NR 4 | GRUDZIEŃ 2009

Magazyn informatyki śledczej

MiŚ po raz czwarty

W tym numerze Magazynu informatyki śledczej prezentujemy kolejne tematy mogące zainteresować organy ścigania oraz innych specjalistów zajmujących się na co dzień przygotowywaniem ekspertyz. Na kolejnych stronach będą mogli Państwo przeczytać czwarty odcinek serii o zabezpieczaniu danych, ciekawy artykuł dotyczący kradzieży sygnału telewizyjnego, poznać wyniki testu optymalizacji analiz śledczych oraz narzędzi do zabezpieczania danych ulotnych.

MiŚ w 2010 roku

Decyzją Wydawcy będziemy mogli kontynuować wydawanie Magazynu w przyszłym roku. Zmienimy jednak jego formę. Chcielibyśmy zwiększyć objętość z 8 do 12 stron. Z uwagi na spore zainteresowanie omawianą tematyką przez specjalistów zatrudnionych w firmach komercyjnych, Magazyn zostanie podzielony na działy. Pierwszy z nich kontynuować będzie tematy interesujące organa ścigania, drugi przedstawiać będzie użyteczność informatyki śledczej od strony wewnątrz korporacyjnych audytów i dochodzeń.

W 2010r. nie planujemy również wprowadzenia odpłatności za kolejne numery Magazynu, zatem będą go państwo otrzymywać bezpłatnie tak jak do tej pory.

Dziękujemy za udział w ankiecie

Redakcja pragnie podziękować wszystkim Czytelnikom, którzy poświęcili swój czas na wzięcie udziału w ankiecie. Nie spodziewaliśmy się aż takiego odzewu. Wszystkie Państwa opinie i komentarze zostały poddane wnikliwej analizie. Będziemy starali się w następnych numerach wdrożyć je w życie. Pierwszych sto osób wypełniających ankietę otrzymała wraz z tym numerem obiecaną „koszulkę informatyka śledczego". Raz jeszcze serdecznie dziękujemy. Namawiamy jednocześnie do kontaktu z Redakcją, np. poprzez e-mail redakcja@mediarecovery.pl

Zabezpieczanie elektronicznych nośników informacji - część 4.

Przestępstwa z użyciem komputera

Przemysław Krejza

W poprzednich częściach naszego cyklu dotyczącego zabezpieczania danych omówiliśmy tematykę dowodu elektronicznego, zabezpieczania i gromadzenia elektronicznego materiału dowodowego. Niniejsza część skupia się na możliwościach dowodowych oraz technikach zabezpieczania poszczególnych urządzeń elektronicznych.

Komputery, laptopy

Potencjalne dowody

Dokumenty, bazy danych, pliki graficzne, pliki video, komunikatory, archiwa, dane skasowane, informacje z różnych stron www, aukcji internetowych, itd. Dowody infekcji, kradzieży tożsamości i kradzieży z bankowych kont internetowych. Własność intelektualna: tzw. "nielegalne oprogramowanie", cracki, programy do rozpowszechniania.

Najlepsze praktyki

1. Jeśli komputer jest wyłączony, nie wolno pod żadnym pozorem go włączać Włączenie komputera na pewno spowoduje naruszenie integralności niektórych informacji np. logów systemowych, a może również prowadzić do uruchomienia zainstalowanych w komputerze programów destrukcyjnych czy szpiegowskich, co w konsekwencji może doprowadzić do zniszczenia dowodu, ostrzeżenia przestępcy itd.
2. Jeśli komputer jest włączony:
   - Skonsultuj się ze specjalistą informatyki śledczej,

   Jeśli specjalista jest niedostępny:
   - Sfotografuj ekran,
   - Odłącz od źródła zasilania kable zasilające z tyłu komputera (odcięcie zasilania z tyłu komputera udaremni działanie UPS-a),
   - Laptopy są zasilane baterią. Bateria jest zwykle ulokowana na spodzie laptopa, gdzie zazwyczaj znajduje się przycisk lub przełącznik pozwalający na jej wyjęcie. Nie należy jej wkładać z powrotem. Wyjęcie baterii może zapobiec przypadkowemu włączeniu się laptopa.
3. Zaklej taśmą zabezpieczającą otwór każdego napędu,
4. Sfotografuj lub zrób schemat połączeń, znakując połączone komponenty komputerowe w jednoznaczny sposób,
5. Oznakuj wszystkie końce przejściówek/kabli, by można było łatwo je ponownie połączyć w razie potrzeby,
6. Jeśli to konieczne, zabierz wszystkie urządzenia peryferyjne, kable, klawiatury i monitory. Dla urządzeń innych niż komputery zabierz instrukcje obsługi, dokumentację i notatki (mogą zawierać hasła),
7. Zapakuj sprzęt co najmniej w folię ochronną, a najlepiej w karton z etykietą „ostrożnie",
8. Przechowuj urządzenia z daleka od magnesów, nadajników radiowych i innych elementów stwarzających potencjalne zagrożenie wpływu na urządzenie,
9. Komputery przechowuj w temperaturze pokojowej w niezwilgoconym pomieszczeniu

Komputery pełniące funkcje biznesowe (serwery)

Potencjalne dowody

Dokumenty, bazy danych programów księgowych, archiwa użytkowników, logi systemowe.

