„Cicha reakcja" na zdalne ataki teleinformatyczne

Adam PATKOWSKI

Instytut Teleinformatyki i Automatyki WAT,
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa
adam.patkowski@ wat.edu.pl

STRESZCZENIE: „Cicha reakcja" systemu zabezpieczeń zasobów teleinformatycznych to zastąpienie blokowania cyberataków innymi działaniami, niedostrzegalnymi dla napastnika. Proponuje się usunięcie atakowanych zasobów przez zastąpienie ich spreparowanymi danymi. Pozwoli to na rozpoznawanie poczynań napastnika przy znacznie mniejszych szansach wykrycia niż użycie oddzielnych honeypotów. Przede wszystkim jednak daje to możliwość prowadzenia dezinformacji przeciwników/konkurentów właściciela systemu na poziomie operacyjnym. Ponadto wprowadzenie mechanizmu opóźnionego zapisu danych w systemie teleinformatycznym, zwiększa graniczny czas na wykrycie cyberataków zanim nastąpią nieodwracalne zmiany zasobów informacyjnych.

SŁOWA KLUCZOWE: cyberbezpieczeństwo, deception solutions, dezinformacja, honeynet, honeypot, piaskownice (sandboxes)

1. Wprowadzenie

Działania w obszarze „cyber" coraz bardziej przypominają walkę informacyjną i to nie tylko w sferze mediów społecznościowych. Szpiegostwo (głownie przemysłowe) zmierza do skrytego zdobycia informacji i wykorzystaniu ich w grze konkurencyjnej na rynku lub do osiągnięcia przewagi operacyjnej na polu biznesowym. Cyberataki tego rodzaju zwykle są przygotowane i wymierzone (*targeted*) w konkretny system. Zdobycie możliwości sterowania zdalnego obiektami automatyki lub finansowymi, niekoniecznie wykorzystywane niezwłocznie, jest również łakomym celem ataków APT (*Advanced Persistent Threats*). W tej sytuacji wśród metod cyberobrony powstaje pole do wykorzystania dezinformacji ([10], [2]) – tak jak to się dzieje w przypadku bardziej kinetycznych sposobów walki. ***Deception*** – oszukiwanie w obronie ([2],

[3], [7], [13], [18], [19]), jest właściwie elementem bardziej walki informacyjnej niż zabezpieczeniem systemów teleinformatycznych. To „oszukiwanie" nie ogranicza się wyłącznie zasobów informacyjnych, ale również obejmuje pozorowanie stanu i siły zabezpieczeń. Ogólna idea, podobnie jak w walce wywiadów, polega na stwarzaniu pozorów słabości tam, gdzie obrona jest silna i zniechęcaniu pozorami siły w słabych punktach.

Systemy infrastruktury krytycznej, wojskowe lub systemy korporacyjne zawierające szczególnie wrażliwe dane mogą wykorzystywać ten sposób działania dla wprowadzenia w błąd przeciwnika.

W pewnych sieciach (np. wojskowych [14], [6], [12]) spodziewana jest dopuszczalność (a nawet preferencja) „cichej reakcji" na incydenty. W przeciwieństwie do tradycyjnych systemów, w razie ataku zamiast blokowania ataków teleinformatycznych, w większości przypadków korzystniejsze będzie zapewne stwarzanie pozorów słabości i/lub podatności; takie postępowanie pozwoli na śledzenie poczynań napastnika i prowadzenie działań dochodzeniowych, przesyłanie napastnikowi fałszywych informacji, a przede wszystkim upewnienie napastnika, że dysponuje skuteczną bronią. Taka broń użyta w warunkach kryzysowych, zawiedzie: zostanie niezawodnie rozpoznana jako atak i będzie mogła być skutecznie blokowana.

Dla wielu organizacji interesującym chwytem jest wykorzystanie skutecznego ataku zdalnego napastnika do podsunięcia mu fałszywych informacji, prowokujących go do działań wbrew własnym interesom a na korzyść pozornie poszkodowanej w teleinformatycznym ataku strony. Tak osiągane korzyści mogą dać korzyści nierównie większe od strat czy kosztów związanych z samym atakiem i to korzyści leżące na zupełnie innych polach operacyjnych niż teleinformatyka. Skutki podsunięcie konkurencji spreparowanych planów finansowych lub po prostu projektu oferty w najbliższym przetargu podobnie jak podsunięcie potencjalnemu przeciwnikowi fałszywych planów mobilizacyjnych czy operacji, mogą być nie do przecenienia. Z punktu widzenia organizacji-dysponenta systemu teleinformatycznego na liście priorytetów reakcji na ataki – dezinformacja powinna być przed blokowaniem: pozorny sukces napastnika pozwala na podsuwanie mu informacji o dużym dlań stopniu wiarygodności. Uprzedzić należy, że wprowadzenie i utrzymywanie tego rodzaju mechanizmu wydaje się stosunkowo drogie – trzeba permanentnie utrzymywać alternatywną wersję wielu informacji („wirtualny świat") i zapewniać jej prawdopodobieństwo, w tym i zmienność w czasie.

Technicznie rzecz biorąc, podsuwanie napastnikowi fałszywych informacji jest tylko jednym ze sposobów ochrony własnych zasobów teleinformatycznych przed atakami za pomocą oszukiwania/wprowadzania w błąd potencjalnych napastników. Chociaż początki takich technik datują się na lata dziewięćdziesiąte (szkice historyczne zawierają opracowania [18], [17] i [2]), to istotne zmiany w podejściu do użycia zwodzenia w cyberobronie można odnotować od drugiej

dekady obecnego wieku. W szczególności elementy oszukiwania napastnika stają się częścią systemu zabezpieczeń organizacji, co więcej – podlegają ciągłemu doskonaleniu i utrzymywaniu w stanie aktualności. Tendencję tę ilustruje analiza Gartnera [15]. Znacznie szersze omówienie problematyki fałszowania obrazu rzeczywistości – ukrywanie, zniekształcanie i stwarzanie pozorów – nie tylko w obronie, ale i w ataku przedstawiono w pracy [13]. W przeciwieństwie do klasycznych skomplikowanych zabezpieczeń, które mają na celu reagowanie na cyberataki, by jak najszybciej izolować napastnika od jego celu, metody zwodzenia pozwalają też na tzw. podejście „proaktywne" – pozwalając napastnikowi na działanie m.in. dla zebrania o nim i jego metodach użytecznych informacji.

1.1. Wybrane pojęcia

W literaturze przedmiotu autorzy używają różnych pojęć związanych z technikami zwodzenia napastnika, bardziej nawet w zależności od roku publikacji niż tematu opracowania. Granice znaczeniowe nieco się zacierają – zbiory desygnatów wymienionych poniżej pojęć nie są rozłączne.

