do kolejnych strat poza Iranem, m.in. w Chinach i Indiach. Przy projektowaniu Stuksneta wykorzystano inżynierię społeczną – ktoś musiał wnieść pendrive bądź laptop zarażony malware i uruchomić go w oddzielonej galwanicznie sieci ośrodka wzbogacającego uran[20]. Autorstwo przypisuje się grupie Equation opisanej w dalszej części rozdziału.

---

[15] D. S. Onley, Patience Wait „ Red storm rising", https://gcn.com/articles/2006/08/17/red-storm-rising.aspx
[16] G. Bradley, Hackers Attack Via Chinese Web Sites, Washington Post. 25.8.2005
[17] Ł. Michalik, Pole walki: cyberprzestrzeń. Kiedy haker staje się żołnierzem?, Gadżetomania https://gadzetomania.pl/1471,pole-walki-cyberprzestrzen-kiedy-haker-staje-sie-zolnierzem [6.9.2018]
[18] E. Nakashima, Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies, The Washington Post, https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?utm_term=.611c5e12a4be [6.9.2018]
[19] M. Sikora, Krótka historia cyberwojen, Gadżetomania, https://gadzetomania.pl/4137,krotka-historia-cyberwojen [6.9.2018]
[20] K. Zetter, Odliczając do dnia zero. Stuxnet, czyli prawdziwa historia cyfrowej broni, Helion 2018

CYBER KILL CHAIN

Dla lepszego zrozumienia ataku cybernetycznego na organizację firma Lockheed Martin wprowadziła pojęcie „Cyber Kill Chain" przez analogię do używanej już w wojsku koncepcji ataku. Proces ten określa, iż atak cybernetyczny składa się z 7 faz i tym samym organizacje mogą i powinny mieć kolejne możliwości wykrycia i powstrzymania ataku na każdym etapie. Etapy ataku ukazuje rysunek 1.

Poszczególne fazy ataku to:

Rozpoznanie – badania, identyfikacja i wybór celu, często obejmujące indeksowanie stron internetowych, takich jak materiały konferencyjne oraz listy adresów e–mail, sieci zależności oraz informacje na temat specyficznych technologii, atakujący nie musi nawet dotknąć sieci organizacji, wszystkie dane może pobrać przez wywiad z dostępnych z sieci źródeł;

Uzbrojenie – łączenie koni trojańskich (RAT – Remote Access Trojan) ze złośliwymi programami (ang. exploit) w celu stworzenia możliwej do dostarczenia paczki, często za pomocą automatycznego narzędzia (ang. weaponizer). Często jest to plik pdf, doc, skrypt, który potem zostanie umieszczony na uczęszczanej przez ofiarę witrynie.

Dostarczenie – przekazywanie ładunku do atakowanego środowiska. Najbardziej rozpowszechnione wektory dostawy dla "cyberbroni" w ramach ataków APT to załączniki e-mail (phising, spear–phishing), witryny internetowe (watering hole) i pendrive.

Wykorzystanie – po dostarczeniu niebezpiecznego ładunku do środowiska ofiary jest uruchamiany złośliwy kod (najczęściej ofiara klika na link w mailu, instaluje „dodatkowy driver" by obejrzeć materiał video). Najczęściej wykorzystuje się luki w aplikacjach lub systemie operacyjnym. Ostatnio faza ta składa się z dwóch części uruchamianiu jest najpierw mały program trudny do zidentyfikowania przez antywirusy tzw. Downloader, który to następnie pobiera z sieci właściwy złośliwy kod.

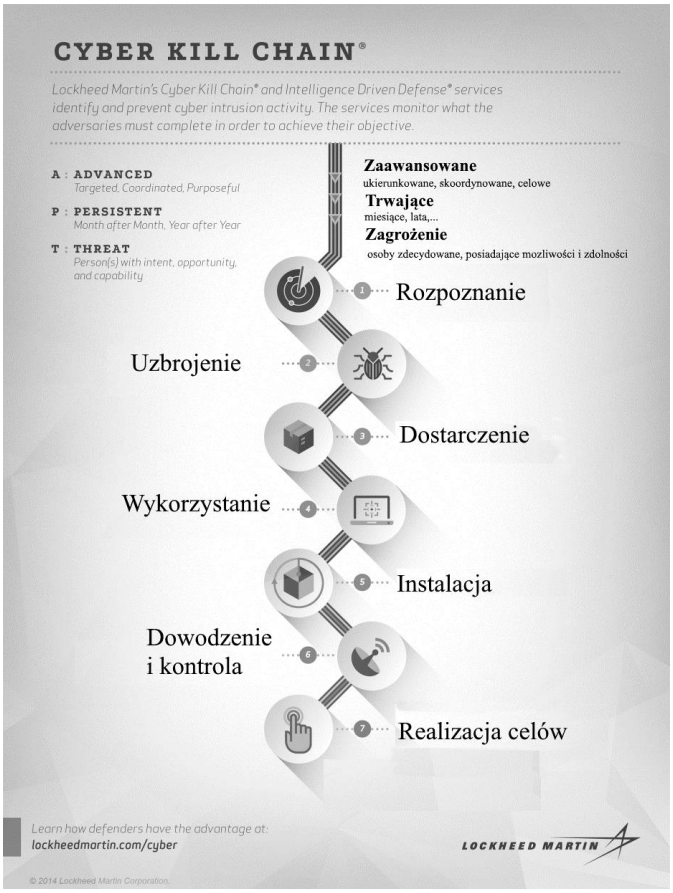
Instalacja – instalacja konia trojańskiego (RAT – Remote Access Trojan) lub tylnych furtek (ang. backdoor) w systemie ofiary pozwala atakującemu na trwałe utrzymanie dostępu do środowiska organizacji.

