A Framework for Attack Patterns Discovery in Honeynet Data

By

Olivier Thonnard, Marc Dacier

Presented At

The Digital Forensic Research Conference

DFRWS 2008 USA Baltimore, MD (Aug 11th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

A Framework for Attack Patterns' Discovery in Honeynet Data

August 13th, 2008

Olivier Thonnard
Royal Military Academy
Polytechnic Faculty
Belgium
olivier.thonnard@rma.ac.be

Marc Dacier
Symantec Research Labs
Sophia Antipolis
France
marc_dacier@symantec.com

Outline

1. Introduction
   - Problem and research context
2. Honeynet-based network forensics
   - Attack patterns discovery
3. Proposed solution
4. Experiments
   - Honeynet time series analysis
   - Results of the clique-based clustering
5. Conclusions and Future Work

1. Introduction

The problem

Research context

The problem

- Improve our understandings of certain network threats observed on the Internet
  - Get insights into global attack phenomena
  - Learn more about the *modus operandi*

- To achieve this, we seek to analyze Internet threats at a global strategic level
  - Enable a « Network Situational Awareness » (Yegneswaran, Barford, Paxson in HOTNETS ’05)

Our approach

1. We want to *discover attack patterns* from large real-world attack datasets:
   - Groups of attack traces sharing important similarities
   - No rigid, pre-defined attack signatures
     → Not so helpful with polymorphic and 0-day attacks
2. We seek to systematically *draw knowledge* from those attack patterns

Research Context

- The WOMBAT Project
  - Worldwide Observatory of Malicious Behaviors and Attack Threats
  - EU-FP7 - http://www.wombat-project.eu

Project coordinator:
France Telecom R&D (FR)

Partners from:
Institut Eurecom (FR)
Technical University Vienna (AT)
Politecnico di Milano - Dip. Elettronica e Informazione (IT)
Vrije Universiteit Amsterdam (NL)
Foundation for Research and Technology (GR)
Hispasec (ES)
Research and Academic Computer Network (PO)
Symantec Ltd. (IE)
Institute for Infocomm Research (SG)

Research Context

- Objectives of WOMBAT
  - Aims at providing new means to understand the existing and emerging threats that are targeting the Internet economy and the net citizens

- To reach this goal: three main workpackages
  1. Data acquisition and sharing of security related datasets
  2. Data enrichment with threat context information
  3. Threats analysis: *root cause* identification and understanding of attack phenomena under scrutiny

The focus of this work

2. Honeynet-based forensics

Leurre.com honeynet

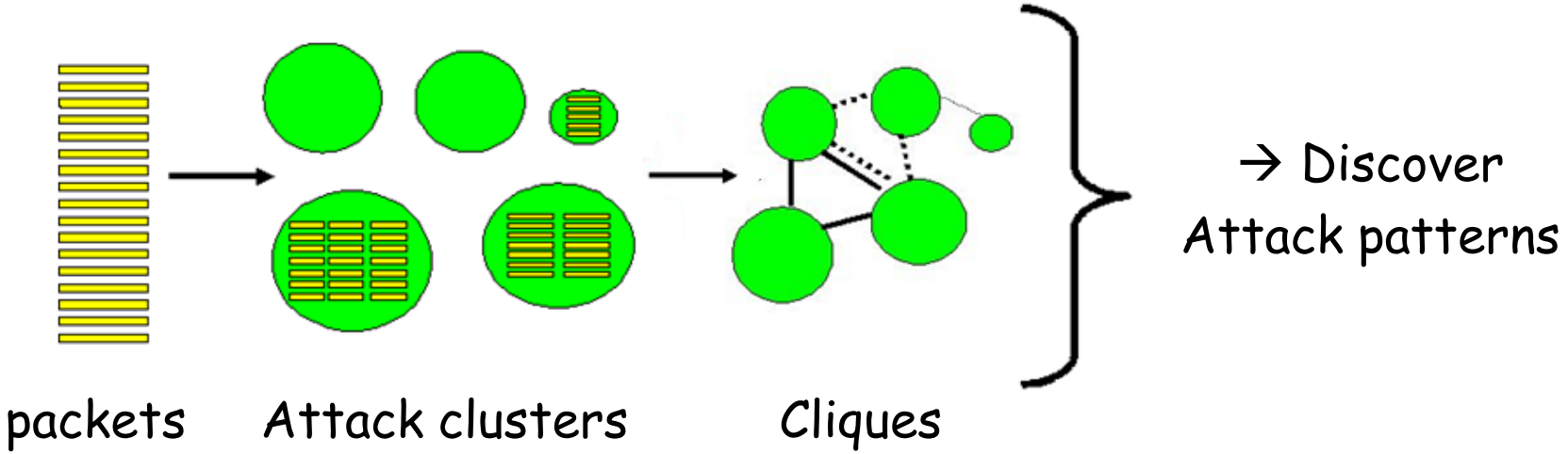
Attack patterns

Leurre.com Honeynet

- Global distributed honeynet (http://www.leurrecom.org)
  - +50 sensors distributed in more than 30 countries worldwide
- Same configuration for all sensors
  - 3 low-interaction honeypots based on *honeyd*
  - 2 x Win2K and 1 x RedHat7.3
- The collected traffic is:
  - Enriched with contextual information (Geo, reverse-DNS, etc)
  - Parsed and uploaded into an Oracle DB
- All partners have full access (for free) to the whole DB