Honeypot – pułapka, zasób teleinformatyczny, z jakichś powodów atrakcyjny dla napastnika. W najprostszym przypadku dostęp do takiego zasobu traktowany jest jako podstawa do wzniesienia alarmu. Zwykle wyróżnia się honeypoty nisko- i wysokointeraktywne. Niskointeraktywne, tzw. statyczne honeypoty służą zwykle po prostu jako detektory działań niepożądanych, zaś wysokointernaktywne symulują działanie rzeczywistych urządzeń i pozwalają na śledzenie działań napastnika. Szeroką klasyfikację, sposoby stosowania i cechy honeypotów zaprezentowano w pracy [2].

Honeynet – to całościowy system pułapek, ze względów bezpieczeństwa lub dla uzyskania większego podobieństwa do symulowanego systemu złożony jest z większej liczby urządzeń. Pierwszą sieć honeypotów opracowała w 1999 r. Honeynet Project, organizacja non-profit poświęcona poprawie bezpieczeństwa internetowego. Te systemy zostały zaprojektowane do celowego angażowania i oszukiwania napastników, aby lepiej zrozumieć ich taktykę i sposób działania. Wykorzystywane są również dla stwarzania fałszywych obrazów struktury sieci napastnikom i wykrywania wrogich działań już we wstępnej fazie – skanowania ([1], [4]).

Decoy – atrapa (cel pozorowany) to ([18]) całościowy system lub usługa oprogramowania, która stanowi atrakcyjny cel napastnika. Zwykle pozoruje sieci produkcyjne zawierając jednak fałszywe dane oraz znane podatności.

Bait – przynęta to ([18], [5]) zwykle niewielkie fałszywe dane, atrakcyjne dla napastnika – najczęściej dane uwierzytelniające. Dostęp do przynęty lub jej użycie stanowią podstawę wykrycia ataku.

Lure – wabik to ([18]) elementy sprawiające, że przynęty są bardziej atrakcyjne niż zasoby sieci produkcyjnej. Pozorowanie szczególnie atrakcyjnych danych lub ustawień fabrycznych zasobów to typowe wabiki.

Breadcrumbs – wewnętrzne odsyłacze (*links*) w sieci organizacji mogą zostać ustawione tak, aby wskazywać na honeypoty ([18]). W przypadku uchwycenia przez napastnika przyczółków (*pivot points*) w sieci, istnieje znaczne prawdopodobieństwo, że w trakcie rozpoznawania otoczenia napastnik będzie kierował się wskazaniami lokalnych odsyłaczy.

Ustaliło się rozumienie honeypotów jako oddzielnych urządzeń komputerowych lub prostych systemów teleinformatycznych z jednym serwerem. Dla nadzorowanych zasobów informacyjnych pełniących funkcję pułapek w systemach przyjęła się nazwa honeyfiles [20].

1.2. Rozwiązania rynkowe

Honeypoty są obecnie najbardziej dojrzałym spośród rozwiązań klasy „*deception*". W opracowaniu ENISy [9] przedstawiono stan sztuki na rok 2012 w zakresie klasycznych, detekcyjnych honeypotów oraz ich kluczowych przedstawicieli na rynku. System Arakis [4] jest uznanym systemem wczesnego ostrzegania o nowych zagrożeniach, który rozwinął się od sieci honeypotów przeznaczonych do rozpoznawania automatycznych ataków oportunistycznych. Analiza Gartnera [15] prezentuje pogląd, że chociaż honeypoty w cyberobronie są użyteczne, honeypot jest skutecznie wykorzystywany przede wszystkim w celu wykrywania (i rozpoznania) działań, a nie opóźniania lub zakłócania działań atakującego. Inaczej mówiąc realizuje raczej funkcje detekcyjne i rozpoznawcze, niż obronne. Rozwiązania honeynet dają więcej możliwości w obronie ([7], [1]).

Nowe rozwiązania ([15]), obejmujące całościowe zabezpieczenia sieci firmowych w znacznej części oparte na technikach zwodzenia (*deceptions*) są oferowane m.in. przez: Illusive Networks[1], XTrap Security[2], a przede wszystkim Attivo Networks[3]. *Deceptions* są integralnym elementem całościowych rozwiązań zabezpieczeń oferowanych przez np. TopSpin Security[4] i GuardiCore[5]. Interesującym rozwiązaniem, opartym na rozpoznawaniu zachowań użytkowników jest oferta firmy Allure[6] (*The Novo Platform*). Szczegóły

[1] https://www.illusivenetworks.com/
[2] https://trapx.com/product/
[3] https://attivonetworks.com/product/deception-technology/
[4] https://www.topspinsec.com/solutions/
[5] https://www.guardicore.com/product/why-guardicore/
[6] https://www.alluresecurity.com/novo/

rozwiązań z tej dziedziny są zazdrośnie strzeżone, chociaż niektóre z nich są chronione patentami (np. [16]), co wymaga publikacji opisów.

Należy podkreślić, że systemy zabezpieczeń wykorzystujące zwodzenie przeciwnika nawet jeśli pozwalają na podsuwanie mu fałszywych informacji operacyjnych w spreparowanych danych (kampanie dezinformacyjne), to nie poświęcają tej możliwości znaczącej uwagi. Przyczyną jest **brak bezpośredniego sprzężenia zwrotnego – wpływu takich przedsięwzięć na** tradycyjnie definiowane bezpieczeństwo systemu i oczywiście na **mierniki** owego **bezpieczeństwa**, niezależnie od tego, jak definiowane. Warto także zauważyć, że organizacje państwowe decydujące się na wdrożenie rozwiązań dezinformacyjnych niechętnie godzą się na stosowanie systemów zabezpieczeń o zamkniętym kodzie i bliżej nieznanych rozwiązaniach, a szczególnie wymagających wsparcia on-line przez producenta.

1.3. Pewne doświadczenia z 2009 roku

W jednym z przedsięwzięć[7] w 2009 r. rozważano elementy reakcji pozwalające na realizację zbiegów dezinformacyjnych ([14], [8]). W uproszczeniu sformułowane wówczas wnioski do implementacji były następujące ([8]):

1. Realizacja najprostszej „cichej reakcji" polegająca na pozorowaniu słabości (np. drogą wyłączania niektórych reguł w filtrach sieciowych) technicznie nie stanowi żadnego problemu w przypadku filtrów o dynamicznych zbiorach reguł.
2. Realizacja przekierowania ruchu sieciowego „w locie", polegająca na przełączaniu w tryb podstawiania fałszywej informacji w strumień ruchu w niskich warstwach modelu ISO/OSI została oceniona jako problematyczna, głownie z powodu trudności technicznych w implementacji.
3. Realizacja podstawiania fałszywych informacji w warstwie aplikacji została oceniona jako implementacyjnie najłatwiejsza, ale wymagająca projektowania aplikacji od początku z możliwością realizacji tej funkcji.
4. Dla aplikacji webowych można wskazać rozwiązanie pośrednie, polegające na włączeniu do sieci tuż przed podstawowym serwerem specjalizowanego serwera proxy, który może przejść (na sygnał ze sterowania) w tryb przesyłania fałszywej informacji na zapytania np. z pewnych adresów IP.

