ISSN 1507-3858
e-ISSN 2450-0003

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu
e-mail: artur.rot@ue.wroc.pl

Bogusław Olszewski
Uniwersytet Wrocławski
e-mail: boguslaw.olszewski@uni.wroc.pl

ZAAWANSOWANE ATAKI TYPU ATP JAKO NOWA FORMA ZAGROŻEŃ DLA CYBERBEZPIECZEŃSTWA

ADVANCED PERSISTENT THREAT ATTACKS AS A NEW CYBERSECURITY THREAT

DOI: 10.15611/ie.2016.2.06
JEL Classification: O30, O32

Streszczenie: Według badań Kaspersky Lab [*Cyberbezpieczeństwo* 2016...] do najpoważniejszych zagrożeń 2016 roku należy zaliczyć długotrwałe, zaawansowane kampanie cyberprzestępcze (APT – *Advanced Persistent Threats*). Zaawansowane ugrupowania kontaktujące się w różnych językach atakowały systemy informatyczne instytucji finansowych, organizacji rządowych, wojskowych oraz dyplomatycznych, firm telekomunikacyjnych oraz energetycznych, aktywistów i przywódców politycznych, mediów, firm prywatnych itp., a wszystkie te ataki miały zasięg globalny. Artykuł przybliża problematykę ataków APT, wskazuje newralgiczne punkty w cyklu życia APT, a także przedstawia największe zagrożenia z nimi związane. Głównym celem artykułu jest przedstawienie APT jako złożonego i wielowymiarowego zjawiska, stanowiącego realne zagrożenie dla przedsiębiorstw, organizacji i podmiotów publicznych.

Słowa kluczowe: ataki APT, cyberbezpieczeństwo, zagrożenia bezpieczeństwa, cykl życia APT.

Summary: According to Kaspersky Lab research, Advanced Persistent Threats which include long-term, advanced cybercriminal campaigns are the most serious threat in 2016. Advanced groups contacting in different languages, are attacking information systems of financial institutions, government, military and diplomatic organizations, energy and telecommunication companies, activists and political leaders, media, private companies, etc. and all these attacks are global. The article presents the problem of APT attacks, indicating critical points in the life cycle of APT and presents the greatest risks associated with them. The main aim of this article is to present the APT as a complex and multidimensional phenomenon, which is a real threat to businesses, organizations and public entities.

Keywords: APT attacks, cybersecurity, security threats, APT lifecycle.

1. Wstęp

Procesy globalizacyjne i erozja władzy państwowej sprawiają, że ofiarami APT padają nie tylko przedsiębiorstwa IT, firmy opracowujące wysokie technologie czy instytucje finansowe, ale w dużej mierze agencje rządowe i sektor militarny. Podczas konferencji Infosecurity Europe 2011 APT zostały zaliczone do największych zagrożeń w cyberprzestrzeni współczesnego świata, a jako stanowiące ich specyficzny rodzaj, wymagają odmiennego podejścia niż stosowane dotychczas. Ta cyberprzestrzeń to wirtualna przestrzeń (najczęściej Internet), w której komunikują się połączone siecią komputery lub inne media cyfrowe. W rankingu najbardziej narażonych celów najwyższe miejsca zajmują organizacje biznesowe i przedsiębiorstwa, w ścisłej czołówce zaś znajdują się branże: edukacyjna, finansowa, wysokich technologii, kosmiczna i lotnicza, energetyczna, chemiczna, telekomunikacyjna medyczna i konsultingowa [Rot 2016]. Wśród dotychczasowych APT głównym motywem okazały się cele biznesowe i finansowe.

Na gruncie cyberbezpieczeństwa istnieje wiele luk badawczych generowanych przez nieustanne zmiany jego desygnatów i środowiska, związanych z jego aspektami technologicznymi, społecznymi, militarnymi, politycznymi itd. Podobna sytuacja panuje w odniesieniu do zagadnienia APT, którego rozwojowy charakter skłania do głębszej refleksji. W kontekście dostępnej literatury poruszającej zagadnienie APT jest zauważalny praktycznie całkowity brak jednolitych polskojęzycznych opracowań w postaci monografii czy raportów, materiały zaś dotyczące tych zagrożeń publikowane w sieci WWW ograniczają się do podstawowych informacji. Przegląd literatury anglojęzycznej prowadzi do wniosku, że informacje w niej zawarte są także fragmentaryczne, mimo szerokiej dostępności zasobów. Stąd też wynika postawiony przez autorów cel kompleksowego przedstawienia ww. zjawiska i częściowego wypełnienia luk w dostępnej literaturze, zrealizowany w postaci niniejszego przeglądowego artykułu, ukazującego cykl życia APT, mechanizm APT i największe zagrożenia wynikające z tego typu ataków. Głównym celem niniejszego artykułu jest przedstawienie *Advanced Persistent Threats* jako złożonego i wielowymiarowego zjawiska, stanowiącego realne zagrożenie dla przedsiębiorstw, organizacji i podmiotów publicznych.

