ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

La rete va in analisi

Traffic Analysis e Information Sharing

Simone Bonetti

Workshop GARR 2019

Presentazione

CERT-UniBo nasce nei primi anni del 2000 per esigenze di sicurezza.

Lavoro a CERT-UniBo dal 2005, mi occupo principalmente di analisi del traffico e della manutenzione e sviluppo della rete di analisi.

ALMANet è una rete distribuita geograficamente per buona parte della regione Emilia Romagna (da Rimini a Bologna). Lo spazio di indirizzi è formato da due classi B e qualche classe C.

Traffic Analysis: perché la facciamo

La scelta di fare analisi del traffico di rete è maturata principalmente per questi motivi:

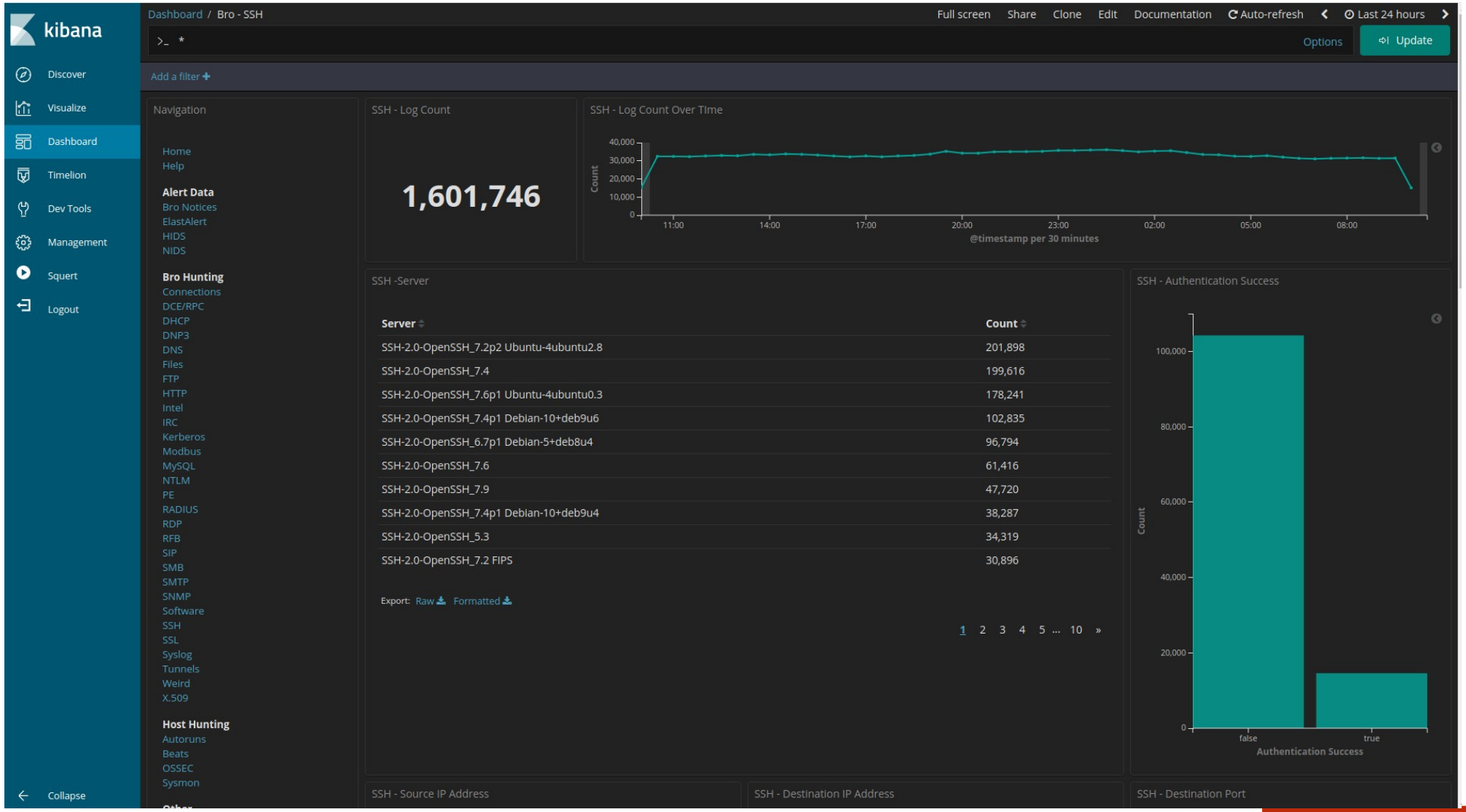
- Negli anni dal 1998 al 2000, la polizia postale era di casa a UniBo
- Supporto alla diagnosi delle problematiche di networking (“quando qualcosa non va è colpa delle reti”)
- Valutazione dei sistemi di network da implementare: c’è sempre discrepanza tra le caratteristiche dichiarate dal produttore e quelle effettive.
- La Traffic Analysis permette di essere più reattivi in caso di compromissione.

