MARIUSZ RÓG

Zdalne zarządzanie: NetBus Pro

Stopień trudności

Artykuł przedstawi trojana NetBus. W prosty sposób wyjaśni zasadę działania oraz poszczególne funkcje aplikacji. NetBus jest jednym ze starszych trojanów, jakie ukazały się w sieci – powstał w 1998 roku. Został napisany przez Szweda, Carla Fredrika Neiktera. Jest to jeden z nielicznych dobrych programów typu backdoor.

Z ARTYKUŁU DOWIESZ SIĘ

jak prawidłowo skonfigurować serwer NetBus i używać klienta,

poznasz zalety oraz wady używania trojana do zdalnego zarządzania,

poznasz funkcjonalność programu oraz zapoznasz się z architekturą aplikacji.

CO POWINIENEŚ WIEDZIEĆ

czym są programy typu backdoor oraz jak się przed nimi zabezpieczyć,

jak konfigurować porty w zaporze ogniowej systemu Windows,

powinieneś posiadać podstawowe informacje na temat sieci LAN oraz konfiguracji protokołów komunikacyjnych.

NetBus, będąc na początku typową aplikacją *backdoor*, przez kilkanaście lat przekształcił się w interesujący program do zdalnego zarządzania komputerami. Jest całkiem bezpieczny, gdyż sygnatura jego kodu znajduje się w większości programów antywirusowych. Wszelka próba uruchomienia klienta lub serwera jest od razu zauważana przez aplikacje antywirusowe. Z tego też względu przed uruchomieniem programu należy skonfigurować program antywirusowy. Wystarczy wykluczyć aplikację z listy analizowanych programów. Narzędzie jest teraz prostsze w obsłudze oraz posiada szereg unikalnych funkcji. Dlatego też jest ciekawą alternatywą dla w pełni komercyjnych i skomplikowanych systemów zdalnego zarządzania.

Instalacja

Proces instalacji wersji 2.10 jest prosty. Po uruchomieniu instalatora oraz wybraniu miejsca instalacji instalator zadaje pytanie, które komponenty mają zostać zainstalowane.

Ze względu na mało intuicyjny podział aplikacji *NetBus* należy wyjaśnić, do czego służą poszczególne komponenty. Aplikacja *NetBus* podzielona jest na dwie części: serwer oraz klient. Część kliencka instalowana jest na komputerze zarządzającym, zaś część serwerowa – na komputerach zarządzanych. Po instalacji, w zależności od wybranych opcji, instalowane są dwa pliki wykonywalne *NetBus.exe* oraz *NBSvr.exe*. Program *NetBus* jest to aplikacja kliencka służąca do administracji innymi komputerami. *NBSvr* jest zaś serwerem udostępniającym usługi. W katalogu instalacyjnym oprócz plików wykonywalnych znajduje się kilka bibliotek dynamicznych.

Konfiguracja serwera

Kluczem do sprawnego oraz bezpiecznego zarządzania komputerem jest prawidłowa konfiguracja serwera. Domyślnie serwer jest wyłączony. Aby go włączyć, należy uruchomić plik *NBSvr.exe*. Po chwili ukazuje się okienko z listą podłączonych klientów (dzięki temu jesteśmy w stanie sprawdzić, kto zarządza komputerem). Okno przedstawione zostało na Rysunku 2.

Autor aplikacji twierdzi, iż jednym serwerem może zarządzać kilka klientów jednocześnie bez wprowadzania konfliktów. Można to wykorzystać używając jednego serwera jako np. repozytorium plików. Oprócz listy klientów, okno zawiera informacje o aktywnych serwerach. Do dyspozycji są trzy serwery – właściwy serwer *NetBus* oraz serwer *telnet* i *http*.

Konfiguracja serwera odbywa się przez wciśnięcie przycisku *Setting*. Włącza on okno konfiguracyjne pokazane na Rysunku 3.

