GRZEGORZ BŁOŃSKI

Złodzieje danych

Stopień trudności

Sieci informatyczne spowodowały dynamiczny rozwój zdalnych technik atakowania ofiary przy wykorzystaniu oprogramowania oraz połączenia sieciowego. Doskonalenie tego rodzaju metod ataku odbywa się cały czas. Czy w kontekście tych faktów należy lekceważyć próby ataków z wykorzystaniem socjotechniki i dostępu fizycznego do komputera?

Przez wiele lat doskonalono techniki zabezpieczania się przez nieautoryzowanym dostępem i robi się to do tej pory, lecz od zawsze najsłabszym ogniwem wykorzystywanym w tego rodzaju atakach był człowiek.

Nawet najlepsze, najnowsze, najbardziej restrykcyjne polityki bezpieczeństwa tworzone przez firmy pragnące uchronić się przez nieautoryzowanym dostępem do ich systemów informatycznych nie są wolne od wad. Wszyscy muszą liczyć się z zagrożeniami związanymi ze słabością takiej polityki bezpieczeństwa, słabością związaną właśnie z jej najsłabszym ogniwem – człowiekiem. Dobrze zaprojektowana i skonstruowana polityka bezpieczeństwa kładzie ogromy nacisk na podnoszenie świadomości personelu firmy w kwestiach minimalizowania podatności na ataki z użyciem socjotechniki. Prowadzone są szkolenia pokazujące w jaki sposób działają osoby dokonujące ataku, przedstawiane są przykłady dla zobrazowania przebiegu ataku. Tego rodzaju działania można określić *prewencyjnymi*, lecz czy są one tak skuteczne jak je oceniamy, czy osławiony czynnik ludzki staje się w ten sposób bardziej odporny – warto przekonać się samemu. W artykule chciałbym przedstawić przykładowy schemat *ataku*, z wykorzystaniem socjotechniki oraz napędu USB z uprzednio przygotowanym zestawem oprogramowania do automatycznego zbierania określonych informacji. Podobne zestawy można znaleźć w Sieci, lecz nie zawsze korzystają z programów darmowych.

Etap 1 – kompletujemy oprogramowanie

Do uzyskania określonych informacji musimy użyć odpowiedniego oprogramowania. Poczyńmy więc wstępne ustalenia, co będzie nas interesowało w momencie uzyskania fizycznego dostępu do komputera-ofiary.

Najważniejszą rzeczą będzie fakt wybrania komputera z systemem Windows 2000/XP/2003server/Vista/2008server. Te systemy mają domyślnie włączoną funkcję autouruchamiania programów na napędach USB.

Z wielu mogących zainteresować włamywacza informacji w komputerach na poniższej liście zawarłem te najbardziej interesujące pozycje:

- hasło administratora systemu i użytkowników,
- hasła do usług sieciowych zapisane w pamięci przeglądarki,
- hasła do kont zdefiniowanych w programach pocztowych,
- hasło sieciowe sieci bezprzewodowej (WLAN).

Z ARTYKUŁU DOWIESZ SIĘ

jak stworzyć napęd USB z programami do zbierania danych,

jak wykonać atak socjotechniczny z użyciem tego napędu.

CO POWINIENEŚ WIEDZIEĆ

znać podstawy pracy w systemach Windows,

znać podstawy tworzenia plików wsadowych.

Wybór padł na te właśnie rzeczy z prostej przyczyny – to najbardziej rozpowszechnione aplikacje, dające dostęp do usług internetowych o masowym już charakterze, takich jak poczta e-mail czy WWW.

Oczywiście listę można rozbudować o kolejne aplikacje, wyciągające kolejne informacje, lecz na potrzeby tego artykuły uważam, że jest to wystarczająca ilość, aby pokazać istotę zagadnienia. Zaczynamy więc pobieranie potrzebnych aplikacji.

Na początek *gethashes*, składnik programu *Saminside*. Pobieramy go ze strony *http://www.insidepro.com*, na której znajdziemy dokładny opis działania programu, a także jego wcześniejsze wersje (Uwaga: Licencja programu pozwala na używanie go tylko na swoim komputerze, wykorzystanie go do uzyskania z innego komputera jest naruszeniem warunków licencji). Za pomocą tego programu uzyskamy hasła w postaci zakodowanej, które później *odkodujemy*. Ten program pozwoli na uzyskanie informacji o koncie administratora, a także innych użytkowników zdefiniowanych w komputerze, który będzie ofiarą. Warunkiem zadziałania tego programu jest uruchomienie go z poziomu użytkownika z uprawnieniami administratora i na to właśnie liczymy.