Traffic Analysis: Con quali strumenti

- Analizzatore di protocollo (tshark, ngrep).
- NIDS (Network Intrusion Detection System, d'ora in poi IDS).
  - Passaggio ad IDS Open source (snort, suricata, zeek [ex bro])
  - Adozione di Security Onion
- NBADS (Network Behaviour Anomaly Detection System, d'ora in poi ADS) per avere un analisi più in profondità
- Sistemi di analisi passiva del DNS

- Stiamo usando e testando strumenti di VA (Vulnerability Assessment), NV (Network Visibility: ntopng), IS (Information Sharing: misp) e IR (Incident Response: the hive)

Attività ssh



Conficker → EternalBlue

Correva l’anno...fine 2008 inizio 2009. La piaga Conficker colpisce UniBo. Si tratta di un worm che sfrutta una vulnerabilità non corretta del servizio di rete Microsoft Windows. L’aggiornamento che risolve il problema era già disponibile nel novembre del 2008.

In pratica al destinatario del worm veniva inviato in porta 445/tcp un pacchetto contenente l’exploit e l’indirizzo da cui scaricare il malware che una volta mandato in esecuzione iniziava a propagarsi sempre su porta 445/tcp.

Dopo aver “combattuto” per mesi con decine di “vittime” al giorno, abbiamo chiesto ed ottenuto la chiusura sul bordo della porta 445.

Questo caso è simile ad un altro di qualche anno fa che sfruttava sempre la porta 445 (EternalBlue, primavera del 2017). La policy di qualche anno prima ci ha “salvato”, almeno in prima battuta. Abbiamo subito avviato un attività di VA per identificare le possibili vittime.

Come nel caso precedente l’aggiornamento che risolveva il problema c’era ma era stato ignorato.

Mirai la botnet che non scorderai...mai

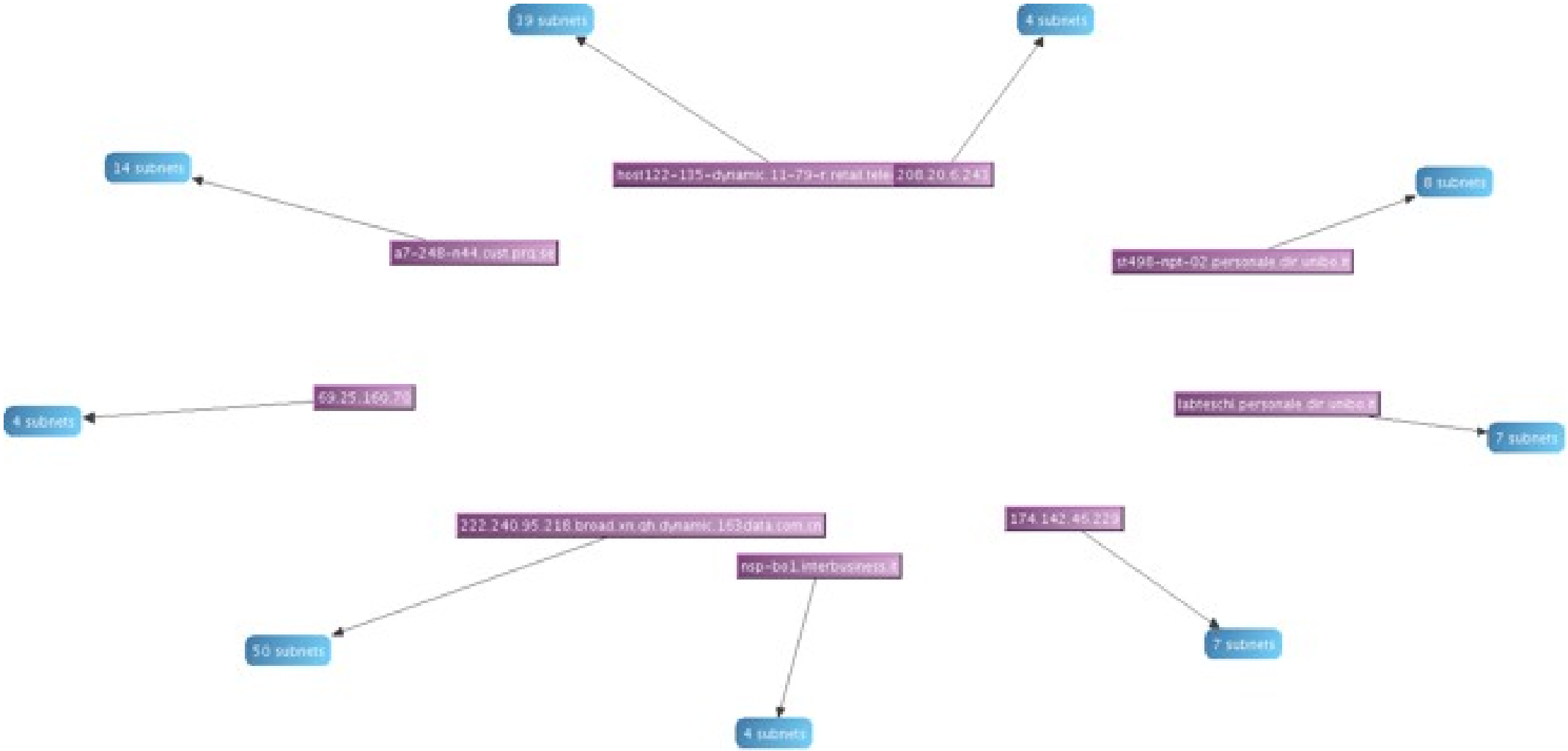
Mirai è un malware progettato per sfruttare vulnerabilità dell'IoT.

