Consortium GARR
8° BORSISTI DAY
"ORIO CARLINI"
MERCOLEDÌ 14 DICEMBRE 2016 - ROMA

Metodi e tecniche per la rilevazione e il contrasto di botnet in reti universitarie

Andrea Balboni

andreabalboni@gmail.com

Tutor: Prof. Michele Colajanni

UNIVERSITAS STUDIORUM MUTINENSIS ET REGIENSIS 1175
UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi - CRIS

Obiettivi del progetto

- **Studio di tecniche e metodi innovativi per l'individuazione e il contrasto di botnet e di server di Comando e Controllo**

- Elementi originali:
  - Acquisizione e integrazione dati da **molteplici sorgenti eterogenee**
  - Focalizzazione sulla correlazione e analisi dei **log DNS**

Analisi focalizzata su DNS

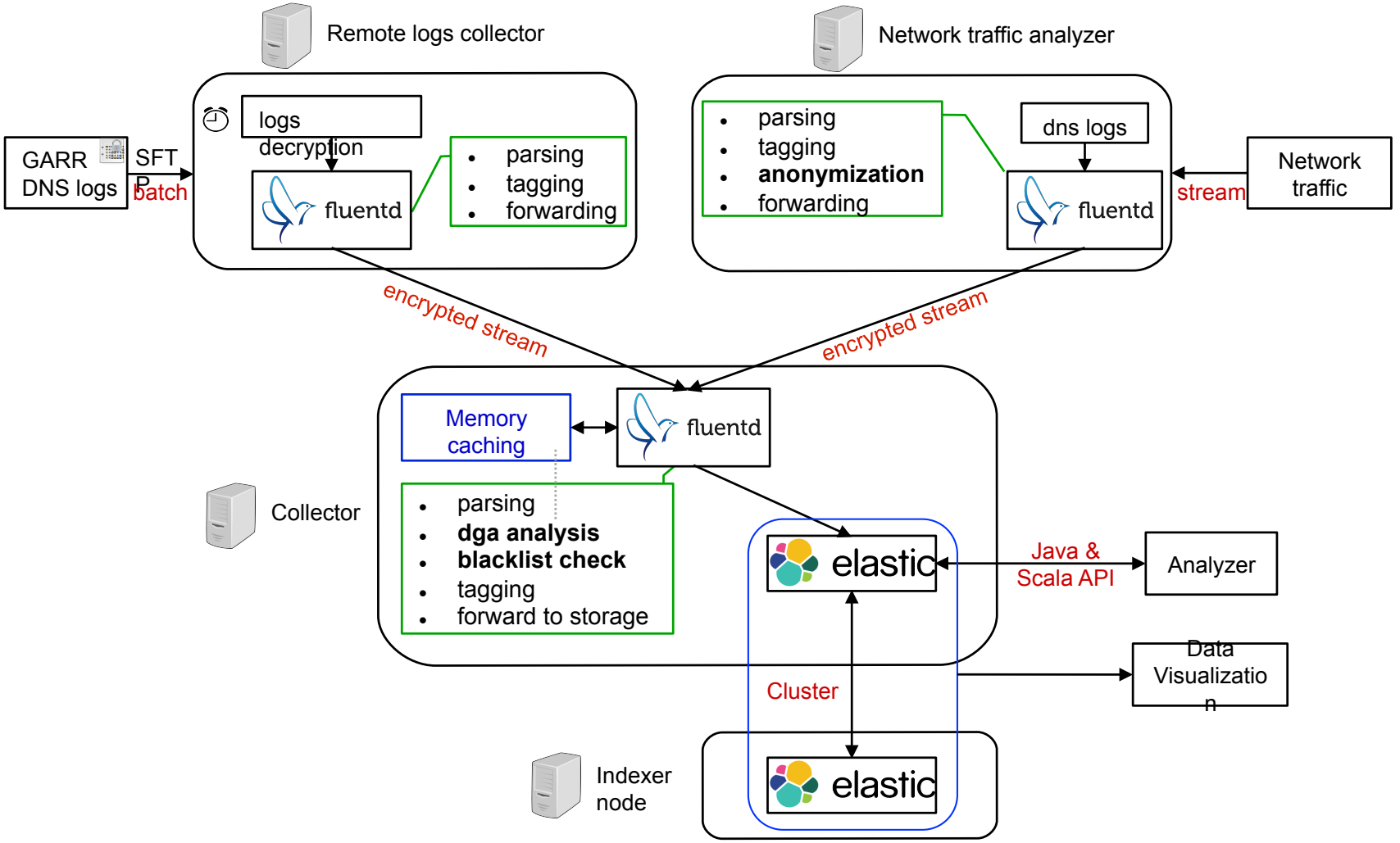
- Le moderne botnet coinvolgono il DNS in diverse fasi:
  - **Comunicazioni** tra bot e server di comando e controllo (C&C)
  - Attività di perlustrazione del bot-master per verificare l'eventuale blacklisting DNS dei **nomi di dominio associati ai bot o ai server di controllo**
- Per diminuire le probabilità di essere individuati, i bot contattano i server di Comando e Controllo e/o i peer attraverso nomi di dominio auto-generati, definiti **DGA**. Es.
  - razzrwsbzum.org
  - jbfygzlcjak.info
- Possibilità di rilevare botnet **indipendentemente dal protocollo** che utilizzano (HTTP, IRC, …)

