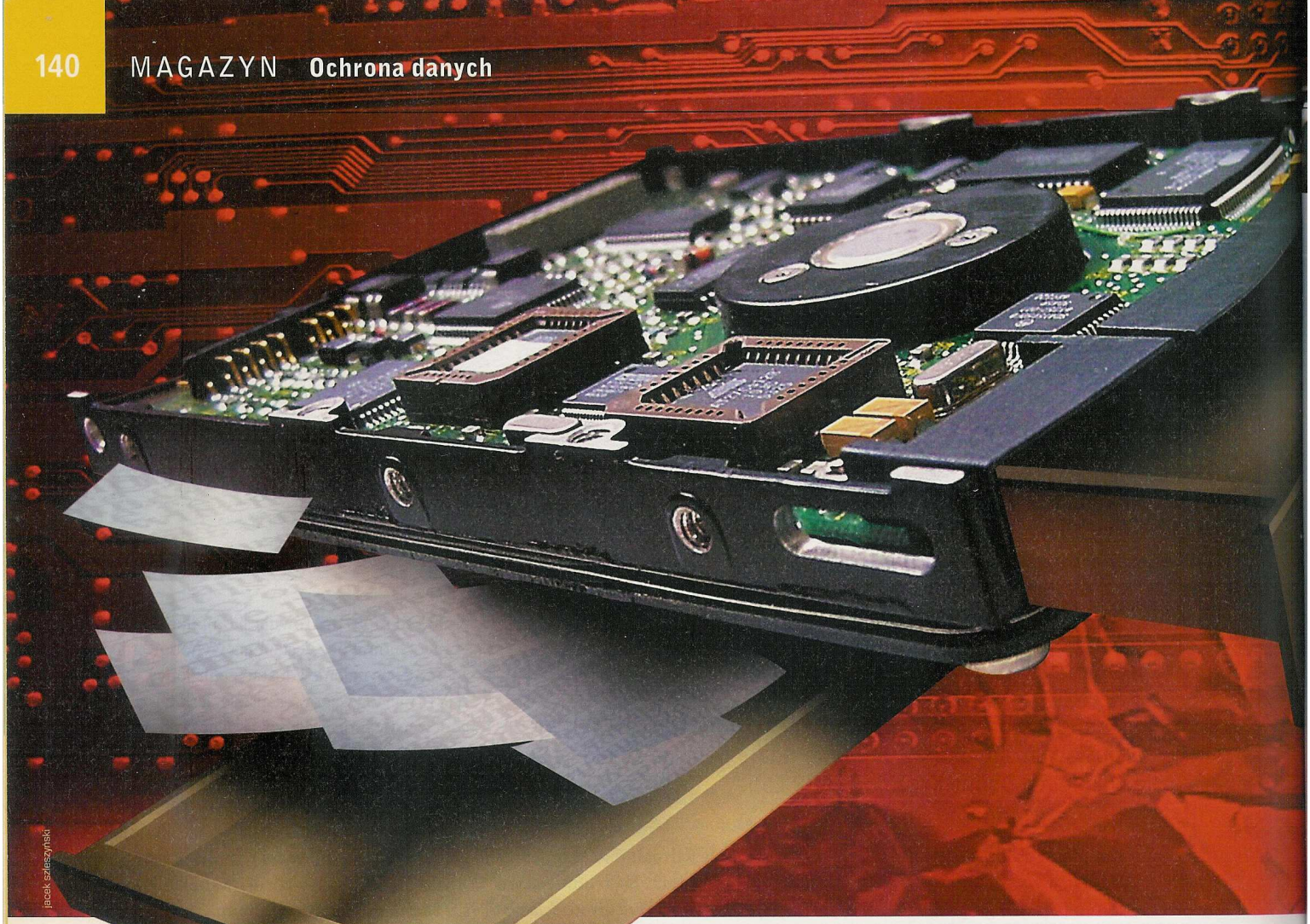


jacek szaleszyński

Odsprzedaż dysku stanowi zagrożenie nie tylko dla prywatności

Niebezpieczne pozostałości

Złodzieje nie muszą włamywać się do komputerów, by zdobyć numery np. cudzych kart kredytowych. Wystarczy, że zainteresują się odsprzedawanymi dyskami twardymi. W laboratoriach PAN sprawdziliśmy, co można znaleźć na starych nośnikach.