Należy jednak zwrócić uwagę, że te wnioski formułowano dla pewnej specyficznej klasy systemów teleinformatycznych.

Na uwagę zasługuje punkt 2 oraz 3. Wspomniany w ostatnim punkcie dla aplikacji webowych model proxy, nasuwa myśl o zastosowaniu modelu takiego

[7] PBZ–MNiSW–DBO–02/I/2007 *Zaawansowane metody i techniki tworzenia świadomości sytuacyjnej w działaniach siecio-centrycznych.*

rozwiązania np. w niskich warstwach dostępu do zasobów dyskowych, To nic innego jak odpowiednik ataku MITM (*man-in-the-middle*) pozwalającego na selektywne fałszowanie informacji – w tym przypadku w zależności np. od numeru procesu generującego żądanie dostępu do dysku.

2. „Cicha reakcja" – system produkcyjny jako rodzaj honeypota

Klasyczne reakcje systemów zabezpieczeń w produkcyjnych systemach teleinformatycznych zmierzają do jak najszybszego zablokowania możliwości oddziaływania zdalnego napastnika na atakowane zasoby. W typowym do niedawna podejściu polegającym na obronie granic, kluczową rolę odgrywają różnego rodzaju filtry ruchu sieciowego, blokującego dostęp agresywnego ruchu do zasobów-celów w chronionym systemie, a najlepiej w ogóle do wnętrza systemu. Idealnym przypadkiem jest blokowanie ruchu już na routerach brzegowych. Obecnie, w dobie rozwiązań chmurowych i rozpraszania usług, taka, tzw. ochrona perymetryczna, jest uznawana za niewystarczającą (por. [15]).

Cechą szczególną „cichej reakcji" jest powstrzymywanie się systemu zabezpieczeń od działań dostrzegalnych dla napastnika. W przypadku honeypotów taki sposób reagowania jest podstawą działania – po detekcji ataku prowadzona jest obserwacja i logowanie działań napastnika. W przypadku systemów produkcyjnych takie zachowanie uznawane jest jednak zwykle za niebezpieczne. Istnieje możliwość włączenia zalet honeypotów (i rozwiązań *honeyfiles*) przez wprowadzenie dynamicznie włączanej funkcji honeypot/honeyfiles do systemów produkcyjnych. Polega ona **wprowadzeniu „cichej reakcji" polegającej na powstrzymaniu się od blokowania dostępu do systemu, a w zamian na usunięciu wrażliwych zasobów z pola oddziaływania napastnika i udostępnieniu w ich miejscu spreparowanych zasobów, nieodróżnialnych dla napastnika od prawdziwych, ale pozbawionych cech wrażliwości z punktu widzenia atakowanej organizacji**. Działania „podmiany" zasobów powinny zostać podjęte jako reakcja systemu zabezpieczeń na wykrycie ataku. Umożliwia to zachowanie funkcji poznawczych honeypota a ponadto osiągnięcie możliwości dezinformacji przeciwnika. Dotyczy to zarówno zwodzenia (*deception*) napastnika co do cech atakowanego systemu teleinformatycznego (w tym jego słabości i zabezpieczeń), jak i ewentualnej kampanii dezinformacyjnej wymierzonej w napastnika na poziomie operacyjnym działania dysponenta atakowanego systemu (*disinformation*).

Rozwiązanie integrujące dynamicznie włączane pliki detekcyjne (*honeyfiles*) do systemu zabezpieczeń pozwala na wykrywanie prób przekroczenia uprawnień (oraz w ogólności podejrzanych zachowań) przez operatorów, którzy przeszli uwierzytelnienie w systemie i zostali uznani za legalnych użytkowników. Ten mechanizm detekcji pozwala na zastosowanie

„cichej reakcji" w odniesieniu do tzw. „*insiders*", czyli legalnych użytkowników zwerbowanych przez przeciwnika oraz operatorów posługujących się wykradzionymi lub odgadniętymi danymi uwierzytelniającymi. Także wrogie działania takich, pozornie legalnych, operatorów mogą wyzwalać proponowane mechanizmy: skryte przełączenie wrażliwych zasobów na ich spreparowane „bezpieczne" odpowiedniki, a następnie monitorowanie działań użytkowników. Szczególnie istotna jest możliwość dopasowania podmienianych zasobów na inne do konkretnych napastników lub pewnych typów według zadanych opisów („profili") napastnika. Dla różnych napastników można podmieniać różne zasoby według potrzeb dla osiągnięcia:

a) możliwie skrytego działania na poziomie taktycznym;
b) celów kampanii dezinformacyjnej na poziomie operacyjnym.

Istotną cechą tak rozumianej „cichej reakcji" jest podsuwanie potencjalnym napastnikom fałszywych informacji w spreparowanych danych i utwierdzanie ich w przekonaniu o prawdziwości tych informacji. W szczególności nawet przeprowadzone po pewnym czasie zablokowanie ataku – dla napastnika stanowiące rodzaj ostrzeżenia – nie powinno wzbudzić wątpliwości co do prawdziwości danych, a ponadto nie powinno sugerować wykrycia wycieku tych danych. Wykrycie wycieku danych zwykle obniża ich wartość dla napastnika, gdyż należy oczekiwać od właściciela podjęcia działań dla minimalizacji start dezaktualizujących te dane.

2.1. Zasoby zastępcze i ich treść

Spreparowanie danych zawierających fałszywe informacje operacyjne organizacji jest przedsięwzięciem trudnym, w szczególności, gdy ma zwieść przeciwnika dysponującego aparatem wywiadowczym pozwalającym ich weryfikację – duże korporacje lub państwa. Ponadto fałszywe dane powinny być ciągle aktualizowane i zwykle stanowić alternatywę do swoich „prawdziwych" odpowiedników, co gorsza powinny znajdować się w miejscach, w których poszukiwane będą prawdziwe dane. Zatem ich pożądane cechy to:

- aktualność,
- podobieństwo do oryginałów,
- lokalizacja w tych samych (!) miejscach w topologii systemu co oryginały,
- w przypadku danych, których ujawnienie mogłoby być szkodliwych wizerunkowo, posiadanie przez nie cechy „ukrytej oczywistej zaprzeczalności".

Ponadto wdrożenie zasobów zastępczych powinna cechować tajność wdrożenia posunięta do granic paranoi i akceptowalne koszty przedsięwzięcia. Znaczenie mają także późniejsze ciągłe koszty utrzymania.

Spreparowanie takich danych to zajęcie dla specjalistów nie należących do zespołu IT obsługującego system, w którym te dane zostaną umieszczone. Ponadto powinni to być specjaliści z dziedziny, której dotyczą preparowane informacje w owych danych zawarte. Zapewne samo **istnienie takiego zespołu powinno być znane tylko niewielkiej grupie pracowników** cyberbezpieczeństwa.