Nell'agosto del 2016 iniziano a sentirsi i primi effetti.

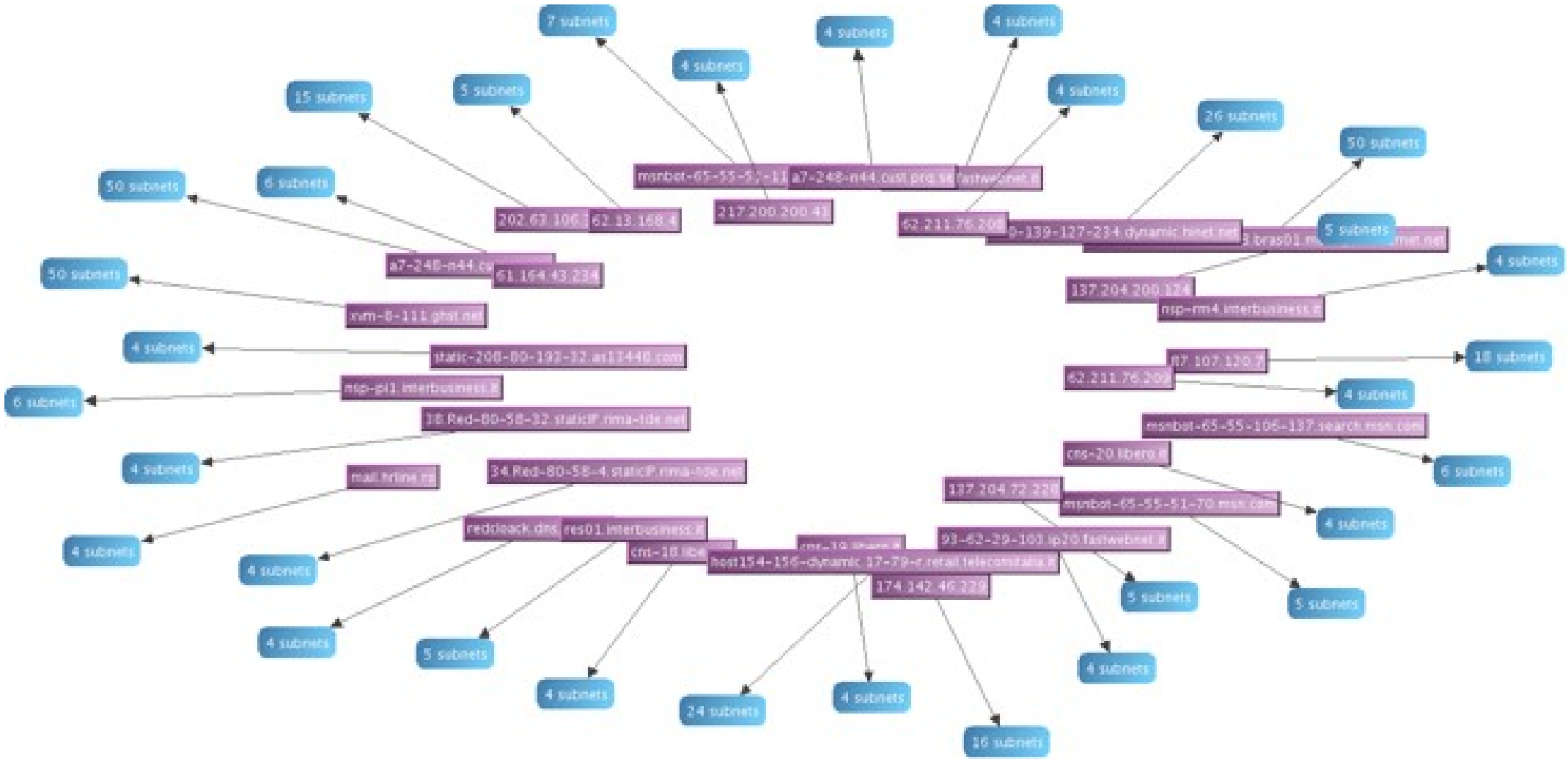
Nella primavera di quell'anno le nostre sonde rilevano un notevole aumento dell'attività in porta 23 (telnet). Quello che emergeva dall'uso dell'analizzatore di protocollo, era il tentativo di distribuire malware per diverse architetture: ARM, Sparc, PowerPC, insolite anche per la nostra rete.

