MAGAZYN

NR 15/PAŹDZIERNIK 2012

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

TROJAN
W SŁUŻBIE LUDZKOŚCI str.7

DANE TRANSMISYJNE W
SYSTEMACH TELEKOMUNIKACYJNYCH str.2

JAK SKUTECZNIE CHRONIĆ
INTERESY PRZEDSIĘBIORCY? str.3

TECHNOLOGIA NETWITNESS
SKALOWALNA I ELASTYCZNA str.4

JAK PRZYDUSIĆ GAUSSA?
JAK UGASIĆ FLAME? str.5

Dane transmisyjne w systemach telekomunikacyjnych

Mateusz Witański

W jednym z poprzednich numerów Magazynu Informatyki Śledczej i Bezpieczeństwa IT ukazał się artykuł postulujący włączenie w krąg zainteresowania informatyki śledczej telekomunikacji. Nawiązując do tamtego artykułu warto zastanowić się nad technicznym aspektem tego zagadnienia. Chodzi przede wszystkim o zdobywanie i analizowanie danych transmisyjnych, ktróre generowane są przez każdy system telekomunikacyjny, a zawierających informacje o przebiegu rozmowy.

Na początek trzeba określić, co to są dane transmisyjne. Są to dane przetwarzane dla celów przekazania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, mogą obejmować informacje odnoszące się do wyznaczania trasy, długości, czasu lub pojemności komunikatu, zastosowanego protokołu, lokalizacji terminala nadawcy lub odbiorcy, sieci, w której komunikat powstaje lub zostaje przerwany oraz początku, końca lub długości połączenia. Jak widać z powyższego opisu, dane transmisyjne zawierają podstawowe informacje o połączeniu, jakie odbyło się między dwoma abonentami. Z zasad kierujących procesem wytwarzania oprogramowania sterującego centralą wynika, że dane te muszą być generowane przez każdą centralę, gdyż są elementem podstawowego w telekomunikacji procesu obsługi połączenia. Z tych założeń wynika także, że dane te pełnią funkcję dwojakiego rodzaju, rozliczeniową i informacyjno-kontrolną.

Dla informatyki śledczej dane transmisyjne powinny być powodem zainteresowania z co najmniej dwóch powodów. Po pierwsze są to dane generowane i magazynowane przez urządzenia posiadające cyfrowe nośniki danych, po drugie dane te mogą być dowodami popełnionych przestępstw lub nadużyć. Praca informatyków śledczych z centralami telefonicznymi staje się coraz łatwiejsza z punktu widzenia technicznego odzyskiwania danych, nadal pozostaje niezwykle trudna ze względu na konieczność analizy odzyskanych danych.

Współczesne systemy telekomunikacyjne stają się coraz częściej systemami informatycznymi z odpowiednim oprogramowaniem i ewentualnie kartami dostępowymi do sieci telefonicznej. Podchodząc do współczesnej centrali IP stykamy się tak naprawdę z typowym serwerem, na którym zainstalowane jest oprogramowanie telekomunikacyjne, łączące się z jednej strony z aparatami telefonicznymi wpiętymi do sieci komputerowej, z drugiej strony z bramami łączącymi całą architekturę telekomunikacyjną z siecią PSTN. Jeżeli mówimy o serwerach, mówimy także o tradycyjnych, cyfrowych nośnikach danych, takich jak dyski twarde czy pamięci Flash. Nawet gdybyśmy mieli do serwerów podpięte urządzenia zewnętrzne gromadzące dane transmisyjne (np. bufory lub karty w komputerach), mają one takie same nośniki danych. Podejmując się odzyskiwania danych transmisyjnych z konkretnej centrali, warto wcześniej zapoznać się ze sposobem gromadzenia tych informacji przez dane urządzenie. Jest bowiem kilka sposobów rozwiązania tego zagadnienia, a wszystko zależy od, wykonanej zarówno przez producenta, jak i użytkownika, konfiguracji sposobu zrzucania danych transmisyjnych w centrali.