W przypadku gdy nie będziemy mieli takich uprawnień, program nie będzie w stanie odczytać tych informacji. Kolejne programy pochodzą ze strony *www.nirsoft.net* i są w pełni darmowe.

- *IE Pass View* – pozwoli podejrzeć hasła zapisane w przeglądarce IE.
- *IE Cache View* - pozwoli przejrzeć pamięć podręczną przeglądarki.
- *Mozilla Cache View* – pozwala przejrzeć pamięć podręczna przeglądarek Firefox/Mozilla/ Netscape.
- *MailPassView* – przeglądniemy hasła do kont pocztowych zdefiniowanych w programach pocztowych OE , MS Outlook , Thunderbird , IncrediMail, Eudora itp
- *PasswordFox* – wyciąga hasła z przeglądarki Firefox.
- *WirelessKeyView* – hasło WLAN.
- *MacAddressView* – informacje o adresie IP oraz MAC.

Wszystkie wymienione powyżej programy oprócz *gethashes*, mogą wygenerować raporty w różnych formatach. Wybramy HTML, który pozwoli na wygodne ich przeglądanie. W tak spreparowanym napędziu może się także znaleźć złośliwy kod (trojan,backdoor), który sprawnie ukryty w systemie może w późniejszym terminie uzupełniać zbierane przez nas dane.

Etap 2 – tworzymy napęd USB

Aby nasze narzędzia działały w pełni automatycznie, należy umieścić je w odpowiednich katalogach na naszym napędzie USB oraz przygotować właściwe pliki wsadowe i skrypty startujące wszystko automatycznie. Prawie automatycznie, z drobną pomocą *użytkownika* komputera ofiary.

Załóżmy, że pliki wykonywalne oraz pliki wsadowe umieścimy w katalogu *binary*, a w katalogu *zrzuty* będziemy zapisywać wyniki naszych działań.

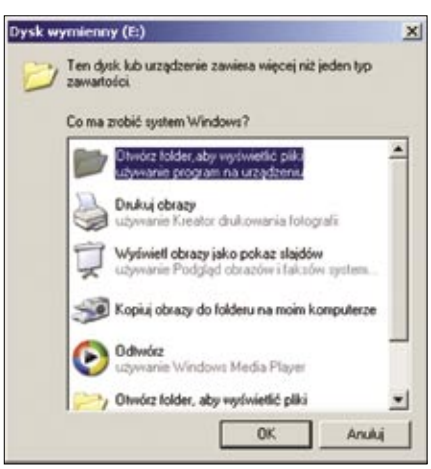
W katalogu głównym musi się znaleźć plik *autorun.inf*, który pozwoli na częściowo automatyczny start naszego zestawu szperacza. Także w głównym katalogu umieścimy aplikację *nircmd.exe,* która pozwoli nam uruchamiać pliki wsadowe i aplikacje w trybie konsoli. Ta aplikacja tak naprawdę potrafi dość sporo, nawet otwierać i zamykać tackę napędu CD/DVD czy wyciszać kartę audio za pomocą prostych przełączników w linii poleceń, ale jej główną zaletą jest możliwość uruchamiania programów w tle, bez widocznych otwartych okien na pulpicie. Nasz napęd będzie mógł wykradać dane z systemów operacyjnych. Będący w fazie RTM Windows 7 jest zabezpieczony i pliki *autorun.inf* będą w nim działały tylko w napędach CD/DVD.

W Listingu 1. można zobaczyć, jak wyglada plik *autorun.inf* na moim napędzie, w momencie podłączenia go do portu USB użytkownik widzi w oknie napis zdefiniowany w linii *action*, a kiedy potwierdzi wykonanie tej operacji w zasadzie będzie się otwierało okno exploratora – czyli standardowo w takich sytuacjach, jednak w tle będą się wykonywały wszystkie zdefiniowane przez nas zadania. Ikona wyświetlana w oknie jest identyczna z domyślną wyświetlaną przez system operacyjny, co dodatkowo powoduje otwarcie naszego napędu bardziej wiarygodne i teoretycznie bezpieczne, o ile pamięci USB można nazwać bezpiecznymi.