W zakładce *General* dostępne są ogólne opcje związane z serwerem. Aby uruchomić

serwer, należy zaznaczyć opcję *Accept connections*. Następnie należy ustawić port, na którym serwer będzie nasłuchiwał połączeń. Domyślnym portem jest 20034. Aby serwer pracował poprawnie, należy odblokować wskazany port w konfiguracji zapory ogniowej. Opcjonalnie można w polu *Password* określić hasło. Ze względu na dostęp do większości krytycznych zasobów komputera zaleca się stosowanie hasła. Następnie należy wybrać stopień widoczności dla serwera. Do dyspozycji są cztery tryby widoczności przedstawione w Tabeli 1.

Należy być szczególnie ostrożnym przy użyciu trybu *Only in tasklist*, gdyż blokuje on całkowicie dostęp do okna konfiguracji, a co za tym idzie – dostęp do trybów. W tym przypadku możliwość zmiany trybu widoczności ma tylko klient znający hasło dostępu.

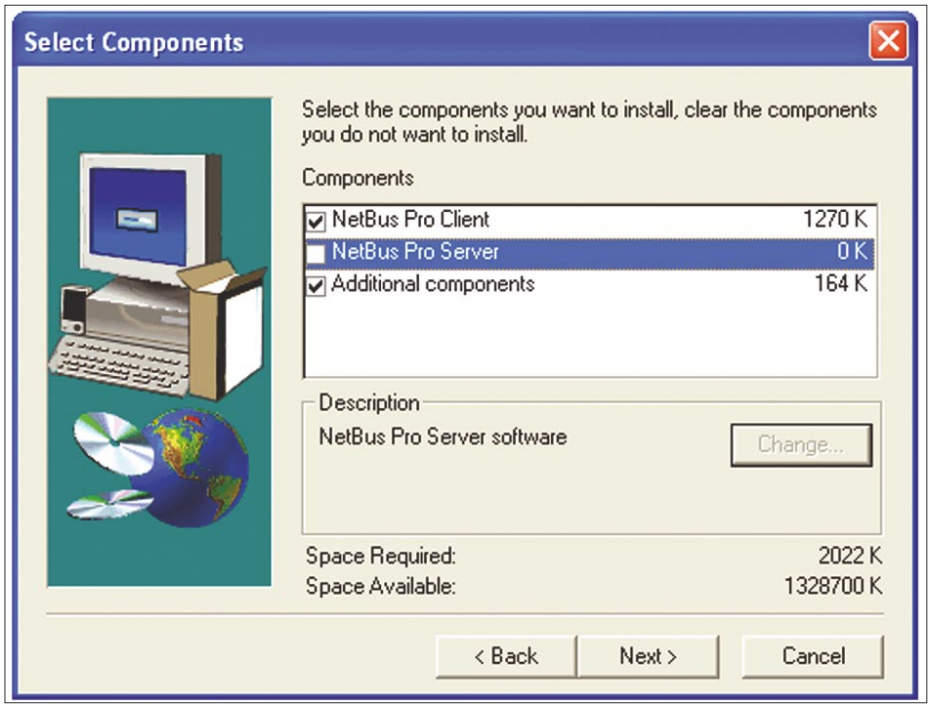
Do wyboru jest także lista trybów dostępu do komputera, odpowiednio od najbardziej restrykcyjnego do pełnego dostępu. Tryby te zostały opisane w Tabeli 2. Zmiana konfiguracji (w pewnym ograniczonym zakresie) może odbywać się również z poziomu klienta. Należy jednak zwrócić uwagę, iż ze względów bezpieczeństwa możliwość zdalnego modyfikowania trybu jest dostępna tylko w trybie pełnego dostępu.

Ostatnim elementem kompletującym konfigurację jest umożliwienie startowania serwera automatycznie. W zależności od potrzeb można włączyć tę opcję lub uruchamiać serwer ręcznie.

W wersji 2.10 opcja wyłączająca logowanie jest nieaktywna. Program zawsze będzie logował połączenia do pliku *Log.txt*, nie ma też możliwości zmiany nazwy pliku.

