MAGAZYN

NR 26 / CZERWIEC 2015
Nr 26 / CZERWIEC 2015

www.magazyn.mediarecovery.pl
www.magazyn.mediarecovery.pl

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Cyberprzestępczość – odpowiedzialność karna

Jak skutecznie analizować aktywność użytkowników w internecie.

Piractwo smartfonowe - nowy trend? Z czym walczą polscy cyberpolicjanci?

ZARZĄDZANIE INCYDENTEM ZA POMOCĄ SECURITY OPERATIONS CENTER (SOC)

ZARZĄDZANIE INCYDENTEM ZA POMOCĄ SECURITY OPERATIONS CENTER (SOC)

Co w numerze?

Jak skutecznie analizować aktywność użytkowników w internecie.

Karol Szczyrbowski

Oprogramowanie specjalistyczne Internet Evidence Finder (IEF) jest dynamicznie rozwijanym narzędziem do analizy historii internetowej, komunikatorów oraz od zeszłego roku, także telefonów, plików aplikacji biznesowych i systemu operacyjnego.

Historia IEF-a związana jest bezpośrednio z historią jego producenta, firmy **Magnet Forensics,** a konkretnie jej założyciela – byłego oficera policji kanadyjskiej. **Jad Saliba,** bo o nim mowa, założył swoją firmę w 2011 roku, gdy ze względów osobistych odszedł ze służby w policji. Zajmował się w niej analizami informatyki śledczej. Sam program zaczął powstawać jako odpowiedź na rosnącą ilość danych pochodzących z aktywności internetowej użytkowników. Analiza stawała się coraz bardziej trudna i czasochłonna ze względu na brak odpowiednich rozwiązań specjalistycznych. Obserwując działania firmy i rozwój ich flagowego produktu, nie sposób odnieść wrażenia, że bazuje on na praktycznym doświadczeniu jego twórców. Początkowo program pozwalał na wyodrębnienia kilkudziesięciu artefaktów internetowych, obecnie w podstawowej wersji, program wspiera analizę ponad 265 artefaktów pochodzących z komputerów pracujących na systemie operacyjnym Windows oraz Mac. Oprócz tego, użytkownik ma możliwość pracy na dodatkowych modułach, znacząco rozszerzjcych możliwości programu.

Moduł **„Business Applications & OS Artifacts”** pozwala na wyodrębnienie 58 różnego rodzaju danych z aplikacji pakietu Microsoft Office oraz systemu operacyjnego Windows i Mac OS. Specjaliści będą mogli poddać badaniu aktywność internetową użytkownika, ale także jego lokalną skrzynkę pocztową, sprawdzić podłączane nośniki zewnętrzne, zdarzenia systemowe i inne cenne w postępowaniu informacje. Moduł „Mobile Artifacts” służy do analizy aktywności użytkownika telefonów komórkowych oraz danych pochodzących z aplikacji na nim zainstalowanych. Funkcja ta pozwala na analizę ponad 165 typów danych pochodzących z urządzeń pracujących na systemie operacyjnym iOS, Android oraz Windows Phone.

Z kolei moduł „Triage” można uruchomić bezpośrednio z klucza USB co umożliwia analizę pracującego systemu. Dzięki tej funkcji, użytkownik może wykonać zrzut pamięci badanego komputera, zabezpieczyć dane ulotne (volatile data) jak np. uruchomione procesy, połączenia sieciowe, podłączone dyski sieciowe, informacje o zalogowanych użytkownikach. Dodatkowo, moduł ten pozwala także na sprawdzenie czy dysk twardy jest zaszyfrowany (obsługuje m. in. szyfrowanie typu Truecrypt, Bitlocker PGP

i inne). Użytkownik za pomocą tej funkcji wie w jaki sposób powinien zabezpieczyć dany sprzęt (wyłączając komputer z zaszyfrowanym nośnikiem, pozbawiamy się dostępu do danych w sytuacji kiedy nie posiadamy danych logowania).

Oprogramowanie Internet Evidence Finder choć jest z nami krótko, zdążyło zająć pozycję lidera pod kątem analizy elektronicznego materiału dowodowego z zakresu internetowej aktywności użytkownika. Warto podkreślić jego dynamiczny rozwój i wsłuchiwanie się w głosy i potrzeby użytkowników, a także ciągłe śledzenie trendów internetowych i analizy najpopularniejszych sposobów komunikacji internetowej. Specjaliści z Mediarecovery są w stałym kontakcie z firmą Magnet Forensics, aby zapewnić jak najlepsze wsparcie użytkownikom z Polski. Ddodatkowo podejmowane są inicjatywy związane z tłumaczeniem interfejsu na język polski oraz próby rozszerzenia możliwości produktu o polskie portale i programy.

Warto podkreślić, że oprogramowanie jest używane przez urzędy egzekwowania prawa w ponad 90 krajach, a w samych Stanach Zjednoczonych, korzysta z niego 49 na 50 stanowych urzędów organów ścigania. W Europie korzysta z niego 19 na 28 krajowych urzędów organów ścigania oraz organy ścigania w każdym kraju z grupy G7. Program jest bardzo intuicyjny, dostosowany także do mniej technicznych użytkowników. Posiada bardzo praktyczne i przydatne w codziennej pracy informatyka śledczego funkcje takie jak - możliwość wyszukiwania słów kluczowych w wynikach, eksportowanie raportu oraz sprawy w trybie „portable" do wglądu dla osób nie posiadających programu, możliwość eksportu wyników w wielu formatach. Jego uniwersalność opiera się także na obsłudze wielu formatów kopii nośników jak i obsłudze dysków logicznych i fizycznych.

Obecnie w podstawowej wersji, program Internet Evidence Finder wspiera analizę ponad 265 artefaktów pochodzących z komputerów pracujących na systemie operacyjnym Windows oraz Mac.