Risultati dopo il primo anno

- Progetto di un'architettura **distribuita** per l'analisi di grandi quantità di dati in modalità streaming
  - Gestione di **fonti eterogenee**
  - Sistema **scalabile** per storage e indexing
  - **Anonimizzazione** dei dati (come da requisito GARR)

- Realizzazione di algoritmi di analisi basati su euristiche in grado di classificare nomi di dominio e di riconoscere DGA.
  - Il risultato delle analisi non dipende dai valori osservati precedentemente → processo parallelizzabile

Architettura realizzata



Individuazione DGA

- Classificatore realizzato mediante euristiche sulle label dei nomi di dominio
  - lunghezza
  - rapporto vocali/consonanti inconsueto
  - numerosità vocali/consonanti inconsueta
  - assenza di parole di senso compiuto
- Classificatore implementato come plugin custom per fluentd
  - dati analizzati e annotati prima di essere memorizzati e indicizzati
- Ogni record DNS viene analizzato per verificare se il nome di dominio richiesto è presente in blacklist configurabili e aggiornate quotidianamente

Volumi di dati dopo un anno

- Alla fine del primo anno sono state analizzate e indicizzate più di 6 miliardi di query DNS (~ 1.3 TB di dati)

- Segnalati numerosi DGA in 1 anno di traffico:
  - GARR: 159.840 query per **130.548 DGA**
  - UNIMORE: 69.840 query per **61.000 DGA**

- Falsi positivi (domini erroneamente classificati come malevoli)

