MAGAZYN

NR 13 / MARZEC 2012

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

JAK PORADZIĆ SOBIE Z ANALIZĄ DANYCH BILLINGOWYCH

GDZIE SZUKAĆ DOWODÓW ELEKTRONICZNYCH

INFORMATYKA ŚLEDCZA A PRAWO I POSTĘPOWANIE KARNE

ANALIZY INFORMATYKÓW ŚLEDCZYCH W 2011 ROKU

Informatyka śledcza, a prawo i postępowanie karne – nękanie (stalking)

Jakub Ślązak

W ostatnim czasie, głośnym echem w mediach, odbiła się nowelizacja kodeksu karnego, wprowadzająca penalizację tzw. stalkingu (Prezydent RP stosowną ustawę podpisał w dniu 24 marca 2011 roku). Pod tym pojęciem mieści się szereg zachowań polegających na uporczywym nękaniu innej osoby (bezpośrednio, bądź za pośrednictwem wszelkich możliwych środków komunikacji), o ile tylko działania te wzbudzają u ich adresata uzasadnione poczucie zagrożenia lub istotnie naruszają jego prywatność. Zachowania takie źródło mają na gruncie amerykańskim, gdzie przejawiały się początkowo w obsesyjnym podążaniu fanów za gwiazdami światowego kina. W miarę rozwoju techniki, nękanie upowszechniło się jednak, przybrało nowe formy oraz znalazło zupełnie nowych adresatów. Obecnie najpopularniejszym narzędziem służącym do popełnienia tego przestępstwa jest komputer oraz telefon komórkowy, za pośrednictwem których sprawca kieruje do pokrzywdzonego szeregi e-maili, bądź wiadomości sms. Innymi słowy, sprawcą stalkingu może być niemalże każdy, a także każdy stać się może jego ofiarą. W tym miejscu zasadnym jest wskazanie, iż zachowania, do których odnosi się przedstawiona powyżej definicja, nie są nowością dla polskiego systemu prawnego. Dotychczas jednak, kwestia ta uregulowana była wyłącznie w kodeksie wykroczeń, który przewidywał karalność czynu określonego jako „dokuczanie, złośliwe wprowadzanie w błąd, bądź niepokojenie innej osoby" (art. 107 k.w.). Dopiero skala zjawiska oraz jego powszechność skłoniła ustawodawcę do zaliczenia nękania do katalogu czynów zabronionych w ramach kodeksu karnego - według stanu na dzień dzisiejszy co dziesiąta osoba przyznaje bowiem, że stała się ofiarą niechcianych zachowań, które w niedopuszczalny sposób naruszały jej dobra osobiste, godziły w sferę prywatności, bądź wywoływały uczucie strachu.

> *W miarę rozwoju techniki, nękanie upowszechniło się jednak, przybrało nowe formy oraz znalazło zupełnie nowych adresatów.*

W kontekście powyższego, reakcja ustawodawcy, przejawiająca się w penalizacji przedmiotowego zjawiska, jak najbardziej zasługuje na społeczną aprobatę. Trzeba jednakże pamiętać, iż możliwość ewentualnego skazania sprawców tego występku z reguły wiązać będzie się z trudnościami dowodowymi oraz wymagać będzie wykazania w tym zakresie inicjatywy przez samego pokrzywdzonego (za wyjątkiem sytuacji, w której pokrzywdzony, targnie się na własne życie – w takim przypadku przestępstwo to podlegać będzie ściganiu z oskarżenia publicznego, bez konieczności składania wniosku). W tym właśnie momencie, z pomocą śledczym, powinni przyjść biegli z zakresu informatyki śledczej, którzy władni będą odpowiednio zabezpieczyć materiał dowodowy. To od nich zależało będzie, czy oskarżyciel przedstawi w toku postępowania należycie przygotowany nośnik informacji, zawierający treść korespondencji wystosowywanej przez sprawcę przestępstwa, wraz z możliwością przypisania jej do konkretnego urządzenia, z którego została wysłana. Pomimo oczywistości tego twierdzenia, w dalszym ciągu zdarzają się przypadki, w których dowodem w sprawie jest sam wydruk z wiadomości e-mail, stanowiący wyłącznie potwierdzenie tego, że ktoś stworzył komunikat określonej treści. Wydruk taki w żadem sposób nie umożliwia natomiast, powiązania go z osobą potencjalnego podejrzanego lub oskarżonego.

