SPB :: Botnet Documentazione Ufficiale

Funzionalità e utilizzo dell'applicazione

In questo testo sarà descritto il funzionamento del software a livello applicativo di "SPB :: Botnet" , saranno spiegati e illustrati tutti i passaggi per il corretto utilizzo del programma. Ricordo inoltre che il creatore di tale software ,nonché sottoscrivente, si solleva dall'assunzione delle responsabilità di carattere legale o illegale per l'utilizzo di suddetto programma da parte di altri utenti .

[1.1][Requisiti]

Questo software è stato progettato e ideato come un centro di comando e controllo per client multipli , nel dettaglio il programma controlla uno spyware da remoto che può essere installato su più macchine . D'ora in avanti denomineremo come applicazione lato "Server" il centro di comando e controllo ,e come "Client" il computer infettato dallo spyware "SPB" .

Nome completo del programma : SPB :: Botnet

Linguaggio di programmazione utilizzato : Python 2.7

Architettura di programmazione : x64

Ultima versione con annessa documentazione rilasciata : 0.1**

Compatibilità : Windows

Ambiente di sviluppo : Windows 10 x64

Ambiente bersaglio : Windows x64

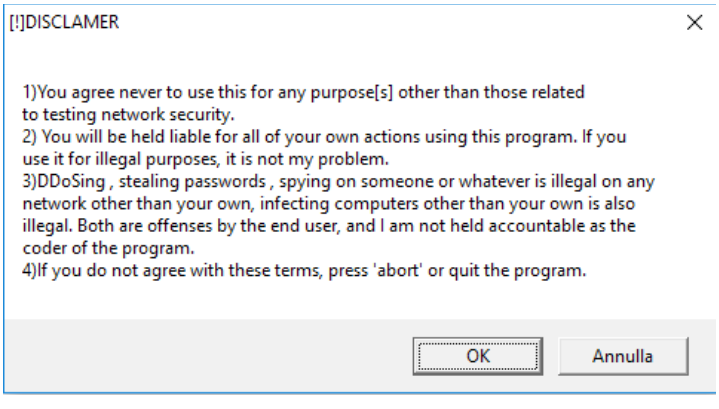
(**)Tutti gli aspetti affrontati ed elencati di seguito , circa la programmazione e il funzionamento fanno riferimento alla versione attualmente riportata su questa documentazione alla voce :

"Ultima versione con annessa documentazione rilasciata : <versione>"

[1.2][Architettura e Design]

L'applicazione è stata ideata per essere un software indipendente , senza integrazione con altri programmi o con pannelli di controllo web o di altra natura . Realizzata con un'interfaccia grafica relativamente semplice, l'applicazione offre molteplici soluzioni per un controllo pressoché totale dei Client. Di seguito vedremo l'analisi approfondita del software in tutti i suoi aspetti.

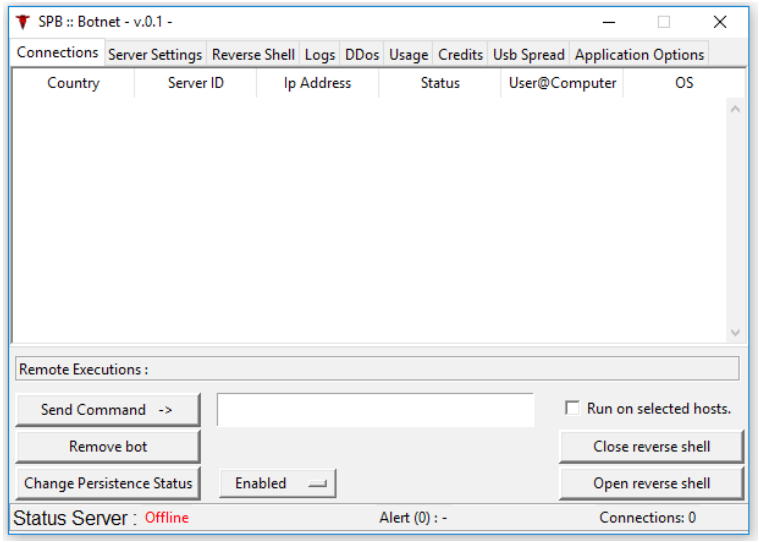
[Immagine 1.1] Avvio del Server



Come prima cosa che viene resa nota all'utente dopo aver lanciato l'applicazione è lo scarico delle responsabilità da parte dell'autore . Se l'utente accetta le condizioni

("OK") sarà autorizzato ad utilizzare l'applicativo , in caso contrario ("Annulla") il programma si terminerà automaticamente .

