Politecnico di Milano
Facoltà di Ingegneria dell'Informazione
Corso di Laurea Magistrale in Ingegneria Informatica

BURN: Baring Unknown Rogue Networks

Analisi e visualizzazione del comportamento di reti malevole

Relatore: **Stefano Zanero**
Correlatore: **Paolo Ciuccarelli**

Luca Di Mario
Matricola 711908
A.A. 2010/2011

Sommario

L'analisi manuale degli incidenti informatici condotta da esperti di sicurezza è necessaria per l'investigazione di minacce o attacchi complessi. Questo compito è particolarmente difficile quando i fenomeni analizzati coinvolgono eventi lenti, poco visibili o su scala troppo ampia, oggi strategia tipica dei criminali informatici. In questo contesto, gli strumenti di visualizzazione possono supportare l'attività degli analisti. In questa tesi presentiamo BURN, uno strumento interattivo per la visualizzazione degli autonomous system (ossia un gruppo di reti sotto il controllo di una specifica autorità amministrativa, come ad esempio un provider di servizi internet) caratterizzati dall'avere un'attività malevola (e.g., spam, phishing, traffico botnet). BURN, attualmente in fase di beta testing (disponibile su `http://burn.vplab.elet.polimi.it`), aiuta nella ricerca di autonomous system dal comportamento malevolo attraverso l'esplorazione di visualizzazioni interattive. In aggiunta, proponiamo delle euristiche per l'identificare lei migrazioni di server malevoli tra diversi autonomous system e per stimare il la stimare il livello di tolleranza degli autonomous system ad attività malevole. Queste euristiche sono utili nella ricerca della *root cause* e nelle investigazioni dell'autorità giudiziaria [3]. Siamo stati in grado di riconoscere 63 shutdown. Le possibili migrazioni trovate sono 61496, di queste 2497 rappresentano migrazioni uno-a-uno.

Indice

1 Introduzione

Nonostante la grande quantità di strumenti automatici atti a rilevare attività malevole nella rete, l'analisi manuale condotta dagli esperti di sicurezza è tuttora fondamentale per l'investigazione degli attacchi informatici. Questo compito è particolarmente difficile quando implica l'analisi di fenomeni poco visibili, su larga scala, o con dinamiche particolarmente lente. BURN propone un'euristica per il riconoscimento delle migrazioni di servizi tra diversi autonomous system. Queste avvengono ad esempio quando un autonomous system blocca una serie di indirizzi ritenuti malevoli o nel caso un autonomous system sia riconosciuto complice dell'attività malevola e venga, suo malgrado, sconnesso. La ricerca delle migrazioni è particolarmente importante perchè non si limita allo studio del singolo attacco o minaccia ma mira alla comprensione delle *root cause* che regolano il fenomeno. Consideriamo una migrazione come uno spostamento di servizi malevoli da un autonomous system ad un altro. La migrazione si compone di due fasi, una fase di shutdown e una fase di activiation, caratterizzate rispettivamente da una diminuzione dell'attività malevola nell'autonomous system sorgente ed un aumento dell'intensità dell'attività malevola nell'autonomous system destinazione. In altre parole il nostro approccio mira all'investigazione della *root cause* con l'obiettivo di poter creare in futuro una politica di prevenzione delle minacce informatiche, in contrasto con l'attuale politica di risposta ad eventi già accaduti.

Inoltre, abbiamo progettato BURN con un'interfaccia grafica innovativa, progettata con l'obiettivo di migliorare superare alcuni dei limiti dei sistemi esistenti. Gli attuali strumenti di visualizzazione di tematiche legate alla sicurezza presentano spesso visualizzazioni confuse ed affollate. Il diffuso utilizzo di heat-map o di altre visualizzazioni basate sulla geolocalizzazione —dove gli eventi sono cioè evidenziati su una mappa con simboli di differente grandezza e colore— porta alla creazione di visualizzazioni confuse e fuorvianti. Ad esempio, aree geografiche con una connettività più sviluppata appariranno molto dense senza necessariamente riflettere l'intensità effettiva dell'attività malevola. Le visualizzazioni proposte coniugano due aspetti fondamentali: ricchezza di contenuti e facilità di lettura. In una singola visualizzazione siamo in grado, ad esempio, di mostrare fino a sette dimensioni contemporaneamente senza che la visualizzazione risulti fuorviante o confusa. BURN organizza le visualizzazioni in due viste, la Global view e la Autonomous System

View. La prima di queste, pensata per un utente non tecnico fornisce informazioni generali sullo stato degli autonomous system mondiali mentre la seconda, pensata per un utente più tecnico si concentra sui dettagli del comportamento del singolo autonomous system.

1.1 Contributi originali

In sintesi, i contributi originali di questo lavoro sono:

- Proponiamo un'euristica efficiente per la scoperta delle migrazioni tra autonomous system. L'euristica riconosce decrementi improvvisi nel numero di host malevoli in una determinata rete seguita da un aumento improvviso del numero di host simili in uno o più reti diverse.
- Proponiamo un'euristica per la stima del livello di tolleranza degli autonomous system. L'euristica, analizzando i tempi di vita medi degli host malevoli nella rete è in grado di localizzare quelle reti che mostrano una politica di controllo particolarmente tollerante.
- Proponiamo infine un sistema di visualizzazione utile per esplorare i dati riguardanti gli autonomous system malevoli, questa visualizzazione rende più facile per gli analisti riconoscere facilmente eventi malevoli.

Siamo stati in grado di riconoscere 63 shutdown nel periodo di tempo a nostra disposizione, di questi ventisei segnano un rapido decremento di più di dieci servizi. Le migrazioni trovate uno-a-uno o uno-a-due sono 61496, di queste 2497 rappresentano una migrazione uno-a-uno mentre le restanti 58999 uno-a-due

I risultati di questa tesi sono stati accettati per la pubblicazione sugli atti di VizSec 2011, la conferenza internazionale di punta nell'area della visualizzazione dei dati nel campo della sicurezza. [1].

2 Stato dell'arte

In questo capitolo presentiamo lo stato dell'arte inerente alla visualizzazione degli eventi relativi alla sicurezza informatica. In particolare, in Sezione 2.1 presentiamo FIRE, l'applicazione che fornisce dati a BURN. In Sezione 2.2 presentiamo i due lavori più recenti e più simili a BURN. Infine, in Sezione 2.3 presentiamo una breve panoramica della visualizzazione della conoscenza (ingl., Knowledge Visualization), concentrandoci sui soli aspetti essenziali per comprendere il resto del documento ed in particolare il Capitolo 3.

2.1 FIRE

FIRE è un sistema di analisi e monitoraggio del livello di attività malevola negli Autonomous System (AS). Un AS è un gruppo di reti sotto il controllo di una singola e ben definita autorità amministrativa. L'obiettivo di FIRE è identificare e diffondere informazioni su tutti quegli AS che mostrano un livello di attività malevola consistente, quindi più probabilmente complici di attività illecite. Per fare questo FIRE monitora giornalmente l'attività nelle reti utilizzando tre fonti di informazione: la prima è legata all'identificazione degli host che controllano il comportamento delle botnet, la seconda fornisce dati sugli host che sono coinvolti nel drive-by-download exploits e la terza riporta gli URL che sono stati identificati come pagine di phishing. FIRE concentra la propria attenzione sulla localizzazione dei server malevoli. In questo senso possiamo distinguere tra due categorie di host che mostrano attività malevola; una prima categoria è formata da server dedicati all'attività stessa, queste macchine sono di solito controllate direttamente dai criminali e dispongono di una grande capacità di trasmissione e di calcolo, alla pari di un comune server web. La seconda categoria è composta da host compromessi (e.g. trojan). Queste macchine, per lo più personal computer, non sono normalmente consapevoli dell'attività malevola eseguita. FIRE concentra la sua ricerca sul primo tipo.

I dati raccolti da FIRE sono poi resi pubblici attraverso il sito `http://www.maliciousnetworks.org`. La pubblicazione dei dati è il punto chiave dell'azione di FIRE: gli AS coinvolti in attività criminali o comunque permissivi non gradiscono l'attenzione su di sé e spesso rispondono alla pubblicazione con il decremento o cessazione di ogni attività malevola. Il termine AS può riferirsi a realtà molto diver-

se tra loro. Tutti gli AS sono responsabili del traffico proveniente dal loro interno ma le dimensioni degli AS posso variare enormemente da un minimo di uno ad oltre un milione di host contemporaneamente connessi. È quindi ovvio che un AS di dimensioni molto ridotte che ospiti attività malevola sarà molto più probabilmente complice nell'attività criminale perpetrata rispetto ad un AS grande.

FIRE classifica le attività malevole in quattro macro-categorie: C&C, malware, phishing e spam.

Command & Control (C&C) Per attività C&C s'intende l'invio di messaggi destinati ad attivare una seconda macchina compromessa; se il messaggio è destinato al controllo di un gruppo di macchine allora chiameremo botnet questo gruppo di macchine. Una botnet è un insieme di macchine compromesse in grado di eseguire delle istruzioni comunicate da remoto; tra le tipiche attività malevole svolte dalle botnet ci sono lo spamming, il phishing e numerosi attacchi informatici (e.g. DDoS). Chi controlla una botnet dispone infatti di una vastissima banda di comunicazione oltre che di una grande capacità di calcolo e difficile tracciabilità.

Malware L'attività malware si riferisce essenzialmente a quegli host che ospitano servizi di drive by download e che hanno quindi l'intento di eseguire un programma, compromettendo un host.

Phishing Si definisce phishing un'attività illegale che, sfruttando messaggi istantanei o di posta elettronica fasulli, mira a ottenere l'accesso ad informazioni personali o riservate con la finalità del furto d'identità. Imitando, nell'impostazione grafica e nel contenuto, le comunicazioni dei siti istituzionali, il phisher raggira l'utente portandolo a rivelare dati personali quali numero di conto corrente, numero di carta di credito e altri dati sensibili.

Spam Per spam si intende l'invio di grandi quantità di messaggi indesiderati a migliaia di indirizzi mail contemporaneamente. Lo scopo di questa attività è generalmente di tipo commerciale e il contenuto pubblicitario può essere di vario genere. Come detto in precedenza, la maggior parte delle volte -identificati ed esposti gli AS malevoli- si verifica una rapida cessazione dell'attività criminale sulla rete. Questa viene causata da un'azione interna o esterna alla rete: per azione interna, s'intende l'intervento degli amministratori della rete; per azione esterna, l'intervento di chi fornisce connettività alla rete (in questo caso depeering).

Si consideri un esempio concreto: il caso Russian Business Network (RBN). Il caso in questione risale alla fine del 2007. Allora era risaputo che RBN ospitasse una

vasta gamma di attività malevole responsabili di un numero significativo di attacchi, truffe e tentativi di phishing. Una volta che il caso fu reso di pubblico dominio, le attività malevole sulla rete diminuirono rapidamente. In entrambi i momenti, l'esposizione pubblica di queste relazioni ha portato i gestori di queste reti a pronti provvedimenti di taglio della connessione alle organizzazioni criminali. È quindi chiaro come l'esposizione pubblica di questi dati possa ritenersi un'importante leva per combattere la diffusione e la proliferazione dei server malevoli all'interno degli AS. Questo però non implica una diminuzione matematica a livello globale del numero di server malevoli in quanto chi gestisce l'attività criminale tende a reagire trasferendo le operazioni in una seconda rete complice o semplicemente più permissiva. Questa migrazione richiede però un intervallo di tempo durante il quale le attività malevole devono necessariamente cessare. La rapida individuazione di queste attività potrebbe quindi rendere difficile per i criminali informatici stabilire una base sicura per i loro traffici, obbligandoli a continui spostamenti.

2.2 Visualizzazione di attacchi informatici

In questa sezione presentiamo i progetti simili a BURN (EMBER in Sezione 2.2.1 e NICTER in Sezione 2.2.2).

2.2.1 EMBER

EMBER , Extreme Malicious Behaviour viewER [7], è un servizio di analisi e visualizzazione delle attività malevoli presenti sulla rete. EMBER rende visibili le attività malevole attraverso l'utilizzo di una mappa geolocalizzata: questo tipo di mappe rappresenta spesso una sfida per chi si propone di utilizzarle per via di alcuni tipici problemi che tendono a rendere la visualizzazione poco efficiente. Il primo ostacolo è rappresentato dai puntatori utilizzati per indicare la posizione degli oggetti di interesse: per diversificare questi puntatori si prediligono forme e colori che però, nelle aree di maggiore densità, tendono a rendere la visualizzazione caotica e al limite del tutto incomprensibile.

Un diverso tipo di approccio è la colorazione di regioni in base alla magnitudo del fenomeno in esame. Il principale limite riscontrato utilizzando questo approccio è dovuto al fatto che —a seconda del particolare tipo di fenomeno analizzato— si può introdurre una distorsione, se ad esempio il fenomeno misurato è la quantità di server malevoli presenti sulla rete, vi saranno aree dove la connettività è più sviluppata, o semplicemente più estese dove questo fenomeno sarà necessariamente più intenso. Un approccio alla soluzione di questo problema è la normalizzazione dei risultati. EMBER propone l'utilizzo dello Standardized Incidence Rate (SIR), che misura il numero di server che ospitano attività malevoli per ogni 100.000 server disponibili

nella stessa area geografica, basandosi sulla localizzazione geografica dei diversi indirizzi IP, la densità di popolazione presente in quel momento e la percentuale di utilizzo di computer nell'area. Grazie a questo metodo, è possibile per l'utente individuare rapidamente le aree di interesse, quelle caratterizzate da un alto livello di attività malevola, valutare un livello di rischio dell'area ed osservare quali zone sono particolarmente colpite da specifici tipi di attacchi e quale sono invece evitate. Oltre a questo EMBER fornisce alcuni dati aggiuntivi attraverso una dashboard. Quest'ultima contiene una mappa geografica dove le attività malevole sono legate alle città e rappresentate con circonferenze di dimensioni e colore variabili a seconda dell'intensità del fenomeno. Inoltre è presente un calendario che fornisce la possibilità di scegliere il giorno da analizzare ed un pannello grazie al quale è possibile selezionare alcuni parametri utili alla visualizzazione. In aggiunta sul lato sinistro, un pannello fornisce indicazioni aggiuntive sui dati riguardanti le singole città.