Ogólna zasada działania systemów „cichej reakcji" powinna być następująca: każdy z operatorów/użytkowników ma dostęp do niezbędnych mu zasobów wrażliwych do chwili detekcji ataku, kiedy to wrażliwe dane zostają skrycie zastąpione danymi fałszywymi. Tę zasadę można wzmocnić, uznając, że **prawdziwe dane dostępne są tylko od chwili przeprowadzenia procedury uwierzytelnienia do chwili utraty zaufania** (np. wykrycia działań nieuprawnionych).

2.2. Dyskusja możliwości rozwiązań

Możliwym rozwiązaniem może być zbudowanie podwójnego systemu – jednego produkcyjnego, zawierającego dane prawdziwe oraz drugiego, równoległego, zawierającego dane spreparowane. Całość powinna zostać wyposażona w mechanizm detekcji, który kierowałby użytkownika do obsługi przez system produkcyjny, zaś napastnika do honeynetu. Główny problem kryje się oczywiście w „mechanizmie detekcji", który musiałby a priori rozpoznawać napastnika i kierować jego ruch do obsługi przez honeynet. Niestety, mechanizmy detekcji w warstwie aplikacji nie powalają na takie rozpoznawanie: przełączanie może nastąpić najwcześniej po zalogowaniu się użytkownika. Ponadto, w przypadku dopuszczenia ataków realizowanych przez autoryzowanych użytkowników, sposobem wykrycia ataku może być właśnie próba dostępu do danych zawierających informacje niespełniające zasady „wiedzy koniecznej" dla tych użytkowników. To po prostu detekcja działań niepożądanych (lub nadużycia danych uwierzytelniających) na podstawie zachowania się (*behawior*) użytkownika. Ten sposób detekcji wymaga dodatkowego udostępnienia użytkownikom danych, których zawartość informacyjna wykracza poza zakres niezbędny do wykonywania ich pracy. Próba dostępu do takich danych detekcyjnych (*honeyfile*) może oznaczać, że nastąpiło przejęcie danych uwierzytelniających legalnego użytkownika i „incydent w toku": trwający atak wydobywania danych z podszywaniem się pod tego użytkownika. W takim przypadku przełączenie użytkownika do wirtualnego świata honeynetu powinno nastąpić niezwłocznie, ale niedostrzegalnie dla użytkownika. Należy zwrócić uwagę, że przełączenie nastąpiłoby w trakcie trwania zdalnej sesji. Przy następnym próbach logowania tego użytkownika powinien on być natychmiast kierowany do honeynetu. Wykonanie takiego przełączenia z systemu

produkcyjnego do oddzielnego honeynetu w trakcie zdalnej sesji niedostrzegalnie dla napastnika nie wydaje się technicznie możliwe.

Nic nie stoi na przeszkodzie, by detekcyjne dane (*honeyfiles*) były zasobami fałszywymi. Ale takie rozwiązanie oznacza obecność w systemie produkcyjnym danych zarówno prawdziwych, jak i sfałszowanych i prezentowanie ich różnych kombinacji dla różnych użytkowników w zależności od tego, jakie zadania wykonują użytkownicy i jakie dane są do owych zadań konieczne, a które pełnią rolę danych detekcyjnych. Skoro i tak dopuszcza się przenikanie napastników do systemu produkcyjnego oraz obecność w tym systemie alternatywnych danych detekcyjnych, zintegrowanie funkcji dynamicznego honeynetu z systemem produkcyjnym wydaje się rozsądne. Oznacza to, że system produkcyjny powinien użytkownikom udostępniać zasoby prawdziwe, zaś po wykryciu ataku niektóre zasoby powinny być zastępowane w widoku napastnika swoimi wirtualnymi odpowiednikami. Te zasoby to oprócz spreparowanych danych wszelkie zasoby symulujące normalną pracę systemu, ale bez ryzyka wystąpienia szkodliwych skutków działań napastnika. Przez „normalną pracę" należy rozumieć również działanie mechanizmów ochrony – zabezpieczeń. Napastnik miałby powody do podejrzeń, gdyby nie napotkał żadnej reakcji na swoje działania.

Typowe obecnie zintegrowane systemy zabezpieczeń opisywane są przez swoje funkcje detekcyjne, obejmujące[8]: zarządzanie logami, korelację zdarzeń, rozpoznawanie dostępu do zasobów, identyfikację podatności, sieciowe i komputerowe IDS (*Intrusion Detection Systems, NIDS i HIDS*), monitorowanie integralności plików, nadzór nad ruchem sieciowym. Zwykle reakcje to natychmiastowe generowanie dla zapór sieciowych dynamicznych reguł blokujących dostęp napastnika, blokowanie powołanych przez niego procesów i alerty do obsługi technicznej. W systemie z „cichą reakcją" można użyć każdej z tych funkcji detekcyjnych i reakcji, dodając jedną zasadniczą reakcję – zastąpienie wybranych wrażliwych zasobów ich atrapami. To pozwala na realizację nowych funkcji:

- funkcji honeypota: monitorowanie działań napastnika;
- funkcji dezinformacji: podsuwanie napastnikowi sfałszowanych informacji na poziomie operacyjnym.

Rozwiązaniem systemu zabezpieczeń pozwalającym spełnić postulat daleko posuniętej tajności jest rozdzielenie klasycznych funkcji honeynetu od funkcji dezinformacji – podsuwania fałszywych danych – oraz powierzenie ich realizacji i obsługi oddzielnym zespołom pracowników. To pozwoli zachować w tajemnicy tę drugą funkcję.

[8] Por. Compare the AlienVault® Approach to Traditional SIEM, AlienVault 2017. https://www.alienvault.com/resource-center/white-papers/usm-vs-siem-alienvault

W praktyce realizacja techniczna systemu z „cichą reakcją" oznacza wyposażenie systemu produkcyjnego w zabezpieczenia o standardowych funkcjach detekcyjnych, natomiast standardowe reakcje powinny być opóźnione. Za to od chwili wykrycia niepożądanych działań należy napastnikowi prezentować fałszywe zasoby informacyjne oraz chronić przed jego działaniami własne zasoby. Formalnie – chroniona powinna być integralność zasobów informacyjnych, dostępność zaś utrzymywana w rozsądnych granicach. Dla utrzymania napastnika w nieświadomości wykrycia jego działania może zostać poświęcona tajność niektórych zasobów. Nieuniknione jest ujawnienie zasobów otwartych przez napastnika przed wykryciem jego działań, ujawnienie innych, niesfałszowanych zasobów powinno być podyktowane rachunkiem strat i zysków kampanii dezinformacyjnej. Ponieważ napastnik zapewne będzie zmieniał treść niektórych zasobów, zabiegi związane z utrzymaniem integralności tych zasobów nie mogą ani powodować zmian już widzianych przezeń treści, ani blokować dostępu do tych zasobów. To wymaganie jest istotne nie tylko dla funkcji dezinformacyjnych, ale również i dla funkcji rozpoznawczych (badania modus operandi napastnika) systemu. Od chwili detekcji poczynione przez napastnika modyfikacje takich zasobów powinny odbywać się na ich chwilowych kopiach. Dla utrzymania integralności chronionych zasobów musi jednak istnieć także możliwość wycofania zmian wprowadzonych przez napastnika **przed** chwilą wykrycia ataku.

