InformaticaUmanistica

UNIVERSITÀ DI PISA

DDoS & World Freedom

Salvatore Ventrone (539872)

Progetto di Laboratorio Progettazione Web
A.A. 2015/16

Sommario

Gli attachi Distributed Denial of Service (DDoS) possono essere utilizzati per rendere non disponibili al mondo importanti informazioni on-line, l'accesso alle informazioni è importantesia per Internet che per la libertà di espressione. Il sito analizza i maggiori attacchi avvenuti nel mondo nell'ultimo biennio (2014 – 2015) e l'indice di libertà del Paese destinazione. Mostra i dati di uno studio quantitativo sulla correlazione tra il numero di attacchi DDoS ricevuti da un paese ed i sui indici di libertà civile e diritti politici.

Introduzione

Raccolta dati DDoS

Sono stati raccolti circa 245000 attacchi DDoS, tra il 2014 e 2015, dal sito web www.digitalattackmap.com, una pagina che permette di visualizzare dati live di attacchi DDoS in tutto il mondo, costruito attraverso una collaborazione tra Google Idee e Arbor Networks. L'applicazione mostra dati anonimi degli attacchi per consentire agli utenti di esplorare le tendenze storiche e cercare le relative news di interruzioni che avvengono in un dato giorno.

DDoS - Distributed Denial of Service

Un attacco Distributed Denial of Service (DDoS) è un tentativo di rendere un servizio online non disponibile, inondandolo con traffico proveniente da più sorgenti. Prendono di mira una vasta gamma di risorse importanti, dalle banche ai siti web di notizie, e rappresentano una grande sfida per assicurare che la gente possa pubblicare ed accedere ad informazioni importanti. Di seguito sono riportati i dettagli sui tipi di attacchi si trovano sul sito:

Attacchi connessione TCP – Occupazione di connessioni

Questi attacchi tentano di utilizzare tutte le connessioni disponibili a dispositivi di infrastruttura, come load-balancer, firewall e server di applicazioni. Anche i dispositivi in grado di mantenere milioni di connessioni possono essere vulnerabili da questo tipo di attacchi.

Attacchi volumetrici – Consumo della bandwidth

Questi attacchi cercano di consumare la banda o tra la rete / servizio di destinazione , o tra la porta di rete / servizio bersaglio ed il resto di Internet. Questi attacchi servono semplicemente a causare congestioni.

Fragmentation Attacks - Flusso di pacchetti

Questi inviano un flusso di frammenti TCP o UDP ad una vittima, travolgendo la capacità della vittima di ricomporre i flussi e riducendo fortemente le prestazioni.

Attacchi ad applicazioni - Applicazioni bersaglio

Questi tentano di sopraffare un aspetto specifico di un'applicazione o di un servizio. Può essere efficace anche con pochissime macchine attaccanti generando un tasso di traffico basso (il che li rende difficili da individuare e mitigare).

Raccolta dati Indici di Libertà

Gli indici di libertà sono stati raccolti dal sito web freedomhouse.org, Freedom in the World è il frutto del report annuale di Freedom House, valuta la condizione dei diritti politici e delle libertà civili in tutto il mondo. Si compone di rating numerici e testi descrittivi di supporto per 195 paesi e 15 territori. Freedom in the World è stato pubblicato dal 1973, permettendo a Freedom House di tenere traccia delle tendenze globali in quanto a libertà per più di 40 anni. E' diventato il rapporto più letto e citato nel suo genere, viene utilizzato regolarmente da politici, giornalisti, accademici, attivisti e molti altri.

Valutazione diritti politici e libertà civili

Ad ogni paese e territorio viene assegnato un punteggio tra 0 e 4 su una serie di 25 indicatori, per un punteggio complessivo massimo di 100. Questi punteggi vengono utilizzati per determinare due valori numerici, uno per i diritti politici e l'altro delle libertà civili, un punteggio di 1 rappresenta le condizioni più libere e 7 le meno libere.

Status: libero, in parte libero, non libero

La media dei rating per i diritti politici e delle libertà civili di un paese o territorio si chiama Freedom Rating, ed è questo punteggio che determina lo stato di libero (1.0 a 2,5), in parte libero (3,0 a 5,0), o non libero (5.5 a 7.0).