Szymon Piłat, Kamil Kulesza

W artykule

Pliki komputerowe są dziś tym, czym kiedyś były dokumenty papierowe, teczki, archiwa itd. Kiedyś sensację wzbudzało odnalezienie tajnych akt, dziś natomiast równie wielkie emocje wywołuje wyciek poufnych danych elektronicznych. Najbardziej znane przykłady to dyski z Ministerstwa Spraw Zagranicznych, które odkupił Jerzy Urban, lub pliki z komputera Aleksandry Jakubowskiej, które stały się ważnym materiałem dowodowym w głośnej sprawie.

Problem jest istotny nie tylko dla polityków, gdyż komputery i Internet wykorzystuje się do przechowywania i przesyłania informacji związanych z operacjami bankowymi, działalnością firm, stanem majątku oraz prywatnymi sprawami z życia osobistego. Zachowanie ich poufności jest sprawą wysokiej wagi, bo stanowi tak o bezpieczeństwie państwa, jak i firm czy zwykłych ludzi.

Karty płatnicze na śmietniku

Postanowiliśmy sprawdzić, czy użytkownicy komputerów dbają o własne dane z dysków, które zamierzają sprzedać, oraz co można znaleźć na nośnikach dostępnych na rynku wtórnym. Zbadaliśmy, czy i jak przeciętny użytkownik komputera usuwa pliki przed sprzedażą „twardziela". W ramach projektu badawczego przeprowadzonego w Instytucie Podstawowych Problemów Techniki Polskiej Akademii Nauk przeprowadziliśmy eksperymenty obejmujące różne aspekty ochrony informacji. Koncentrowaliśmy się na sprawdzeniu, jakie dane można znaleźć na używanych dyskach twardych.

Podobny eksperyment przeprowadzili przed trzema laty w USA Simson L. Garfinkel i Abhi Shelat z Massachusetts Institute of Technology. W ciągu dwóch lat zebrali oni 158 dysków twardych. Dyski kupowali w sklepach z używanym sprzętem komputerowym firm, które wyprzedawały towar, oraz na aukcjach internetowych (eBay). Na dyskach znaleźli m.in. ponad 5000 numerów kart kredytowych (jeden z napędów pochodził z... ban-

Dlaczego kasowanie plików jest nieskuteczne?

Kasowanie plików poprzez przesuwanie ich do systemowego Kosza pozostawia dane w zasadzie nietknięte. Technicznie rzecz biorąc, kasowanie to niewielka modyfikacja w tablicy alokacji plików. Podobnie przedstawia się sprawa z formatowaniem. Każdy program przeznaczony do odzyskiwania sformatowanych danych potrafi je całkowicie odtworzyć. Dopiero zastosowanie specjalnej aplikacji skutecznie usuwa pliki.

Odtworzona biografia

Oto informacje o pewnej osobie, utworzone na podstawie danych odzyskanych z dysku kupionego na aukcji internetowej. Dane pozwalające na identyfikację tej osoby zostały zmienione.