Zachęcamy do testowania 30-dniowej wersji próbnej, którą można pozyskać bezpośrednio ze strony producenta lub za pośrednictwem firmy Mediarecovery.

Autor jest specjalistą informatyki śledczej w laboratoriuym Mediarecovery oraz trenerem w Akademii Informatyki Śledczej.

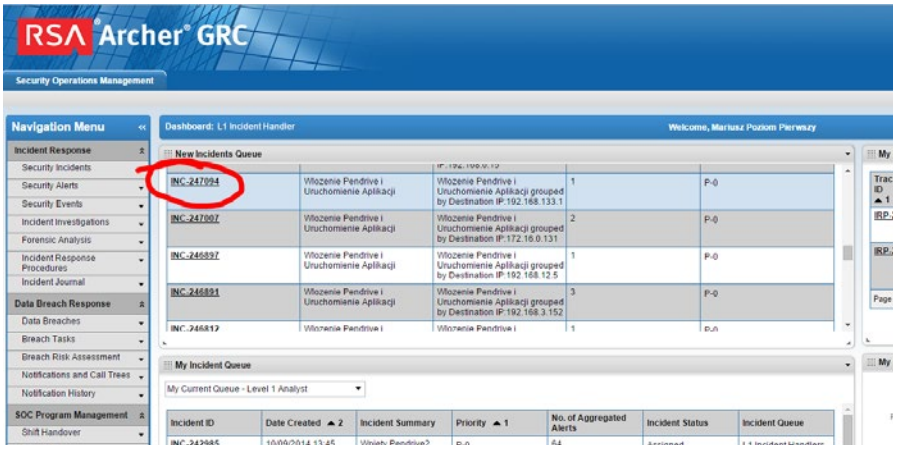
Zarządzenie incydentem za pomocą Security Operations Center (SOC)

Marcin Gryga

Od pewnego czasu bardzo modnym terminem w środowisku IT security staje się SOC (Security Operations Center), czyli tzw. Operacyjne Centrum Bezpieczeństwa. Ten trzyliterowy skrót przebija się do świadomości osób odpowiedzialnych za bezpieczeństwo nie tylko w dużych firmach, ale zaczyna być dostrzegana również w segmencie małych i średnich przedsiębiorstw, który w Polsce staje się istotnym rynkiem pod względem usług informatycznych.

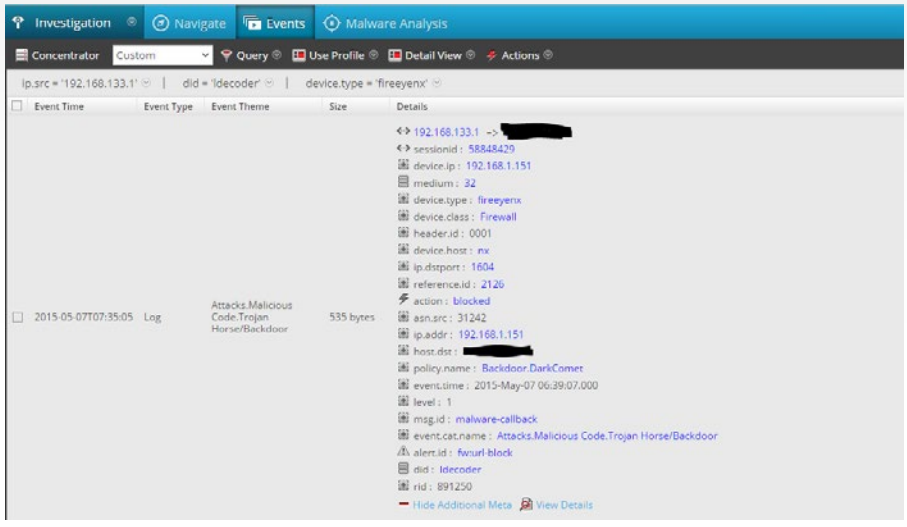
Obecnie same narzędzia służące podnoszeniu szeroko rozumianego bezpieczeństwa informatycznego nie są już w stanie zapobiec coraz liczniejszym włamaniom, które są na tyle skomplikowane, iż często administratorzy mają problem ze zidentyfikowaniem miejsca ataku w ramach infrastruktury IT danej organizacji. Mowa tutaj o atakach typu APT (Advanced Persistent Threats) wykorzystywanych w długim okresie czasu do osiągnięcia celu jakim jest np. uzyskanie najważniejszych informacji dla danej organizacji. W związku z tym firmy coraz częściej decydują się na budowanie własnych SOC'ów w celu wczesnego wykrycia włamania, odparcia ataku, a na następnie przeprowadzenia dochodzenia, tak aby w przyszłości wyeliminować potencjalne luki w zabezpieczeniach, a tym samym uszczelnić politykę bezpieczeństwa.

Dzisiaj chciałbym pokazać jak może wyglądać obsługa przykładowego incydentu przez operatorów w centrum bezpieczeństwa (SOC). Skupimy się na firmie z branży budowlanej. Dyrektor IT jako osoba z dużym doświadczeniem świadomy jest istniejącego ryzyka. Uzyskanie niewielkiej przewagi cenowej podczas przetargów może skutkować poważnymi konsekwencjami finansowymi. Kontrakty warte wiele milionów złotych mogą zostać przegrane ze względu na uzyskanie poufnych informacji przez konkurencję. Dlatego też zdecydował się na zwiększenie bezpieczeństwa poprzez wdrożenie odpowiednich rozwiązań jak i uruchomienie centrum, w którym operatorzy badają na co dzień stan zabezpieczeń w organizacji. W skład SOC wchodzą 2 linie analityków oraz kierownik który bezpośrednio podlega pod dyrektora IT. Ponieważ firma prowadzi kontrakty międzynarodowe cały zespół pracuje w trybie 24/7, tak aby na bieżąco reagować w przypadku wystąpienia incydentów. Całość pracy analityków opiera się na produktach oraz procedurach, które odpowiednio wdrożone umożliwiają szybką i poprawną reakcję na zagrożenia. SOC team podzielony jest na dwie linie analityków, które odpowiadają za identyfikację oraz eliminację pojawiających się zgoszeń (alertów). Pierwsza linia (L1) skupia się przede wszystkim na potwierdzaniu czy zarejestrowane incydenty są faktycznie uzasadnione, natomiast linia druga (L2) potwierdza incydent oraz w zależności od sytuacji stara się wyeliminować zagrożenie.