2.2.2 NICTER

NICTER, Network Incident analysis Center for Tactical Emergency Response [2], nasce dall'esigenza di monitorare l'attività di una rete. Questa operazione solitamente implica l'analisi manuale di grosse quantità di dati. NICTER mira ad automatizzare questo processo fornendo all'utente un'interfaccia in grado di guidarlo nell'attività, migliorando l'efficienza con cui queste informazioni sono visualizzate e cercando di individuare nel traffico monitorato comportamenti anomali che potrebbero interessare maggiormente all'utente.

Questo sistema si avvale di diverse tecniche di analisi e data mining e intende fornire agli operatori uno strumento in grado di individuare le anomalie nel traffico monitorato, classificare il flusso malevolo in base al comportamento degli host e offrire una predizione sui cambiamenti nella circolazione della rete.

Il core di NICTER è formato da quattro diversi sistemi di detection: the Macro analysis System, il Micro analysis System, il Network and Malware Enchaining System, l'Incident Handling System. Questi tool si focalizzano sull'analisi di malware e si differenziano per il livello di analisi, che va dalla disanima del traffico globale presente sulla rete all'indagine dei singoli malware con l'intento di ottenere maggiori informazioni sulle loro caratteristiche e facilitare così sia il processo di riconoscimento sia il processo di bonifica. Il Macro analysis System utilizza una serie di sensori per il monitoraggio in tempo reale delle darknet. Una darknet (in italiano, letteralmente, rete scura) è una rete virtuale privata dove gli utenti connettono solamente persone con affidabilità provata. Nel suo significato più generale, una darknet può essere qualsiasi tipo di gruppo chiuso e privato di persone che comunicano, ma il nome è più spesso usato nello specifico per reti di condivisione file.

Micro analysis System è composto da un insieme di honeypot in grado di catturare analizzare identificare e catalogare diversi tipi di attacchi. Network and malware enchaining System ha lo scopo di legare uno specifico attacco ad un lista di malware compatibili con l'attacco stesso attraverso l'analisi del traffico presente sulla rete che ospita l'host compromesso dal malware. Incident Handling System è un insieme di tool creati con lo scopo di guidare l'operatore nell'analisi dei dati raccolti dai sistemi precedentemente descritti. Tutti questi sistemi prevedono un resa dei risultati anche visiva attraverso singoli grafici specifici per ogni tipologia di dati, per aiutare l'operatore nell'analisi e nel report degli stessi.

2.3 vantaggi della visualizzazione

In questa sezione è introdotto il concetto di visualizzazione e, in Sezione 2.3.1, è spiegato come questa sia applicata come processo per la visualizzazione della conoscenza [4].

Visualizzare significa rappresentare visivamente —quindi in forma intuitiva e immediata— l'andamento di un particolare fenomeno. Nella maggioranza dei casi, le informazioni sono espresse soltanto sotto forma di testo e questo rende più difficoltosa l'operazione di estrapolazione del significato se questo è espresso solamente tramite le parole. Infatti per il nostro cervello è maggiormente complesso processare un testo, mentre figure e immagini necessitano di un tempo minore per essere comprese ed assimilate. Una visualizzazione è quindi una rappresentazione grafica che consente di raffigurare l'informazione in modo tale da poter acquisire conoscenza, sviluppare una comprensione dei contenuti e comunicare esperienze.

Seppur sussista la consapevolezza che ciascun individuo reagisce in modo assolutamente unico e personale al contenuto presentato, è possibile senza dubbio affermare che esistano particolari fattori di riferimento che influenzano effettivamente la performance cognitiva del soggetto. Biologicamente, la percezione dell'individuo è supportata e migliorata da fattori quali la scoperta del movimento in un contesto di caccia, la scoperta del colore nella scelta del cibo, la configurazione figura-sfondo ed oggetto-ombra nell'applicazione di strumenti. A questo proposito è utile ricordare i principali benefici derivanti dal ricorso ad un artefatto grafico. Innanzitutto, una visualizzazione svolge una serie di funzioni basilari che influenzano le dimensioni percettive umane, tra cui:

Richiamo La funzione di richiamo, intesa come l'abilità di suggerire e trasmettere un contenuto in modo memorabile. Un'immagine è certamente più evocativa e impressionante nel tempo rispetto ad una lunga descrizione ed argomentazione testuale riferita allo stesso materiale informativo. Alcune caratteristiche distintive di una rappresentazione grafica, quali ad esempio la forma, il colo-

re, la dimensione ed il movimento contribuiscono alla facilità di rievocazione e richiamo a mente a distanza nel tempo dell'informazione analizzata.

Visione d'insieme La visione d'insieme, ovvero la capacità di sintetizzare dettagli e fornire macrostrutture che organizzino e gestiscano moltitudini di dati in un *unicum* coerente. Una visualizzazione, per sua natura, dovrebbe sfruttare al massimo la sua capacità di sintesi per creare un risultato che inglobi in se un numero elevato di informazioni. La lunghezza di un testo che cerca di descrivere ed analizzare le componenti di un oggetto, è meno efficace di artefatto grafico che mostra -in toto- le singole componenti dell'oggetto considerato, assemblate.

Comprensione La funzione di comprensione, ovvero l'abilità delle rappresentazioni visive di incoraggiare e migliorare la conoscenza, l'apprendimento ed il processo di *sense-making* selezionando gli elementi in modo tale per mostrarne le relazioni inedite.

Scoperta La scoperta, ovvero il potenziale di una visualizzazione nell'evidenziare contributi ed elementi significativi spesso non svelati da una sola descrizione testuale.

Emozioni le emozioni, ovvero la tattica di provocare reazioni e risposte emotive allo stimolo presentato. Come evidenziato in precedenza, una visualizzazione -oltre al trasferimento di informazioni- è in grado di veicolare un impatto emotivo che porta ad un aumento del coinvolgimento del lettore e alla memorabilità dell'informazione stessa.

Coordinazione La coordinazione, intesa come la capacità di guidare ed orientare un gruppo di persone e fornire loro punti di riferimento comuni. Le immagini dimostrano di superare i limiti di fruibilità spazio-temporali, riuscendo a diminuire le barriere relative all'utilizzo di codici comunicativi differenti. Una visualizzazione è potenzialmente capace di essere compresa ed interpretata anche da utenti che parlano lingue differenti, che appartengono a contesti socio-culturali differenti, che presentano abitudini e predisposizioni comunicative diverse. Si costruisce in questo modo una vera e propria validità universale della visualizzazione grafica.

2.3.1 Knowledge Visualization

Lo studio del Knowledge Visualization (visualizzazione della conoscenza) nasce dall'integrazione di recenti ed importanti domini di ricerca quali il campo dello human-computer interaction, il graphic design, il knowledge management, principi di architettura e, non da ultimi, linguistica e psicologia cognitiva. Proprio la trasversalità

di questi studi, testimonia sia la ricchezza sia la difficoltà che sono alla base della progettazione di un artefatto grafico. Il concetto di knowledge visualization si occupa degli strumenti grafici che possono essere utilizzati per migliorare la creazione ed il trasferimento della conoscenza tra almeno due individui. Oltre che il semplice e statico trasferimento di dati, tale concetto implica l'importante possibilità di comunicare "esperienze, attitudini, valori, aspettative, opinioni e predizioni permettendo, in questo modo, al singolo interlocutore di ricostruire, ricordare ed applicare l'insight cognitivo correttamente". Si realizza quindi un processo ciclico, di costante rimando, che inizia con la presentazione dell'artefatto ma che si perpetua nel tempo, ogni volta che il singolo individuo legge ed interpreta lo stesso input secondo sfaccettature diverse in virtù del proprio bagaglio esperienziale e socio-culturale.

Una progettazione corretta della visualizzazione, oltre che favorire e semplificare l'accesso alla conoscenza, queste determina un impatto visivo tale da aumentare e stimolare una maggiore memorabilità ed espressività dell'informazione stessa. Inoltre un'immagine contribuisce anche allo sviluppo della dimensione collaborativa: in quest'ottica l'utilizzo di tools grafici permette di gestire compiti di *collaborative knowledge*, in quanto, grazie ad un costante confronto tra i soggetti ed una gestione comune del contesto, viene costantemente aggiornato un vocabolario comune di significanti grafici.

Le raffigurazioni visive sono caratterizzate da forme, colori, dimensioni, posizione, movimento e tutta un'altra serie di attributi che contribuiscono a fornire a chi osserva una grande quantità di dati contemporaneamente in uno spazio definito. Ad esempio, se un'immagine presenta un determinato colore, questa variabile costituirà un elemento molto significativo per la sua comprensione. Questo attributo trasmette all'utente sensazioni e percezioni che leghiamo specificatamente ad alcune tonalità. Inoltre un colore può essere più o meno visibile, capace di attrarre in maniera diversa l'attenzione dell'utente, essere usato come legante tra due zone diverse di una stessa visualizzazione o, al contrario, costituire un codice utile all'immediata segmentazione concettuale di un argomento in sottoargomenti, e così via. L'immagine, in definitiva, contiene in se più elementi di indagine e interpretazione di quanti possa contenerne un testo, soprattutto se quest'ultimo è redatto in forma scientifica o matematica. Inoltre, l'immagine possiede una potenzialità a livello cognitivo non indifferente: la capacità di generare in chi la osserva nuovi quesiti e dubbi, primo e fondamentale passaggio logico per ogni fase di ricerca e progettazione. La mente umana di fronte ad un'immagine individua spontaneamente andamenti, pattern ed incongruenze. Effettuare la stessa operazione cognitiva su un documento testuale risulterebbe invece molto più difficile. Le immagini inoltre stimolano l'ispirazione: analizzare rappresentazioni visive agevola la formazione di nuove considerazioni su quanto stiamo vedendo, riguardo possibili e ancora insondati relazione tra i dati. Trasferire, quindi,

l'informazione dalla forma scritta a quella simbolico-visiva è un processo che può essere utile anche e soprattutto alla comprensione dei dati e nei processi di analisi degli stessi. Inoltre, l'immagine riesce a restituire nello stesso momento l'intera complessità di un fenomeno e non solo una parte. Può fornire informazioni senza dover fruire della complessa articolazione e scarsa accessibilità dei dati. Poniamo il caso in cui un professionista di settore abbia necessità di reperire un certo dato all'interno di un set di informazioni archiviate in un classico database. La rappresentazione visiva dell'intera sequenza di dati interessanti faciliterebbe sicuramente la loro analisi, rispetto ad un'ispezione manuale di tutta questa serie di eventi. Per questo motivo, gli strumenti di visualizzazione costituiscono un fondamentale supporto in aiuto ad esperti, analisti e ricercatori del settore. Da qui il bisogno, e la relativa soddisfazione di questo, di riuscire a tradurre al meglio ad un pubblico sia di ricercatori ed esperti del settore sia di utenti meno esperti, ingenti quantità di informazioni appoggiandosi ad uno strumento in grado di raccogliere le suddette quantità in un intervallo definito di spazio e tempo e capace di palesare in maniera semplice e immediata all'occhio umano fenomeni altrimenti poco riconoscibili nella moltitudine di dati incolonnati in tabelle. Usufruire dello strumento della visualizzazione significa dunque avere la possibilità di comprendere più a fondo il fenomeno analizzato, avanzare ipotesi non ancora esplorate, dedurre relazioni tra i dati che si osservano cogliendone a pieno l'intero carico conoscitivo.

In generale, quindi, un artefatto di visualizzazione grafica consente di mostrare e trasmettere conoscenza favorendo un'esposizione chiara e immediata volta anche al confronto tra i diversi fruitori e creare nuova conoscenza attraverso la scoperta di nuove e diverse combinazioni possibili del medesimo input cognitivo.

In conclusione, la visualizzazione aumenta la chiarezza e la semplicità espositiva dell'informazione sfruttando alcuni dei principi organizzativi della conoscenza che governano la nostra percezione della realtà. Ad esempio, il principio della vicinanza, per cui oggetti vicini ci appaiono come uniche unità coerenti mentre oggetti lontani ci appaiono come elementi separati; la somiglianza, ovvero la nostra naturale tendenza a raggruppare gli elementi che sono, per qualche aspetto, simili tra loro. Applicando questi principi di organizzazione cognitiva (riferimento ai principi di organizzazione della conoscenza della scuola Gestaltica [9]), aumenta il livello e la coerenza della percezione finale della rappresentazione dati.

L'attuale stato dell'arte in merito ad applicazioni, prodotti o strumenti orientati in questa direzione presenta già dei casi noti (riferimento al capitolo in cui parli di Fire, Ember, etc). Nella maggioranza dei casi però, si tratta di progetti sviluppati *in toto* da equipe costituite esclusivamente da esperti del settore informatico, nelle quali competenze non rientra lo studio delle potenzialità offerte dalla visualizzazione, quindi il conseguente sviluppo efficace di una data-visualization che sfrutti al meglio

i dati in proprio possesso. Per questo motivo si rende utile la collaborazione interdisciplinare tra almeno due diverse figure professionali: l'ingegnere informatico e il progettista della comunicazione. La visualizzazione di dati tecnici quindi deve essere affidata ad una figura che sappia orientare alla sintesi tutti i dati grezzi in input disordinati, producendo una visualizzazione ordinata, chiara, leggibile, funzionale e immediata. Proprio per mantenere un buon grado di semplificazione, in modo tale da fornire all'utente solo i dati di cui ha realmente bisogno e non creare un inutile sovraffollamento informativo (le informazioni devono essere distribuite in maniera coerente sui diversi livelli di dettaglio dell'applicazione) si necessita del supporto professionale di un esperto della comunicazione, oltre che del necessario apporto informatico alla progettazione.

I contenuti fino a qui presentati servono a presentare il contesto e l'approccio con cui BURN è stato sviluppato, tenendo conto delle criticità dei sistemi realizzati in precedenza, delle risorse disponibili e dello stato dell'arte delle tecniche di visualizzazione. Nel capitolo seguente sarà presentato BURN, sarà data una panoramica dell'applicazione e i dettagli sulle euristiche implementate.