Sposobem na techniczną realizację elastycznego udostępniania spreparowanych zasobów i opóźniania zapisu jest wykorzystanie piaskownicy (*sandbox*).

2.3. Piaskownice

Pomijając spodziewane problemy zarządzania działaniami ochronnymi, ideę wdrożenia „cichej reakcji" w warstwie aplikacji można w uproszczeniu przedstawić jako wywoływanie wszelkich procesów użytkowników w piaskownicach (*sandboxes*). Dla ilustracji można przedstawić działanie każdej takiej piaskownicy podobne do działania popularnej aplikacji Sandboxie[9] z katalogiem różnicowym. Katalog różnicowy jest strukturą podkatalogów odpowiadającą systemowi plików systemu. Jeśli w katalogu różnicowym istnieje jakiś plik, to przesłania on swój odpowiednik z katalogu systemowego – odwołania następują do zasobu z katalogu różnicowego. Jakikolwiek zapis dotyczy wyłącznie katalogu różnicowego – w razie potrzeby tworzona jest w nim kopia modyfikowanego zasobu z systemu plików. Ten sposób postępowania chroni integralność zasobów systemu, wszelkie zmiany zbierając w katalogu różnicowym. W dowolnym momencie można dokonać tzw. przywracania, zapisując wybrane zmienione

[9] https://www.sandboxie.com/HowItWorks

zasoby z katalogu różnicowego na ich miejsce w systemie. Możliwe są również inne manipulacje zmienionymi zasobami z piaskownicy.

Ideę wykorzystania takiej piaskownicy w systemie z „cichą reakcją" można przedstawić następująco:

- Na początku piaskownica startuje z pewną wartością początkową katalogu różnicowego, w której mogą znajdować się liczne spreparowane zasoby (pliki). Z punktu widzenia procesu w piaskownicy, pliki z katalogu różnicowego zastępują odpowiednie pliki znajdujące się w systemie.
- W trakcie procedury uwierzytelniającej użytkownika, w przypadku powodzenia, następuje przełączenie do oddzielnej, przypisanej mu piaskownicy, w której w katalogu różnicowym nie występują pliki, które powinny być widziane przez tego użytkownika w oryginale (pliki leżące poza zakresem wiedzy koniecznej mogą pozostać spreparowane).
- W przypadku wykrycia niepożądanych działań użytkownika, do katalogu różnicowego zostają wprowadzone liczne spreparowane pliki (zapewne poza tymi, do których wcześniej uzyskał dostęp) chroniące przed dostępem wrażliwe zasoby systemu.
- Po zakończeniu działania użytkownika, z piaskownicy zostają „przywrócone" pliki według pewnych ustalonych zasad. Najprościej – jeśli nie wykryto symptomów działań niepożądanych przywracana jest cała zawartość katalogu różnicowego, zaś jeśli wykryto atak takie przywracanie nie występuje. Zawartość piaskownicy można pozostawić do przyszłych badań i analizy przez zespół bezpieczeństwa, jeśli istnieją do tego przesłanki, takie jak działania podejrzane i/lub nietypowe.

Naszkicowane tu rozwiązanie może być rozbudowane i reagować na sygnały alarmowe od mechanizmów detekcji analizujących zdarzenia w niższych niż aplikacyjna warstwach. Nawet zresztą w przypadku pozostania tylko w warstwie aplikacji, demon wywołujący nowe procesy powinien mieć możliwość identyfikacji wywołań i wyboru różnych (w tym już istniejących) piaskownic, gdyż napastnik może wracać do systemu bez logowania, w tym również wykorzystując wprowadzone przez siebie nieautoryzowane furtki tzw. *backdoory*. Przez „piaskownicę" w tym kontekście rozumie się przede wszystkim pewną zawartość katalogu różnicowego. Należy zauważyć, że „zmiana piaskownicy" w przypadku rozpoznania, że aktualna komunikacja pochodzi od użytkownika/napastnika innego niż zakładany, sprowadza się do uzupełnienia katalogu różnicowego treścią piaskownicy (zasobami/plikami) specjalnie przygotowaną na takie okazje lub przechowywaną z poprzedniego jego połączenia.

Przedstawione rozwiązanie udostępnia łatwe podmienianie widzianych przez zdalnego użytkownika zasobów oraz ochronę integralności zasobów informacyjnych systemu. Wymaga jednak zbudowania dodatkowych

mechanizmów zarządzających piaskownicami i wykrywających połączenia od napastników działających w przeszłości. Jednym z prostszych rozwiązań problemu obsługi „powracającego napastnika" jest założenie „jednego ataku na raz" i rozpoczynanie każdego nowego procesu w kopii piaskownicy napastnika, z natychmiastową zmianą na stan neutralny po rozpoznaniu innego użytkownika.

Po zidentyfikowaniu ataku można byłoby wygenerować, na podstawie zawartości piaskownicy, kopię atakowanego hosta na maszynie wirtualnej i przerzucić na tę maszynę ruch od napastnika, wymaga to jednak skomplikowanych rozwiązań technicznych działających w niższych warstwach stosu ISO/OSI (w szczególności w warstwie drugiej). W przypadku zaawansowanych ataków APT (*Advanced Persistent Threats*), gdy w atakowanym systemie osadzony zostaje kod wykonywalny przeznaczony do długotrwałej akcji szpiegowskiej, opłacalne może być „ręczne" dobudowanie honeypota – zapewne przez zwirtualizowanie systemu komputera, w którym nastąpiło osadzenie się wrogiego kodu. Jeśli połączenia z tym kodem nie są realizowane w trybie połączeń zwrotnych („*reverse*" TCP lub UDP) takie rozwiązanie będzie wymagało należytego przekierowywania przychodzącego ruchu sieciowego.

Ogólnie w postępowaniu z piaskownicami można przyjąć jedną z dwóch następujących strategii:

a) w systemie zasoby prawdziwe, zaś w piaskownicy zasoby wybrane zasoby spreparowane; ten sposób pozwala na umieszczanie w piaskownicy danych detekcyjnych ze zmienionymi prawami dostępu;
b) wszystkie zasoby w systemie są spreparowane, zaś w piaskownicy użytkownika umieszczone są „zasoby konieczne" użytkownika (przywracane z piaskownicy na koniec sesji).