Świadomość takiego stanu rzeczy staje się coraz powszechniejsza. Obecnie, zarówno organy ścigania, jak i obrońcy zdają sobie sprawę, iż coraz częściej zmuszeni będą do sięgania po pomoc biegłych, w sprawach, w których do niedawna wiadomości specjalne nie były w ogóle wymagane. Brak takiej współpracy skutkować będzie jednakże możliwością narażenia na szwank interesów klientów, a w konsekwencji porażką w aktualnie prowadzonej sprawie.

Autor jest aplikantem radcowskim w Kancelarii Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy, Spółka Komandytowa w Katowicach

Jak poradzić sobie z analizą danych billingowych?

Mateusz Witański

Jedno zestawienie, kilka kolumn, dużo cyfr. Tak wygląda typowy billing. Jakie informacje za sobą niesie i jak bardzo przydatne są one dla jego odbiorcy, można przekonać się samemu, próbując dojść do tego, co w nim jest zawarte. Aby wyciągnąć z takiego zestawienia informacje bardziej szczegółowe, trzeba naprawdę się natrudzić. Poniżej krótki przewodnik po tym, co trzeba zrobić, aby taki billing poddać prawidłowej analizie.

Przeciętne zestawienie billingowe wystarcza do uzyskania satysfakcjonujących nas informacji jedynie w niewielu i nieskomplikowanych przypadkach. Będzie ono pomocne, gdy będziemy chcieli dowiedzieć się, z kim i kiedy rozmawialiśmy, ewentualnie sprawdzić, czy operator nas nie oszukuje. Te podstawowe informacje nie są wystarczającymi w przypadku, gdy chcielibyśmy poznać rozmowy telefoniczne osób obcych, czy to w celach dowodowych czy identyfikacyjnych. W tym przypadku powinniśmy sięgnąć do źródła informacji, jakim są dane billingowe generowane przez centrale telefoniczne. I tutaj pojawia się problem, gdyż dane te w większości przypadków nie są podane w sposób przyjazny dla użytkownika. W celu ich poprawnej analizy trzeba nierzadko fachowej wiedzy telekomunikacyjnej, prawie zawsze planu działania, który pozwoli nam na wykonanie wszystkich niezbędnych czynności. Poniżej pozwalam sobie zaproponować autorską metodę analizy danych telekomunikacyjnych central telefonicznych.

1. Poznanie źródła danych billingowych

Poznanie źródła danych billingowych jest jednym z kluczowych elementów dla rozpoczęcia procesu analizy danych. Zdobycie wiedzy na temat sprzętu i jego konfiguracji powinno być wyjściem dla dalszych prac analitycznych. Wiedza taka będzie przede wszystkim pomocna w kontekście oceny, jakich danych możemy spodziewać się po rozpracowaniu danego urządzenia, a także jakie dane powinny znaleźć się w generowanych przez sprzęt telekomunikacyjny rekordach.

2. Weryfikacja czy dane są wystarczające

Weryfikacja danych pod kątem ich przydatności dla procesu analizy będzie wynikała z poznania urządzeń, a zawierać powinna porównanie tych danych z oczekiwanymi przez nas informacjami. Zazwyczaj będzie ograniczała się do określenia, czy dana centrala generuje interesujące nas dane. Na tym etapie powinniśmy mieć jasność, czy analiza da nam jakiekolwiek informacje, czy powinniśmy ją przerwać.

3. Poznanie pliku źródłowego

Poznanie pliku źródłowego ma na celu ocenę jego zawartości pod kątem ilości kolumn, na jakie podzielony jest plik, oraz zawartości tych kolumn. Na szczególną uwagę zasługuje format rejestrowanych w pliku danych, który różni się w zależności od wielu czynników, w tym także konfiguracji centrali.

4. Przygotowanie schematu przeszukiwania pliku źródłowego

Przygotowanie schematu przeszukiwania pliku źródłowego pozwoli nam na szybkie przeglądnięcie wszystkich danych i wychwycenie tych, które nas interesują. Schemat taki powinien przede wszystkim odzwierciedlać, jaki typ informacji, z jakich kolumn i w jakim formacie powinien zostać wyszczególniony w raporcie podsumowującym analizę.