3 BURN (Baring Unknown Rogue Networks)

In questo capitolo presentiamo BURN (Baring Unknow Rogue Networks), uno strumento di visualizzazione ed analisi interattiva degli Automonous System (AS) caratterizzati da attività malevola. In particolare, in Sezione 3.1 descriviamo le visualizzazioni che compongono l'applicazione, nella Sezione 3.2 introduciamo l'euristica per la ricerca di migrazioni tra diversi AS, nella Sezione 3.3 descriviamo l'euristica per la stima della tolleranza mostrata da un AS, infine nella Sezione 3.4 introduciamo alcuni dettagli riguardanti la visualizzazione.

3.1 Panoramica

Aspetti chiave che abbiamo implementato in BURN sono l'interattività, la ricchezza di informazioni e la dinamicità. BURN si sviluppa essenzialmente su due viste: una per utente-base chiamata Global View e una per utente tecnico detta Autonomous System View (o AS View). La Global View mostra nel complesso l'andamento dell'attività malevola negli AS monitorati: BURN è in grado di evidenziare quali siano gli AS che mostrano più attività malevola e la loro localizzazione geografica e inoltre riconoscere picchi di attività nel tempo o identificare AS con comportamenti simili o correlati. La Global View si divide ulteriormente in 3 diversi tipi di visualizzazione: Bubble Chart, Geographical Map e Trend Chart. La AS View mostra invece dettagli sul singolo AS e sul suo comportamento. I dettagli qui evidenziati includono indicazioni sulla posizione geografica, dettagli amministrativi e, per finire, sulla vita dei server malevoli ospitati dall'AS. L'AS View autonomous system si divide ulteriormente in History Chart, Service Migration Screen e Service Longevity Chart.

3.1.1 Global view

La sezione Global View comprende le tre visualizzazioni globali: Bubble Chart, Geographical Map e Trend Chart. Queste schermate possono essere visualizzate in modo mutuamente esclusivo e per il passaggio da una all'altra sarà sufficiente un click su uno dei tre appositi pulsanti.

Oltre a questo è presente, nella parte inferiore dello schermo una timeline: questa sarà visibile utilizzanto la Bubble Map e la Geographical Map, ma non la Trend Chart.

Bubble Chart

La Bubble Chart è la schermata principale dell'applicazione e rappresenta un'evoluzione del concetto di classifica già presente in FIRE (si veda`http://www.maliciusnetworks.org`). Ogni AS è rappresentato da un bubble, un oggetto grafico che raccoglie in sé molte delle proprietà dell'AS rappresentato e del quale parleremo in modo più approfondito nella Sezione 3.1.3.

L'asse delle ordinate rappresenta inizialmente il maliciuos score dell'AS mentre all'asse delle ascisse non è data alcuna dimensione, utilizziamo questo stratagemma per permettere ad AS con score simili di disporsi secondo il proprio score senza sovrapporsi tra loro occupando automaticamente lo spazio disponibile. Grazie a questo meccanismo di disposizione automatica nello spazio gli AS con valori simili tenderanno in modo del tutto autonomo a formare dei cluster visivi associati a classi di AS con caratteristiche comuni. Come già accennato, è possibile per l'utente assegnare all'asse delle ordinate altre dimensioni, oltre al malicious score, come l'incremento dell'attività nel periodo selezionato e la dimensione dell'AS stimata (cioè il numero di macchine effettivamente connesse all'AS).

Cliccando su un singolo bubble vengono mostrate informazioni aggiuntive come descritto in Sezione 3.1.3.

Geographical Map

La Geographical Map mostra la distribuzione degli AS in base alla loro localizzazione geografica. L'utente ha a disposizione due livelli di zoom: un livello globale e un secondo zoom a livello dello stato. A livello globale gli AS sono raggruppati per stato ai fini di una visione d'insieme più chiara e sintetica, la mappa a livello globale consiste in una choropleth map [5] dove il livello di saturazione del colore associato allo stato indica lo score medio degli AS presenti e catalogati nello stato. A livello di stato la mappa evidenzia gli AS effettivamente presenti nello stato collocandoli sulla mappa in base alla loro posizione geografica, gli AS sono rappresentati dallo stesso oggetto grafico che è stato utilizzato nella Bubble Chart. Per la rappresentazione è stata scelta una mappa con bassa risoluzione, questo per evitare che l'utente inesperto possa essere portato a credere di potere localizzare con estrema sicurezza la posizione di un AS che invece è legata all'area in cui quell'AS offre connettività più che ad un preciso indirizzo.

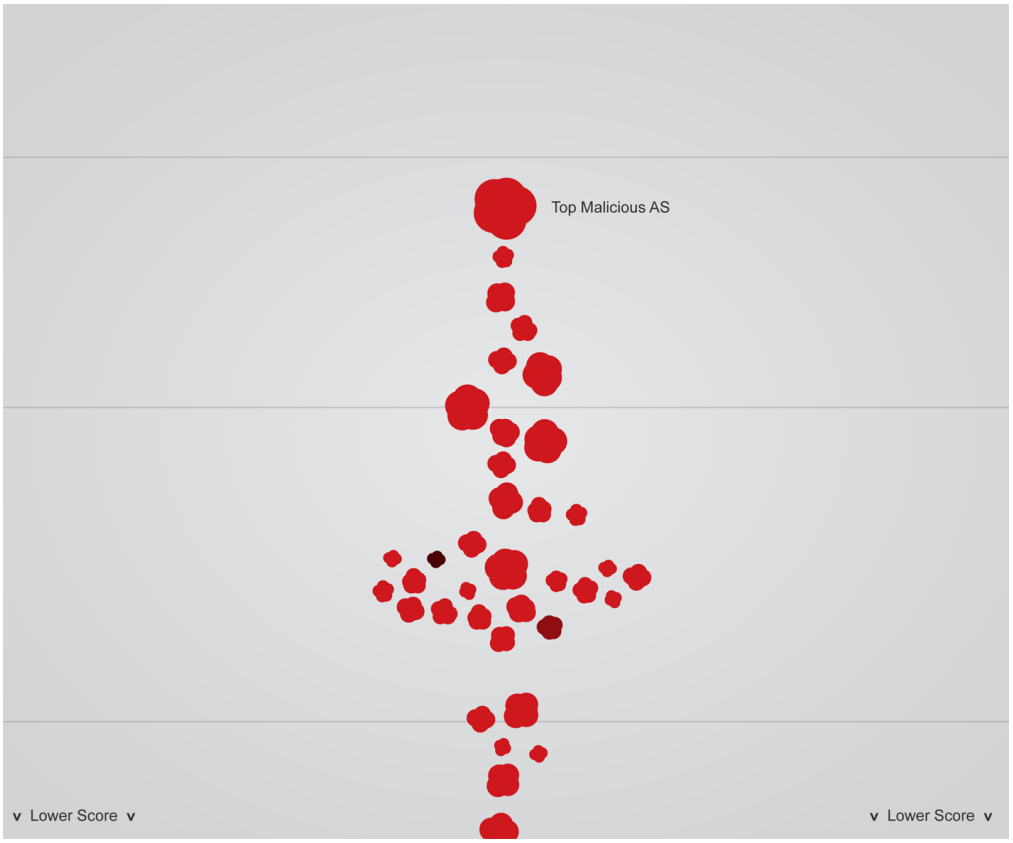

Figura 3.1: Bubble Map. In questa visualizzazione i bubble sono disposti verticalmente a seconda del malicious score. I diversi bubble mostrano animazioni e caratteristiche diverse aiutando l'utente nell'esplorazione. E' possibile scorrere la mappa utilizzando delle apposite aree per raggiungere diversi livelli di score.

Figura 3.2: Geographical Map a livello mondiale

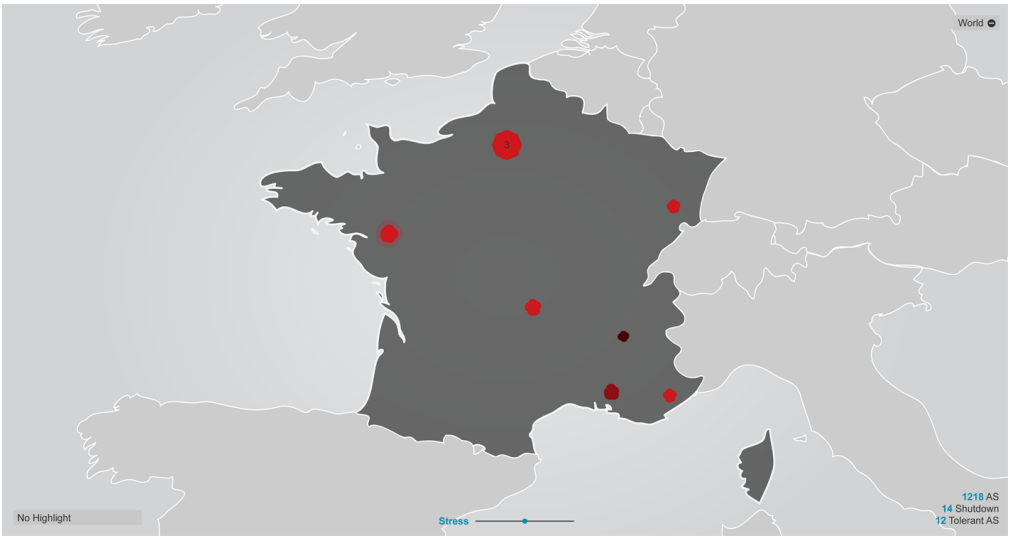

Figura 3.3: Geographical Map a livello stato. Gli AS maligni sono visualizzati all'interno dello stato di appartenenza, la posizione che occupano è calcolata in basa all'effettiva posizione geografica dell'AS.

Trend Chart

La Trend Chart visualizza il trend annuale del numero di malicious servers globale. I trend sono visualizzati in un grafico multilinea dove ogni linea rappresenta una diversa attività malevola, più una linea rappresentante la somma delle altre quattro. Questo grafico è stato ideato per permettere all'utente di localizzare picchi di attività o altre singolarità.

Posizionando il cursore su una linea si visualizzano informazioni aggiuntive quali il valore esatto del numero di server e la data della rilevazione.

Timeline

La Timeline occupa la parte inferiore della schermata e compare nelle visualizzazioni Bubble Map e Geographical Map, essa mostra l'andamento del numero di attacchi nel tempo, nel caso si sia scelto una particolare tipo di attività malevola la Timeline mostrerà i valori corrispondenti alla specifica attività confrontandoli con il totale delle attività.

La Timeline ha come principale scopo l'evidenziare all'utente il periodo selezionato per la visualizzazione e di permettere all'utente di modificare questo'ultimo intervenendo su due pulsanti trascinabili, rispettivamente l'inizio e la fine del periodo osservato.

La imeline si presenta all'utente in due forme: compatta ed estesa. La forma compatta è stata pensata per assicurare alla view attualmente visualizzata il mag-

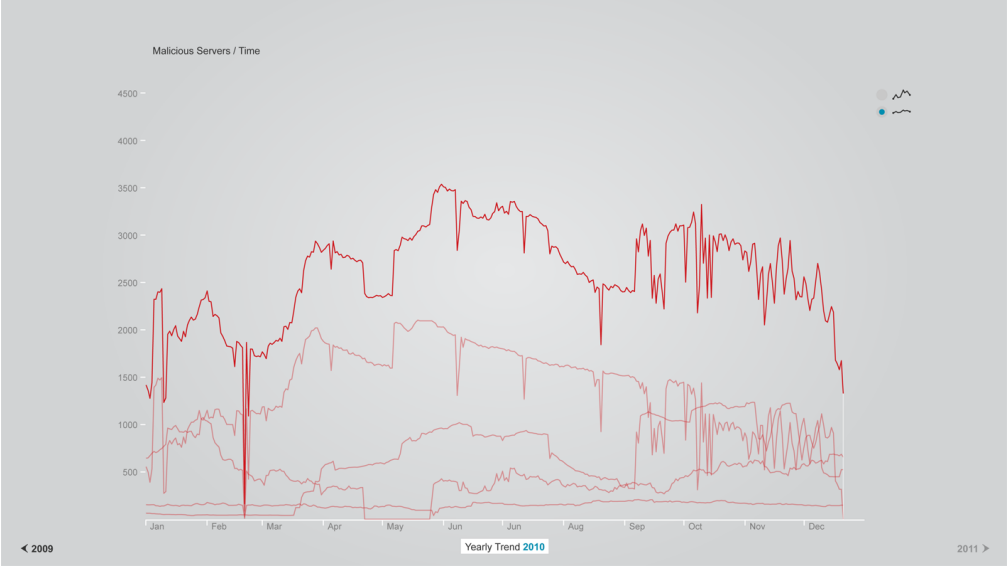

Figura 3.4: Trend Chart. Sono visualizzati gli andamenti del numero di server malevoli nelle reti lungo tutto il corso dell'anno. Ogni linea corrisponde ad un diverso tipo di attività malevola.

Figura 3.5: Timeline: in alto la versione compatta, sotto quella estesa. Permette in ogni punto dell'applicazione di modificare in tempo reale il periodo di tempo selezionato mediante la semplice interazione con i due cursori di inizio e fine periodo.

gior spazio possibile, in questa forma il periodo selezionato è evidenziato dalle due etichette di inizio e fine periodo e non sono visibili i livelli di attività registrati.

La forma estesa della Timeline permette all'utente di visualizzare oltre al periodo selezionato i livelli di maliciousness giorno per giorno rappresentati da barre di altezza proporzionale al numero di server malevoli attivi, inoltre sono presenti due bottoni per permettere lo scorrimento orizzontale che consentono di selezionare anche periodi di tempo distanti dall'attuale.

Il passaggio da compatta ad estesa è effettuato al passaggio del mouse sulla Timeline stessa, allo stesso modo la Timeline passerà in forma compatta nel caso il cursore esca da questa.

Header

L'header occupa la parte superiore dell'applicazione ed è sempre presente ed attivo in ogni visualizzazione Globale, mentre nelle visualizzazione a livello Autonomous System è presente ma non fruibile in tutte le sue funzionalità.

L'header fornisce all'utente l'opportunità di filtrare i risultati per meglio evidenziare alcune caratteristiche. I tipi di filtri applicabili sono:

Activity Filter Questo filtro consente di filtrare il tipo di attività visualizzata tra cinque categorie: attività totali, C&C, malware, phishing, spam. Utilizzando questo filtro tutte le view e la Timeline sono filtrate secondo l'attività selezionata. Scegliendo di filtrare per una specifica tipologia di attività le view e la Timeline si modificano in modo da mostrare la percentuale dell'attività prescelta rispetto al totale delle attività registrate.