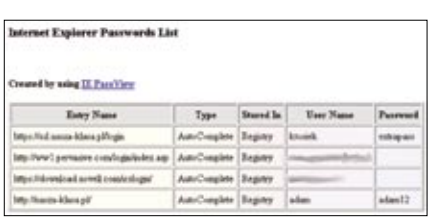
W linii *shellexecute* uruchamiany jest w pierwszej kolejności plik wsadowy a w drugiej kolejności wywoływana jest aplikacja *gethashes*, która odczytuje z pliku *C:\windows\repair\sam* zakodowane hasła użytkowników.

Czas na plik wsadowy *startuj.bat*, w którym ustalimy jakie programy, w jakiej kolejności mają się wykonać i gdzie mają się zapisać wyniki ich działania lub kolejne pliki wsadowe, o ile zachodzi taka potrzeba.

Plik *lista.bat* zawiera instrukcje uruchamiające poszczególne programy. Natomiast plik *okno.bat* zawiera



Rysunek 1. *Podświetlona pozycja wygląda identycznie jak domyślna systemowa u dołu*



Rysunek 2. *Raport HTML z programu IEPassView pokazujący hasła do usług zapisane w przeglądarce Internet Explorer*

instrukcje wymuszające pracę naszych aplikacji w tle. Szczegóły na temat opcji można znaleźć w pomocy programu *nircmd.exe*.

Mamy gotowy zestaw zgodnie z poczynionymi założeniami, który powinien zebrać dla nas informacje. Aby zapewnić odrobinę bezpieczeństwa w naszym, dość ryzykownym, wykradaniu danych, powinniśmy odpowiednio ukryć katalogi i pliki na naszym napędzie. W tym celu zarówno katalogom *binary*, *zrzuty*, jak plikom *autorun.inf* i *nircmd.exe* nadajemy atrybut *ukryty*, tak aby były niewidoczne w systemie, licząc na to iż w komputerze-ofierze spotkamy ustawienia niewyświetlające plików ukrytych, co zapewni nam więcej bezpieczeństwa podczas próby wykradania danych.

Co jednak w przypadku, gdy użytkownik, na którego koncie będziemy zbierać dane nie będzie miał uprawnień administratora systemu – nie uzyskamy dostępu do zakodowanego hasła administratora, będziemy mieli po prostu o jedną, ale dość ważną informację mniej. Jak pokazuje życie, niestety większość użytkowników (nawet w dużych firmach !) pracuje na kontach z uprawnieniami administratora systemu.

Na podstawie uzyskanych informacji będziemy mogli poczynić przygotowania do ataku – mamy uprawnienia, aby podglądać pocztę użytkownika, korzystać z serwisów internetowych, do których hasła uzyskamy, będziemy mogli śledzić jego działania, co może pomóc nam zbierać coraz więcej informacji przydatnych podczas ataku zdalnego. Gdy uzyskamy hasło do sieci bezprzewodowej, z której korzystał użytkownik, otworzy się przed nami kolejny teren do działań przygotowujących atak.

Do zestawu narzędzi można dodać całe mnóstwo ciekawych programów które zbiorą dla nas informacje jak zainstalowane poprawki, zainstalowane programy, otwarte porty czy wreszcie uruchomione usługi. Możemy także dodać programy/skrypty, które włączą usługę zdalnego pulpitu oraz inne usługi, które mogą przydać się nam podczas późniejszego ataku zdalnego.

Etap 3 – wykradamy dane – więcej socjotechniki niż myślisz

Czas na próbę naszych socjotechnicznych zdolności. Przedstawiamy zupełnie hipotetyczną sytuację. Zabieramy nasz napęd USB ze sobą, a dodatkowo zabieramy teczkę z dokumentami, jakieś CV i inne dokumenty potrzebne czasem przy poszukiwaniu pracy. Na napędzie umieszczamy także plik z naszym listem motywacyjnym, który będzie jednym z bohaterów naszego wykradania.

Wchodzimy do budynku firmy X i pierwszą napotkaną osobę – najlepiej kobietę, gdyż są bardziej ufne – pytamy o możliwość wydrukowania listu motywacyjnego, gdyż w drodze na rozmowę w sprawie pracy zauważyliśmy brak tego dokumentu w teczce, lecz przezornie posiadamy go na napędzie USB.