5. Przeszukanie i wyszczególnienie interesujących połączeń

Plik źródłowy zawiera wszystkie połączenia, jakie zostały wykonane przy użyciu danego urządzenia. Zadaniem analityka będzie wyłowienie i zestawienie wszystkich interesujących połączeń w celu dalszej analizy. Efektem pracy powinna być lista połączeń spełniających nasze oczekiwania, na podstawie których można będzie przeprowadzić wnioskowanie. Na tym etapie powinniśmy mieć jasność, czy połączenia, których szukamy doszły do skutku. ▸

6. Analiza połączeń i ustalenie źródła porównawczego

Znalezione w poprzednich krokach połączenia należy ocenić pod kątem ich przydatności dla analizy. Jeżeli dane w rekordach będą poprawne, jednak budzić będą wątpliwości lub domniemania, należy te rekordy skonfrontować z drugim źródłem danych, jakim jest druga strona uczestnicząca w połączeniu telekomunikacyjnym. Jeżeli dane w rekordach będą jednoznaczne, można przystąpić do formułowania wniosków z analizy.

ROZLICZENIE SZCZEGÓŁOWE

Klient: Firma A Sp. z o.o.
Adres: 70-456 Szczecin, pl. Armii Krajowej 1
Okres rozliczeniowy: 2012.01.01 00:00:00 - 2012.01.31 23:59:59
Numer abonenta: 91 430 03 36

Lp.	Strefa	Numer	Data i czas rozpoczęcia	Czas trwania	Kierunek	Liczba jednostek	Kwota netto	Kwota brutto	Rodzaj jednostki
1	22	225484738	2012.01.03 09:23:08	00:01:16	WARSZAWA	76	0,09	0,1082	sek.
2	22	225484738	2012.01.08 12:19:23	00:00:35	WARSZAWA	35	0,05	0,0641	sek.
3	22	225484738	2012.01.13 08:21:17	00:02:55	WARSZAWA	175	0,26	0,3203	sek.
4	22	225484738	2012.01.22 14:14:58	00:00:05	WARSZAWA	5	0,01	0,0092	sek.
5	22	225484740	2012.01.02 10:15:32	00:01:33	WARSZAWA	93	0,91	1,1197	sek.
6	22	225484740	2012.01.05 13:47:50	00:02:45	WARSZAWA	165	0,56	0,6838	sek.
7	22	225484740	2012.01.06 15:07:44	00:01:12	WARSZAWA	72	0,08	0,1025	sek.
8	22	225484740	2012.01.09 11:17:14	00:00:22	WARSZAWA	22	0,05	0,0615	sek.
9	22	225484740	2012.01.11 09:18:44	00:20:41	WARSZAWA	1241	12,20	14,8879	sek.
10	22	225484740	2012.01.12 10:45:29	00:42:49	WARSZAWA	2569	3,00	3,6566	sek.
11	22	225484740	2012.01.12 12:05:26	00:00:42	WARSZAWA	42	0,41	0,5039	sek.
12	22	225484740	2012.01.14 12:14:31	00:00:08	WARSZAWA	8	0,08	0,096	sek.
13	22	225484740	2012.01.16 09:34:54	00:00:39	WARSZAWA	39	0,05	0,0555	sek.
14	22	225484740	2012.01.20 15:59:29	00:08:51	WARSZAWA	531	5,22	6,3702	sek.
15	22	225484740	2012.01.29 13:16:33	00:05:37	WARSZAWA	337	3,31	4,0429	sek.