Najlepsze praktyki

1. Skonsultuj się ze specjalistą informatyki śledczej, aby otrzymać dalsze wsparcie,
2. Zabezpiecz miejsce przeszukania i nie pozwalaj zbliżać się osobom z poza grupy mającej doświadczenie w obchodzeniu się z systemem sieciowym,
3. Zastanów się czy nie należy niezwłocznie odłączyć systemu od sieci internetowej w celu uniemożliwienia dostępu z zewnątrz
4. Nie wyłączaj zasilania - odcięcie zasilania może spowodować uszkodzenie systemu lub zakłócenia w normalnym przebiegu procesu biznesowego,
5. W oczekiwaniu na specjalistę ustal kto posiada prawa administracyjne do systemu,

Różne nośniki danych typu dysk zewnętrzny, pendrive, itd.

Potencjalne dowody

Dokumenty, pliki graficzne, archiwa, odzyskane informacje, zapisy związane z danymi logowania do różnych usług sieciowych.

Najlepsze praktyki

1. Jeśli nie ma potrzeby, nie podłączaj urządzenia. Jeśli jest to konieczne, odnotuj wszystkie czynności związane z podłączaniem.
2. Jeśli urządzenie jest podłączone i zamontowane to, jeśli to możliwe skopuj zawarte na nośniku dane – urządzenie może być zaszyfrowane. Następnie odmontuj je zgodnie z zasadami systemu. W ostateczności po prostu odłącz, licząc się z ew. uszkodzeniami danych.
3. Zapakuj w opakowanie antystatyczne I kartonowe.

Telefony komórkowe

Potencjalne dowody

Książka telefoniczna, wiadomości sms, połączenia przychodzące i wychodzące, nazwiska i inne dane kontaktowe, zdjęcia, dane logowania do różnych usług, odzyskane informacje.

Najlepsze praktyki

1. Jeśli telefon jest włączony, zastanów się zanim wyłączysz.
   - Wyłączenie może powodować konieczność ustalenia PUK od operatora,
   - Wyłączenie może aktywować opcję zablokowania urządzenia,
   - Włączony telefon nadal odbiera połączenia i wiadomości SMS (może to powodować nadpisanie skasowanych informacji),
   - Opisz lub sfotografuj wszystkie informacje z wyświetlacza,
   - Odłącz zasilanie przed transportem, zabierz ładowarkę jeśli jest dostępna.
2. Jeśli urządzenie jest wyłączone, nie włączaj go.
   - Włączenie urządzenia zmienia zapisane w nim informacje,
   - Weź pod uwagę, że opóźnienie w przeprowadzeniu ekspertyzy może skutkować utratą informacji jeśli bateria zostanie wyczerpana. Postaraj się o zapewnienie zasilania.
   - Aby przeanalizować telefon niezbędny może być kod PIN lub PUK. Jeśli nie uzyskałeś go od podejrzanego możesz zwrócić się do dostawcy usług. Może on zostać zidentyfikowany poprzez numer ICC wydrukowany na karcie SIM. W Polsce 5 i 6 cyfra tego numeru oznaczają:

01	Plus	Polkomtel S.A.
02	Era	Polska Telefonia Cyfrowa Sp. z o.o.
03	Orange	Polska Telefonia Komórkowa Centertel Sp. z o.o.
04	Tele2	Tele2 Polska Sp. z o.o.
06	Play	P4 Sp. z o.o.
07	Premium Internet	Premium Internet S.A.

3. Zapakuj telefon co najmniej w folię ochronną, a najlepiej w kartonik z etykietą „ostrożnie”,

Aparaty cyfrowe, kamery, sprzęt audio

Potencjalne dowody

Aparaty, kamery oraz sprzęt audio mogą działać zarówno niezależnie jak i w sieci, być wykorzystywane w warunkach domowych oraz biznesowych. Mogą zawierać oprócz treści oczywistych, ze względu na funkcjonalność obrazy, również dokumenty i archiwa. Niektóre urządzenia mogą być bardzo zaawansowane i przechowywać wiele informacji.

Najlepsze praktyki

1. Jeśli urządzenie jest wyłączone, nie należy go włączać,
2. Jeśli urządzenie jest włączone
   1. Sfotografuj ekran, następnie odłącz od źródła zasilania, odłącz kable z urządzenia.
   2. Wyłącz urządzenie przyciskiem, a jeśli to niemożliwe, wyciągnij baterię.
   3. Zidentyfikuj i zabezpiecz nośniki (karty pamięci) poprzez przełączenie przełącznika zapisu w pozycję „locked”, w celu zabezpieczenia przed przypadkowym nadpisaniem,
   4. Zabezpiecz urządzenie
      - Zabezpiecz plombą otwór lub osłonkę do instalowania kart pamięci,
      - Traktuj urządzenie jako wrażliwe – odpowiednio je zapakuj,
      - Pamiętaj, że w niektórych modelach opóźnienia w przeprowadzaniu ekspertyzy mogą skutkować utratą informacji z powodu rozładowania baterii,
      - Wraz z urządzeniem zabezpiecz wszelkie instrukcje, odnoszące się do niego wraz z kablami zasilającymi i innymi urządzeniami powiązanymi.