2. Definicja APT

W inauguracyjnym dokumencie na temat APT firmy Mandiant, publikującej raporty dotyczące cyberzagrożeń i specjalizującej się w materii związanej z tym problemem, zawarto definicję, w myśl której jest to „grupa wyrafinowanych, zdeterminowanych i skoordynowanych atakujących, którzy przez lata systematycznie kompromitują sieci komputerowe rządu Stanów Zjednoczonych i sektora komercyjnego" [Mandiant 2010]. Stąd też jej okresowe publikacje dotyczące stanu faktycznego i panujących trendów opisują członków grup APT, sposoby, w jaki działają oraz jak rozpoznać

stosowane przez nich narzędzia, taktyki i procedury [*Cyber Threat Intelligence...* 2016]. Z kolei inne ujęcie stanowi, że APT „jest formą wielostopniowego ataku prowadzonego w większym ukryciu, wymierzonego w szczególności dla osiągnięcia sprecyzowanego celu, najczęściej cyberszpiegostwa" [Ghafir, Prenosil 2014]. Podsumowując, część definicji APT podkreśla udział aparatu państwowego, pozostałe zaś skupiają się raczej na samych mechanizmach, kładąc jednocześnie nacisk na sektor komercyjny jako punkt odniesienia. W tym drugim przypadku stosuje się zamiennie termin *Advanced Targeted Attacks*, „który generalnie odnosi się do tego samego obiektu" [Hudson 2014].

Zaawansowanie (*Advanced*) jest związane zarówno z rodzajem zastosowanego złośliwego kodu czy narzędzi programistycznych, jak i samym charakterem zagrożeń. Stwarzający je oponenci są zdolni do użycia całego zakresu znanych środków programistycznych i podatności, a także do wykorzystania i stworzenia zupełnie nowych. Zaawansowanie APT wynika z zastosowania wyrafinowanych narzędzi i jest obliczone na przeprowadzenie akcji sabotażowych, kradzież zastrzeżonych informacji, wyłudzenia czy szantaże. W tym wypadku uwidacznia się złożoność tej formy oddziaływania, będąca wynikiem ewolucji globalnego otoczenia teleinformatycznego. Inne elementy decydujące o wysokim poziomie skomplikowania to szyfrowanie w celu ukrycia tożsamości i ograniczenia wszelkich śladów cyfrowych czy rekompilacja złośliwego kodu w czasie rzeczywistym (już w trakcie trwania ataku). Hakerzy stojący za APT są nie tylko doskonale wykształceni, ale i korzystają z zaplecza finansowego oraz szerokiej gamy narzędzi pozwalających uczynić taki atak niezwykle skutecznym. Wyrafinowane metody służące pozyskiwaniu informacji na wstępnym etapie, jak i towarzyszące szerszemu kontekstowi związanemu z rozpoznaniem, nie są jednak odkrywcze i zawierają znane zabiegi socjotechniczne. Pozostają one uniwersalne pomimo bogatej literatury przedmiotu i podejmowanych przeciwdziałań. Dopiero uzyskanie dostępu do sieci i właściwy atak nadają zagrożeniom atrybut „zaawansowanych".

Druga składowa wyróżniająca ataki APT, długotrwałość (*Persistent*), jest związana z charakterem operacji, której element stanowią. Nie są one bowiem prowadzone incydentalnie, lecz wynikają z wytycznych służących realizacji większego przedsięwzięcia. Jak będzie można zauważyć na przykładach podanych poniżej, niektóre z nich są prowadzone latami, a trwałość w czasie „niekoniecznie oznacza, że przeciwnicy przejawiają potrzebę nieustannego wykonywania złośliwego kodu na komputerach ofiary. Raczej utrzymują pewien poziom interakcji wymagany do osiągnięcia ich celów" [*What is APT…* 2016]. Priorytetem jest pozostanie jak najdłużej niewykrytym, sukcesywnie osiągając wcześniej założone cele. Sprowadzają się one generalnie do profitów natury finansowej, zarówno jeśli mowa o zleceniodawcach (oszczędności na badaniach naukowych, korzyści ekonomiczne czerpane z patentów i pierwszeństwa w eksploatacji złóż, dokumentacja dotycząca wdrażania nowych technologii itp.), jak i zleceniobiorcach (wynagrodzenie, uzyskanie dostępu do złożonych narzędzi programistycznych, ewentualna stała współpraca).