W każdym przypadku zasoby prawdziwe, spreparowane i detekcyjne powinny być określane przez pewien zbiór opisu nazwany „profilem użytkownika/operatora". Po zakończeniu sesji użytkownika lub w wybranych momentach sesji można dokonywać zabiegu „przywracania" (czyli synchronizacji danych piaskownicy) w odniesieniu do zasobów prawdziwych. W przypadku utraty zaufania przez operatora, przywracanie zostanie zatrzymane, zaś poziom szczegółowości monitorowania (logowanie zdarzeń) zwiększony. **Strategia b) jest zdecydowanie lepsza: zapewnia ochronę zasobów wrażliwych w przypadku, gdy napastnik osiągnie uprawnienia użytkownika (lub systemu) przez włamanie**: za pomocą eksploita, a nie drogą przejścia procedury uwierzytelniania.

3. Ryzyko

Wprowadzenie „cichej reakcji" do systemu teleinformatycznego powoduje, że w przypadku niektórych działań niepożądanych – ataków lub niewłaściwych zachowań zaakceptowanych użytkowników – reakcja uniemożliwiająca napastnikowi kontynuację działania zostanie wstrzymana. To znaczne pogorszenie właściwości klasycznego modelu zabezpieczeń. Już samo opóźnienie momentu wykrycia względem początku działań napastnika daje mu czas na poczynienie szkód w chronionym systemie. W konsekwencji należy oczekiwać zwiększenia ryzyka spowodowanego działaniami niepożądanymi, dla których stosuje się „cichą reakcję". Przez ryzyko rozumie się wartość oczekiwaną strat (spowodowanych przez wybrane zdarzenia) ponoszonych przez podmiot właścicielski zasobów informacyjnych w pewnym standardowym/jednostkowym czasie. W tej chwili rozważane jest ryzyko generowane przez klasę działań niepożądanych, dla których stosuje się „cichą reakcję".

Co prawda „cicha reakcja" w klasycznym modelu oznacza usunięcie z pola oddziaływania napastnika niektórych (zapewne kluczowych) zasobów informacyjnych, ale ta ochrona nie dotyczy wszystkich zasobów. Dla zachowania maksymalnej skuteczności działań dezinformacyjnych pożądane będzie zachowanie dostępności dla napastnika takich zasobów, których niedostępność lub zmiana zawartości byłoby sygnałem alarmowym dla napastnika lub wzbudziłaby wątpliwości jego zleceniodawców. W szczególności zasoby, do których dostęp napastnik uzyskał przed chwilą detekcji, powinny pozostać dla niego niezmienione. Również te zasoby, do których treści napastnik lub jego zleceniodawcy mają dostęp z innych źródeł powinny pozostać zgodne z ich oczekiwaniami podczas weryfikacji.

Należy zauważyć, że od chwili detekcji istotne są szczególnie zagrożenia związane z tajnością (atrybutem bezpieczeństwa) atakowanych zasobów. Zagrożenia związane z ich integralnością nie są problemem dzięki wykorzystaniu piaskownic – od chwili detekcji jakiekolwiek poczynione zmiany uznane zostaną za niebyłe w chwili zakończenia interakcji z napastnikiem. Co więcej, wprowadzenie zasady działania użytkowników w piaskownicach, daje możliwość uznania na niewłaściwe i wycofania wszystkich zmian wprowadzanych przez rozpoznanego napastnika także przed chwilą detekcji.

Zagrożenie dla dostępności zasobów, a zatem i ryzyko dla rozważanej klasy zdarzeń nie powinno ulec zmianie – ataki DoS są łatwo identyfikowalne i nie należą do klasy zdarzeń, dla których znajduje zastosowanie „cicha reakcja". Wyjątkiem jest scenariusz ataku DoS zgodny w swej początkowej fazie z innymi atakami „*drive-by download*", sprowadzającymi się do wprowadzenia do atakowanego systemu kodu wykonywalnego i jego uruchomieniu. Wyróżnikiem jest główny cel działania uruchomionego kodu – uniemożliwienie dostępu do zasobów. Rozwiązanie jest proste: wprowadzenie zasady eliminacji procesów

napastnika natychmiast po wystąpieniu pierwszych objawów spadku dostępności z pewnością zredukuje ryzyko do akceptowalnej wartości.

Podsumowując – wprowadzenie mechanizmów „cichej reakcji" jako dodatek do pewnego systemu zabezpieczeń może wprowadzić zwiększone ryzyko wynikające z zagrożeń naruszeniami atrybutu tajności zasobów informacyjnych. Akceptacja tego ryzyka powinna odbywać się z dość nietypowym postępowaniem uwzględniającym nie tylko potencjalne straty, ale również potencjalne korzyści wynikające z dezinformacji przeciwnika (z obszaru operacyjnego dysponenta zasobów informacyjnych). Pewnym problemem jest to, że zespół pracowników zajmujących się utrzymaniem bezpieczeństwa teleinformatycznego (administratorów) najprawdopodobniej nie będzie zdolny do oceny tych wartości, o ile w ogóle zostanie dopuszczony do tajemnicy istnienia lub wdrożenia kampanii dezinformacyjnej.

Nowym zagrożeniem, pojawiającym się z wprowadzeniem „cichej reakcji" udostępniającej sfałszowane co do treści zasoby informacyjne, jest to, że dezinformacja dosięgnie użytkowników legalnych i wpłynie na ich działania w sposób prowadzący do działań na szkodę interesów pracodawcy. Pracownik, naruszając zasadę „wiedzy koniecznej" może sięgnąć do zasobów zawierających fałszywe informacje. Jeśli treść zasobów leżących (według organizatorów dezinformacji) poza obszarem wiedzy koniecznej do wykonywania obowiązków pracownika może jednak wpłynąć na jego decyzje biznesowe, to w konsekwencji może doprowadzić do działań gorszych niż podejmowane bez dezinformacji. Ten specyficzny „błąd drugiego rodzaju" powinien zostać uwzględniony podczas planowania dostępności fałszywych zasobów. Poza systemem automatycznych zabezpieczeń, po wykryciu dostępu pracownika do fałszywych zasobów zapewne użyteczna będzie, oprócz sprawdzenia pracownika w ramach obsługi incydentu, także analiza potencjalnego wpływu poznanych treści na działanie pracownika i w razie potrzeby podjęcie stosownych kroków. To zadanie dla ścisłego zespołu obsługującego kampanię dezinformacyjną.

4. Wybrane problemy

4.1. Problemy techniczne

Główne problemy w realizacji technicznej mechanizmów „cichej reakcji" wynikają stąd, że dla skrytego działania dezinformacyjnego działania muszą być adresowane do konkretnych napastników/użytkowników. Niekoniecznie identyfikacja tożsamości cyfrowej musi być dostateczna, by wskazać osobę, ale powinna rozpoznawać działania wykonywane przez tego samego napastnika.