Autor jest prezesem Stowarzyszenia Instytut Informatyki Śledczej, szefem największego w tej części Europy laboratorium informatyki śledczej.

Internetowy język – Trudna język.

Autor przedstawia najpopularniejsze wyrażenia stosowane przez internautów, będące zagadką nawet dla zaawansowanych użytkowników komputerów.

Oskar Klimczak

„vvI74|V| vv4$ vv$|-|y$7|<|-| vv N4$7EPNy|V| 4r7y|<|_3 |34r|)z() F4JNI3 ż3 vvP4|)|_IS<$7 P() 7() ż3|3y Prz3JS(|)() <4vv$|-|y<|-| ()PI$oovv JEzy|<4 PIr47oovv |<7oory $vv()Ja |)r()6a J3$7 |34r|)z() |3|_I$|<()vvI IN73rN47oovv |V|I|_3J |_3|<7ry".

A teraz trochę łatwiej : „W!tam ffa$ ffChytk!ch ff na$tenpnym artykoOole bardzo faI!n!e $che ffpadl!śc!e mam nadz!eI!en $che p$Chebrn!ec!e p$Chez ten tek$t po to $cheby p$CheI!ść do c!ekaff$Chych op!$uUff I!enzyka p!ratuUff ktuUry $ffoI!ą drogą I!e$t bardzo bl!$k! I!enzykoff! !nternaoOotuUff m!łeI! LektoOory".

OK, a teraz wersja minimalistyczna: „Witam was wshystkich w następnym artykoOole bardzo faiinie she wpadliście mam nadzieiię she pshebrniecie pshez ten tekst po to sheby psheiiść do ciekawshych opisuw iiężyka piratuw ktury swoiią drogą iiest bardzo bliski iiężykowi internaoOotuw miłeii lektoOory".

Mam na dzieje, że ostatnia wersja była w miarę zrozumiała. Chciałem pokazać jak wyglądają pokemonizmy, czyli specyficzny język, którym posługują się niektórzy użytkownicy internetu. Jest on jednak głównie używany przez młodszą część internautów ;)

Kolejna kwestia to wszędobylskie emotikony, buźki i uśmieszki. Dlaczego są w użyciu? Ponieważ w prosty sposób przekazują treść wiadomości przy użyciu niewielu znaków. Zaoszczędzony czas można przeznaczyć na przeszukiwanie internetu bądź też pisanie kolejnego „crack'a". Swoją popularność emotikony zawdzięczają również uniwersalności, uśmiech czy to po polsku czy w suahili będzie zawsze uśmiechem ;) Z racji tego, że niektórzy odczuwają wciąż niedające im spokoju poczucie, żeby być oryginalniejszym od innych powstają przeróżne mutacje już działających emotikon np. **:O** - oznacza zdziwienie tak jak i ***.*** Niektóre emotki są ułożone wertykalnie inne zaś horyzontalnie.

Internet jest bardzo dynamicznym środowiskiem. Język przechodzi ciągłe mutacje i poddaje się rozmaitym kombinacjom. Przykład: kiedyś ktoś wyjątkowo podekscytowany chciał to podkreślić wykrzyknikami jednak palec omsknął mu się z wrażenia z klawisza „shift" i do użycia wszedł niepisany symbol podekscytowania: **!!!1** ,aktualnie ten błąd wyewoluował do czasem abstrakcyjnych form np.**"!111134((tysiąc2!1"**

Na forach jesteśmy praktycznie anonimowi, więc język jakim posługują się użytkownicy forum jest silniejszy i bardziej bezpośredni. Forumowicze są często bezlitośni względem swych interlokutorów. Cóż „życie!" można by rzec, jednak to internetowo-forumowe jest wyjątkowo niemiłe i pełne ludzi, którzy tylko czekają na czyjąś pomyłkę po to, by po niej zbombardować go inwektywami. Często posługują się skrótami angielskich zwrotów, na pierwszy rzut oka niezrozumiałymi. Najczęściej angielskich zwrotów. Najpopularniejsze to: **OWNED, PWNED, OMG, OMFG, STFU, WTF?, MOAR, SOS, PLZ, VIDZ, GTFO, IMHO, IMO, LOL, RORFL, LMAO, BTW, OFFTOP, FTW** i wiele innych.