Tabela 1. *Lista trybów widoczności*

Widoczność	Opis
Full visible	Serwer będzie aktywny tylko, gdy okno aplikacji będzie włączone. Po wyjściu z programu serwer automatycznie kończy pracę.
Minimize as trayicon	Tryb podobny do pierwszego, lecz w tym przypadku serwer może być zminimalizowany do paska tray.
Only in tasklist	Tryb widoczności, w którym okno konfiguracji nie włącza się w ogóle. Serwer w tym trybie widoczny jest tylko za pośrednictwem managera zadań (taskmgr).
Invisible (95/98)	Tryb identyczny z poprzednim, lecz dostosowany do systemów Windows 95 i 98.



Rysunek 1. *Wybór komponentów przy instalacji NetBus*

Dostęp do serwera

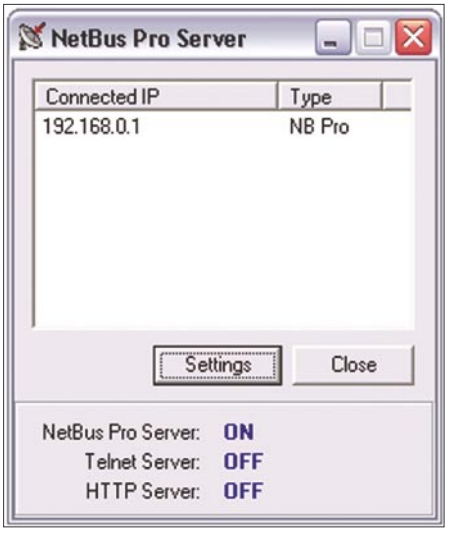
Każdy administrator zdaje sobie sprawę, że zabezpieczenie takiej funkcjonalności tylko hasłem nie jest dobrym rozwiązaniem. Jednak NetBus posiada dodatkową formę zabezpieczeń w postaci listy akceptowanych adresów, które mogą się połączyć z serwerem. Ustawia się ją przy pomocy klienta, przy użyciu menu *Server admin* (opcja *Restrict access*). Pozwala ona ręcznie określić konkretne adresy lub zakresy adresów, które są upoważnione do połączenia z serwerem.

Przykładowe prawidłowe wpisy listy to:

- 192.168.0.1 (zezwala na połączenie z adresu 192.168.0.1),
- 192.168.0.* (zezwala na połączenia z adresów rozpoczynających się oktetami 192.168.0),
- 192.168.0.1-10 (zezwala na połączenie z każdego adresu z zakresu od 192.168.0.1 do 192.168.0.10).

Uruchomienie klienta

Prawidłowo skonfigurowany serwer udostępnia usługi na wskazanym porcie. Aby z nich skorzystać, należy uruchomić klienta za pomocą pliku wykonywalnego *NetBus.exe*. Sygnatura trojana zawarta jest również w programie klienckim. Należy więc odpowiednio skonfigurować program antywirusowy – tak, aby pozwolił załadować biblioteki aplikacji. W przeciwnym wypadku użytkownikowi zostaną zgłoszone błędy związane



Rysunek 2. *Okno włączonego serwera NetBus*

z brakiem możliwości załadowania procedur aplikacji.

Jeśli klient został uruchomiony prawidłowo, to wyświetli się okno z listą hostów. Domyślnie dodany jest jeden host związany z adresem lokalnym klienta. Jeśli więc podczas instalacji zaznaczono opcje klienta i serwera, to istnieje możliwość podłączenia od razu do komputera klienta. Aby dodać dowolny host, należy znać jego adres IP lub nazwę hosta w sieci lokalnej. Odbywa się to przy użyciu menu opcji *New...* z menu *Host*. Następnie należy podać adres hosta, numer portu, dowolną nazwę identyfikującą komputer oraz opcjonalnie hasło i nazwę użytkownika na serwerze. Po wciśnięciu przycisku *OK* host zostanie dodany do listy. Mając tak przygotowaną listę, można dowolnie łączyć się z wybranym komputerem poprzez dwukrotne kliknięcie na element listy lub za pomocą menu podręcznego i opcji *Connect*. Należy zwrócić uwagę na fakt, że klient w konkretnym momencie może być podłączony tylko do jednego serwera. Jest to trochę kłopotliwe, jeśli zamierza się wykonać określoną operację na kilku hostach.