Dla informatyki śledczej ważne jest to, aby spośród wielu danych wychwycić te, które przedstawiają wartość dowodową. Rozpoczynając analizę danych transmisyjnych musimy być przygotowani w kilku istotnych obszarach. Po pierwsze powinniśmy wiedzieć, gdzie szukać takich danych, czy w odpowiedniej części pliku konfiguracyjnego, w pliku zlokalizowanym w odpowiednim katalogu, a może w pamięci urządzenia zewnętrznego. Po drugie powinniśmy wiedzieć, jaką postać ma interesujący nas rekord z danymi transmisyjnymi, w jakiej postaci zapisane są poszczególne dane. Po trzecie musimy wiedzieć, jak interpretować uzyskane dane, aby dawały wiarygodne wyniki. Odrębnym obszarem analizy jest konieczność oceny, czy dane uzyskane w wyniku procesu odzyskiwania są kompletne, czy wymagają porównania z innymi danymi, np. listą abonentów czy danymi z innych central tego samego lub niezależnych systemów telekomunikacyjnych. W przypadku danych transmisyjnych pochodzących z systemów telekomunikacyjnych proces analizy danych jest dużo bardziej skomplikowany niż w przypadku odzyskiwania danych z tradycyjnego oprogramowania komputerowego. Tak jak w przypadku każdego specjalistycznego oprogramowania, analiza informatyczna danych wymagać będzie wiedzy specjalistycznej z zakresu rozwiązań centralowych oraz specyfiki działania systemów billingowych.

Na koniec pozostaje pytanie, dlaczego angażować informatykę śledczą w odzyskiwanie danych transmisyjnych z central telefonicznych, skoro łatwiejszy jest dostęp do billingów? Najprostszą odpowiedzią jest stwierdzenie, że billing zawiera dużo mniej danych i czasami także te mniej istotne. Zgodnie z Prawem telekomunikacyjnym dane billingowe, służące do generowania popularnych billingów, są tylko elementem większej grupy danych zawierających dane transmisyjne. Tak więc, aby wiedzieć więcej o połączeniu, trzeba sięgnąć dużo głębiej, niż tylko do prostych zestawień kosztowych. ■

Jak skutecznie chronić interesy przedsiębiorcy?

Jakub Ślązak cz.2

3 kwietnia 2007 roku, Europejski Trybunał Praw Człowieka orzekł w sprawie skargi złożonej przez Lynnette Copland przeciwko Wielkiej Brytanii. Wyrok dotyczył kwestii monitoringu stosowanego przez jedną z Brytyjskich wyższych uczelni państwowych (pracodawcy) wobec skarżącej (pracownika). W stanie faktycznym, który analizował Trybunał, pracodawca uzyskał dostęp do całości korespondencji e-mail prowadzonej przez skarżącą oraz podsłuchiwał prowadzone przez nią rozmowy telefoniczne. Co więcej, celem ustalenia tożsamości rozmówców, pracodawca niejednokrotnie sam łączył się z wybranymi przez Lynette Copland numerami. Przez cały okres tak prowadzonej inwigilacji skarżąca nie posiadała wiedzy co do podejmowanych wobec niej działań, rząd brytyjski uzasadniał natomiast podejmowane działania koniecznością ustalenia czy skarżąca nie nadużywa urządzeń szkoły do celów prywatnych.

> Aby bowiem pracodawca mógł stosować monitoring, powinien w pierwszej kolejności poinformować pracowników o jego wprowadzeniu oraz podstawowych zasadach, które regulują jego funkcjonowanie.

Orzeczenie, poza swoim zakresem pozostawiło kwestię oceny tego czy skarżąca mogła, w godzinach pracy, wykorzystywać infrastrukturę pracodawcy do celów prywatnych oraz czy postępując w ten sposób naruszała obowiązki pracownicze. Trybunał wskazał natomiast jednoznacznie, iż takie postępowanie pracodawcy, wobec faktu, iż pracownik nie został o nim poinformowany, stanowi naruszenie prawa do prywatności i w żadnej mierze nie powinno korzystać z ochrony obowiązujących regulacji.

Przytoczony wyrok jest o tyle istotny, iż w momencie jego wydawania, Wielka Brytania nie posiadała prawnie uregulowanej kwestii monitoringu. Jego treść Trybunał wyprowadził bezpośrednio z art. 8 Europejskiej Konwencji Praw Człowieka, gwarantującego każdemu prawo do poszanowania życia prywatnego, rodzinnego, mieszkania oraz korespondencji. Ostatecznie Trybunał przyznał rację skarżącej oraz zasądził na jej rzecz kwotę niemalże 10.000 funtów.