Dowodzenie i kontrola (ang. *Command and Control* – C2) – zaatakowany system wysyła sygnał do serwera kontrolnego o działaniu malware w celu ustanowienia kanału C2. Kierowanie aplikacją odbywa się ręcznie bądź automatycznie. Po ustanowieniu kanału C2 intruzi otrzymują pełny dostęp do zainfekowanego systemu. Do komunikacji używane są porty

zwykle nie blokowane przez firewalle: http/https, ftp, dns ostatnio także wykorzystywane są do sterowania komunikaty przekazywane przez sieci społecznościowe (Twitter, Facebook).

Realizacja celów – po przejściu przez pierwszych sześciu faz intruzi mogą podjąć działania w celu osiągnięcia zamierzonych celów. Najczęściej jest to wykradzenie danych lub użycie systemu jako stacji przesiadkowej do przesłania emaila lub dojścia do innej sieci lub systemu[21].

Rysunek 1 Rysunek 2. Fazy ataku cybernetycznego. Źródło: opracowanie własne na podstawie Hutchins, et al., 2011[22]



W celu maksymalizacji wykrycia zagrożeń, konieczne jest, aby wszystkie fazy ataku były monitorowane. Matryca możliwych działań, które można podjąć na każdym etapie ataku przedstawiona jest w tabeli 1.

Raport ENISA przedstawiony na tabeli 2 ukazuje typowe ataki rozłożone na poszczególne fazy kill-chain.

[21]Hutchins, E. M., Cloppert, M. & Amin, R., 2011. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, s.l.: Lockheed Martin.
[22] Ibid.

Tabela 1. Sposoby postępowania z atakami. Źródło: (Hutchins, et al., 2011)[23]

Faza	**Detekcja**	**Blokada**	**Zakłócenie**	**Pogorszenie**	**Oszukanie**
Rozpoznanie	Analityka witryny	Firewall			
Uzbrojenie	NIDS	NIPS			
Dostarczenie	Czujny Użytkownik	Filtr proxy	Antywirus	Kolejkowanie	
Wykorzystanie	HIDS	Aktualizacja	DEP		
Instalacja	HIDS	Środowisko chroot	Antywirus		
Dowodzenie i kontrola	NIDS	Firewall	NIPS	Serwer opóźniający (tarpit)	Przekierowanie DNS
Realizacja celów	Audyt logów			QoS	Honeypot

Tabela 2 Ataki cybernetyczne rozłożone na poszczególne fazy, Źródło: opracowanie własne na podstawie (ENISA, 2014)[24].

Rozpoznanie	Uzbrojenie	Dostarczenie	Wykorzystanie	Instalacja	Dowodzenie i kontrola	Realizacja celów
				MALWARE		
	Ataki bazujące na sieci WEB					
			Atak na aplikacje WEB			
DoS					DoS	
					BOTNET	
PHISING						
	SPAM					
				RANSOMWARE		
ZAGROŻENIE WEWNĘTZNE						
						ZNISZCZENIE/KRADZIEŻ/UTRATA
	ZESTAWY EXPLOITÓW					
UTRATA DANYCH						
KRADZIEŻ TOŻSAMOŚCI						
WYCIEK INFORMACJI						
CYBERSZPIEGOSTWO						