Anna mieszka na Żoliborzu. Ma 25 lat, jest bardzo pogodną i ładną dziewczyną o rudych włosach. Ukończyła filologię ukraińską na UW. Zajmuje się redakcją i korektą tekstów. Do tej pory pracowała w kilku wydawnictwach, obecnie stara się o pracę w kolejnym (niestety, w CV, które wysłała e-mailem popełniła literówkę). Jedną z jej pasji są sporty ekstremalne, szczególnie bungee jumping i spadochroniarstwo. Jej zainteresowania to również literatura i historia współczesna. Ma konto w banku Inteligo, często odwiedza portal wizaz.pl poświęcony kosmetykom. Lubi zwierzęta, ma gekona, którego uwielbia. Często udziela się na forum hodowców gekonów. Na dysku przechowywała również wiele zdjęć (niektórych z nich na pewno nie pokazałaby znajomym), olbrzymie archiwum e-maili, kompletne dane adresowe i osobowe (swoje oraz rodziny, chłopaka i innych osób). Anna sprzedała swój dwugigabajtowy dysk, gdy zmieniała komputer.

Źródło pochodzenia dysku: Allegro.pl

komatu). Prawie wszystkie nośniki zawierały jakieś informacje, a jedynie mały ich odsetek był prawidłowo oczyszczony z danych w taki sposób, że nie udało się niczego odzyskać (9% dysków, czyli 12 sztuk). Dotyczył on jednak realiów amerykańskich. Postanowiliśmy przekonać się, na ile tamte rezultaty pozostają aktualne w naszym kraju.

Publikacji wyników grupy z MIT towarzyszył duży rozgłos. Sprawdziliśmy więc, czy ówczesna wrzawa wokół uzyskanych w USA wyników wpłynęła w znaczący sposób na zachowanie użytkowników komputerów w Polsce, czyli czy sytuacja u nas jest równie katastrofalna.

Myśleć jak przestępca

W trakcie przygotowań do eksperymentu staraliśmy się zdobyć jak najwięcej używanych dysków twardych. Następnie odzyskiwaliśmy z nich dane, sprawdzaliśmy, czy zdobyte pliki są poufne oraz czy mogą stanowić niebezpieczeństwo w razie dostania się w niepowołane ręce. Nasze działania miały jednocześnie być symulacją postępowania potencjalnego napastnika, jednak wszystkie odzyskane i przeanalizowane dane nie były wykorzystywane do żadnych celów poza naukowymi. Każdy dysk, który był później odsprzedawany na aukcjach, został przez nas zabezpieczony programami do kasowania danych, tak aby nikt nie był w stanie odtworzyć oryginalnych informacji.

Jednym z założeń eksperymentu była kwota, którą przeznaczyliśmy na projekt. Budżet ograniczyliśmy do około 1500 zł, przyjęliśmy bowiem założenie, że potencjalny przestępca dysponuje skromnymi środkami.

Użyty przez nas sprzęt jest ogólnodostępny i względnie tani, a zastosowane oprogramowanie do pobrania z Internetu. Użytą przez nas metodę mógłby zastosować każdy, kto ma podstawową wiedzę informatyczną, także osoby, których podstawową motywacją działań jest zysk, osiągnięty nawet metodami niezgodnymi z prawem, jak np. oszustwa i wyłudzenia.

200 zdobytych dysków

Zakładaliśmy, że część użytkowników komputerów będzie przezorna i skasuje pliki lub sformatuje dyski, dlatego nasz eksperyment zaczęliśmy od wyboru oprogramowania, które miało odzyskiwać informacje. Przeprowadziliśmy trwające ponad tydzień testy tego rodzaju software'u. Spośród ogólnodostępnych aplikacji wyłoniliśmy trzy najlepsze naszym zdaniem programy, które odzyskują dane utracone na skutek kasowania, formatowania lub uszkodzenia systemu plików.

Badane dyski twarde były głównie kupowane na aukcjach internetowych, choć udało się uzyskać też sporą liczbę napędów od różnych ofiarodawców. Po przebadaniu nośniki były z powrotem wystawiane na aukcjach, ponieważ zasoby finansowe, jakimi dysponowaliśmy, były niewielkie. W sumie, dysponując kwotą 1500 zł, udało się nam pozyskać ponad 200 dysków!