Rysunek 1. Widok systemu RSA Archer

Załóżmy, iż Pan Mariusz, niedawno przyjęty analityk (L1) wraca z obiadu, loguje się do systemu obsługi SOC - RSA Archer SecOps i widzi nowo wygenerowany incydent (rysunek 1). Incydent został zarejestrowany na podstawie alarmu z systemu Bit9, który wykrył włożenie pendrive'a, a następnie skopiowanie i uruchomienie nowego pliku wykonywalnego. Po wejściu w szczegóły incydentu Pan Mariusz widzi, iż alarm pochodzi z laptopa prezesa firmy. Odpowiedni priorytet incydentu został nadany na podstawie wcześniej określonych zasobów IT firmy. W incydencie została zawarta procedura obsługi, która jasno wskazuje co w tym przypadku analityk powinien wykonać. Sprawdza pierwszy etap i otrzymuje informację, iż powinien upewnić się czy stacja robocza faktycznie wykonuje podejrzane połączenia od momentu wykrycia incydentu. Jeżeli tak, analityk L1 powinien eskalować zadanie na poziom L2. W zgłoszeniu został umieszczony link do systemu RSA Security Analytics, który umożliwia bezpośrednie i szybkie sprawdzenie ruchu sieciowego z podejrzanego hosta, po zalogowaniu się widzi, iż w ruchu przesyłanym z podejrzanego laptopa system FireEye NX wykrył i zaraportował komunikację do serwera C&C (rysunek 2).



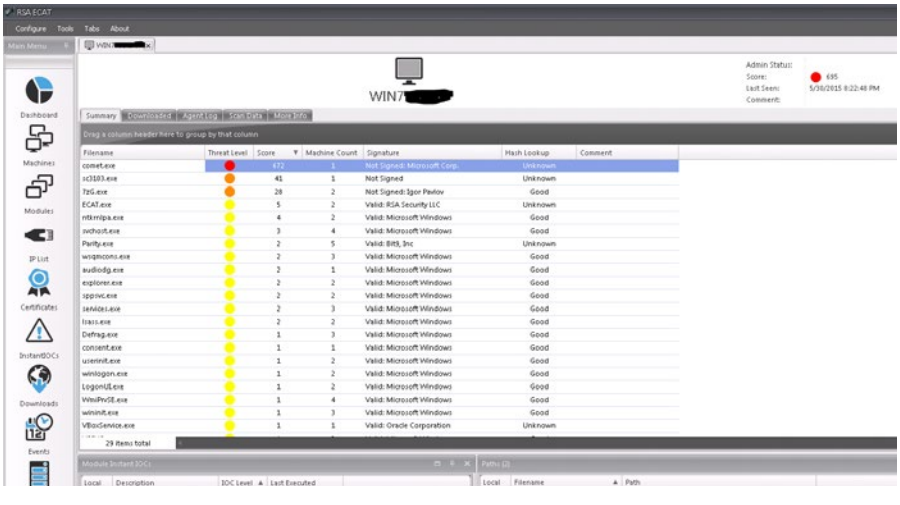
Rysunek 2. Szczegółowy widok na log z systemu FireEye NX w RSA Security Analytics

Daje więc to podstawę do potwierdzenia możliwej infekcji na laptopie prezesa. Pan Mariusz uzupełnia więc zgłoszony incydent o uzyskane informacje (dołącza link do systemu RSA SA, tak aby analityk L2 był w stanie szybko sprawdzić podjęte działania). W tym momencie jako, iż jest pracownikiem z mniejszymi uprawnieniami jego praca zostaje zakończona. Eskaluje więc incydent bezpośrednio do drugiej linii (L2), tak aby odpowiednio doświadczone osoby mogły zająć się rozwiązaniem problemu. Po wykonaniu tego zadania przechodzi do obsługi kolejnego zgłoszenia. Czas wymagany na realizacje zadania został zarejestrowany na podstawie uzupełnionych danych. Jest to o tyle istotne, iż daje kierownikowi SOC ważne informacje odnośnie czasochłonności na poszczególnych stanowiskach, jak i umożliwia sprawdzanie które typy incydentów są rozwiązywane wolno i co za tym idzie jakie kroki może podjąć kierownik aby zwiększyć efektywność swoich pracowników.

