MAGAZYN

NR 20/GRUDZIEŃ 2013

www.mediarecovery.pl/magazyn

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Podsumowanie roku 2013 w informatyce śledczej

Karol Szczyrbowski

Malware okiem prawnika – część druga

Jarosław Góra

FireEye – jeszcze jedna „piaskownica" na rynku?

Tomasz Pietrzyk

Analiza danych transmisyjnych - czym ją wspomagać?

Mateusz Witański

UWAGA! KONKURS!

szczegóły na str. 2

Od redakcji

20 numer Magazynu Informatyki Śledczej zbiega się z końcem 2013 roku, w którym może nie odnotowano przełomowych premier urządzeń sprzętowych w obszarze informatyki śledczej, jednak pojawiły się nowe metody, takie jak Triage i Live Forensic, które wręcz w rewolucyjny sposób ułatwiają pracę informatyków śledczych.

Wydarzeniem w 2013 roku, o którym nie sposób nie wspomnieć, to ujawnienie przez Edwarda Snowdena jednego z największych przecieków w historii amerykańskich służb specjalnych. To dzięki temu 29-letniemu informatykowi pracującemu dla Narodowej Agencji Bezpieczeństwa, świat dowiedział się że amerykański rząd na masową skalę szpieguje internautów na całym świecie.

Rok 2013 to czas w którym dość często pojawiały się w mediach informacje o wycieku haseł z różnych serwisów do Internetu, czy o skutecznych atakach hakerskich, których ofiarami padły różne instytucje. Specjaliści Mediarecovery szacują, że tylko w 2012r. z atakami hakerskimi zetknęło się 2/3 firm, a już teraz możemy stwierdzić, że mijający rok pod tym względem nie był lepszy.

Zagrożenia związane z cyberprzestępczością przenoszą się z komputerów na urządzenia mobilne takie jak tablety czy smartfony. Prognozy pokazują, że w roku 2014 ze względu na dalszy rozwój rynku mobilnego, a co za tym idzie przenoszenia coraz większej ilości danych na te urządzenia, rozwiązania typu Mobile Device Management (MDM), będą się cieszyć dużym zainteresowaniem wśród działów IT w firmach i instytucjach.

Jednego możemy być pewni – informatyka śledcza oraz bezpieczeństwo IT będą popularnymi tematami w Nowym Roku.

Redakcja Magazynu Informatyki Śledczej i Bezpieczeństwa IT

Konkurs

- Interesujesz się informatyką śledczą?
- Wiesz jak odpowiednio dokonać zabezpieczenia dowodów elektronicznych?
- Chcesz podzielić się swoją wiedzą i doświadczeniem w zakresie informatyki śledczej?

Atrakcyjne nagrody czekają.

Tableau SATA TK3u jest blokerem zapisu stworzonym dla dysków SATA. Jako jeden z nielicznych posiada bezpośrednią obsługę dysków z interfejsem Serial-ATA (bez użycia adaptera). TK3u jest kompatybilny z portami SATA1 i SATA 2.

Bezpłatny udział w wybranym szkoleniu Akademii Informatyki Śledczej

Kurtka Softshell, koszulka i torba Mediarecovery

Szczegóły konkursu znajdują się na stronie www.mediarecovery.pl/konkurs

Podsumowanie roku 2013 w informatyce śledczej

Karol Szczyrbowski

Rok 2013 był ciekawym czasem w obszarze informatyki śledczej. Choć nie było spektakularnych premier sprzętowych to nie można powiedzieć, że producenci siedzieli z założonymi rękoma.

