symantec™

Confidence in a connected world.

Le point de vue d'un WOMBAT sur les attaques Internet

Marc Dacier

Directeur, Symantec Research Labs Europe

Overview

- **Introduction**
  - Data Acquisition
  - Data Enrichment
  - Threats Analysis
- Conclusions

Foreword

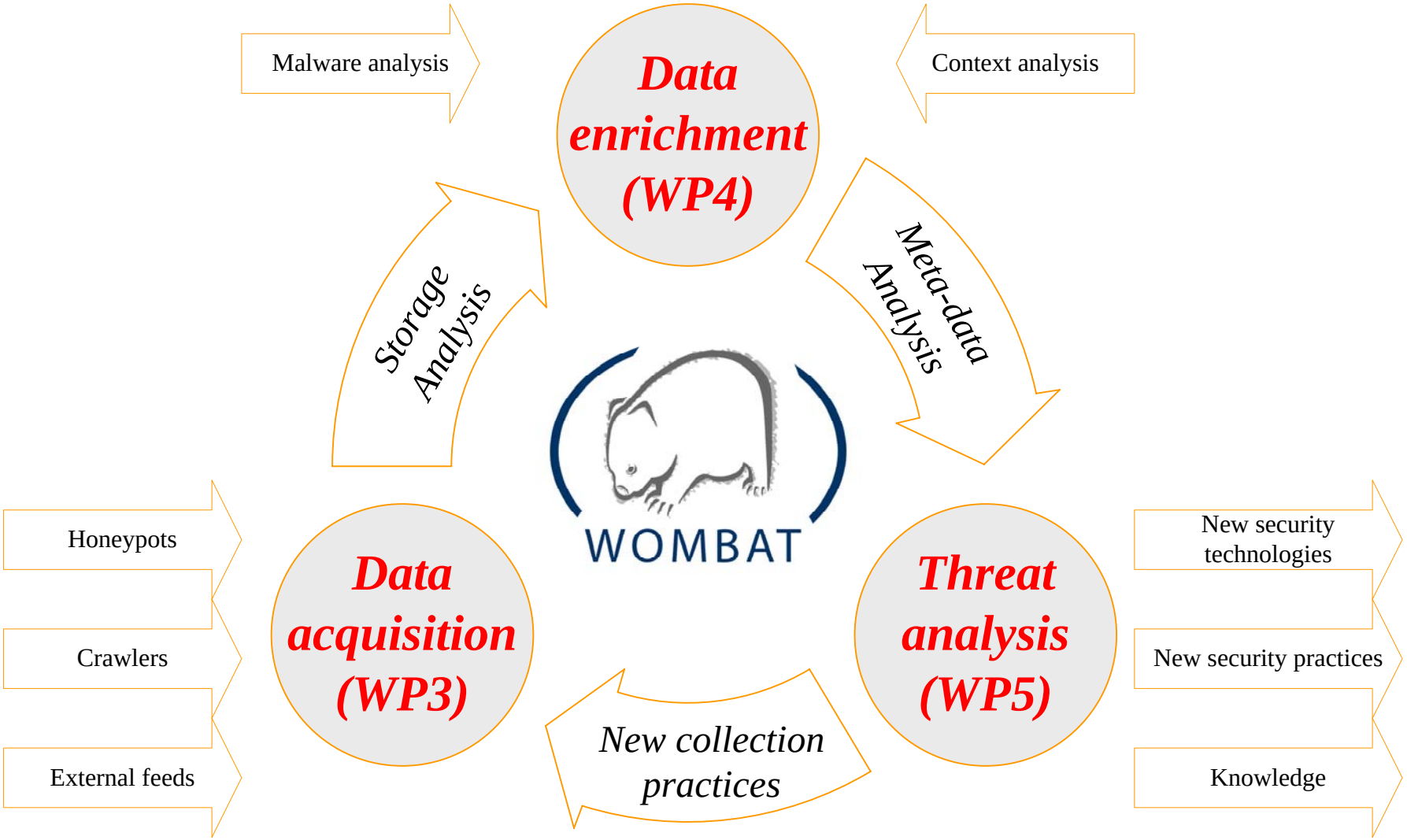
- What is presented here is the result of a joint collaboration between all WOMBAT partners over the last 14 months

  (see www.wombat-project.eu for the list of publications and deliverables)

Take-away Message

- WOMBAT is collecting and offering data for collaboration with other organizations
- A lot remains to be done to efficiently identify, analyze and counter the modus operandi of the malicious actors on the Internet
- Understanding these strategies is key to enable ciber security situational awareness.
- Looking at raw material, eg malware, is not enough. We must enrich it with metadata and contextual information.

The WOMBAT approach



Overview

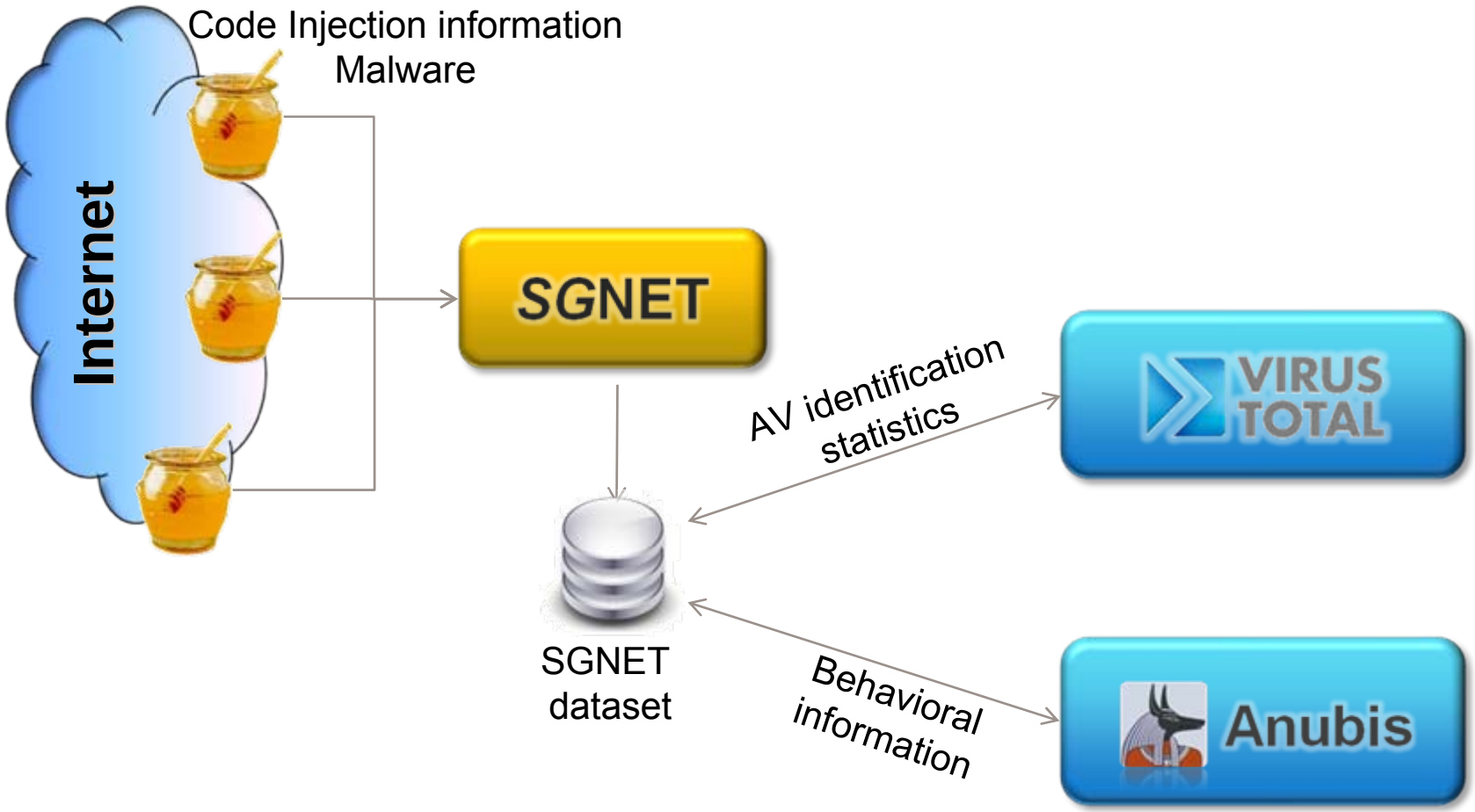
- Introduction
  - **Data Acquisition**
  - Data Enrichment
  - Threats Analysis
- Conclusions