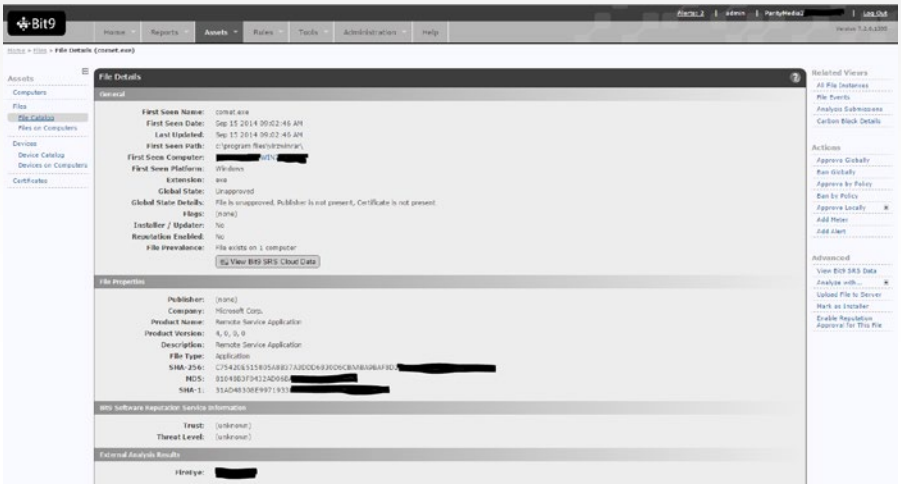
Wracając do problemu, analityk drugiej linii (L2) przystępuje do obsługi incydentu, w pierwszym kroku sprawdza co zostało wykonane na pierwszej linii (L1) i jakie są wnioski. Po zapoznaniu się z informacjami przystępuje do kolejnego etapu procedury, który polega na analizie malware'u znajdującego się na komputerze oraz potwierdzeniu czy inne stacje robocze w tym momencie nie są zainfekowane podobnym złośliwym oprogramowaniem. Do tego zadania mają zostać wykorzystane narzędzia RSA ECAT oraz FireEye AX. Analityk L2 – Pani Anna sprawdza więc nazwę komputera oraz IP, z którego został wygenerowany podejrzany ruch i loguje się na konsolę systemu ECAT. Już po chwili zauważa, iż interesujący ją komputer otrzymał wysoki wskaźnik punktowy (rysunek 3). Po wejściu w szczegóły widzi, iż uruchomiony został plik o nazwie comet.exe który uzyskał wysoką ocenę punktową (rysunek 4).

Analityk otrzymuje informację dlaczego taki wynik został przypisany. Plik po uruchomieniu modyfikował w systemie ustawiania LUA, polityki firewall'a, skopiował się do ukrytego katalogu oraz uruchomił dodatkowo proces w systemie. W zakładce „Paths" analityk widzi jakie nazwy plików są powiązane ze sobą w tym wypadku, a w zakładce „Tracking" może dokładnie prześledzić ścieżkę zmian. Ponieważ firma zainstalowała oprogramowanie ECAT na wszystkich laptopach i serwerach, Pani Anna w zakładce „Machines", zauważa, obecnie ten plik oraz proces znajduje się tylko na jednym komputerze. Zapisuje więc tę informację w dzienniku incydentu, aby po chwili przystąpić do analizy malware'u. Dodatkowo upewnia się czy dany plik nie był widoczny wcześniej w sieci firmowej, kopiuje sumę MD5 i zakłada filtr w systemie Bit9, który wskaże jej gdzie jeszcze mógł znajdować się podejrzany plik (rysunek 5). Mając potwierdzenie z systemu Bit9 iż plik znajduje się obecnie tylko na jednym stacji roboczej Pani Anna wykorzystuje integrację systemów Bit9 oraz FireEye AX i przesyła plik bezpośrednio do analizy. Po kilku minutach loguje się do systemu

Rysunek 3. Ogólny widok na status maszyny w systemie RSA ECAT



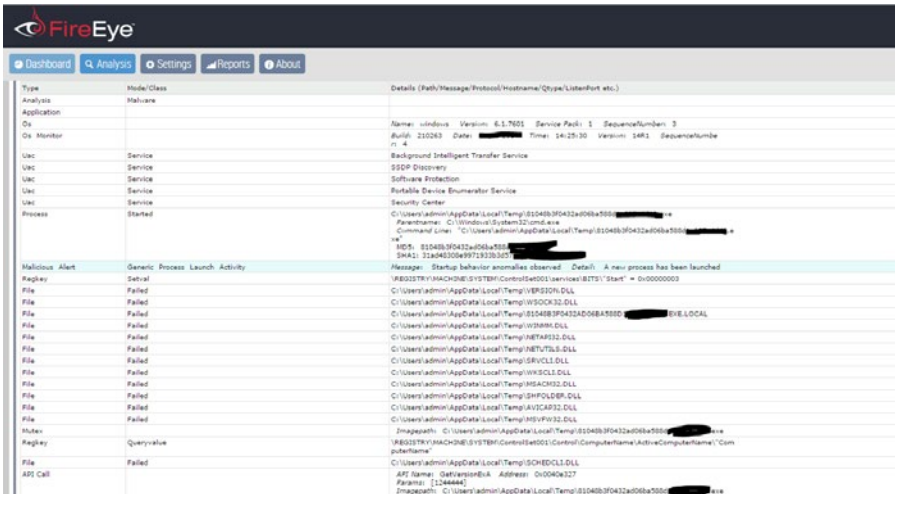
Rysunek 4. Szczegółowy widok stanu hosta w RSA ECAT



Rysunek 5. Szczegółowy widok statusu pliku w systemie Bit9

FireEye AX i sprawdza wynik zadania, otrzymuje potwierdzenie, iż plik faktycznie jest zagrożeniem dla systemów. Może również zapoznać się ze szczegółową analizą malware'u, która pokazuje krok po kroku jak zachwouje się podejrzane oprogramowanie (rysunek 6).