Zagrożenie (*Threat*) jest związane przede wszystkim z czynnikiem ludzkim i dotyczy grup działających na wysokim poziomie zorganizowania. Są one silnie zmotywowane (wskutek zależności służbowych lub istotnych bodźców finansowych), tworzą łańcuchy powiązań i dedykowane podgrupy zajmujące się poszczególnymi aspektami całego procesu APT. A zatem zagrożenie nie wynika tu z samej dostępności narzędzia w postaci chociażby *malware*, ale z kompleksowego podejścia stosujących je podmiotów – dlatego w dalszej części niniejszego artykułu będzie także stosowany termin „operacja typu APT". Co za tym idzie, podmioty te nie muszą mieć pełnego obrazu całej misji, realizując przydzielone zadania dotyczące wąskiego zakresu kompetencji. Autorami zagrożeń typu APT są zazwyczaj wysoko wyspecjalizowane zespoły informatyków, a także rządy państw występujące w roli mocodawców, wykorzystujące zaawansowane technologie oraz szerzej nieznane wektory ataku w celu pozyskiwania wrażliwych informacji. Określa się je również mianem ataków ukierunkowanych, ponieważ każda ofiara jest obejmowana uprzednią obserwacją w celu określenia najlepszej metody uderzenia.

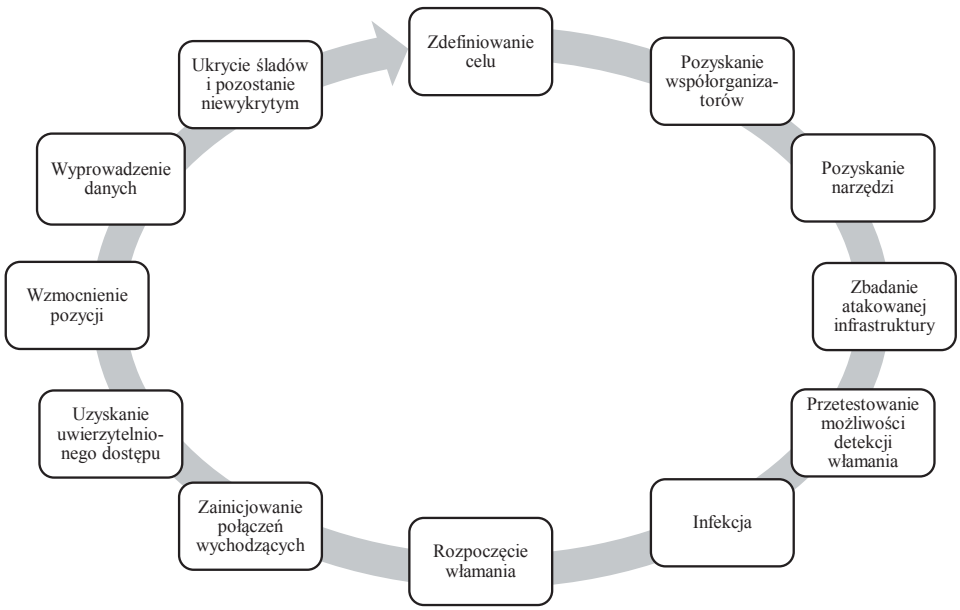
Niewidoczność i kompleksowy charakter działań oraz zaawansowanie ataku po uzyskaniu dostępu do sieci – celu stanowią konglomerat wyróżniający APT spośród innych zagrożeń IT. Jest to wiązany atak wielostopniowy, w którym powodzenie kolejnego etapu zależy od pozytywnej realizacji poprzedniego. Jako nowa kategoria zagrożeń, znajdują się coraz częściej w centrum zainteresowania z racji generowanych strat. Na przykład rząd Wielkiej Brytanii stwierdził w 2011 r., że APT „kosztują państwo około 27 mld funtów rocznie, zaś w odniesieniu do niektórych szacunków ich globalny koszt wynosi 1 bilion dolarów rocznie" [Tankard 2011]. Ilość danych wyprowadzanych z organizacji jest liczona w petabajtach i należy podkreślić, że obecnie zostało udowodnione, że wykryte APT może być przeprowadzone w trywialny sposób, z użyciem rynkowego sprzętu i oprogramowania [Xenakis, Ntantogian 2015].

