Matteo Bracci #505239 Progetto gestione di Rete Starcraft 2 Dissector

Introduzione

Motivazioni

Durante il corso e' stato mostrato come, persino in una situazione in cui apparentemente nulla che coinvolga l'interfaccia di rete di un PC stia accadendo, in realta' i data flow "nascosti" verso e provenienti dal mondo esterno possono essere numerosi. Su questa idea e' nato l'interesse verso nDPI.

Starcraft II

Dovendo scegliere un protocollo/applicazione per la quale scrivere un dissector, la scelta e' stata forse inusuale, ma nondimeno interessante. Starcraft II e' un gioco strategico single/multiplayer pubblicato nel 2010 dalla Blizzard, durante il quale anno ha venduto oltre 3 milioni di copie.
Il servizio online e' gestito da una piattaforma chiamata Battle.net, condivisa da tutti i giochi Blizzard.

Analisi del problema

nDPI

Alla base di nDPI sta il riconoscimenti dei flussi. Ogni volta che un nuovo flusso viene catturato, questo viene passato, secondo una determinata politica, ai *dissectors*, i quali lo analizzano brevemente alla ricerca di una firma. Se uno ritiene di averla trovata, l'analisi del flusso si interrompe e segue il tracciamento e registro della sua attivita'.
Essenzialmente e' parso chiaro fin dall'inizio che il problema sta nel trovare una firma che permetta di minimizzare o, idealmente, rimuovere del tutto.la possibilita' di falsi positivi e negativi. I primi soprattutto sono, probabilmente, i piu' pericolosi, in quanto andrebbero praticamente a rubare traffico ad altri dissectors, compromettendone cosi' l'attivita'.

Starcraft II

L'analisi del traffico dell'applicazione ha fin dall'inizio rivelato che l'attivita' di rete e' molto variegata. Sono presenti download di contenuti statici quali file XML e PNG, ma anche e soprattutto comunicazione real-time client-server durante il gioco o a causa dell'interazione col client di gioco. In questi casi vengono utilizzati protocolli proprietari, dalla struttura privata.
E' importante notare che, nonostante tutti i giochi Blizzard condividano la piattaforma Battle.net, test hanno mostrato che ogni gioco ha il suo protocollo unico e adatto alla situazione. Di conseguenza, il problema di differenziare specificatamente i giochi Blizzard non si pone.

Soluzioni adottate

Contenuti statici (HTTP)

Per il contenuto statico sono usate richieste HTTP esplicite verso diversi host. Dai test effettuati la lista sembra essere facile da riconoscere, poiche' composta da vari sottodominii di `.battle.net` e un server CDN/CMS con hostname `bnetcmsus-a.akamaihd.net`.
Dunque e' stato facile aggiungere questi host alla struttura gia' presente in nDPI, identificando tale contenuto con il nome generico `Battle.net`.

Traffico dinamico (TCP / UDP)

Per il traffico di dati dinamico, invece, il tentativo iniziale e' stato quello di cercare di interpretare il protocollo, almeno in qualche frammento specifico sufficiente all'identificazione del flusso, ma alla fine ci si e' limitati ad ignorare il contenuto semantico inviato e cercare particolari stringhe di byte nei pacchetti inviati che sembrato ricorrenti e caratteristiche.

In particolare, un elemento che ha facilitato molto il procedimento e' il fatto che il flusso da client di gioco a server e viceversa e' uno solo, e' TCP e ha inizio con il login e rimane attivo fino al logout. Similmente, ogni partita corrisponde ad un flusso UDP, e questi nascono e muoiono insieme. Dunque in pratica e' stato sufficiente identificare due sole firme.
Quella del flusso TCP e' una semplice sequenza di 10 bytes, che dai test risulta apparire in ogni tentativo di login.
Quella del flusso UDP invece e' leggermente piu' complessa, ovvero viene controllata la dimensione dei primi 8 pacchetti. Sebbene forse un po' insolito come metodo, dai test sembra comportarsi bene.

In aggiunta al byte matching, si effettuano controlli sull'identita' del server con cui si sta comunicando.
Una piacevole sorpresa e' stato scoprire che Blizzard ha registrato la porta 1119 alla IANA (denominata `bnetgame`) e, apparentemente, nello scambio di dati relativi a client e gioco questa viene sempre utilizzata. Questo e' di aiuto nell'identificazione dei flussi di Starcraft e, soprattutto, nell'evitare di catturare erroneamente altri flussi: sebbene non sia una garanzia certa, e' accettabile assumere che non siano molte le applicazioni ad utilizzare la porta "senza permesso".
Inoltre dai test e' emerso che vengono utilizzati server specifici per il login, uno per regione di gioco (US/EU/Korea/Singapore) piu' uno per il server di beta testing, attualmente attivo e ad accesso limitato. Di conseguenza l'IP dell'altra macchina e' sempre confrontata con questa lista quando si tenta di identificare il flow TCP di login, ottenendo possibilita' di falsi positivi pressoche' nulla. Ovviamente, l'unico inconveniente e' che occorre essere certi che tali indirizzi IP non cambieranno in futuro o, piu' realisticamente, assicurarsi che la lista verra' aggiornata in caso di cambiamenti.