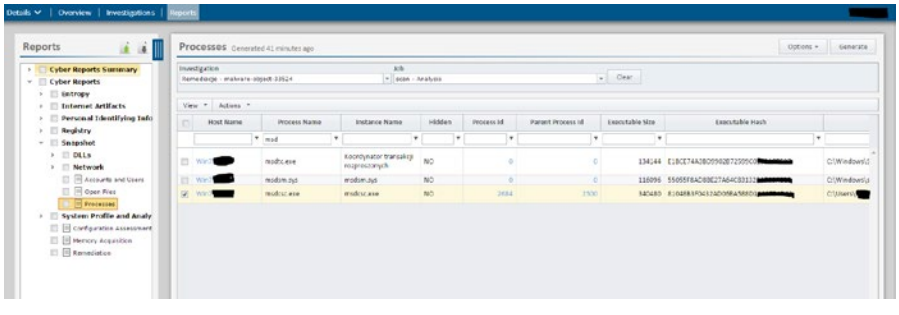
Tak więc w tym momencie Pani Anna posiada już potwierdzenie, faktycznie na laptopie prezesa zostało uruchomione szkodliwe oprogramowanie, które próbowało wykonać połączenie do serwera C&C (połaczenie te zablokował system FireEye NX). Malware został zidentyfikowany jako Backdoor.Darkcomet, już po chwili analityk L2 wyszukuje informację o tym zagrożeniu, okazuje się, iż jest to popularny zestaw narzędzi typu RAT (Remote Access Tool). System FireEye AX jest ogromnym wsparciem dla analityków malware'u, gdyż umożliwia wykonanie analizy w ciągu kilku lub kilkunastu minut, normalnie ta praca zajęłaby osobie z odpowiednim doświadczeniem nawet kilka godzin pracy. Informacje o potwierdzonym zagrożeniu jak i plikach obecnych w systemach zostają zapisane w dzienniku incydentów. W tym momencie analityk przechodzi do trzeciego etapu zapisanego w procedurach, który nakazuje przeprowadzenie



Rysunek 6. Szczegółowy raport z analizy malware w systemie FireEye AX

dochodzenia na zainfekowanych stacjach roboczych w celu sprawdzenia czy faktycznie doszło do wycieku danych. W tym celu Pani Anna wykorzysta narzędzie RSA Security Analytics. Dzięki logowaniu całego ruchu sieciowego będzie w stanie sprawdzić czy nastąpiło połączenie do zewnętrznych serwerów i czy zostały przesłane jakieś dane. Wykorzystując wbudowany link w alercie do systemu RSA SA szybko filtruje potrzebne informacje, widzi iż system zarejestrował połączenia do zewnętrznego hosta C&C (zidentyfikowane przez system FireEye NX), filtruje widok pakietów sieciowych tak, aby potwierdzić wyciek.

Analityk potwierdza, iż pomimo próby nawiązania połączenia nie została zestawiona sesja oraz nie zostały przesłane dane na zewnątrz (zerowy payload w pakietach). Wgląd w pakiety sprawia że, w przypadku zagrożenia firma ma możliwość odtworzenia ruchu sieciowego, co daje spore możliwości pod kątem analizy wycieku. Dzięki temu możemy szybko zlokalizować pliki, które zostały wysłane (oczywiście jeżeli wcześniej nie zostały zaszyfrowane przez malware). Inną ciekawą funkcją systemu jest możliwość odtworzenia przeglądanych stron www, podglądu plików graficznych, nagrywanie rozmów VoIP na poziomie pakietów. Daje to spore możliwości analizy zdarzeń dla osób odpowiedzialnych za bezpieczeństwo IT w przedsiębiorstwach. Po potwierdzeniu, iż faktycznie nie mieliśmy wycieku danych w firmie, Pani Anna uzupełnia dziennik incydentu i przechodzi do czwartego, ostatniego już etapu procedury. Jej zadaniem jest w tym mo-



Rysunek 7. Widok opcji wykonanego snapshoot'u z systemu EnCase CyberSecurity

mencie oczyszczenie laptopa zainfekowanego w tym momencie, wykorzysta w tym celu system EnCase CyberSecurity, który dzięki współpracy z systemem FireEye NX w momencie wykrycia połączenia callback do serwera C&C z laptopa prezesa, wykonał snapshoot maszyny, co sprawia, że mamy możliwość usunięcia złośliwego malware'u ze stacji (rysunek 7).

Po usunięciu złośliwego kodu, analityk uzupełnia informacje w dzienniku incydentów. W tym momencie zamyka również jego obsługę. Całe zadanie od momentu otrzymania alertu do rozwiązania problemu zostało sprawnie wykonane dzięki doświadczeniu osób zatrudnionych w SOC jak i procedurom, które odpowiednio prowadziły analityków w tym przypadku. Kierownik IT dzięki swojemu widokowi w systemie RSA Archer na bieżąco jest w stanie monitorować status zadań, widzi trendy historyczne. Dlatego jest w stanie odpowiednio reagować na pojawiające się problemy. Dzięki swojej pracy jest w stanie utworzyć odpowiednie polityki reagowania na poszczególne zagrożenia. Sam system Archer również posiada funkcjonalność przekazywania zmiany, co w przypadku pracy w trybie 24/7 jest dosyć istotne, aby osoby zatrudnione w SOC mogły od razu zajmować się najważniejszymi w tym momencie incydentami.

W opisie tego przykładowego incydentu i sposobu jego obsługi przyjąłem pewne założenia. System Bit9 jest ustawiony w polityce zezwalającej na uruchomienie każdej aplikacji na stacji końcowej, czyli laptop prezesa nie jest odpowiednio chroniony. Niestety często spotykamy się przy prawdziwych analizach z bardzo wieloma przypadkami luźnego podejścia do bezpieczeństwa przez osoby decyzyjne w przedsiębiorstwach. Gdyby system ten był poprawnie wdrożony mielibyśmy możliwość wcześniejszej automatycznej analizy nowego pliku w systemie FireEye AX. Dzięki temu uruchomienie tego oprogramowania zostałoby zablokowane na wszystkich stacjach roboczych w organizacji po potwierdzeniu jego szkodliwości. Cały proces obsługi incydentu jest jedynie przykładem w jaki sposób praca SOC może być zorganizowana. Ten artykuł jest jedynie wstępem do budowy polityk i procedur pracy SOC, które muszą być zawsze indywidualnie przystosowane do każdego klienta. Mam nadzieję, iż udało mi się pokazać jak może wyglądać obsługa jednej z takich procedur.