Country Filter In modo del tutto simile all'Activity Filter il Country Filter permette di filtrare le informazioni visualizzate in modo da mostrare solo i dati inerenti ad uno specifico stato attraverso un menu a tendina. Selezionando uno stato attraverso questo filtro tutte le visualizzazioni, compresa la Timeline, verranno filtrate mostrando soltanto i dati relativi a quello stato, e la geographical map sarà automaticamente centrata sullo stato selezionato.

Tracked AS L'utente che volesse tenere traccia di uno specifico AS ha la possibilità di marcare quest'ultimo ed inserirlo così in una lista di tracked AS. Il menù tracked AS prsenta all'utente la lista di AS marcati, questi sono resi più visibili anche all'interno delle altre view mediante l'utilizzo di particolari marcatori grafici. Questo strumento è particolarmente importante per assicurare una continuità alla ricerca nello spostamento tra le diverse schermate.

Search Nell'angolo in alto a destra dell'applicazione è sempre presente un box per la ricerca. Quest'ultima può avvenire tramite indirizzo IP o numero identificativo di un AS. Inserendo uno di questi due oggetti il sistema selezionerà automaticamente sulla visualizzazione attiva l'AS a cui l'indirizzo IP od il numero identificativo appartiene. In questa maniera è possibile trovare facilmente un oggetto di cui si conosce l'esistenza, verificare a quale AS appartiene un determinato indirizzo IP, e così via.

L'impostazione di ognuno di questi filtri ha un preciso impatto a seconda della visualizzazione all'interno della quale ci troviamo.

Figura 3.6: Bubble Header. L'header contiene i filtri e le funzioni di tracking degli AS.

3.1.2 Autonomous System View.

La sezione AS View comprende le tre visualizzazioni : History Chart, Service Migration Screen e Service Longevity Chart. Queste visualizzazioni forniscono all'utente un livello di dettaglio maggiore sul comportamento dell'AS scelto, sui server ospitati e forniscono inoltre indicazioni sulle possibili migrazioni da un AS ad un altro.

History Chart.

La schermata History Chart è stata concepita per fornire all'utente un'idea dell'andamento nel tempo dei parametri dell'AS scelto, è composta da un grafico in cui sono mostrati i valori.

Una serie di bottoni nella parte superiore dello schermo consente di spostarsi tra diversi tipo di grafico:

Servers visualizza il numero di server malevoli ospitati dall'AS, i dati sono mostrati attraverso un grafico multilinea, l'asse delle ascisse rappresenta il tempo, sulle ordinate invece è presente il numero di server, ogni linea diversa rappresenta un diverso tipo di attività malevola.

Score visualizza lo score dell'AS calcolato da FIRE. Il tempo occupa l'asse delle ordinate il punteggio ottenuto quello delle ascisse.

Rank visualizza l'andamento della posizione in classifica. Il tempo è presente sull'asse delle ordinate mentre la posizione in classifica sulle ascisse.

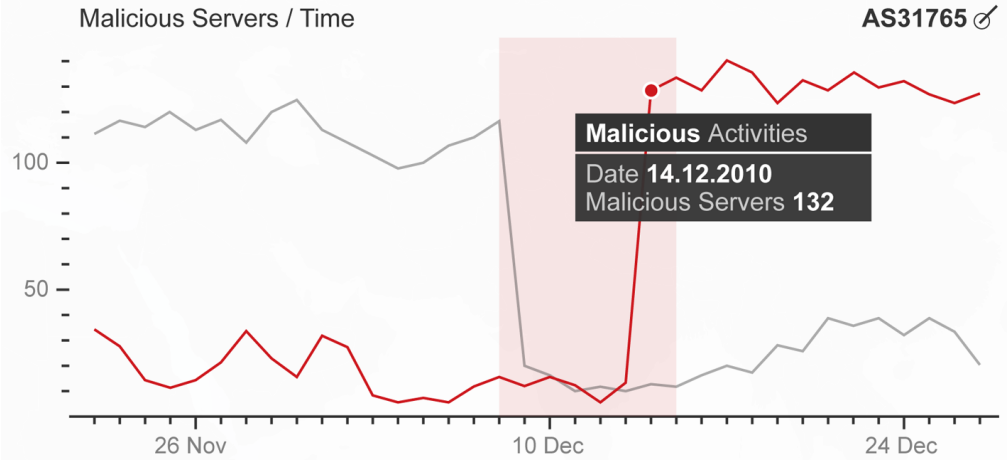

Figura 3.7: History Chart. Permette di analizzare l'andamento dell'attività malevola in uno specifico AS nel periodo di tempo selezionato.

Service Longevity Chart.

Nonostante FIRE prediliga, nell'assegnazione del malicious score, gli AS che presentano un'attività malevola stabile è stato osservato che alcune reti presentano server con un'attività molto più irregolare di altre: su alcune reti si trovano server che occupano un indirizzo IP stabile per molti giorni mentre, all'opposto, altre reti presentano server che pur mantenendo uno stesso indirizzo fisico hanno un'attività intermittente nel tempo.

La schermata service longevity chart è costituita da un "grafico a punti", le righe del grafico rappresentano i diversi IP malevoli mentre le colonne rappresentano i giorni, in ogni cella è mostrato un marcatore rosso solo nel caso in cui l'indirizzo della riga corrispondente si presenti attivo nel giorno della rispettiva colonna. Si noti che ogni marcatore può corrispondere ad una diversa attività o anche ad un insieme di attività (su una stessa macchina fisica possono essere presenti più servizi malevoli).

Serie non interrotte di marcatori sulla medesima riga rappresentano un server malevolo che continua indisturbato la sua attività, serie con interruzioni potrebbero rappresentare server malevoli che subiscono interruzioni del servizio di connettività come anche server malevoli "che cercano di mantenere un basso profilo, comunque indice dell'attuazione di una qualche politica di controllo.

La service longevity chart è raggiungibile sia dalla Bubble Map che dalla Geographical Map, gli AS considerati tolleranti sono segnalati con un opportuno effetto grafico. Il calcolo del livello di tolleranza legato all'AS vedere Sezione 3.3.

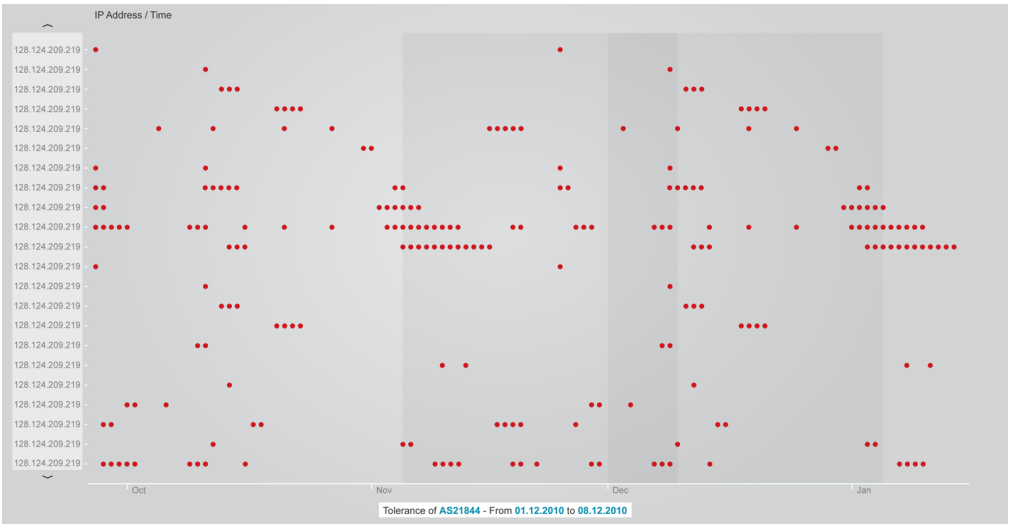

Figura 3.8: Service Longevity Chart. Permette di visualizzare i tempi di attività dei singoli server maligni ospitati dall'AS, ordinati per IP. Ogni punto rappresenta un giorno di attività del server.

Service Migration Screen.

La schermata di service migration evidenzia la capacità di BURN di riconoscere fenomeni di shutdown (decrementi improvvisi dell'attività malevola dell'AS preso in considerazione) e, al contrario, di attivazione (aumenti improvvisi dell'attività malevola in altri AS) all'interno delle reti.

In questa schermata vengono proposti all'utente dei fenomeni di shutdown rilevati nel periodo scelto. Selezionando uno shutdown vengono mostrate una serie di alternative corrispondenti alle altrettante attivazioni in diversi AS ordinate per compatibilità nello shutdown selezionato. Per esempio, se in un dato periodo è stato evidenziato un calo di 100 server corrispondenti ad attività di phishing, questo avrà una alta compatibilità con quegli AS che nello stesso periodo di tempo hanno registrato un incremento di circa 100 server di phishing.

La posizione geografica degli AS coinvolti nella migrazione è visualizzata cliccando su una delle alternative proposte per la migrazione, dove gli AS sono rappresentati come punti non animati e linee connettono sorgenti (l'AS dove è stato registrato uno shutdown) e destinazioni (AS con attivazioni compatibili).

3.1.3 Bubble

In questa sezione discutiamo i bubble, descriviamo l'oggetto grafico, i suoi attributi e il suo comportamento. Esponiamo infine un problema presentatosi durante lo sviluppo dell'applicazione e il nostro approccio alla sua soluzione.

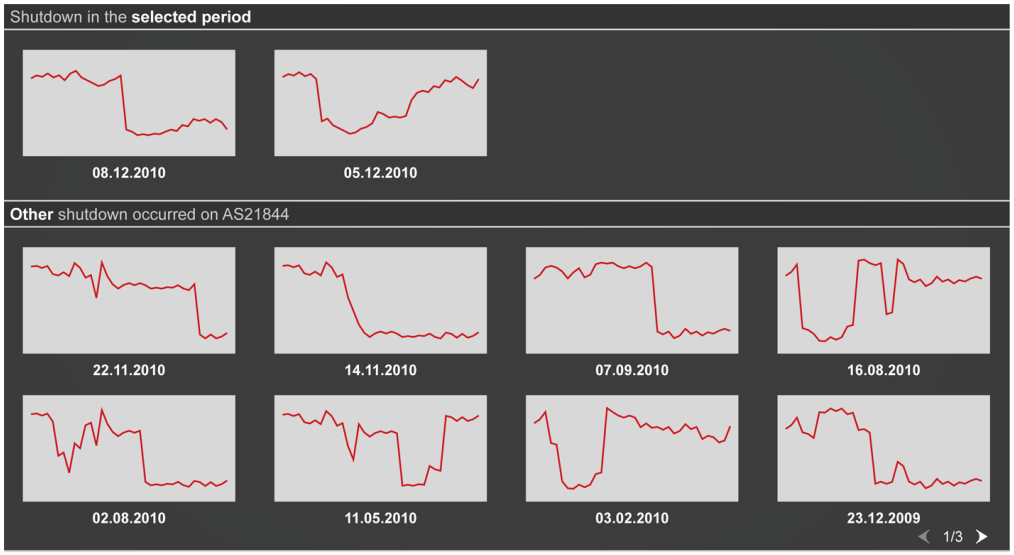

Figura 3.9: Service Migration Screen. Attraverso questa visualizzazione possiamo esplorare le migrazioni proposte da BURN ed associate ad un certo shutdown.

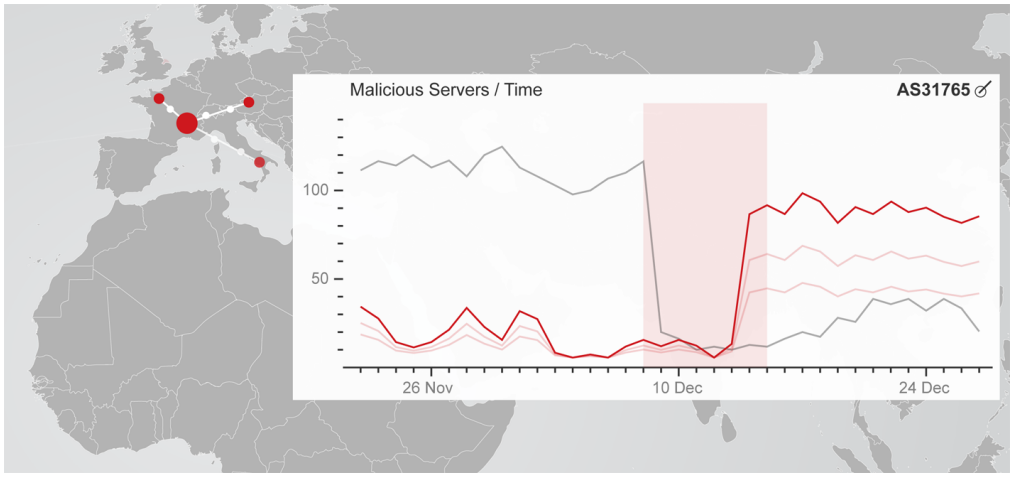

Figura 3.10: Service Migration Screen: dettaglio migrazione.

Bubble.

Chiamiamo bubble la rappresentazione assegnata al singolo AS che all'interno delle schermate di BURN, molte delle proprietà dell'AS corrispondono a proprietà visive del bubble.

Maliciousness L'oggetto bubble è stato progettato per monitorare il livello di maliciousness di ogni AS e allo stesso tempo legare il concetto di maliciousness all'intensità dell'attività, Esso è composto da un set di cerchi sovrapposti che modificano continuamente la propria posizione nello spazio, quanto più il livello di maliciousness è alto tanto più il movimento sarà veloce creando una sorta di "vibrazione".

Shutdown Gli As che mostrano uno shutdown nel periodo selezionato sono visualizzati con dimensioni che decsrescono nel tempo. L'effetto grafico è mostrato in loop così che tali AS si possano riconoscere a prima vista. La dimensione originale del bubble è sempre visibile in background, anche durante l'animazione.

Tolerance Gli AS tolleranti sono caratterizzati dallo scurimento del loro colore che gradualmente giunge fino al nero.