Nowe wersje oprogramowania

Najwięksi gracze na rynku oprogramowania do informatyki śledczej, czyli firmy Guidance Software oraz AccessData cały czas pracują nad udoskonalaniem swoich produktów ku uciesze ich użytkowników. Sztandarowy produkt Guidance Software (GS) - EnCase doczekał się już wersji 7.08.02, a najważniejszy program ich konkurencji, czyli Forensic Toolkit (FTK) jest już w wersji 5.0.1. Przy okazji warto wspomnieć, ile zamieszania w środowisku informatyków śledczych wywołały zmiany w nowej wersji EnCase w stosunku do wersji oznaczonej numerem 6. Były one na tyle rewolucyjne, że jego producent zaczął tworzyć materiały pomocnicze oraz szkolenia dotyczące przejścia z wersji 6 na 7. W przypadku FTK, przejście z wersji 4.x do nowej, piątej wersji, nie stanowiło dla większości użytkowników problemu, gdyż zmiany nie dotknęły tak bardzo nawigacji oraz interfejsu. Dodając smaku w konkurowaniu między sobą tych dwóch firm, warto wspomnieć, że GS stworzył darmowy program EnCase Forensic Imager, będący odpowiedzą na również bezpłatny FTK Imager, który zdobył już szerokie grono użytkowników. Jeżeli takie konkurowanie ze sobą będzie służyć poprawie jakości tych rozwiązań, to użytkownicy powinni się tylko cieszyć. Trzeci program z czołówki oprogramowania do informatyki śledczej, tj. X-Ways Forensics w tym roku doczekał się już wersji 17.4, co nie powinno dziwić, ze względu na jego częste aktualizacje.
Dużym zainteresowaniem w mijającym roku odnotowało oprogramowanie Triage, które można wykorzystać w przypadku prewencyjnego badania komputera lub podczas zabezpieczania materiału dowodowego, wykorzystując metodologię wstępnej analizy, np. w celu uniknięcia zabezpieczenia zbyt dużej ilości komputerów. Tematyka to została opisania w poprzednim numerze Magazynu Informatyki Śledczej, który można pobrać ze strony mediarecovery.pl/magazyn

Nowe rozwiązania sprzętowe

Mijający rok nie przyniósł rewolucji sprzętowej. Firma Tableau nadal rozwija wprowadzone w 2012 roku rozwiązania, wykorzystujące szybką technologię USB 3.0, czyli bloker sprzętowy T35U oraz duplikator TD3. Wspomniany produkt w ostatnich tygodniach 2013 roku bądź na początku 2014, ma otrzymać dodatkową kieszeń na twardy dysk oraz aktualizację oprogramowania. Wprowadzone zmiany, pozwalają na tzw. twinning, czyli możliwość wykonywania kopii binarnej na dwóch dyskach docelowych jednocześnie. Funkcja znana z poprzedniej wersji duplikatora TD2, dla wielu użytkowników była brakującym elementem, który utrudniał efektywne korzystanie z urządzenia. Jednak firma Tableau posłuchała głosu swoich klientów i ponownie wprowadziła to rozwiązanie do najnowszej wersji swojej kopiarki.
Nowością, godną polecenia jest natomiast kieszeń T3iu Forensic SATA Imaging Bay. Posiada ona wbudowany bloker sprzętowy oraz obsługuje dyski SATA 3,5 i 2,5 cala. Urządzenie to pozwoli nam na uniknięcie bałaganu wokół naszej stacji roboczej oraz na szybki montaż dysków w celu wykonania kopii binarnej, bądź przeglądu zawartości bez ingerencji w dane.

Lektura obowiązkowa dla informatyków śledczych

Każdy informatyk śledczy powinien poszerzać swoją wiedzę i być na bieżąco z nowinkami technicznymi, zwłaszcza tymi, które mogą wpłynąć na jego pracę. Książka Harlana Carvey'a „Analiza śledcza i powłamaniowa. Zaawansowane techniki prowadzenia analizy w systemie Windows 7. Wydanie III", została w połowie tego roku wydana w Polsce i jest polecana każdej osobie zajmującej się informatyką śledczą, bądź bezpieczeństwem komputerowym. Warto się z nią zapoznać by usystematyzować posiadaną wiedzę, oraz poznać nowe interesujące zagadnienia. Nadal brakuje takich publikacji na polskim rynku, ale może w 2014 roku sytuacja ulegnie poprawie.
W Nowym Roku życzę wszystkim informatykom śledczym oraz osobom związanym zawodowo z bezpieczeństwem IT wielu spokojnych analiz, niezaszyfrowanych dysków oraz szybkich transferów danych.

