NR 3 | WRZESIEŃ 2009

Magazyn informatyki śledczej

Temat numeru

W trzecim numerze Magazynu informatyki śledczej prezentujemy czytelnikom zagadnienia związane z „piractwem komputerowym".

Z problemem tym spotykają się policjanci i prokuratorzy z całego Kraju. Jak szacuje Business Software Alliance straty producentów oprogramowania w Polsce z powodu piractwa wyniosły ponad 680 milionów dolarów. Z drugiej strony firma AuditPro kilka tygodni temu opublikowała raport na podstawie audytów legalności oprogramowania w polskich firmach i urzędach. Wynika z niego, że całkowity udział „piractwa" na audytowanych komputerach wyniósł ponad 33%. Z czego w administracji publicznej 39%, a w firmach prywatnych 28%. Odsetek nielegalnego oprogramowania u użytkowników prywatnych jest zapewne zdecydowanie wyższy. Podchodzimy do zagadnienia poważnie, choć zamieszczamy również jeden tekst z przymrużeniem oka.

W bieżącym numerze pojawia się też kolejna część cyklu „Zabezpieczanie elektronicznych nośników informacji". Tym razem autor skupia się na przygotowaniu do przeprowadzenia zabezpieczenia oraz samym zabezpieczaniu. A na zakończenie można zapoznać się z kolejnym przykładem z życia wziętym.

e-MIŚ

Wszystkich Czytelników, którzy chcieliby otrzymywać wersję elektroniczną Magazynu informatyki śledczej prosimy o przesłanie e-maila na adres:

redakcja@mediarecovery.pl

...wpisując w tytule PDF. Od 4 numeru Magazynu będziemy oprócz wersji papierowej dystrybuować również wersję elektroniczną. Dotychczasowe numery Magazynu są dostępne pod adresem:

www.mediarecovery.pl/magazyn

W następnym numerze

Skupimy się na zagadnieniu przechwytywania danych ulotnych czyli informacji pojawiających się w pamięci RAM. Temat zainteresuje z pewnością wszystkich tych Czytelników, którzy mieli do czynienia z kradzieżą danych związanych z bankowością internetową.

Zabezpieczanie elektronicznych nośników informacji - część 3.

Przestępstwa z użyciem komputera

Przemysław Krejza

W poprzednich częściach cyklu omówiliśmy podstawowe cechy dowodu elektronicznego oraz przedstawiliśmy przykładową sprawę, w której zachodzi konieczność zabezpieczania dowodów elektronicznych. Niniejsza część poświęcona jest przygotowaniu do przeprowadzenia zabezpieczania oraz samemu zabezpieczaniu.

Rozpoznanie operacyjne

Z technicznego punktu widzenia zabezpieczanie dowodów powinno być poprzedzone zwiadem operacyjnym w celu określenia środowiska informatycznego, ilości komputerów i środowiska w jakim pracują. Dzięki temu możliwe będzie przygotowanie właściwej ilości zasobów ludzkich, planów awaryjnych oraz dobór właściwych środków informatycznych czy ekspertów. **Niewłaściwe przygotowanie operacji może doprowadzić do sytuacji, w której zamiast oczekiwanego jednego komputera zastaniemy ich sto połączonych w sieci lokalnej, połączonych z kilkusetkilogramowym serwerem.** W efekcie może dać to czas podejrzanemu na usunięcie dowodów lub radykalnie przedłuży zadanie.

Rozpoznanie operacyjne w ramach przytoczonego powyżej przykładowego postępowania powinno przede wszystkim zakładać sprawdzenie ustalonego adresu. Załóżmy, że będzie to dom jednorodzinny. Możemy zatem przyjąć, że zabezpieczenie nie będzie wymagało szczególnych środków technicznych. Do rozważenia pozostaje kwestia zabezpieczenia sprzętu czy danych.

Bardziej skomplikowane sprawy będą wymagały jednak dodatkowych działań. W przypadku większych środowisk informatycznych wskazany jest kontakt z odpowiednim biegłym już na etapie rozpoznania operacyjnego w celu właściwego przygotowania zabezpieczenia.