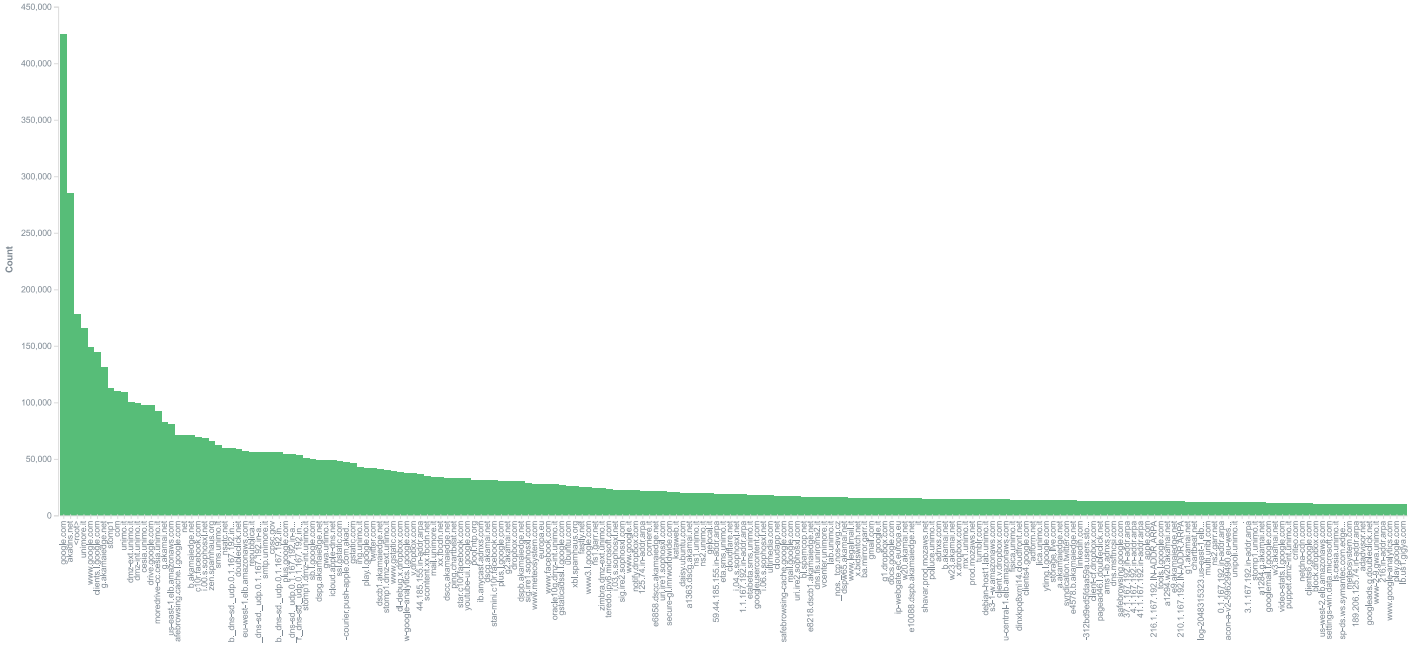
<3%

Attività del secondo anno di ricerca

1. Miglioramento delle prestazioni del sistema di analisi
2. Implementazione di classificatori più robusti basati su tecniche di *machine learning*
3. Analisi di nomi di dominio internazionalizzati (IDN)
4. Risultati: individuazione di nuove tipologie di attacchi

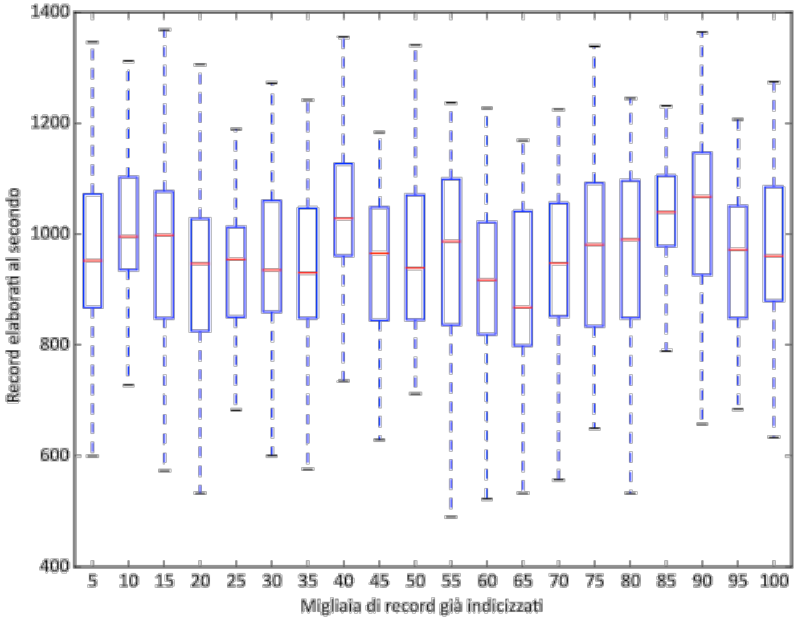
1. Miglioramento delle prestazioni del sistema

- Analisi della frequenza dei nomi di dominio osservati
  - I nomi di dominio appaiono nei record dei log da analizzare con distribuzione di tipo heavy tailed: la maggioranza delle richieste su pochi domini.
  - Pattern indipendente dalla granularità temporale di osservazione



Miglioramento delle prestazioni del sistema di analisi - soluzione adottata

- Introduzione di meccanismi di caching dei risultati delle analisi effettuate sui nomi di dominio
- I risultati relativi ai domini richiesti più frequentemente sono mantenuti in RAM
  - Cache hit rate 93.8%
  - Velocità di analisi e indicizzazione ~ 1000 record DNS/s
  - Prestazioni costanti con la crescita del numero di elementi già indicizzati



2. Classificatore di nomi di dominio

- Implementazione di un classificatore basato su Support Vector Machine
- Scelta delle caratteristiche sintattiche e morfologiche del nome di dominio:
  - f1. lunghezza del nome di dominio
  - f2. numero di label contenute nel dominio
  - f3. massima lunghezza delle label del dominio
  - f4. numero di cifre contenute nel nome
  - f5. numero di caratteri alfabetici contenuti nel nome
  - **f6. numero di caratteri speciali**
  - **f7. lunghezza totale di parole di senso compiuto**
  - f8. numero di vocali
  - f9. numero di consonanti

Classificatore di nomi di dominio - Dataset

Fonte: nomi di dominio osservati durante il primo anno di ricerca, Alexa top 500 e blacklist pubblicamente disponibili

- 3673323 nomi di dominio etichettati come leciti
- 224092 nomi di dominio etichettati come DGA

- Training set: 5000 elementi per ogni classe

- Risultati della classificazione:
  - Accuracy: 0.9804
  - False positive rate: 0.0196
  - False negative rate: 0.0000