Funkcje kontrolne

Podłączony klient ma do dyspozycji bardzo szeroki wachlarz funkcji związanych ze zdalnym zarządzaniem komputera. Niektóre z tych funkcji umożliwiają głęboką ingerencję w sam system, na którym zainstalowany jest *NetBus*. Zaleca się dużą ostrożność w ich użyciu. Funkcje podzielone są na logicznie powiązane moduły.

Rysunek 3. *Ustawienia serwera NetBus*

Tabela 2. *Tryby dostępu do komputera z zainstalowanym serwerem*

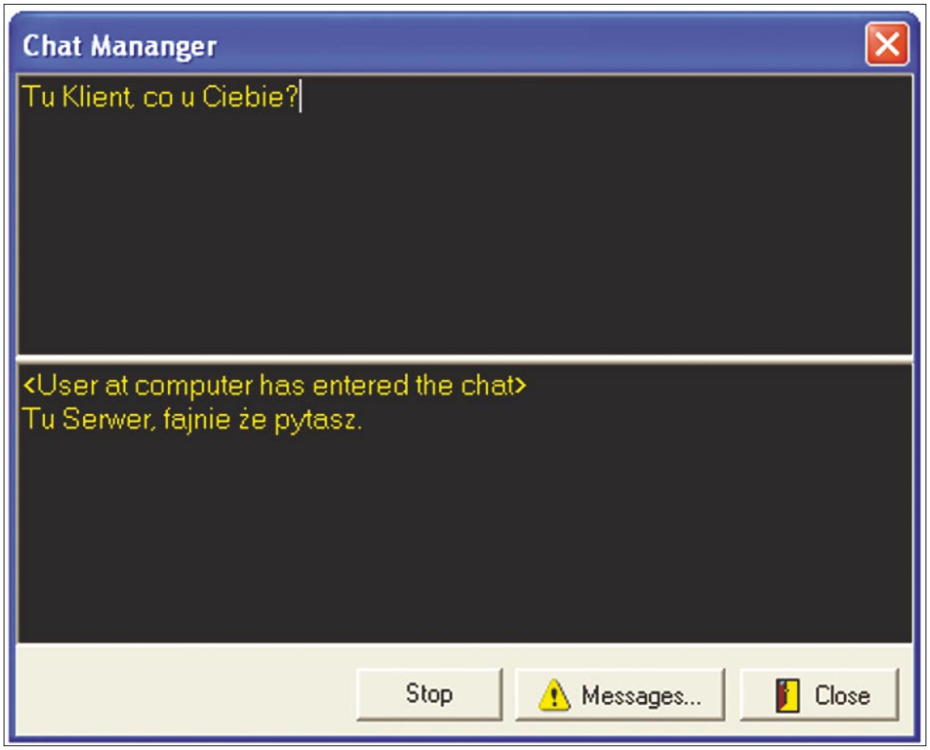
Widoczność	Opis
Basic access	Podstawowy tryb umożliwiający tylko otrzymanie informacji o hoście.
Spy mode access	Umożliwia tylko śledzenie działań użytkownika.
Full access	Tryb dający pełną kontrolę nad funkcjonalnością serwera NetBus.

Tabela 3. *Lista funkcji podmenu Spy functions*

Nazwa funkcji	Opis funkcji
Keyboard listen	Pozwala na podsłuchiwanie komunikatów klawiatury.
Capture screen image	Generuje zrzut ekranu do pliku.
Capture camera video	Przechwytuje obrazy z kamery podłączonej do serwera.
Record sound	Przechwytuje dźwięk z mikrofonu podłączonego do serwera.

Tabela 4. *Lista funkcji podmenu Cool functions*

Nazwa funkcji	Opis funkcji
CD-ROM	Pozwala na wysuwanie oraz wsuwanie podstawki napędu optycznego.
Disable keys	Umożliwia tylko śledzenie działań użytkownika.
Key click	Włącza dźwięk klawiszy w systemie.
Swap mouse	Zamienia miejscami przyciski myszki.
Go to URL	Uruchamia wskazany adres w domyślnej przeglądarce internetowej.
Send text	Wstawia wskazany tekst w pole edycyjne (jeśli istnieje) aktywnego okna.