Valutazioni di Freedom of the World

Freedom of the World valuta i diritti e le libertà di cui godono gli individui nel mondo reale, piuttosto che valutare i governi o le sue prestazioni di per sé. I diritti politici e le libertà civili possono essere influenzate sia da fattori statali e non, incluso ribelli e altri gruppi armati.

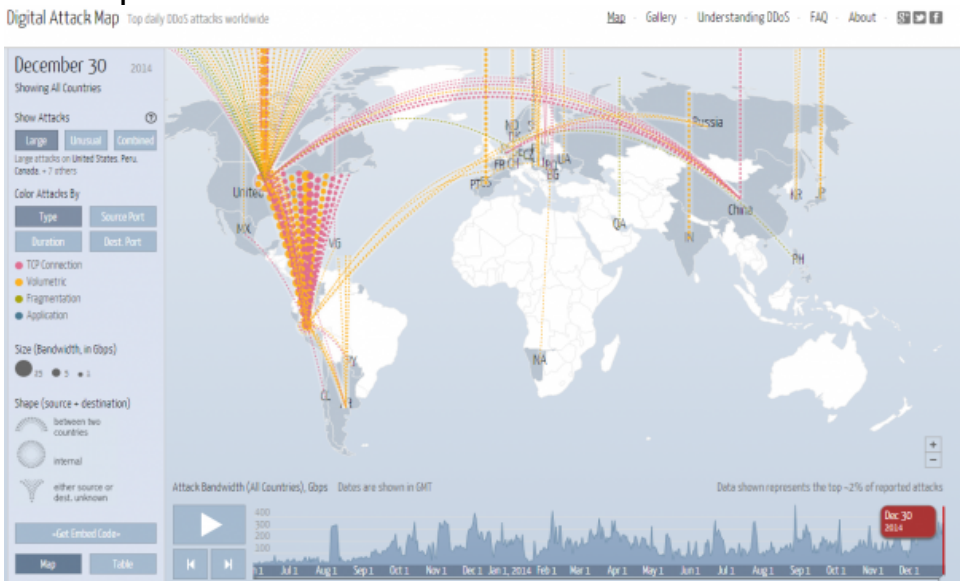
Produzione di Freedom of the World

Analisti valutano i 210 paesi e territori, utilizzando una combinazione di ricerca in loco, consultazioni con i contatti locali, e le informazioni dai giornali, organizzazioni non governative, i governi, e una varietà di altre fonti. Consulenti esperti e specialisti regionali poi riesaminano le conclusioni degli analisti. Il prodotto finale rappresenta il consenso degli analisti, consulenti ed il personale Freedom House.

Lo stato dell’arte

Esistono molti siti internet ed applicazioni web che permettono di visualizzare gli attacchi DDoS in tempo reale, alcuni offrono anche una linea temporale visualizzare gli attacchi precedenti. Per la libertà nel mondo Freedom House è la migliore risorsa. Di seguito vengono riportati i siti web analizzati più importanti:

Digital Attack Map



La mappa è alimentata da dati alimentati da 270 + clienti ISP di tutto il mondo che hanno accettato di condividere le statistiche anonime di traffico di rete e attacchi. Si tratta di un servizio veramente utile perché permette visualizzare i dati dal giorno corrente a ritroso fino a giugno 2013.