Autor jest inżynierem IT w firmie Mediarecovery. Posiada wieloletnie doświadczenie w zakresie administracji systemów IT oraz wdrożeń rozwiązań z obszaru bezpieczeństwa. Szczególnie zainteresowany jest tematami sieci oraz pentestów. W firmie odpowiada za wdrożenia i wsparcie produktów w ramach Security Operations Center (SOC). Nie są mu obce ITIL oraz ISO27k.

Cyberprzestępczość – odpowiedzialność karna

Jarosław Góra

Przestępczość komputerowa ewoluowała. Wirusy komputerowe, których celem było dokonywanie drobnych aktów komputerowego wandalizmu oraz przysporzenie rozgłosu ich twórcom zastąpił wyrafinowany malware, mający na celu paraliżowanie działania systemów określonych organizacji, instytucji i przedsiębiorstw oraz pozyskiwanie informacji chronionych. Działających w pojedynkę hackerów zastąpiły zorganizowane na wzór korporacji przedsiębiorstwacyberprzestępcze.

W głębokiej sieci przestępczość wszelkiego rodzaju kwitnie, a serwisy takie jak Silk Road i jego kolejne klony tworzą wyśmienite warunki do rozwijania karier przestępczych. Różnego rodzaju oszuści przenieśli się do cyberświata, a ich celem stały się dane osobowe i wszelkiego rodzaju informacje o internautach oraz ich pieniądze.

Czy obowiązujące przepisy dają organom ścigania odpowiednie narzędzia umożliwiające ściganie cyberprzestępców, a sądom orzekanie o odpowiedzialności karnej? Czy na tle obowiązujących przepisów subsumcja zachowań cyberprzestępców pod przepisy ustawy karnej jest oczywista?

Czy prawo nadąża za zmieniającą się rzeczywistością cyberprzestępczości? Przede wszystkim wskazać należy, że polski ustawodawca unika w ogóle tego pojęcia. Co zatem należy rozumieć pod pojęciem przestępczości komputerowej? W literaturze przedmiotu znajdziemy definicje, zgodnie z którymi cyberprzestępczość to wszelka aktywność, w której komputer lub sieć komputerowa stanowi narzędzie, przedmiot albo środowisko działalności przestępczej.

Spotkać się można również z podziałem na cyberprzestępstwa w wąskim sensie (przestępstwa komputerowe) rozumiane jako zamachy przeciwko bezpieczeństwu systemów komputerowych i elektronicznie przetwarzanych przez nie danych, popełnione przy użyciu operacji elektronicznych oraz cyberprzestępstwa w szerokim sensie (przestępstwa dotyczące komputerów). Obejmują one czyny popełnione przy użyciu lub skierowane przeciwko systemowi komputerowemu lub sieci komputerowej, takie jak nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji za pomocą komputera lub sieci. Na poziomie ustawodawstwa europejskiego cyberprzestępstwa rozumie się jako czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciw-

ko takim sieciom i systemom, wyróżniając przy tym trzy typy tych czynów:

- „tradycyjne" formy przestępstw, takie jak oszustwo, czy fałszerstwo popełnione przy użyciu elektronicznych sieci i systemów informatycznych,
- publikacje nielegalnych treści w mediach elektronicznych,
- przestępstwa „typowe" – ataki przeciwko systemom informatycznym, ataki typu DoS, sabotaż informatyczny.

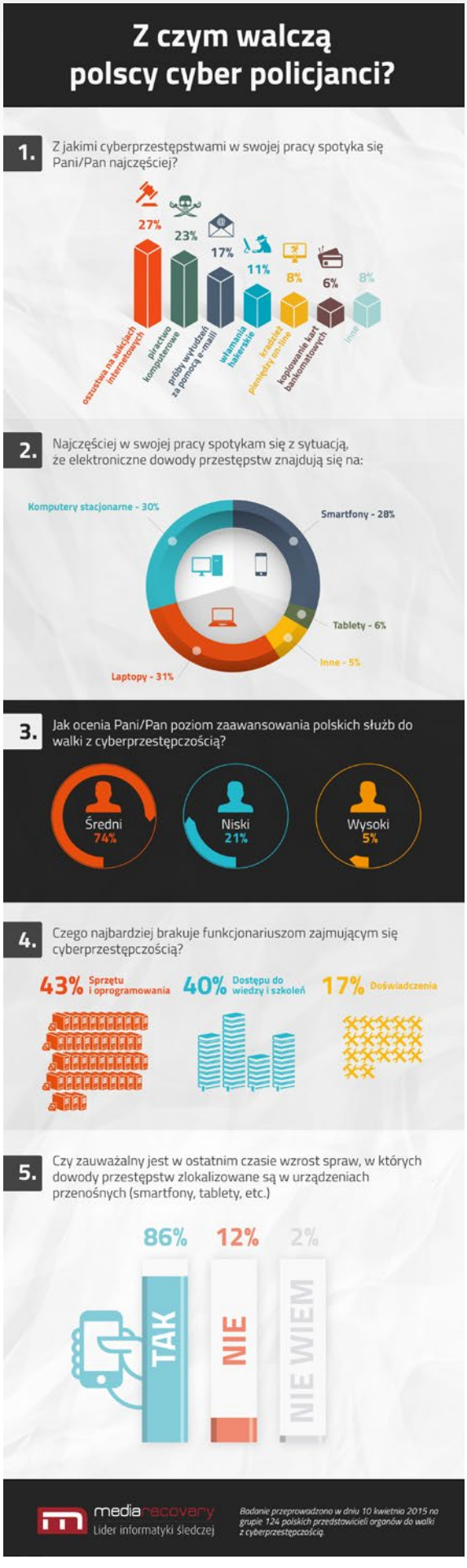
Polski ustawodawca nie zdecydował się zebrać przepisów dotyczących przestępstw komputerowych w jednym miejscu. Regulacje dotyczące tej materii znajdziemy w kodeksie karnym, jak i w ramach przepisów karnych innych ustaw. Czy wśród tych przepisów znajdziemy opisy wszelkich bezprawnych działań, jakie możemy zaobserwować? Obowiązujące w Polsce przepisy opisujące przestępstwa komputerowe możemy podzielić na trzy podstawowe grupy.