Billing operatorski

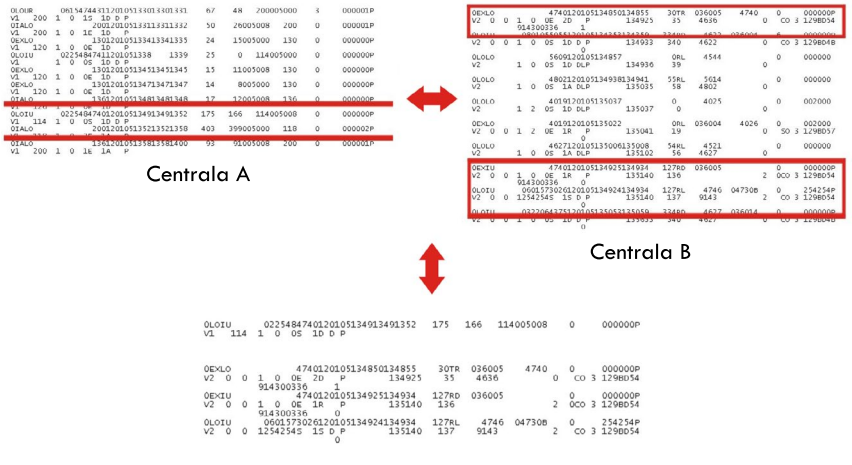
7. Poznanie alternatywnego źródła danych billingowych

Jeżeli pierwotny rekord będzie zawierał informacje niejednoznaczne lub będzie istniało podejrzenie, że rozmowa odbywała się między innymi niż zarejestrowane podmiotami, należy zgodnie z krokami 1-5 przeprowadzić analizę alternatywnego źródła danych billingowych, jakim będzie urządzenie, z którym łączył się będący przedmiotem analizy sprzęt telekomunikacyjny. W przypadku, gdy któryś z etapów analizy źródła alternatywnego przyniesie niezadowalający rezultat, należy wnioskowanie przeprowadzić na bazie rekordów urządzenia pierwotnego.

8. Ustalenie poziomu zbieżności między rekordami

Analiza porównawcza rekordów z dwóch źródeł danych billingowych pozwala na ich porównanie i określenie poziomu zbieżności lub rozbieżności. Pozwala także na stworzenie pełnego opisu połączenia telekomunikacyjnego, z jego rzeczywistymi podmiotami oraz wszystkimi elementami pośredniczącymi. Uzyskane w wyniku porównania wyniki pozwolą na dokładne przeanalizowanie interesującego przypadku, pozwolą uniknąć także błędów wnioskowania, będącego pochodną źle działającego sprzętu.

Metoda ta została przedstawiona podczas spotkania tematycznego Stowarzyszenia Instytut Informatyki Śledczej pod koniec lutego br., szczegółowy jej opis znajdzie się w przygotowywanej, pod redakcją prof. nadzw. dr hab. Jerzego Koniecznego, monografii „Analiza informacji w służbach policyjnych i specjalnych", wydanej nakładem Wydawnictwa C.H. Beck w 2012 roku.



Rekordy taryfikacyjne dotyczące tej samej rozmowy

Autor jest specjalistą w zakresie projektów teleinformatycznych, ekspertem w zakresie billingów, doktorantem Wydziału Prawa i Administracji Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego.

Gdzie szukać dowodów elektronicznych?

Emil Melka

Ostatnie ogólne rozważania na temat tego, czym są dowody, a w szczególności dowody elektroniczne, w postępowaniu karnym i jak można je w takim postępowaniu wykorzystać [Nr 10/czerwiec 2011] zakończono postawieniem otwartej kwestii, gdzie znajdować się mogą dowody elektroniczne i jak organy ochrony porządku prawnego (mam tu na myśli Sądy, prokuraturę, policję, Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Centralne Biuro Śledcze, Centralne Biuro Antykorupcyjne, jak i inne instytucje) zabezpieczają je procesowo, by je potem odczytać, odtworzyć i ocenić.

Spróbuję więc przybliżyć tę tematykę Czytelnikowi w części dotyczącej ▸

Można śmiało, choć z lekkim przymrużeniem oka stwierdzić, że dowody elektroniczne znajdują się wszędzie tam, gdzie dotarła elektryczność(...)

kwestii, gdzie organy ochrony porządku prawnego mogą poszukiwać dowodów elektronicznych. Zakładam przy tym, iż Czytelnik nie jest znawcą procedury karnej.

Gdzie więc znajdują się dowody elektroniczne ?

Czytelnikowi może wydawać się błędnie, że tylko tam, gdzie korzysta się z komputerów lub urządzeń z nimi skomunikowanych; względnie tam, gdzie przeciętny Jan Kowalski – potencjalny sprawca przestępstwa – jest podłączony do sieci internetowej.