Zabezpieczanie dowodów

Moment zabezpieczania dowodów elektronicznych opiera się o problem uwierzytelnienia dowodów w sposób nie pozostawiający wątpliwości, że zostały one uzyskane z danego komputera w określonym miejscu i czasie. W zależności od sprawy, może to wymagać różnego podejścia. np. w przypadku zdarzeń związanych z Internetem istotne mogą być wszelkiego typu logi, odwiedzane strony WWW, adresy email, nazwy użytkowników itp.

W przypadku innych spraw mogą to być inne informacje – np. księgowość elektroniczna. **Odpowiednie spojrzenie na zdarzenie pozwala na ustalenie czy wystarczające jest tylko badanie komputera osobistego podejrzanego czy też zabezpieczenia wymagają serwery, urządzenia peryferyjne czy również nośniki kopii zapasowych.** W ramach przygotowań do zabezpieczania należy wziąć pod rozwagę następujące elementy:

- Podczas zabezpieczenia dowodów należy zapewnić odizolowanie urządzeń od osób, które mogłyby – celowo lub przypadkowo – zmienić bądź usunąć zapisy informacji na nich się znajdujących.
- Jeśli komputery są podłączone do sieci komputerowej możliwa jest zdalna ingerencja osób trzecich i np. wymazanie istotnych danych.
- Niektóre informacje mogą być przechowywane nie w kluczowych systemach tylko na pamięciach przenośnych (np. breloczki z pamięciami USB).
- Podejrzany nie musi być właścicielem urządzeń lub nośników. Informacje mogą być przechowywane na „wspólnych" dla wielu podmiotów serwerach, a nawet na nośnikach należących do osoby trzeciej, do których to nośników przestępca uzyskał dostęp bez jej wiedzy i zgody.
- Przechowywane w systemach informacje są często chronione prawami administracyjnymi, których podejrzany może nie posiadać.
- W systemie informatycznym mogą być przechowywane informacje prawnie chronione, np. tajemnica radcowska.
- Informacje mogą być zabezpieczone za pomocą haseł, kluczy szyfrowych, kluczy fizycznych i innych urządzeń z kontrolą dostępu.

Dokończenie na stronie obok.

Zabezpieczanie, ze względu na szczególną cechę dowodów elektronicznych - możliwość szybkiego zniszczenia zapisów, w pierwszej kolejności powinno obejmować uniemożliwienie dostępu do komputerów oraz niedopuszczenie do wydostania się na zewnątrz informacji o trwającym zabezpieczaniu materiału dowodowego (w szczególności w przypadku, gdy taka informacja może być ostrzeżeniem dla przestępcy). Jednocześnie należy pamiętać, że nie zawsze posiadacz sprzętu, na którym znajdują się informacje o popełnieniu przestępstwa jest jego sprawcą, zaś informacje odeń uzyskane mogą pozwolić na szybkie ustalenie istotnych dla sprawy okoliczności.

Dobrym zwyczajem jest sfotografowanie miejsca, w którym znajduje się sprzęt komputerowy, serwerownie itd. Sam proces zabezpieczania powinien przebiegać bez jakiejkolwiek „pomocy informatycznej" podejrzanych. Cechy właściwe dowodowi elektronicznemu pozwalają na różnorakie podejście począwszy od zwykłego zatrzymania komputerów, skończywszy na wyodrębnieniu przez specjalistę fragmentu danych z dużego systemu, bez jego wyłączania. Należy pamiętać, że **unieruchomienie systemów informatycznych w czasie przeszukania czy ich zatrzymanie może pociągnąć za sobą daleko idące konsekwencje dla posiadacza sprzętu**, począwszy od trudności natury osobistej (brak dostępu do danych takich jak przygotowywane pisma, listy e-mail itd.), poprzez zakłócenie ciągłości działania biznesowego (brak możliwości wystawienia faktury, naliczenia płac itd.) aż do zagrożenia zdrowia i życia włącznie (np. unieruchomienie komputerów stanowiących część stanowiska diagnostyki medycznej), dlatego też działania takie należy starannie planować.

Część techniczna powinna opierać się na zaufanych narzędziach a wszelkie operacje na nośnikach dowodowych powinny być wykonywane przez urządzenia blokujące zapis. Każda czynność powinna być udokumentowana oraz w protokole zabezpieczania powinna być odnotowana data i czas systemowy zatrzymywanych urządzeń. Chociaż na ogół nie jest to konieczne, może być również uzasadnione dokonanie oględzin włączonego sprzętu komputerowego, np. w celu oceny jakie są przyłączone zasoby sieciowe lub czy nie jest zainstalowane oprogramowanie szyfrujące. Co do zasady działania takie powinien je prowadzić specjalista. Jeśli to nie jest możliwe, wszelkie czynności szczegółowo powinno się odnotować a kolejne ekrany najlepiej jest fotografować do celów późniejszej analizy.