Pierwszą grupą są przestępstwa popełniane przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji, tj.: nielegalny dostęp do systemu (hacking) – art. 267 § 1 i 2 k.k, naruszenie tajemnicy komunikacji (sniffing) – art. 267 § 3 k.k., naruszenie integralności danych (wirusy, robaki, trojany) – art. 268 k.k. oraz art. 268a k.k., naruszenie integralności systemu (ataki DDos, Ping flod itp.) – art. 269 k.k. oraz wytwarzanie „narzędzi hakreskich" – art. 269a k.k oraz art. 269b k.k..

Kolejną grupą są przestępstwa związane z treścią informacji, tj.: przestępstwa seksualne na szkodę małoletniego (grooming itp.) – art. 200a k.k., art. 202 k.k. oraz przestępstwa przeciwko czci (zniewaga, zniesławienie) – art. 212 k.k. oraz art. 216 k.k. Do ostatniej grupy zaliczyć można natomiast przestępstwa związane z instrumentalnym wykorzystaniem sieci i systemów teleinformatycznych skierowane przeciwko mieniu (np. oszustwo, naruszenie praw własności intelektualnej, w tym praw autorskich) oraz inne, tj.: cyberstalking, kradzież tożsamości, fałszerstwo komputerowe. W tej grupie kwalifikacja prawna zależy od rodzaju „tradycyjnego" przestępstwa popełnionego z wykorzystaniem cyberprzestrzeni. Dodatkowo wspomnieć należy o art. 130 § 3 k.k., zgodnie z którym przestępstwo „cyberszpiegostwa" zagrożone jest karą pozbawienia wolności od 6 miesięcy do lat 8.

Biorąc pod uwagę szerokie spektrum obowiązujących w Polsce przepisów, w dużej mierze będących odbiciem regulacji unijnych i międzynarodowych, wydawać by się mogło, iż dla każdego niepożądanego zachowania zaistniałego w cyberrzeczywistości „znajdzie się paragraf". W praktyce jednak stosowanie przedmiotowych przepisów, w szczególności należących do pierwszej z wymienionych grup, sprawia spore trudności, tak organom ścigania, jak i sądom, a ocena zebranego materiału dowodowego i rozstrzygnięcie o odpowiedzialności niejednokrotnie wymaga powołania biegłego z zakresu informatyki, którego wiedza z zakresu technologii informatycznych umożliwia dopiero zrozumienie sprawy.

Autor jest adwokatem, szefem zespołu prawa własności intelektualnej i nowych technologii w kancelarii Ślązak, Zapiór i Wspólnicy. Trener w Akademii Informatyki Śledczej.



Piractwo smartfonowe - nowy trend? Z czym walczą polscy cyberpolicjanci?

Jak wskazują wyniki badania laboratorium informatyki śledczej Mediarecovery polscy policjanci zajmujący się cyberprzestępczością najczęściej prowadzą sprawy dotyczące oszustw na aukcjach internetowych. O wiele częściej niż w latach ubiegłych dowody przestępstw znajdują w smartfonach.

Badanie przeprowadzono na grupie ponad 120 funkcjonariuszy policji oraz innych służb odpowiedzialnych za bezpieczeństwo podczas zamkniętego spotkania organizowanego przez Mediarecovery. Biorąc pod uwagę grupę, na której przeprowadzono badanie, czyli funkcjonariuszy na co dzień zwalczających cyberprzestępczość, jego wyniki są szczególnie istotne.

Z jakimi cyberprzestępstwami spotykają się najczęściej? 27% ankietowanych wskazało oszustwa na aukcjach internetowych, jako najczęstszy rodzaj spraw, które prowadzą. Na drugim miejscu z 23% wskazań znalazło się piractwo komputerowe. Kolejna grupa to próby wyłudzeń za pomocą e-maili - 17%. Włamania hakerskie 11%, kradzież pieniędzy on-line 8%, kopiowanie kart bankomatowych 6%. Inne grupy przestępstw wskazało 8% ankietowanych.

Czego najbardziej brakuje funkcjonariuszom zajmującym się cyberprzestępczością? 43% funkcjonariuszy odpowiadając na to pytanie wskazało sprzęt i oprogramowanie. Narzędzia takie, jak UFED Field Series do analiz urządzeń mobilnych w terenie wykorzystywane są przez policje całego świata i brakuje ich na wyposażeniu polskich służb. 40% ankietowanych wskazuje, że najbardziej brakuje dostępu do wiedzy i szkoleń, a 17% doświadczenia. Odpowiedzi na to pytanie świadczą o tym, że funkcjonariusze doskonale rozumieją potrzebę ciągłego rozwoju. Dzięki temu są w stanie bardziej skutecznie zwalczać cyberprzestępczość, która rozwija się bardzo szybko.

Gdzie znajdują elektroniczne dowody przestępstw? Pierwszy raz w tego typu badaniach urządzenia przenośne (tablety, smartfony liczone razem) wyprzedziły komputery stacjonarne i laptopy.

Wymienione urządzenia wskazało odpowiednio: 34%, 30% i 31%. Wśród innych miejsc poszukiwania elektronicznego materiału dowodowego (5% wskazań) ankietowani wyliczyli między innymi zapisy monitoringu i serwery.

