WaVeR's Heavy Industries 2000

WHI

DarkFTP

Trojan FTP Server

Manuale d'uso
v1.6

0. Legal Stuff

Non mi ritengo responsabile dell'uso che sarà fatto di questo materiale. Il codice sorgente, come il binario sono stati distribuiti con un unico scopo e cioè quello didattico-informativo. L'unica funzione di DarkFTP è quella di descrivere il funzionamento di un trojan basato sia su un client IRC che su un server FTP. Ogni utilizzo diverso da quello didattico non è contemplato e le conseguenze derivanti da un uso improprio non devono in alcun modo essere ricollegate all'autore di questa applicazione. Pertanto l'uso di questo materiale per uno scopo diverso da quello didattico solleva l'autore da ogni responsabilità e implica che si accetti questa condizione.

1. Cosa è DarkFTP

DarkFTP è un trojan che si installa nella macchina sulla quale viene lanciato e vi attiva un server FTP tramite il quale sono possibili operazioni di lettura e scrittura su qualsiasi file o directory del filesystem della macchina; contemporaneamente viene attivato un piccolo client IRC che si collega ad un IRC server, entra in un canale e vi rimane fino a quando viene a mancare la connessione o la macchina viene riavviata, un po nello stile di un bot. Mediante una sorta di chat col Dark, attraverso IRC, è possibile impartire una serie di comandi che vengono eseguiti sulla macchina ospite e che sono atti alla gestione completa del trojan.

2. Principali funzionalità

- Accesso completo al filesystem della macchina ospite (con WinNT limitato ai diritti dell'utente loggato in quel momento)
- Accesso multiutente
- Controllo remoto tramite IRC grazie ad un esteso set di comandi
- Possibilità di esecuzione da remoto di comandi o applicazioni locali
- Capacità di bypassare il firewall WRQ AtGuard agendo sulle chiavi del registro
- Completa configurabilità
- Gestione completa della configurazione da remoto

3. Configurazione

Tra le novità della versione 1.65 vi è anche un nuovo tool di configurazione molto più evoluto e potente dei sui predecessori. E' possibile creare una configurazione anche manualmente ma, a differenza delle versioni precedenti, nella versione attuale questa risiede all'interno dell'eseguibile, che può perciò essere tranquillamente compresso anche dopo essere stato configurato e soprattutto non è più obbligatorio che l'eseguibile del Dark si trovi in fondo ad un pacchetto generato ad esempio con il SilkRope. Il nuovo tool si presenta come una semplice form nella quale iserire i dati della configurazione, esattamente come nelle sue versioni precedenti; in più, oltre al fatto di essere una applicazione a 32bit per Windows, il nuovo tool ha la possibilità di modificare la lunghezza dei campi di configurazione e il loro offset, in modo da poter essere utilizzato per versioni successive del Dark oppure per configurare direttamente pacchetti già preparati che contengono un Dark. Tanto per fare un esempio supponiamo di aver creato qualcosa del genere:

NOTEPAD.EXE +	DARKFTP.EXE +	PAYLOAD.EXE =	TOY.EXE
57344 bytes +	451584 bytes +	18476 bytes =	527404 bytes

Volendo configurare il file TOY.EXE direttamente, usando il tool del Dark, è sufficiente impostare tutti gli offset presenti nella griglia "Field Offsets" al loro valore originale più la dimensione di NOTEPAD.EXE. In questo modo il tool modificherà i valori di configurazione direttamente nell'eseguibile TOY.EXE puntando i campi agli offsets che gli abbiamo indicato.
I campi di configurazione sono gli stessi delle versioni precedenti, solo che sono cambiate le loro lunghezze.
In alternativa al tool è possibile usare un editor esadecimale, e modificare l'eseguibile agli offsets che si possono ricavare dal tool. Nell'eseguibile originale ogni campo della configurazione è rappresentato da una quantità di asterischi pari alla sua lunghezza. E' sufficiente sostituire agli asterischi un contenuto arbitrario, lasciandone eventualmente in sostituzione di bytes non utilizzati che verranno interpretati come spazi vuoti.

4. Utilizzo

Per usare il Dark sono necessari un client FTP e un client IRC. Naturalmente nessuno è obbligato ad usare un client se predilige il Telnet. Si tratta solo di comodità... Dopo aver preparato il "pacco regalo" e averlo consegnato al nostro migliore amico, non ci resta che collegarci ad IRC col nostro client e aspettare. A proposito del client, il migliore per Windows (e quello con il quale è stato provato il Dark) è il mIRC, mentre per Linux vanno più o meno tutti bene, dal KVirc al BitchX, a patto che si utilizzino fonts "fixed". Alcune cose inviate dal Dark, come ad esempio l'help, sono tabelle che diventano difficilmente leggibili se non si usano fonts dai caratteri larghi tutti uguali. Detto questo, il nostro migliore amico vuole leggere la posta e si collega ad Internet. Qualche secondo dopo che è avvenuta la connessione lo vedremo comparire nel canale IRC che abbiamo scelto nella configurazione sotto forma di un nick nella maggior parte dei casi, generato in random. A questo punto cosa possiamo fare? Beh, la risposta è abbastanza semplice: tutto. La cosa più logica è digitare /DNS nickname nel client IRC e copiare lindirizzo IP così ottenuto nel client FTP, aggiungere USERNAME e PASSWORD, qualora siano stati impostati nella configurazione, e premere connect. Ecco che abbiamo sottomano tutti i drives del suo PC.