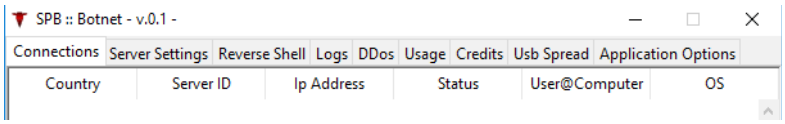
[Immagine 1.2] Pagina principale del Server



L'immagine 1.2 mostra la pagina iniziale del Server , il vero e proprio cuore del programma . Il software viene subito suddiviso in due grandi categorie per facilitare l'orientamento e l'utilizzo all'utente , per facilità saranno definite come :

- Parte superiore
- Parte inferiore

[Immagine 1.3] Parte superiore dell'applicazione



La parte superiore è composta da 9 pagine che suddividono il programma, per una migliore consultazione e funzionamento.

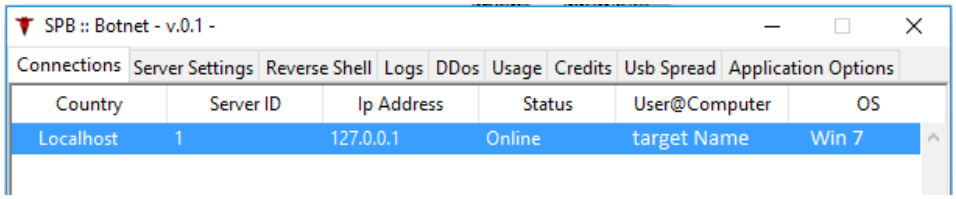
1. Connections
2. Server Settings
3. Reverse Shell
4. Logs
5. Ddos
6. Usage
7. Credits
8. Usb Spread
9. Application Options

Il funzionamento di ciascuna pagina sarà affrontato in seguito.

Subito sotto al menù delle pagine , sempre nella pagina iniziale , troviamo una tabella che raccoglie 6 informazioni identificative per ciascun Client connesso :

1. **Country** : Una volta stabilità la connessione con il bot , il programma identifica la posizione del paese di provenienza .
2. **Server ID** : Variabile assegnata dinamicamente dal Server utilizzata per gestire le operazioni sulla tabella.
3. **Ip Address** : Indirizzo Ip esterno del bot connesso alla rete .
4. **Status** : Il Server è programmato per mostrare se il dispositivo è raggiungibile dalla rete oppure se è semplicemente in funzione ; in ogni caso se il Client non sarà raggiungibile sarà automaticamente rimosso dall'albero . Se il Server non lo rimuoverà , sarà quindi mostrata la scritta "Offline" , in caso contrario il bot sarà pienamente funzionante quindi "Online".
5. **User@Computer** : Questo identifica il nome del computer bersaglio.
6. **OS** : Mostrerà il sistema operativo installato sul Client , nel caso in cui le versioni di Windows siano superiori al "2008 Server" , il programma stamperà "Win 8-10" , ergo "Windows 8" oppure "Windows 10" , nulla toglie che il sistema bersaglio possa essere "Windows 2012" o variante .

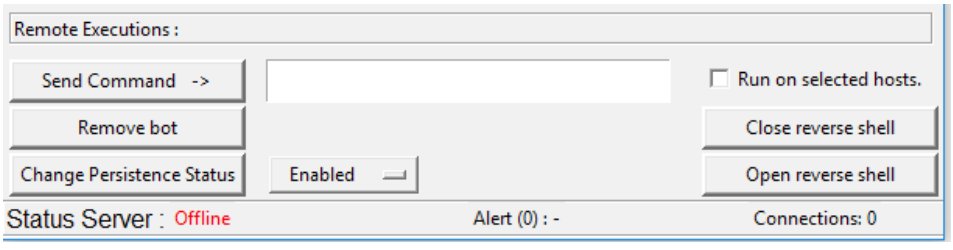
[Immagine 1.4] Un Client connesso con le relative informazioni



Nell'Immagine 1.4 una semplice dimostrazione di connessione da parte di un Client.