Autor jest młodszym specjalistą informatyki śledczej w laboratorium Mediarecovery.

MAGAZYN
INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

mediarecovery
Lider informatyki śledczej

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

Redakcja
Sebastian Małycha (red. nacz.),
Przemysław Krejza
Skład, łamanie, grafika: Marcin Wojtera
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

FireEye – jeszcze jedna „piaskownica" na rynku?

Tomasz Pietrzyk

Od kilku lat (wg różnych źródeł od czasu wykrycia ataku znanego jako Operacja Aurora w 2009r.) wśród zagrożeń, z jakimi walczymy, następuje coraz szybsza ewolucja metod ataków i sposobów ukrywania złośliwego kodu. Ataki są wieloetapowe i poprzedzają je przygotowania, które mają wykryć luki w zabezpieczeniach umożliwiających dotarcie do zaatakowanej instytucji, w sposób niewykrywany przez klasycznie stosowane zabezpieczenia.

Sam atak jest trudny do wykrycia, a jego konsekwencje poważne - wyprowadzenie chronionych danych, przejęcie kontroli nad zainfekowanymi komputerami, dotarcie za ich pośrednictwem do innych zasobów firmy, wykorzystanie zainfekowanych maszyn do prowadzenia ataków na inne instytucje. Co w konsekwencji prowadzi często do zniszczenia reputacji firmy. Ogólnie tego typu zagrożenia są określane jako advanced malware (czasami też jako zero-day, APT – advanced persistent threat lub TPT – targeted persistent threat).
Wraz ze wzrostem ilości i niestety, skuteczności tego typu ataków, od pewnego czasu narasta problem zabezpieczenia się przed takimi zagrożeniami.

Najpopularniejsze obecnie zabezpieczenia (nazywane dalej zabezpieczeniami klasycznymi) bazują przede wszystkim na wcześniejszej znajomości ataku: na sygnaturze pliku (suma kontrolna, wzorce bajtów/bitów), reputacji strony web/domeny pocztowej, czarnych listach (blacklist) adresów IP/domen. Definicje te są uzupełniane często tzw. heurystyką czyli mechanizmem odnajdowania podobieństw do wcześniej opisanych zagrożeń.

Ochrona z użyciem takich mechanizmów jest realizowana przez zdecydowaną większość klasycznych zabezpieczeń: systemy antywirusowe (AV) na stacjach i serwerach, gateway'e web i email, rozwiązania IPS, firewalle Next Generation i UTM, itp.

W każdej z tych metod detekcji ataku, aby wykrywanie kolejnego wystąpienia zagrożenia było skuteczne musimy zakładać, że:

- producent rozwiązania posiada dostęp do danych z pierwszego ataku – nie zawsze jest to możliwe, jeśli atak jest celowany, przeznaczony dla jednego lub kilku celów, wykorzystuje nieznane wcześniej podatności aplikacji lub systemu operacyjnego (wg badań firmy FireEye około 61% wykrywanych ataków to ataki, które nie powtórzyły się w innych miejscach).
- producent potrafi poprawnie przeanalizować dane (to również może stwarzać problem w przypadku advanced malware), ale mogą trafić do niego tylko niektóre pliki wykorzystane w ataku, a dodatkowo zaszyfrowane lub w inny sposób zaciemnione (obfuscated).
- producent posiada odpowiednio dużo czasu na opracowanie definicji opisującej atak (np. sygnatury dla produktów bezpieczeństwa) i jej przetestowanie celem uniknięcia tzw. false positive, czyli niepoprawnych wykryć ataku.
- klient korzystający z rozwiązania bezpieczeństwa musi posiadać pewien czas na ściągnięcie nowych definicji ataku, rozesłanie ich do wszystkich produktów zabezpieczających jego sieć i komputery, a czasami też na przetestowanie nowych definicji w warunkach laboratoryjnych dla upewnienia się, że nie spowodują problemów w sieci produkcyjnej.