3. Cykl życia APT i jego newralgiczne punkty

Typowy cykl życia APT składa się z czterech głównych etapów: rozpoznania, wstępnej infekcji, przejęcia kontroli i infiltracji. Szczegółowe etapy tego procesu zostały zobrazowane na rys. 1. Rozpoznanie umożliwia wybór potencjalnych wektorów ataku, określenie podatności i katalogu osób w obrębie organizacji, mogących w sposób aktywny lub bierny umożliwić ominięcie zabezpieczeń sieciowych. Czasami są to pracownicy posiadający dostęp do zasobów bez większego znaczenia strategicznego, jednak w perspektywie pozwalających na dalszą ekspansję we wnętrzu systemu wybranego przedsiębiorstwa. Mogą to być również prezesi, członkowie zespołów IT czy pracownicy zewnętrznych podwykonawców, stali kontrahenci, byli pracownicy z wciąż aktualnym firmowym loginem i hasłem, członkowie ich rodzin itd. Zaufanie, jakim są darzeni, lub pozycja zajmowana w strukturze firmy przekłada się na ich ewentualną rolę na pierwszym etapie APT. Rozpoznanie dotyczy także formy zabez-

pieczeń fizycznych i informatycznych organizacji – szczególnie użyteczne okazują się tutaj upublicznione dane: rodzaj stosowanych systemów operacyjnych, architektura sieci, udostępnione numery IP (w tym urządzeń PLC czy SCADA), podział kompetencji, udział w przetargach związanych z bezpieczeństwem IT, dostarczane i stosowane rozwiązania.

Faza preparacyjna przygotowuje grunt pod drugi etap cyklu życia APT. Wstępne zainfekowanie jest następstwem uzyskania dostępu do jednego z elementów składowych sieci informatycznej: desktopa, urządzenia sieciowego, a czasami komputera, pendrive'a lub smartphone'a wybranej osoby, posiadającej uprawnienia wysokiego poziomu lub korzystającej ze sprzętu takiego pracownika w swoim otoczeniu zawodowym lub prywatnym. Sprzyja temu nieautoryzowane wykorzystywanie prywatnych urządzeń w miejscu pracy oraz włączanie ich w sieć korporacyjną i internetową. Całkowitego obrazu działań na tym poziomie, podobnie zresztą jak i na poprzednim, dopełnia socjotechnika. Najczęściej to właśnie dzięki niej do systemów organizacji zostaje wprowadzone *malware* w postaci konia trojańskiego lub aplikacji umożliwiającej prowadzenie zdalnych czynności administracyjnych.



Rys. 1. Cykl życia APT

Źródło: [Virgillito 2016].

Negatywny wynik przeprowadzonej próby detekcji otwiera drogę do drugiego etapu związanego z dostarczeniem *malware*, po inicjującym wtargnięciu zaś zostaje ustanowiony kanał komunikacyjny z atakującym (*Command&Control Server*,

C&C). Trzeci etap jest równoznaczny z przejęciem kontroli nad pożądanymi funkcjonalnościami systemu i ewentualnie nad kolejnymi użytkownikami, w celu ostatecznego uzyskania dostępu do danych stanowiących główny cel operacji. Mogą one być integralną częścią aktualnie penetrowanych zasobów sieciowych lub dotyczyć personalnie konkretnego użytkownika, zwłaszcza jeśli mają być zgromadzone informacje leżące wyłącznie w jego gestii. Podobna sytuacja ma miejsce, gdy niezbędne są dane służące skompromitowaniu konkretnej osoby lub gdy mają one stanowić punkt wyjścia do przeprowadzenia właściwego APT.

Poziom czwarty wiąże się z długotrwałym procesem infiltracji prowadzonym w oparciu o uzyskiwane uprawnienia systemowe. Na jego dalszym etapie podejmuje się działania służące poszerzeniu dostępu i przyznaniu dodatkowych przywilejów w systemie, co skutkuje dalszym umocowaniem i „rozmyciem" obecności intruza. Rozpoczyna się pozyskiwanie/niszczenie właściwych danych stanowiących obiekt zainteresowania jego samego lub zlecającej strony trzeciej. Po jego zakończeniu następuje wycofanie z systemu i zatarcie nie tylko śladów działań, ale i wszelkich danych umożliwiających precyzyjne określenie źródła pochodzenia ataku.