Gdy spotkamy się z aprobatą i chęcią pomocy jesteśmy na wygranej pozycji. Prosimy o włożenie napędu do portu USB w komputerze ofiary oraz o kliknięcie w pojawiającą się opcję *Otwórz folder, aby wyświetlić pliki.*

W tym momencie użytkownik zobaczy w oknie eksploratora to, co tam umieściliśmy, czyli plik z listem motywacyjnym oraz inne pliki i katalogi, które umieściliśmy tam jako *zasłonę dymną* – katalog ze zdjęciami z wakacji, katalog z jakimś sterownikiem czy programem.

W czasie, gdy pomagająca nam osoba będzie otwierała i drukowała nasz list motywacyjny, w zupełnej ciszy, bez widocznych śladów na ekranie wykonają się programy, które do tego zaprzęgliśmy wcześniej i zbiorą dla nas cenne informacje. Jedyną oznaką pracy naszych narzędzi będzie migająca dioda aktywności naszego napędu. Po wydrukowaniu prosimy o odmontowanie naszego napędu i go odłączamy. Uprzejmie dziękujemy za pomoc i ... znikamy gdzieś w korytarzu udając, że szukamy właściwych drzwi.

W taki prosty, banalny wręcz sposób, o ile wszystko się powiedzie, możemy zdobyć istotne i cenne informacje.

Oczywiście takie działanie jest już nie tylko wykroczeniem, ale nawet przestępstwem zagrożonym karą, stąd w tytule artykułu pojawiło się słowo *złodziej*, mające spowodować zastanowienie się nad możliwościami prostych narzędzi w połączeniu z odrobiną sprytu i socjotechnicznych sztuczek.

Etap 4 – przegląd wyników

Czas sprawdzić co udało nam się *upolować*, a więc podłączamy nasz napęd do komputera (najlepiej już naszego własnego) i przeglądamy katalog zrzuty.

Znajdziemy w nim raporty w postaci plików HTML, a więc obejrzenie wyników nie będzie problemem, będzie wręcz wygodne.

Zebrane w ten sposób hasła z przeglądarek mogą nam dać także dostęp do różnych aplikacji oraz

Email Accounts List

Created by using Mail PassView

Name	Application	Email	Server	Type	User	Password	Profile
mail user	Outlook Express	user@domain.com	domain.com	POP3	user	super_tajne_hASLO	

Rysunek 3. *Raport przedstawiający dane konta pocztowego w programie Outlook Express*

Listing 1. *Struktura pliku autorun.inf*

```
@echo off
nircmd.exe execmd CALL binary\lista.bat
nircmd.exe execmd CALL binary\okno.bat
```

Listing 2. *Struktura pliku startuj.bat*

```
@echo off
nircmd.exe execmd CALL binary\lista.bat
nircmd.exe execmd CALL binary\okno.bat
```

systemów biznesowych, które coraz częściej opierają się o usługę WWW.

Pozostaje jednak kwestia zdekodowania haseł wyciągniętych przy użyciu programu *gethashes*.

Możemy do tego celu użyć jakiegokolwiek programu korzystającego z tęczowych, na przykład *rainbowcrack*, ale nie to jest tematem tego artykułu – na temat tęczowych tablic oraz programów je wykorzystujących, ukazywały się już artykuły na łamach hakin9.

Można powiększyć ilość zbieranych informacji, operując na koncie administratora, w przypadku gdyby udało się nam dokonać zrzutu zawartości pamięci operacyjnej, przy użyciu choćby programu dd czy mdd.

Przeciwdziałanie

Czy nadal czujesz się bezpieczny? *Pod slurping* nie jest nowym zjawiskiem, lecz nadal niewiele osób jest świadomych jego obecności, a jeszcze mniej zdaje sobie sprawę, że można się przed nim w prosty sposób bronić. Jak? Wystarczy wyłączyć automatyczne uruchamianie programów dla wszystkich dysków zewnętrznych w rejestrze. W kluczu *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer* należy otworzyć wartość DWORD o nazwie *NoDriveTypeAutoRun* i przypisać jej wartość szesnastkową 9D. Takie działanie wyłączy *autorun* dla dysków pamięci masowych. Szesnastkowa wartość FD w tym miejscu wyłączy *autorun* dla wszystkich napędów w tym również CD/DVD.

W związku z tym, że zrobiliśmy to w gałęzi użytkownika, zmiany będą dotyczyły tylko tego użytkownika, aby dokonać zmian wpływających na cały system musimy wpisów dokonać w gałęzi *HKEY_LOCAL_MACHINE*.