Nel giro di breve tempo, seguendo anche i consigli di shadowserver (https://www.shadowserver.org/), abbiamo deciso di impostare politiche più restrittive (sul link di uscita verso la rete GARR) riguardanti protocolli in chiaro o "inutili" (es. chargen).

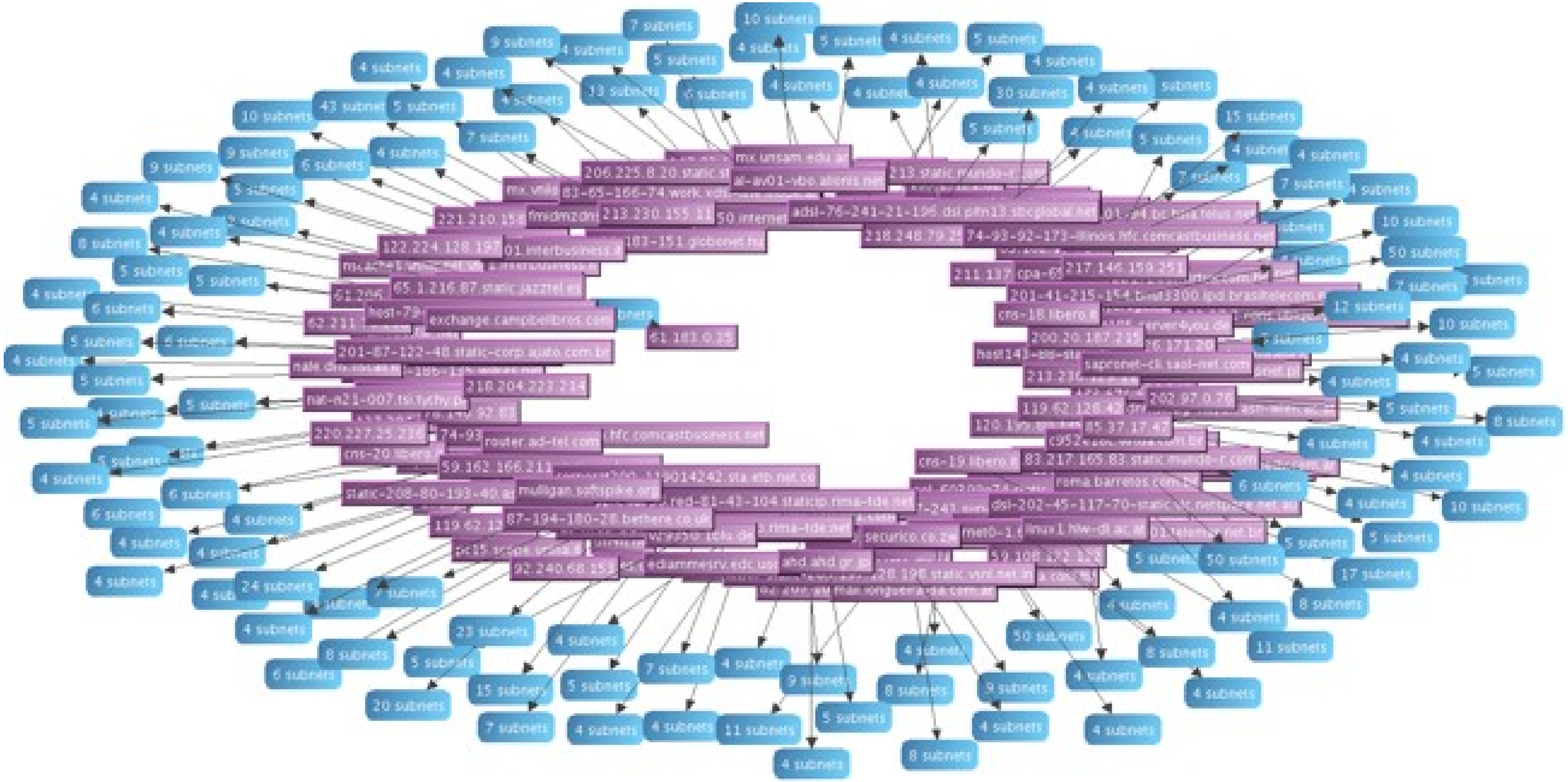
Botnet ssh bruteforce e .satan (Bday -1)