Podsumowując, identyfikacja celów (infrastruktura i zasoby ludzkie), wytypowanie oraz wykorzystanie świadomych i nieświadomych współsprawców, pozyskanie lub opracowanie niezbędnych narzędzi programistycznych, test na wykrywalność, zainicjowanie włamania, ustanowienie połączenia, transfer/modyfikacja danych i zatarcie śladów (także przy zachowaniu dalszej obecności w systemie) stanowią kluczowe elementy całego procesu.

4. Wykorzystywanie podatności w atakach APT

Stosunkowo niedługa historia APT i szum medialny wpływają na ich błędną ocenę i sprawiają, że są one niedoceniane, a specjaliści od cyberbezpieczeństwa „nie uświadamiają sobie, że istnieją zaawansowane zagrożenia, które ominęły ich tradycyjne techniki ochrony i rezydują niewykryte w ich systemach bezpieczeństwa" [Pingree, MacDonald 2016]. Traktowanie APT jako taniej sensacji czy kolejnej kampanii marketingowej zaciemnia obraz tego zjawiska, niejednokrotnie je deprecjonując. Jako pierwszą podatność należy zatem wskazać czynnik ludzki, związany z samą świadomością istnienia APT i towarzyszących im mechanizmów wykorzystywanych przez zainteresowane grupy za nim stojące. Brak takiej wiedzy prowadzi do bezrefleksyjnych zachowań w miejscu pracy i na gruncie prywatnym, generując sytuacje umożliwiające przejście na kolejny poziom i wykonanie APT. Nie bez znaczenia jest także odpowiednia wiedza administratorów sieci i zespołów odpowiedzialnych za bezpieczeństwo IT organizacji, a przede wszystkim racjonalne podejście osób decyzyjnych, od których zależy wyasygnowanie funduszy i wdrożenie określonych strategii.

Socjotechnika i ogólnodostępne zasoby informacji na temat konkretnego pracownika (blogi, media społecznościowe i branżowe, strony firmowe) pozwalają

wytypować osoby posiadające dostęp do wrażliwych danych, dysponujące hasłami umożliwiającymi penetrację zasobów sieciowych organizacji lub mogące służyć swoją wiedzą na drodze do uzyskania kolejnych informacji, stanowiących ostateczny obiekt zainteresowania lub punkt wyjścia dla następnego etapu APT. Znając profil psychologiczny i zawodowy danego pracownika, dokonuje się oceny jego potencjalnych słabości możliwych do wykorzystania, także w ramach szantażu czy bezpośredniej oferty związanej z gratyfikacją finansową w zamian za udostępnienie posiadanych zdolności i środków wynikających z funkcji pełnionych w organizacji. Dotyczy to przede wszystkim zwalnianych pracowników, aktualnie zatrudnionych, lecz wyrażających negatywne zdanie na temat pracodawcy czy osób subiektywnie pokrzywdzonych, z poczuciem bycia wykorzystywanym lub niedocenianym przez organizację, jako że przestępcy używają różnych wektorów ataków, różnych typów exploitów i słabości po to, by uzyskać dostęp do ważnych firmowych danych [Bequerel 2013]. W zależności od wagi informacji docelowych, a zwłaszcza w przypadku zaangażowania służb specjalnych zainteresowanego państwa, wśród celów ludzkich mogą się znaleźć rodzina lub znajomi osoby stanowiącej główny cel APT. W skrajnych wypadkach mogą być również zastosowane negatywne środki lub przymus fizyczny, niepozostawiające wyboru osobom otrzymującym propozycję udziału w operacji APT.