Ulteriori informazioni sono visualizzate cliccando sull'AS, in un apposito box:

AS Number Il codice che identifica in modo univoco l'AS in questione.

Name Il nome dell'AS

Owner Intestatario dell'AS

Malicious Score La media del punteggio di maliciousness calcolato da FIRE, sul periodo selezionato

Size La dimensione/20 dell'AS

Location Lo stato entro cui l'AS risiede

Daily Average Malicious Activities Il numero medio di server malevoli presenti nell'AS nel periodo selezionato

C&C Activities Il numero medio di server C&C presenti sull'AS nel periodo selezionato e la loro percentuale sul totale.

Malware Activities Il numero medio di server Malware presenti sull'AS nel periodo selezionato e la loro percentuale sul totale.

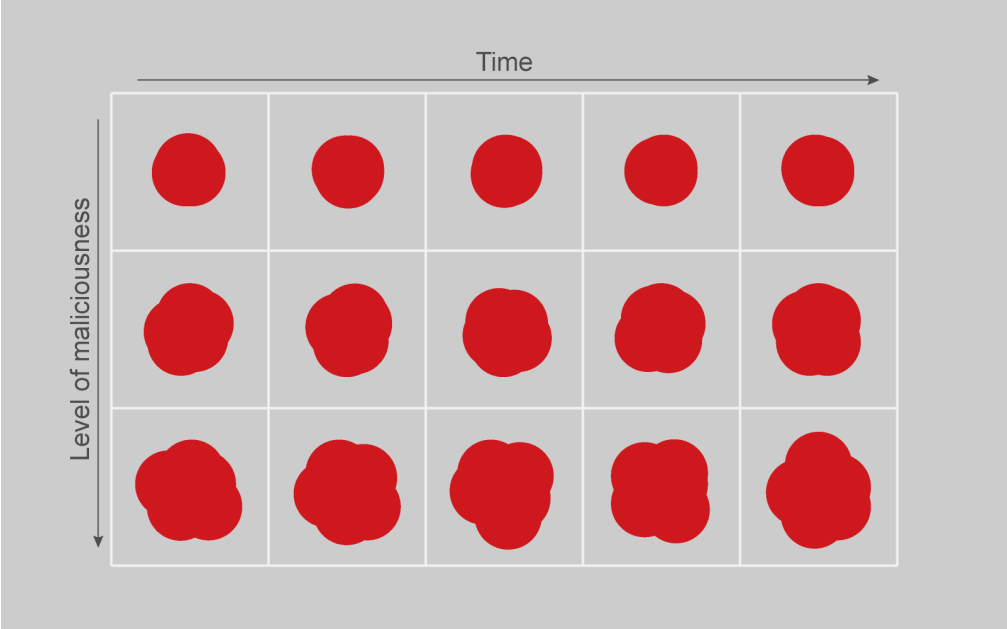

Figura 3.11: Animazione Bubble

Phishing Activities Il numero medio di server Phishing presenti sull'AS nel periodo selezionato e la loro percentuale sul totale.

Spam Activities Il numero medio di server Spam presenti sull'AS nel periodo selezionato e la loro percentuale sul totale.

In aggiunta a queste informazioni è data la possibilità all'utente di marcare l'AS, di accedere alla longevity chart, e nel caso l'AS in questione abbia subito un Shutdown alla Service Migration Chart.

Problematiche di posizionamento.

Una delle problematiche affontate durante lo sviluppo del progetto riguarda i dati forniti da FIRE ed il loro utilizzo in BURN. Il problema riguarda più nel dettaglio la visualizzazione globale Trend Chart. Come abbiamo già visto, la Trend Chart visualizza una sorta di classifica degli AS ordinati per malicious score, l'ordinata dei bubble rappresentanti gli AS fornisce il valore dello score mentre l'ascissa avrebbe dovuto essere impostata automaticamente dal sistema in modo da evitare sovrapposizioni. Questa scelta è stata fatta per dare all'utente, oltre che la semplice relazione d'ordine, anche un'informazione sulla distanza (nello score) tra due AS e poter quindi notare —ad esempio, scorrendo la classifica— cluster di AS aventi valori simili o salti di valore. La prima implementazione dell'algoritmo di posizionamento affidava ai bubble una posizione statica scegliendo l'ordinata in base allo score e l'ascissa facendo si che fosse la più piccola (in modulo) che evitasse le collisioni tra diversi

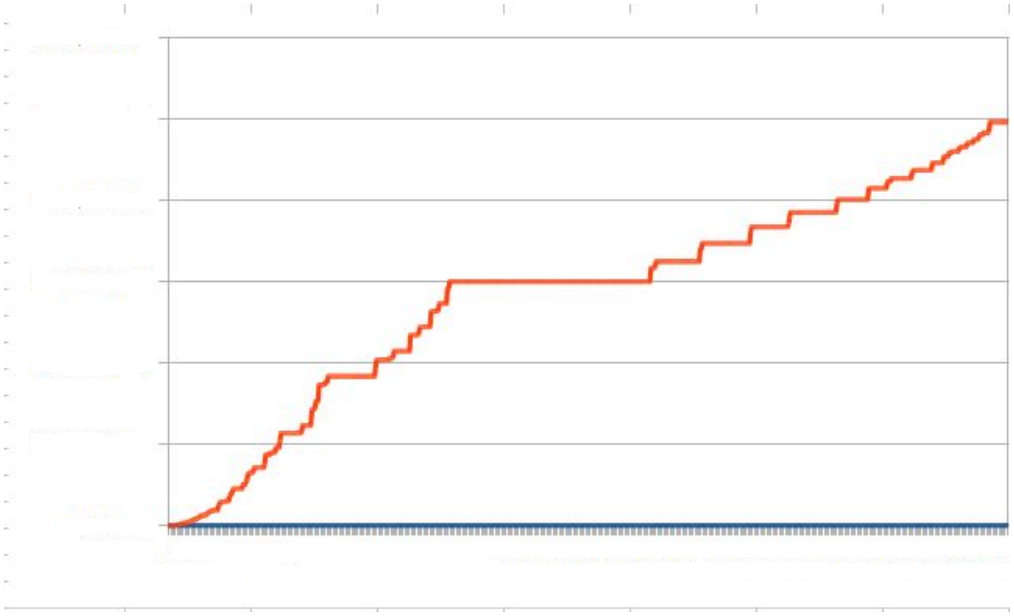

Figura 3.12: I tratti orizzontali rappresentano cluster di AS con il medesimo score.

bubble. Questo tipo di implementazione non teva conto del fatto che nel dataset fornitoci da FIRE esistono AS con il medesimo score; in alcuni casi gli AS aventi lo stesso attributo score sono talmente numerosi da rendere impossibile un approccio alla visualizzazione come quello sopra descritto. In Figura 3.12 possiamo vedere che quasi un quinto degli AS ha il medesimo attributo score e si trova circa a metà classifica; l'indagine di questo fenomeno va oltre gli obiettivi di questa tesi. Abbiamo quindi seguito un diverso approccio conferendo alla posizione dei bubble un certo grado di libertà introducendo un semplice motore fisico in cui sono presenti due tipi di forze:

- Ogni particella associata alla posizione di un bubble è attratta dal punto associato alla sua posizione in base allo score.
- Una forza repulsiva tra le particelle assicura che i bubble non si sovrappongano.

Nel caso di pochi bubble distanziati il comportamento ottenuto è simile al primo approccio, invece in caso di un eccesso di bubble associati allo stesso score, questi si raggrupperanno attorno allo score di riferimento (formando un cluster visivo) anzichè formare una lunga linea.

3.2 Ricerca di migrazioni.

Come già anticipato, BURN include uno strumento di analisi dell'attività delle reti e della ricerca delle migrazioni tra diversi AS. In questo capitolo presenteremo

l'euristica di ricerca della migrazioni, dopo avere fornito al lettore la terminologia utilizzata.

3.2.1 motivazione

FIRE pone di fronte a due diversi aspetti dell'analisi dell'attività malevola che possono spingerci a questo tipo di indagine. Il primo è rappresentato dallo studio della longevità dei server. Esistono alcune categorie di server malevoli che mostrano una vita media dei server stessi molto breve e praticamente costante. Sorge spontanea la domanda: cosa accade ad un server che scompare improvvisamente? Ad oggi sappiamo che una buona percentuale dei server quando bloccati dall'AS attende semplicemente un certo periodo di tempo prima di riattivarsi sul medesimo indirizzo fisico, il restante si divide tra server che si trasferiscono ad un diverso indirizzo IP all'interno dello stesso AS e server che vengono trasferiti ad un diverso AS. Non viene considerata l'ipotesi di uno spegnimento definitivo del server in analisi poiché, analizzando il grafico in Figura 3.4 possiamo notare che esistono categorie di server malevoli per le quali il numero di server globali rimane praticamente costante nel tempo. Da qui l'ipotesi che, a fronte di un improvviso calo all'interno di una data rete, debba corrispondere un aumento dell'attività in una diversa rete.

Il secondo aspetto è rappresentato dall'esperienza. Esistono casi documentati in cui è chiara la migrazione da un AS non più così ospitale ad uno diverso. Uno dei casi più famosi (arrivò ad occupare le prime pagine dei giornali) è il caso della RBN. Il caso in questione risale alla fine del 2007, allora era risaputo che la RBN ospitasse una vasta gamma di attività malevole responsabili di un numero significativo di attacchi, truffe e tentativi di phishing. Una volta che il caso fu reso di dominio pubblico le attività malevole sulla rete incriminata diminuirono velocemente per poi migrare verso altre reti. Come discusso in [6], studi approfonditi del fenomeno sono riusciti a tracciare alcuni degli spostamenti delle attività presenti sulla RBN, ad esempio verso l'AS Abdallah Internet Hizmetleri.

3.2.2 Definizione e terminologia utilizzata

E' chiaro quindi che il primo passo per la ricerca di una migrazione da un AS ad un altro sia il riconoscimento di una diminuzione di attività interna di uno specifico AS. Non siamo però interessati ad una qualsiasi diminuizione di attività ma concentriamo la nostra attenzione sui decrementi di attività dovuti a dei fenomeni di depeering o di intervento dei gestori della rete, cioè fenomeni che possano portare ad un trasferimento massivo di servizi tra due AS. Come già detto, siamo alla ricerca di una migrazione di servizi da una rete ad un'altra, d'ora in poi chiamate rispettivamente *sorgente* e *destinazione*.

Definiamo una migrazione come composizione di due fasi: una fase *shutdown* e una fase *activation*. La fase di *shutdown* interessa l'AS *sorgente* ed è caratterizzata da un improvviso decremento del numero di server maligni rilevati all'interno della rete. La fase di *activation* viceversa interessa l'AS *destinazione* ed è caratterizzata da un aumento del numero di server malevoli. La fase di shutdown potrebbe verificarsi sia in seguito ad una deattivazione dei server malevoli prima di trasferirli ad un nuovo AS sia in seguito all'inibizione da parte dell'AS sorgente della connettività di macchine ritenute malevole costringendo i criminali ad emigrare su un diverso AS. In entrambi i casi il numero di server maligni sull'AS sorgente scende improvvisamente; questo evento sarà seguito da un aumento dell'attività sull'AS destinazione. Il nostro sistema marca questo comportamento come una possibile migrazione. L'euristica prende in considerazione anche migrazioni da una singola sorgente a destinazioni multiple.

3.2.3 Euristica

In questa sezione forniamo i dettagli sugli algoritmi di ricerca degli shutdown, di ricerca delle migrazioni e di calcolo della compatibilità di una particolare migrazione.

Caso uno-a-uno

Per ogni giorno i, che chiameremo *current day* analizziamo il numero di host malevoli in ogni AS utilizzando due finestre scorrevoli nel tempo. La prima delle due finestre, *observation window*, si estende dal giorno OW_b a OW_e, la lunghezza della finestra di osservazione è $\hat{W} = OW_e - OW_b$ dove OW_b e OW_e sono entrambi precedenti a *current day*. La seconda finestra, *current window*, si estende da CW_b a CW_e, la lunghezza della finestra è quindi $W = CW_e - CW_b$, $\hat{W} > W$, i giorni CW_b e CW_e sono posizionati rispettivamente in $OW_e + 1$ ed in *current day*. In altre parole mentre la *observation window* deve precedere *current day* *current window* si posiziona esattamente tra la *observation window* e *current day*.

Chiamiamo rispettivamente $\hat{\mu}$ e $\hat{\sigma}^2$ il numero medio e la varianza del numero di server maligni ospitati nell'AS considerato e calcolati utilizzando i dati corrispondenti alla *observation window*. Chiamamo rispettivamente μ ed σ^2 il numero medio e la varianza del numero di server maligni ospitati dall'AS nel periodo corrispondente a *current window*. L'idea generale è che quando la current average μ è significativamente inferiore alla observed average $\hat{\mu}$ consideriamo l'AS corrente in *shutdown*. Più nello specifico andremo a testare l'ampiezza della differenza tra le due medie utilizzando un test parametrico.

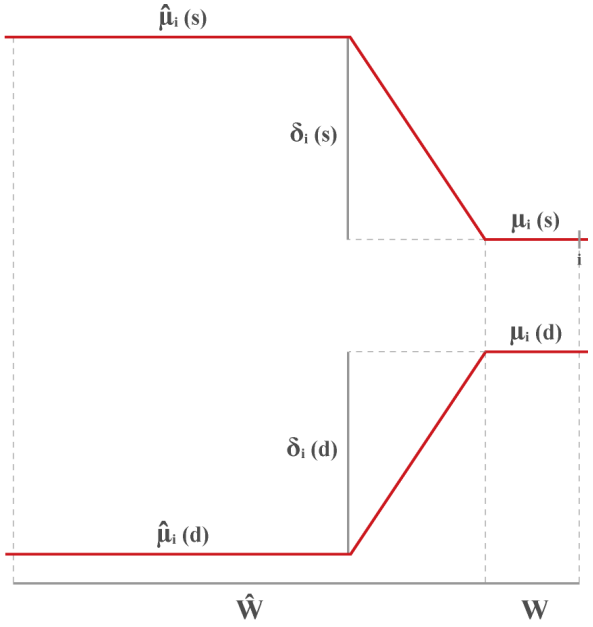

Figura 3.13: Definizione dei parametri per la rilevazione delle migrazioni.