Teraz tłumaczenie:

- **OWNED!** - Wyraża przytłaczający tryumf nad druga osobą ma on na celu poniżenie go/wyśmianie/zbłaźnienie,
- **PWNED!** - jak wyżej tyle, że tryumf jest już bardzo przytłaczający. Powstał również przez błąd (nietrafienie w klawisz „O" lecz w klawisz „P"; występuje również jako p0wn3d,
- **OMG! - Oh My God!** – O Mój Boże! – zwrot używany w wielu sytuacjach zarówno zaskoczenia jak i obrzydzenia; bardzo uniwersalny,
- **OMFG! - Oh My Fucking God!** - O Mój Dobry Boże! - Mocniejsza forma wcześniejszego zwrotu,
- **STFU! – Shut The Fuck Up!** – Zamknij Się! + nic dodać nic ująć,
- **WTF? - What The Fuck?** - Co Do Cholery ? - najłatwiej będzie to zobrazować następującą rozmową : *„**A:**Abstrahując elokwentnie o ekstrapolacyjnej konwencji dochodzimy do konkluzji, która jest rzeczą absurdalną, albowiem każda najmniejsza część inteligencji, wytworzona w strefie neurastenii, jest tą skandaliczną orbitą morfologii, przy której kakofonia kompozytorska staje się absurdalnym melodramatem. **B:**WTF!?"* Znana jest też mniej wulgarna wersja :**WTH – What The Hell** – Co Do Diaska? Jednak jest rzadko używana,
- **MOAR** – to „fonetyczny" zapis słowa **„more"**- więcej – zwrot jest używany, gdy coś komuś się spodobało i chce więcej np. odcinków serialu, który ktoś nielegalnie umieścił w sieci.
- **SOS** – na pierwszy rzut oka kojarzy się desperacką wiadomością oznaczającą **„Save Our Ship"** jednak na forach jest często używany jako prośba o źródło „Source". Przykład: ktoś wrzuca obrazek z filmu jednak nie wie jaki to film i najczęściej pozostawia następujący komunikat: „sos plz!!" Równie często też używana wersja to „souse", który w dokładnym tłumaczeniu na język angielski znaczy nie więcej jak zanurzenie w wodzie. Jednak w języku internetowym znaczy kompletnie co innego,

- **PLZ** – to skrót od słowa „Please" - proszę , warto zwrócić uwagę na zmianę „S" na „Z", która jest dosyć popularnym zabiegiem,
- **VIDZ – skrót od „Videos"** - czyli pliki wideo,
- **GTFO – Get The Fuck Out** – Wyjdź Stąd! - zwrot używany w momentach, w których jeden z forumowiczów zaczyna pisać niestworzone rzeczy, jest grzecznie proszony o opuszczenie forum,
- **IMHO - In My Honest Opinion** – Szczerze Według Mnie – jeżeli chcemy się podzielić swoim zdaniem z resztą świata, jest to wzmocnienie komunikatu,
- **IMO - In My Opinion** – Według Mnie,
- **LOL - „Laughing Out Loud"** lub „Lots Of Laughs" - Śmieję Się Na Głos lub Wiele Śmiechu. Tu mamy do czynienia z dylematem pokroju „Co było pierwsze Jajko czy Kura ?" jednak nawet najstarsi Indianie nie pamiętają, które tłumaczenie było pierwsze i które jest poprawne. Jedno jest pewne, pisząc LOL chcemy pokazać że coś nas rozśmieszyło.
- **ROTFL - „Rolling On The Floor Laughing"** - Tarzam Się Ze Śmiechu Po Podłodze – mocniejsza wersja komunikatu LOL, występuję również w wersji skróconej tj. ROFL
- **LMAO – „Laughing My Ass Off"** - Ależ Się Obśmiałem – jeszcze bardziej wzmocniona wersja LOL'a , jednak eskalacji nie ma końca ponieważ powstał jeszcze skrót:
- **LMFAO - „Laughing My Fucking Ass Off"** - Ależ Się Kurcze Obśmiałem,
- **ROTFLMAOMG – ROTFL + LMAO + OMG - „Rolling On The Floor Laughing + Laughing My Ass Off + Oh My God** - Turlam Się Po Podłodze, Mój Boże Ależ Się Obśmiałem. Najmocniejsza wersja LOL'a można ją wzmocnić tylko wulgaryzmem Fuck wtedy komunikat wyglądałby następująco : **ROTFLMFAOMFG**,
- **BTW – „By The Way"** - przy okazji – zwrot służący do abstrahowania od głównego tematu, czasem prowadzi do OFFTOP'u,
- **OFFTOP – pochodzi o określenie „Off Topic",** czyli dygresja która nie ma nic wspólnego z tematem,
- **FTW! – „For The Win!"** wg. Graczy – Do Wygranej! - okrzyk mobilizujący resztę graczy / „ Fuck The World" wg. reszty świata - Nie lubię Świata. Jeżeli chcemy podkreślić swoje stanowisko wobec niedobrego świata,
- **3K** – Najbardziej chyba dyskusyjny skrót który w zależności od kontekstu może za każdym razem znaczyć co innego. Opcji jest wiele:
  - **Kino Kolacja Kopulacja** – kiedy chcemy dyskretnie przekazać znajomemu swoje niecne plany wobec innych osób,
  - **"Freak"** - Wariat ,
  - **Trzy tysiące** – gdzie K oznacza tysiąc, stąd często spotykamy się z oznaczeniem skrótowym : 2K9 co znaczy nic innego jak 2009, użyty również do nazwania błędu Windowsa Y2K, czyli błąd 2000- zapewne dziś stoczniowcy wołaliby Wałęsa oddaj moje 100Y (i nie chodziło by im o japońską walutę),
  - **Ku Klux Klan** – organizacja rasistowska.