Kluczowym elementem działań był sam proces odzyskiwania danych ze zdobytych nośników. Po podłączeniu badanego dysku najpierw kopiowano zapisane na nim dane (jeśli takowe były). Następnie, korzystając z oprogramowania do odzyskiwania danych, odtwarzano pliki, które przechowywano na dysku przed jego formatowaniem. Wszystkie zdobyte informacje gromadzono na wyodrębnionym komputerze, wyposażonym w dyski twarde o dużych pojemnościach.

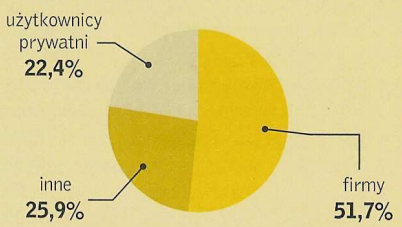
Kopalnia danych

Następnym etapem prac była analiza zebranych danych. Było ich bardzo dużo, więc należało zmierzyć się z problemem odsiewu nieistotnych dla nas plików oraz wyselekcjonowanie tych najbardziej interesujących. Jest to klasyczny przykład data miningu. Problem został rozwiązany przez częściową automatyzację procesu analizy danych. W pierwszej kolejności automatycznie odrzucane były pliki systemowe, sterowniki, biblioteki i wiele innych plików, które z punktu widzenia badań były nieprzydatne. To, co zostawało na dyskach, to najczęściej dokumenty pakietów biurowych, bazy danych i multimedia.

W dalszej kolejności analiza przebiegała na dwa sposoby. Po pierwsze korzystając ze skanerów plików, wyszukiwaliśmy frazy odpowiadające poufnym informacjom, np. „numer karty kredytowej" lub „dane tajne". Po drugie przeglądaliśmy informacje ręcznie. Określaliśmy poufność i zagrożenie, jakie spowodowałby wyciek takich danych.

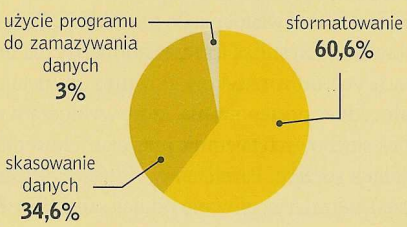
Wszystkie te operacje wymagały dużego nakładu pracy. W projekcie brało udział jedenaście osób, a jego realizacja zajęła ponad dwa miesiące. Ze zdobytych dysków udało się wydobyć ponad dwa terabajty danych, z czego ręcznie przeanalizowano trzynaście gigabajtów najbardziej interesujących dokumentów (łącznie 140 tysięcy plików).

Pochodzenie dysków



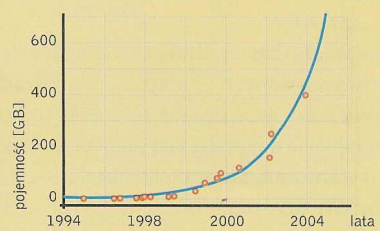
Połowa przebadanych przez nas dysków pochodziła z firm. Ryzyko wycieku tajemnic służbowych jest więc duże.

Jak zabezpieczamy dane



Dane z badanych dysków były usuwane przez pierwotnych właścicieli w różny sposób. **Najczęściej dysk był tylko sformatowany.**

Wzrost pojemności dysków



Pojemność dysków podwaja się co półtora roku. Użytkownicy **nie mają motywacji do usuwania danych** gromadzonych przez lata.

Od danych osobowych po dowody zdrady

Dyski, które badaliśmy, były „oczyszczone" przez ich poprzednich właścicieli w różny sposób (patrz wykres). Często dane były po prostu skasowane. Bardziej zaawansowani użytkownicy formatowali dysk. Jedynie niewielki odsetek dysków był zabezpieczony w wystarczający sposób. Systemem plików na badanych dyskach był z reguły NTFS lub FAT32. Tylko kilka z ponad 200 dysków miało uniksowe systemy ext2 i ext3.