Jednak pamiętajmy, że wyłączenie *autorun* dla dysków USB nie zwalnia nas od myślenia , traktowania poważnie naszych danych oraz rozsądnego podejścia do zarządzania bezpieczeństwem.

Podsumowanie

Zapewne wielu czytelników spotkało się już z narzędziami podobnymi do tych zaprezentowanych w tym artykule. Każdy kto używał oprogramowania do wykonywania audytu stacji roboczej, wie że tym sposobem można zdobyć ogrom informacji. Mimo tego że fizyczny dostęp do komputerów w wielu miejscach jest ograniczony, przy odrobinie szczęścia opisany scenariusz lub podobny może mieć miejsce.

Wiele firm w swoich rozbudowanych politykach bezpieczeństwa uwzględnia te kwestie i zakazuje użytkownikom komputerów podłączania *obcych* napędów. Czy jednak poziom świadomości zagrożenia poszczególnych użytkowników jest dostatecznie wysoki? Wielu ludzi zajmujących się bezpieczeństwem systemów informatycznych podziela opinię, iż każdy system jest tak bezpieczny jak jego najsłabsze ogniwo. Wiadomo także, że to właśnie człowiek/użytkownik jest najsłabszym ogniwem polityki bezpieczeństwa, więc im bardziej świadomy zagrożeń użytkownik, tym bardziej wprowadzona polityka ma szanse uchronić przed wyciekiem danych, mogącym w efekcie doprowadzić do kompromitacji czy to konkretnego systemu, czy całej sieci firmowej.

Przedstawione w artykule programy na pierwszy rzut oka są programami prostymi i niegroźnymi, lecz nawet proste narzędzia potrafią być źródłem kłopotów. Niestety problem może być o wiele bardziej skomplikowany, gdy weźmiemy pod uwagę możliwość spreparowania w opisany sposób kart pamięci wykorzystywanych w aparatach fotograficznych, telefonach komórkowych, odtwarzaczach mp3 i innych podobnych, wykorzystujących interfejs USB jako połączenie pamięci masowej z komputerem, które także mogą posłużyć jako narzędzie kradzieży danych.

Rynek dostarcza coraz więcej ciekawych urządzeń korzystających z interfejsu USB, a więc możliwości cały czas rosną.

Polityka bezpieczeństwa w wielu firmach powinna zostać zweryfikowana, a personel niewątpliwie przeszkolony, aby minimalizować możliwości wystąpienia tego rodzaju incydentów.

Działania mające na celu kradzież danych przy użyciu pamięci zewnętrznych w USA otrzymało miano *podslurpingu* i jest ścigane.

Opisany scenariusz można by porównać do sytuacji, gdy ktoś przychodzi do firmy, udaję mu się na chwilę uzyskać klucze do różnych drzwi i robi ich odciski w plastelinie celem późniejszego dorobienia takich kluczy. Taka sytuacja spowoduje, iż każdy z nas pomyśli, że ta osoba planuje włamanie i nikt nie będzie się nawet zastanawiał nad innym możliwym wytłumaczeniem takiego zdarzenia. Czy nie należy w taki sam sposób, z dużą ostrożnością podchodzić do urządzeń typu dysk USB, pendrive, karta pamięci podłączanych do naszych komputerów. Mam nadzieję, że ten artykuł spowoduje chwilę refleksji nad tematem oraz natchnie kilka osób do czujniejszego, poważniejszego traktowania przenośnych pamięci – one naprawdę mogą być bardzo niebezpieczne.

W Sieci

- *http://www.insidepro.com,*
- *http://www.nirsoft.net,*
- *http://www.usbhacks.com/2006/10/29/how-to-simple-podslurping-example-with-a-usb-flash-drive/,*
- *http://www.businessweek.com/the_thread/techbeat/archives/2005/07/pod_slurping_to.html,*
- *http://www.gfi.com/whitepapers/pod-slurping-an-easy-technique-for-stealing-data.pdf.*

Grzegorz Błoński
Z wykształcenia jest informatykiem, certyfikowanym specjalistą IBM. Pracuje w dużej firmie o zasięgu światowym. Zajmuje się administracją, bezpieczeństwem sieciowym. Należy do międzynarodowych organizacji ISOC oraz ISACA zajmujących się szeroko pojętym bezpieczeństwem IT. Jest członkiem Digital Forensic Association.
Kontakt z autorem: *mancymonek@mancymonek.pl.*