Wiadomo też, że zarówno piraci jaki i zwykli forumowicze muszą się jakoś rozróżniać, oddzielać od ciemnej masy. Toteż stworzyli nie tylko własny specyficzny język, który został bardzo powierzchownie przeanalizowany, ale też sposób do nazywania siebie jako elity:

- **1337 = l33t = Leet = lit = elit = elita**.
  Przykład: im s0 leet cuz i pwned ur @ss!! - Jestem tak dobry, że Cię pokonałem!

Nie ma też miejsca na uśrednione wyniki albo jest się **n00b'em** albo **pr0**.Są też **HAXOR 'zy** czyli hakerzy oraz **SUXOR'zy** czyli ludzie nieudolni.

Powstało również specyficzne abecadło które wyglądałoby następująco :
a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,w,x,y,z
@,8,C,d,3,f,G,H,I,j,k,l,m,N,0,P,q,r,$,7,U,w,X,y,Z

Bądź też tak:
a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,w,x,y,z
ä,ß,c,d,é, ⌐g,H,í,) ,K, └m,Ñ, σp,Q, r ,t,ú,W,x,ÿ,z

I najbardziej wyewoluowana wersja:
a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,w,x,y,z
@,8,C,|),3,f,G,|-|,i,j,k,l,|V|,n,0,P,q,r,5,7,|_|,w,x,y,Z

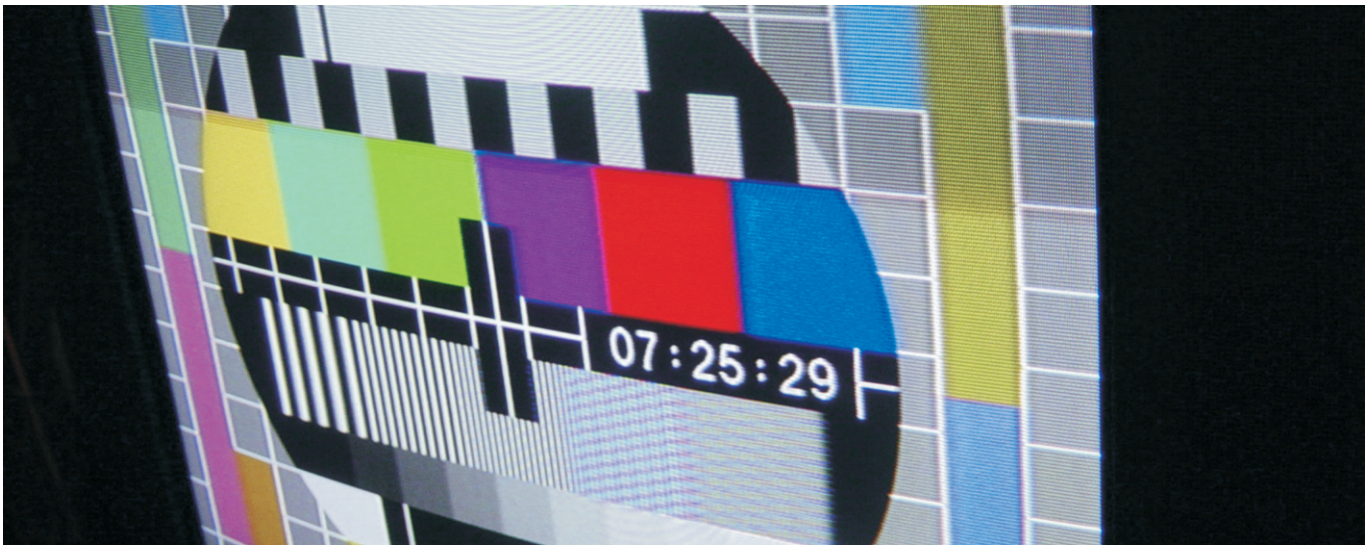
Mam nadzieję, że ten artykuł przybliżył trochę słownictwo, którym posługują się m.in. piraci. Dla bardziej zainteresowanych tematem polecam śledzenie słowniczka internetowego w następnych numerach MIŚ'a.

Inaczej:
m@M N@Dzi3Ję ż3 7en @r7ykUł PrZY8lIżył 7R0CHę 5ł0wNIc7W0 k7óryM P05łuGUJą $ię m.in. pIR@ci. Dl@ 8@RDzI3J Z@In73R350W@nYCh 7em@73m P0l3caM śledZ3NIe $ł0WNiCZK@ iN73Rn370w3g0 W n@57ępNYcH Num3r@Ch MiŚ'@

Lub:
MaM NaDzIeJeM RzE TeN ArTyKól PrZyBlIrZyl TrOcHeM SlOfFnIcTfFo kTóRyM PoSlógójOm sIeM M.In. PiRaCi. DlA BaRdZiEj zAiNtErEsOfFaNyCh tEmAtEm pOlEcAm sLeDzEnIe sloFfNiCzKa iNtErNeToFfEgO Ff nAsTeMpNyCh nómErAcH MiS\'a. :*:* xD xP ;)

Piractwo telewizyjne to kradzież sygnału telewizyjnego.

Autor omawia przepisy prawne związane kradzieżą sygnału telewizyjnego wskazując najistotniejsze z punktu widzenia organów ścigania.