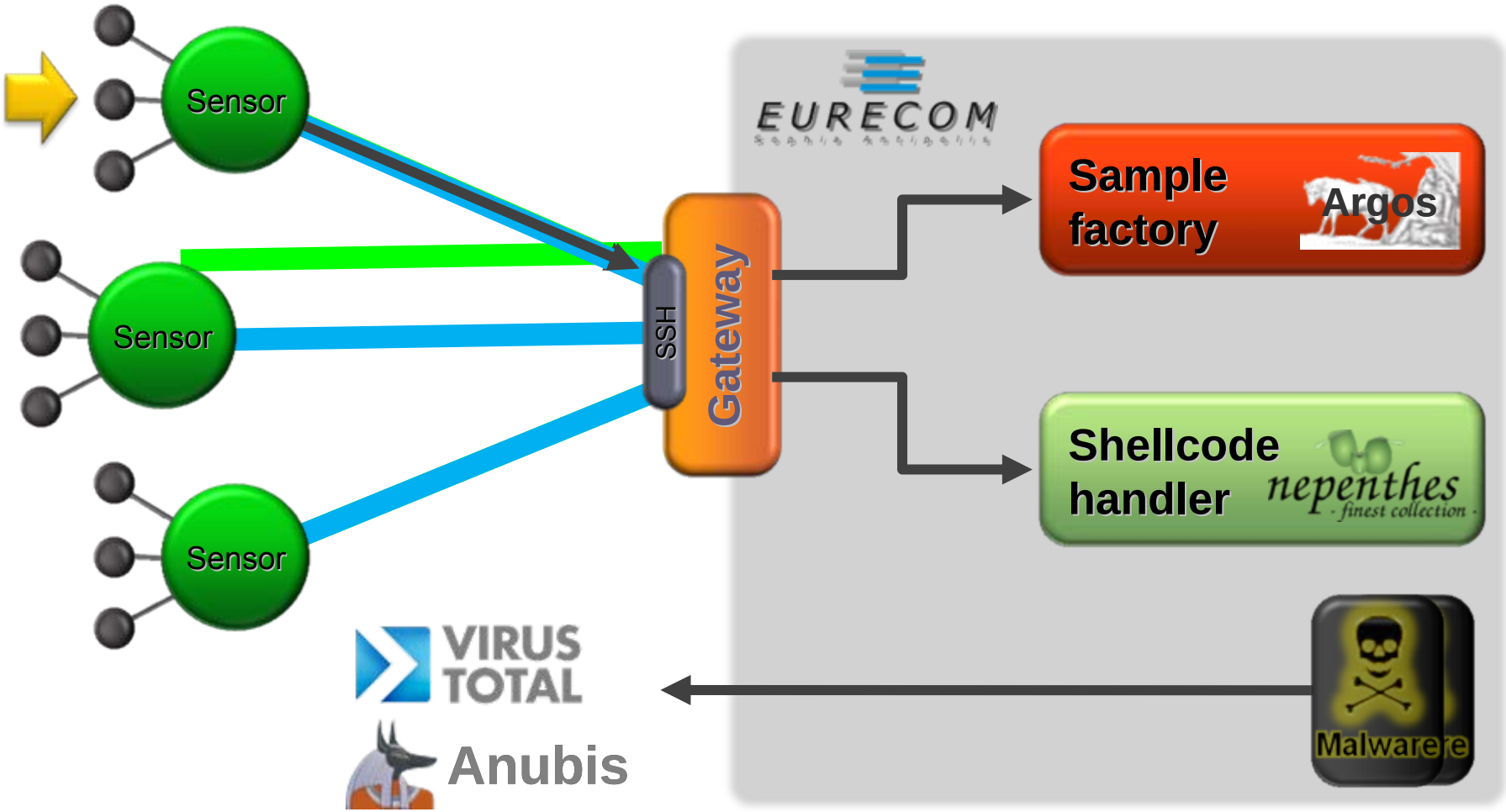
Data ?

- Wombat builds upon two complementary approaches:
  - A WAPI API
  - A federated Database (proxy) for non persistent datasets

- New sensors are developed
  - SGNET
  - Honey clients
  - Bluetooth, WIFI
  - …

Example of a new sensor: SGNET

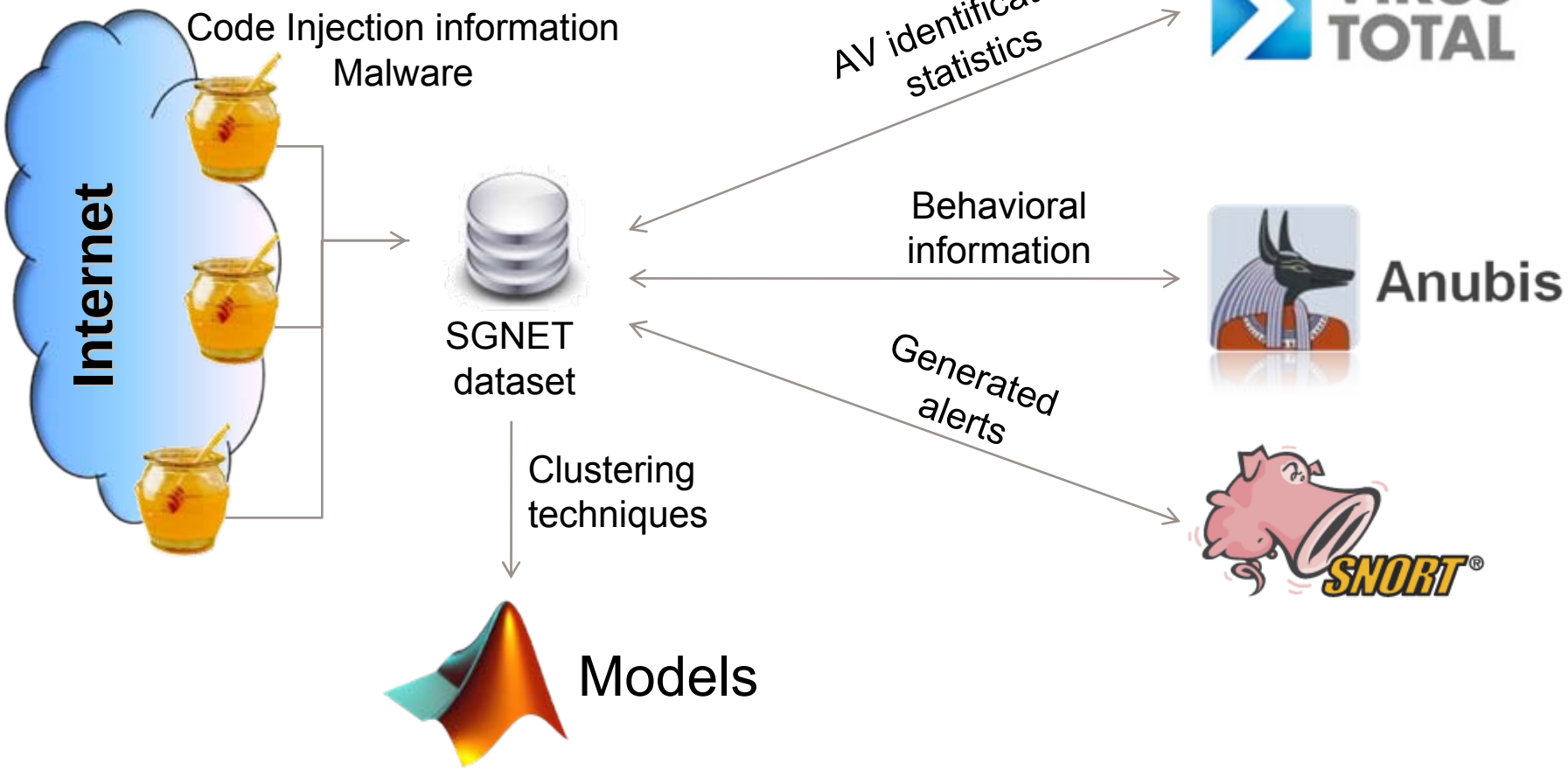



Sensor
Sensor
Sensor
SSH
Gateway
EURECOM
Sample factory
Argos
Shellcode handler
nepenthes
finest collection
Malware
VIRUS TOTAL
Anubis

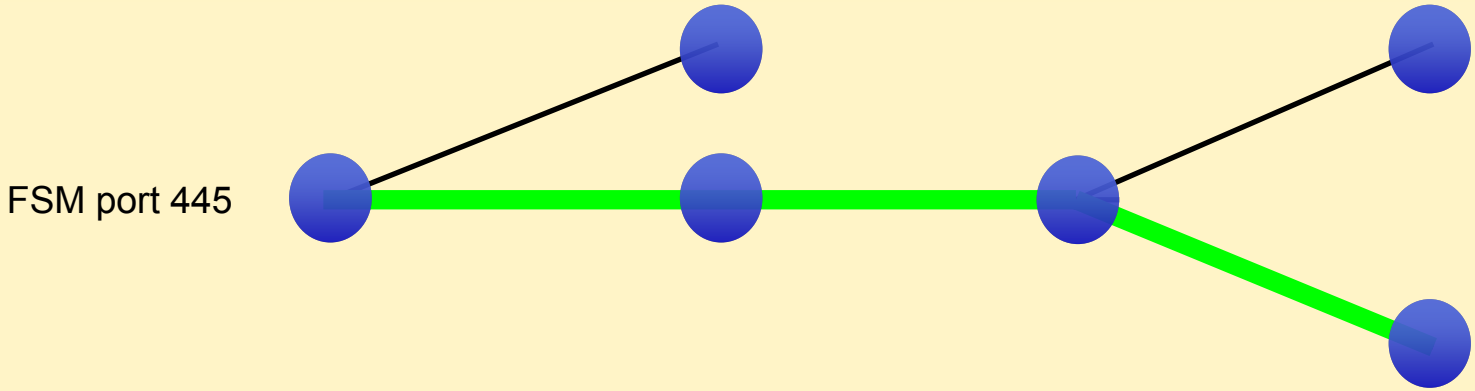
Overview

- Introduction
  - Data Acquisition
  - **Data Enrichment**
  - Threats Analysis
- Conclusions