Czytelnik może też uznać, iż poszukiwanie przez organy ochrony porządku prawnego dowodów elektronicznych dotyczy przedsiębiorstw, spółek prawa handlowego, firm, które prowadzą działalność gospodarczą, instytucji państwowych i samorządowych (prawnicy mówią: osób prawnych) lub osób prywatnych (określanych przez prawników osobami fizycznymi), które dokonują działań przestępczych w ramach zorganizowanych grup. Czytelnik może twierdzić, że skoro nie posiada stałego dostępu do internetu lub nawet nie korzysta na co dzień z komputera, to u niego w domu dowodów elektronicznych nie ma i organ ścigania (które to pojęcie uważam za węższe od pojęcia organów ochrony porządku prawnego, bo wyłączam z niego Sądy i prokuraturę) nie będzie u niego ich poszukiwał.

Jednak takie stanowisko chyba jest niesłuszne.

Moim zdaniem można śmiało, choć z lekkim przymrużeniem oka, postawić tezę, że dowody elektroniczne znajdują się wszędzie tam, gdzie dotarła elektryczność, a nawet tam, gdzie elektryczności co prawda nie ma, ale gdzie znajduje się jakiekolwiek urządzenie elektryczne lub elektroniczne – chociażby niesprawne i od dawna nieużywane lub też gdzie znajduje się rzecz, która współdziała z wyżej wymienionymi urządzeniami, choćby sama nie była zasilana z zewnętrznego źródła energii.

Dowody elektroniczne organy ścigania przede wszystkim odnajdują na twardych dyskach komputerów, na dyskach zewnętrznych i wszelkich pamięciach zewnętrznych, dyskietkach, taśmach magnetycznych, kasetach, kartach pamięci, telefonicznych kartach SIM, kartach bankomatowych w każdej ich dostępnej obecnie na rynku wersji, pamięciach wewnętrznych central telefonicznych, czy rejestratorach systemowych urządzeń przemysłowych. Poza tym, dowody takie organy ścigania odnajdują w pamięciach wewnętrznych coraz to bardziej skomplikowanych telefonów, smartfonów, notebooków, netbooków, w odtwarzaczach plików mp3 i mp4, urządzeniach nawigacyjnych GPS, tachografach samochodów ciężarowych i w aparatach fotograficznych.

Niewiele osób wie, że znakomitym miejscem na odkrywanie śladów działalności przestępczej lub ustalaniu alibi dla osoby niesłusznie pomówionej o taką działalność może być także zawartość pamięci nagrywarek telewizyjnych, konwerterów telewizji satelitarnych lub zawartość ... pamięci komputera samochodowego, zwłaszcza posiadającego funkcję tzw. „Phone-book", która pozwala na inkorporację zawartości pamięci telefonu komórkowego (spisu telefonów) w systemie Bluetooth lub nawet na rejestrację połączeń przychodzących i wychodzących z telefonu, współpracującego z systemem pokładowym pojazdu.

Możliwości odnajdywania dowodów elektronicznych są więc praktycznie nieograniczone. Z jednej strony jest to rzecz jak najbardziej pozytywna – ułatwia bowiem ujawnianie przestępstw i wykrywanie sprawców tych przestępstw przez upoważnione do tego służby i instytucje. Z drugiej strony – skłania nas do refleksji, czy wszechobecne „ucyfrowienie" naszego codziennego życia nie odsłoni zbyt wiele prawdy o nas samych. Ocenę tego stanu rzeczy pozostawiam jednak Czytelnikowi.

Nieprawdziwe jest z pewnością stwierdzenie, iż jeżeli nie posiadamy dostępu do internetu lub komputera, to w naszym domu nie ma żadnych dowodów elektronicznych. Jeżeli mamy choć jedno z urządzeń wskazanych powyżej – dowody takie organy ścigania mają na wyciągnięcie ręki, o ile oczywiście będą one im potrzebne, co jest tożsame rzecz jasna z tym, że musielibyśmy uprzednio popełnić czyn zabroniony.

Ciąg dalszy artykułu w kolejnym numerze.