Honeynet-based forensics

- Analyze honeynet traces by means of data mining techniques, in two different steps:
  1. Raw packets → Attack clusters (« fingerprints »)
  2. Attack clusters → discovery of *attack patterns*



Step 1: Attack clusters

- Some *Leurre.com* definitions:
  - A *source* = an IP address that targets a honeypot platform on a given day, with a certain port sequence.
  - Every source is attributed to an "*attack (cluster)*" based on its network characteristics(*):
    - targeted port sequence,
    - #packets,
    - #bytes ,
    - attack duration,
    - average packet IAT, and
    - attack payload (Levenshtein)

Attack tool

↓

Fingerprint(s)

(*) F. Pouget, M. Dacier, **Honeypot-Based Forensics**. AusCERT Asia Pacific Information technology Security Conference 2004.

Step 2: Attack patterns discovery

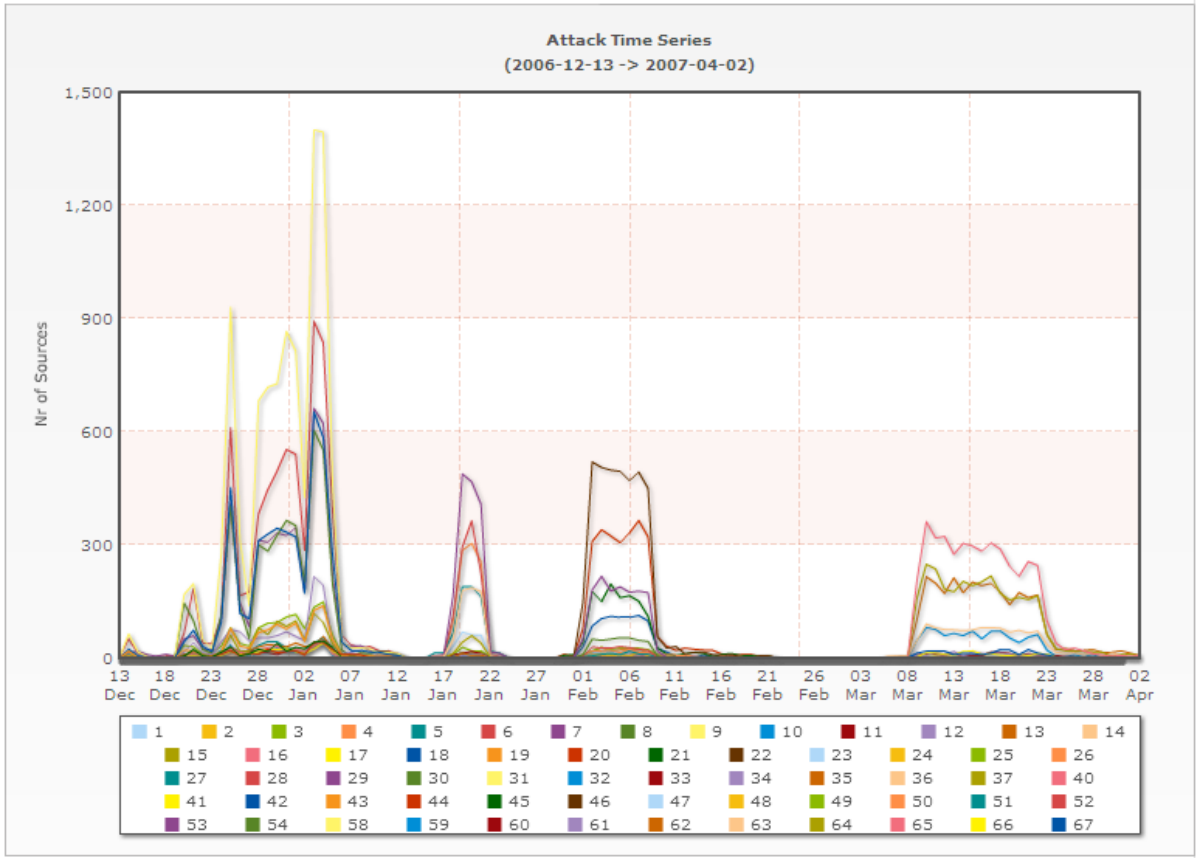
- We use the attack fingerprints to discover *patterns* shared by a group of attacks, by using a data mining process:
  - *Objects* = attack (fingerprints)
  - *Clustering parameter* = selected *attack feature*

- In this work:
  - Clustering parameter → *Attack time series*
    - = aggregated source count by day for a given attack on a given platform

Attack time series

Attack port sequences:

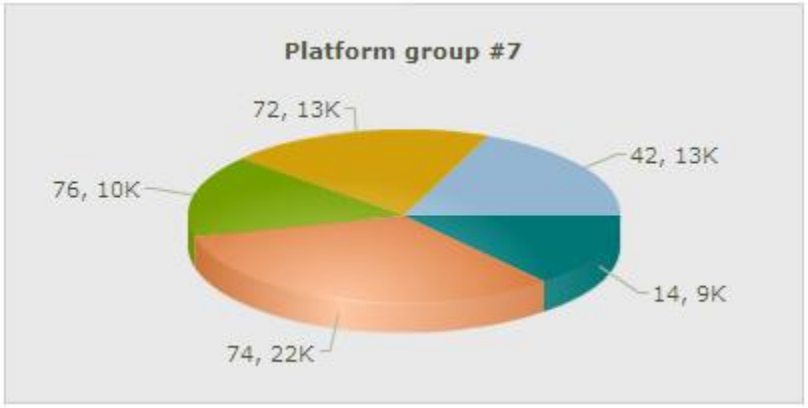
- I
- I-445T
- I-445T-139T
- I-445T-80T



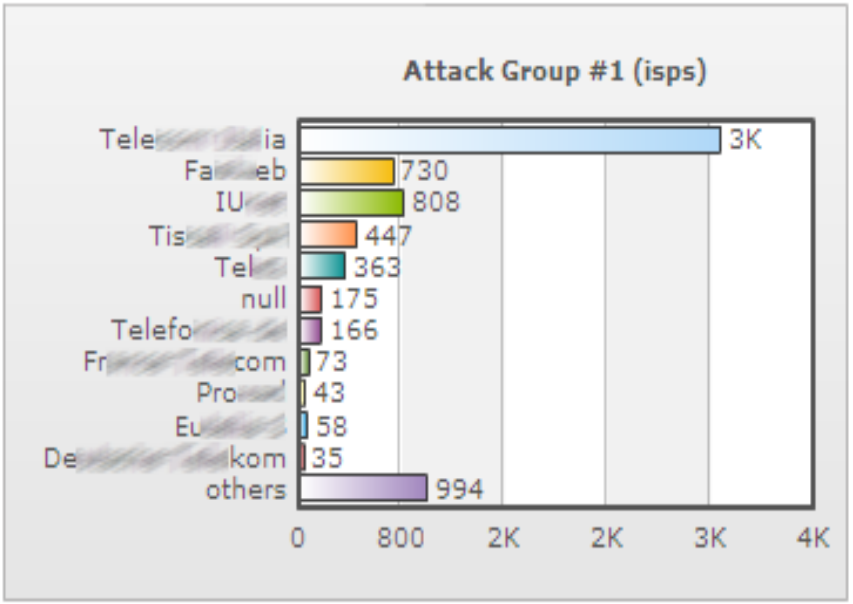
Some other attack features for patterns discovery

- Attackers' characteristics
  - Countries of origin
    - Identify localized botnets
    - Identify "safe harbors" for cybercriminals
  - ISP's and Subnets of origin
    - "uncleanliness" of certain networks
- Targeted sensors