Rysunek 4. *Moduł Chat Manager*

Chat manager

Moduł *Chat manager* jest przydatną funkcją pozwalającą na komunikację w obie strony (między użytkownikiem klienta i użytkownikiem serwera). Rysunek 4 przedstawia okno uruchomionego modułu *Chat Manager*.

Górne pole służy do wprowadzania, a dolne – do wypisywania otrzymanego tekstu. Aby rozpocząć rozmowę, wystarczy nacisnąć przycisk *Start*. W tym momencie na ekranie serwera pojawi się podobne okienko rozmowy i zostanie uruchomiony system konwersacji. Ciekawym jest fakt, że rozmowa odbywa się w czasie rzeczywistym, tzn. każdy z naciśniętych znaków jest natychmiast transportowany protokołem do odbiorcy i wypisywany na ekranie. Niesie to za sobą kilka problemów implementacyjnych, których autor w wersji 2.10 nie rozwiązał. Dla przykładu – próba poprawienia wpisanego tekstu klawiszem *Backspace* powoduje wypisanie u odbiorcy pionowej kreski. Oprócz tego moduł posiada kilka błędów implementacyjnych, np. możliwe jest pisanie tekstu w okienku odczytu, zaś wpisanie tekstu, a następne naciśnięcie przycisku *Start* powoduje naruszenie ochrony pamięci oraz brak możliwości przewijania tekstu u odbiorcy.

Moduł, pomimo swoich niedoskonałości, posiada pewną dodatkową funkcjonalność rekompensującą niedopatrzenia autora – mianowicie wbudowany moduł *Message manager*. Uruchamia się go za pomocą przycisku *Messages...* w oknie modułu *Chat manager*. Uruchomiony moduł widać na Rysunku 5. Służy on do wywoływania okienek informacyjnych przy wykorzystaniu *WinApi* na hoście. Okienka mogą mieć różną postać w zależności od rodzaju wybranych opcji, wszystkie jednak bazują na funkcji *MessageBox* i jej flagach. Informacja zwrotna przekazywana jest do klienta, a ten wywołuje własną funkcję *MessageBox* z odpowiedzią.

Rysunek 5. *Moduł Message manager*

File manager

Moduł *File manager* pozwala, dzięki protokołowi aplikacji, ingerować w system plików hosta. Wykorzystanie modułu nie jest skomplikowane – użycie sprowadza się do naciskania odpowiednich przycisków w okienku. Niestety, *File manager* nie radzi sobie dobrze z plikami zajętymi przez inne aplikacje. Przegrywanie pewnych plików z systemu hosta w tym przypadku jest po prostu niemożliwe. Na dokładkę użytkownik klienta nie jest poinformowany o problemie kopiowania plików, zmuszony jest czekać. Jedyne, co pozostaje w takiej sytuacji, to wciśnięcie przycisku *Cancel* w okienku transportowym. Uruchomiony moduł można zobaczyć na Rysunku 6. Obrazki reprezentujące przyciski są raczej intuicyjne. Po prawej stronie okienka ułożone są trzy przyciski – odpowiednio: przejście do folderu powyżej, usunięcie folderu oraz stworzenie nowego folderu. Operacji na strukturze katalogów wykonuje się przy użyciu przycisków z dołu ekranu i nie wymagają one wyjaśnień. Niestety, funkcje udostępniania stworzone zostały pod system Windows 95/98. Na systemach opartych o NT ta funkcjonalność nie będzie działać.

Windows manager

Windows manager to skomplikowany w obsłudze moduł, pozwalający w pewnym zakresie zarządzać oknami uruchomionych programów na systemie hosta. Dla osoby zarządzającej lista okien na serwerze widoczna jest w postaci drzewa. W początkowej fazie korzystania z modułu ciężko jest się zorientować w hierarchii okien. Na szczęście po krótkiej