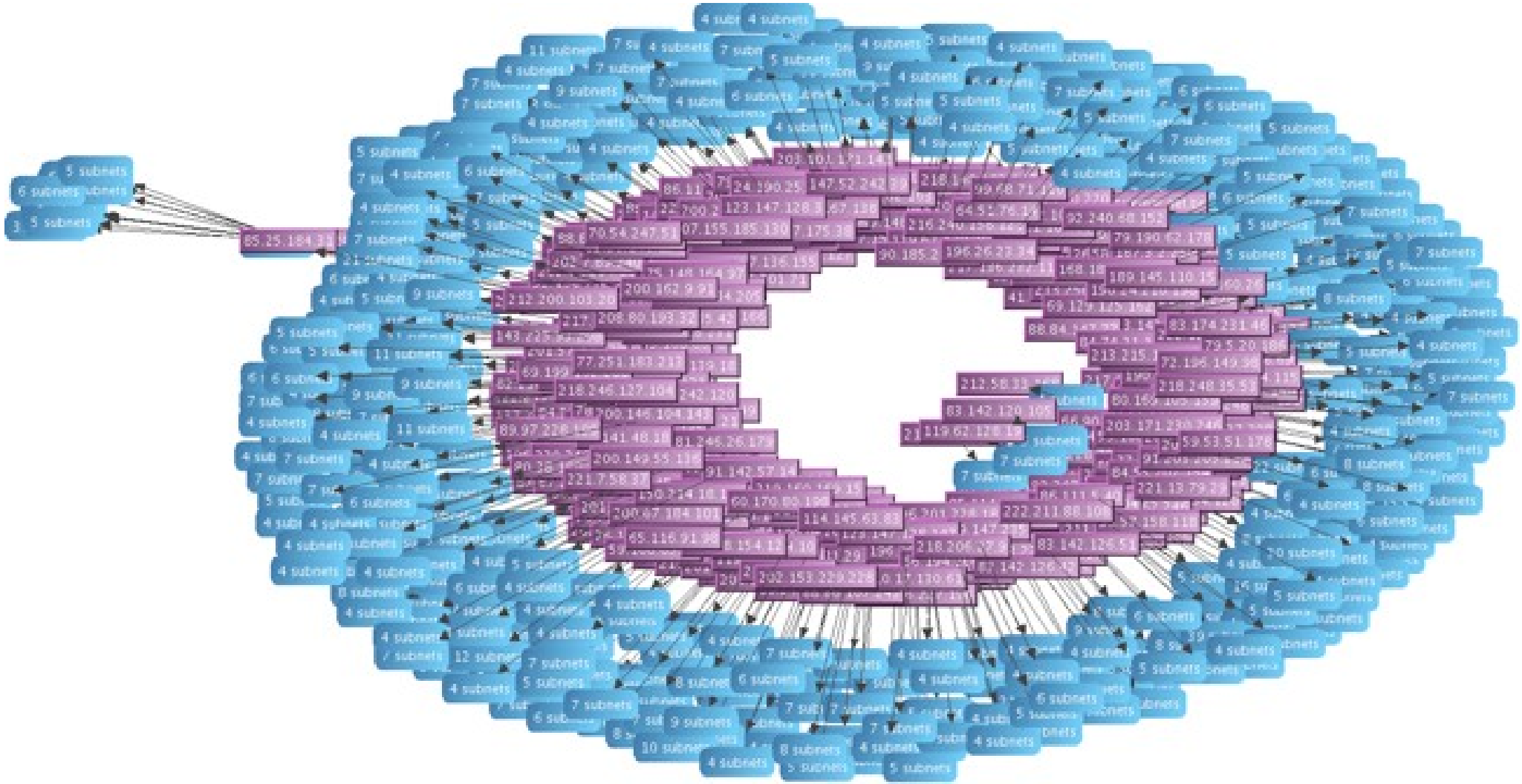
Botnet ssh bruteforce e .satan (Bday 0)



Botnet ssh bruteforce e .satan (Bday 1)



Botnet ssh bruteforce e .satan (Bday 2)



Botnet ssh bruteforce e .satan (sandbox)

Le macchine compromesse entravano a far parte della botnet e scaricavano via http dai C&C liste di ip, username e password, quindi eseguivano brute force ssh facendo pochi tentativi su ogni bersaglio (novembre 2009).

Relativamente al caso .satan (marzo-maggio 2019), abbiamo identificato una macchina linux che faceva attività mining all'insaputa dell'utente (non consentita all'interno della rete GARR).

Una volta messa in quarantena sono state cercate le tracce della compromissione precedente l'attività di mining. Siamo risaliti allo scaricamento di un file (.satan) perché il dispositivo aveva una bassa attività di rete (non produceva "rumore").

Questo file purtroppo non rappresentava l'inizio della compromissione ma bensì l'inizio dell'attività di mining.