Z badania wynika jeszcze jedno nowe zjawisko. Do piractwa komputerowego dochodzi piractwo smartfonowe. Pierwszy raz głośniej na ten temat zrobiło się w 2012 roku kiedy FBI zamknęło kilka stron internetowych udostępniających pirackie wersje aplikacji.

Staje się to też coraz bardziej dostrzegalne w Polsce. Jest o tym ciszej bo aplikacje tworzą często pojedyncze osoby nie mają ani środków, ani doświadczenia by głośno dopominać się o swoje tak, jak to robią giganci rynku oprogramowania komputerowego.

Aż 86% funkcjonariuszy zauważa wzrost ilości spraw gdzie głównym źródłem dowodów przestępstw są smartfony i tablety. Wpływ na to ma oczywiście coraz większa dostępność i popularność urządzeń tego typu.

mediaeraser

DEGAUSSER MD 205

Rewolucja w kasowaniu danych!

Laboratorium Mediarecovery poinformowało właśnie o wprowadzeniu na rynek urządzenia do nieodwracalnego kasowania danych. Degausser Mediaeraser MD205 kasuje dane ze wszystkich rodzajów nośników magnetycznych.

Mediaeraser MD205 został zaprojektowany w oparciu o 10 letnie doświadczenia inżynierów z laboratorium Mediarecovery. Degausser jest kolejnym z linii urządzeń zaprojektowanych i wyprodukowanych w Mediarecovery. Wcześniejszy model Mediaeraser MD103, posiadający certyfikację Służby Kontrwywiad Wojskowego, cieszy się dużym zainteresowaniem na rynkach polskim i europejskim.

Zgodność z normami ISO

Urządzenie Mediaeraser MD205 kasuje dane zgodnie z wytycznymi zawartymi w normach ISO 27001 i ISO 27040. Jest to szczególnie istotne w przypadku firm, funkcjonujących w zgodzie z ISO w zakresie bezpieczeństwa informacji. Użycie degaussera Mediaeraser MD205 daje pewność, że cały proces nieodwracalnego kasowania danych przebiega zgodnie z wytycznymi tych norm.

Szybkość i moc

Nowy model polskiego deagussera charakteryzuje się dużą szybkością działania. Proces kasowania danych z jednego nośnika zajmuje jedynie 18 sekund. Urządzenie generuje moc 18 000 Gausów, ponad dwukrotnie więcej niż poprzedni model Mediaeraser MD103.

Prace rozwojowe

Inżynierowie z laboratorium Mediarecovery planują dodatkowe funkcjonalności degaussera Mediaeraser MD205. Pierwszą z nich, która zainteresuje klientów mających wdrożoną normę ISO 27001 i ISO 27040 jest możliwość automatycznego skanowania kodu kreskowego dysku twardego i wykonanie zdjęcia kasowanego nośnika. Ułatwi to znacząco pracę osób odpowiedzialnych za utylizację zużytego sprzętu elektronicznego w zakresie kwestii organizacyjnychiarchiwizacyjnych.

mediaeraser DEGAUSSER MD 205

Proces kasowania danych z nośników magnetycznych przy użyciu Degaussera Mediaeraser MD 205.

Specyfikacja techniczna:

- Czas operacji kasowania: 20 sekund
- Rodzaje nośników: dyski twarde 2,5', 3,5', dyskietki, taśmy magnetyczne DLT, LTO, 3490 i inne
- Generowane pole magnetyczne: 18 000 Gaussów / 18 000 Oe
- Temperatura pracy: 15 - 40 °C
- Wilgotność otoczenia: 10% -70% bez kondensacji
- Wymiary (długość x szerokość x wysokość): 485 x 440 x 280 mm
- Maksymalny rozmiar nośnika: 170 x 120 x 45 mm
- Waga: ok. 30 kg
- Zasilanie: 230V AC 50/60 Hz
- Pobór prądu: 0,5-7A (230V, 50-60Hz)
- Gwarancja: 2 lata
- System rozmagnesowywania: pojemnościowy, wyładowujący zapewnia duży impuls przy umiarkowanym, rozciągniętym w czasie, poborze prądu z sieci
- Typ degaussera: komorowy
- Wskaźnik osiągnięcia wymaganego poziomu pola magnetycznego
- Wskaźnik kontroli energii wyładowania impulsu magnetycznego
- Wskaźnik zbyt niskiej indukcji pola magnetycznego
- Instrukcja obsługi: język polski
- Automatyczny transport nośnika
- Automatyczny pomiar długości nośnika
- Możliwość podłączenia zewnętrznego podajnika
- Możliwość zeskanowania kodu kreskowego oraz wykonanie zdjęcia kasowanego nośnika: OPCJA
- Tryb pracy: manualny lub automatyczny
- Licznik skasowanych nośników
- Automatyczne przechodzenie w stan czuwania
- Urządzenie spełnia wymogi polskiej normy dotyczącej bezpieczeństwa informacji, PN-ISO/IEC 27001:2007 w zakresie niszczenia nośników magnetycznych

Generowane przez Degausser Mediaeraser MD 205 pole magnetyczne gwarantuje kasowanie nośników o współczynniku koercji 18 000 Oe. Zgodnie z danymi amerykańskiego National Institute of Standards and Technology, współczesne nośniki cyfrowe osiągają koercję 5 000 Oe.

Więcej informacji znajduje się na stronie www.mediaeraser.com

MAGAZYN INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: magazyn@mediarecovery.pl
www.magazyn.mediarecovery.pl

Redakcja
Sebastian Małycha (red. nacz.),
Przemysław Krejza
Skład, łamanie, grafika: Mariusz Ruski
Reklama: Damian Kowalczyk

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: biuro@mediarecovery.pl
www.mediarecovery.pl

mediarecovery Lider informatyki śledczej