Osservando ora la "Parte Inferiore" del Server , Immagine 1.5 , osserviamo una particolare sezione denominata come "Remote Executions" .

[Immagine 1.5] "Parte Inferiore" del Server



In questa sezione sono raccolti tutti i comandi che possono essere trasmessi a Client multipli . Di seguito le spiegazioni.

- **Send Command →** : Basta inserire un comando nella casella di testo , selezionare sulla tabella (SHIFT + Tasto Sinistro Mouse per selezionare uno per volta , SHIFT + Tasto Sinistro Mouse, seleziona bot di inizio e di fine) i Client a cui si vuole inoltrare il

comando , e premere il suddetto pulsante . Se il comando sarà eseguito correttamente , in basso in centro dove vi è la scritta “Alert” , sarà segnata una notifica di avvenuta esecuzione , in caso contrario sarà ugualmente notificato il fallimento.

- **Remove bot** : Nel caso in cui si voglia rimuovere lo spyware da uno dei Client e quindi rimuoverlo permanentemente dalla Botnet , basta selezionare il Client sulla tabella (SHIFT + Tasto Sinistro Mouse per selezionare uno per volta , SHIFT + Tasto Sinistro Mouse, seleziona bot di inizio e di fine) e cliccare sul tasto suddetto . Una volta fatto ,la riga del bot selezionato sarà rimossa e lo spyware sul computer vittima si rimuoverà completamente .
- **Change Persistence Status** : La persistenza è una funzione aggiunta allo spyware che gli consente di essere avviato ad ogni riavvio del sistema vittima . In sintesi la backdoor crea un registro di sistema che punta all’eseguibile , in modo che ad ogni avvio di Windows , il programma , resterà sempre attivo , garantendo l’accesso remoto al Server. Questa funzione è abilitata di base sullo spyware , naturalmente la si può modificare selezionando la riga del Client , selezionando sul menù a tendina vicino al suddetto tasto se mantenerla “Enabled” o rimuoverla “Disabled” a quel punto cliccare su “Change Persistence Status” e la modifica sul Client avrà effetto immediato , rimuovendo o aggiungendo la relativa chiave di sistema .
- **Close Reverse Shell** , **Open Reverse Shell** : SPB :: Botnet offre la possibilità di agire più specificatamente sul controllo remoto di un Client , selezionando il bot desiderato e cliccando su “Open Reverse Shell” il programma darà un secondo accesso all’utente remoto attraverso il quale, potrà ricevere l’output dei comandi via console direttamente sull’applicativo , sotto la pagina “Reverse Shell” . (**) Per terminare la connessione secondaria con il Client basterà selezionare il bot e premere su “Close Reverse Shell” .

  (**)Il funzionamento della Reverse Shell sarà spiegato in seguito.

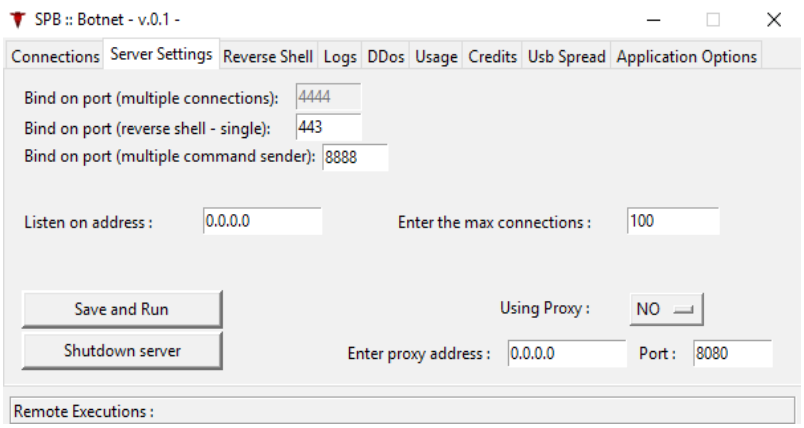
- **Status Bar , footer** : La status bar mostra tre messaggi fondamentali :
  - Status del server , può essere Offline se la connessione è assente e/o i socket sono arrestati e Online invece se è tutto funzionante.
  - Alert (<numero>) , fornisce informazioni sulla corretta esecuzione dei programmi sopra elencati o sulla mancata esecuzione .
  - Connections <numero> : mostra a video tutte le connessioni attive al momento , quindi il numero di Bot disponibili .