Riconoscimento shutdown e migrazioni Quando la current average μ è significativamente inferiore alla observed average $\hat{\mu}$ consideriamo l'AS corrente in *shutdown*; più precisamente, definiamo lo scostamento dalla media corrente come $\delta = \hat{\mu} - \mu$, se questo scostamento è superiore a $\hat{\mu} \cdot \bar{\delta}$ dove $\bar{\delta} \in [0, 100\%]$ allora lo shutdown è rilevato. Assumiamo che uno shutdown riguardi una percentuale notevole di servizi e che si completi in un tempo relativamente breve. Vogliamo, date le caratteristiche delle due finestre ($\hat{W}$ e W) e la soglia $\hat{\mu} \cdot \bar{\delta}$, decidere se la differenza della media delle due popolazioni è almeno pari alla soglia scelta. Per fare questo decidiamo di impostare un test statistico con media e varianza ignota, supponendo inoltre che le varianze incognite delle due popolazioni siano uguali. In aggiunta notiamo che i dati non sono abbastanza numerosi da giustificare l'utilizzo del teorema centrale del limite quindi imposteremo quindi un t-Test.

Prima di impostare il test notiamo che, nonostante non siamo a conoscenza della varianza delle popolazioni che andremo a confrontare, queste provengono dalla stessa rete e da periodi di tempo adiacenti, è quindi ragionevole supporre che la le due popolazioni abbiano stessa varianza incognita. Definiamo le ipotesi utilizzate nel test sulla differenza tra le medie:

$$H_0 : \hat{\mu} - \mu < \hat{\mu} \cdot \bar{\delta} \tag{3.1}$$

$$H_1 : \hat{\mu} - \mu > \hat{\mu} \cdot \bar{\delta} \tag{3.2}$$

Un nuovo shutdown è registrato ogni qualvolta il test di impostato rifiuta l'ipotesi

H_0 in favore di H_1.

Più formalmente $\hat{\mu} = \hat{\mu}_i = \hat{\mu}_i(a)$, $\mu = \mu_i = \mu_i(a)$, e $\delta = \delta_i = \delta_i(a)$ dove $a \in \mathcal{AS}$ indica un AS, e $\mathcal{AS}$ è l'insieme di tutti gli AS.

Le variabili qui utilizzate sono riassunte nella figura[rif].

Definiamo il set shutdown $\mathcal{S}_i$ come il set che soddisfa la seguente condizione:

$$\mathcal{S}_i = \left\{ a \in \mathcal{AS} \mid \frac{(\hat{\mu}(a) - \mu(a)) - \bar{\delta}\hat{\mu}(a)}{S_p\sqrt{1/n + 1/m}} \geq t(\alpha) \right\} \tag{3.3}$$

Per il quale cioè il test impostato rifiuta H_0 in favore di H_1 ed α è il livello di significatività del test e dove

$$S_p = \sqrt{\frac{(n-1)S^2 + (m-1)S^2}{n+m-2}} \tag{3.4}$$

Per il quale cioè il test impostato rifiuta H_0 in favore di H_1, α è il livello di significatività del test.

Questi AS sono sorgenti candidate per una possibile migrazione. Le migrazioni sono cercate per ogni AS segnalato in shutdown cercando un AS che presenti uno scostamento di attività simile ma di segno opposto, cioè cercando per ogni shutdown una corrispondente activation in un AS diverso.

In condizioni ideali, questo significa che per un dato AS sorgente s, cerchiamo una destinazione d tale che $\delta_i(s) = -\delta_i(d)$.

Più precisamente definiamo il *migration set* come:

$$\mathcal{M}_i = \left\{ (s,d) \in \mathcal{S}_i \times \mathcal{AS}\backslash\{s\} \mid \begin{array}{l} \delta_i(s) < 0 \\ \delta_i(d) > 0 \end{array} \wedge \left| \frac{\delta_i(s) + \delta_i(d)}{\delta_i(s)} \right| \leq \bar{\Delta} \right\}, \tag{3.5}$$

dove $\delta_i(s)$ e $\delta_i(d)$ sono rispettivamente lo scostamento dell'AS sorgente (candidato) e dell'AS destinazione.

$\bar{\Delta}$ è la soglia di accettazione della migrazione e rappresenta nello specifico il rapporto limite tra la compensazione degli scostamenti (tra la sorgente e destinazione) e lo scostamento della sorgente; $\bar{\Delta} = 0$ rappresenta il caso limite in cui lo scostamento dell'AS sorgente corrisponde esattamente allo scostamento dell'AS destinazione, a meno del segno. In altre parole questa soglia tiene conto del fatto che le organizzazioni criminali potrebbero trasferire solo parte dei loro servizi (in caso di reti di grandi dimensioni è poco probabile che tutti i server malevoli siano controllati da una stessa fonte). Similmente al caso di riconoscimento dello shutdown impostiamo un test che ci permetta di decidere se lo scostamento $\delta_i(d)$, è tale da verificare $\left|\frac{\delta_i(s)+\delta_i(d)}{\delta_i(s)}\right| \leq \bar{\Delta}$ Suddividiamo i due casi a seconda del valore del rapporto $\left|\frac{\delta_i(s)+\delta_i(d)}{\delta_i(s)}\right|$ che chiameremo *compensazione*:

reti sovracompensate $\delta_i(d) > \delta_i(s)$

Dobbiamo verificare se:

$$\delta_i(d) \leq \bar{\Delta}\delta_i(s) - \delta_i(s) \tag{3.6}$$

Impostiamo le ipotesi del test:

$$H_0 : \delta_i(d) = \bar{\Delta}\delta_i(s) - \delta_i(s) \tag{3.7}$$
$$H_1 : \delta_i(d) < \bar{\Delta}\delta_i(s) - \delta_i(s) \tag{3.8}$$

Rifiutiamo H_0 in favore di H_1 se verifichiamo:

$$\frac{(\hat{\mu}(a) - \mu(a)) - (\bar{\Delta}\delta_i(s) - \delta_i(s))}{S_p\sqrt{1/n + 1/m}} \leq -t(\alpha) \tag{3.9}$$

dove α è il livello di significatività del test.

reti sottocompensate $\delta_i(d) < \delta_i(s)$

Verifichiamo se:

$$\delta_i(d) \geq \delta_i(s) - \bar{\Delta}\delta_i(s) \tag{3.10}$$

Impostiamo le ipotesi del test:

$$H_0 : \delta_i(d) = \bar{\Delta}\delta_i(s) - \delta_i(s) \tag{3.11}$$
$$H_1 : \delta_i(d) > \bar{\Delta}\delta_i(s) - \delta_i(s) \tag{3.12}$$

Rifiutiamo H_0 per H_1 se verifichiamo:

$$\frac{(\hat{\mu}(a) - \mu(a)) - (\delta_i(s) - \bar{\Delta}\delta_i(s))}{S_p\sqrt{1/n + 1/m}} \geq t(\alpha) \tag{3.13}$$

al solito, α è il livello di significatività del test.

Compatibility score

BURN facilita la revisione manuale delle migrazioni trovate utilizzando una funzione di compatibilità. La compatibilità è definita come una relazione d'ordine "$<_C$" definita sul set delle migrazioni $\mathcal{M}_i$ come media della funzione di compatibiltà $C^{(j)} : \mathcal{S}_i \times \mathcal{AS} \mapsto [0, 1]$ tra l'AS sorgente e l'AS destinazione rispetto alle attività malevole di tipo $j \in \mathcal{J} = \{phishing, malware, spam, bot\}$.

Semplificando, la funzione compatibility quantifica la discrepanza tra due AS in termini di ogni tipo di attività. Ad esempio, un AS con un decremento di 10 server dedicati al phishing e 5 al malware, è più compatibile con un AS che ha 10 nuovi server

che mostrano attività di phishing e 5 di malware che ad uno avente un incremento di 9 server phishing, 3 spam e 1 malware. Più formalmente:

$$C^{(j)}(s,d) := \frac{\min_{a\in\{s,d\}} \delta^{(j)}(a)}{\max_{a\in\{s,d\}} \delta^{(j)}(a)}, \tag{3.14}$$

Dove $\delta^{(j)}_{min}$ e $\delta^{(j)}_{max}$ sono il minimo e il massimo valore dello scostamento $\delta^{(j)}(\cdot)$. Questa funzione quantifica il rapporto tra il minimo e il massimo scostamento, in numero di servizi di tipo j. Definiamo quindi *compatibility score* la media pesata delle funzioni di compatibilità calcolata su tutte le attività in $\mathcal{J}$ come:

$$C_{s,d} := \frac{\sum_{j\in\mathcal{J}} C^{(j)}(s,d)\cdot\delta^{(j)}(s)}{\sum_{j\in\mathcal{J}} \delta^{(j)}(s)} \tag{3.15}$$

dove i pesi sono gli scostamenti nell'AS sorgente.

Caso uno a molti

Ci siamo occupati, fino a questo punto, di riuscire ad evidenziare delle possibili migrazioni da un AS ad un altro in seguito ad un trasferimento di servizi tra questi. In uno scenario realistico, però, è possibile e probabile che -a fronte di un trasferimento necessario da una rete- si scelga di effettuare questo trasferimento non verso una singola destinazione ma verso un insieme di AS destinazione. L'approccio che utilizzeremo è molto simile al caso di singola destinazione ma più generale.

L'insieme $\mathcal{S}_i$ degli shutdown è costruito esattamente come nel caso uno-a-uno: non siamo più alla ricerca di una singola destinazione ma dobbiamo identificare delle tuple di destinazioni.

Notiamo che la cardinalità dell'insieme delle possibili destinazioni, dato uno shutdown sorgente, cresce in modo lineare con la dimensione dello shutdown (fino ad arrivare al limite ad una destinazione per ogni servizio in meno nell'AS sorgente) ma le combinazioni possibili crescono in modo combinatorio.

In aggiunta a questo, vi è il fatto che quanto più grande è la cardinalità del set di AS destinazione quanto meno questo risulterà probabile. Un insieme di destinazione molto grande sarà formato dal molti AS che compensano solo in piccola parte la caduta dei servizi dell'AS sorgente. Il loro contributo all'effettiva compensazione dei servizi dell'AS sorgente è dubbio ed è difficile distinguere quei contributi provenienti da un effettivo trasferimento di servizi da quelli dovuti alla naturale fluttuazione del valore analizzato.

Per evitare questi problemi, limitiamo la dimensione massima del set di destinazione a K AS. Per ridurre ulteriormente il numero di tuple di AS prese in considerazione per ogni shutdown, filtriamo $\mathcal{AS} = \mathcal{AS}_i$ ammettendo solo set di AS dove ognuno degli elementi partecipa alla compensazione per almeno $\bar{\Gamma} = 20\%$. Questo aiuta ad

evitare le situazioni in cui un singolo AS è effettivamente la destinazione mentre gli altri AS nel set sono inseriti in modo casuale solo per riempire la differenza tra il decremento e l'incremento di attività.

Per costruire l'insieme delle migrazioni $\mathcal{M}_i$ a partire da un dato insieme shutdown $\mathcal{S}_i$ calcoliamo, per ogni $s \in \mathcal{S}_i$, l'insieme filtrato:

$$\bar{\mathcal{AS}}(s) := \left\{ a \in \mathcal{AS} \backslash \{s\} \mid \frac{|\delta_i(s) + \delta_i(a)|}{\delta_i(s)} \geq \bar{\Gamma} \right\} \tag{3.16}$$

A questo punto possiamo costruire:

$$\mathcal{M}_i := \left\{ (s, D) \mid s \in \mathcal{S}_i, D \in \bigcup_{k=1}^{K} \bar{\mathcal{AS}}(s)^k \mid \frac{|\delta_i(s) + \delta_i(D)|}{|\delta_i(s)|} \right\} \tag{3.17}$$

dove $\delta_i(D) = \sum_{a \in D} \delta_i(a)$. Notiamo che in questa definizione di $\delta_i(D)$ ci permette comunque di calcolare il compatibility score tra s e D.

Per la realizzazione del test statistico si è seguito il medesimo approccio del caso uno-a-uno. Ricordiamo che la media della somma è la somma delle medie e la varianza della somma è la somma delle varianze.

3.3 Classifica degli AS tolleranti

I server malevoli spesso sono caratterizzati da una vita piuttosto breve: la ragione di questo è da trovarsi principalmente nel bisogno dei server di rendersi difficilmente rintracciabili e quindi perseguibili in caso di indagini da parte delle forze dell'ordine ma anche nel tentativo di mantenere un basso profilo evitando così a monte la possibilità di ripercussioni legali.

Gli autori di FIRE hanno analizzato la durata della vita media di un server malevolo e i risultati sono sintetizzati in Figura 3.14; si è scelto di suddividere i risultati in base alla tipologia di server malevolo considerato. Possiamo notare dai grafici che la durata media di un server malevolo, generalmente inferiore ai quattro giorni, è molto breve se paragonata al tempo medio di vita di un IP generico (fig in alto a sinistra).

Fanno eccezione a questo comportamento i server ospitanti malware: questi mostrano un comportamento diverso e una durata media della vita non regolare; il fenomeno è dovuto al fatto che spesso questi server sono ospitati da AS molto permissivi o complici delle loro attività malevole. Ricordiamo che gli AS sono un'unità autonoma nello stabilire le proprie politiche di security e quindi responsabili di quest'ultime.