Przed odłączeniem jakiegokolwiek urządzenia należy zwrócić uwagę, czy nie będzie konieczne zabezpieczenie jakichkolwiek danych ulotnych (pamięć RAM). Np. w przypadkach związanych

np. z infekcjami i kradzieżami z kont internetowych. Pozyskane w ten sposób informacje mogą być bezcenne w dalszym badaniu przez biegłego, gdzie zwyczajne wyłączenie komputera może trwale uniemożliwić odnalezienie dowodów. Podobnie **wyłączenie komputera, w przypadku gdy mamy do czynienia z danymi szyfrowanymi, może doprowadzić do sytuacji w której deszyfracja nie będzie już nigdy możliwa bez znajomości hasła.** W takich przypadkach, jeśli mamy dostęp do sytemu, należy wykonać kopię danych przed jego wyłączeniem.

W zależności okoliczności wyłączanie sprzętu należy przeprowadzić albo zgodnie z procedurą systemu albo poprzez inne procedury (np. przez wyjęcie wtyczki zasilania zasilającej). Pierwsza z opisanych sytuacji powoduje zapisanie dodatkowych informacji w logach systemowych oraz uruchomienie programów przeznaczonych do uruchomienia w momencie zamykania systemu, a więc może spowodować np. wymazanie pliku wymiany w Windows czy uaktywnienie pozostawionego przez włamywacza programu destrukcyjnego, druga – jako że nie zapewnia bezpiecznego zakończenia trwających procesów zapisu – może spowodować zaburzenia integralności danych aktualnie przetwarzanych w systemie. Odpowiedni sposób działania należy dobrać od konkretnej sytuacji. **Urządzeń wyłączonych nie wolno pod żadnym pozorem włączać ponieważ każde uruchomienie powoduje zmiany zapisów zawartych na nośnikach.**

W kolejnej części cyklu skupimy się na najlepszych praktykach zabezpieczania poszczególnych urządzeń mogących zawierać elektroniczny materiał dowodowy.

Nielegalność - historia prawdziwa.

Artykuł zawiera praktyczne informacje związane z wydawaniem opinii w zakresie „piractwa komputerowego".

Marcin Kulawik

Pod pojęciem nielegalności w odniesieniu do biegłego należy rozumieć oprogramowanie dostarczone wraz z dowodowym nośnikiem danych, na które nie przedstawiono atrybutów legalności. Atrybutami takimi mogą być oryginalne nośniki, opakowania, podręczniki, faktury zakupu, naklejki licencyjne (np. COA – Certificate of Authenticity) lub przesłane drogą elektroniczną dowody zakupu. **Całość dotycząca tego aspektu jest zawarta w licencji oprogramowania, która jest podstawą analizy „nielegalności".** Należy zwrócić na to szczególną uwagę ponieważ dość często zdarza się iż po wykonaniu ekspertyzy podejrzany dostarcza oryginalne nośniki i okazuje się, że od 50 do 100% ujawnionego oprogramowania jest „legalne". Sytuacja prowadzi do powiększenia kosztów, ponieważ wystawia się ekspertyzy uzupełniające.

Następną rzeczą, którą należy poruszyć jest samo słowo „nielegalność", ponieważ **co do tego czy ujawnione oprogramowanie będzie „legalne" lub „nielegalne" stanowi sąd, a nie biegły.** Dlatego wszelkie użyte w opiniach słowa „nielegalne" należy tłumaczyć tak jak to zostało zapisane powyżej czyli, że nie przedstawiono na oprogramowanie atrybutów legalności zawartych w licencji. Jest to sprawa na tyle istotna, że w większości przypadków poruszana na rozprawach dotyczących „nielegalności", często kończąca się stwierdzeniem oskarżonego, iż biegły nie miał prawa mówić co jest nielegalne, a co nie. Zdarza się też taka sytuacja, że sami producenci nie roszczą sobie żadnego zadośćuczynienia za ujawnioną „nielegalną" kopię programu. Spowodowane to jest zazwyczaj niechęcią uczestniczenia w rozprawach sądowych.