Z dysków wydobyliśmy zaskakujące informacje. Najciekawsze to szczegółowe dane osobowe (liczone w tysiącach rekordów), skany dokumentów tożsamości, numery kont bankowych, zestawienia transakcji, zeznania podatkowe (często kolekcje z kilku lat), kosztorysy inwestycji. Dane dotyczące firm to najczęściej – obok PIT-ów – umowy z innymi firmami, listy płac, dane pracowników, kontrahentów i różne bazy danych. Na dyskach było również bardzo dużo informacji z życia osobistego, archiwa rozmów Gadu-Gadu, hasła do kont e-mail. Znalezione dane mogłyby nawet stanowić dowody zdrad małżeńskich (korespondencja, zdjęcia, adresy, telefony)!

Trzeba zaznaczyć, że nawet cache lub historia przeglądarki internetowej dostarczały niekiedy zaskakujących informacji, np. wysoko postawieni pracownicy różnych firm mieli w cache'u megabajty twardej pornografii.

Coraz grubsze archiwa

Jednym z zaobserwowanych zjawisk było, że dane na dyskach były niekiedy bardzo stare. Wynika to oczywiście stąd, że pojemności dysków stale się zwiększają i już od dawna zwykłemu użytkownikowi trudno je „zapchać". Kiedyś, gdy dysk na domowym czy firmowym pececie miał kilkadziesiąt megabajtów pojemności, trzeba było regularnie usuwać stare pliki, aby było miejsce na nowe. Wzrost pojemności nośników spowodował, że w zasadzie nie trzeba już „sprzątać", więc stare dokumenty po prostu spoczywają zapomniane w jakimś katalogu. Zresztą dyski są coraz tańsze, więc gdy miejsce na starym „twardzielu" się wyczerpie, można kupić nowy, a stary po prostu... sprzedać.

Na przebadanych dyskach zalegały więc archiwa wysłanych e-maili o rozmiarach sięgających setek megabajtów. Była to korespondencja odebrana i wysłana przez kilka lat użytkowania komputera. Wiele ze znalezionych dokumentów tekstowych było datowanych na lata 90. (najczęściej były to pliki w formacie DOC i RTF). Tak potężne archiwum informacji pozwalało nam odtworzyć całą historię życia osoby lub proces rozwoju firmy (patrz ramka). Można było uzyskać niewiarygodnie wiele szczegółów.

Zaproszenie dla szantażystów i złodziei

Wyraźnie widać, że użytkownicy komputerów – tak indywidualni, jak i firmy – nie usuwają danych z dysków, które oddają lub sprzedają. Jest to skandaliczna lekkomyślność, gdyż sposobów na szkodliwe wykorzystanie takich danych są setki: kradzież osobowości, handel danymi osobowymi, szantaże, fałszerstwa, wyłudzenia – to tylko najprostsze przykłady. Większość użytkowników komputerów domowych i firmowych nie zdaje sobie sprawy z dwóch rzeczy. Po pierwsze z tego, że na pozór zwyczajne dane, takie jak książka adresowa, szczegółowe dane osobowe, archiwum e-maili, a nawet cache przeglądarki WWW, mogą stanowić zagrożenie dla właściciela. Po drugie skasowane lub nawet sformatowane dane można z łatwością odzyskać programami dostępnymi w Sieci. Nie stanowi to najmniejszego problemu dla początkującego użytkownika komputera. Kolejnym problemem jest fakt, że wiele osób w ogóle nie wie, jak chronić swoje dane.

Jak się okazało, uzyskane przez nas wyniki badań są podobne do tych, które otrzymała grupa z MIT: dane, które zostały znalezione na dyskach twardych, mogłyby stanowić bardzo duże niebezpieczeństwo, gdyby znalazły się w rękach fałszerza, szantażysty lub hakera. Natomiast rozgłos, który amerykańskie badania wywołały trzy lata temu, nie wywarł większego wpływu na zachowania użytkowników komputerów w naszym kraju. Bezpieczeństwo danych to nadal problem traktowany marginalnie.