Sulla base di queste osservazioni possiamo stimare il livello di permissività di un AS qualsiasi monitorando la longevità dei server ospitati da quest'ultimo. A livello intuitivo un AS sarà considerato maligno quando la lunghezza della vita dei server

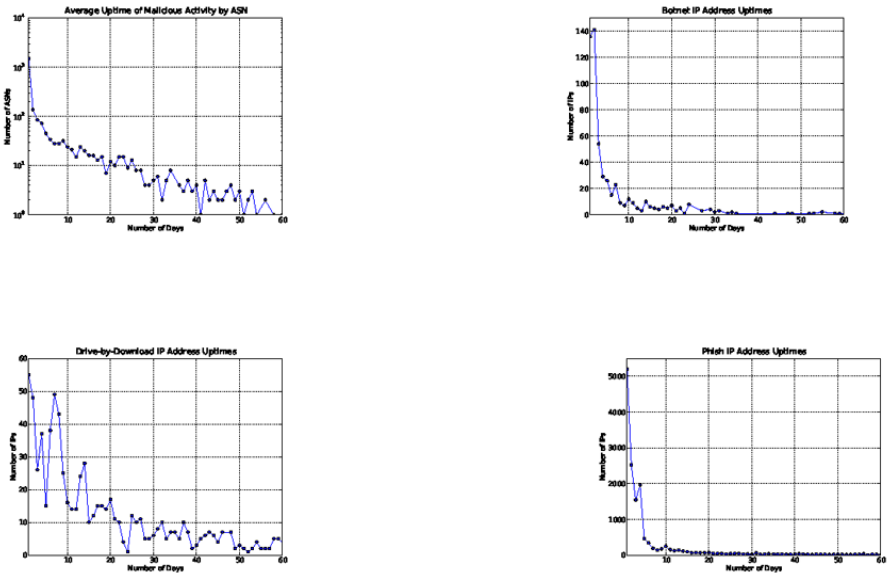

Figura 3.14: Vita media di un IP. Da in alto a destra abbiamo: IP generico, phishing, malware,C&C. Immagine tratta da [6].

malevoli è superiore alla lunghezza di vita media t_m che un server mostra su una rete non permissiva. FIRE ha stimato il valore $t_m = 4$ [6].

3.3.1 Euristica

BURN calcola la longevità dei server malevoli presenti sulla rete come il numero di giorni consecutivi di attività rispetto ad un minimo di giorni di attività richiesti per poterli marcare come tollerati. Più formalmente, dato un AS $a \in \mathcal{AS}$ definiamo la tolleranza rispetto ad un singolo host $IP \in a$ come la longevità dell'IP:

$$T_i(IP) := \frac{\sum_{t=0}^{\tau} \mathbf{1}_{IP}(i+t)}{\tau} \tag{3.18}$$

dove $\mathbf{1}_{IP}(i+t) = 1$ se l'IP è attivo nel giorno $i+t$ e 0 altrimenti, e i è il giorno corrente.

La tolleranza dell'intero AS è calcolata come

$$T_i(a) := \frac{\sum_{IP \in a} T_i(IP)}{|a|} \tag{3.19}$$

dove $|a|$ è il numero di server malevoli nell'AS.

3.4 Dettagli sulle tecniche di visualizzazione

Una delle sfide con cui ci siamo voluti misurare progettando BURN è il superamento delle classiche codifiche visive come forma colore dimensione ect. queste hanno una sicura e provata valenza a cui però l'abbinamento di strutture visuali più complesse come layout animati e basati su principi fisici e visualizzazioni dinamiche può essere un importante aiuto nel processo di riconoscimento dell'informazione attraverso l'aggregazione di più dati grezzi.

3.4.1 Uso del colore

BURN propone una visualizzazione che utilizza un singolo colore, questa scelta va in controtendenza rispetto alla maggioranza degli altri sistemi di visualizzazione creati nell'ambito della security i quali utilizzano spesso differenti gradazione di colore per rappresentare diversi gradi di sicurezza o insicurezza dei sistemi, grado di rischio, tipologia di attacchi, eccetera.

L'utilizzo all'opposto di un singolo colore ci permette di raggiungere tre obiettivi:

- le tonalità rosse sono spontaneamente associate ad una sensazione di rischio
- Utilizzare diversi colori per marcare diversi tipi di attività malevola avrebbe potuto inconsciamente portare l'utente ad associare alle attività diversi gradi di pericolosità.
- l'utilizzo di un unico colore ci ha dato la possibilità di ridurre in maniera significativa molte delle problematiche inerenti a problemi legati alla visione, come ad esempio il daltonismo o la cecità ai colori.

3.4.2 Animazioni

In questo progetto abbiamo inserito una serie di animazioni, che agiscono sulle bolle animate presenti nella Bubble Chart e nella Geographical Map (quando al maggiore livello di zoom), per i seguenti motivi: arricchire le due mappe sopra citate con variabili visive che permettano l'aggiunta di informazioni senza compromettere la leggibilità delle mappe; inserire elementi che trasmettano all'utente sensazioni visive strettamente legate a ciò che si sta osservando (ad esempio un elemento che si muove freneticamente può trasmettere una sensazione di elevata attività); attirare l'attenzione dell'utente sui fenomeni interessanti che altrimenti rischierebbero di perdersi nella massa delle informazioni. Per l'inserimento delle animazioni è stata condotta una breve ricerca sperimentale, associando alle bubble svariati comportamenti, per studiare quali reazioni e soprattutto quali sensazioni queste suscitassero negli utenti.

Questa breve ricerca, incrociata con la necessità di utilizzare variabili che non interferissero tra loro, poiché i comportamenti rappresentati tramite le animazioni non si escludono l'un l'altro ma potrebbero comparire sulla stessa bubble anche tutti contemporaneamente, ha portato alla scelta di utilizzare animazioni che agissero su variabili differenti. Più precisamente sono state utilizzate tre animazioni, che agiscono rispettivamente sulle variabili di forma, dimensione e colore. La prima è sempre attiva, mentre la seconda e la terza agiscono come filtro visivo e si attivano per evidenziare la presenza di un determinato fenomeno.

Maliciousness Il livello di malevolenza di un AS è legato all'animazione del bubble associato, ogni bubble è formato da un serie di cerchi sovrapposti ed in continuo movimento attorno ad un centro gravitazionale, la velocità di questo movimento è proporzionale al punteggio emphmalicious score dell'AS, Questo effetto, mostrato in Figura 3.11 mira a trasmettere la sensazione che ogni AS sia composto da più elementi, vivi e attivi (i server che compongono la rete) e dà una sensazione di maggiore attività con l'incremento dello score associato. Questa animazione permette all'utente di identificare immediatamente all'interno di un gruppo di AS quelli che mostrano un comportamento malevolo e di associare inconsciamente il livello di attività malevola all'intensità del movimento

Shutdown Gli AS registrati in shutdown nel periodo di tempo selezionato sono caratterizzati da un'animazione di graduale diminuzione della dimensione e dell'opacità del bubble, fino alla totale scomparsa. La diminuzione del numero di server interni alla rete è suggerita dal decremento della dimensione del bubble, grandezza legata appunto al numero di server malevoli ospitati. La dimensione originale dell'AS viene sempre mantenuta sullo sfondo dell'animazione.

Tolerance L'animazione legata alla tolleranza agisce sulla luminosità del bubble legato all'AS tollerante. La luminosità del colore diminuisce gradualmente, scurendo il bubble e dando l'impressione visiva di una rete corrotta. dove l'attività malevola viene tollerata, senza prendere le necessarie contromisure per mitigare la situazione.

3.4.3 Dati

BURN è stato sviluppato con l'intento di creare una visualizzazione che rendesse più fruibili i dati presenti in FIRE. Il database di FIRE contiene informazioni su AS che si ritiene ospitino server malevoli, per ogni AS si conoscono il numero di server maligni ospitati, il tipo di attività malevola che ogni server si sospetta ospitare e il punteggio "malicious score" indicante il grado di malignità dell'AS calcolato come in [6].

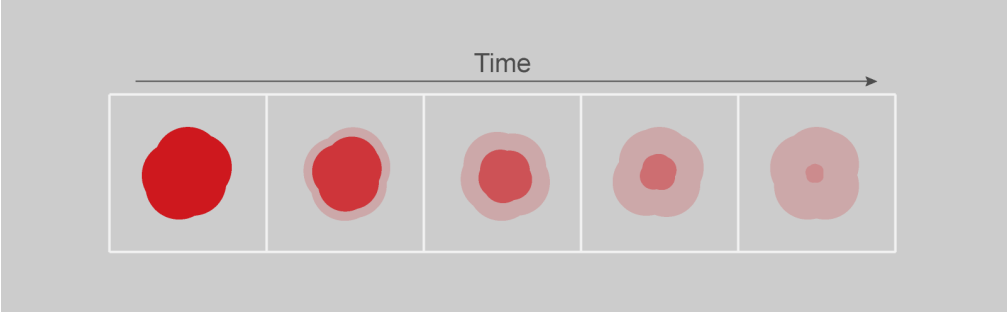

Figura 3.15: Animazione shutdown.

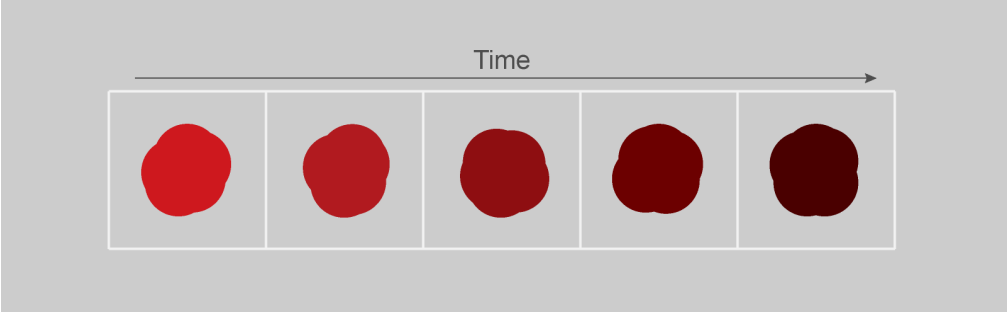

Figura 3.16: Animazione AS tollerante.

BURN utilizza e ottimizza i dati già presenti su FIRE. Nello specifico calcola l'integrale di tutte le variabili numeriche presenti nel database associandolo al loro valore giornaliero, grazie a questo stratagemma è stato in grado di computare semplici statistiche (come ad esempio la media mensile) in un tempo costante e non dipendente dalla lunghezza del periodo preso in considerazione ma soggetto invece solo da ai legati al primo e all'ultimo giorno del periodo.

Tutti i valori integrali sono calcolati online non appena i dati sono disponibili sul database di FIRE. Inoltre, su base giornaliera, vengono eseguiti gli algoritmi di ricerca delle migrazioni e analisi della longevità tramite una serie di script batch. Questi algoritmi sono particolarmente efficienti perchè implementati su una finestra temporale scorrevole: per analizzare il giorno successivo è sufficiente aggiungere il nuovo dato e sottrarre il più vecchio ad ogni valore (Sezioni 3.2 e 3.3).

3.5 Scenari d'uso

In questa sezione saranno descritti tre tipici scenari di utilizzo di BURN utilizzando dati reali forniti dal database di FIRE (i dati vanno da gennaio a dicembre 2010). In questo arco temporale il nostro sistema ha riconosciuto 63 shutdown, associati a questi shutdown il sistema ha proposto 2400 migrazioni uno-a-uno e circa 1.500.000

migrazioni a destinazioni multiple (una,due,tre destinazioni). Il numero così alto di migrazioni proposte da BURN è giustificato dalla scelta della minima dimensione della migrazione riconosciuta (4–5 server). In ogni modo il compatibility score ci permette di ordinare le migrazioni in base alla loro rilevanza e verosimiglianza, le migrazioni ritenute rilevanti sono 5–10 per ogni shutdown.

Trovare, dato un periodo di tempo gli AS più malevoli L'obiettivo dell'analista è di esaminare reti con un alto livello di maliciousnes nel 2010. Per raggiungere l'obiettivo ha bisogno innanzi tutto di trovare le reti con livello di maliciousness più alto sia per quanto riguarda lo score generale sia per tipo di attività malevola.

Lanciando l'applicazione è visualizzata l'ultima settimana di attività nella Bubble Chart (Figura 3.1). Per trovare picchi di attività malevola nell'arco dell'intero anno l'utente accede alla Trend Chart (Figura 3.4) che visualizza i livelli di attività malevola globale e la loro variazione nell'arco dell'anno. A questa scala si riconosce facilmente il picco di attività tra la fine di maggio e la prima metà di giugno.

Utilizzando la Timeline (Figura 3.5) situata sotto la Bubble Chart possiamo selezionare, utilizzando i due apposti cursori il periodo selezionato e la Bubble Chart viene immediatamente aggiornata mostrando i dati relativi al periodo selezionato, vengono mostrati a partire dall'alto gli AS che mediamente nel periodo hanno mostrato un'attività malevola maggiore.

Con pochi click riusciamo a identificare AS21844 come l'AS più malevolo nel periodo di tempo attorno al picco di attività malevola. E' interessante notare che con score leggermente inferiori sono classificati AS aventi numero di server malevoli più alto, ma considerati meno maliziosi a causa delle loro grandi dimensioni. In aggiunta cliccando sul bubble associato all'AS21844 sono visualizzate le informazioni riassuntive nel relativo dialog box.

Finita l'analisi di questo AS, rimanendo nella sezione history, attraverso il menù a tendina della lista Tracked AS, l'analista seleziona gli altri AS che si era segnato, ed accorgendosi così che il terzo AS segnato, l'AS21740, è caratterizzato da un elevato numero di server implicati in attività di C&C. Per avere ulteriore conferma di ciò che ha appena notato, l'analista torna alla Bubble Chart e, utilizzando l'activity filter, filtra l'attività visualizzata per C&C, e utilizzando il bottone apposito riordina la mappa in base all'attività appena selezionata. Questa azione porta ad un aggiornamento dei dati visualizzati e l'AS21740 guadagna la prima posizione, come maggiore AS implicato in attività di tipo C&C. Questo conferma la congettura che l'AS21740 può essere il leader globale nell'attività C&C nell'intorno del picco di attività. Selezionando dall'activity filter anche le altre tipologie di attività presenti, l'analista può velocemente trovare gli AS maggiormente implicati in ogni tipologia di attacco.