Czym jest licencja oprogramowania? Jest to dokument w postaci elektronicznej lub papierowej określający ogólne warunki korzystania z programu, którego licencja dotyczy. Często producent oprogramowania zawiera w niej ewentualne różne możliwości użytkowania programu lub rodzaj udzielonej licencji. Ogólny podział licencji oprogramowania można podzielić na następne kategorie:

Shareware

Jest to rodzaj licencji oprogramowania, które zazwyczaj jest rozpowszechniane bez opłat. Oprogramowanie to czasami posiada pewne ograniczenia których zniesienie wymaga uiszczenia opłaty. Ograniczeniami tymi może być liczba uruchomień, czas trwania wersji próbnej, niedostępne opcje lub np. logo pojawiające się na wykonanym projekcie.

Trail

Jest to rodzaj licencji oprogramowania, którego można używać przez z góry określony czas (zazwyczaj 7 do 90 dni). Program w odróżnieniu od wersji shareware jest dostarczany jako w pełni funkcjonalny. Po upływie okresu próbnego należy oprogramowanie odinstalować bądź zarejestrować co wiąże się w większości przypadków z opłatą licencyjną.

Freeware

Jest to rodzaj licencji oprogramowania umożliwiający jego darmowe użytkowanie bez możliwości wprowadzania zmian w kod źródłowy. Należy zwrócić szczególną uwagę na to iż w większości przypadków darmowe użytkowanie jest dostępne tylko i wyłącznie w zakresie niekomercyjnym, zabronione jest czerpanie korzyści majątkowych bez zgody producenta oprogramowania. Dozwolona jest natomiast dystrybucja programowania, czyli np. kopiowanie na inne nośniki.

Licencja komercyjna

Jest to rodzaj licencji oprogramowania, która umożliwia pełne wykorzystanie jego możliwości. W zależności od zawartych w dokumencie licencyjnym punktach, użytkowanie może być wieczyste lub czasowe np. rok za którą wnosi się opłatę licencyjną. Dla przykładu gry, programy - zarówno wersje pudełkowe jak i pobierane przez Internet.

Chciałbym teraz poruszyć sprawę najważniejszą czyli napisać o tym co jest możliwe do ustalenia przy wykonywaniu ekspertyzy/opinii. Podstawową rzeczą jest oczywiście ustalenie czy na zainstalowane programy, bądź ich wersje instalacyjne zostały przedstawione przez podejrzanego wymagane w licencji atrybuty legalności, wersji oprogramowania, ewentualnie użytego klucza licencyjnego. Następnie ustala się datę zainstalowania bądź skopiowania programu. Tu należy zauważyć iż **jeśli nie ma możliwości odczytania z rejestru systemowego informacji dotyczącej wyżej wymienionej daty, ustala się ją na podstawie dat utworzenia katalogów na dysku twardym.** Jest to ważne dlatego że program mógł zostać przeniesiony do innej lokalizacji co uniemożliwia...

Dokończenie na stronie obok.

ustalenie poprawnych danych. Jest również możliwe ustalenie kto zainstalował dany program, a dokładniej, który z użytkowników systemowych, jeśli oczywiście takie dane są umieszczane przez program w rejestrze.

Dodatkowo ujawnia się zamieszczone na dysku twardym crack'i, klucze licencyjne w postaci plików tekstowych, generatory kluczy itp., których już samo posiadanie w rozumieniu Ustawy o prawie autorskim i prawach pokrewnych jest zabronione. Często w plikach z licencją oprogramowania jest ujęta informacja mówiąca o tym, iż program może być dystrybuowany tylko i wyłącznie taki jaki jest. Czyli nie mogą się znajdować w tym samym katalogu inne programy, jak nie trudno się domyśleć jest to odwołanie się do crack'ów i kluczy. Reasumując, **programy instalacyjne choćby nawet na licencji shareware lub trial dla których ujawniono zainstalowane crack'i itp. powinny być traktowane jako „nielegalne"** (naruszenie licencji).