SGNET data enrichment framework

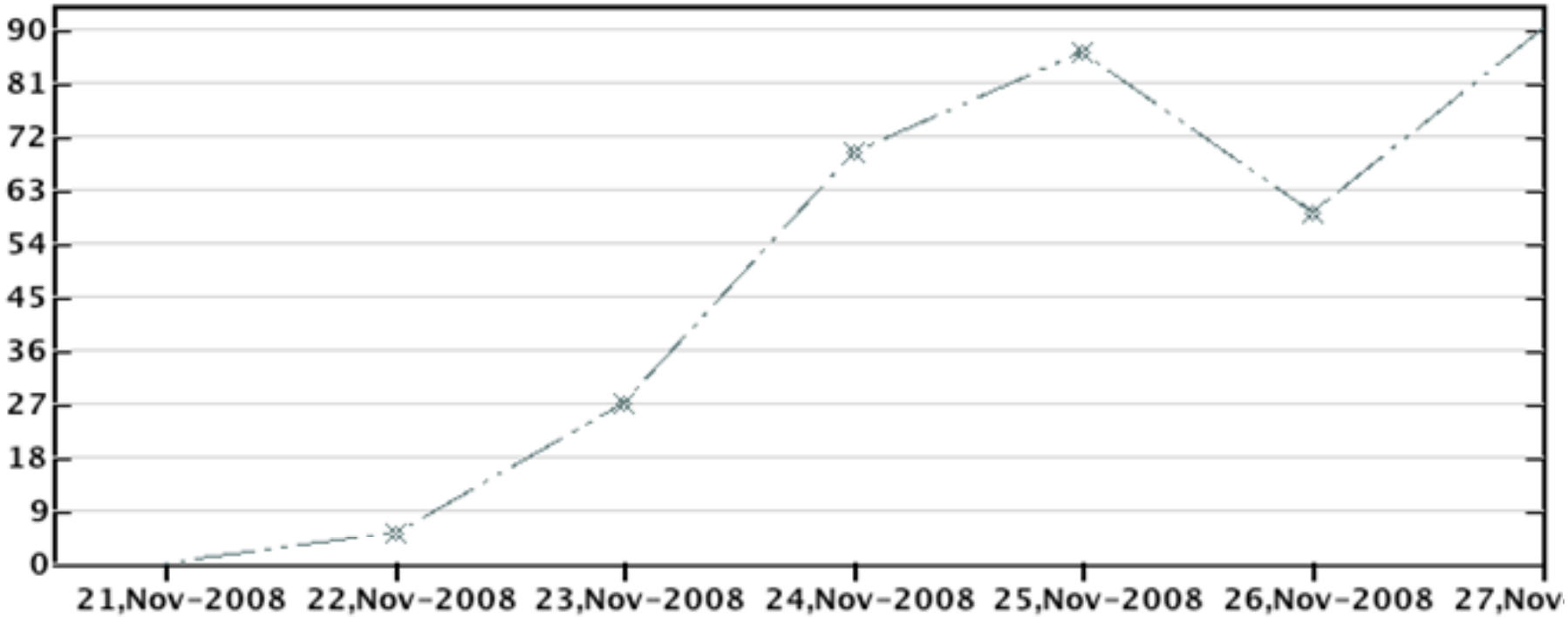


1. Activity classification



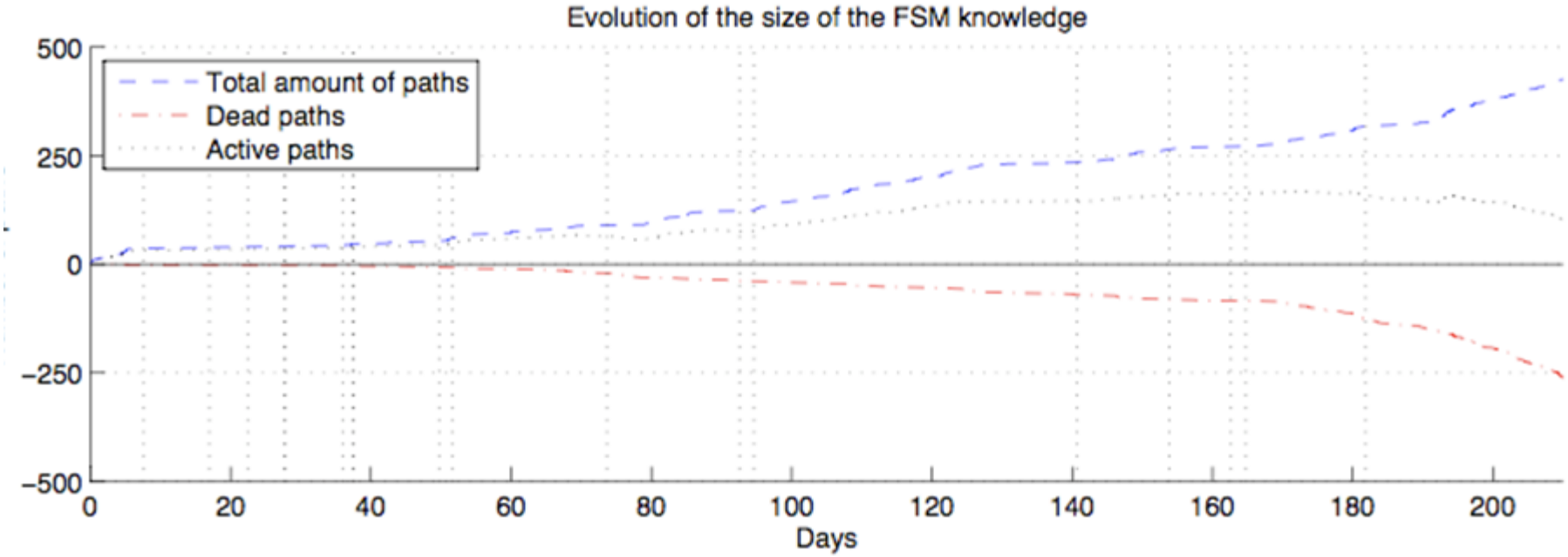
- The interaction with the FSM model can be used to characterize the network interaction
- What is taken into account
  - Features of the protocol (e.g. “HELO”)
  - Features of the specific exploit tool (e.g. same username)

1. Activity classification
The Conficker example



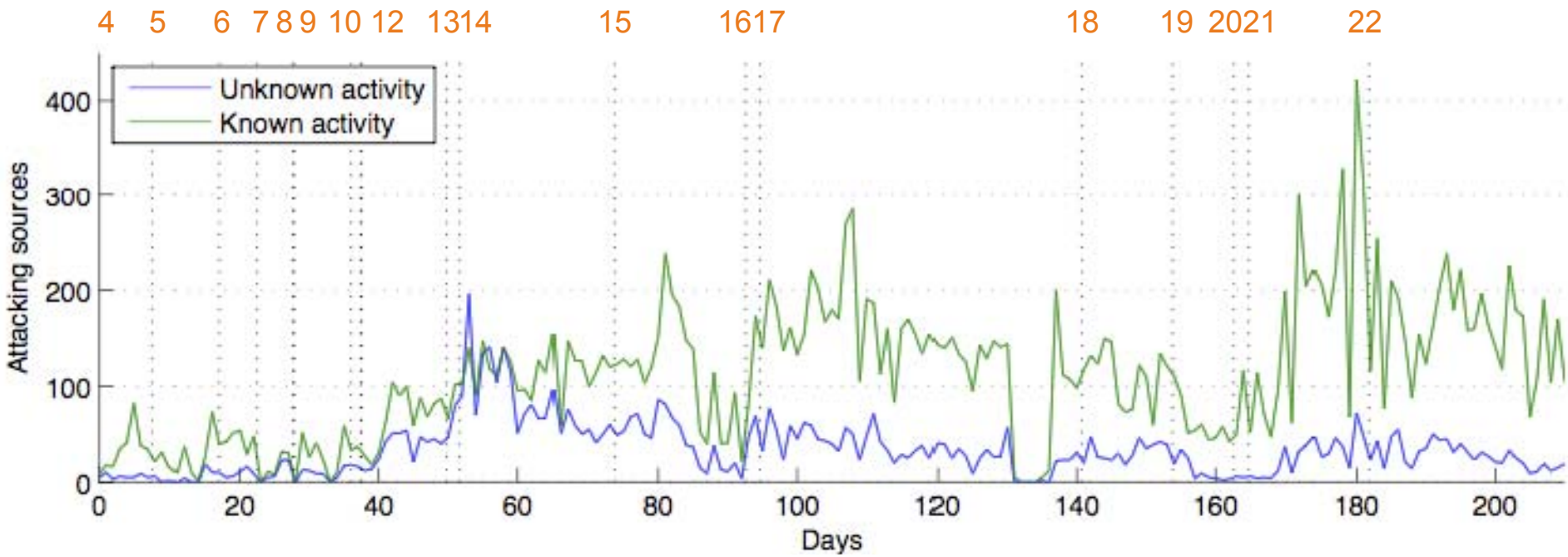
- November 2008: raise of the Conficker worm
  - SGNET generates a new path for the anonymous NetBIOS authentication used by the worm

How difficult is it?



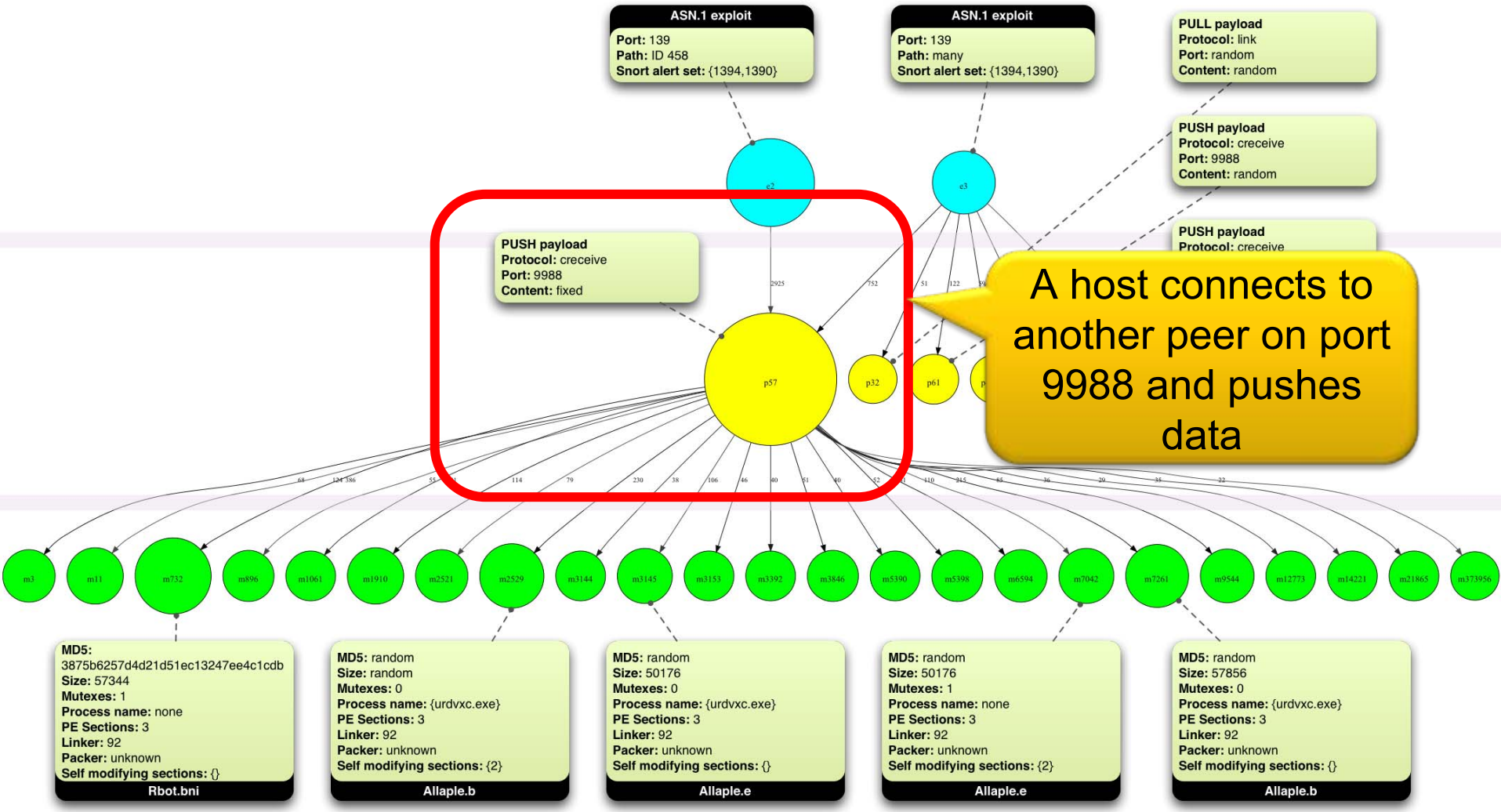
- Total number of traversals generated by the deployment
- Process of death and birth of traversals