Wszystkie te etapy przygotowania i rozpowszechnienia definicji ataku tworzą tzw. dziurę bezpieczeństwa (security gap), w której sieć i zasoby Klienta są narażone na ataki przeciwko którym nie chronią klasyczne sposoby zabezpieczeń. Problem staje się jeszcze bardziej skomplikowany, kiedy weźmiemy pod uwagę, że czas życia próbki malware jest liczony w pojedynczych godzinach – potem ten sam atak jest wykonywany z użyciem innego pliku. Podobnie dzieje się ze źródłami ataków – zainfekowane strony web czy adresy pocztowe, skąd pochodzi zagrożenie

są rejestrowane i działają przez kilka dni lub nawet godzin, a kolejne infekcje pochodzą już z zupełnie innych źródeł.

Stosowane przez advanced malware techniki modyfikowania kodu, używanie coraz to nowych domen web/email i adresów IP powoduje, że nie jest praktycznie możliwe określenie sygnatury ataku, zdefiniowania reputacji domeny i adresu IP, czy umieszczenie ich na listach blacklist. Szybko modyfikowany kod złośliwy powoduje, że nie można na czas dostarczyć sygnatury wykrywającej taki atak.

Ważną cechą nowoczesnych ataków jest ich wielo-etapowość. Można wskazać następujące charakterystyczne etapy ataku:

1. *Exploit* – mały kod umieszczony zwykle na stronie web lub przenoszony w spreparowanym załączniku do email, który ma za zadanie uruchomić proces infekcji stacji przez wykorzystanie, często nieznanej wcześniej, podatności aplikacji, przeglądarki, wtyczki do niej, czy systemu operacyjnego. Exploit inicjuje kolejne fazy ataku.

2. *Malware / Dropper* – kod używany do przygotowania „środowiska pracy" dla malware, a często też właściwy kod ataku. Malware jest zwykle ściągany przez exploita, który też uruchamia jego instalację, wcześniej wykonując na przykład jego deszyfrację.

3. *Callback* – komunikacja zwrotna z zainfekowanej stacji do serwera Command and Control (CnC) kontrolowanego przez cyberprzestępcę. Callback może służyć do wysłania zgromadzonych danych podczas ataku, informowania o skutecznej infekcji, pobrania kolejnych części kodu ataku lub aktualizacji kodu ataku, czy wreszcie do otwarcia połączenia umożliwiającego zdalną kontrolę nad stacją i oczekiwanie na instrukcje.
4. Rozpowszechnienie się ataku na inne stacje w organizacji i pozyskiwanie danych z firmy.

Skutecznie wykonany atak z użyciem advanced malware jest trudno wykrywany wewnątrz chronionej sieci.

Skutecznie wykonany atak z użyciem advanced malware jest trudno wykrywany wewnątrz chronionej sieci. Poprzez zainfekowane komputery, intruzi zdobywają chronione dane oraz uzyskują dostęp do innych, wewnętrznych zasobów. Infekcja pozwala często na zdalne przejęcie kontroli nad stacją i może posłużyć do jednokrotnego ataku lub dostęp może być sprzedany „zainteresowanym" cyberprzestępcom.

Czy więc wszystkie dotychczasowe inwestycje w zabezpieczenia były nietrafione? Oczywiście nie można tak powiedzieć... Pomimo rosnącego znaczenia ataków advanced malware cały czas mamy do czynienia z atakami, które są szeroko rozpowszechniane. Dla przykładu spam, malware typu ransomware, który z założenia przynosi profity atakującemu kiedy jak najwięcej komputerów jest zainfekowanych, itp. W tych wypadkach szansa, że nasz producent AV pozyskał próbkę ataku jest dużo większa i rośnie też prawdopodobieństwo, że opublikowane przez niego sygnatury ochronią nas przed takimi atakami. No chyba, że to my jesteśmy tym pierwszym zaatakowanym celem...
Poza tym bezpieczeństwo IT to nie tylko wykrywanie malware, to także filtracja dostępu, kontrola uprawnień, monitorowanie dostępu, itd.