Zdarza się, iż w przesyłanych postanowieniach pojawia się pytanie następujące pytanie: czy program został skopiowany z oryginalnych nośników lub czy został pobrany przez Internet? W przypadku pierwszego członu jest to praktycznie niemożliwe do ustalenia z prostego powodu, nośnik nie przechowuje informacji tego typu, jedyne co można ewentualnie ustalić to jaki program został użyty do kopiowania (chodzi o nośniki optyczne CD/DVD). W drugim przypadku jeśli zainstalowane oprogramowanie do pobierania danych takie jak np. P2P (lub inny program, przeglądarka internetowa) nie przechowuje historii pobranych danych, nie ma możliwości ustalenia tej informacji.

Podsumowując wszystkie przytoczone dane, przed ewentualną analizą nośników dowodowych, należy zastanowić się nad doborem pytań, na które biegły będzie musiał odpowiedzieć. Brak jakiegokolwiek z przedstawionych w postanowieniu zagadnień wiąże ręce biegłego, który aby nie narazić się na zarzut wykraczania poza zakres opinii pomija pewne dane, które mogą okazać się w toku toczącego się śledztwa istotne dla sprawy. Dlatego tak ważny jest ewentualny kontakt telefoniczny lub **dopisanie do pytań prostego**

zdania „inne spostrzeżenia lub uwagi biegłego" co w dalszym okresie w elastyczny sposób rozszerza możliwości biegłego podczas wykonywania opinii i zapobiega ewentualnym uzupełnieniom.

Oczywiście temat nie został wyczerpany, jest na to zbyt obszerny i zbyt wielu zagadnień, i możliwości wystąpień różnych sytuacji dotyczy. Jednym z podstawowych celów tego artykułu było przekazanie przynajmniej podstawowych informacji dotyczących tematu jakim jest „piractwo" czy też tak zwana „nielegalność".

Autor jest specjalistą w laboratorium informatyki śledczej Mediarecovery, prowadzi również szkolenia związane z zabezpieczaniem sprzętu komputerowego oraz oprogramowaniem śledczym.

Portret psychologiczny piratów

O piratach komputerowych z przymrużeniem oka lecz w oparciu o doświadczenia w przygotowywaniu prawdziwych ekspertyz.

Oskar Klimczak

Jako że od pewnego czasu zajmuję się piratami, zdążyłem zauważyć pewne specjalne tendencje jeżeli chodzi o ich osobowość i sposób zachowania oraz gusta. Można wyróżnić różne rodzaje piratów, ci z papugą na ramieniu, ci z drewnianą nogą bądź też z hakiem. Jednak współcześnie takich piratów nie spotykamy dlatego przejdźmy do bardziej interesującego nas tematu mianowicie ludzi bezprawnie kopiujących oprogramowanie bądź też własność intelektualną do których nie posiadają żadnych praw.

Piractwo niestety jest bardzo powszechne i nie potrzeba wielkiej wiedzy żeby natknąć się na nielegalne kopie. Wystarczy komputer z dostępem do Internetu i chwilka czasu, żeby dostać się do bardzo rozległych wirtualnych zasobów muzyki, filmów oraz programów gier i na dobrą sprawę wszystkiego czego sobie tylko zażyczymy. Obserwując ten ocean informacji można zauważyć, że piractwo to już ogromny przemysł zrzeszający grupy ludzi udostępniających zcrackowane wersje oprogramowania mowa tu m. in. o grupach typu Pizzadox czy Razor 1911. Dostanie się do takiej grupy jest bardzo trudne, a bycie członkiem w niektórych kręgach uważane jest za swego rodzaju wyróżnienie. Powstają też pilnie strzeżone fora na których ludzie wymieniają się przeróżnymi materiałami. Jedynym sposobem aby dostać się na takie forum jest otrzymanie zaproszenia w zależności od wielkości udostępnionych zasobów.

Przez moje ręce przeszło wiele spraw związanych z nielegalnością i na tej podstawie postanowiłem wyodrębnić typy piratów. Postaram się przedstawić krótki opis każdego typu. Jednak chciałbym zaznaczyć że niektórzy piraci to mutacje i kombinacje różnych profili psychologicznych. Ważną kwestią jest też to, że praktycznie każdy typ posiada swój antagonistyczny odpowiednik np. pedant-maniakalny powielacz. Poniżej opisy poszczególnych typów:

Maniakalny powielacz

Powiela i kopiuje wszystko co mu tylko wpadnie w ręce bez względu na to co i jakiej jakości. Cokolwiek dopadnie jest automatycznie kopiowane. Opisy w folderach komputera są kompletnie inne od tego co w środku, a opisy płyt nie zgadzają się z zawartością.