Trovare ed evidenziare le possibili migrazioni di attività In questo scenario un esperto di sicurezza monitora l'attività di una botnet coinvolta in attacchi di DDoS. La botnet è notoriamente controllata da alcuni server C&C situati in AS noti, ad esempio AS36536. Questi server in aggiunta sono stati recentemente segnalati come inattivi. L'obiettivo dell'esperto è di indagare la veridicità di queste segnalazioni. A differenza dello scenario precedente dove abbiamo utilizzato il search box a partire dalla mappa geografica (con l'obiettivo di attivare lo zoom automatico sull'AS cercato), l'AS qui è cercato all'interno della Bubble Chart (Figura 3.1). Questo attiva l'apertura del box dettagli realativo al bubble, esattamente come nel caso di click sul bubble. L'animazione come riportata in Figura 3.15 sulla bubble indica la presenza di uno shutdown recente.L'utente clicca sull'icona relativa allo stato di shutdown dell'AS per visualizzare una lista di grafici che riportano l'andamento dell'attività malevola nel periodo associato dallo shutdown. L'utente sceglie di cliccare sullo primo (e più recente) shutdown. Questo apre il Service Migration Screen (Figura 3.10), dove una mappa geolocalizzata mostra il luogo dell'AS sorgente e le corrispondenti possibili destinazioni. Spostando il cursore sul punto rosso associato all'AS sorgente appare un piccolo grafico che mostra l'andamento dello shutdown. A questo punto per una ricerca manuale della migrazione all'interno delle alternative proposte è sufficiente spostare il cursore tra le destinazioni suggerite. I grafici associati allo shutdown e all'activation sono sovrapposti e mostrati in trasparenza. Due connessioni tra sorgente e possibile destinazioni sono caratterizzate da impulsi frequenti e alta opacità dell'AS destinazione. Questo pattern visivo suggerisce una significativa compatibilità tra shutdown e activation e attira l'attenzione dell'utente. Passando il muose su una di queste due migrazioni notiamo che questa viene evidenziata insieme ad una seconda migrazione, il sistema suggerisce all'utente una migrazione verso una destinazione multipla confermata dall'alta compatibilità verso le destinazioni: AS44050 e AS32592.

Tracciare un attacco Questo scenario sottolinea come BURN rende facile investigare, partendo da un evento isolato, il costesto all'interno del quale l'evento di è verificato.

Nello specifico un'e-mail sospetta contenente un URL che sospettiamo essere phishing, questo attira l'attenzione dell'analista perchè il corristondente IP (75.126.207.92, ottenuto con un semplice servizio whois) risulta appartenere ad un server connesso ad un AS considerato tollerante, i server malevoli connessi a questo AS mostra infatti un tempo di vita medio molto superiore alla media. L'utente visualizza l'ultima settimana di dati nella Geographical Map (Figura 3.2) per avere un'idea della situazione globale e ottenere specifiche informazioni sugli stati, le informazioni sono date al passaggio del mouse in un apposito box. Attraverso il box search nell'angolo in alto

a destra l'utente localizza l'AS che ospita l'IP sospetto. Una volta trovato il sistema si centra automaticamente sulla Germania e vengono mostrati i dati riferiti all'AS cercato, evidenziandolo sulla mappa. Allo stesso tempo l'analista nota l'AS cercato che a causa dell'alto livello di maliciousness a causa dell'animazione di questo.

L'attenzione dell'esperto è altresì attirata dal'animazione legata al colore del bubble associato all'AS, il colore di quest'ultimo tende lentamente al nero evidenziando un AS con un alto livello di tolleranza (Figura 3.16). Un bottone sula lato destro del bubble suggerisce di controllare la tolleranza dell'AS aprendo la longevity chart, dove gli IP dell'AS associati ad attività malevole posso essere visualizzati e fatti scorrere verticalmente fino a trovare l'IP di nostro interesse. In questa visualizzazione server longevi sono caratterizzato da lunghe sequenze di punti adiacenti (Figura 3.8). Come sospettato, il server in questione mostra recentemente attività di phishing mentre in passato era caratterizzato da una forte attività C&C. (Notare che posizionando il cursore su un punto, l'opacità dei punti appartenenti ad altre categorie si abbassa permettendo di identificare cambiamenti nel tipo di attività).

In questo capitolo sono è stato presentato BURN, dagli elementi dell'interfaccia grafica ai dettagli sul funzionamento delle euristiche per finire con la descrizione di tre possibili scenari di utilizzo. Nel prossimo capitolo saranno presentati i risultati degli esperimenti condotti sulla ricerca di shutdown e migrazioni.

4 Analisi sperimentale delle migrazioni

In questo capitolo presenteremo i risultati ottenute con le euristiche presentate in questa tesi, più nello specifico ci concentreremo sull'euristica di riconoscimento degli shutdown e sull'euristica di proposta delle possibili migrazioni a partire dagli shutdown riconosciuti. Siamo stati in grado di riconoscere 63 shutdown nel periodo di tempo a nostra disposizione, di questi ventisei segnano un rapido decremento di più di dieci servizi. Le migrazioni trovate uno-a-uno o uno-a-due sono 61496, di queste 2497 rappresentano una migrazione uno-a-uno mentre le restanti 58999 uno-a-due.

4.1 Metodo e dati

Il datset fornitoci da FIRE copre il periodo di tempo compreso tra 1/1/2010 e il 21/12/2010. Sfortunatamente, mentre gli shutdown proposti possono essere riconosciuti e validati con un'analisi visiva non vi è alcun modo di validare le migrazioni proposte dall'euristica, il dataset in nostro possesso pur riportando dati sui singoli server malevoli non contiene dati sufficienti ad identificare univocamente l'host. D'altra parte non esiste una traccia univoca lasciata da un host connesso ad una rete e che permetta di riconoscerlo qual'ora questo cambi indirizzo fisico. Un'analisi parziale può essere fatta analizzando il comportamento degli host sospettati di essere migrati da un AS ad un altro. Ad esempio, ci aspettiamo che un server che manda messaggi di C&C ad una certa botnet continui a farlo anche dopo la migrazione, o un server ospitante un certo malware continuerà ad ospitarlo anche se spostato ad un'altra rete. Questo tipo di indagine però non sarebbe sufficiente ad assicurare un risultato, è fatto noto che spesso chi controlla server malevoli lavori su commissione dedicando le proprie macchine a compiti diversi nel tempo e rendendo così inutili le analisi basate sulle caratteristiche dell'attività malevola. Arrivando alla radice del problema, non esiste una ground truth per validare le migrazioni trovate.

4.2 risultati

Come riassunti in Tabella 4.1 abbiamo rilevato 63 shutdown rilevati e 2497 migrazioni per una media di 39.6 migrazioni associate ad ogni shutdown. Analizzando il compatibility score questo risulta in media piuttosto basso. Tuttavia oltre il 70%

	Numero di migrazioni.	Compensazione media.	Media compensazione massima per shutdown.
uno-a-uno	2497	0.73	0.97
uno-a-due	58999	0.78	0.99

	Compatibilità media.	Media compatibilità massima per shutdown.
uno-a-uno	0.23	0.78
uno-a-due	0.17	0.93

Tabella 4.1: Caratteristiche delle migrazioni proposte (uno-a-uno ed uno-a-due), i parametri utilizzati per la computazione sono $\alpha = 0.95$, $\bar{\delta} = 66\%$, $W = 5$ e $\hat{W} = 20$

delle migrazioni presenta almeno una migrazione con compatibility score maggiore del 90%. Questo risultato ci permette di affermare che, per la quasi totalità degli shutdown rilevati, siamo stati in grado di localizzare una rete che ha subito un incremento di attività in un periodo compatibile e che le attività che hanno subito un incremento sono compatibili con le attività scomparse dalla rete sorgente.

Nelle tabelle 4.2, 4.3, 4.4 sono riassunti i test di ricerca di shutdown al variare dei parametri. In Tabella 4.2 vediamo il numero di shutdown rilevati al variare del parametro α. Il numero di shutdown rivelati, come ci aspettavamo, aumenta al diminuire di α. Possiamo trovare un numero maggiore di shutdown rinunciando alla qualità di quest'ultimi e includendo anche diminuzioni di attività più rumorose(meno nette). In Tabella 4.3 sono contenuti invece i dati sul numero di shutdown e sul valore della statistica test al variare del parametro $\bar{\delta}$. Diminuendo $\bar{\delta}$ prendiamo in considerazione anche shutdown con uno scostamento δ inferiore e cioè meno profondi, il numero di shutdown restituiti aumenta quanto più δ diminuisce, gli shutdown trovati risulteranno più lievi. Infine in Tabella 4.4 mostriamo i dati riferiti al numero di shutdown rilevati al variare del parametro $\hat{W} = 20$, lunghezza della observation window. Una observation window breve richiede shutdown più rapidi ma è anche più soggetta al rumore del segnale. Il numero di shutdown rilevati in questo caso aumenta al decrescere della lunghezza della observation window.

Osservando il valore della media e della varianza della statistica test notiamo come la media della statistica test aumenti utilizzando un test più permissivo mentre diminuisca con un test più severo. Questo risultato è coerente con il tipo di test impostato nel quale richiediamo che la statistica test sia maggiore di un certo valore, fissato in base ad α.

Limitazioni e sviluppi futuri Nonostante l'obiettivo principale della Bubble Chart sia fornire una classifica degli AS più pericolosi, il numero molto alto di reti con il

α	Numero shutdown.
0.95	63
0.9	81
0.8	123

Tabella 4.2: Numero di shutdown rilevati al variare del parametro α, il numero di shutdown rilevati cresce al diminuire di alpha. I parametri utilizzati per la computazione sono $\bar{\delta} = 66\%$, $W = 5$ e $\hat{W} = 20$.

Compensazione minima.	Numero shutdown.	Media statistica.	Varianza statistica.
0.5	174	2.45	7.42
0.66	63	2.15	10.19
0.85	9	1.40	5.44

Tabella 4.3: Numero di shutdown rilevati e valore dalla statistica del test effettuato al variare $\bar{\delta}$ (compensazione minima). I parametri utilizzati per la computazione sono $\alpha = 0.95$, $W = 5$ e $\hat{W} = 20$.

Lunghezza observation window	Numero shutdown.	Media statistica.	Varianza statistica.
15	84	2.52	15.91
20	63	2.15	10.19
30	45	1.62	2.94

Tabella 4.4: Numero di shutdown rilevati e valore dalla statistica del test effettuato al variare $\hat{W}$ (lunghezza observation window). I parametri utilizzati per la computazione sono $\alpha = 0.95$, $\bar{\delta} = 66\%$ e $W = 5$

medesimo punteggio rende la visualizzazione a tratti confusa, questa limitazione può essere mitigata calcolando gli score con una maggior precisione. Le migrazioni proposte non sono validate, questa limitazione può essere in parte mitigata dall'inclusione di nuovi set di dati in grado di dare informazioni aggiuntive, seppur non complete, sui singoli server malevoli e rendere così possibile un riconoscimento. Ad esempio confrontando il tipo di malware ospitato su un determinato server o confrontando i messaggi di C&C inviati ad una botnet.

5 Conclusioni

In questo capitolo presentiamo le conclusioni della tesi analizzando criticamente i conrtibuti originali proposti e fornisco una panoramica sugli sviluppi futuri.

Le euristiche di ricerca degli shutdown e di ricerca delle migrazioni ci hanno permesso di tracciare i possibili spostamenti di alcuni host malevoli tra diversi AS. Anche se l'assenza di una *ground truth* non permette di validare i risultati ottenuti, le ricerche effettuate su alcuni casi particolari (utilizzati poi per gli scenari) permettono, anche in assenza di validazione, di cogliere la verosimiglianza delle ipotesi. Inoltre, l'esistenza, in molti casi, di almeno una migrazione con alta compatibilità per ogni shutdown registrato rende possibile una completa analisi del fenomeno.

L'applicazione web realizzata permette anche agli utenti meno esperti la fruizione dei dati raccolti (dati che in forma grezza sarebbero risultati incomprensibili). L'esposizione dei dati raccolti, in linea con la strategia di FIRE, ha un importante valore nella lotta alla criminalità informatica, BURN permette di fruire di questi dati in modo più facile ed intuitivo aumentando di molto il numero potenziale di utilizzatori. Inoltre la nostra strategia di visualizzazione permette anche ad analisti o esperti di sicurezza di trarre alcuni vantaggi, le informazioni trasmesse all'utente in modo inconscio o implicito arricchiscono il contesto della ricerca di nuovi elementi permettendo di valorizzare il processo cognitivo portando a nuove intuizioni o deduzioni prima impedite dall'incapsulamento dei dati.

Bibliografia

[1] L. Di Mario, F. Roveta, F. Maggi, G. Caviglia, S. Zanero and P. Ciuccarelli. BURN: Baring Unknow Rogue Networks. In *Proc. of the 8th Intl. Symposium on Visualization for Cyber Security (to appear)*, VizSec '11.

[2] D. Inoue, K. Yoshioka, M. Eto, M. Yamagata, E. Nishino, J. Takeuchi, K. Ohkouchi, and K. Nakao. An incident analysis system nicter and its analysis engines based on data mining techniques. In *Proc. of the 15th intl. conference on Advances in neuro-information processing - Volume Part I*, ICONIP'08, pages 579–586, Berlin, Heidelberg, 2009. Springer-Verlag.

[3] R. Marty. *Applied Security Visualization.* Addison-Wesley Professional, 1 edition, 2008.

[4] L. Masud, F. Valsecchi, P. Ciuccarelli, D. Ricci, and G. Caviglia. From data to knowledge - visualizations as transformation processes within the data-information-knowledge continuum. *Information Visualisation, Intl. Conference on*, 0:445–449, 2010.

[5] A. H. Robinson, J. L. Morrison, P. C. Muehrcke, A. J. Kimerling, and S. C. Guptill. *Elements of Cartography.* Wiley, 6 edition, Mar. 1995.

[6] B. Stone-Gross, C. Kruegel, K. Almeroth, A. Moser, and E. Kirda. Fire: Finding rogue networks. In *Proc. of the 2009 Annual Comp. Security Applications Conference*, ACSAC '09, pages 231–240, Washington, DC, USA, 2009. IEEE Comp. Society.

[7] T. Yu, R. Lippmann, J. Riordan, and S. Boyer. Ember: a global perspective on extreme malicious behavior. In *Proc. of the Seventh Intl. Symposium on Visualization for Cyber Security*, VizSec '10, pages 1–12, New York, NY, USA, 2010. ACM.

[8] C. Ziemkiewicz and R. Kosara. Beyond bertin: Seeing the forest despite the trees. *IEEE Comp. Graphics and Applications*, 30:7–11, 2010.

[9] Ernst Mach. Beiträge zur Analyse der Empfindungen. 1886, pp. 43 ss., 104, 128.