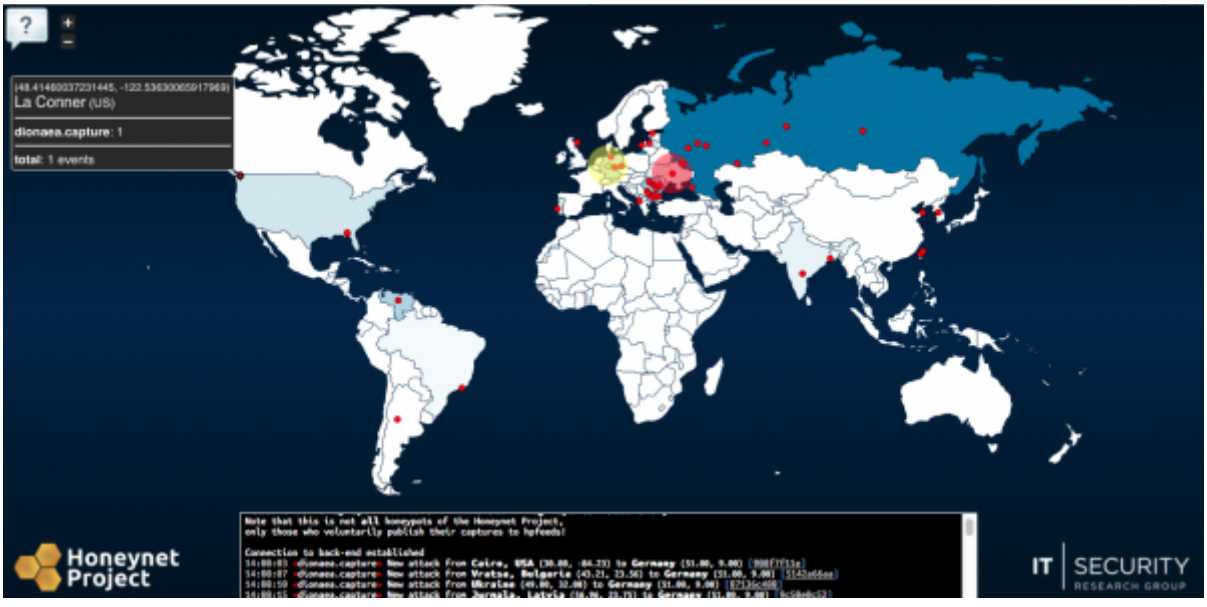
Cyberthrear Real-time Map

La mappa è alimentata da dati anonimi provenienti dai vari servizi di scansione di Kaspersky. La grafica 3D lo fa sembrare quasi più un video gioco, è anche abbastanza interattiva, consente di personalizzare il layout filtrando alcuni tipi di minacce come malware e-mail, attacchi a siti web, etc.

IPViking

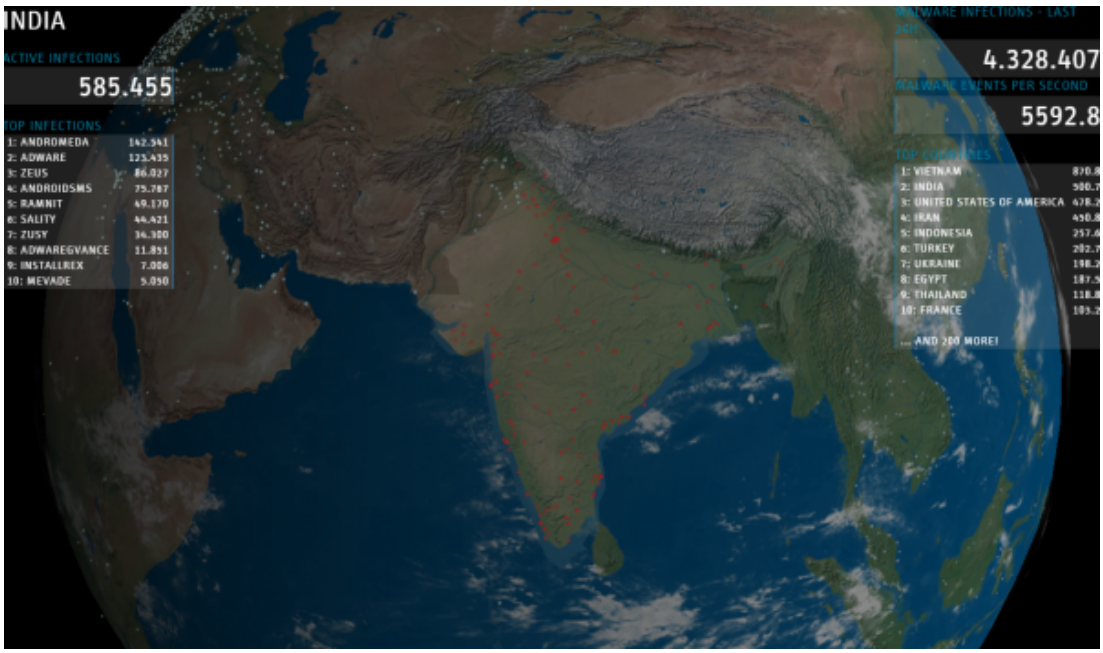
La mappa di Norse Corp include una vasta gamma di dati relativi ad ogni attacco, come ad esempio il nome dell'organizzazione attaccante e l'indirizzo internet, la città ed il servizio del bersaglio, così come i paesi di destinazione e di origine più popolari.