Każdy jest zagrożony

Przedstawione wyniki powinny być ostrzeżeniem dla wszystkich tych, którzy do tej pory podchodzili do kwestii ochrony informacji z lekceważeniem. Ten problem dotyczy każdego użytkownika komputera, zarówno w domu, jak i w firmie. Nawet jeśli wydaje nam się, że nie mamy na komputerze żadnych istotnych danych, informacje wydobyte z e-maili czy cache'u przeglądarki w wielu wypadkach wystarczą przestępcy na przykład do zaplanowania włamania do mieszkania. Przedstawione kwestie są jeszcze istotniejsze dla firmowych informatyków. Powinni oni ustalić procedury postępowania, które wykluczą wyciek służbowych tajemnic przy okazji inwentaryzacji sprzętu. Pamiętajmy, że nasze bezpieczeństwo zależy głównie od nas samych. ■

Szymon Piłat jest studentem Wydziału Fizyki Uniwersytetu Warszawskiego. W czasie opisanych badań był koordynatorem laboratorium odzysku danych.
Kamil Kulesza jest adiunktem w Instytucie Podstawowych Problemów Techniki PAN, prowadzi też projekt badawczy dotyczący trwałości zapisu na nośnikach magnetycznych.

Jak zniszczyć dane

Przed sprzedażą lub oddaniem niepotrzebnego już dysku twardego należy usunąć z niego dane w taki sposób, aby nie można było ich odzyskać. Do tego celu najlepiej wykorzystać specjalne programy, które korzystając ze sprawdzonych algorytmów nadpisują (zamazują) dane. Sprawdziliśmy, że skuteczność tego typu programów jest na tyle wysoka, iż uniemożliwia w domowych warunkach odzyskanie informacji.

Przykładami takich programów są Media-Eraser, Acronis Drive Cleanser, R-Wipe and Clean, BCWipe, Eraser i wiele innych, łatwo dostępnych w Internecie. Użytkownicy Linuksa mają łatwiej, gdyż prawie każda dystrybucja tego systemu zawiera polecenie shred, za pomocą którego możemy skutecznie kasować pliki. Można również skorzystać z nieco bardziej zaawansowanego programu wipe (do pobrania z wipe.sourceforge.net).

O krok od więzienia

Przemysław Krejza, dyrektor ds. badań i rozwoju MediaRecovery www.mediarecovery.pl

Z pewnej placówki medycznej nastąpił wyciek dużej ilości danych osobowych pacjentów. Sprawą zajęła się prokuratura, a w stan oskarżenia został postawiony administrator sieci komputerowej, gdyż plik zawierający dane miał jego sygnaturę. Oskarżony zwrócił się do nas z prośbą o pomoc w wykazaniu jego niewinności. Po przeprowadzeniu analiz okazało się, że dane pochodzą z okresu, kiedy wymiana informacji pomiędzy systemami odbywała się za pomocą dyskietek. Na podstawie nagłówka pliku udało nam się również ustalić imię i nazwisko osoby, która pośredniczyła w sprzedaży danych. Wskazanie prokuraturze tej osoby pozwoliło na jej zatrzymanie i przesłuchanie. Podejrzany zeznał, że odnalazł wyrzucone stosy pustych dyskietek, z których odtworzył zapisane na nich wcześniej informacje. Tak odzyskane pliki z danymi osobowymi pacjentów postanowił sprzedać.

Druga historia dotyczy danych pewnego prezesa, kóry oddał swój komputer przenośny z uszkodzonym dyskiem do naprawy. Prezes ten stał się ofiarą ciekawskiego serwisanta, który wymienił w dysku elektronikę i przeglądnął zawarte na nim dane. Odnalezione tam informacje i zdjęcia postanowił wykorzystać do szantażu. Ten przypadek jest zresztą dosyć typowy – przeglądanie danych przez serwisantów. Dlatego zalecamy utylizację danych przed wysłaniem dysku do serwisu.