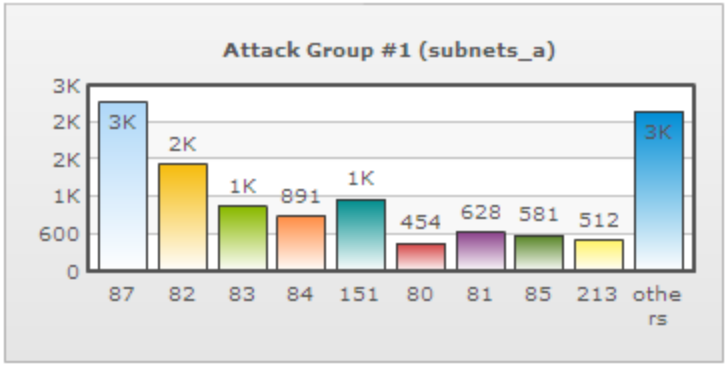
Some other patterns…



Targeted platforms



ISP's of origin



Subnets of origin

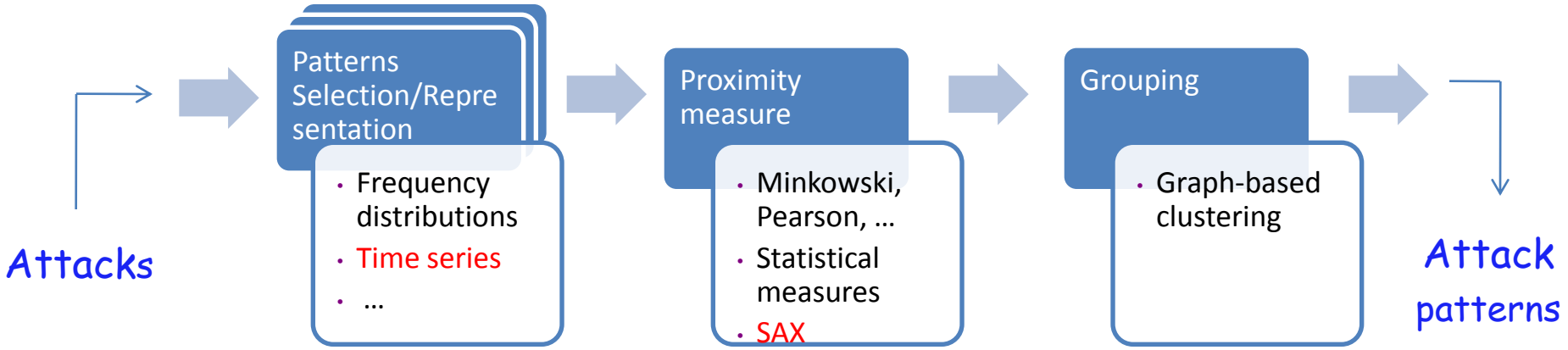
3. Proposed solution

Method overview

Clique-based clustering

Method overview

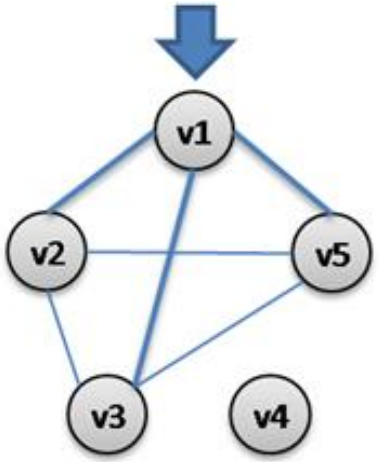
- Basically a KDD application.



Grouping step

- Graph-theoretical formulation
  - The vertices = data objects (e.g. the attack time series)
  - The edges = similarity relationships

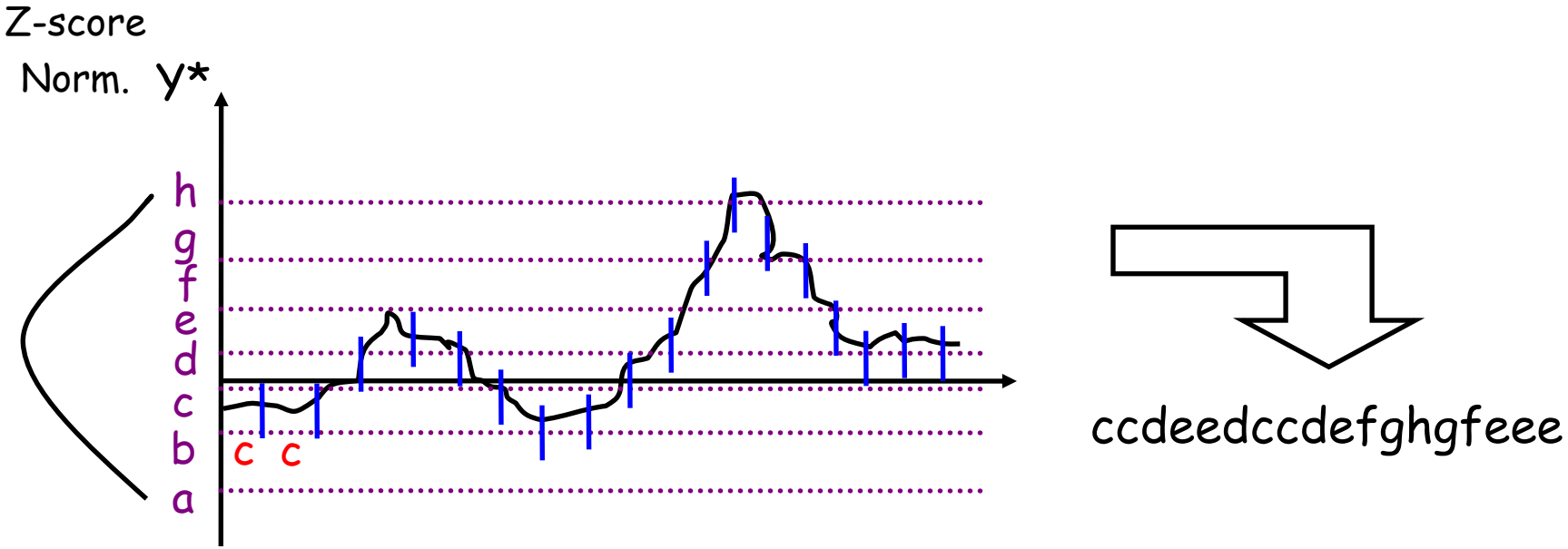
- Clique-based clustering
  - Extraction of *(maximal) cliques*, or complete sub-graphs
  - Greedy algorithm based on the quality of the cliques.