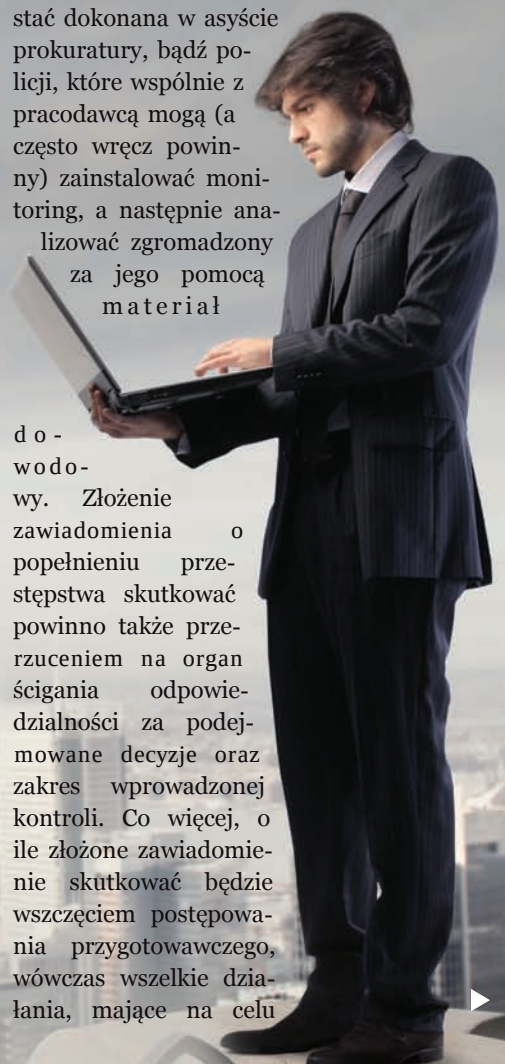
Omawiane orzeczenie natychmiast przełożyło się na stosowanie prawa we wszelkich krajach uznających jurysdykcję Europejskiego Trybunały Praw Człowieka, w tym w Polsce. Wprawdzie nie skutkowało one uchwaleniem odrębnego aktu prawnego regulującego kwestię monitoringu, nie mniej usankcjonowało podstawową zasadę dotyczącą jego stosowania, jaką jest jawność.

Aby bowiem pracodawca mógł stosować monitoring, powinien w pierwszej kolejności poinformować pracowników o jego wprowadzeniu oraz podstawowych zasadach, które regulują jego funkcjonowanie. Co więcej, w zależności od rodzaju monitoringu, obowiązek informacyjny powinien objąć także osoby postronne, które mogą zostać poddane działaniom pracodawcy – np. klientów wszelakich instytucji, w którym zainstalowane zostały kamery. W takich przypadkach obowiązek informacyjny wypełniany jest z reguły poprzez piktogramy opatrzone jednozdaniowym komentarzem, z jednej strony mające na celu odstraszenie potencjalnych złodziei, z drugiej natomiast poinformowanie klientów o stosowanych zabezpieczeniach.

Obowiązek informacyjny nie musi zostać natomiast dotrzymany w sytuacji, w której pracodawca doświadcza działań godzących w jego interesy, a wprowadzenie monitoringu ma na celu wykrycie sprawcy takich zachowań. Nie będzie więc naruszeniem prawa, monitoring sieci komputerowej, który doprowadzić ma do wskazania pracownika wykradającego tajemnice przedsiębiorstwa, bądź instalacja ukrytych kamer w hotelowej recepcji, o ile ich przeznaczeniem będzie ustalenie tożsamości, działającego w jej obszarze, złodzieja.

W takich przypadkach ważne jest natomiast, aby podejmowane działania spełniały dwa dodatkowe kryteria, którymi są adekwatność (proporcjonalność) oraz usprawiedliwiony cel. Oba w/w pojęcia mają co prawda charakter uznaniowy, nie mniej intuicyjnie jesteśmy w stanie określić czy stosowane przez pracodawcę środki nie mają charakteru nadmiernej ingerencji w prawnie chronione dobra pracowników oraz czy ich wprowadzeniu towarzyszy realna i uzasadniona przyczyna.