Tabela 5. *Lista poleceń skryptów*

Polecenie	Opis polecenia
MessageBox	Wyświetla okno informacyjne. Parametry: typ okna, wiadomość.
DeleteFile	Kasuje plik. Parametr: ścieżka do zdalnego pliku.
NewFolder	Tworzy nowy katalog. Parametr: ścieżka do katalogu.
DownloadFile	Pobiera plik ze zdalnego systemu plików.
UploadFile	Ścieżka do katalogu zdalnego.
AddRegData	Dodaje wpis do rejestru. Parametry: ścieżka w rejestrze, nazwa i wartość wpisu.
	Usuwa wpis z rejestru. Parametry: ścieżka w rejestrze, nazwa wpisu.
RunPlugin	Uruchamia plugin z biblioteki dynamicznej.
ExecuteFile	Uruchamia plik wykonywalny. Parametr: ścieżka do uruchamianego pliku.
PlaySound	Odtwarza dźwięk. Parametr: ścieżka do pliku w formacie *wav*.
ShowImage	Wyświetla obraz. Parametr: ścieżka do pliku obrazu.
OpenCD	Otwiera napęd CD-ROM. Parametr: liczba 1, reprezentująca wartość *true*.
ScreenDump	Zapisuje obraz ekranu do podanego katalogu. Parametr: katalog zapisu obrazu.
ExitWindows	Zamyka system Windows.
DisableKeys	Wyłącza wybrane klawisze. Parametr: zestaw klawiszy do wyłączenia.
KeyClick	Aktywuje dźwięk klawiszy. Parametr: liczba 1, reprezentująca wartość *true*.
SendText	Wpisuje tekst w pole edycyjne aktywnego okna. Parametr: tekst do wpisania.
SwapMouse	Zamienia klawisze myszki. Parametr: liczba 1, reprezentująca wartość *true*.

chwili można już wykonać podstawowe czynności związane z poszczególnymi okienkami. Zaznaczenie opcji *Show only visible windows* oraz *Show only named windows* pozwala odfiltrować drzewo z okien, które nie są widoczne i nie posiadają nazwy. Funkcjonalność modułu nie jest zbyt rozbudowana, sprowadza się do prostego wyłączania okienek, zmiany wielkości, zmiany położenia oraz ustawiania tzw. fokusu. Pozwala również na modyfikacje czterech flag okna (*Is visible*, *Is enabled*, *Is checked* oraz *Always on top*). W module brakuje niestety podglądu wykonywanych czynności. Wszystkie operacje wykonuje się zatem bazując na współrzędnych oraz pikselach. Oczywiście zawsze można użyć funkcji *Capture screen image* w celu podejrzenia wyniku działania modułu.

Registry manager

Jak sama nazwa wskazuje, moduł pozwala przeglądać i modyfikować strukturę rejestru hosta. Jest to bardzo niebezpieczne, a sam moduł nie jest tak poręczny, jak aplikacja Edytor Rejestru w systemie Windows. Moduł umożliwia edycję, tworzenie i kasowanie kluczy w rejestrze oraz modyfikację, tworzenie i kasowanie samych wpisów. Nie dostarcza jednak funkcjonalności przeszukiwania rejestru. Korzystając z *Registry managera* użytkownik musi posiadać podstawową wiedzę o drzewie kluczy rejestru. Dlatego też używanie tego modułu rekomenduję tylko doświadczonym użytkownikom.

Spy functions

NetBus posiada cztery funkcje służące do śledzenia działań użytkownika. Wraz z opisem znajdują się one w Tabeli 3. Biorąc pod uwagę uwarunkowania prawne – ich używanie jest zabronione, jeśli osoba śledzona nie jest o tym poinformowana. Najbardziej niebezpieczna jest funkcja przechwytująca zdarzenia klawiatury. Dzięki niej od razu możemy wychwycić loginy i hasła do dowolnego systemu, do którego użytkownik będzie się logował lub zwyczajnie podglądać pisane przez nieświadomego użytkownika teksty.

Cool functions

Niewątpliwie *Cool functions* jest zestawem najmniej przydatnych funkcji w programie, z reguły służących do zabawy i denerwowania użytkownika. Listę funkcji oraz ich opis znaleźć można w Tabeli 4. Należy przyznać, iż funkcje z tej kategorii nie są dostępne w innych programach służących do zdalnego zarządzania.