How effective is it?



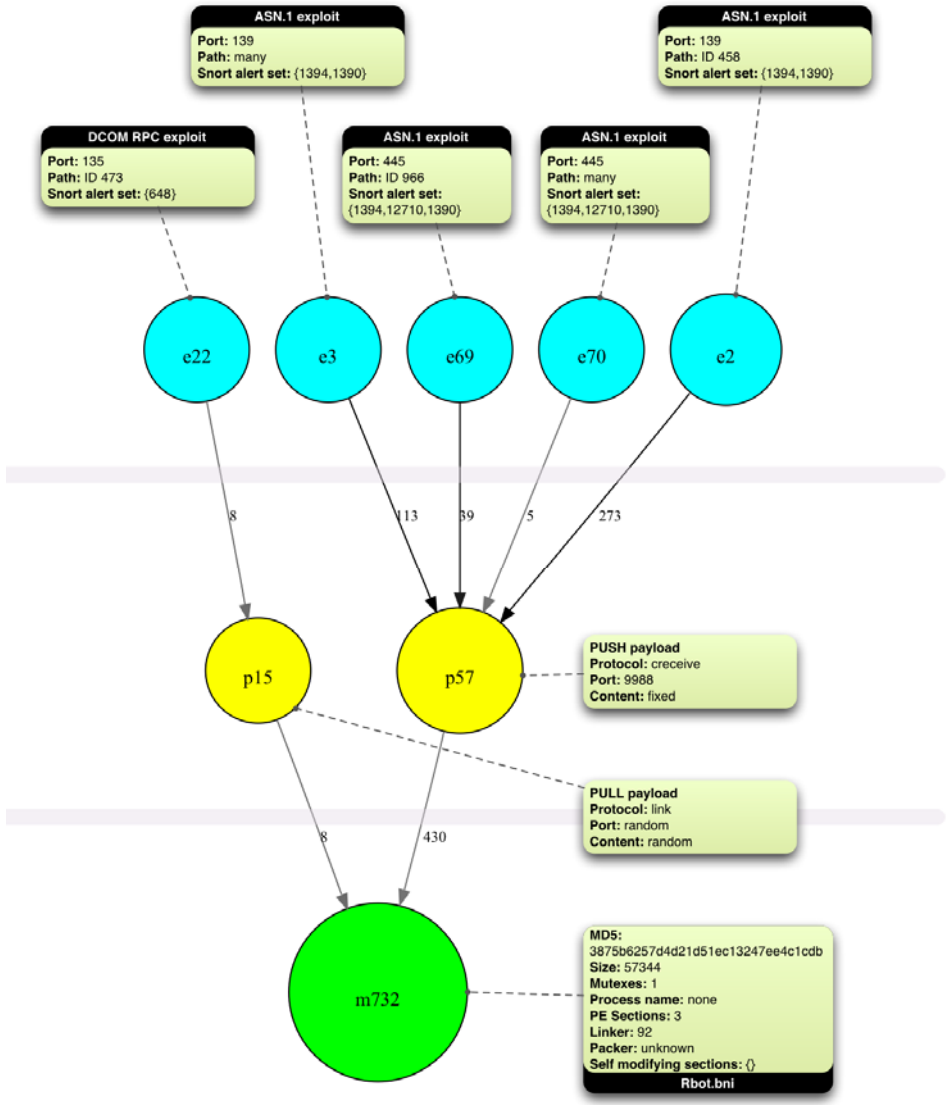
- An increase in load handled by the system is “absorbed” by the learning process

Exploit reuse (ASN.1)



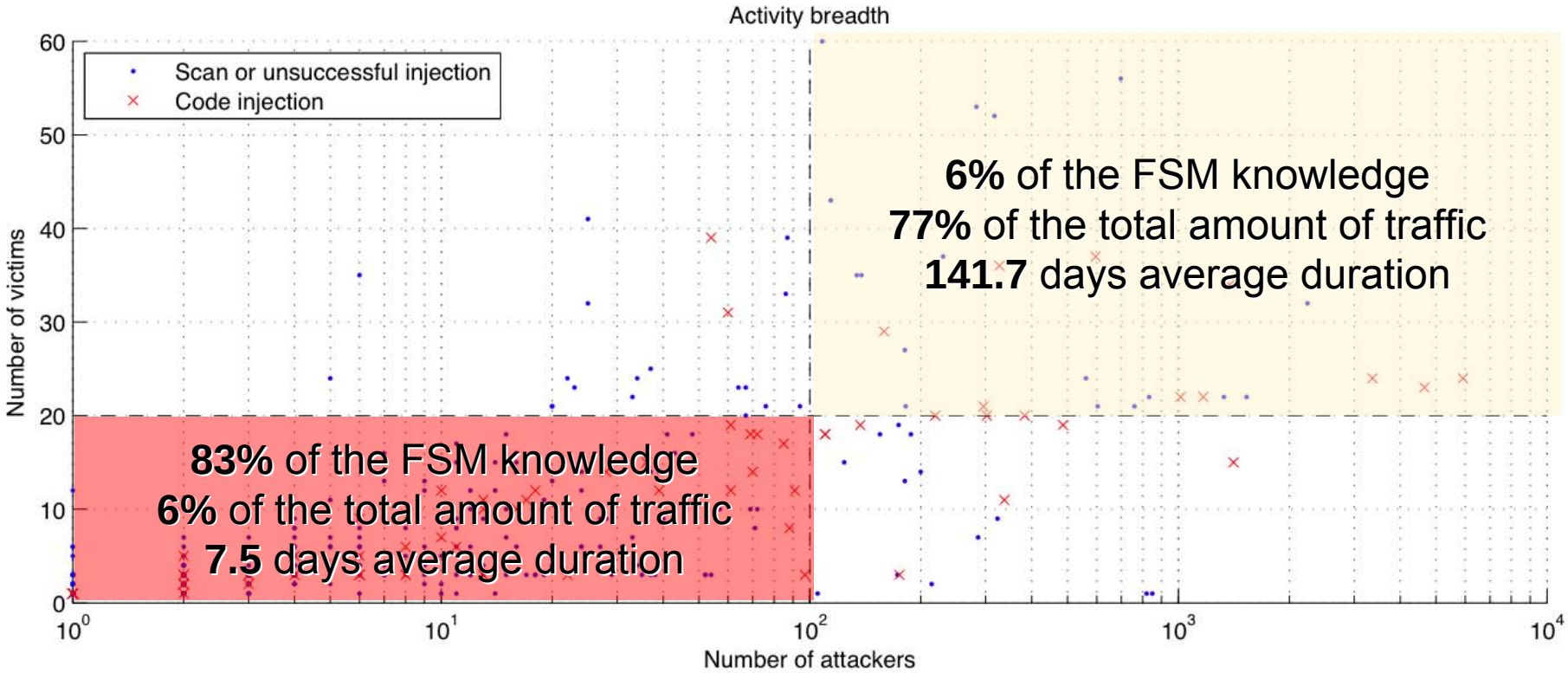
Multi-headed propagation

- Known propagation strategies for Rbot.bni
  - The same malware type uses very different propagation strategies
  - IDS such as Snort expect the ASN.1 exploit only on port 445, instead we are witnessing it also on port 139!