Warto także pamiętać, ze większość podejmowanych działań może zostać dokonana w asyście prokuratury, bądź policji, które wspólnie z pracodawcą mogą (a często wręcz powinny) zainstalować monitoring, a następnie analizować zgromadzony za jego pomocą materiał dowodowy. Złożenie zawiadomienia o popełnieniu przestępstwa skutkować powinno także przerzuceniem na organ ścigania odpowiedzialności za podejmowane decyzje oraz zakres wprowadzonej kontroli. Co więcej, o ile złożone zawiadomienie skutkować będzie wszczęciem postępowania przygotowawczego, wówczas wszelkie działania, mające na celu



wykrycie sprawcy określonego przestępstwa, najprawdopodobniej przeprowadzone zostaną na koszt Skarbu Państwa. Z drugiej natomiast strony, uczciwie należy podkreślić, iż Prokuratura nie posiada odpowiednich narzędzi, umożliwiających identyfikację sprawcy wycieku tajemnicy przedsiębiorstwa, w szczególności, w spółce zatrudniającej kilkudziesięciu, bądź kilkuset pracowników. Co więcej, często okres dzielący złożenie zawiadomienia o popełnieniu przestępstwa od pierwszych czynności procesowych, jest na tyle odległy, ze straty poniesione przez przedsiębiorcę mogą okazać się już nieodwracalne.

W takim przypadku znacznie skuteczniejszymi działaniami, okazać powinny się te, podejmowane na własną rękę przez samego pracodawcę. Może on bowiem stosowny monitoring wprowadzić bezpośrednio po uzyskaniu wiedzy o naruszeniach prawa.

Przez cały czas, przedsiębiorca, nie może natomiast z pola widzenia stracić dwóch kryteriów, które zostały wskazane powyżej, tj. adekwatności i usprawiedliwionego celu podejmowanych działań. Samodzielnie gromadząc materiał dowodowy musimy także pamiętać, aby został on zabezpieczony w odpowiedni sposób oraz aby nie zgromadzić niczego ponad to, na co zezwala nam prawo. Innymi słowy, wskazanym jest, aby działania pracodawcy podejmowane były przy pomocy biegłego z zakresu informatyki śledczej oraz w asyście prawnika. Tak zgromadzony materiał można z powodzeniem przedstawić prokuraturze oraz wykorzystać jako podstawę do wyciągnięcia wobec pracownika konsekwencji służbowych (włącznie z rozwiązaniem stosunku pracy bez okresu wypowiedzenia). Wreszcie, w toku postępowania karnego, bądź cywilnego można starać się odzyskać od sprawcy środki, które utracone zostały celem jego wykrycia. ■