Transitive distance

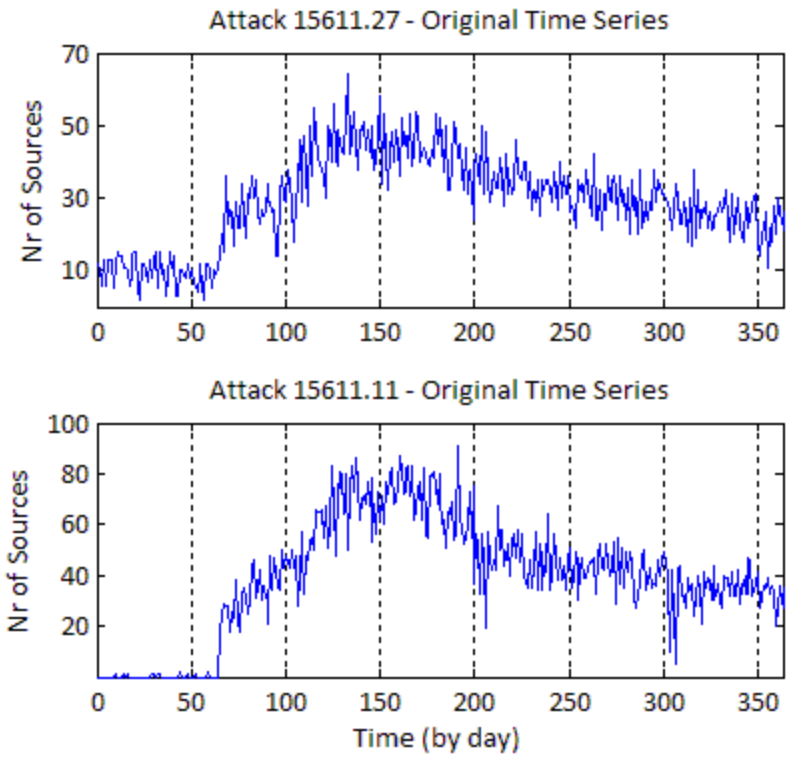
S.A.X.

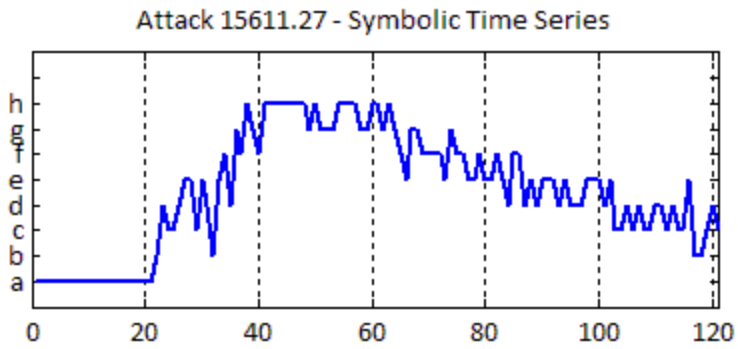
- Symbolic aggregate approximation
  - Per segment, it attributes the mean value to a *symbol*
  - Provides a lower-bounding distance between 2 strings
  - Needs some adaptation to fit to non-Gaussian signals (especially for skewed distributions)

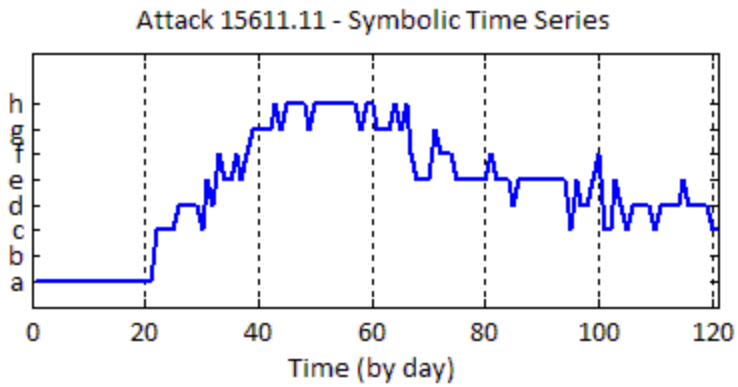


S.A.X.

- An example







4. Experiments

Honeynet Environment

Experimental results

Honeynet environment

- *Leurre.com* dataset used for the experiments
  - Data collected with 44 platforms, located in 22 different countries and IP subnets
  - Period: Sep 1st, 2006 → Jan 1st, 2008 (486 days)
  - Raw data volume: ~27 GB (1,738,565 distinct sources)
- 1268 attack time series, each composed of 486 days
  - Selected on basis of a source volume criterion (at least one peak of activity with min. 10 sources)
  - Corresponds to ~85% of the total traffic data

Cliques results overview

- We observe only three broad classes of activities:
  - **Continous activities** (33%)
  - **Sustained bursts** (12%)
  - **Ephemeral spikes** (6%)