3. Automated threat response
The problem

- Each different activity type is plotted according to the number of involved attackers and victims (its “size”)



Overview

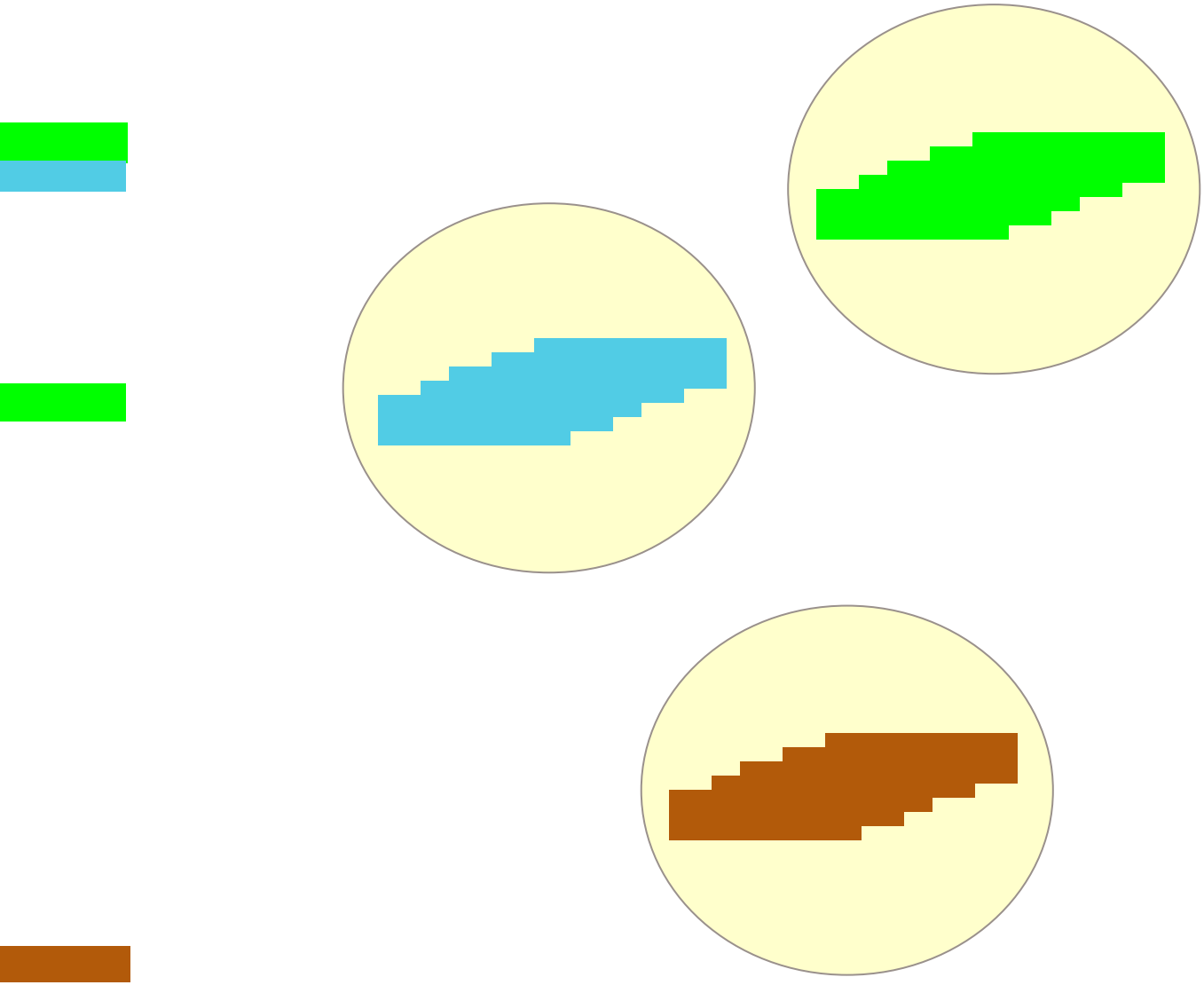
- Introduction
  - Data Acquisition
  - Data Enrichment
  - **Threats Analysis**
- Conclusions

From raw events to meta data

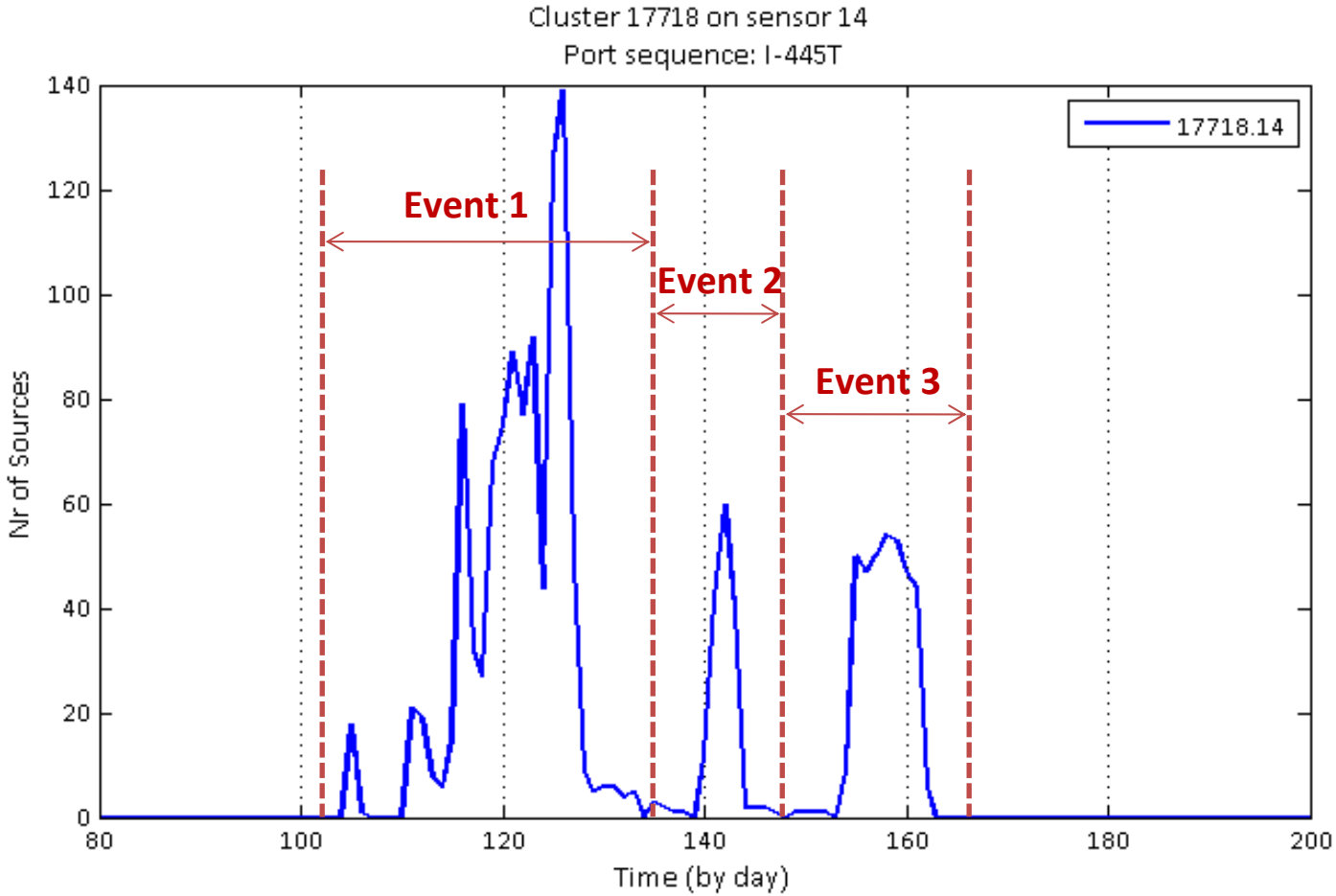
```
13:08:05.737768 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: . 342:342(0) ack 1449 win 31856 <nop
,nop,timestamp 1247771 114849487> (DF)
13:08:07.467571 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: . 1449:2897(1448) ack 342 win 31856
<nop,nop,timestamp 114849637 1247771> (DF)
13:08:07.707634 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: . 2897:4345(1448) ack 342 win 31856
<nop,nop,timestamp 114849637 1247771> (DF)
13:08:07.707922 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: . 342:342(0) ack 4345 win 31856 <nop
,nop,timestamp 1247968 114849637> (DF)
13:08:08.057841 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1045 > ns.de.ibm.net.domain: 8928+ PTR? 110.107.102.209.in-addr.arpa. (46)
13:08:08.747598 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: P 4345:5793(1448) ack 342 win 31856
<nop,nop,timestamp 114849813 1247968> (DF)
13:08:08.847870 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: FP 5793:6297(504) ack 342 win 31856
<nop,nop,timestamp 114849813 1247968> (DF)
13:08:08.848063 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: . 342:342(0) ack 6298 win 31856 <nop
,nop,timestamp 1248082 114849813> (DF)
13:08:08.907566 ppp0 < ns.de.ibm.net.domain > slip139-92-26-177.ist.tr.ibm.net.1045: 8928* 3/1/1 PTR dsl-usw-cust-110.inetarena.com., P
TR fingerless.or (199)
13:08:09.151742 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: F 342:342(0) ack 6298 win 31856 <nop
,nop,timestamp 1248112 114849813> (DF)
13:08:10.137603 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: . 6298:6298(0) ack 343 win 31856 <no
p,nop,timestamp 114849967 1248112> (DF)
13:09:01.984210 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: S 920197285:920197285(0) win 32120 <
mss 1460,sackOK,timestamp 1253395 0,nop,wscale 0> (DF)
13:09:03.097569 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: S 1222277738:1222277738(0) ack 92019
7286 win 32120 <mss 1460,sackOK,timestamp 114855252 1253395,nop,wscale 0> (DF)
13:09:03.098197 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 1:1(0) ack 1 win 32120 <nop,nop,ti
mestamp 1253507 114855252> (DF)
13:09:03.102171 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: P 1:322(321) ack 1 win 32120 <nop,no
p,timestamp 1253507 114855252> (DF)
13:09:04.147613 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 1:1(0) ack 322 win 31856 <nop,nop,
timestamp 114855369 1253507> (DF)
13:09:04.507608 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 1:1449(1448) ack 322 win 31856 <no
p,nop,timestamp 114855369 1253507> (DF)
13:09:04.507934 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 322:322(0) ack 1449 win 31856 <nop
,nop,timestamp 1253648 114855369> (DF)
13:09:05.627604 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 1449:2897(1448) ack 322 win 31856
<nop,nop,timestamp 114855491 1253648> (DF)
13:09:05.857649 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 2897:4345(1448) ack 322 win 31856
<nop,nop,timestamp 114855491 1253648> (DF)
13:09:05.857918 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 322:322(0) ack 4345 win 31856 <nop
,nop,timestamp 1253783 114855491> (DF)
13:09:06.907557 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: FP 4345:5792(1447) ack 322 win 31856
 <nop,nop,timestamp 114855627 1253783> (DF)
13:09:06.907887 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 322:322(0) ack 5793 win 31856 <nop
,nop,timestamp 1253888 114855627> (DF)
13:09:07.401205 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: F 322:322(0) ack 5793 win 31856 <nop
,nop,timestamp 1253937 114855627> (DF)
13:09:08.317623 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 5793:5793(0) ack 323 win 31856 <no
p,nop,timestamp 114855780 1253937> (DF)
```