Technologia NetWitness skalowalna i elastyczna

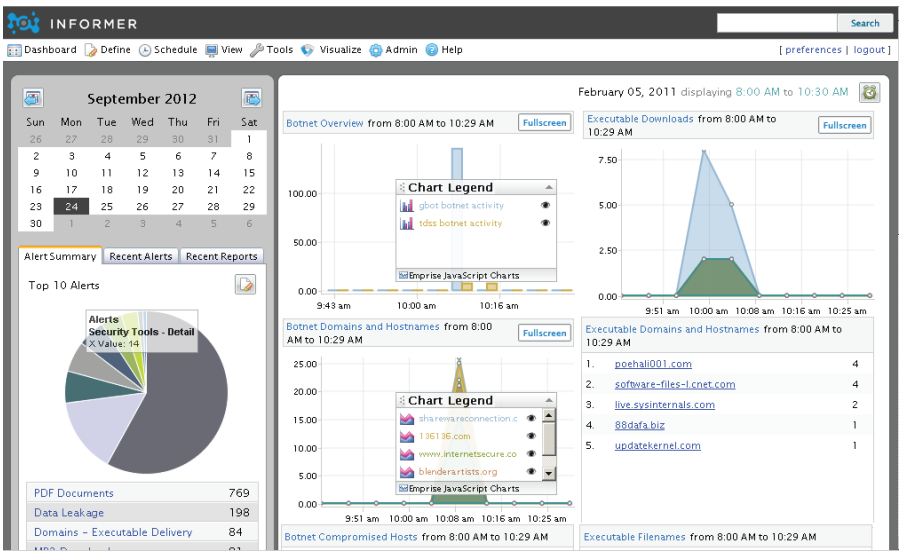
Adrian Wróbel

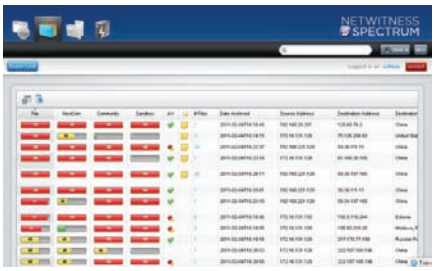
NetWitness jest technologią, która ma zabezpieczyć organizację przed wielopoziomowym zagrożeniem. Opierając się na gromadzeniu, przetwarzaniu i ciągłym analizowaniu całości ruchu sieciowego zapewnia ochronę przed takimi zagrożeniami jak zero-day, APT oraz tym najtrudniejszym do wykrycia, płynącym z wnętrza organizacji, od użytkownika działającego świadomie lub nie na szkodę przedsiębiorstwa. Rozwiązanie zbiera informację o stanie sieci i przepływających przez nią danych z całej infrastruktury począwszy od bram internetowych, newralgicznych punktów sieci czy połączeń sieciowych. NetWitness wykorzystując opatentowany proces ekstrakcji meta danych pozwala na ich szybką analizę. Terabajty danych, zapisanych na dyskach w uporządkowanej, hierarchicznej strukturze są przetwarzane w locie poprzez zaimplementowane rozwiązania sprzętowo-programowe. Dzięki temu całość jest w pełni skalowalna i elastyczna.

Warstwa programowa.

Sercem systemu jest moduł Investigator. Zapewnia on analizę sesji opartą na danych warstw 2 do 7 oraz dostęp w czytelnej i przejrzystej formie do milionów danych. Umożliwia wielowarstwową analizę biorąc pod uwagę praktycznie dowolne kryterium wyboru. Dzięki Investigator'owi można filtrować zdarzenia, pojedyncze akcję, wychwytywać błędy czy nieprawidłowości w zachowaniu urządzeń oraz użytkowników. Niewątpliwym atutem jest możliwość przeglądania zapisanych sesji w niezmienionej formie, widzianej dosłownie oczami użytkownika.

Równie istotnym modułem systemu jest Infromer. Odpowiedzialny jest za zarządzanie raportami oraz alarmowanie. Ułatwia znacząco pracę z modułem Investigator dzięki czytelnemu mechanizmowi ekspresji danych. W połączeniu z graficznym, w pełni renderowanym interfejsem zapytań – Visualize pozwala na generowanie i wyświetlanie raportów w ▶





postaci przeglądów zawartości, które następnie można swobodnie konfigurować (m.in. dzięki mechanizmom drill down) i wyświetlać np. na panelach multi-touch.
Nie bez znaczenia jest również moduł Spectrum, który nastawiony jest na analizę plików pod kątem możliwości wystąpienia zero-day lub APT.

Warstwa sprzętowa.

Dane, w postaci pakietów sesji są przechowywane na urządzeniu „Decoder". Jest on głównym źródłem zapisu, przygotowanym tak, aby dopasować go idealnie do infrastruktury niemal każdego przedsiębiorstwa. Z warstwy programowej generowanych jest miliony zapytań, które są następnie przetwarzane przez „Concentrator". Odpowiada on za agregację i analizę danych z wielu „Decoder'ów". W przypadku rozproszonych, dużych instalacji niezbędny jest „Broker" odpowiedzialny za rozdzielanie zapytań na całą infrastrukturę.
Całość została zaprojektowana aby w pełni odzwierciedlać pełny ruch sieciowy zapewniając przy tym zwiększenie poziomu bezpieczeństwa wewnętrznego organizacji oraz uchronienia się przed nieznanym zagrożeniem dla rozwiązań opierających się o sygnatury. ■

Jak przydusić Gaussa? Jak ugasić Flame?

Zbigniew Engiel

Zagrożenia związane ze szkodliwym oprogramowaniem w przypadku firm i instytucji już w najbliższym czasie mogą przejść do historii – twierdzą specjaliści z laboratorium informatyki śledczej Mediarecovery.