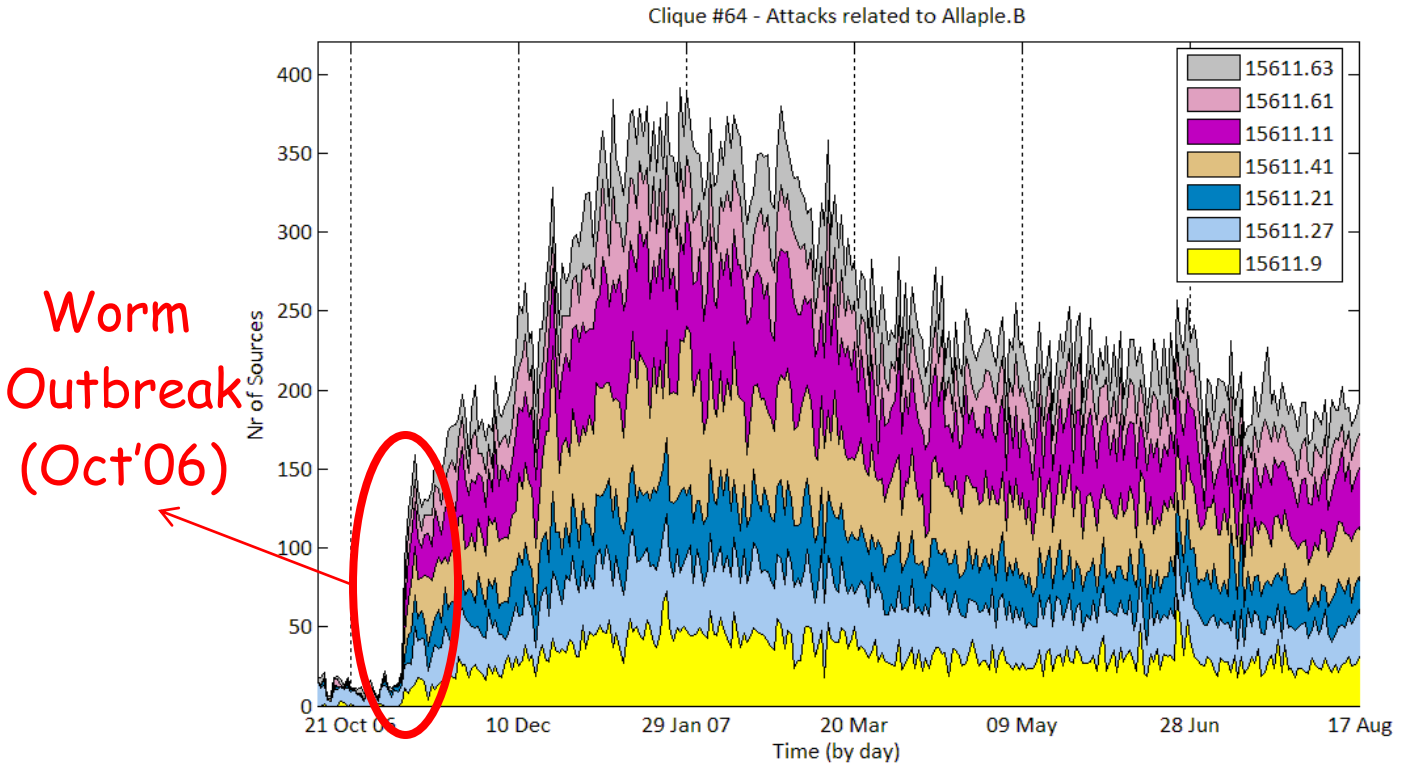
Classes of Activities	Nr of Cliques	Nr of Time Series	Nr of Sources	Main Port Sequences	Plausible Root Causes
Continuous	19	58 (4.6%)	581,136 (33.4%)	|1026U|1027U|1028U |I|139T|445T |1434U |135T |I	Scam on Messenger Svc Classical worms (Allaple.B, Slammer) Continous scan
Sustained Bursts	24	107 (8.4%)	204,336 (11.8%)	|I|445T|139T |5900T and |1433T |2967T, |2968T |445T	Large botnet activity Multi-headed worm Sustained scan activities
Ephemeral Spikes (Epiphenomena)	109	554 (43.7%)	98,610 (5.7%)	|6644T, |17838T, |6769T |5168T, |53842T, |12293T |6211T, |50286T, |9661T |135T, |139T, |445T |2967T, |2968T |1025T, |80T, |1433T |5900T, |5901T |4662T, |4672T	Ephemeral probes on unusual high TCP ports Targeted scans on common Windows ports (NetBios, Symantec, RPC, VNC, etc) Misconfigurations (P2P)
Inconsistencies or misclassifications	12	36 (2.8%)	25,716 (1.5%)	|135T, |139T, |445T |1433T	Background noise on common services

Continuous activity

A clique of attacks observed on 7 different sensors, targeting:

|I, |I|139T, and |I|139T|445T

(root cause: **W32/Allaple.B**)