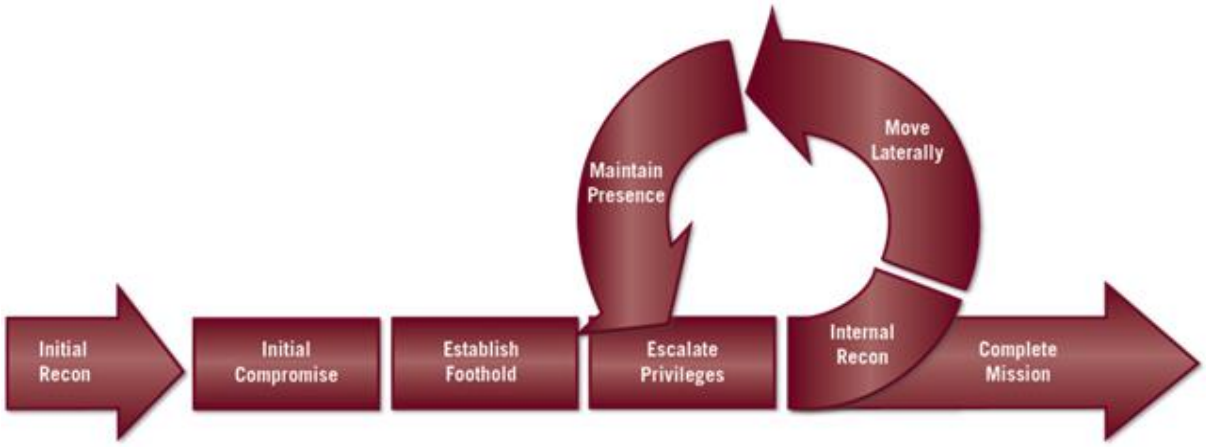
[23] Ibid.
[24] ENISA, Threat Landscape 2014, Heraklion, Grecja European Union Agency for Network and Information Security

Jednym z argumentów przeciw temu modelowi jako narzędzia oceny i zapobiegania zagrożeniom jest to, że wiele z tych kroków odbywa się poza bronioną siecią, co praktycznie uniemożliwia identyfikację lub przeciwdziałanie działaniom na tych etapach. Podobnie, ta metodologia jest oskarżana o skupienie się na "defensywnej" strategii obronnej. Ponadto nie uwzględnia np. osób wewnątrz (insider).

ATTACK LIFE CYCLE firmy Madiant

Firma Madiant (obecnie zakupiona przez FireEye) badając atak chińskiej grupy hackerów (grupie nadano nazwę kodowa APT1 i udowodniono, iż jest to jednostka Chińskiej Armii Ludowo-Wyzwoleńczej nr 61398 zajmujących się włamaniami komputerowymi) opracowała swój model cyberataku nazwany Attack Life Cycle przedstawiony na rysunku 2

Rysunek 2 ATTACK LIFE CYCLE



Cykl ten składa się z następujących faz:

- **rekonesans** – przez osint (otwarte źródła informacji) skanowana jest infrastruktura sieciowa, zdobywane są informacje o kluczowych osobach, maile, profile społecznościowe, zakupy, przetargi, ogłoszenia, wersje systemu operacyjnego, przeglądarek, office, antywirusa, firewall, sprawdzane są wycieki informacji;
- **początkowa kompromitacja** pierwsze przełamanie zabezpieczeń, otrzymanie danych logowania poprzez watering hole (przykład: KNF), phising, spearphising (załączniki zip/rar /binarki/ pdf/office/skrypty);
- **ustanowienie przyczółku** – atakujący utrzymuje się jak najdłużej chroniąc się przed wykryciem, instalacja backdorów, (może trwać to tygodnie a nawet lata);

- **podniesienie uprawnień** - zdobycie uprawnień administratora;
- **wewnętrzny rekonesans** – skanowane są wewnętrzne serwery, sieci, zasoby architektura, sprawdza się słabości, podatności, serwisy i bazy danych;
- **ruch boczne** - rozglądanie się, skanowanie dostępnych podsieci, mostów pomiędzy sieciami współpracujących instytucji ;
- **utrzymanie obecności** (cicha reakcja łańcuchowa) – rozszerzenie obecności na innych maszynach, zwykle aktualizują malware i instalują więcej zaawansowanych backdorów.

ATT&CK

Organizacja MITRE rozszerzyła Cyber Kill Chain skupiając się na zachowaniach behawioralnych i technikach, bazując na wieloletnim doświadczeniu i analizie ataków. Uznano, że o ile wiedza o początkowych etapach jest dobrze opisana, to należy skupić się na działaniach przeciwnika po otrzymaniu dostępu do systemów. Metodykę nazwano ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) Celem badaczy MITRE było rozbicie i klasyfikacja ataków w spójny i przejrzysty sposób, co ułatwi porównywanie i przeciwdziałanie im, aby dowiedzieć się, w jaki sposób atakujący wykorzystał badane sieci i punkty końcowe oraz przeniknął do nich.
ATT&CK bazuje na dużych macierzach, które opisują model działań przeciwnika, które przeciwnik może podjąć w celu złamania zabezpieczeń i pracy w sieci. Macierze pokrywają funkcjonowanie w systemach operacyjnych Linux, Windows oraz MacOS[25].