Potężny rynek programów antywirusowych coraz słabiej radzi sobie w realiach w których rocznie powstaje kilkaset milionów wersji szkodliwego oprogramowania. Dla przykładu, w ubiegłym roku pojawiło się ponad 403 miliony nowych odmian malware. Z drugiej strony firmy i instytucje coraz częściej padają ofiarą tzw. ataków APT czyli Advanced Persistent Threats. Polegają na ciągłych próbach ataku na daną firmę z użyciem różnorodnych i zaawansowanych technicznie metod.

Stuxnet, Duqu, Flame, Gauss

Wymienione cztery nazwy odnoszą się do znanych przykładów szkodliwego oprogramowania. Ich zaawansowanie, sposób działania i możliwości zaskakują ekspertów bezpieczeństwa. Co najgorsze zanim zostały rozpoznane i nazwane przez producentów programów antywirusowych miesiącami bezkarnie działały w sieciach wewnętrznych firm i instytucji wielu krajów na świecie – mówi Zbigniew Engiel z laboratorium informatyki śledczej Mediarecovery.

Producenci antywirusów przyznają się do słabości. Niską skuteczność programów antywirusowych dostrzegają sami producenci. Mikko Hypponen, Chief Research Officer u jednego z producentów programów antywirusowych w swoim artykule na łamach magazynu „Wired" przyznaje, iż przy obecnym poziomie zaawansowania cyberzagrożeń antywirusy mogą być skuteczne jedynie dla mniej wyrafinowanych przykładów szkodliwego oprogramowania.

Flame ugaszony zanim został nazwany

8 miesięcy wcześniej zanim pierwszy raz publicznie padła nazwa Flame w jednej z firm owo szkodliwe oprogramowanie próbowało wykraść interesujące jego twórców informacje. Próbowało, ponieważ firma używała rozwiązania Bit9 Parity, które m.in. uniemożliwia uruchomienie jakiekolwiek procesu, który nie jest zaufany. W sieci korporacyjnej nie jest w stanie funkcjonować nic co nie znajduje się na tzw. białej liście.

Gartner zaleca białe listy

John Pescatore, Wiceprezes Gartnera, posiadający 34 letnie doświadczenia w branży IT, w zaleceniach jednego ze swoich ostatnich raportów wskazuje używanie białych list wszędzie tam gdzie to możliwe. Gartner jest jedną z najbardziej poważanych instytucji przygotowujących raporty dotyczące rynku IT w ujęciu globalnym. Znalezienie się w słynnym kwadracie Gartnera dla wszystkich firm stanowi znaczące wyróżnienie.

Przyszłość bezpieczeństwa IT w whitelsitingu?

Jak mówią specjaliści z Mediarecovery – Rozwiązania takie jak Bit9 Parity, opierające się na białych listach z pewnością nie rozwiązują wszystkich problemów związanych z bezpieczeństwem. Są jednak punktem zwrotnym w podejściu do walki ze szkodliwym oprogramowaniem. Walkę z malware stawiają niejako na głowie, zamiast powolnego i mało efektywnego tworzenia baz sygnatur oferują specjalistom bezpieczeństwa proste i skuteczne w działaniu narzędzie ■

Badanie dotyczące bezpieczeństwa

Kancelaria Adwokatów I Radców Prawnych Ślązak, Zapiór i Wspólnicy przeprowadza obecnie projekt badawczy dotyczące bezpieczeństwa IT w polskich firmach. Projekt ma na celu ocenę świadomości zagrożeń naruszenia bezpieczeństwa informacji oraz stanu bezpieczeństwa informacji w przedsiębiorstwach państwowych i prywatnych, organizacjach, jednostkach samorządu terytorialnego, wagi, jaką podmioty te przywiązują do jej znaczenia oraz sposobów jej zabezpieczenia. Na tej podstawie zostanie przygotowany raport udostępniony wszystkim uczestnikom badania. Serdecznie zapraszamy do udziału http://www.kancelaria-szip.pl/Bezpieczna firma

Pełny stadion specjalistów analiz śledczych

Jak informuje Guidance Software, producent EnCase, do tej pory przeszkolono już 50 000 specjalistów. Gdyby zebrać ich w jednym miejscu to wypełnili by Stadion Narodowy w Warszawie prawie w całości. Pięćdziesięciotysięcznym ekspertem jest Amerykanin o polsko brzmiącym nazwisku – Christopher Nowicki z Komendy Policji w Schaumburgu, w stanie Ilinois. Jak sam przyznaje zdobytą na szkoleniach wiedzę wykorzystuje w codziennej służbie. Podobne szkolenia w Polsce organizuje Akademia Informatyki Śledczej.