Aktualizator

Posiada wiele kopii tego samego programu, ale w różnych wersjach. Gdy tylko pojawia się aktualizacja on już ją ma przez co można spokojnie śledzić ewolucje niektórych programów od wersji beta testowych aż po najaktualniejsze. Jeżeli ma jakieś filmy to najczęściej ma je w kilku wersjach, różniące się jakością obrazu i dźwięku, poczynając od wersji nagrywanych w kinie kończąc na wersjach w jakości DVD bądź też HD.

Operator szalonej matrycy

Charakteryzuje się masą kopii tych samych programów, gier, a ilość posiadanych płyt można liczyć w tysiącach. Najczęściej osobniki te mają zainstalowane w jednostkach centralnych 4 nagrywarki, a wewnątrz absolutne minimum mogące je obsługiwać.

Cichociemny guerilla

Ciekawy przypadek, bo sprawia wrażenie bycia świadomym tego, że to co robi jest nielegalne mimo to dalej kontynuuje ten przestępczy proceder jednakże w sposób ukryty do granic możliwości. Wszelkie klucze do programów czy crack'i ma poukrywane w specjalnych folderach, w których znalezienia ich najmniej byśmy się spodziewali.

Dokończenie na stronie obok.

Pedant

Jak sama nazwa wskazuje wszystkie płyty są dobrze opisane, najczęściej mają wydrukowane naklejki tak żeby udawały płyty oryginalne. Na dysku przykładny porządek wszystko odpowiednio nazwane i poprawnie opisane. Płyty są ponumerowane wg odpowiedniej nomenklatury najczęściej alfabetycznie.

Kompresor

Tego typu pirat najczęściej upycha duże ilości programów na pojedynczych płytach. Czasami wartość oprogramowania na takich płytach sięga setek tysięcy złotych. Bardzo oszczędny jeśli chodzi o miejsce na dysku wszystko co tylko się da ma skompresowane.

No-life

No-life - nie ma realnego życia. Żyje grami, żywi się łączem internetowym, jest odporny na głód, a jego gałki oczne ulegają dyfuzji z płaszczyzną monitora. Posiada ogromne zasoby gier, nie potrafi o niczym innym rozmawiać. Komunikacja z takim osobnikiem jest możliwa jedynie poprzez chat w świecie World of Warcraft. Trzeba przyznać, że potrafi grać jak mało kto ale nic poza tym. Jego świat dzieli się na n00bów i pro'sów.

Wesołek

Posiada wiele różnych programów oraz komedii ale przede wszystkim masę śmiesznych zdjęć, komiksów i plików tekstowych z dowcipami. Jeśli ma swoje osobiste zdjęcia przedstawiają one ludzi wyglądem przypominających byłych pacjentów Joker'a tuż po zabiegu poszerzania uśmiechu.

Antysystemowy anarchista

Nie lubi niczego i nikogo. W jego zbiorach muzyki przodują dyskografie Sex Pistols oraz formacji takich jak Dezerter czy Sedes. Posiada masę przepisów na bomby domowej roboty, biografie Che i prowadzi własne pamiętniki. Oprogramowanie które kopiuje to głównie programy pozwalające tworzyć strony o dywersyjnym wydźwięku oraz grafiki i teksty anarchistyczne w koncepcji DIY (Do It Yourself). Permanentnie przygotowuje włamania na strony internetowe wielkich korporacji.

Przedstawione przeze mnie typu piratów wraz z krótką charakterystyką to jedynie płytkie zagłębienie się w temat. W rzeczywistości jest ich o wiele więcej. Polecam czasem dla zabawy spróbować rozpoznać typ pirata wg. przedstawionej przez mnie klasyfikacji.

Autor jest współpracownikiem laboratorium informatyki śledczej Mediarecovery. Specjalizuje się w ekspertyzach związanych z piractwem komputerowym.

Zagadkowa hurtownia

Z życia wzięte czyli ciekawe przypadki zabezpieczenia danych.