[1.3][Analisi delle funzioni]

In questa sezione si andrà ad analizzare le soluzioni che offrono le altre pagine dell’applicativo . Si inizia dalla pagina : “Server Settings” , procedendo verso sinistra .

[1.3.1][Server Settings]

[Immagine 1.6] "Server Settings" Page



In questa pagina vengono offerte le personalizzazioni del Server C&C per quanto riguarda : porte , indirizzo ip e proxy .

1. Bind on port (multiple connections) : Questa porta non è modificabile in quanto vi sono funzioni a livello di codice basate sul servizio offerto solo sulla porta 4444 .
2. Bind on port (reverse shell – single) : Questa porta configura la connessione della Reverse Shell con ogni bot , modificabile .
3. Bind on port (multiple command sender) : Questa porta configura l'invio dei comandi multipli , modificabile .
4. Listen on address : Qui si può inserire l'indirizzo ip su cui il Server deve ascoltare per le connessioni . Solitamente 0.0.0.0 ascolta su tutti gli indirizzi ip della macchina :
    - 192.168.x.x : Lan IP
    - 127.0.0.1 : Localhost
    - IPV6

   E' consigliato impostare o 0.0.0.0 oppure l'ip della Lan .
5. Enter the max of connections : Questa voce gestisce il numero massimo di connessioni che il Server deve aspettarsi di ricevere . E' bene modificarla in base al numero di bot che dovranno connettersi.
6. Using Proxy : Questo menù a tendina offre la possibilità di attivare l'opzione di proxy . Selezionando "YES" bisognerà necessariamente inserire di seguito l'indirizzo ip e la porta su cui connettersi al Proxy . Nel caso in cui si selezioni "NO" (default) la connessione ai bots sarà diretta (**)

(**) Azione sconsigliata per fini malevoli in quanto la connessione potrebbe essere rintracciabile .

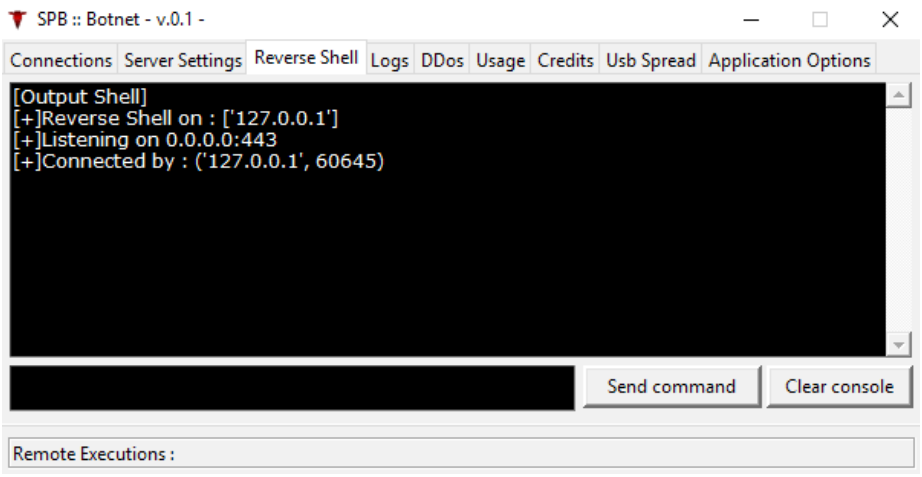
- **Save and Run** : Una volta settati i parametri di configurazione si clicca sul suddetto pulsante . Se i parametri saranno accettati dal server si sentiranno due suoni acuti

ripetuti e lo status del server (in basso a sinistra) , cambierà da "Offline" a "Online". Attivando le funzionalità del server il servizio si porrà in ascolto di connessioni.