Zbigniew Taras

Naruszenie praw twórców, producentów i innych podmiotów majątkowych praw autorskich i praw pokrewnych, potocznie nazywane piractwem, tak naprawdę jest zwyczajną kradzieżą, która występuje zarówno w sieciach telewizji kablowych jak i na cyfrowych platformach satelitarnych. **Podstawowym narzędziem umożliwiającym walkę ze złodziejami sygnału telewizyjnego jest Ustawa z dnia 5 lipca 2002r. o ochronie niektórych usług świadczonych drogą elektroniczną, opartych lub polegających na dostępie warunkowym.** Celem tej Ustawy jest zapewnienie ochrony podmiotom wykonującym tego typu usługi przed pozbawieniem ich należnych wynagrodzeń przez osoby, które bez upoważnienia wytwarzają, udostępniają, używają lub tylko posiadają urządzenia niedozwolone umożliwiające nieuprawniony odbiór programów telewizyjnych. Ustawa zawiera szereg specjalistycznych pojęć, wyjaśnienie których umożliwi nie tylko prawidłową identyfikację czynu zabronionego, ale również jego karną kwalifikację. **Dostęp warunkowy** są to wszelkiego rodzaju urządzenia oraz instalacje niezbędne do odbioru programów przez indywidualnego odbiorcę. **Usługi oparte na dostępie warunkowym** to usługi, korzystanie z których uzależnione jest od uprzedniego nabycia przez usługobiorcę urządzenia dostępu warunkowego lub uzyskania indywidualnego upoważnienia dostępu do danej usługi. **Usługi polegające na dostępie warunkowym** to usługi, których przedmiotem jest umożliwienie korzystania z dostępu warunkowego. Są to w szczególności usługi kodowania, szyfrowania, takie które służą zabezpieczeniu innych usług przed dostępem osób, które nie nabyły do nich praw.

Art. 6 Ustawy z dnia 5.07.2002r. mówi: **1. Kto, w celu użycia w obrocie, wytwarza urządzenia niedozwolone lub wprowadza je do obrotu, podlega karze pozbawienia wolności do lat 3. 2. Tej samej karze podlega, kto świadczy usługi niedozwolone.** Omówienia wymagają sformułowania: **„w celu użycia w obrocie”**: chodzi o czyn o charakterze kierunkowym, z winy umyślnej w zamiarze bezpośrednim. **Wytwarzanie** - rozumiane jako produkcja urządzeń niedozwolonych lub ich przeróbka w stopniu umożliwiającym nielegalny dostęp do świadczonych usług. **Urządzenia niedozwolone** dzielimy na: **sprzęt zaprojektowany** (specjalnie stworzony na potrzeby kradzieży sygnału telewizyjnego, np. blokery, karty, splittery), sprzęt przystosowany (przerobione oryginalne urządzenia, np. dekodery z wbudowanym blokerem, karty abonenckie ze zmienionym oprogramowaniem) oraz **oprogramowanie** (do dekoderów, modułów dostępu, kart, czy umożliwiające pracę w systemie sharingu internetowego). Zgodnie z ustawą **usługami niedozwolonymi** są: instalacja, serwis, wymiana urządzeń niedozwolonych, zmiana oprogramowania dekoderów lub kart, wszelkie publikacje, ogłoszenia oraz promocje usług i urządzeń niedozwolonych.

Art. 7 Ustawy: **1. Kto w celu osiągnięcia korzyści majątkowej posiada lub używa urządzenia niedozwolone, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. 2. Jeżeli sprawca używa urządzenia niedozwolonego wyłącznie na własne potrzeby, podlega grzywnie.**

W celu osiągnięcia korzyści majątkowej: przestępstwo kierunkowe z winy umyślnej, popełnione w zamiarze osiągnięcia korzyści. **Posiada lub używa**: istotny jest sam fakt posiadania urządzenia umożliwiającego nielegalny dostęp do usług chronionych. Dla zaistnienia przestępstwa nie jest istotne zrobienie z takiego urządzenia użytku. **Na własne potrzeby**: odpowiedzialność ponosi tu wyłącznie bezpośredni użytkownik urządzenia niedozwolonego, najczęściej osoba korzystająca z urządzenia niedozwolonego w prywatnym lokalu, niedzieląca się sygnałem z innymi osobami.

Art. 9 pkt. **3 Ustawy: Ściganie przestępstw określonych w art. 6 i 7 następuje na wniosek krajowych lub regionalnych organizacji, których celem statutowym jest ochrona interesów przedsiębiorców świadczących usługi oparte lub polegające na dostępie warunkowym.**

Taką organizacją jest Stowarzyszenie Dystrybutorów Programów Telewizyjnych **Sygnał**, które zgodnie ze statutem stowarzyszenia upoważnione jest do reprezentowania wyłącznie podmiotów będących członkami stowarzyszenia.

SYGNAŁ **www.sygnal.org.pl**

Autor jest wiceprezesem Stowarzyszenia Dystrybutorów Programów Telewizyjnych "Sygnał", dyrektorem Działu dw. z Piractwem w Spółce CANAL+ Cyfrowy.

Narzędzia do zabezpieczania danych ulotnych.