Raw tcpdump traces

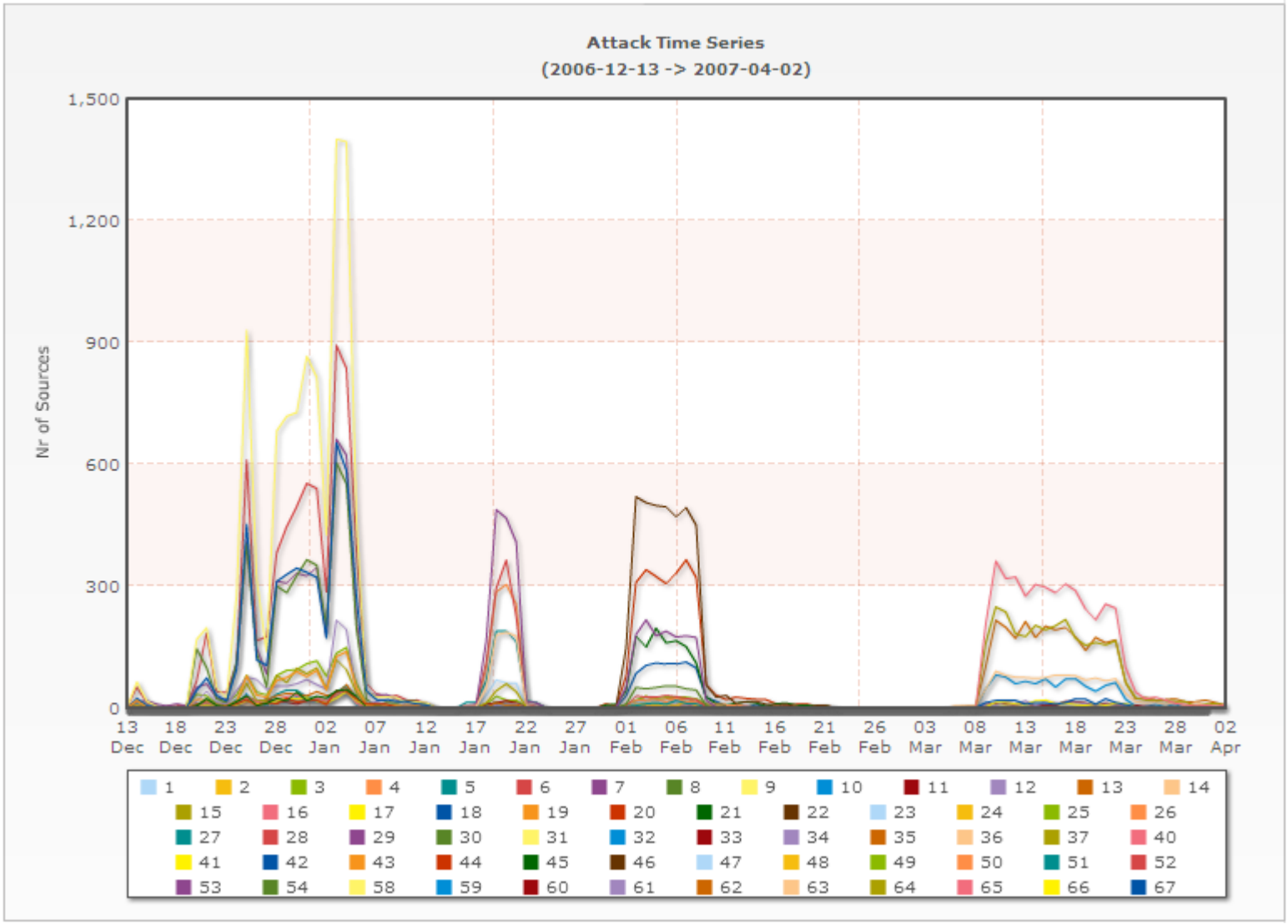
Clusters



Attack Events



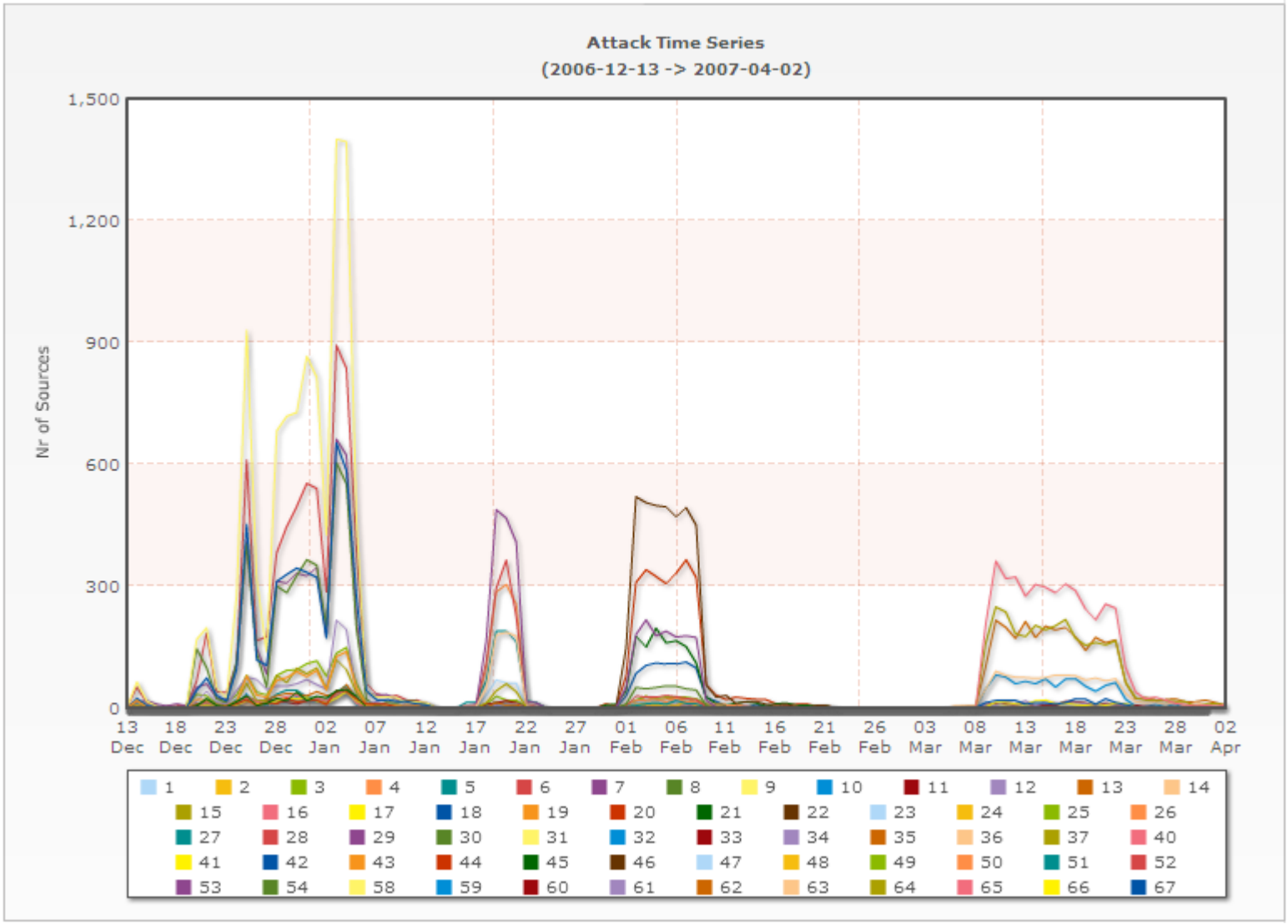
Attack Events



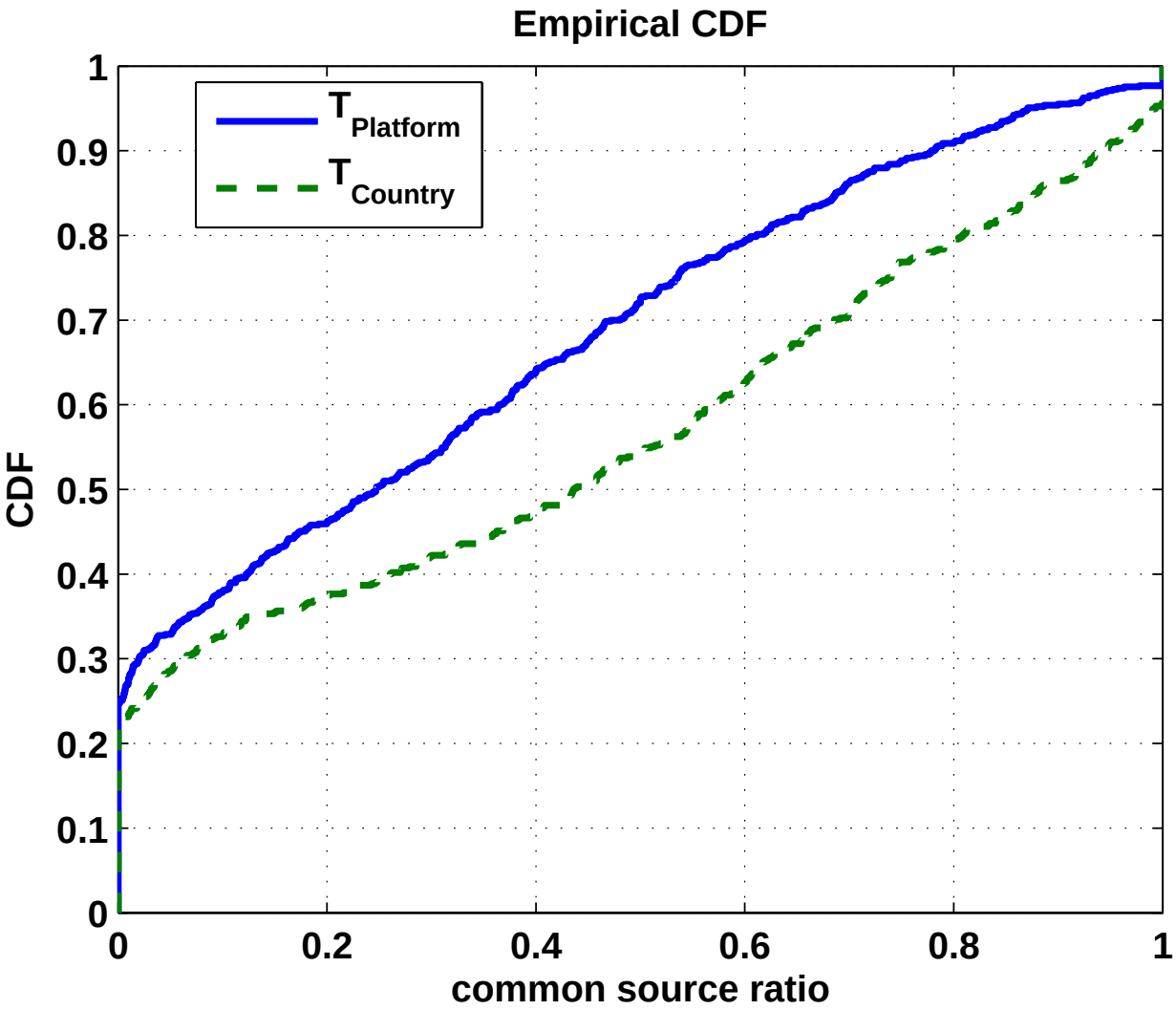
A few examples of ongoing work

- Evolution of attack events may reveal information about the “keep alive” strategies of the attackers
- Multi dimensional analysis enables us to derive hidden links between attack events.
- Contextual information regarding the malware gives insight on code evolution, transformation.