- **mining e .satan**

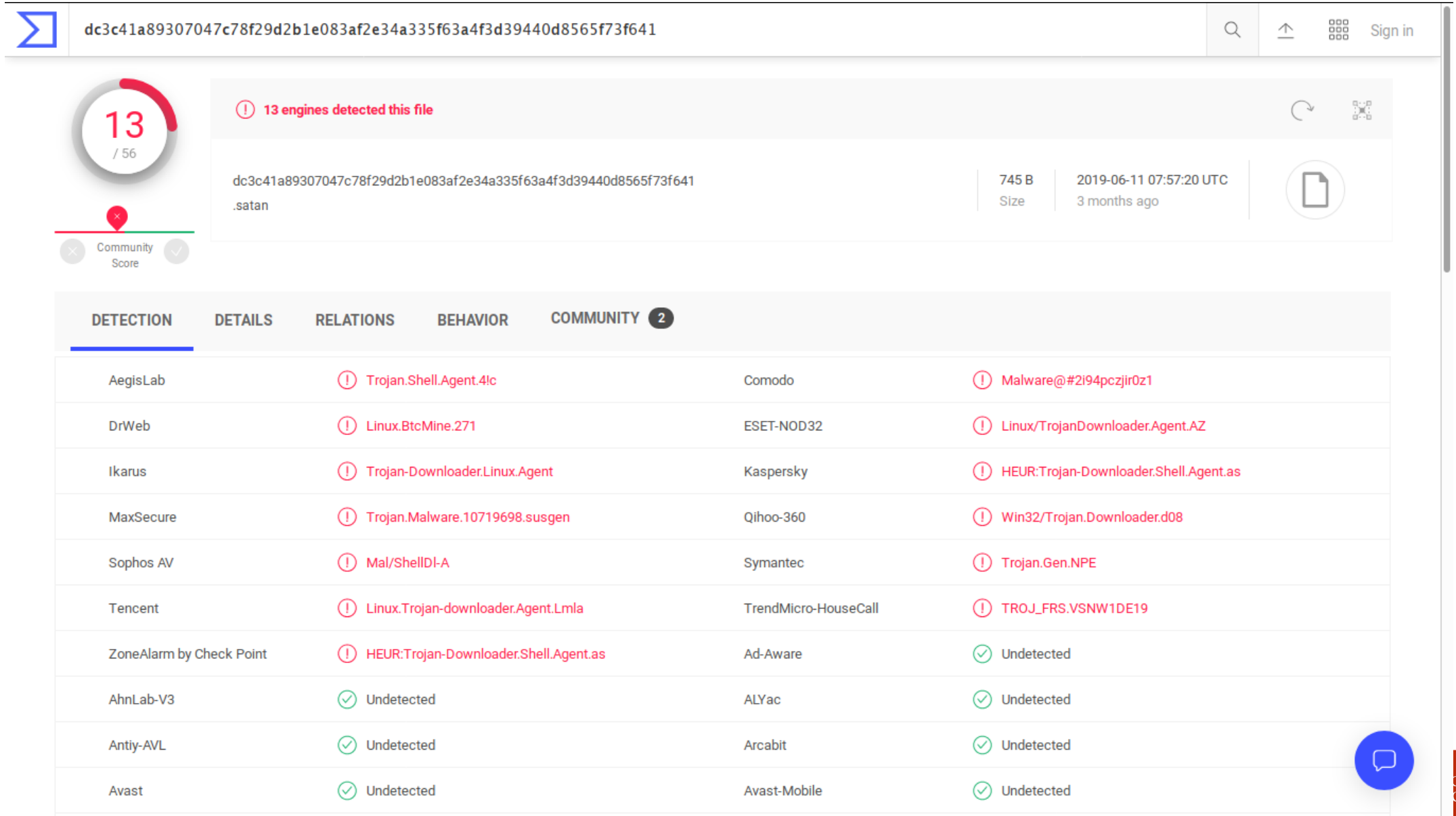
Non sappiamo come la macchina sia stata compromessa per mancanza di prove. Possiamo ipotizzare che sia avvenuta tramite brute force ssh o browser exploit.

L'analisi del file .satan, un semplice script bash, rivela che una volta eseguito:

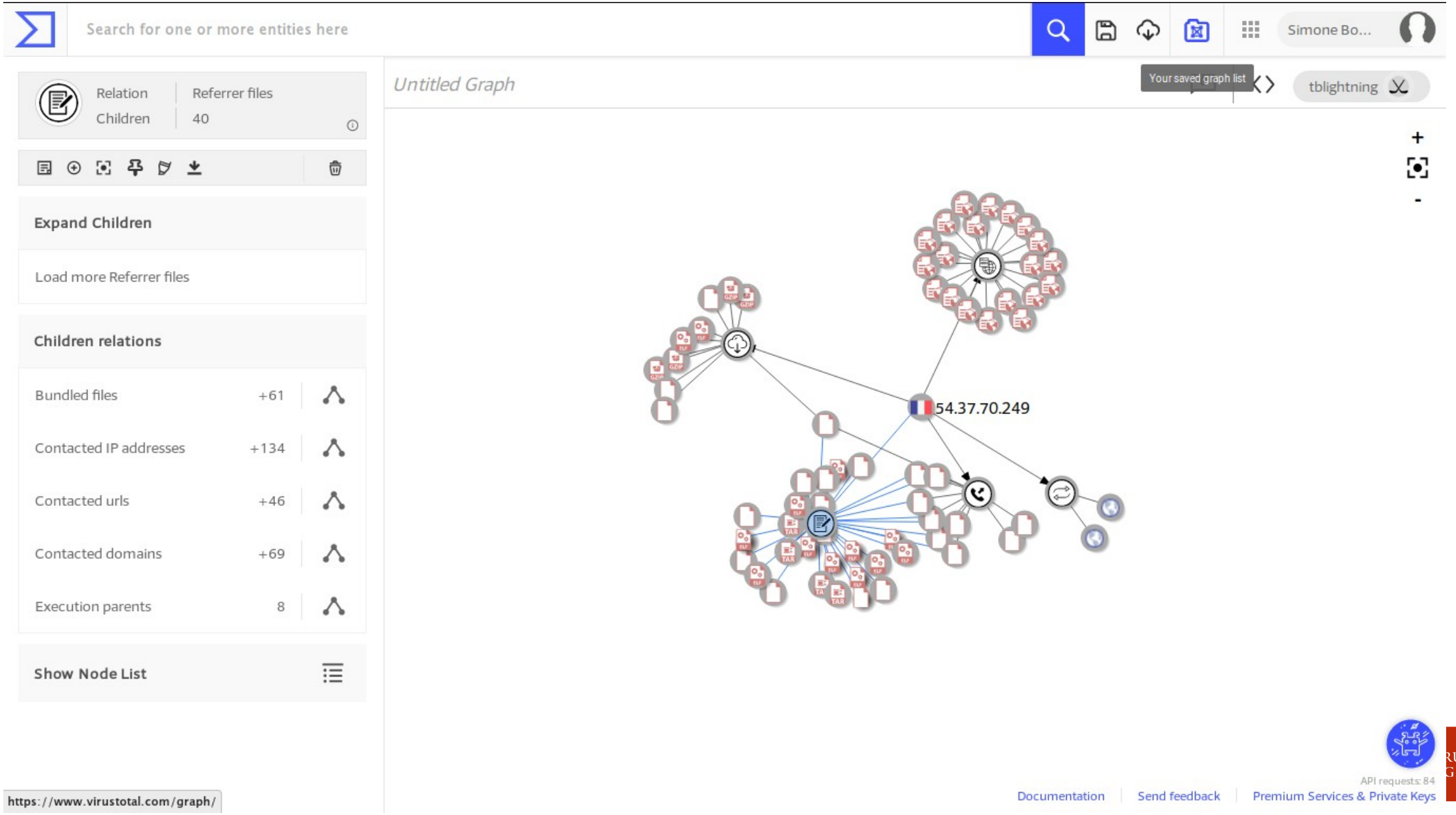
- Crea un servizio IRC (rsync.pl) in porta 443 (quindi invisibile per le sonde) per il controllo della macchina. Il codice era scritto in perl offuscato. Sembra abbastanza datato a giudicare dalle tracce trovate nel codice ($VERSION = "20000118")
- Crea una backdoor ssh con tanto di chiave
- Scarica diversi eseguibili (anacron, cron, rsync.pl, ps.bin), non sovrascrivendo gli "originali" e posizionandoli in */usr/*local/bin. Ad uno sguardo poco attento alla lista dei processi può sembrare del tutto normale. Dopo lo scaricamento ogni traccia viene cancellata e alcuni di questi processi vengono configurati come demoni. Uno di questi eseguibili è xmrig adeguatamente ricompilato e rinominato.
- Abbiamo sottoposto i campioni virali a virustotal questo ci ha permesso di estendere l'analisi ad altri campioni a cui erano correlati (OSINT Open Source Intelligence).

Queste attività necessitano privilegi di root, motivo per cui la macchina doveva aver già subito un exploit.

- **mining e .satan**



- **mining e .satan**



.satan

.satan sposa in pieno l’idea open source: riuso di codice benevolo

```
#!/bin/sh

################################################################################
#####################\
### A script for killing cryptocurrecncy miners in a Linux enviornment
### Provided with zero liability (!)
###
### Some of the malware used as sources for this tool:
### https://pastebin.com/pxc1sXYZ
### https://pastebin.com/jRerGP1u
### SHA256: 2e3e8f980fde5757248e1c72ab8857eb2aea9ef4a37517261a1b013e3dc9e3c4
################################################################################
#####################\
```

Quindi veniva lanciata l’attività di mining.

.satan

Cosa hanno in comune .satan e la botnet brute force (caso del 2009)?