Possiamo fare qualsiasi cosa con i files e le cartelle tenendo conto di qualche semplice regola di base di Windows (come ad esempio il fatto che non si possono cancellare i files in uso, quindi scordatevi di cancellare C:\WINDOWS anche se la tentazione è forte). Non fate i lamer….
In congiunzione con l'FTP possiamo inoltre impartire comandi tramite una chat in privato con il DarkFTP del nostro amico. I comandi devono essere impartiti nella forma:

USERNAME:PASSWORD NomeComando Parametro1 Parametro2

Qualora l'username sia "anonymous" (come di default), non è necessario specificare il segmento "username:password" e si può impartire direttamente il comando. I comandi disponibili sono riassunti in questa tabella e sono anche disponibili on-line digitando come comando "helpme".

CHUP usr:pwd	Cambia username e password con quelli specificati
CHFTPPORT port	Cambia la porta sulla quale l'FTP starà in ascolto.*
CHUSEIRC [Y/N]	Attiva o disattiva il sistema di notifica/comandi IRC.*
CHCHAN chan	Cambia il canale o i canali sui quali risiedere.*
CHIRCSRV srv	Cambia il server IRC da usare per accedere ai canali.*
CHIRCPORT port	Cambia la porta del server IRC.*
CHMAXUSER maxusr	Cambia il numero di clients FTP ammessi contemporaneamente.
DESTROY	Distrugge il trojan.
SHUTDOWN	Disattiva il trojan fino al riavvio di Windows
RESTART	Riavvia il trojan implementando CLOSEALL
CLOSEALL	Disconnette tutti gli utenti connessi al server FTP
FTPRESTART	Riavvia il server FTP implementando CLOSEALL
DRIVES	Restituisce la lista dei drives rilevati sull'host
GEOMETRY drv	Restituisce la geometria del drive specificato
ABOUTYOU	Fornisce alcune informazioni sul trojan
VIEWCFG	Visualizza la configurazione corrente
SWAPEXE path	Termina il trojan e avvia l'applicazione specificata nel path. Si usa per aggiornare il Dark.
EXEC path	Esegue l'applicazione specificata nel percorso
FIND file path	Cerca "file" nel percorso "path". Si può continuare ad impartire comandi anche durante la ricerca.
STOPFIND	Interrompe il processo di ricerca. Può essere lanciato solo da chi ha avviato il processo di ricerca. Può essere eseguito un solo processo di ricerca alla volta.
CLIENTSIP	Mostra una lista degli IP dei clients connessi all'FTP server
HELPME	Mostra l'elenco dei comandi

*Necessita riavvio del trojan

5. Compressione dell'eseguibile

Come già accennato, in questa nuova versione del Dark la configurazione è interna all'eseguibile. Questo comporta degli svantaggi e dei vantaggi. Lo svantaggio più grande sta nel fatto che se prima era sufficiente "appendere" alla fine del file una stringa opportunamente codificata per avere una configurazione, adesso è necessario modificare manualmente dei segmenti di codice dell'eseguibile tramite un editor esadecimale; il problema tuttavia è stato risolto con il nuovo tool di configurazione che automatizza questa procedura per chi non va troppo d'accordo con l'esadecimale. Il più grosso vantaggio sta invece nel fatto che una volta configurato un eseguibile ci si può fare tutto quello che si vuole: lo si può comprimere, attaccare in cima ad un altro eseguibile, inserire in mezzo a due segmenti, infettarlo con un virus, ecc. senza doversi preoccupare se la configurazione verrà ancora letta o sarà danneggiata. La configurazione, in questa forma, non potrà mai essere alterata se non assieme al codice perché è come se fosse stata scritta al momento della compilazione. Quindi qualora si volesse comprimere l'eseguibile configurato lo si potrà fare tranquillamente. Inutile dire che, a differenza delle versioni precedenti, non si può configurare un eseguibile già compresso.

6. Autoinstall

Il DarkFTP è dotato di un sistema di autoinstallazione. In pratica avviandolo da una directory differente da quella \WINDOWS\SYSTEM automaticamente creerà una copia di se stesso proprio in questo percorso, creerà una chiave nel registro di sistema che lo avvierà assieme a Windows, si autoterminerà e lancerà la copia di se stesso appena effettuata. Ciò significa che se si posiziona l'eseguibile direttamente all'interno di \WINDOWS\SYSTEM e lo si esegue non verrà creata la chiave nel registro e non verrà effettuata alcuna copia. Quindi molto probabilmente il trojan non partirà al riavvio di Windows.

7. Outro

Ho concepito questo trojan solo per divertirmi e fare un po' di giochetti col Delphi (tra l'altro a parer mio una delle migliori suite di programmazione mai realizzate, superiore a molte altre talvolta fin troppo osannate); ho distribuito il codice sorgente per dare la possibilità di imparare a programmare in Delphi a chi ne ha voglia, e non voglio che DarkFTP diventi il solito trojan-commerciale-perfetto-per-i-lamers. Chi lo vuole usare cerchi almeno di porsi la domanda "Ma come accidenti funziona!?" e si autosuggerisca "Quasi quasi leggo il codice….". Vedrete che non ci vorrà molto prima che capiate come funziona e ci vorrà ancora meno prima che vi venga la voglia di farne uno tutto vostro. Questo non è uno strumento da "acher", questo è uno strumento per newbies che hanno voglia di imparare.

7. Thanks/Kicks

Many thanks goes to:
StoLenByte (docs), Francois Piette (vcl), Sinus (logo), Metallica (moral support), Opium, Ginny, Vale ;), Made, Sdra, Rosella V, Yuza and many others for the betatesting ;)

Great kick in the ass goes to:
Silvio Berlusconi (suxsuxsux), Microsoft (repeat sux until 1>2) , Cyberbob (yet another stupid lamah) and many many many many others…