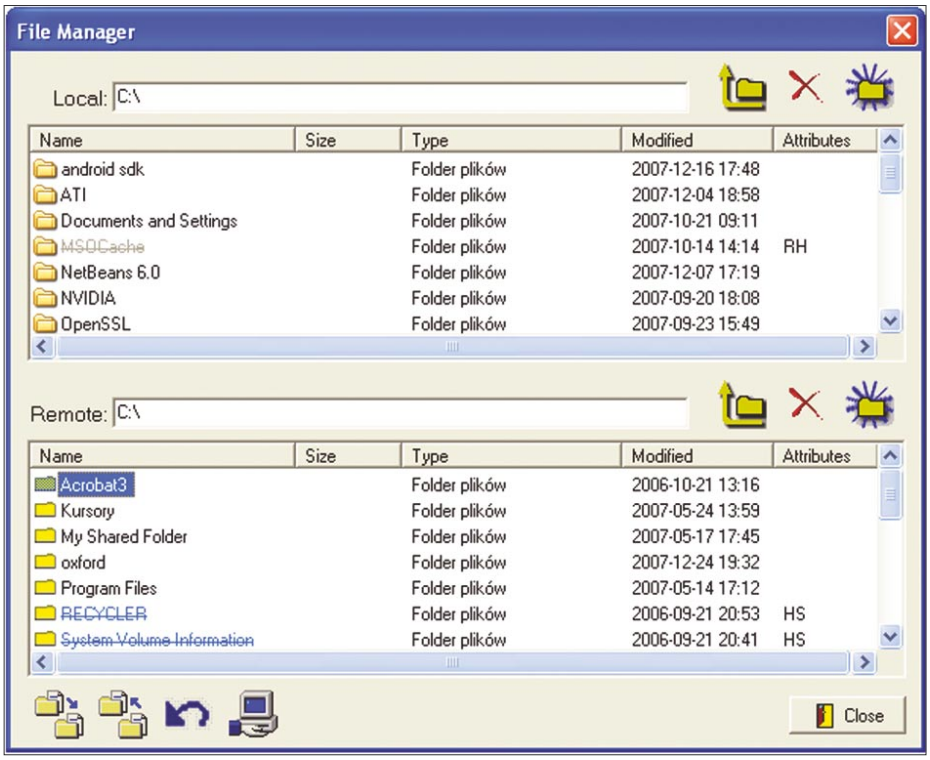
Zarządzanie hostami

Menu *Host* posiada kilka funkcji, z których część posiada oczywiste znaczenie, a inne wymagają omówienia. Są to funkcje, dzięki którym *NetBus* ma prawo być traktowany jako aplikacja do zdalnego zarządzania komputerami.

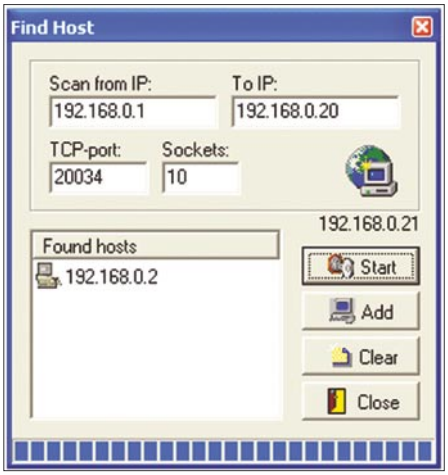
Find Host

Uruchomienie funkcji *Find Host* powoduje otwarcie okienka przedstawionego na Rysunku 7.

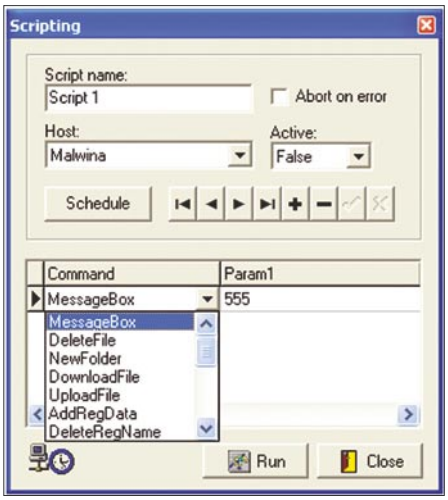
Służy ono do znalezienia hostów z zainstalowanym serwerem *NetBus* w sieci lokalnej. Dzięki tej funkcjonalności administrator nie ma potrzeby pamiętania adresów wszystkich serwerów. Aby odnaleźć interesujące hosty, należy podać zakres adresów IP do przeszukania, po czym określić port, na którym serwery nasłuchują