Podstawowe informacje dotyczące przechwytywania danych ulotnych

Przemysław Krejza

Informatyka śledcza w „tradycyjnym ujęciu" kojarzy się głównie z zapisami zawartymi na twardym dysku i innych nośnikach przechowujących dane w sposób trwały. Większość śledczych zakładała, że tylko w informacji zapisanej na takim nośniku można odnaleźć coś „ciekawego". Tak jednak nie jest. Pamiętajmy bowiem, że zanim cokolwiek zostanie zapisane na dysku twardym musi „przejść" przez pamięć operacyjną. Co więcej – pamięć może zawierać również informacje, które nigdy na dysk twardy nie trafią, jak np.:

- Uruchomione procesy,
  - Wszelkiego typu malware - rootkity i trojany,
- Otwarte pliki,
  - Edytowane dokumenty, nawet nie zapisane,
  - Pozostałości emaili, nawet pochodzących z poczty www,
  - Zawartość stron internetowych, nawet szyfrowanych,
  - Otwierane obrazy,
- Połączenia sieciowe i otwarte porty,
- Otwarte klucze rejestru,
- Informacje związane z uruchomionymi aplikacjami (np. aktywne rozmowy komunikatorów),
- Bufory związane z ekranem, klawiaturą, dyskiem itd. (np. rekordy MFT),
- Hasła zapisane w sposób jawny,
- Informacje związane z BIOS,
- Inne informacje systemowe,

Akwizycja pamięci

Proces ten sprowadza się do wykonania kopii binarnej pamięci w „żywym" systemie. W uproszczeniu, pozyskana w ten sposób kopia jest podobna do kopii binarnej np. dysku twardego, jednak aby ją wykonać musimy przystosować swoje narzędzia i techniki do warunków związanych z koniecznością pracy na działającym materiale dowodowym. Pracujący system operacyjny jest w stanie nieustannej zmiany a wykonany zrzut pamięci jest niejako „zamrożeniem czasu" tj. stanu w danej chwili. Choć sam proces akwizycji pamięci RAM jest stosunkowo prosty, łatwo tu o pomyłkę oraz działania, które mogą zatrzeć oczekiwane ślady. Dlatego przed rozpoczęciem „prawdziwych spraw" warto przygotować własny set narzędzi i przećwiczyć odpowiednie procedury.

O czym trzeba pamiętać:

1. Dokumentuj każdy krok.
2. Musisz mieć pełny dostęp do systemu.
3. W docelowej maszynie nie zamykaj żadnych okien, dokumentów lub programów
4. Staraj się wykonać akwizycję w jak najmniejszej ilości kroków. Miej przygotowane narzędzia.
5. Pamiętaj aby nośnik na który wykonujesz "zrzut" pamięci był większy niż zainstalowana w docelowej maszynie ilość pamięci.
6. Stosuj odrębny nośnik na plik kopii a przed użyciem wyzeruj całkowicie przygotowaną na nim partycję.
7. Używaj wyłącznie zaufanych narzędzi. Im mniej pamięci alokuje narzędzie tym lepiej.

Zachęcamy do samodzielnych prób!

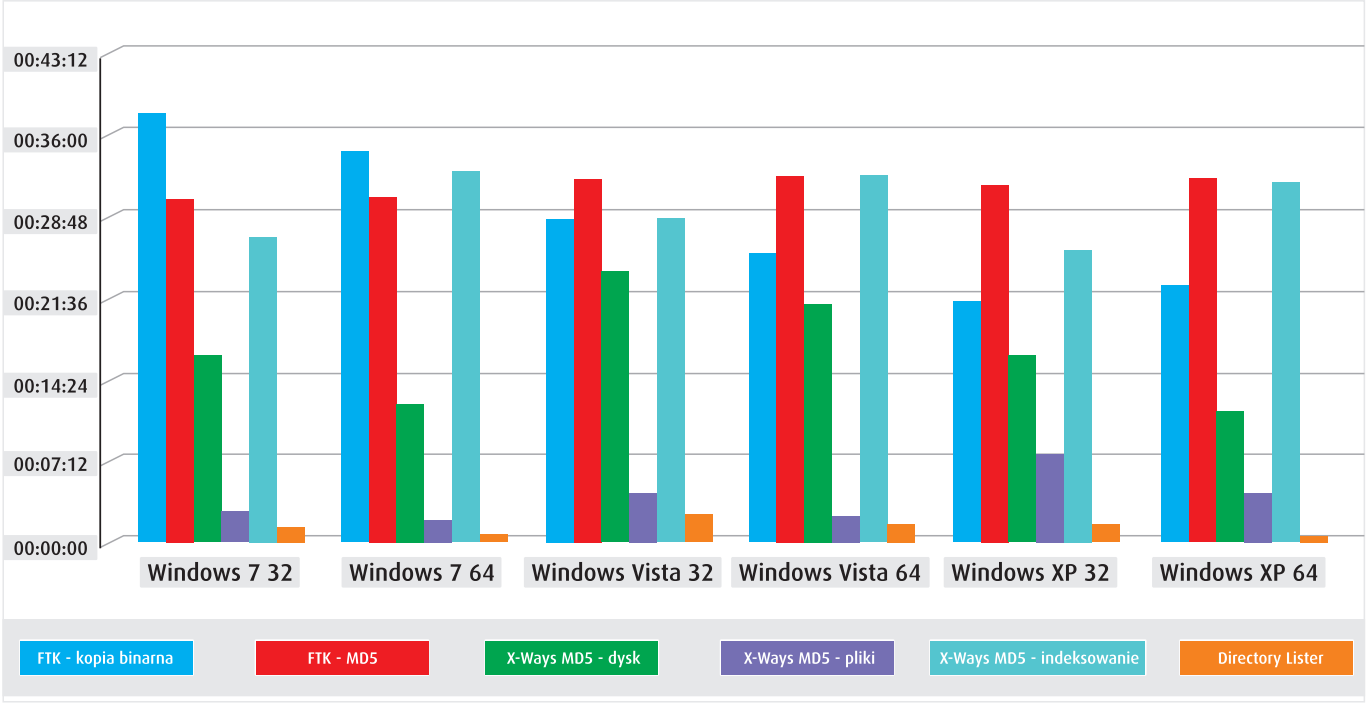
Autor jest prezesem Stowarzyszenia Instytut Informatyki Śledczej, szefem największego w tej części Europy laboratorium informatyki śledczej.