Najbardziej znane grupy dokonujące ataków

- APT1

Według raportu firmy Mandiant jednostka 61398 ma siedzibę w Szanghaju i zatrudnia tysiące osób biegłych w języku angielskim, programowaniu i zarządzaniu sieciami komputerowymi. Tajna komórka wykradła „od 2006 roku setki terabajtów danych co najmniej od 141 organizacji, reprezentujących różne sektory gospodarki" - czytamy w raporcie[26].

[25] MITRE, Adversarial Tactics, Techniques & Common Knowledge, https://attack.mitre.org/wiki/Main_Page [6.9.2018]
[26] Mandiant, APT1: Exposing One of China's Cyber Espionage Units, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Dokonywano kradzieży informacji różnego rodzaju, od decyzji o fuzjach czy przejęciach przedsiębiorstw po e-maile pracowników na kierowniczych stanowiskach. Autorzy raportu twierdzą, że większość przedsiębiorstw, które padły ofiarą chińskich hakerów, znajduje się w USA, a niektóre także w Kanadzie i Wielkiej Brytanii.

- EQUATION GROUP

Grupa działa od 2001 r. (domeny jakich używa zarejestrowano już od roku 1996). Zdaniem Kaspersky Lab prowadzi ona najbardziej zaawansowane ataki, jakie kiedykolwiek udało się wykryć. Wiadomo, że wykorzystuje wirtualne systemy plików, szkodliwe oprogramowanie Equation Group ukrywa się w formie zaszyfrowanych plików w różnych miejscach rejestru Windows, przez co jest niemożliwe do wykrycia przez oprogramowanie antywirusowe.
Nazwa Equation Group została nadana ze względu na szczególne upodobanie grupy do metod silnego szyfrowania. Do 2015 roku Kaspersky udokumentował 500 infekcji szkodliwym oprogramowaniem grupy w co najmniej 42 krajach, uznając, że rzeczywista liczba może dochodzić do dziesiątek tysięcy.

Moim zdaniem Equation Group ma najbardziej zaawansowane narzędzia hakerskie na świecie. Udostępnili je twórcom *Stuxneta i Flame'a, ale to ich narzędzia. Equation Group to mistrzowie, innym udostępniają jedynie okruchy tego, czym dysponują. Od czasu do czasu pozwalają na zintegrowanie niektórych swoich narzędzi z takim kodem jak Stuxnet i Flame* - mówi Costin Raiu, dyrektor ds. badań i analiz w Kaspersky Lab, jeden z badaczy robaka Stuxnet. Pierwsze informacje wskazujące, że grupa Equation jest powiązana z administracją Stanów Zjednoczonych pojawiły się w 2015 roku, kiedy Kaspersky Lab przeprowadziło analizę złośliwego oprogramowania używanego do ataków[27]. Od samego początku grupa Equation wiązana była z agencją NSA[28], która jest odpowiedzialna za większość operacji USA w cyberprzestrzeni. Informacje dotyczące oprogramowania wykorzystywanego przez grupę hakerów pojawiły się w 2013 roku, wraz upublicznieniem dokumentów przez Edwarda Snowdena.

W 2012 roku specjaliści z moskiewskiej firmy Kaspersky Lab odkryli bardzo skomplikowany złośliwy program o nazwie Flame, który wykradał dane z systemów informatycznych na całym świecie przez ponad pięć lat przed wykryciem. Flame potrafił

[27] Cyberdefence24, Grupa Equation założona przez CIA i NSA, https://www.cyberdefence24.pl/grupa-equation-zalozona-przez-cia-i-nsa [6.9.2018]
[28] National Security Agency – amerykańska wewnętrzna agencja wywiadowcza koordynująca m.in. zadania wywiadu elektronicznego.

aktywować mikrofony w komputerach i nagrywać toczące się w pomieszczeniach rozmowy. Dodatkowo wykonywał regularne zrzuty ekranu i szukał telefonów w pobliżu przy pomocy protokołu Bluetooth[29]. Mikko Hypponen, cieszący się wielkim szacunkiem dyrektor pionu badawczego w firmie F–Secure, nazwa ten przypadek porażką branży antywirusowej i stwierdzi, że on i jego koledzy mogą być „*poza ligą we własnej dyscyplinie*"[30]. Na bazie Flame, uznanego jako najbardziej skomplikowany wirus jaki kiedykolwiek odkryto[31] (wielkość 20 MB czyli około 50 krotnie większy od standardowego malware), powstały inne:

- STUXNET - wycelowany w ściśle określoną instalację komputerową (sterowniki PLC Siemensa wykorzystywane w wirówkach do wzbogacania uranu) skutecznie blokujący kompleks nuklearny w Iranie, korzystał jednocześnie z 5 exploitów[32]. NewYork Times ujawnił, że to Barack Obama wydał nakaz ataku komputerowego na Iran. W efekcie stworzono Stuxnet, który wymknął się z pod kontroli[33].
- DUQU – posiadający kod bardzo zbliżony do Stuxnet'a jednakże mający inne cele – służył jedynie do wykradania danych z tym, że jego ofiary to komputery wykorzystywane w przemyśle. Najprawdopodobniej wykradane przez Duqu dane miały pomóc w przeprowadzaniu kolejnych, bardziej ukierunkowanych ataków[34].
- GAUSS - podobnie jak jego poprzednicy Stuxnet, Duqu i Flame został stworzony w tym samym frameworku i dzieli z nimi część kodu (m.in. funkcje odpowiedzialne za infekcję via USB). potrafi przechwytywać ciastka i hasła z przeglądarek, wykradać pliki konfiguracyjne i wysyła je swoim autorom, infekować dyski USB, kraść dane dostępowe do banków (głównie ze Środkowego Wschodu) oraz dane dostępowe do portali społecznościowych, skrzynek e-mail.

Oprogramowanie i techniki stosowane przez Equation Group

- FANNY zastosowany w Stuxnecie – przejęty z chińskiego ataku Operacja Aurora (dowód na to, iż cyberbroń może być ponownie zastosowana przez ofiarę ataku)

---

[29] D. McElroy, C Williams, Flame: world's most complex computer virus exposed, The Telegraph, 28.05.2012 https://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html [6.9.2018]

[30] T. Simonite, MIT Technology Review, https://www.technologyreview.com/s/428166/the-antivirus-era-is-over/

[31] CrySyS Lab, sKyWIper (a.k.a. Flame a.k.a. Flamer), Budapest University of Technology and Economics, Budapeszt 2012.

[32] R. McMillan, Siemens: Stuxnet worm hit industrial systems. Computerworld, 14.09.2010,

[33] D. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&pagewanted=2&seid=auto&smid=tw-nytimespolitics&pagewanted=all [6.9.2018]

[34] Symantec, 2011. W32.Duqu The precursor to the next Stuxnet, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf [6.9.2018]

- GREYFISH modyfikuje firmware dysków twardych 12 producentów, tak by przetrwać formatowanie, informacje przechowuje zaszyfrowane w rejestrze, lub ukrytych przed skasowaniem fragmentach dysku twardego.
- Ataki przeprowadzano również przez płyty CD rozdawane na konferencjach naukowych.

- APT 28

Znani jako: Pawn Storm, Sednit, Sofacy, Fancy Bear albo Strontium. Specjaliści od bezpieczeństwa teleinformatycznego określają, że jest to rosyjskojęzyczna instytucja państwowa, prawdopodobnie część GRU – wywiadu wojskowego Federacji Rosyjskiej[35].
Główne cele grupy to rządy Ukrainy, Gruzji, państw środkowoeuropejskich, podwykonawcy i instytuty pracujące dla Departamentu Bezpieczeństwa USA, krytycy prezydenta Putina. Głównym celem działalności jest pozyskanie wiedzy oraz operacje dezinformacyjne Stosowanymi narzędziami jest co najmniej 9 podatności wykorzystywanych w exploitach (kilka z nich to „zero day"), używanie innych często następuje w ciągu zaledwie jednego dnia od ogłoszenia Swoje narzędzia rozwijają i utrzymują przez długi czas. Sam malware jest dostosowywany do celu ataku (użycie serwera pocztowego ofiary ataku do wysłania skradzionych danych, Opracowanie ataków odbywa się w sformalizowanym środowisku programistycznym IDE. Na celowniku grupy w roku 2016 była polska instytucja rządowa zaatakowana z użyciem malware „Sourface"/"Coreshell", w tym czasie skuteczny atak został przeprowadzony na MSZ Czech - wiadomości "przynęty" (decoy) były m.in. powiązane z ćwiczeniami "Baltic Host" i zestrzeleniem samolotu MH17 nad Ukrainą. Używane domeny q0v.pl, mail.q0v.pl, poczta.mon.q0v.pl -w pasku przeglądarki wizualnie podobna do gov.pl, standartnevvs.com – bułgarska Sandart News, qov.hu -domena węgierskich instytucji rządowych gov.hu)

- APT 29

Grupa znana jako CozyDuke, CozyBear, SeaDuke albo MiniDionis powiązana z cywilnym wywiadem rosyjskim SWZ FR. Jej główne cele to rządy USA, państw europejskich, osoby oraz instytucje wpływające na politykę państw a szczególnie pozyskiwanie wiedzy i informacji.
Główne cechy charakteryzujące grupę:
- bardzo zaawansowane i specjalizowane ataki oraz dobre i kosztowne wyposażenie,
- kompleksowa i innowacyjna infrastruktura C2,

[35] CrowdStrtike, Who is FANCY BEAR?, https://www.crowdstrike.com/blog/who-is-fancy-bear/ [6.9.2018]