Niemniej musimy mieć na uwadze, że korzystanie tylko z klasycznych rozwiązań bezpieczeństwa nie umożliwia skutecznej ochrony przed aktualnymi zagrożeniami.

Jak sobie radzić?
Niekończący się wyścig między zagrożeniami i sposobami ich wykrywania prowadzi do wprowadzania nowych metod ochrony przed najnowszymi atakami. Podobnie jest w przypadku omawianych poniżej rozwiązań do automatycznej, dynamicznej analizy malware. Rozwiązania te stanowią kolejny etap rozwoju systemów zabezpieczeń, odpowiadając na zmiany w zagrożeniach i dodając następną warstwę ochrony.

Analiza „static" (statyczna) to rozwiązania, które były tu już wspominane – klasyczne zabezpieczenia korzystające z wcześniejszej wiedzy o ataku. Nowością są systemy analizy dynamicznej (dynamic), które w końcu zostały dostosowane do potrzeb firm i instytucji opuszczając mury laboratoriów zajmujących się analizą malware.

Na czym polega analiza dynamiczna? Ogólnie można podsumować ją jako badanie zachowania podejrzanego obiektu w kontrolowanym środowisku wyposażonym w instrumenty do wykrywania tego zachowania i wnioskowania na jego podstawie czy mamy do czynienia z zagrożeniem czy jednak nie. Nie ma tu więc stosowania sygnatur opisujących konkretny atak. Najczęściej analiza jest wykonywana na maszynach wirtualnych, które łatwo można kopiować, zamykać, otwierać, a przede wszystkim mogą być jednocześnie uruchamione na tym samym sprzęcie. Często systemy do analizy dynamicznej zachowania kodu są nazywane sandboxami.

Dynamiczna analiza może być dalej podzielona na:
• analizę pojedynczych obiektów (discrete object analysis).
• analizę kontekstową (contextual analysis) – często określana też jako analiza „flow" lub „sesji".

Rozwiązania FireEye, jako jedyne na rynku, realizują dynamiczną analizę ataków badając ich zachowanie w ujęciu kontekstu ataku, nie tylko pojedynczych, wybranych obiektów.

Koniec części pierwszej. ■

Autor jest inżynierem systemowym w firmie FireEye. Od ponad 10 lat rozwija swoje doświadczenie i pasje, które są związane z dziedzinami bezpieczeństwa IT. W ostatnim czasie szczególnie interesuje się rozwiązaniami sieciowymi zabezpieczającymi przed nowymi zagrożeniami.

Analiza danych transmisyjnych – czym ją wspomagać?

Mateusz Witański

W jednym z poprzednich numerów Magazynu Informatyki Śledczej i Bezpieczeństwa IT mogliśmy zapoznać się z metodą analizy danych transmisyjnych central telefonicznych. W artykule tym przedstawionych zostało osiem kroków, które powinniśmy przejść, aby dokonać fachowej oceny materiału, jaki trafia do nas z firm użytkujących abonenckie centrale telefoniczne. Wśród tych ośmiu kroków były takie zadania, jak np. stworzenie schematu przeszukiwania, analiza pól rekordu taryfikacyjnego, wyodrębnienie interesujących rekordów itp. Na pierwszy rzut oka może wydawać się to dosyć proste, szczególnie dla osoby, która nie miała do czynienia z rekordami taryfikacyjnymi central telefonicznych. Sprawa znacząco się komplikuje, gdy dostajemy do ręki materiał do analizy.

Trudność związana z analizą danych transmisyjnych central abonenckich, a także danych źródłowych central operatorskich, wynika przede wszystkim z braku standardu w zakresie rekordu taryfikacyjnego, a co za tym idzie dowolnością producentów w kształtowaniu zawartości i formy takiego rekordu.

Centrala telefoniczna to urządzenie teleinformatyczne, pracujące w odpowiednim środowisku informatycznym, generujące dane w postaci plików tekstowych bądź binarnych. Wręcz prosiłoby się o wykorzystanie narzędza informatycznego do wykonania analizy, które spośród wszystkich danych wyszuka te, które spełniają nasze kryteria poszukiwań. Narzędzia, które porówna dane z kilku źródeł i wychwyci wszelkie zależności między tymi danymi. Narzędzia, które po przeprowadzeniu analizy pokaże nam raport będący podstawą dla dalszego wnioskowania. Narzędzia, którego na razie na rynku nie ma.