- **Shutdown Server** : Questo pulsante arresta istantaneamente i servizi del Server , chiudendo tutte le connessioni attive , reimpostando il server in modalità "Offline".

[1.3.2][Reverse Shell]

[Immagine 1.6] Reverse Shell in azione



Dopo aver premuto il tasto "Open Reverse Shell" , sulla pagina "Reverse Shell" otterremo ,se la connessione sarà stabile , una shell vera e propria con alcune funzioni estese .

Le funzionalità offerte da questa variante del "Meterpreter" sono le seguenti :

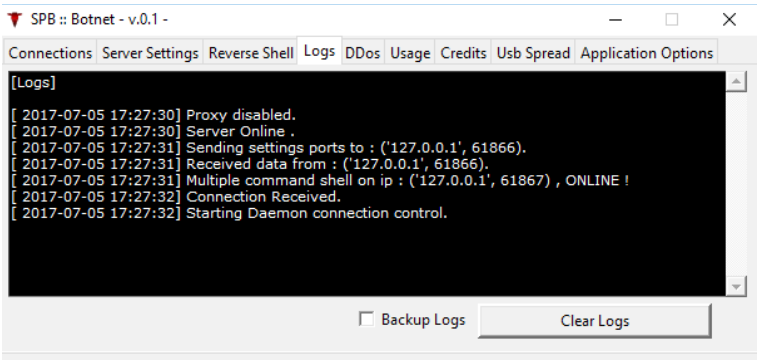
- chrome_to_file : Se la vittima ha installato il web browser Chrome , questa funzione estrae le password memorizzate dal browser e le mostra a video al Server .
- webcam : Questa funzione avvia una live stream sfruttando la webcam del Client , se ne ha una . (Se il Client ha una webcam "nuovo modello" questa funzione attiverà la luce di notifica dell'utilizzo della webcam). **La libreria utilizzata per la creazione del webcam stream è instabile quindi l'avvio della funzione potrebbe causare un crash del Server** .
- keylogger <start> <stop> <show> :
  - start : Questa funzione intercetta la finestra e i tasti premuti , salvandoli in memoria.
  - stop : Smette di intercettare .
  - show : Mostra a video , nella finestra "Reverse Shell" del Server , i dati salvati .

[Immagine 1.7] Webcam Stream in azione (nella dimostrazione l'immagine è oscurata)

Per usufruire di queste funzioni basta digitare i comandi sopra elencati nella finestra "Reverse Shell" come comando e inviarlo .

[1.3.3][Logs]

[Immagine 1.8] Cronologia dei Logs



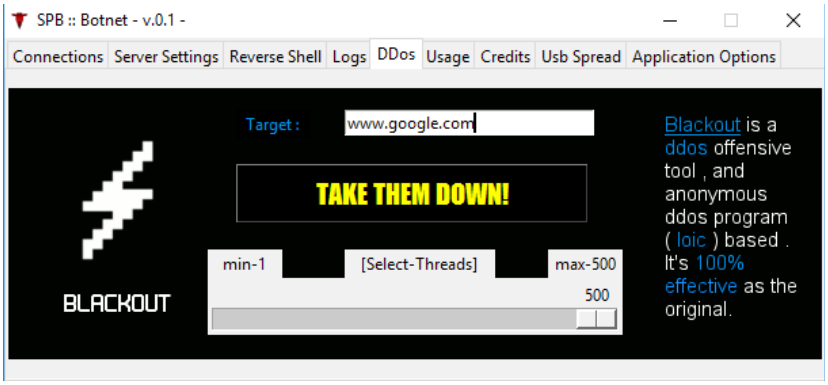
Nella sezione "Logs" , verrà riportata ogni azione effettuata con relativa ora e data . In questa pagina si possono effettuare due sole azioni :

1. **Clear Logs** : La cronologia dei Logs sarà svuotata.
2. **Backup Logs** : Se spuntata , questa casella , attiverà ogni 2 minuti il salvataggio della cronologia attuale dei Logs su un file di testo . Tale file sarà salvato nella cartella dove è s tato lanciato il Server

.