Honey Map



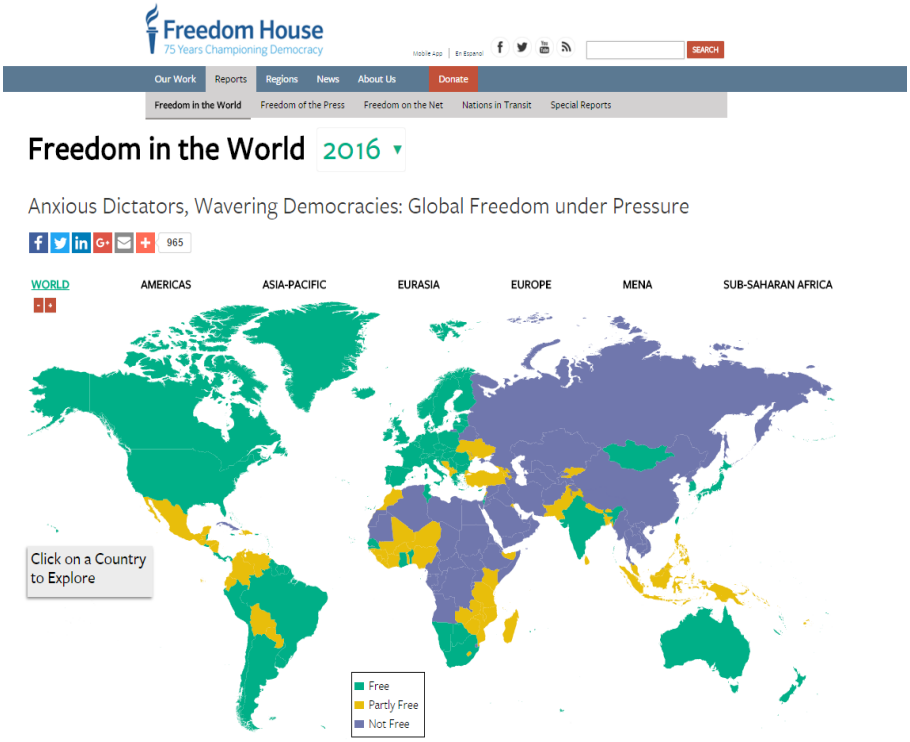
La mappa di Honey Project include una discreta quantità di informazioni utili sulle minacce in tempo reale su sistemi honeypot, compresi i collegamenti per l'analisi del malware da Virustotal per ogni minaccia o attacco.

The Cyberfeed



La mappa di Anubis Networks conduce il visitatore in un tour automatizzato del mondo, utilizza qualcosa di simile a Google Earth e mappe le locazioni di infezioni alle più note famiglie di malware. E più una mappa di infezioni da malware che una mappa attacco.

Freedom in the World



Freedom House è un'organizzazione indipendente dedicata all'espansione della libertà e della democrazia in tutto il mondo. Analizzia le sfide alla libertà e fornisce report su Freedom in the World, Freedom of Press, Freedom on Net etc.

Elaborazione dati

Creazione tabella attacchi

Dal sito di Digital Attack Map è stato scaricato il file JSON degli attacchi, e tramite uno script JavaScript, raccolti 245000 attacchi DDoS avvenuti nel 2014 e nel 2015. Gli attacchi nel file originale rappresentavano diversi tipi: "IP Fragment", "DNS Misuse", "TCP SYN", "TCP RST", "TCP ACK", “Protocol”, "UDP Misuse", “ICMP", “Bandwidth”, "Total Traffic". Sono stati raggruppati quindi nelle loro 4 sopra-classi:"TCP Connection", "Volumetric", "Fragmentation" ed "Application".