3. Analisi di nomi di dominio internazionali

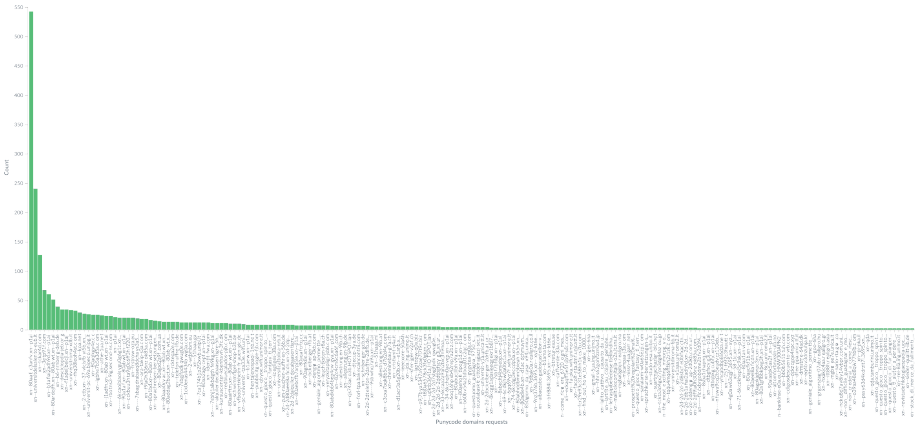
- I nomi di dominio IDN vengono registrati sempre più frequentemente
- La codifica punycode consente di esprimere attraverso l'utilizzo dei soli simboli della codifica ASCII qualsiasi parola rappresentabile con codifiche più complesse come UTF-8
- Meccanismo di codifica:
  - la stringa è preceduta dal prefisso xn-
  - seguono tutti i caratteri già rappresentabili mediante codifica ASCII preceduti dal simbolo -
  - segue una successione di numeri in base 36 che identificano caratteri e delimitatori relativi ai simboli non altrimenti rappresentabili

Esempi:

- башпсп.рф → xn-80ab7baj4b.xn-p1ai
- università.it → xn--universit-y1a.it

Dataset disponibile

- I record DNS analizzati e indicizzati relativi a nomi codificati in punycode rappresentano lo 0.0007% delle richieste
  - attualmente ~ 1.806.472.776
- Analisi della distribuzione dei nomi IDN richiesti
  - Distribuzione heavy tailed



- Filtering dei nomi:
  - 39,11% domini non validi, errori utenti
  - 11,87% record TXT di sistemi antimalware (sophos, kaspersky, …)
  - 49.02% domini utilizzabili per le analisi

Metodologia adottata basata su quattro fasi

1. Conversione del nome di dominio da codifica punycode a UTF8

2. Applicazione di algoritmi di machine learning per il riconoscimento della lingua dei componenti del nome di dominio ottenuti dopo la conversione

3. Sulla base della lingua riconosciuta, traduzione automatica delle varie componenti del nome di dominio dalla lingua individuata alla lingua inglese. Non applicato se si rileva la lingua italiana

4. Classificazione mediante SVM

4. Risultati

- Nessuno dei nomi di dominio IDN analizzati è stato classificato come DGA
- Tuttavia, è stato verificato l'aumento della tipologia di attacco definito: **IDN Homograph Attack**
  - Nomi di dominio codificati con simboli visivamente simili a quelli dell'alfabeto latino
  - L'utente non esperto non si accorge della differenza e contatta un sito malevolo
- Ad esempio, si sono riscontrate diverse richieste per siti con **ш** (carattere sha cirillico) utilizzato al posto di **w**

шшш.uniroma2.it (xn--x1aaa.uniroma2.it)

Contrasto a IDN Homograph Attack

Metodologia automatica per l'identificazione di nomi di dominio potenzialmente illeciti (utilizzata dai principali browser Web)

1. Conversione da punycode a UTF8
2. In caso di errori al punto precedente, all'utente viene mostrata la codifica punycode
3. Se il nome contiene simboli particolari oppure contiene simboli appartenenti a più di due alfabeti, all'utente viene mostrata la codifica punycode
4. Se il nome contiene numeri in sistemi di numerazione differenti viene mostrata la codifica punycode
5. Se il nome contiene caratteri invisibili, all'utente viene mostrata la codifica punycode
6. Se il nome contiene pattern pericolosi, viene mostrata la codifica punycode

Sviluppi: Integrazione con il sistema di analisi

- È in fase di implementazione l'algoritmo per l'individuazione di attacchi di tipo omografico

- L'integrazione nel sistema di analisi consente di segnalare tempestivamente all'amministratore di rete le richieste per nomi di dominio potenzialmente sospetti

- Contromisure possibili:
  - Segnalazione all'utente
  - Blocco del traffico verso il dominio individuato