[1.3.4][DDos]

[Immagine 1.9] Main page del tool "Blackout"



"Blackout" è uno script integrato nell'applicativo che si occupa di gestire un potente attacco DDOS . Questo tool è stato creato come replica del noto programma "LOIC" (Low Orbit Ion Cannon) realizzato dagli "Anonymous" per lanciare attacchi a grande efficacia contro i vari domini bersaglio . Il funzionamento di "Blackout" è relativamente semplice .

- Una volta digitato il dominio o l'indirizzo ip da attaccare , bisogna impostare il numero di Thread . La logica consiste in :

  + Thread = + Ddos

  Bisogna tenere contro che su macchine con una bassa capacità di elaborazione , utilizzare 500 Thread (Max) potrebbe comportare la caduta della connessione , in quanto si manderebbe in overload il processore del pc bersaglio .

Lo script invierà il comando a tutti i Client Online al momento e in base ai Thread selezionati , l'attacco Ddos sarà lanciato .

- Per lanciare l'attacco basta cliccare su "TAKE THEM DOWN!".

[1.3.5][Usage]

La pagina "Usage" contiene un riassunto dell'intero file di documentazione in lingua inglese per favorire la consultazione universale .

[1.3.6][Credits]

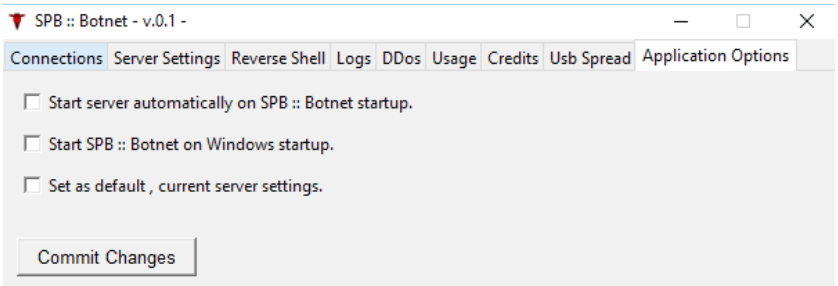
La pagina "Crediti" contiene i riconoscimenti dei creatori dell'intero software.

[1.3.7][Usb Spread]

Lo spyware è stato programmato per infettare tutti i dispositivi connessi alla macchina bersaglio , ogni volta che il virus si replica su una chiavetta USB , sarà notificato in questa sezione "Usb Spread" il percorso e l'indirizzo ip su cui è avvenuta l'infezione .

[1.3.8][Application Options]

[Immagine 2.0] Application Options Page



In questa sezione vi saranno 3 opzioni disponibili

- Start server automatically on SPB :: Botnet startup : Se selezionata questa voce avvierà il Server non appena l'applicazione sarà lanciata.
- Start SPB :: Botnet on Windows startup : Se selezionata questa voce installerà una key nel registro di sistema dell'utente in modo da avviare l'applicazione ad ogni riavvio .
- Set as default , current server settings : Se selezionata , salverà su un file .txt i settaggi correnti relativi alla pagina "Server Settings" così una volta lanciata di nuovo l'applicazione , i settaggi saranno caricati automaticamente .

Una volta selezionate le relative opzioni , cliccare su "Commit Changes" per salvare i settaggi correnti .

[1.4][File e Risorse]

L'applicazione necessita di 4 file che vengono creati in automaticamente all'avvio se mancanti .

- Immagini
  - icon.ico = icona che l'eseguibile utilizzerà .
  - Asteroid.gif = il background della pagina "Ddos".
- File di configurazione
  - config.txt = sarà utilizzato per memorizzare le impostazioni della pagina "Server Settings"
  - Tree-data.txt = sarà utilizzato come database per memorizzare i bot online e offline.

Per un corretto utilizzo dell'applicativo è necessario lasciare questi file nella cartella dell'eseguibile .

[1.5][Crediti]

Questo software e relativa documentazione sono state scritte e testate da Spaceb4r .

La versione corrente del software viene rilasciata come file eseguibile (x64) con relativa documentazione annessa per il sito brigaterozze.club . Non distribuire questo software in quanto proprietà individuale e privata della crew di brigaterozze.club.

Se dovessero presentarsi : errori , crash , arresti o quant altro li si può notificare all'email seguente e l'autore provvederà al fix.

Per qualsiasi informazione mandare una mail a : 111000spacebar000111@gmail.com