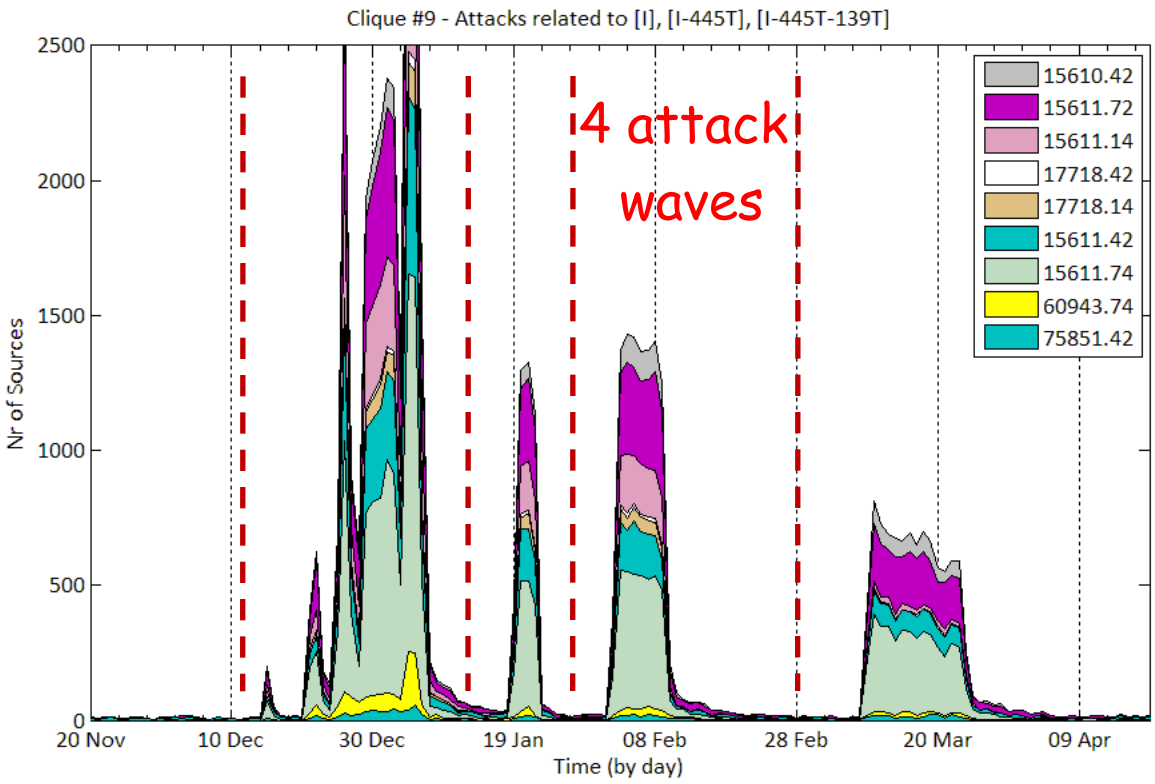


Sustained Bursts

A clique of attacks observed on 3 different sensors, targeting:

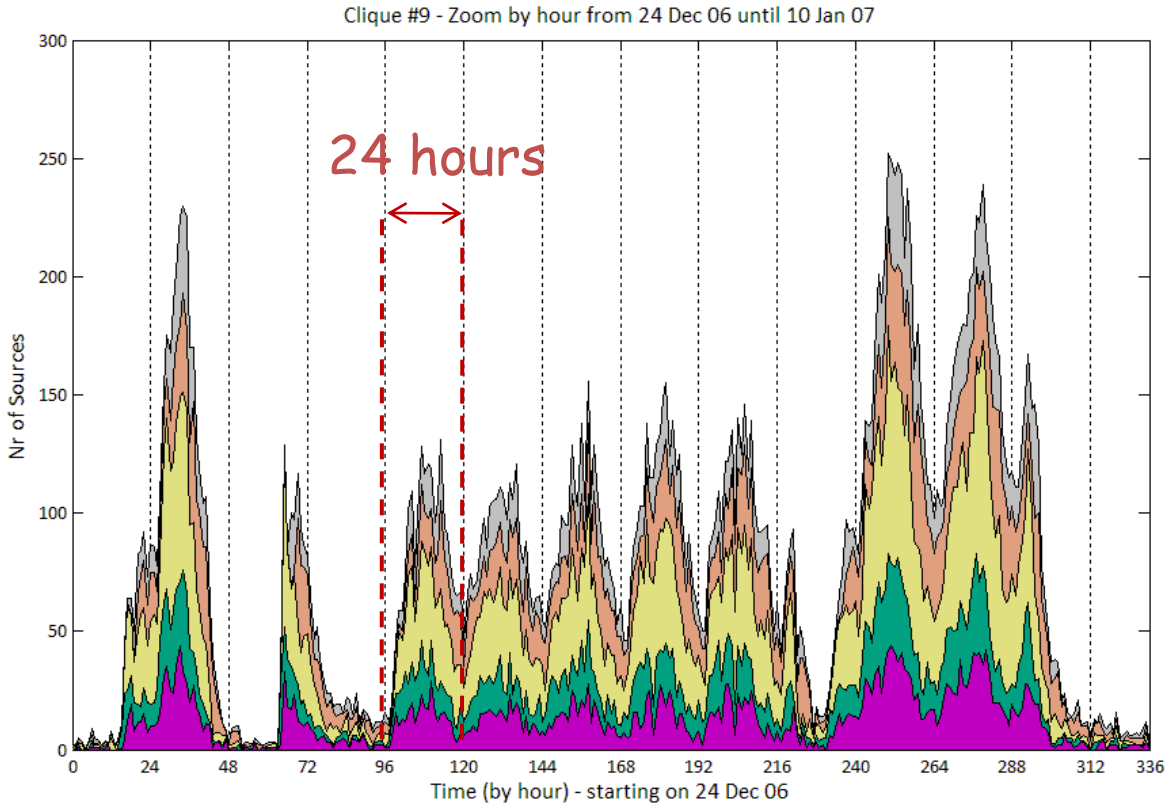
|I, |I|445T, |I|445T|139T and |I|445T|80T

