UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

FACOLTA' DI INGEGNERIA

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea di Primo Livello

Analisi Comportamentale di Malware Botnet-Related

Relatore:
Prof. Giuseppe F. Italiano

Candidato:
Lorenzo Paris

Correlatore:
Dott. Giovanni Bottazzi

Anno Accademico
2015/2016

Riassunto

La continua espansione dei dispositivi connessi alla rete Internet, sta portando la comunità di criminali informatici a studiare tecniche sempre più avanzate ed efficienti per l'accesso non autorizzato ai sistemi in questione; per questo motivo, il tema della Sicurezza Informatica diventa un aspetto delicato ed essenziale.

Da un resoconto del 2015, risulta che più del 32% della popolazione mondiale ha involontariamente e inconsciamente installato un Malware all'interno del proprio dispositivo informatico. In particolare, questo lavoro di tesi è rivolto allo studio e all'analisi di una specifica classe di Malware, il cui intento è di costruire una rete di dispositivi infetti (fissi o mobili), il più estesa possibile, controllati da remoto attraverso uno o più Server C&C, ossia di Comando e Controllo. Queste tipologie di reti prendono il nome di *Botnet*.

Una Botnet è quindi una rete di dispositivi infetti controllati da remoto dal cosidetto *Botmaster* utilizzata per una vasta gamma di scopi illegali quali attacchi DDoS, Phishing, Spam, Ransom, etc.

La caratteristica che contraddistingue questo genere di Malware è la loro peculiarità di contattare il rispettivo (anche molti) Server di Comando e Controllo mediante un'elevata periodicità.

Al giorno d'oggi esistono diverse tecniche di analisi per intercettare la cadenza di tali connessioni. La più utilizzata è la Fast Fourier Transform, che si ritiene abbia il difetto di essere alquanto ostica al livello computazionale. Il seguente lavoro di tesi, invece, utilizza una nuova metodologia che permette di ridurre al minimo i requisiti in termini di memoria utilizzata e complessità computazionale.

Al fine di testare la bontà di tale metodo, è stato creato un ambiente virtuale costituito da una serie di client e da un server che funzionerà da gateway per i client stessi.

Inizialmente è stato riprodotto il funzionamento di un Malware mediante due semplici programmi Java. Nel primo test, un client effettua delle richieste HTTP ad

un dominio prestabilito ad intervalli regolari. Nel secondo test, incrementando il livello di complessità, il client effettua le richieste HTTP verso la URL predefinita, utilizzando una periodicità random all'interno di un range fisso.

Al termine dei test, mediante i dati forniti dal Server, viene analizzato il comportamento del client attraverso tutta una serie di calcoli appartenenti al metodo proposto. I risultati delle analisi sembrano di fatto portare alla luce il valore esatto della periodicità delle connessioni precedentemente stabilito a livello di codice.

Successivamente viene studiato ed analizzato, mediante il metodo medesimo, il comportamento periodico di 3 Malware reali:

1. **DriveDDoS**: risultato il più attivo dei tre, ha come modus operandi quello di eseguire attacchi di tipo DDoS;
2. **Andromeda**: avendo al suo interno un sistema anti-Virtual-Machine, è risultato il più sofisticato tra quelli analizzati;
3. **NjRAT**: è un Remote Administration Tool, ossia fornisce tutti gli strumenti necessari per avere il controllo totale della macchina infettata.

La periodicità con la quale avvengono le connessioni tra macchina infetta e Server di Comando e Controllo, è un fattore di estrema importanza ai fini della scalabilità del Malware stesso. Questa peculiarità è stata infatti confermata ed analizzata per tutti i Malware presentati in questo lavoro di Tesi. In particolare, il metodo utilizzato si è dimostrato essere particolarmente affidabile e molto semplice al livello computazionale.

A causa dell'elevato tasso di crescita dei dispositivi informatici connessi alla rete Internet, diventano sempre più importanti le misure di protezione offerte dagli esperti della Cyber Security. Questo metodo, ancora in fase di sperimentazione, potrebbe quindi rientrare all'interno della vasta gamma di strumenti utilizzati per l'analisi passiva del traffico generato da un software malevolo.