Celowany *Advanced Persistent Threat* oznacza w istocie wielopłaszczyznowe działania ukierunkowane na sukcesywne osiąganie kolejnych etapów. Na płaszczyźnie socjotechniki wyraża się to przez atak spersonalizowany (*spear-phishing*), którego celem jest nieuprawnione wejście w posiadanie danych leżących w gestii konkretnej osoby lub uzyskanie z jej pomocą dostępu do właściwych zasobów i urządzeń sieciowych, w tym także należących do innej organizacji lub pracownika. Rozpoczyna się on już na etapie rozpoznania, przyjmując postać wywiadu środowiskowego (*on-line*, ale i w świecie rzeczywistym) i jest to *de facto* dedykowany atak phishingowy. Ofiara otrzymuje spersonalizowaną wiadomość email i przekonana o zaufanym statusie źródła otwiera załączniki lub uruchamia załączone linki. Wywiad środowiskowy umożliwia poznanie zależności służbowych i kontaktów prywatnych potencjalnej ofiary, jej preferencji politycznych i światopoglądu, zainteresowań itd. Wszystko to w efekcie pozwala przygotować precyzyjnie skonstruowany mail. Na tym etapie niejednokrotnie są wybierane osoby pozornie niewiązane z dostępem do docelowych zasobów, *spear-phishing* zaś z użyciem poczty mailowej nadal jest częstym środkiem używanym przez napastników APT do infiltrowania sieci docelowej [*Spear-phishing email*…2012]. Według analiz Trend Micro w okresie od lutego do września 2012 r. 91% celowanych ataków zostało przeprowadzonych z wykorzystaniem komponentu *spear-phishing email*, a 94% maili zawierało załączniki uruchamiające sekwencję instalacji *malware*.

Socjotechnika zajmuje najważniejsze miejsce wśród skutecznych sposobów zainicjowania infekcji sieci docelowej i jest najczęściej stosowanym zabiegiem pozwalającym uzyskać dostęp do zasobów stanowiących obiekt zainteresowania.

Ataki w rodzaju *zero-day* stanowią drugą co do skuteczności grupę wykorzystującą tym razem podatności związane z oprogramowaniem. Dzięki nim hakerzy omijają klasyczne zabezpieczenia oparte na bazach sygnatur programów antywirusowych i antywłamaniowych. Poza lukami w oprogramowaniu liczne podatności istnieją w warstwie fizycznej – w dobie wzmożonej komunikacji bezprzewodowej są one nagminnie wykorzystywane. Dlatego też cele natury technicznej obejmują m.in. dane na temat prac badawczych prowadzonych nad samym APT, sieciowymi systemami zabezpieczeń czy kodów źródłowych. Podatności *hardware* stanowią dopełnienie programowych w wypadku mikroprocesorów, gdyż niektórzy producenci celowo pozostawiają lukę dostępową na potrzeby testów powytwórczych [Jover, Giura 2013].

Jak już wspomniano na początku artykułu, w rankingu najbardziej narażonych celów najwyższe miejsca zajmują organizacje biznesowe i przedsiębiorstwa, w ścisłej czołówce zaś znajdują się branże: edukacyjna, finansowa, wysokich technologii, kosmiczna i lotnicza, energetyczna, chemiczna, telekomunikacyjna, medyczna i konsultingowa. W ich przypadku konsekwencją przeprowadzonego ataku typu APT są nie tylko początkowe koszty finansowe związane z utratą własności intelektualnej (sklonowaniem, sprzedażą, wykorzystaniem w dalszych badaniach, dostarczeniem na ich podstawie konkurencyjnych produktów i usług), ale przede wszystkim spadek wiarygodności oraz wtórne, długookresowe efekty w postaci odpływu klientów (jeśli mowa o podmiotach komercyjnych) czy podważenia kompetencji instytucji międzynarodowych i rządów państw (w tym negatywny wpływ na bezpieczeństwo infrastruktury krytycznej i militarnej). Utrata chronionych zasobów w postaci danych osobowych i innych wrażliwych informacji ma wpływ na dynamikę globalnej konkurencji i zmiany struktury ekonomicznej państw, a ponadto destabilizuje rynki finansowe. D. Alpetrovitch, wiceprezydent Threat Research w McAfee, mówi na ten temat: „Jestem przekonany, że każda firma w każdej możliwej do wyobrażenia branży o znacznych rozmiarach i cennej własności intelektualnej oraz tajemnicach handlowych została skompromitowana (lub wkrótce zostanie), wraz z przeważającą większością ofiar rzadko odkrywających włamanie lub jego skutki" [Alpetrovich 2011]. Niezwykłej skuteczności *Advanced Persistent Threats* sprzyja fakt, że 68% menedżerów nie posiada podstawowej wiedzy na ich temat [*The Risk of an Uncertain*… 2013].