Pozostaje więc posiłkowanie się dostępnymi na rynku systemami taryfikacyjnymi oraz oprogramowaniem do analizy kryminalnej. Niedoświadczoną osobę działanie to może zaprowadzić w ślepy zaułek. Trzeba bowiem znać specyfikę tych systemów, aby odpowiednio je wykorzystać. Oprogramowanie do analizy kryminalnej korzysta z zestawień billingowych, a więc z przetworzonych już danych, z których próbuje wydobyć powiązania danego numeru. Odpowiednio użyte, narzędzia te mogą ułatwić pracę analityczną, gdyż na etapie wstępnego przeglądu mogą pokazać, co zawiera plik z danymi oraz na co trzeba zwrócić szczególną uwagę w trakcie dalszych prac. Nie są jednak narzędziami, na których powinno opierać się analizę danych transmisyjnych central telefonicznych.

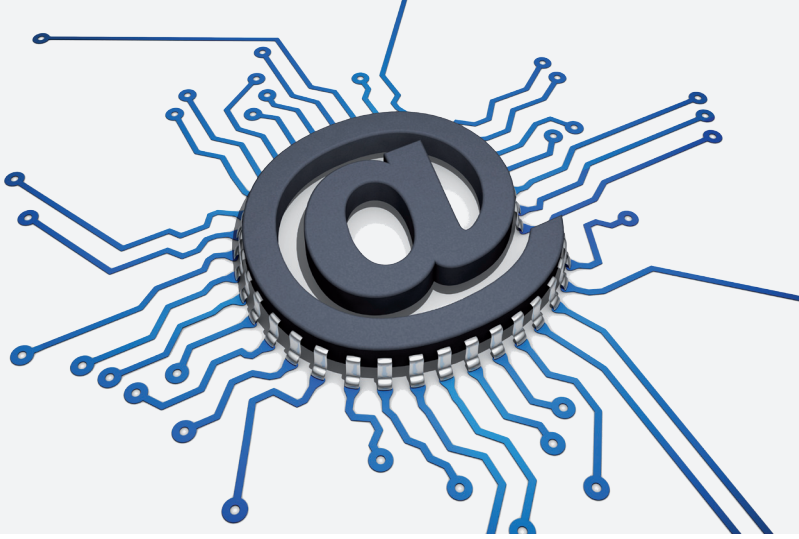
Czego więc należałoby oczekiwać od profesjonalnego narzędzia służącego wspomaganiu analizy danych transmisyjnych central telefonicznych? Jakie cechy powinna taka aplikacja posiadać, aby w pełni móc wspierać pracę informatyków śledczych? Wydaje się, że narzędzie takie powinno cechować się przede wszystkim łatwością obsługi i wszechstronnością. Powinno posiadać minimalną ilość elementów konfigurowalnych i możliwość przetwarzania danych z maksymalnie dużej liczby central. Oprogramowanie powinno mieć zaimplementowane wszystkie algorytmy, aby dać nam satysfakcjonujący wynik. Jak stwierdzili kiedyś prof. Jan Widacki i prof. Jerzy Konieczny, analiza danych transmisyjnych jest niezwykle trudna z uwagi na skomplikowany charakter materiałów dostarczanych przez operatorów telekomunikacyjnych. Jeżeli do tego dodamy jeszcze jego różnorodność, będziemy mogli wyobrazić sobie, z czym mamy do czynienia. Niech powyższe zobrazuje przykład. Jeżeli chcemy znaleźć w pliku źródłowym, kto podczas naszej nieobecności odebrał skierowaną do nas rozmowę telefoniczną, będziemy musieli wykonać kilka zadań bądź wykorzystać odpowiadające im moduły. Po pierwsze, będziemy musieli skorzystać z modułu pobierającego dane z centrali. Po drugie, będziemy musieli skorzystać z modułu importującego te dane do bazy danych. Po drugie bis, być może wykorzystamy moduł pobierający konfigurację centrali lub moduł rozpoznający typ centrali po importowanym pliku. Po trzecie, będziemy musieli skorzystać z modułu przetwarzającego uzyskane dane do postaci czytelnej dla nas. Po czwarte, będziemy musieli skorzystać z modułu analizowania zawartości pliku. Po piąte, będziemy musieli skorzystać z modułu wprowadzania warunków przeszukiwania pliku. Po szóste, będziemy musieli ... tak wymieniać moglibyśmy jeszcze długo.