Autor jest obecnie adwokatem specjalizującym się w kwestiach z zakresu cyberprzestępczości, w latach 2008-2009 kierował Wydziałem do Spraw Przestępczości Gospodarczej Prokuratury Okręgowej w Katowicach, jest uznanym wykładowcą wielu konferencji i szkoleń. Ukończył angielskojęzyczne studium szkoleniowe „Prawo Unii Europejskiej", „Współpraca sądowa w sprawach karnych" i „Brytyjskie prawo karne".

W skrócie

Guidance Software przejęło CaseCentral

Guidance Software, producent EnCase przejęło firmę CaseCentral. Połączone siły dwóch liderów w swoich klasach zapewnią nową jakość platformy EnCase eDiscovery. Klienci zyskają rozwiązanie o większej efektywności, wyższym stopniu automatyzacji, a z drugiej strony wymiernie zmniejszą koszty związane z zakupem.

Nowa wersja XRY

Oprogramowanie XRY jest od 2003 roku stosowane przez śledczych do szybkiego i skutecznego pozyskiwania danych z urządzeń przenośnych. Powstało na potrzeby szwedzkiej policji, po czym rozpoczęła się jego ekspansja. XRY daje możliwość eksploracji danych przy wykorzystaniu analizy logicznej i fizycznej, pozwalającej również na odzyskiwanie usuniętych informacji. XRY pozwala na przeprowadzanie analiz śledczych większości przenośnych urządzeń elektronicznych GSM/CDMA, telefonów satelitarnych, systemów nawigacji satelitarnej, modułów GSM 3G oraz urządzeń multimedialnych (typu MP3/MP4). Obecna wersja (6.1) daje wsparcie dla niemal 6000 modeli telefonów i innych urządzeń przenośnych.

Mediarecovery na Facebooku

Polub nasz fanpage FB. Dostarczamy najciekawszych, niecodziennych i najważniejszych informacji dotyczących szeroko rozumianego bezpieczeństwa IT.

Sprawdź na:

facebook.com/**mediarecovery**

Wirtualny seks, piractwo, wyłudzenia i lewe papiery – analizy informatyków śledczych w 2011 roku

W 2011 roku w laboratorium informatyki śledczej Mediarecovery wykonano 618 ekspertyz komputerów oraz urządzeń mobilnych: telefonów, smartfonów czy nawigacji GPS. W większości przypadków nie dotyczyły przestępstw typowo komputerowych lecz były cyfrową częścią „tradycyjnych" dochodzeń.

Przeprowadzone ekspertyzy można podzielić na następujące grupy – 22% przestępstwa przeciwko mieniu, 13% to piractwo komputerowe, 11% przestępstwa przeciw obrotowi gospodarczemu, 10% przeciwko wolności seksualnej i obyczajności, 8% przeciwko działalności instytucji państwowych oraz samorządu, 5% przestępstwa przeciwko zdrowiu i życiu, a 3% przeciwko ochronie informacji. 4% wszystkich zleceń dotyczyło akcji „w terenie" polegających na zabezpieczeniu elektronicznego materiału dowodowego w siedzibach firm i miejscach zamieszkania podejrzanych.

Zmiana podejścia przedsiębiorców

W poprzednich latach zlecenia ze strony podmiotów prywatnych realizowane były przede wszystkim na potrzeby wewnętrzne. Zarząd podejrzewał pracownika o zachowania nielojalne lub przestępcze, informatycy śledczy Mediarecovery zabezpieczali dowody elektroniczne, które były wykorzystywane podczas rozmów z podejrzanym pracownikiem. W efekcie zazwyczaj był zwalniany z pracy.

W 2011 roku dało się zaobserwować zmianę podejścia przedsiębiorców. Obecnie elektroniczny materiał dowodowy jest częścią składową pozwu do sądu. Pracodawcy coraz częściej decydują się na oddanie sprawy do sądu, a pracownicy ponoszą bardziej dotkliwe konsekwencje niż zwolnienie z pracy.