Już same wykradzione hasła do skrzynek mailowych nie tylko pozwalają śledzić komunikację korporacyjną, ale umożliwiają wgląd w realizowane projekty i informacje ściśle związane z zarządem, w tym wszelkie materiały pozwalające na kradzież tożsamości jego członków czy uzyskanie autoryzacji dającej dostęp do zastrzeżonych i poufnych danych. Celem APT są wyniki czaso- i kapitałochłonnych badań (własność intelektualna, *know-how*), tajemnice handlowe w postaci baz kontrahentów i planów przyszłych negocjacji handlowych czy przetargów, dokumentacja procesów przemysłowych, schematy organizacji systemów nadzoru przemysłowego ICS (SCADA, DCS) oraz informacje na temat lokalizacji i zasobności złóż

ropy i gazu ziemnego – wykorzystywane także w celach sabotażowych. Na przykład sektor energetyki stanowi część infrastruktury krytycznej państwa i nie jest zaskoczeniem jego infiltracja z uwagi na obecność wielu wrażliwych danych w powiązanych systemach – tak komercyjnych, jak i rządowych. Stanowią one etap czy punkt wyjścia do dalszej eksploracji w kierunku ujawnienia tajemnic przedsiębiorstwa, ale jednocześnie tworzą relacje umożliwiające dalszą eksplorację zasobów sieciowych i dostęp do celów wojskowych i politycznych o wyższym priorytecie.

Korporacje globalne realizujące zamówienia rządowe w branży zbrojeniowej stają się zastępczym lub pośrednim obiektem dla APT wymagających w przypadku sieci wojskowych (NIPRNet, SIPRNet) znacznego wyrafinowania i umiejętności. Choć niektórzy badacze uważają, że to raczej w przeszłości APT były w większości ukierunkowane na cele polityczne i militarne [Giura, Wang, za ASE 2012], a przez ostatnie kilka lat atakujący coraz częściej używają APT do uderzeń na przedsiębiorstwa dla uzyskania korzyści finansowych, to wszystkie te płaszczyzny się przenikają, zwłaszcza w zaawansowanych technologicznie postindustrialnych gospodarkach opartych na wiedzy. Cele czysto militarne obejmują przede wszystkim infiltrację systemów obronnych, aby znaleźć ich potencjalne słabości. Związane z nimi cele polityczne obejmują niejawne i tajne zasoby danych dotyczące powiązań, dyplomacji, przeszłych i aktualnych działań rządów państw i organizacji międzynarodowych oraz kierunków przyszłej aktywności. To także działania odnoszące się do własnej struktury społecznej, prowadzone w imię zachowania stabilności – stąd na gruncie bezpieczeństwa wewnętrznego powołuje się takie komórki organizacyjne, jak Office of Tailored Access Operations (TAO), stanowiące część National Security Agency (NSA) [*Documents Reveal*… 2016].

5. Zakończenie

Głównym celem niniejszego artykułu było przedstawienie *Advanced Persistent Threats* jako złożonego i wielowymiarowego zjawiska, stanowiącego realne zagrożenie dla współczesnych przedsiębiorstw, organizacji i podmiotów publicznych. Mając na uwadze złożoność ataków i dotychczasowe tendencje, autorzy mieli zamiar dokonać pewnej ekstrapolacji i przedstawienia APT jako procesu obejmującego stopniowo kolejne newralgiczne obszary – nie ograniczonego wyłącznie do samego bezpieczeństwa IT w organizacjach, ale wywierającego szerszy wpływ na rzeczywistość, a także umożliwiającego osiągnięcie celów, na drodze do których APT jest co prawda kluczowym, ale wciąż jednym z wielu środków. APT jest zatem złożonym i wielowymiarowym zjawiskiem, stanowiącym poważne zagrożenie dla dzisiejszych organizacji, ale nie tylko dla nich. Analiza zagadnienia i dotychczasowej ewolucji ataków skłania do postawienia hipotezy, że *Advanced Persistent Threats* przechodzą obecnie w fazę związaną z ich dalszą modyfikacją i testowaniem jako środka działań ofensywnych w konfliktach międzypaństwowych i asymetrycznych. Siły zbrojne i służby specjalne państw dostrzegły w nich nie tylko narzędzie *per se*,

pozwalające osiągnąć przewagę ekonomiczną i militarną, ale podstawę teoretyczną do dalszych badań związanych z opracowywaniem cyberbroni.

Literatura

Alpetrovich D., 2011, *Revealed: Operation Shady RAT*, McAfee White Paper, s. 2, http://www.mcafee.com/us/ resources/white– papers/wp– operation– shady– rat.pdf (06.09.2016).

ASE 2012, s. 1, http://web2– clone.research.att.com/techdocs/TD_101075.pdf (3.10.2016).