Warto pamiętać o jednej rzeczy, która szczególnie informatykom śledczym powinna być bliska. Jeżeli korzystamy z danego rozwiązania informatycznego, nawet najbardziej profesjonalnego i dedykowanego dla danego rodzaju analizy, musimy brać pod uwagę wszelkie braki tego oprogramowania i ewentualne błędy, jakie mogą pojawić się podczas przeprowadzania analizy. Nie ma bowiem na chwilę obecną idealnego rozwiązania. ■

Autor jest specjalistą w zakresie billingów w aspekcie handlowym, technicznym i prawnym oraz biegłym sądowy w zakresie analizy danych transmisyjnych generowanych przez centrale telefoniczne.

Malware okiem prawnika – część druga

Jarosław Góra



Wirusy, robaki, trojany i wreszcie zaawansowany malware. W poprzednim artykule dotyczącym złośliwego oprogramowania poruszyłem kwestie związane z odpowiedzialnością karną cyberprzestępców i innych podmiotów posługujących się malwarem. Dziś postaram się opisać jak sprawa wygląda z cywilistycznego punktu widzenia i jak kształtuje się odpowiedzialność osób, które posługują się malwarem, podmiotów świadczących szeroko rozumiane usługi w cyberrzeczywistości i innych użytkowników Internetu.

Okiem prawnika

Na skutek złośliwego oprogramowania osoby, które padają ofiarą jego działania często ponoszą realne szkody. Z jednej strony chodzi o bezpośrednie skutki działania malware-u, takie jak utrata, zmiana lub wyciek posiadanych informacji (często stanowiących tajemnice przedsiębiorstwa lub dane osobowe i informacje poufne), nieprawidłowe działanie lub uszkodzenie systemu (np. strony internetowej e-sklepu, ERP przedsiębiorstwa), czy nawet sprzętu. Z drugiej strony chodzi o skutki pośrednie, takie jak utrata zysku spowodowana niedziałającym systemem, utratę lub brak pozyskania klientów, koszty naprawy systemu, czy wreszcie prozaiczna kradzież środków pieniężnych z konta (po przejęciu przez przestępcę danych dostępu).

Na skutek złośliwego oprogramowania osoby, które padają ofiarą jego działania często ponoszą realne szkody.

Kto ponosi odpowiedzialność za działania malwaru? Jego twórca? Osoba, która zainfekowała system złośliwym oprogramowaniem? Dostawca usług w Internecie? Podmiot odpowiedzialny za bezpieczeństwo? Jak to zwykle w takich sprawach odpowiedź brzmi: to zależy.

Zgodnie z ogólną zasada prawa cywilnego kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia. Odpowiedzialność można przypisać, jeśli spełnione zostaną następujące przesłanki: bezprawność czynu, szkoda, związek przyczynowy między czynem, a szkodą oraz zawinienie. Bezprawność zachowania polega na przekroczeniu mierników i wzorców wynikających zarówno z wyraźnych przepisów, zwyczajów, utartej praktyki, jak i zasad współżycia społecznego. Nie ogranicza się zatem do naruszania konkretnych przepisów.