Oszustwo na „skradziony samochód"

Największą grupę – 22%, wśród wykonanych ekspertyz stanowiły przestępstwa przeciwko mieniu – głównie oszustwa, kradzieże czy przywłaszczenia. Wśród nich znajdziemy historię kobiety, która zgłosiła na policji kradzież samochodu. Policja wystawiła stosowne zaświadczenie, z którym kobieta zwróciła się do ubezpieczyciela. Ten zażądał dokumentów samochodu i drugiego kompletu kluczyków. Kobieta nie widziała, że w nowych samochodach w kluczyku zapisywane są informacje m.in. o ostatnim użyciu. Informatycy śledczy Mediarecovery z pomocą autoryzowanego serwisu producenta luksusowych aut zabezpieczyli dane elektronicz- ▸

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, Łukasz Pasek
Skład, łamanie, grafika: Beata Stępień
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

ne. Jak się okazało ktoś z domowników jeździł „skradzionym" autem już po dniu zgłoszenia jego zaginięcia.

Naiwna próba wyłudzenia kredytu

Na kolejnych miejscach uplasowało się piractwo komputerowe – 13% oraz przestępstwa przeciw obrotowi gospodarczemu - 11% wszystkich ekspertyz. Wśród nich znajdziemy przypadek mężczyzny, który chciał koniecznie dostać kredyt z banku. Na domowym komputerze sporządził sobie zaświadczenie o zatrudnieniu i zarobkach w nieistniejącej firmy. Wydawało mu się, iż skanując pieczątki oraz mając podstawową wiedzę z obsługi programów graficznych osiągnie swój cel. Bank jednak sprawdza tego typu informacje. Specjaliści Mediarecovery zabezpieczyli dużą ilość plików graficznych obrazujących kolejne etapy powstawania fałszywych dokumentów. Finał? Mężczyzna nie będzie miał zarówno kredytu, jak i czystej kartoteki w sądzie.

Komunikator i internetowy pedofil

10% stanowiły ekspertyzy dotyczące przestępstw przeciwko wolności seksualnej i obyczajności. Pewien mężczyzna wykorzystywał popularny komunikator i powiązane z nim serwisy lokalizacyjne by znajdować sobie nieletnie ofiary swych żądz mieszkające w najbliższej okolicy. Namawiał je potem do wysyłania pornograficznych zdjęć i tzw. cyberseksu. Rodzicie jednej z ofiar zreflektowali się, iż ich dziecko spędza dużo czasu przy komputerze i zachowuje się inaczej po kilkugodzinnych rozmowach przez internet. Dzięki ich interwencji mężczyzna został namierzony. Efektem analizy śledczej Mediarecovery było odtworzenie treści prowadzonych rozmów i przesyłanych wiadomości e-mail.

BHP i Curriculum Vitae

8% to przestępstwa przeciwko działalności instytucji państwowych oraz samorządu terytorialnego, w tym sprzedajność, płatna protekcja i nadużycie uprawnień. Jest to również przypadek tzw. „behapowca", który stworzył własne, bardzo bogate CV. Podobnie jak w opisywanym wcześniej przypadku mężczyzna postanowił podrobić dokumenty. Wystawił sam sobie zaświadczenia o uprawnieniach do pracy na wysokości, operatora koparki, dźwigu itp. W rzeczywistości musiałby ukończyć wielomiesięczne kursy, zdać egzaminy i wnieść stosowne opłaty. Informatycy śledczy Mediarecovery znaleźli w jego komputerze dowody na samodzielną produkcję zaświadczeń.

Jak się to robi?

Analizy informatyki śledczej różnią się od innych analiz informatycznych. Przed wszystkim działania opierają się na zasadzie „widzę wszystko nie zmieniam nic" co ma kolosalne znaczenie dla wartości dowodowej zebranych informacji. Zabezpieczenie danych elektronicznych bez wiedzy oraz specjalistycznego sprzętu i oprogramowania może prowadzić do podważenia wiarygodności każdej informacji – nawet prawdziwej. Stąd też w przypadku kiedy pracodawca czy też prokurator chce mieć wartościowy dowód musi on zostać zabezpieczony zgodnie z tzw. najlepszymi praktykami informatyki śledczej.

Analizy laboratorium informatyki śledczej Mediarecovery w 2011 roku

Źródło: dane laboratorium informatyki śledczej Mediarecovery

mediarecovery
Wyższy poziom bezpieczeństwa