- nacisk na ukrywanie ataku i jego innowacyjność,
- agresywne zachowanie w momencie odkrycia ataku,
- przechodzenie do wykorzystania narzędzi open source lub systemowych (Powershell, Carberp, PAS webshell, Metasploit FireFox plugin),
- używanie przynęt w kampaniach speraphisingowych, sprawy dotyczące dyplomacji, giełdy lokalnych i centralnych instytucji rządowych USA, lub uniwersytetów,
- zaciemnianie ataku, Wykorzystanie popularnych serwisów web: Twitter, GitHub, usługi cloud

- TURLA

Grupa znana jako Snake, Uroburos lub Venomous Bear. Dan Goodin w swym portalu "Ars Technica" opisuje grupę Turla jako „Rosyjskich szpiegów". Przykład działania grupy jest następujący - szkodliwe oprogramowanie Epic przeprowadza profilowanie ofiar. Po wykryciu celu wysokiego szczebla atakujący wykorzystują mechanizm komunikacji satelitarnej, co pomaga im zatrzeć swoje ślady. Podszywa się pod użytkowników legalnie korzystających z transmisji satelitarnej i przechwytuje pakiety wysyłane od ofiar.
Polski ślad w działalności grupy to operacja Red October 2012 – atak trwający 5 lat, tworzący zrzuty konfiguracji przełączników sieciowych, zawartości nośników USB, telefonów komórkowych wraz z odzyskiwaniem skasowanych danych; jednen z plików używanych do ataków nazywał się „Katyn_-_opinia_Rosjan.xls"

- SANDWORM

Inne nazwy grupy: Black Energy Quedagh, VoodooBear albo Telebots. Ich zadaniem są operacje ukierunkowane na Ukrainę, zakłócanie oraz monitorowanie mediów. Główne cele to ukraiński: rząd, media, wojsko, siły graniczne, instytucje finansowe. Grupa najbardziej znana z ataku na sieć energetyczną Ukrainy 23 grudnia 2015- malware BlackEnergy dostarczony w załączniku .XLS w mailu skutkujący atakiem na systemy SCADA i wyczyszczeniem dysków – próbki oprogramowania znaleziono również w USA. Grupa dokonała również rekonesansu przeprowadzanego również w Polsce w instytucjach związanych z infrastrukturą krytyczną[36]

- LAZARUS

[36] M. Broersma, Russian 'Sandworm' Hackers Targeted NATO, EU, Poland, iSIGHT, https://www.silicon.co.uk /workspace/ russian-sandworm-153576? inf_by=5b90f79d671db8fb298b522f [6.9.2018]

Znana jako Hidden Cobra, utożsamiana z rządem Korei Północnej, grupa 1,7 tys. hakerów, wspomaganych przez 5 tys. osób. Ze względu na złą infrastrukturę w kraju wielu z nich pracuje poza granicami, np. w Chinach, a nawet w Europie. Grupa początkowo stosowała jedynie ataki DDOS[37]. Zajmuje się głównie atakami na instytucje Korei Południowej (Operation Flame, Ten Days of Rain, Operation Troy, DarkSeoul) Lazarus stoi za atakiem na międzynarodowy bankowy system SWIFT skutkujący kradzieżą 81 mln USD banku w Bangladeszu. Są autorami ataku na firmę SONY oraz ataku na polski KNF (Komisję Nadzoru Finansowego) w lutym 2017 - atak typu watering hole[38]. Częstym atakiem grupy są portfele i giełdy kryptowalut za pomocą ataku wykorzystującego spearphising. Najbardziej głośnym atakiem przypisywanym grupie Lazarus jest WANNACRY ransomware[39], który przyniósł grupie zysk ok. 123 tyś USD[40].

Grupy przestępcze działające w celu osiągnięcia zysków (FIN)

- FIN 10 –atakuje organizacje w Ameryce Północnej od co najmniej 2013 do 2016 roku. Grupa wykorzystuje skradzione dane od ofiar w celu wyłudzenia środków.
- FIN 5 – ukierunkowana na dane osobowe i informacje o kartach płatniczych. Grupa działa od co najmniej 2008 r. i skupia się na branżach restauracyjnych, hazardowych i hotelarskich, członkowie prawdopodobnie mówią po rosyjsku
- FIN 6 – kradną dane kart płatniczych i sprzedają dla zysku w DarkNecie. Atakują dość agresywnie branżę hotelarską i detaliczną skupiając się na punktach sprzedaży PoS.
- FIN 7 – ukierunkowani głównie na sektor handlu detalicznego i hotelarskiego, często wykorzystując złośliwe oprogramowanie w punkcie sprzedaży, zbliżone do innej grupy Carbanak (być może grupy są powiązane)
- FIN8 – uruchamiająca specjalizowane kampanie spearphishingowe skierowane do branży detalicznej, restauracyjnej i hotelarskiej

