

<MaRCo> abbiamo parlato dei cloni
<MaRCo> dei cloni che mette a disposizione il venom, in particolare gli assault bot
<MaRCo> abbiamo detto come caricarli
<MaRCo> e soprattutto come connetterli
<MaRCo> abbiamo dato i seguenti server irc su cui provarli
<MaRCo> riepilogo server di esempio per i cloni: sg.ircgate.net, clamm.ircgate.net, battle.ircgate.net, webberia.ircgate.net, omni.ircgate.net, csn.ircgate.net, magic.ircgate.net, legend.ircgate.net
<MaRCo> abbiamo spiegato come utilizzare la console che comanda tutti i nostri cloni
<MaRCo> a questo punto però vanno fatte delle importanti precisazioni
<MaRCo> che riguardano il mass flood ad un utente
<MaRCo> prima di farlo è bene riuscire a reperire alcune informazioni base sulla vittima
<MaRCo> vale a dire cosa sta usando per chattare su irc
<MaRCo> ora faccio una premessa
<MaRCo> i flood che trovate nella console
<AlexMalex> ricordo dove trovate la console che controlla i cloni : dal menù Siege Of Darkness - Assault BOT - Max Control Console
<MaRCo> sono flood da ctcp
<MaRCo> quindi sono flood di ping, version, finger, ecc.
<MaRCo> questi hanno come effetto quello di sconnettere la vittima dal server irc a cui è connessa per questa causa: excess flood
<MaRCo> un utente esce per excess flood quando in pratica effettua un flood, ovvero continua ripetere la stessa cosa più volte
<MaRCo> il server irc come protezione lo fa uscire
<MaRCo> con questa causa, appunto... excess flood
<AlexMalex> Per chi non lo sapesse :
<AlexMalex> un PING è un comando che viene usato per sapere se un utente è connesso
<AlexMalex> Se faccio un PING a UTENTE, UTENTE mi risponderà con un PONG e saprò che è connesso
<AlexMalex> Il VERSION invece è un comando che chiede al client IRC dell'utente il nome e la versione del client stesso
<AlexMalex> Se faccio un VERSION a UTENTE, UTENTE mi risponderà con "mIRC 5.2..." o altri script per mIRC (le java chat in genere non conoscono questo comando e non rispondono nulla)
<AlexMalex> Questi comandi sono "benefici" ma con i cloni si possono usare per scopi più "cattivi"
<MaRCo> tutti quei flood hanno effetto perchè si parte dal presupposto che se io invio un FINGER, un PING, ecc, e se la vittima usa un client IRC per chattare, questo risponderà ai seguenti comandi
<MaRCo> gli mando un ping, risponde dicendomi il lag
<AlexMalex> Il termine "LAG" indica il ritardo di risposta di un utente
<AlexMalex> Se faccio PING a UTENTE e UTENTE mi risponde PONG dopo 2 secondi si dice che UTENTE ha 2 secondi di lag (è laggato)
<MaRCo> è chiaro quindi che se noi ne mandiamo tantissimi di questi ping, version, finger, ecc
<MaRCo> il client irc della vittima tenterà di rispondere ad ognuno di questi
<MaRCo> ed essendo moltissimi quelli che inviamo
<MaRCo> le sue risposte verranno interpretate dal server irc come un flood e l'utente verrà disconnesso per excess flood
<MaRCo> quindi è come se fosse lui a floodare :)
<AlexMalex> La vittima presa per colpevole :-)
<AlexMalex> Supponendo di usare 12 cloni, se noi inviamo 10 PING da ogni clone a una sola persona, i nostri cloni non verranno disconnessi per excess flood perchè hanno inviato solamente 10 comandi
<AlexMalex> lo script della sfortunata persona invece dovrà rispondere 120 PONG (10 per ogni clone)
<AlexMalex> di conseguenza sarà disconnessa per excess flood
<MaRCo> premesso questa cosa
<MaRCo> c'è da fare quindi una grossa distinzione
<MaRCo> 1) la vittima usa un client irc (es.: mirc o un mirc script)
<MaRCo> 2) la vittima usa una javachat (tipo quella del nostro sito o tante altre in circolazione)