Snippet significativo JavaScript caricamento file JSON e filtro per data:

```
function loadJSON(callback) {
   var xobj = new XMLHttpRequest();
   xobj.overrideMimeType("application/json");
   xobj.open('GET', 'file.json', true);
   xobj.onreadystatechange = function () {
         if (xobj.readyState == 4 && xobj.status == "200") {
           callback(xobj.responseText);
         }
   };
   xobj.send(null);
}
function toTable(table, dataObj, tipo){
   var count = 0;
      console.log(dataObj.attacks.length);
      for (var i = 0; i <dataObj.attacks.length; i++){
         var a = dataObj.attacks[i];
         if ((a.start <= 1451606399) && (a.start >= 1388534400) ) {
            count++;
            table.push(makeRow(a, tipo));
         }
      }
   console.log("Large: "+ count + " - In array "+ table.length);
   count=0;
   return table;
}
```

La tabella ricavata è stata importata in un database temporraneo dove poi si è passato alla seconda fase di filtraggio usando SQL. Per lo scopo del progetto degli attacchi è sufficente averrer una tabella con 500 record, contenente ogni paese e quantita di attacchi subiti per tipo, dimensione e durata media.

Snippet SQL significativo filtraggio dati attacchi:

```
SELECT dest, type, COUNT(*) as n, AVG((size/1048576)/1024) as dimGbs, AVG((end - start)/60) as dMins
     FROM attacks
    GROUP BY type, dest

SELECT dest, type, SUM(n) as num, SUM(n * size) / SUM(n) as dimgbs, SUM(n * dur) / SUM(n) as minuti
    FROM dublicatetype
    GROUP BY type, dest

SELECT dest, SUM(n) as tot
     FROM attacksmall
    GROUP BY dest
```

Creazione tabelle database

Il database finale del progetto consiste di due tabelle, una per gli attacchi DDoS (*attacksmall*) e la seconda per i paesi ed i suoi indici di libertà (*country*).
La tabella degli attachi è formata dai campi *id*, *dest* (destinazione), *type* (classe attacco), *n* (totale di attacchi), *size* (dimensione media), *mins* (durata minuti media). La tabella dei paesi invece è composta dai campi *name* (nome, code (ISO code), *pr* (political rights), *cl* (civil liberties), *status* (stato: F-NF-PF). La chiave primaria *code* di *country* fa da chiave esterna per il campo *dest* di *attacksmall.*

attacksmall

Column	Type	Null	Default	Links to	Comments
id	int(11)	No			
dest	varchar(2)	Yes	*NULL*	country -> code	
type	varchar(14)	Yes	*NULL*		
n	int(5)	Yes	*NULL*		
size	decimal(10,4)	Yes	*NULL*		
mins	int(9)	Yes	*NULL*		

Indexes

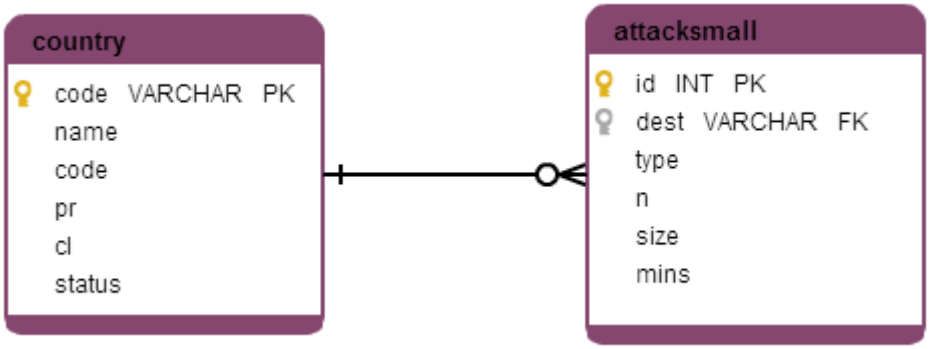
Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	id	499	A	No	
dest	BTREE	No	No	dest	499	A	Yes	

country

Column	Type	Null	Default	Comments
name	varchar(26)	Yes	*NULL*	
code	varchar(2)	No		
pr	int(1)	Yes	*NULL*	
cl	int(1)	Yes	*NULL*	
status	varchar(2)	Yes	*NULL*	

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	code	197	A	No	



Realizzazione sito web

Obbiettivo

Realizzare un sito web che mostri dati su attacchi DDoS in relazione alla libertà dei paesi destinazione degli attacchi. Analizzando i dati ricavati tramite l'utilizzo del software IBM SPSS è stata rilevata una correlazione significativa tra libertà di un paese e la quantità di attacchi da esso ricevuti. In particolare è stato utilizzato il metodo di Spearman:

Correlazioni

			tot	cl	pr
Rho di Spearman	tot	Coefficiente di correlazione	1,000	-,349**	-,367**
		Sign. (a due code)	.	,000	,000
		N	149	149	149
	cl	Coefficiente di correlazione	-,349**	1,000	,950**
		Sign. (a due code)	,000	.	,000
		N	149	149	149
	pr	Coefficiente di correlazione	-,367**	,950**	1,000
		Sign. (a due code)	,000	,000	.
		N	149	149	149

**. La correlazione è significativa a livello 0,01 (a due code).

I risultati dell'analisi mostrano come ci sia una leggera, ma significativa, correlazione negativa trà la libertà di un paese ed il numero di attacchi che esso subisce.
In breve, più un paese è libero (minore il suo indice di PR e CL) maggiore sarà la probabilita di subire maggior numero di attacchi.

Per rendere il sito web interattivo verranno utilizzati script con PHP e Javascript, verrano utilizzate chiamate AJAX, al caricamento della pagina, il database viene interrogato tramite delle query mysq. La libreria jQuery,verrà utilizzata per realizzare le interazioni con la pagina e database. Per la visualizzazione dei grafici verranno utilizzate le librerie HighCharts e JvectorMap.

Utenti

Il sito è di interesse per qualsiasi persona si interessi di cyber attacchi o diritti umani. Dallo studente curioso, ai professionisti sia del settore informatico che umanistico.

Le categorie individuate sono dunque:

- Utente Generico: Un qualunque individuo che abbia accesso ad un pc.
- Umanista: Professionista interessato a questioni di Diritti Umani o altro.
- Informatico: Qualsiasi informatico con interesse verso cyber threaths.
- Studente: Istruzione liceale ed interesse nel informatica e diritti umani.

Obiettivi per ciascuna categoria di utenti

Categoria di utenti	**Bisogni principali degli utenti in relazione al sito**	**Obiettivi**
Studente	Raccogliere informazioni generali	Trovare ispirazione
Informatico	Avere informazioni su attacchi DDoS	Visualizzare dati su DDoS
Umanista	Avere informazioni su Libertà nei paesi	Visualizzare dati su World Freedom
Utente generico	Soddisfare curiosità	Visualizzare informazioni interessanti

Progettazione

Il sito sarà composto di tre sezioni principali. Una sezione con descrizione del progetto. Una sezione con informazioni sui dati raccolti. Una sezione con i grafici realizzati con i dati elaborati. Si utilizzerà come stile il “Material Design”, una metafora, che cela l’idea di rendere come “materiali” gli elementi grafici, che non risultino piatti ma con un loro spessore fisico e con una loro ombra. Dando l'idea di oggetti tridimensionali con uno spessore.

Requisiti funzionali e non funzionali

- Il layout deve essere responsive in modo da adattarsi alle risoluzioni di dispositivi differenti.
- Dovrà essere un sito one-page con smooth scrolling tra le varie sezioni grazie.
- Per il mobile dovrà essere presente un menù di navigazione apposito.
- Il sito dovrà essere compatibile con tutti i maggiori browser e dispositivi. Prevederà accortezze stilistiche per schermi medi e piccoli.
- Le immagini saranno ottimizzate per il web in modo da assicurarne la leggerezza.

Considerazioni sull'interfaccia utente:

L'utente avrà chiara visibilità dello stato del sistema trattandosi di un sito one-page ed avendo sempre su scherrmo un comodo menu che permette di spostarsi tra le varie sezioni rapidamente. Gli utenti hanno la libertà di controllo tramite appunto la barra di navigazione ed il menu nel caso di dispositivi mobile. Verrà mantenuta la corrispondenza tra i pulsanti della barra di navigazione (menu per mobile) ed i titoli delle sezioni. Consistenza e standard sono garantiti dall'uso di un layout simile in tutte le sezioni. La palette di colori uniforme per ogni pagina concorre a dare uniformità al sito. Non sono presenti particolari situazioni che possono creare errori, in quanto il menu/barra sono sempre presenti. Una legge, quasi universale, del design di interfacce, è che si deve cercare di diminuire il più possibile i tempi di risposta. Per questo motivo le immagini saranno ottimizzate il più possibile. E’ stato scelto lo stile one-page dato che non c'è alcuna curva di apprendimento per la navigazione e l'aumento della telefonia mobile ha reso il meccanismo di scorrere le pagine una seconda natura per la maggior parte degli utenti.