Attack Events split by …

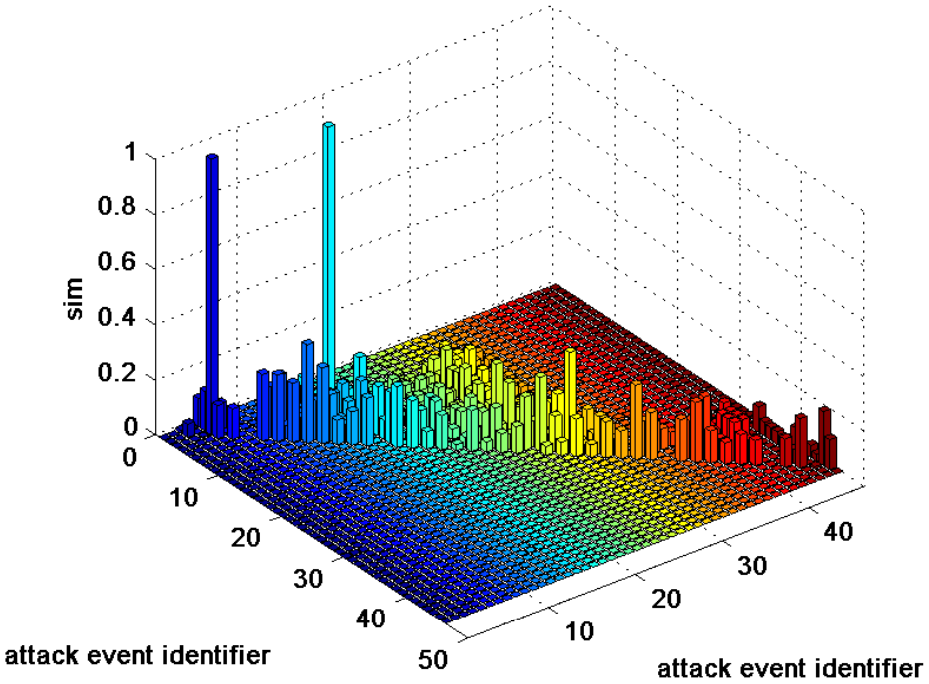


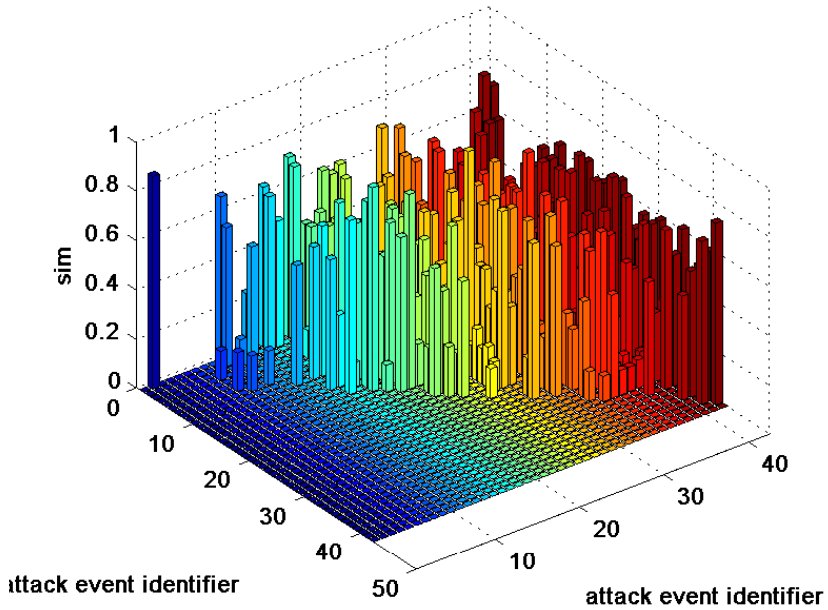
Not a single explanation



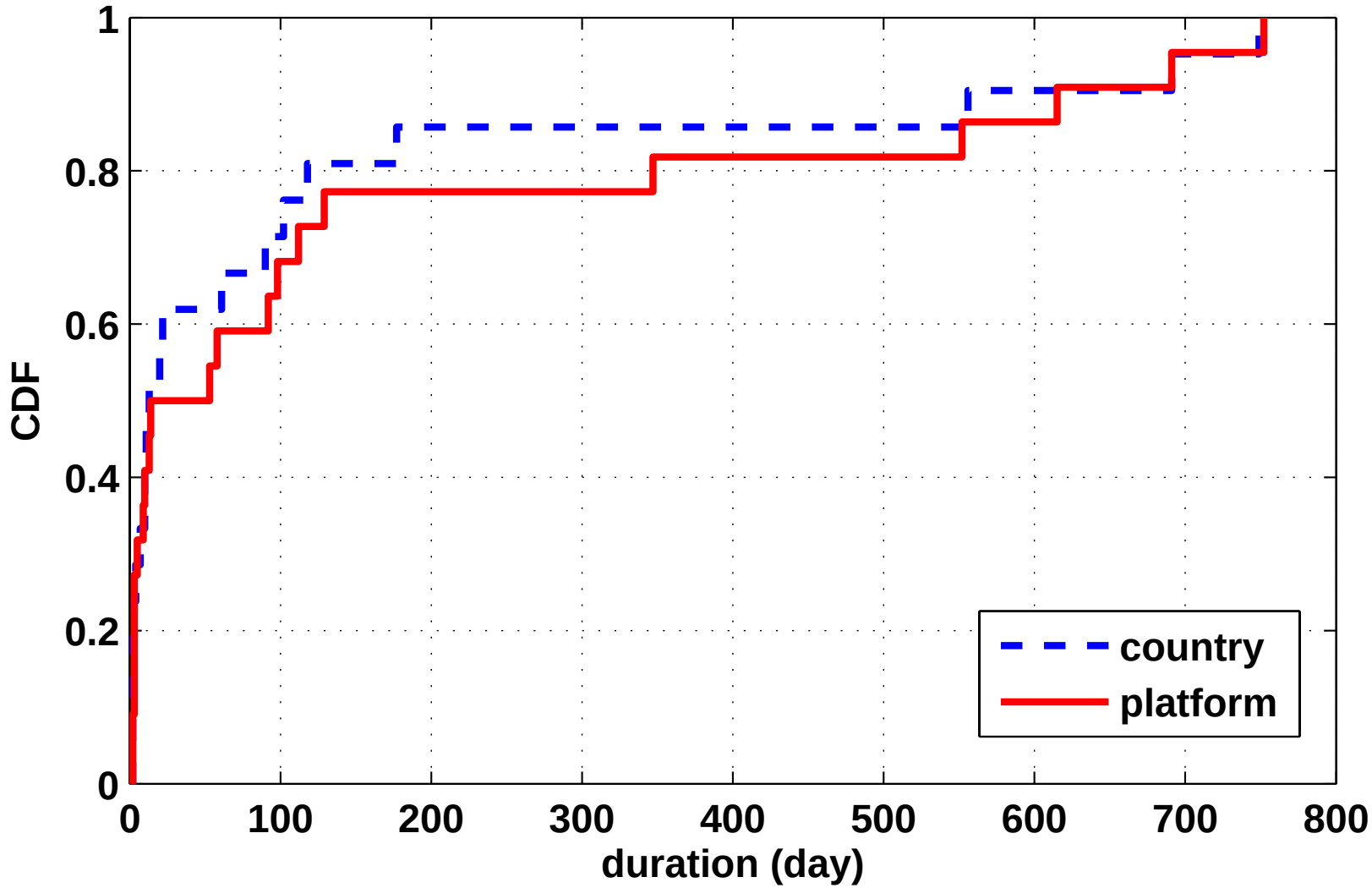
2 distinct survival strategies

- 2 distinct groups of attack events highlighting different evolutions
  - Left side: attack events have common IPs only with their direct predecessor and successor event
  - Right side: attack events have common IPs with all other events over a 700 days period of time





Can zombie armies exist for that long?