Rysunek 6. *Moduł File Manager*



Rysunek 7. *Uruchomione okno Find Host*



Rysunek 8. *Okno edycji skryptu*

połączeń, a na końcu – ilość gniazd (*Sockets*) używanych podczas szukania. Następnie, po naciśnięciu przycisku *Start*, uruchomiony zostanie proces przeszukiwania. Każdy z adresów z zakresu zostanie odpytany o połączenie na wskazanym porcie. Jeśli host będzie miał aktywny serwer oraz zezwoli na połączenie, to zostanie dodany do listy *Found hosts*. Z listy można wybrać znalezione serwery i dodać je przyciskiem *Add* do głównej listy.

Script

Funkcja *Script* jest potężnym narzędziem, które pozwala na wykonanie sekwencji operacji na zdalnym serwerze. Okno edycji skryptu przedstawione zostało na Rysunku 8.

Stworzenie skryptu rozpoczyna się od wybrania opcji *Script* z menu *Host*. Następnie należy podać nawę skryptu, jednoznacznie identyfikującą jego działanie. Nie jest zabronione powtarzanie nazw skryptów, tak więc zaleca się używanie nazw unikalnych. Opcja *Active* ustawiona na wartość *false* pozwala na wykonanie skryptu w późniejszym czasie. Skrypt składa się z zestawu poleceń opisanych w Tabeli 5. Naciśnięcie przycisku *Run* uruchamia proces wykonywania wybranych poleceń na zdalnym hoście. Uruchomienie skryptu można uzależnić od czasu na serwerze. Służy do tego opcja *Schedule*.

Broadcast

Ostatnia z omawianych funkcji aplikacji *NetBus* jest ściśle związana z funkcją *Script*. Służy ona do dystrybucji skryptu na wiele serwerów w tym samym czasie. Umożliwia to masowe wykonywanie zaplanowanych zadań. Przed wykonaniem funkcji *Broadcast* należy stworzyć skrypt w menu *Script*. Następnie trzeba go wybrać z listy wyboru *Script name* w oknie *Broadcast*. Ostatnią czynnością do wykonania jest podanie zakresu adresów IP, do których będzie wysłany skrypt. Uruchomienie wysłania odbywa się przez naciśnięcie przycisku *Run*. W tym momencie każdy z hostów z wskazanego zakresu otrzymuje kopię skryptu.

Podsumowanie

Aplikacja *NetBus* posiada kilka błędów, które potrafią być dokuczliwe. Mimo wszystko dostarcza wielu użytecznych i unikatowych funkcji, pozwalających w przyjemny sposób zarządzać komputerami. Dużym plusem aplikacji jest fakt, iż użytkownik zdalnego komputera może bezproblemowo pracować w czasie wykonywania operacji przez aplikację. Same funkcje narzędzia są logicznie poukładane i intuicyjne. Jak na tak niewielki program, wachlarz możliwości jest naprawdę szeroki. W zupełności wystarczy dla małych i średnich sieci.

Mariusz Róg
Autor jest programistą Javy. Posiada wiedzę z zakresu metod sztucznej inteligencji oraz rozwiązań klasy biznesowej i rozwiązań mobilnych. Obecnie pracuje na stanowisku Specjalisty ds. Produkcji Oprogramowania w firmie BLStream Sp. z o. o. BLStream jest międzynarodowym dostawcą i integratorem nowoczesnych systemów informatycznych oraz producentem oprogramowania mobilnego dla sektora medialnego, telekomunikacyjnego, finansowego i ubezpieczeniowego. Główna siedziba firmy mieści się w Szczecinie, a jej przedstawicielstwa i centra programistyczne ulokowane są we Wrocławiu, Warszawie, Helsinkach i Lwowie.
Kontakt z autorem: *mariusz.rog@gmail.com*