[37] Atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania, polegający zwykle na przeciążeniu aplikacji serwującej określone dane
[38] Atak polegający na zaobserwowaniu, z których stron internetowych często korzysta ofiara, zainfekowanie jednej lub więcej z tych stron- w efekcie, cele korzystające z zarażonych witryn zostaną w końcu zainfekowane.
[39] Oprogramowanie szantażujące ofiary w celu osiągnięcia zysku z okupu za odszyfrowanie danych
[40] https://www.blockchain.com/btc/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw [6.9.2018]

Zakończenie

Jak pokazują statystyki[41], ilość ataków cybernetycznych rośnie wykładniczo. Państwa, organizacje lub przestępcy nie musza już używać przemocy fizycznej w celu osiągnięcia swych celów. Zakres działań cyberprzestępców jest związany z funkcjonowaniem każdego z nas w Internecie, od kluczowych dokumentów, skrzynek mailowych, po konta bankowe. Przestrzeń wirtualna stwarza potencjalne zagrożenie dla naszych interesów. Na każdy z nas ma w swoim telefonie lub komputerze prywatne dane, po ujawnieniu których może stracić oszczędności. Dotyczy to też listów, prywatnych zdjęć czy notatek. Nikt nie chciał by pokazywać całemu światu swojego życia prywatnego. Szczególnie narażone są osoby zajmujące ważne stanowiska, mogą być one szantażowane przez hakerów.

W dzisiejszych czasach ochrona cyberprzestrzeni stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa i obronności państw. Stworzenie mechanizmów rozpoznania zagrożeń istniejących w cyberprzestrzeni, takich jak: cyberterroryzm, cyberprzestępczość, cyberwojna lub wojna hybrydowa oraz innych form działań, mogących powodować zakłócenia w funkcjonowaniu krytycznej infrastruktury kraju jest bez wątpienia koniecznością. Tworzenie struktur rozpoznania i reagowania na zagrożenia cybernetyczne powinno odbywać się w każdej instytucji i służbie państwowej wraz z prowadzeniem specjalistycznych szkoleń i ćwiczeń dla członków tych zespołów. Kluczowym jest także budowanie świadomości zagrożeń oraz ustawiczne przeprowadzanie szkoleń wszystkich użytkowników systemu informatycznego.

Nie ma wątpliwości, iż cyberprzestępcy nie spoczywają na laurach i ciągle analizują możliwości przeprowadzenia skutecznego ataku, wiele ze zgłaszanych co chwila odnalezionych luk w programach komputerowych na pewno były lub są wykorzystywane przez nich. Równocześnie zwiększona ostatnio aktywność znanych grup APT świadczy o tym, że kolejne złośliwe kampanie ukierunkowane na infrastrukturę krytyczną z pewnością są już zaplanowane.

Zbliżające się kolejno wybory samorządowe, parlamentarne, do Parlamentu Europejskiego a na końcu prezydenckie w Polsce bezsprzecznie zwrócą uwagę różnym grupom

[41] Kerravala Z, Cisco CEO Chuck Robbins: Get ready for the network's next act, https://www.networkworld.com article / 3281052/ lan-wan/ cisco-ceo-chuck-robbins-get-ready-for-the-networks-next-act.html [6.9.2018]

hakerskim powiązanym ze służbami obcych państw. Projekt Lakhta czyli ingerencja Rosjan na wybory prezydenckie w USA ukazały jak niewielkim kosztem można uzyskać określone cele polityczne (budżet ok 1mln USD rocznie oraz 13 osób bezpośrednio zaangażowanych w działania)[42]. W tym aspekcie nie należy zapomnieć o zjawisku fake-news oraz fabrykach trolli, zignorowanie tego zjawiska, jak ukazuje przykład amerykański powoduje spolaryzowanie społeczeństwa, a co za tym idzie osłabienie państwa. Narzędzia kontrolowania tych przejawów wojny hybrydowej są tożsame do nowoczesnych narzędzi do walki z klasycznym malware, czyli analiza BigData oraz algorytmy służące uczeniu maszynowemu.

Literatura:

Applegate, S.D. The Principle of Maneuver in Cyber Operations, 2012 4th International Conference on Cyber Conflict 2012, NATO CCD COE Publications, Tallinn

Bejtlich, R. What Is APT and What Does It Want? https://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html

Bradley, G. Hackers Attack Via Chinese Web Sites, Washington Post. 25.8.2005

Broersma, M., Russian 'Sandworm' Hackers Targeted NATO, EU, Poland, iSIGHT, https://www.silicon.co.uk/workspace/russian-sandworm-153576?inf_by=5b90f79d671db8fb298b522f

CrowdStrtike, Who is FANCY BEAR?, https://www.crowdstrike.com/blog/who-is-fancy-bear/

CrySyS Lab, sKyWIper (a.k.a. Flame a.k.a. Flamer), Budapest University of Technology and Economics, Budapeszt 2012.