.satan, mentre esegue il mining, scarica due liste: una formata da “ip porta” e l’altra da “username password” poi con questi dati inizia a cercare nuove vittime.

A distanza di tanto tempo le tecniche non sono cambiate così tanto e anche il codice usato non è all’ultimo grido. **Si punta verso mal configurazioni, password banali o di default, software non aggiornato**…

Frasi celebri e luoghi comuni

Siamo sotto attacco?

Sempre costantemente. Abbiamo ricevuto da un IP l'intera scansione di una nostra classe B in solo 1/2 s

Non aggiorno il PC perché gli aggiornamenti fanno più male che bene

Ci sono utenti che pensano che aggiornare il proprio pc sia sbagliato perché causa malfunzionamenti. Gli attaccanti la pensano diversamente. Spesso ci è capitato di trovare malware che aggiornava il dispositivo per evitare che qualcun altro se ne impossessasse.

I dispositivi Apple sono immuni da malware

È vero il contrario

Sto usando un protocollo sicuro (es. ssh) sono a posto

Probabilmente no, sopratutto se stai usando una password banale

Il mio Pc non contiene nulla di interessante

Ogni dispositivo può diventare un'arma cibernetica. I dispositivi personali sono solitamente poco curati/presidiati. Il valore di un dato è compreso meglio da chi attacca piuttosto che dal proprietario del dato.

Policy

Lo scopo di una policy è quello di:

- eliminare rumore molesto
- rendere più semplice la ricerca guasti
- migliorare la sicurezza.
- Evitare l'acquisto di apparati sovradimensionati

Non limita l'attività accademica

Es. Policy che elimina l'attività di mining (anche quella via web).

Pro

- Smettiamo di finanziare il cybercrime
- Eliminiamo rumore inutile

Cons

- Ostacola la ricerca sul mining. **Problema di facile soluzione con una whitelist**

L'attività di mining non va confusa con l'uso delle cripto valute
Le policy non riguardano solo il network

Information Sharing (IS) e Incident Response (IR)

L’IS nasce dall’esigenza di condividere l’informazione.

Spesso accade che analisti diversi approccino lo stesso problema da angolazioni diverse a causa degli strumenti che usano, del loro settore d’impiego, o delle conoscenze acquisite:

- Ci sono analogie tra il traffico di UniBo e quelle di un altro socio GARR?
- Cosa accade se mettiamo insieme queste informazioni?
- Siamo più resilienti?
- Siamo più reattivi?

L’IR spesso lo identifichiamo con il sistema di ticketing che è solo una parte dell’insieme.

Cosa succede se l’IR diventa una parte dell’IS?

Le risorse scarseggiano e la condivisione (fatta nel modo giusto) aiuta tutti.

Attualmente come piattaforma di IS stiamo usando misp in modalità consumatore. Per l’IR stiamo pensando a The Hive

Esempi di IS sono GARR-CERT, CERT-PA e il gruppo di lavoro GARR sulla sicurezza

La Traffic Analysis è solo un tipo di analisi...

Esistono altri tipi di analisi, vediamone alcuni:

- **Threat Hunting**: consiste nel dimostrare la validità di un ipotesi. Es. ci sono tracce di movimento laterale nella mia rete?
- **ETA (Encrypted Traffic Analysis)**: da tempo il malware nasconde le sue attività nel traffico cifrato. Per identificarlo occorre analizzare quel tipo di traffico. Se non si vuole usare la tecnica del MitM, ci si può affidare a nuovi progetti di ricerca che studiano le caratteristiche del traffico ([ja3,ja3s] fingerprint, fatt, joy)

La Traffic Analysis è solo un tipo di analisi...2

- **Data Analytics**: “analisi statistica” del traffico. Ha molto in comune con NBADS e Threat Hunting. Progetti interessanti sono threathunting project, bat, Rita.
- **HIDS (Host Intrusion Detection System) con vocazione da SIEM**: può essere interessante spingere l’analisi più in profondità: Wazuh + OSQuery + ELK stack
- **AIL (Analysis Information Leak)**: is a modular framework to analyse potential information leaks from unstructured data sources like pastes from Pastebin or similar services or unstructured data streams (such as Tor hidden services). AIL framework is flexible and can be extended to support other functionalities to mine sensitive information.

Problemi e/o curiosità

- Stiamo analizzando il traffico di dispositivi mobili. Di compromissioni ne rileviamo parecchie. Purtroppo la maggior parte dei dispositivi sarà sempre vulnerabile perché non aggiornabile.
- Prima interveniamo isolando un dispositivo compromesso, meglio è, però un utente eduroam con un dispositivo compromesso di fatto non è possibile isolarlo tempestivamente.
- Essere troppo tempestivi nella mitigazione di una compromissione non ci permette di imparare dal malware :-(

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Domande?

cert@unibo.it - https://cert.unibo.it