Narzędzia do akwizycji

	FastDump Pro	FastDump Community	WinEn / WinEn64	MDD	Memoryze	Win32DD	EnCase
Producent	HBGary	HBGary	Guidance Software	ManTech	Mandiant	Mattieu Suiche	Guidance Software
Licencja	Free	Płatna	Płatna	Free	Free	GNU	Płatna
64bit	Nie	Tak	Tak	Nie	-	-	Tak
>4Gb	Nie	Tak	Tak	-	-	-	Tak
Win 2008 serwer	Nie	Tak	-	-	-	Tak	Tak
Win 2003 serwer	Nie	Tak	Tak	Tak	Tak	Tak	Tak
Win XP	Tak	Tak	Tak	Tak	Tak	-	Tak
Vista	Nie	Tak	Tak	Tak	SP1	Tak	Tak

Windowsy do CF – praktycznie.

Test optymalizacji przeprowadzania analiz z zakresu informatyki śledczej



Tomasz Sidor wraz z zespołem
Laboratorium Informatyki Śledczej
Biura Ekspertyz Sądowych w Lublinie

Gdy pewnego dnia stanął w laboratorium pachnący nowością komputer, a z nim pudełko Windows Vista Business, gdzie w ramach jednej licencji można użyć trzech wersji systemu (XP, Vista i 7). Powstało pytanie – co lepiej się sprawdzi i do jakich zastosowań. Tak powstał pomysł testu, do optymalizacji zasobów własnych.

W procesie analizy śledczej materiałów występują sztywne punkty jak wykonanie kopii binarnej, wygenerowanie sumy kontrolnej czy też wyszukiwanie słów kluczowych na dysku. Czynności te posiadają jedną wspólną cechę – są czasochłonne. Skrócenie, nawet o kilka procent, punktów przerabianych za każdym razem przyniesie zysk.

Na pierwszy ogień poszła czynność nieunikniona, tworzenie kopii binarnej z dysku testowego przez blocker za pomocą FTK-Imager. Najgorzej poradziły sobie najnowsze okienka, czas wykonywania kopii w stosunku do najszybszego XP 32 był niemal dwukrotnie dłuższy. Powtórzono badanie korzystając z Windows 7 RC (pierwszy test w wersji RTM), czas kopiowania spadł o 10%. Dodatkowa uwaga do systemu: po sformatowaniu dysku pod Windows 7 przy próbie montowania partycji do Linuxa pojawia się komunikat o niewłaściwym odmontowaniu ntfs.

Kolejnym etapem jest generowanie sumy kontrolnej (w tym przypadku MD5) dla całego dysku lub poszczególnych plików. Przy korzystaniu z FTK-Imager'a, wynik nie różnił się bardziej niż granica błędu. Natomiast w przypadku wykonania sumy kontrolnej w programie X-Ways Forensics można stwierdzić znaczące różnice (z powodu różnych procedur nie należy wyników FTK odnosić do X-Ways). Systemy Vista odstają o ponad 40%. Dodatkowo widoczna jest różnica od 12% do 30% pomiędzy 64 a 32 bitowymi, ze wskazaniem na systemy 64 bitowe. Sprawdziły się one również w generowaniu listingu plików za pomocą Directory Lister.

W operacji indeksowania przeprowadzonej w X-Ways Forensics widoczna jest kilkunasto procentowa stała różnica pomiędzy systemami 32 a 64, na korzyść 32 bitowych. Systemy 64 bitowe pozwalają jednak na przyspieszenie procesu poprzez zwiększenie wykorzystania pamięci RAM (jeśli jest jej wystarczająco dużo).

Podsumowując, poczciwy już Windows XP 32, nadal świetnie sprawdza się w większości zadań jak kopia binarna czy proces indeksowania. Windows 7 64 w wersji finalnej zapowiada się ciekawie, choć zapewne nie obędzie się bez niespodzianek, może jednak warto spróbować zaprząc go do części zadań?

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