W przypadku posługiwania się złośliwym oprogramowaniem przez cyberprzestępcę na pewno będziemy mieli do czynienia z czynem bezprawnym, bo obok faktu, iż działanie takie naruszać może kilka przepisów kodeksu karnego, to z całą pewnością będzie to działanie naruszające zasady współżycia społecznego. Na skutek tego działania ktoś doznaje szkody, a związek między tymi dwoma faktami również nie budzi wątpliwości. Cyberprzestępcy działającemu z premedytacją przypiszemy również winę, zatem jego odpowiedzialność, np. odszkodowawcza, zazwyczaj będzie bezsprzeczna. Co w przypadku innych osób? Gdy podmiot zobowiązany do jakiegoś zachowania zaniecha go lub nie dopełni obowiązku, albo na skutek swojego zachowania, którego nie powinien podejmować doprowadzi do zainfekowania jakiegoś systemu złośliwym oprogramowaniem i w rezultacie szkody, również może odpowiadać względem poszkodowanego. Jeżeli zatem bank zobowiązał się do zapewnienie bezpieczeństwa swojego systemu bankowości elektronicznej, a dopuści do tego, aby ten został zainfekowany złośliwym oprogramowaniem, na skutek czego klienci banku poniosą szkody, bank będzie odpowiedzialny wobec swoich klientów. Oczywiście będzie miał roszczenia wobec cyberprzestępcy, jeśli tego uda się ustalić.

Podobnie sytuacja będzie się kształtować z innymi podmiotami świadczącymi usługi w cyberświecie – jeśli nie dopełnią swoich zobowiązań, wynikających z umów i obowiązujących przepisów, na skutek czego złośliwe oprogramowanie doprowadzi do powstania szkód, mogą ponieść odpowiedzialność. W związku z powyższym częstą praktyką usługodawców jest ograniczanie swojej odpowiedzialności poprzez konstruowanie odpowiednich zapisów w umowach, czy regulaminach.

W praktyce spotkałem się kiedyś z ciekawą sprawą, kiedy na skutek złośliwego oprogramowania strona internetowa zaczęła generować dużą ilość transferu. Właściciel strony miał podpisaną umowę z hostem, w której określono górny limit transferu danych na dany okres rozliczeniowy, po przekroczeniu którego host naliczał dodatkową opłatę. Właściciel strony zorientował się, że coś jest nie tak i zablokował sztucznie generowany transfer, ale nie uniknął konieczności uregulowania rachunku za przekroczenie limitu. Czy słusznie?

I znów, to zależy komu przypisać odpowiedzialność za zaistniałą sytuację. Jeżeli w umowie z hostem ten zobowiązał się, bez ograniczeń, do zapewnienie bezpieczeństwa na poziomie serwerów, na których zainstalowano stronę internetową i właśnie tam doszło do infekcji, właściciel strony mógłby mieć roszczenia do hosta. Jeśli natomiast do infekcji doszło na poziomie administrowania stroną, np. poprzez komputer właściciela strony, to raczej wina leży po jego stronie. Powyższe oznacza, że każdy przypadek należy badań indywidualnie. Z całą pewnością odpowiadać będzie osoba, która doprowadziła do infekcji, jednak tą zazwyczaj najtrudniej ustalić. Co więcej, na skutek zainfekowania naszego systemu malwarem sami, nieświadomie, możemy dalej rozprzestrzeniać „zarazę" lub bezwiednie uczestniczyć w działalności przestępczej, jako element botnetu, albo „dystrybutor" nielegalnych treści (np. chronionych prawem autorskim), czy też spamu. Wtedy poszkodowani mogę zwrócić się ze swoimi roszczeniami w naszą stronę i unikniemy odpowiedzialności wtedy, gdy udowodnimy, że nie uchybiliśmy żadnym obowiązkom (nasze działanie nie było bezprawne).

Autor jest szefem Zespołu Prawa IP i Nowych Technologii w kancelarii Ślązak, Zapiór i Wspólnicy, Kancelaria Adwokatów i Radców Prawnych. Specjalizuje się w zakresie prawa własności intelektualnej i nowych technologii. Prelegent na wielu konferencjach, a także prowadzący szereg szkoleń związanych z IP, IT oraz bezpieczeństwem informacji. Trener w ramach Akademii Informatyki Śledczej.