<MaRCo> detto questo approfondiamo i 2 casi
<MaRCo> 1) se usa un client IRC
<MaRCo> possiamo tranquillamente utilizzare i flood di cui parlavamo prima, quindi il mass ping, il mass finger, ecc. Questo perchè essendo un client irc risponderà a questi comandi e si disconetterà per excess flood
<AlexMalex> Ovviamente moltissimi script sono programmati per proteggersi da questo tipo di "attacco" e dopo un certo numero di PING ricevuti da un utente (tipicamente 3) ignorano il nick che li invia
<AlexMalex> E' perciò consigliabile fare un VERSION prima di un max ping flood a una persona per capire che script usa
<MaRCo> uno di questi script che ha queste potezioni è lo stesso Venom Script poi ne troviamo altri tipo promirc
<MaRCo> nel caso in cui vediamo che lo script è uno di quelli che ha le protezioni del caso (ci vuole un po' di esperienza per sapere quali sono, cioè bisogna conoscerli), non ci resta che utilizzare altri tipi di flood
<MaRCo> quello ad esempio del messaggio ripetuto da tutti i cloni
<MaRCo> al limite possiamo tentare un max dcc chat flood
<MaRCo> però esistono le protezioni anche su questo; purtroppo molti script garantiscono buone protezioni
<MaRCo> purtroppo per noi, ovviamente... :-)
<AlexMalex> ovviamente :-))
<MaRCo> però se vediamo che la vittima ad esempio usa un mirc puro e semplice
<MaRCo> con i nostri mass flood cadrà facilmente soprattutto poi se non sa come ignorare il nostro ip/host
<MaRCo> 2) se la vittima usa una javachat
<MaRCo> in tal caso mandargli ad esempio un flood di ping non ha molto senso visto che la vittima non risponderà
<MaRCo> però c'è da dire che ci sono diversi tipi di javachat
<MaRCo> se questa è tipo quella del sito di alex
<MaRCo> mandandogli una query vi si apre una finestra privata in tal caso l'unico flood fastidioso è quello del messaggio privato (ripetuto magari più volte) da parte di tutti i cloni
<AlexMalex> (dato che il canale ufficiale dei LunaPop usa la stessa java chat, consiglio di usarlo per questi tipi di flood perchè il 90% degli utenti è in queste condizioni) :-)
<MaRCo> il danno consiste nel fare aprire tante finestre private
<MaRCo> che nelle finestre ci sia un solo carattere oppure migliaia, il danno non cambia
<MaRCo> quindi inutile fare il text blast
<AlexMalex> Per chi non lo sapesse il max text blast è un normale text flood dove il testo del messaggio è costituito da tantissimi caratteri incomprensibili e ogni clone invia 10 di questi messaggi
<MaRCo> quindi nel caso la javachat sia come quella del sito di alex, il nostro consiglio è di floodare con il mass comando (ex: /msg nickvittima :-P)
<AlexMalex> come spiegato nella scorsa "lezione"
<MaRCo> se invece la javachat è meno bella cioè meno sofisticata
<MaRCo> e quindi i nostri messaggi privati non provocano un apertura di una finestrella a parte ma vengono visti dall'utente nella stessa finestrella il danno più grande che possiamo fargli è quello appunto di riempirgli lo schermo :))
<MaRCo> quindi in questo caso vivamente consigliato, è il MASS TEXT BLAST
<AlexMalex> :-))
<MaRCo> con questo, oltre al fastidio visivo che gli procuriamo molto probabilmente la javachat non reggerà e la vittima cadrà
<AlexMalex> molto ma molto probabilmente
<AlexMalex> dipenderà anche dal tipo di connessione che ha la vittima
<MaRCo> (es. cadrà per connection reset by peer)
<MaRCo> poi il messaggio può variare a seconda del server irc, comunque cadè come se fosse stata vittima di un nuke
<AlexMalex> con il max text blast con probabilità alcuni dei vostri cloni saranno disconnessi per excess flood ma si riconnetteranno automaticamente
<MaRCo> questo perchè come abbiamo detto all'inizio, siccome i cloni invieranno molte volte la stessa stringa alla vittima, il server irc li sconnetterà per excess flood
<AlexMalex> I cloni avete imparato ieri a connetterli
<AlexMalex> e a fare un tipo di flood
<AlexMalex> nel paragrafo dedicato al VENOM Script (sezione mlRC)
<AlexMalex> Quindi una volta caricati i cloni li manovrate

<AlexMalex> dalla Max Control Console

<AlexMalex> Trovate tutti i tipi di flood in quella console di comando

<AlexMalex> è inutile che ve li spieghi uno ad uno perchè i pulsanti hanno le stesse descrizioni

<AlexMalex> che abbiamo usato qui per spiegare

<AlexMalex> ULTIMA COSA : usate max ping flood sugli utenti che usano mIRC semplice, è come la manna :-) (cadono dopo 1 secondo per excess flood)

<AlexMalex> OK, via alle domande

<Erma|{> yahooooo

<Red-Vex> come faccio a mandare i flood?

<MaRCo> per madare i flood c'è la console che permette la gestione di tutti i cloni contemporaneamente

<Daemon> cosa significa ping timeout?

<AlexMalex> ping timeout è quando il lag di una persona è troppo elevato e il server IRC non può più aspettare

<AlexMalex> in quel caso il server IRC decide di far uscire la persona perchè la presuppone disconnessa (ogni tanto i server IRC fanno un PING a un utente che non invia bytes da un po' per sapere se è ancora vivo :-)

<Cyran0> non credo di aver ben capito cosa sia un "connection reset by peer"

<Mat_Jack1> mi è capitato reset by peer durante la lezione. è qualcuno che mi sta floodando??

<AlexMalex> No, può capitare anche senza flood o nukes, dipende dallo stato della rete, della connessione, del server IRC ...

<MaVerick> quanti bot occorrono circa x provocare un apertura continuata di finestrelle x fare sclerare il tpo?

<AlexMalex> Il VENOM ne consente 12 e sono sufficienti :-)

<Sauzer> scusate ma il venom seleziona automaticamente le barriere contro gli attacchi es excess flood

<Sauzer> o li devi settare tu?

<editor> ping timeout : ping fuori tempo ovvero il mirc non risponde per tempo alla richiesta del server

<Mat_Jack1> senza ù

<MaRCo> quando uno cade per ping timeout significa che in realtà, da qualche minuto, quello era un ghost

<ferdinand> cioè?

<AlexMalex> ghost = l'utente era già caduto ma era rimasto il suo nick "appeso"

<ferdinand> cosa è un ghost?

<gigi0500> marco cosa intendi con ghost

<MaRCo> a quel nick non era associato un utente

<F|i|Zs> il server si era accorto della sua scomparsa dopo che li ha fatto il ping

<LeNNyD^> se i cloni hanno una mask differente dalla nostra quindi è meno probabile che ci becchino?

<AlexMalex> diciamo che se non cambi la mask ti beccano al 100%

<Erma|{> è possibile rilevare i cloni con il venom?

<AlexMalex> sì, click destro su un utente - controlla canale - cerca cloni