Bequerel S., 2013, *Wszystko, co powinieneś wiedzieć o APT*, https://plblog.kaspersky.com/ wszystko– co– powinienes– wiedziec– o– apt/696/ (18.08.2016).

Cyber Threat Intelligence on Advanced Attack Groups and Technology Vulnerabilities, https://www.fireeye.com/ current– threats/threat– intelligence– reports.html (18.08.2016).

Cyberbezpieczeństwo 2016: 5 trendów, jakich powinniśmy się obawiać, http://serwisy.gazetaprawna.pl/nowe– technologie/artykuly/914855,cyberbezpieczenstwo– 2016– 5– trendow– jakich– powinnismy– sie– obawiac.html.

Documents Reveal Top NSA Hacking Unit, http://www.spiegel.de/international/world/the–nsa–uses–powerful–tool box–in–effort–to–spy–on–global–networks– a– 940969.html (04.10.2016).

Ghafir I., Prenosil V., 2014, *Advanced Persistent Threat attack detection: An overview*, [w:] *Proceedings of International Conference On Advances in Computing, Electronics and Electrical Technology*, Kuala Lumpur, s. 154, http://www.seekdl.org/nm.php?id=3901.

Giura P., Wang W., *Using large scale distributed computing to unveil Advanced Persistent Threats*, Science Journal No. 1(3), s. 93. ASE 2012, s. 1, http://web2–clone.research.att.com/techdocs/TD_101075.pdf (3.10.2016).

Hudson B., 2014, *Advanced Persistent Threats: Detection, protection and prevention*, Sophos White Paper, s. 2, https://www.lifeboatdistribution.com/content/vendor/sophos/whitepaper–sophos– advanced– persistent– threats– detecti on– protection– prevention.pdf (23.09.2016).

Jover R.P., Giura P., 2013, *How vulnerabilities in wireless networks can enable Advanced Persistent Threats*, International Journal on Information Technology (IREIT), no. 1(2), s. 145-151, http://www.research.att.com/ techdocs/TD_100739.pdf.

Mandiant M., *Trends. The Advanced Persistent Threat*, Mandiant 2010, s. 1, http://static1.1.sqspcdn.com/static/f/ 956646/23348947/1377032203613/M– Trends+by+Mandiant.pdf?token=rHVNRdmJOeNXpYxvBtLi1LiZcAk%3 D (03.10.2016).

Pingree L., MacDonald N., *Best practices for mitigating Advanced Persistent Threats*, http://apac.trendmicro.com/cloudcontent/apac/pdfs/solutions/enterprise/best_practices_for_mitigating_apts_224682.pdf (30.08.2016).

Rot A., 2016, *Zarządzanie ryzykiem w cyberprzestrzeni – wybrane zagadnienia teorii i praktyki*, [w:] T.M. Komorowski, J. Swacha (red.), *Projektowanie i realizacja systemów informatycznych zarządzania. Wybrane aspekty*, Polskie Towarzystwo Informatyczne, Warszawa.

Spear-phishing email: Most favored APT attack bait, 2012, Trend Micro Incorporated Research Paper, s. 1, http://www.trendmicro.com/cloud– content/us/pdfs/security– intelligence/white– papers/wp–spear– phishing– email– mo st– favored– apt– attack– bait.pdf (5.09.2016).

Tankard C., 2011, *Advanced Persistent threats and how to monitor and deter them*, Network Security, Issue 8, s. 16, http://www.sciencedirect.com/science/article/pii/S1353485811700861.

The Risk of an Uncertain Security Strategy. Study of Global IT Practitioners in SMB Organizations, 2013, Ponemon Institute, s. 10, fig. 12, http://sophos.files.wordpress.com/2013/11/2013– ponemon– institute– midmarket– trends– sophos.pdf (07.09.2016).

Virgillito D., *Cyber crime security risks for healthcare companies*, http://www.massivealliance.com/2013/12/18/cyber–crime–security–risks–healthcare (24.09.2016).

What is APT and What Does It Want?, http://taosecurity.blogspot.be/2010/01/what–is–apt–and–what–does–it–want.html (23.09.2016).

Xenakis Ch., Ntantogian Ch., 2015, *Attacking the Baseband Modem of Mobile Phones to Breach the Users' Privacy and Network Security*, [w:] Maybaum M., Osula A.-M., Lindström L. (eds.), *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, NATO CCDCOE, s. 234, https://ccdcoe.org/sites/default/files/multi media/pdf/CyCon_2015_book.pdf.