(presumed root cause*:* ***botnet propagation***)



Sustained burst: A zoom on the 1st wave

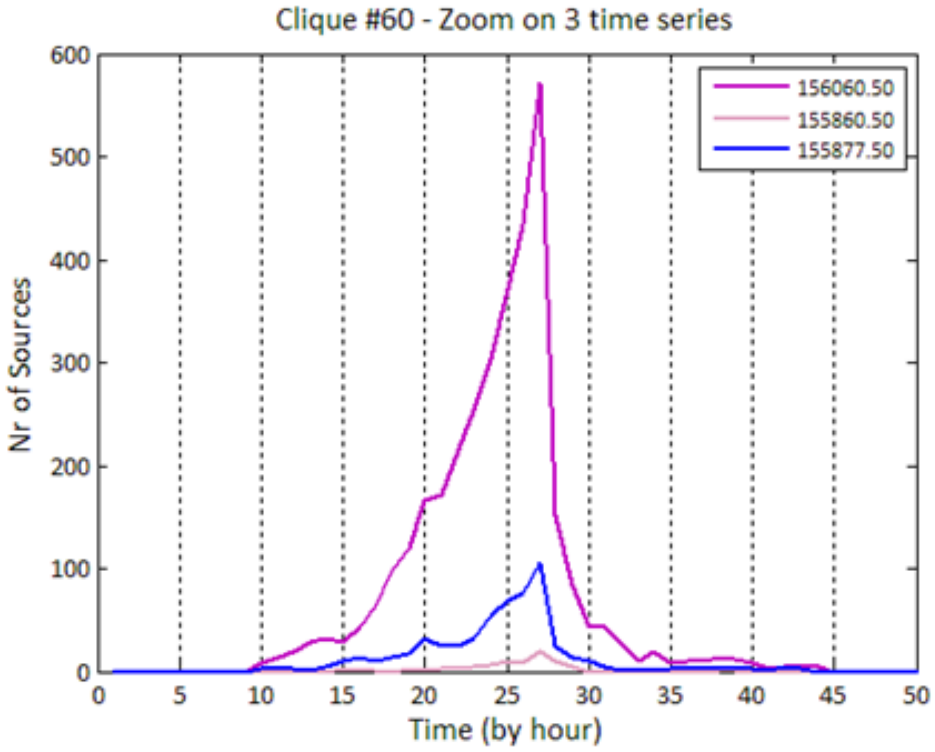
- Time frame: 24 Dec until 10 Jan
- Time granularity: *1 hour*



Ephemeral Spikes

A clique of attacks observed on a single sensor, targeting:

|6769T (root cause: ??)



5. Conclusions

Strengths / limitations

Future directions

Strengths of the framework

- Can discover any sort of attack pattern via attack trace similarity
  - Rather than via rigid signatures
- Resistant to *polymorphic* attack tools
- Can produce concise, high-level summaries of attack traffic, which deliver much more insights into global attack phenomena and their *modus operandi*

Some limitations

- Currently, no information is *automatically* provided regarding the type of attack, i.e.:
  - Botnet or worm propagation?
    - → We look to implement some techniques to separate botnet, worm and misconfigurations within attack events.
  - Name or family of the botnet / worm / malware ?
    - → Recently we've upgraded our threats collection infrastructure with controlled high-interaction honeypots based on SGNET (*)
    - → SGNET = ScriptGen + Nepenthes + Argos + Anubis + VirusTotal

(*) Corrado Leita and Marc Dacier. **SGNET: a worldwide deployable framework to support the analysis of malware threat models.** (EDCC 2008, Lithuania)

Future work

- Botnet / worm patterns separation
- Integration of other *relevant* attack features:
  - Malware characteristics (e.g. from SGNET traffic)
  - External contextual information
    - IP Data from other projects (Shadowserver, EmergingThreats, SpamHaus, …)
- Combination of many different attack features
  - Generation of higher-level "concepts" describing real-world phenomena
    - A concept is similar to a hyperclique
  - Knowledge engineering based on extracted concepts

Thank you.

Any question?

If you'd like to join *WOMBAT* or *Leurre.com* projects, please do not hesitate to contact us:

Engin Kirda: engin.kirda@eurecom.fr
Marc Dacier: marc_dacier@symantec.com
Olivier Thonnard: olivier.thonnard@rma.ac.be

WOMBAT

EURECOM