Nowy produkt do analiz telefonów

Szwedzki producent narzędzia XRY do analiz śledczych telefonów komórkowych i smartfonów przygotowuje premierę nowego rozwiązania. XAMN, bo taką nazwę będzie nosiło, pozwoli na lepszą prezentację danych zebranych z wielu różnych urządzeń. Rozwiązanie będzie w pełni kompatybilne z XRY i pozwoli śledczym na tworzenie wykresów, złożonych siatek powiązań pomiędzy poszczególnymi użytkownikami telefonów wymienianych wiadomości lub połączeń.

APT vs ATP

20 września w Warszawie Mediarecovery zorganizowała konferencję „Advanced Persistent Threats vs Advanced Threats Protection". Przybliżono podczas niej zagadnienie jakim są nowe zaawansowane zagrożenia. Ataki APT charakteryzują się dużym stopniem zaawansowania, łączeniem wielu sposobów ataku poprzez socjotechnikę, szkodliwe oprogramowanie na atakach hakerskich kończąc. Kolejną cechą je wyróżniającą jest czas trwania. Cyberprzestępcy poświęcają wiele tygodni, a nawet miesięcy żeby osiągnąć interesujące ich efekty. Celem tego typu ataków są informacje, ofiarą - firmy i instytucje. Inżynierowie z laboratorium informatyki śledczej pokazali uczestnikom jak wykorzystać korelację i synergię pomiędzy kilkoma systemami bezpieczeństwa tak by jak najwyżej podnieść poziom bezpieczeństwa i wdrożyć w firmie Advanced Threats Protection.

Trojan w służbie ludzkości

Przemysław Krejza

W ostatnim czasie, oczywiście poza kryzysem, codzienność naszego życia co pewien czas wypełniają zamachy na naszą wolność i prawa osobiste (czyt. ACTA). Jak każdy wolny obywatel w sposób naturalny jestem szczerze zainteresowany tą tematyką. Tym razem, czytając sierpniowe newsy na Vagla.pl, natrafiłem na temat związany ze stosowaniem oprogramowania szpiegowskiego przez uprawnione organy w „służbie bezpieczeństwa i pokoju światowego". W myśl tej idei, co rusz podejmowane są próby legislacyjne umożliwiające wprowadzenie takich rozwiązań w życie - w sposób bardziej lub mniej jawny. Tym razem, zdaniem Wagli, stało się to w kontekście senackiego projektu zmiany ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu

Przeczytałem z uwagą dyskusję wokół tematu i postanowiłem podzielić się swoją refleksją na ten temat. Aby lepiej zrozumieć atmosferę, nie argumentując szczególnie, załóżmy że Wagla ma rację pisząc, że zmiany te „otwierają furtkę dla zastosowania tego typu oprogramowania", choć myślę, że nie popełnię błędu zakładając, iż w świetle przepisów obecnie obowiązującego art. 27 Ustawy jest to już możliwe. W określonych okolicznościach, bowiem sieć telekomunikacyjna może być siecią teleinformatyczną, a pojęcia „przekazywania" i „treść korespondencji" są wystarczająco elastyczne, aby wobec „bezskuteczności lub nieprzydatności innych środków", uzasadnić w wymaganym przez Ustawę wniosku użycie „lepszych" możliwości. A o tym, że tak jest, świadczy chociażby pomysł MSWiA z roku 2011 na stworzenie „Autonomicznych narzędzi wspomagających zwalczanie przestępczości", pod którymi kryje się właśnie oprogramowanie szpiegowskie.

Co więcej, po przeczytaniu ustawy, aktów związanych a nawet proponowanej przez Senat poprawki dojdziemy do wniosku, że służby mają całkowitą dowolność w doborze stosowanych środków technicznych, jeśli wypełniają określony ustawą cel np. zatrzymania treści korespondencji. I nie liczmy, że sąd okręgowy wydając decyzję na podstawie wniosku ABW będzie w stanie ocenić czy proponowane narzędzia są odpowiednie w danym przypadku...