Podczas interakcji z systemem napastnik może dokonywać różnych połączeń zdalnych i:

1. W każdym przypadku powinien otrzymywać spójny zestaw treści zasobów informacyjnych.
2. Nawet jeśli działania zdalne odbywają się za pomocą ruchu sieciowego interpretowanego w różnych warstwach stosu ISO/OSI, to pożądane jest przypisanie ich konkretnemu napastnikowi. W przypadku, gdy nie jest to możliwe, należy zrezygnować z „cichej reakcji".
3. Zasoby dostępne dla działań zdalnych przed zidentyfikowaniem zdalnego operatora raczej nie powinny należeć do zasobów zmiennych w zależności od użytkownika/napastnika.

Jeśli systemy wykrywające działanie niepożądane nie mają funkcji wiązania identyfikatorów z różnych warstw (adresy MAC, adresy IP, charakterystyczne cechy pakietów – tzw. *fingerprints* oprogramowania sieciowego napastnika, dane uwierzytelniające użytkownika w warstwie dostępu i w warstwie aplikacji, czy wreszcie zachowanie operatora) to może się okazać, że symptomów nie da się przypisać jednoznacznie działającemu operatorowi.

4.2. Problemy organizacyjne

Zespół planowania i utrzymywania „cichej reakcji" powinien składać się z pracowników IT, administrujących zasobami i środkami ich udostępniania, oraz pracowników organizujących kampanię dezinformacyjną, bo to jest zasadniczym celem działania mechanizmów „cichej reakcji". Utrzymanie tajemnicy jest kluczowe dla sukcesu tego zabezpieczenia, a to wymaga ograniczenia przepływu informacji między członkami zespołu. Analiza ryzyka i wyznaczenie poziomu akceptowalnego ryzyka szczątkowego w tym przypadku jest zadaniem dla ścisłego zespołu najbardziej zaufanych pracowników, gdyż tylko oni mają podstawy do oszacowania korzyści z dezinformacji oraz strat z błędów pracowników pomyłkowo uzyskujących dostęp do sfałszowanych treści. Oceny ryzyka „klasycznego" – skutków działań niepożądanych przy opóźnionej reakcji zabezpieczeń można powierzyć pracownikom pionu bezpieczeństwa nie wtajemniczonym w szczegóły.

Należy zwrócić uwagę na znaczny nakład pracy na utrzymanie aktualności systemu dezinformującego. Wynika on nie tylko stąd, że zasoby powinny zachowywać zgodność z sytuacją operacyjną podmiotu, ale również i stąd, że do kategorii zdalnych napastników mogą zostać zaliczeni także pracownicy – od momentu, gdy zostaną z ich strony wykryte niepożądane działania. Nie dość zatem, że należy opracować zasoby dezinformacyjne, to jeszcze trzeba zbudować „profile użytkowników" obejmujące także pracowników, a wskazujące które z technicznie dostępnych każdemu z nich zasobów powinny być prawdziwe. Dla każdego pracownika za zmianą zadań może zmieniać się zestaw treści należących

do „wiedzy koniecznej", a zatem i to, które z dostępnych mu do tej pory zasobów dezinformacyjnych powinny zostać zmienione na prawdziwe.

Analogiczne „profile napastników" mogą być również zróżnicowane.

5. Zakończenie

Można zaproponować uzupełnienie systemów zabezpieczeń systemów teleinformatycznych o mechanizmy dezinformacyjne – środki pozwalające osiągnięcie podobnych korzyści jak w przypadku użycia honeynetów, ale z możliwością wprowadzenia w błąd napastników przez udostępnienie im fałszywych zasobów informacyjnych.

Trudno przeprowadzić oszacowanie ryzyka takich rozwiązań, ale można wskazać, że w porównaniu do systemu bez proponowanego mechanizmu, wzrost ryzyka, jeśli wystąpi, będzie się mieścić w zaakceptowanych kosztach kampanii dezinformacyjnej. To ryzyko to wartość oczekiwana strat wynikająca z ujawnienia napastnikowi, który nie jest celem kampanii dezinformacyjnej, informacji prawdziwych, w zamierzeniu potwierdzających oczekiwanemu przeciwnikowi prawdziwość pozostałych informacji pozyskanych w trakcie ataku. Nieuniknionym zagrożeniem będzie błąd zespołu utrzymującego system „cichej reakcji" powodujący niezamierzone ujawnienie informacji prawdziwych lub błąd powodujący niezamierzoną prezentację legalnemu użytkownikowi informacji sfałszowanych zamiast niezbędnych do poprawnego działania. To odpowiedniki błędów miskonfiguracji w klasycznych systemach zabezpieczeń.

Systemy „cichej reakcji" mogą okazać się szczególnie owocne przeciw atakom wewnętrznym, czyli niepożądanym działaniom podejmowanym przez pracowników – legalnych użytkowników. Dają one możliwość płynnego przełączenia na fałszywe zasoby, czyli włączenie w funkcji honeypota, natychmiast detekcji bez wzbudzania podejrzeń zdalnego operatora, co w klasycznym honeypocie jest nieosiągalne.

Dodanie funkcji „cichej reakcji" do pewnego systemu zabezpieczeń wymaga rozwiązania typowego dla takich systemów problemu: wiązania sygnalizacji detektorów pracujących w różnych warstwach z napastnikiem. Symptomy zdarzeń niepożądanych mogą zostać wykryte drogą analizy ruchu sieciowego i oddziaływania na system w różnych warstwach modelu ISO/OSI, więc i cechy identyfikujące napastnika będą właściwe dla tych warstw. System „cichej reakcji" dla skutecznego działania potrzebuje informacji czy, i który z działających operatorów/użytkowników utracił zaufanie i należy prezentować mu fałszywe dane. Należy zatem się spodziewać, że do implementacji „cichej reakcji" najlepszy będzie system zabezpieczeń, którego zasadniczą część stanowić będzie system SIEM. Na podstawie raportu Gartnera [11] można

wnioskować, że Splunk[10] i AllienVault[11] są najlepszymi kandydatami, chociaż sposób licencjonowania, wymagający w przypadku Splunk połączenia sieciowego z producentem może okazać się nie do zaakceptowania dla niektórych właścicieli systemów.

Obiecującym rozwiązaniem technicznym systemów „cichej reakcji" na poziomie urządzenia komputerowego wydaje się wykorzystanie systemu piaskownic. Pozwoli on na mocną ochronę atrybutu integralności chronionych zasobów, obejmującą także czas sprzed zidentyfikowania działań niepożądanych podejmowanych przez napastników.

Podsumowując – systemy „cichej reakcji" spiszą się w obronie lepiej niż oddzielne honeypoty, dostarczając jednocześnie dużych możliwości dezinformowania napastników i ich zleceniodawców. Niestety należy oczekiwać znacznych kosztów związanych z przygotowaniem i utrzymaniem aktualności treści zasobów niezbędnych w kampanii dezinformacyjnej. Zakonspirowany zespół realizujący to zadanie powinien składać się raczej ze specjalistów z dziedziny działalności operacyjnej organizacji-celu, niż teleinformatyki.