Jarosław Wójcik

Data: Czerwiec 2009r.
Miejsce: Miasto w województwie śląskim
Cel:likwidacje wytwórni nielegalnego oprogramowania, gier i filmów

Funkcjonariusz Sekcji Wsparcia Zwalczania Cyberprzestępczości monitorując internet, natknął się na forum jednego z portali miejskich, którego użytkownicy wskazują gdzie można pozyskać nielegalnie oprogramowanie, gry i filmy. Informacja ta niezwłocznie została przekazana do działu PG. Wstępne rozpoznanie operacyjne potwierdziło, iż w kilku miejscach w mieście można kupić nielegalne kopie. Analiza pozyskanych materiałów pozwoliła stwierdzić iż kopie pochodzą z jednej wytwórni. Kilkudniowe obserwacje targowisk pozwoliły określić prawdopodobne źródło. Okazał się nim dom jednorodzinny położony na obrzeżach miasta. Decyzja mogła być tylko jedna – trzeba dokonać przeszukania.

Rozpoznanie:
Obserwacja wytypowanego miejsca pozwoliło zebrać następujące informacje:

- Domek jednorodzinny wolnostojący połączony z hurtownią odzieży używanej.
- Cały teren jest ogrodzony wysokim płotem, do tego monitoring, brama z furtką i wideo domofonem.
- Hurtownię prowadzi młode małżeństwo.
- We wtorki i czwartki ok. 15-tej przyjeżdża samochód z dostawą towaru.

Zabezpieczenie zostało zaplanowane na wtorek. Do realizacji zadań oprócz grupy policjantów zaangażowano dwóch specjalistów informatyki śledczej.

Realizacja:
Od samego rana w dzień planowanego zabezpieczenia policjanci obserwowali dom podejrzanych, wszystko szło zgodnie z planem. Podjechaliśmy w rejon akcji ok godziny 14:30, czekaliśmy na dostawę cierpliwie. **Jest!** Samochód podjechał do bramy wjazdowej. Pada hasło **Wchodzimy!** W biurze zatrzymano podejrzane małżeństwo oraz dwóch pracowników hurtowni. **Czyżby pomyłka?** Na pierwszy rzut oka nic nielegalnego tutaj nie zastaliśmy. Równocześnie do pracy przystąpili informatycy śledczy, do przeanalizowanie mieli 2 komputery i laptop. **Czysty** – powiedział jeden z informatyków, **drugi również czysty** – potwierdził drugi z informatyków. Pozostał laptop właściciela. W nim też nie znaleziono nic ciekawego.

Nie dało to jednak spokoju dociekliwym informatykom. Dogłębna analiza laptopa, a w szczególności połączeń wykazała, iż oprócz standardowej sieci LAN, laptop łączył się z siecią WI-FI. Sygnał był mocny co wskazywało iż gdzieś w pobliżu znajduje się router. Komisarz zarządził przesłuchanie małżeństwa oraz dokładne przeszukanie pomieszczeń hurtowni. W jego wyniku odnaleziono router, umiejętnie schowany w niewielkiej szafce. Dostanie się do panelu administracyjnego nie stanowiło najmniejszego problemu. Analiza połączeń wykazała, iż oprócz laptopa do routera przewodowo podłączone były 2 komputery. Ich odnalezienie było kwestią czasu.

Jak się okazało to, piwnica do której wejście prowadziło od strony podwórka, była miejscem w którym policjanci odnaleźli komputery oraz profesjonalną linię do produkcji nielegalnych kopii. Analiza dysków odnalezionych komputerów potwierdziła ustalenia. Na jednym z nich informatycy odnaleźli obrazy płyt oraz wzory okładek.

W wyniku czynności został zatrzymany właściciel pseudo hurtowni oraz 2 współpracowników. Policjanci zabezpieczyli ok. 5 tyś wytłoczonych płyt, 12 tysięcy okładek oraz 2 tysiące gotowych produktów przygotowanych do dystrybucji. Łączna wartość zabezpieczonych materiału została oszacowana na ponad 300 tyś. złotych.

Podsumowanie:
Sprawa wydawałoby się łatwa, prosta i przyjemna, jednak bez informatyków śledczych i ich analitycznego podejścia mogło być się okazać, iż poza normalnym biznesem odzieżowym nic nadzwyczajnego się nie działo.

Magazyn informatyki śledczej

mediarecovery Instytucja Specjalistyczna

Adres redakcji:
Instytucja Specjalistyczna 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, Jarosław Wójcik.
Skład, łamanie, grafika: Tomasz Panek.
Reklama: Anna Czepik.

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