Cyberdefence24, Grupa Equation założona przez CIA i NSA, https://www.cyberdefence24.pl/grupa-equation-zalozona-przez-cia-i-nsa

ENISA, Threat Landscape 2014, Heraklion, Grecja European Union Agency for Network and Information Security

Hutchins, E. M., Cloppert, M. & Amin, R., 2011. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, s.l.: Lockheed Martin.

Jalonen, J. „Dni, które wstrząsnęły Estonią" https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html

[42] Pełny akt oskarżenia przygotowany przez ławę przysięgłych powołaną przez Roberta Muellera, prokuratora specjalnego ds. Russiagate https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rwUFGxaf6nlA/v0 [6.9.2018]

Kerravala Z, Cisco CEO Chuck Robbins: Get ready for the network's next act, https://www.networkworld.com/article/3281052/lan-wan/ cisco-ceo-chuck-robbins-get-ready-for-the-networks-next-act.html

Kaspersky LAB. Cyberpaleontologia: 20-letni zaawansowany atak, który nadal jest istotny https://www.kaspersky.pl/o-nas/informacje-prasowe/2767/cyberpaleontologia-20-letni-zaawansowany-atak-ktory-nadal-jest-istotny

Kaspersky, Lab, 2013. Kaspersky Daily blog: https://plblog.kaspersky.com/robak-morris-konczy-25-lat/669/

Kozłowski, A. Szczyt NATO w Warszawie – konsekwencje dla polityki cyberbezpieczeństwa. http://www.cyberdefence24.pl/406632,szczyt-nato-w-warszawie-konsekwencje-dla-polityki-cyberbezpieczenstwa

Lakomy M. „Cyberwojna jako rzeczywistość XXI wieku", Stosunki Międzynarodowe – International Relations • nr 3–4 (t.44) 2011.

Mandiant, APT1: Exposing One of China's Cyber Espionage Units, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Marks, P., 2011. "Dot-dash-diss: The gentleman hacker's 1903 lulz". New Scientist, 24 12, https://www.newscientist.co

McElroy, D., Williams, C., Flame: world's most complex computer virus exposed, The Telegraph, https://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html

McMillan, R., Siemens: Stuxnet worm hit industrial systems. Computerworld, 14.09.2010,

Michalik, Ł., Pole walki: cyberprzestrzeń. Kiedy haker staje się żołnierzem? , Gadżetomania https://gadzetomania.pl/1471,pole-walki-cyberprzestrzen-kiedy-haker-staje-sie-zolnierzem

MITRE, Adversarial Tactics, Techniques & Common Knowledge, https://attack.mitre.org/wiki/Main_Page

Nakashima, E., Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies, The Washington Post, https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?utm_term=.611c5e12a4be

Onley, D.S. , Patience Wait „ Red storm rising", https://gcn.com/articles/2006/08/17/red-storm-rising.aspx

Parnell, B. A., Cyber crime now bigger than the drugs trade, http://www.theregister.co.uk/2011/09/07/cost_is _more_than_some_drug_trafficking,

Pełny akt oskarżenia przygotowany przez ławę przysięgłych powołaną przez Roberta Muellera, prokuratora specjalnego ds. Russiagate https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rwUFGxaf6nlA/v0

Phillips, T., The Telegraph, https://www.telegraph.co.uk/news/worldnews/asia/china/10083296/Chinese-hackers-access-sensitive-US-weapons-systems.html

Safire, W., The New York Times, 2004. "The Farewall Dosier". http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?_r=1

Sanger. D., Obama Order Sped Up Wave of Cyberattacks Against Iran. http://www.nytimes.com/2012/06/01 /world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&pagewanted=2&seid=auto&
smid=twnytimespolitics&pagewanted=all

Sikora, M., Krótka historia cyberwojen, Gadżetomania, https://gadzetomania.pl/4137,krotka-historia-cyberwojen

Simonite, T., MIT Technology Review, https://www.technologyreview.com/s/428166/the-antivirus-era-is-over/

Symantec, 2011. W32.Duqu The precursor to the next Stuxnet, http://www.symantec.com/content/en/us/
enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Świechowski G. „Hacktywizm, czyli bunt internautów" http://www.pcworld.pl/news/Hacktywizm-czyli-bunt-internautow,368875.html

Traynor, J. The Guardian, Russia accused of unleashing cyberwar to disable Estonia. https://www.theguardian.com/world/2007/may/17/topstories3.russia

Zetter, K., Odliczając do dnia zero. Stuxnet, czyli prawdziwa historia cyfrowej broni, Helion 2017