Należy zwrócić uwagę na to, że klasyczna, wąska definicja ataku zdalnego: „celowe oddziaływanie napastnika za pomocą ruchu sieciowego na systemy informatyczne ofiary prowadzące do skutków potencjalnie szkodliwych dla interesów ofiary" zmienia sens w przypadku użycia w obronie „cichej reakcji". Napastnik osiąga swe taktyczne cele, np. zdobywając dostęp do zasobów informacyjnych, ale to zatruty owoc – wykorzystanie fałszywych danych doprowadzi do skutków niekorzystnych dla niego, a nie ofiary. Zatem role napastnika i ofiary się zamieniają. Im dłużej napastnik pozostaje nieświadomy tego faktu, tym większy sukces obrońcy. Interesującą okolicznością jest to, że w przypadku większości wrażliwych zasobów informacyjnych, napastnik (lub jego zleceniodawca) jest również zainteresowany tym, aby fakt jego dostępu do tych zasobów pozostał tajemnicą, gdyż w jego przekonaniu zmniejszy to szanse podjęcia przez ofiarę kroków dezaktualizujących pozyskane przez napastnika treści. To z kolei zmniejsza możliwości weryfikacji tych treści.

Literatura

[1] ACHLEITNER S., LA PORTA T., MCDANIEL P., SUGRIM S., KRISHNAMURTHY S.V., CHADHA R., *Cyber Deception: Virtual Networks to Defend Insider Reconnaissance*. MIST'16 Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, October 28, 2016, Vienna, ACM 2016, pp. 57-68.

[10] https://www.splunk.com/
[11] https://www.alienvault.com/

[2] ALMESHEKAH M.H. SPAFFORD E.H., *Cyber Security Deception*. [In]: JAJODIA S. et al. (eds.), *Cyber Deception*. Springer International Publishing Switzerland, 2016, pp. 25-52.

[3] ALMESHEKAH M.H., SPAFFORD E.H., *Planning and Integrating Deception into Computer Security Defenses*. [In]: Proceedings of the 2014 New Security Paradigms Workshop. ACM, NY 2014, pp. 127-138.

[4] *ARAKIS-GOV*. CERT Polska 2017. http://www.arakis.pl/pl/ews/ (dostęp 28.08.2017)

[5] BOWEN B.M., HERSHKOP S., KEROMYTIS A.D., STOLFO S. J., *Baiting Inside Attackers Using Decoy Documents*. Security and Privacy in Communication Networks. 5th International Conference on Security and Privacy in Communication Systems SecureComm, 2009, pp. 51-70.

[6] CLIMEK D., MACERA A., TIRENIN W., *Cyber Deception*. Journal of Cyber Security and Information Systems, Vol. 4, No. 1, CSIAC, 2016, pp. 14-17.

[7] COLE E., *Deception Matters: Slowing Down the Adversary with illusive networks.* A SANS Product Review. SANS™ Institute. May, 2017.

[8] DWORAKOWSKI W., GOLEŃ P., *Specyfikacja informacyjno-funkcjonalna modelu mechanizmów reagowania w systemie bezpieczeństwa domeny koalicyjnej*. PBZ–MNiSW–DBO–02/I/2007. Zaawansowane metody i techniki tworzenia świadomości sytuacyjnej w działaniach sieciocentrycznych, WIŁ, Zegrze, 2009.

[9] GRUDZIECKI T., JACEWICZ P., JUSZCZYK Ł., KIJEWSKI P., PAWLIŃSKI P., *Proactive Detection of Security Incidents. Honeypots*. ENISA, 2012.

[10] HUTCHINS E.M., CLOPPERT M.J., AMIN R.M., *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockheed Martin, 2014, https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (dostęp 26.08.2017).

[11] Kavanagh K. M., Rochford O., Bussa T., *Magic Quadrant for Security Information and Event Management*, Gartner, 10 August 2016, https://www.gartner.com/doc/3406817/magic-quadrant-security-information-event (dostęp 26.08.2017).

[12] LAST D., MYERS D., HEFFERNAN M., CAIAZZO M., PALTZER N., *Command and Control of Proactive Defense*. Journal of Cyber Security and Information Systems, Vol. 4, No. 1, CSIAC, 2016, pp. 8-13.

[13] MCQUEEN M.A., BOYER W.F., *Deception Used for Cyber Defense of Control Systems*. HSI '09, Human System Interaction 2009, pp. 624-631.

[14] PATKOWSKI A. E., AMANOWICZ M., *Koncepcja ochrony przed działaniami nieuprawnionymi domeny narodowej w działaniach koalicyjnych*. PBZ–MNiSW–DBO–02/I/2007. Zaawansowane metody i techniki tworzenia świadomości sytuacyjnej w działaniach sieciocentrycznych, WIŁ, Warszawa, 2009.

[15] PINGREE L., *Emerging Technology Analysis: Deception Techniques and Technologies Create Security Technology Business Opportunities*. Gartner, 2016. https://www.gartner.com/doc/reprints?id=1-3M8C54V&ct=161118&st=sb&aliId=3170968 (dostęp: 26.08.2017).

[16] ROBERTSON S., *US Patent Application Publication Pub. No.: US 2017/0093911 A1*. Pub. Date: Mar. 30, 2017.

[17] ROWE N.C., ROTHSTEIN H.S., *Two Taxonomies of deception for Attacks on Information System*. Journal of Information Warfare, 3 (2), July 2004, pp. 27-39.

[18] *Deception 2.0 For Dummies®.* Acalvio Special Edition, John Wiley & Sons, Inc., Hoboken, New Jersey, 2017.

[19] YUILL J., DENNING D., FEER F., *Using Deception to Hide Things from Hackers: Processes, Principles, and Techniqu*es. Journal of Information Warfare, Vol. 5, No. 3, 2006, pp. 26-40.

[20] YUILL J., ZAPPE M., DENNING D., FEER F., *Honeyfiles: Deceptive Files for Intrusion Detection*. Proceedings of the 2004 IEEE Workshop on Information Assurance, 2004, pp. 116-122.

The "Hidden response" on cyberattacks

ABSTRACT: A "hidden response" of an ICT security system is a substitution of cyberattack blocking by other actions invisible to an attacker. It is proposed to remove attacked resources from the attacker's operating field by replacing them with dissected data. This allows to investigate attacker's actions with much less chance of detection than by using separated honeypots. First of all, it gives the ability to perform disinformation activities against opponents/competitors of the system owner. In addition, the introduction of the delayed data recording mechanism increases the time limit for detecting cyberattacks before irreversible changes to information resources occur.

KEYWORDS: cybersecurity, deception solutions, disinformation, honeynets, honeypots, sandboxes

Praca wpłynęła do redakcji: 25.09.2017 r.