A formalnie sprawa nie jest taka prosta jak się z pozoru wydaje, bo oprogramowanie szpiegowskie to nie podsłuch operacyjny. Tu możemy o wiele więcej – wystarczy zainfekować komputer podejrzanego i od tego momentu, bez większych kosztów i zaangażowania, wierny program szpiegowski będzie wysyłał określone (lub nie?) dane na swój zaufany serwer. No właśnie „zainfekować komputer". A przecież ustawowy wniosek musi zawierać „dane osoby lub inne dane pozwalające na jednoznaczne określenie podmiotu [...] wobec którego stosowana będzie kontrola operacyjna". A czy w sieci jesteśmy tylko numerem IP? Co się więc wydarzy, jeśli wskazany we wniosku numer IP, pod którym zidentyfikowano podejrzanego, to sieć osiedlowa? Jaką metodę infekcji wybierze prowadzący sprawę? Podpowiem, że ustawa nie wymaga specjalnego tłumaczenia się z tego aspektu, ponieważ przytoczony już wniosek powinien jedynie zawierać „cel, czas i rodzaj prowadzonej kontroli operacyjnej". A co z aspektem

MAGAZYN
INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

mediarecovery
Lider informatyki śledczej

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 032 782 95 95, fax 032 782 95 94
e-mail: redakcja@mediarecovery.pl

Redakcja
Zbigniew Engiel (red. nacz.),
Przemysław Krejza
Skład, łamanie, grafika: Marcin Wojtera
Reklama: Zbigniew Engiel

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 032 782 95 95, fax 032 782 95 94
e-mail: biuro@mediarecovery.pl

czasu? „Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące" oraz kontrola „powinna być zakończona niezwłocznie po ustaniu przyczyn jej zarządzenia, najpóźniej jednak z upływem okresu, na który została wprowadzona". Jak zostanie to zrealizowane w przypadku trojana? Zaprogramowanie go na określony czas raczej nie wchodzi w grę, ponieważ wiemy, że czas w komputerze „ofiary" może być inny niż rzeczywisty co może zaskutkować niezadziałaniem robala. Zatem może zostanie wydane mu polecenie deaktywacji? A co jeśli śledzony komputer nie pojawi się w sieci przez pół roku? Zakładam, że będzie jednak zbierał dane a po połączeniu z internetem posłusznie wyśle je na swój serwer. Ufając służbom oczywiście mamy pewność, że nadmiar informacji zostanie usunięty, ale jak zapewnimy rozliczalność i niezaprzeczalność tych działań? Dane informatyczne to przecież nie zapis rozmowy telefonicznej, której autentyczność możemy zweryfikować. Zapisane cyfrowo maile, dokumenty i inne informacje można w prosty sposób przygotować i zmodyfikować tak, jakby to robił trojan. A przecież dane operacyjne mogą być podstawą wszczęcia postępowania karnego, a to już wystarczy żeby komuś zaszkodzić. I konia z rzędem biegłemu, który będzie w stanie stwierdzić, że dane zostały spreparowane przez kogoś a śledztwo zostało wszczęte bez uzasadnienia. Takich wątpliwości wobec braku odpowiednich regulacji a nawet najlepszych praktyk mógłbym wysnuć jeszcze wiele. Ale nie chciałbym, aby ktoś z mojego krótkiego tekstu wyciągnął wniosek, że jestem przeciw. Otóż nie, nie jestem. W świecie, w którym żyjemy, gdzie przestępczość wykorzystuje nowoczesne środki przekazu, a szyfrowanie jest na porządku dziennym, oraz wobec braku innych możliwości walki z przestępczością i terroryzmem wymagane są odpowiednie środki. Państwo musi mieć możliwość zapewnienia bezpieczeństwa nam - obywatelom. Ale środki te są na tyle niebezpieczne i trudne do kontrolowania, że mechanizmy ich zastosowania wymagają gruntownego przemyślenia i takiego wprowadzenia w życie, żeby ich użycie nie wynikało z możliwości interpretacyjnych tej czy innej ustawy.
I to polecam rozwadze. ■