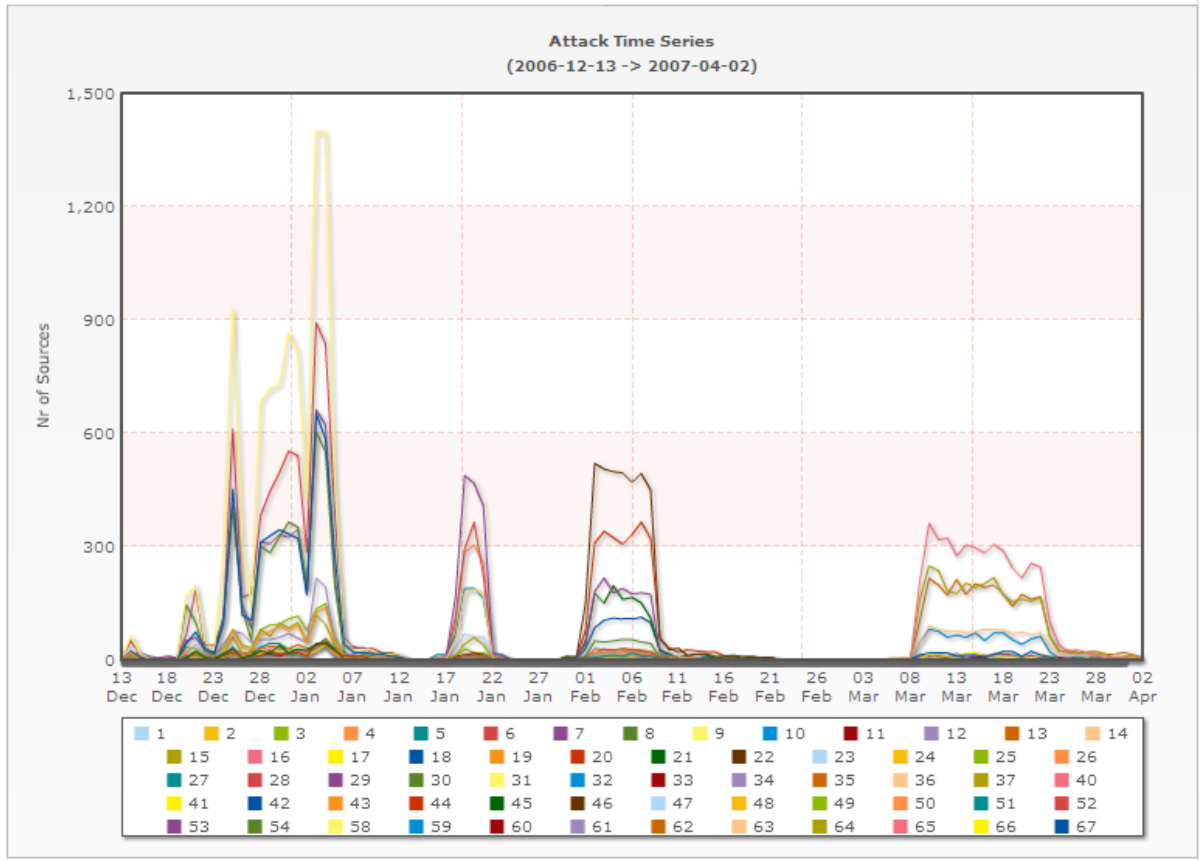


Multidimensional analysis

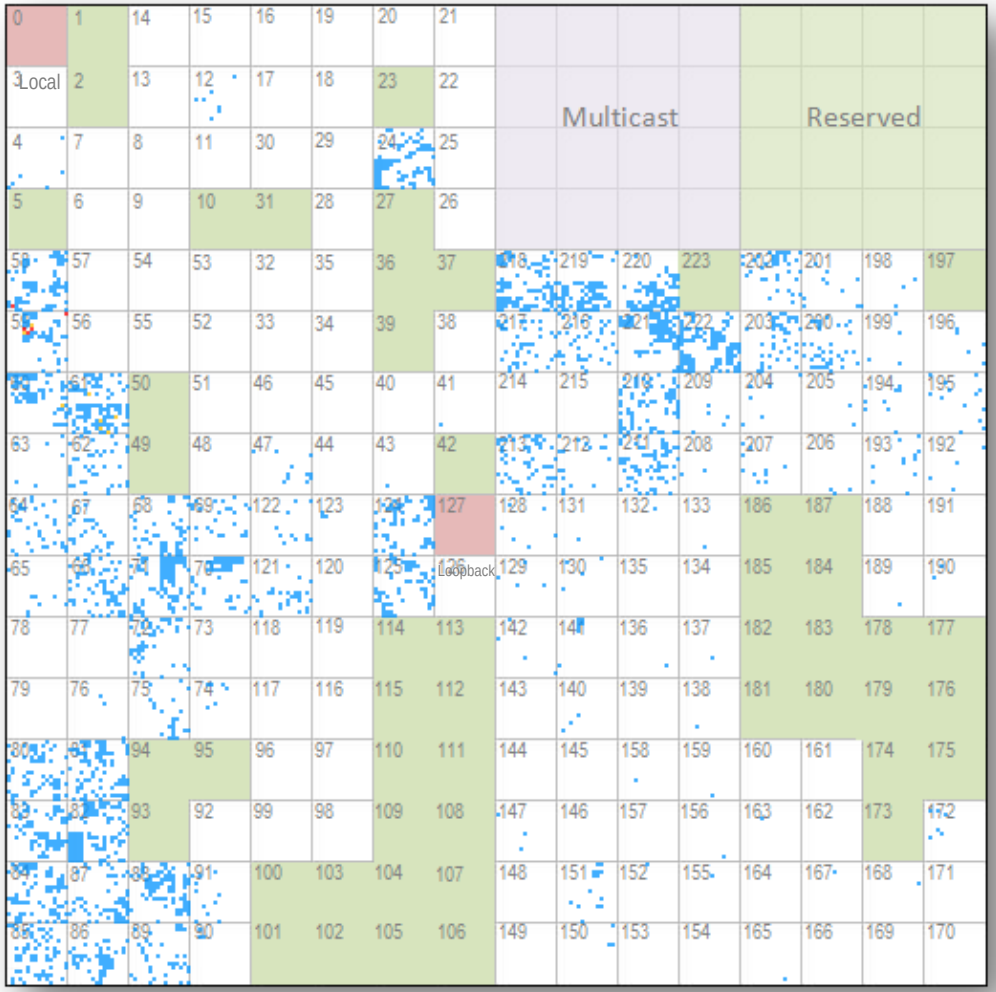
- If long term phenomena exist, how can they be explained ?
- Are they simply due to some coincidence or experimental errors?
- If these events have not been grouped randomly together, they should have some other characteristic(s) in common

Example 1+: Adding the platforms viewpoint

- Those 4 botnet waves have hit the same group of platforms
- <u>But</u>: not all botnet waves came from the same groups of IP Netblocks
  - Dynamic evolution of the botnet population
  - Still, certain “stable” clusters of IP blocks (see ipmaps on next slides)



Example 1: Botnet wave 1



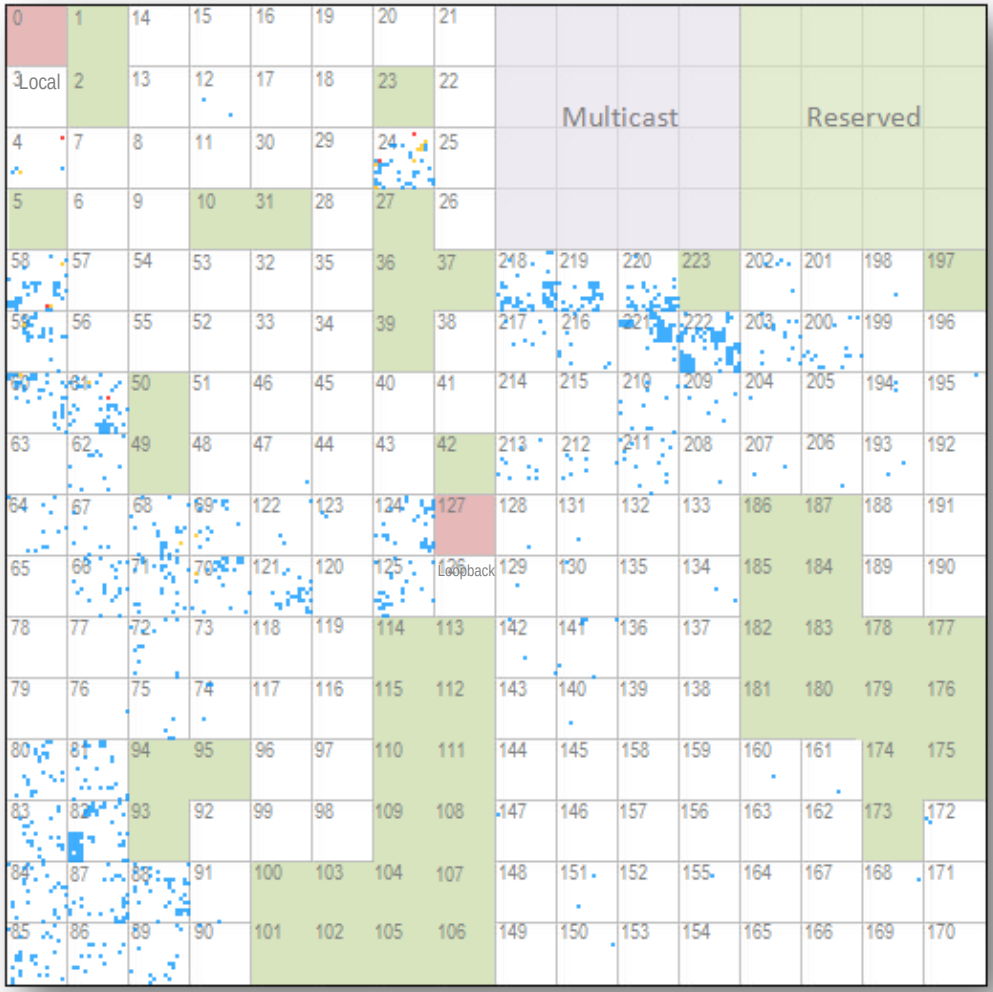
Intensity (rel. to max)

- > 0.66
- 0.33 < x < 0.66
- < 0.33

IPv4 Map

= IANA reserved

Example 1: Botnet wave 2



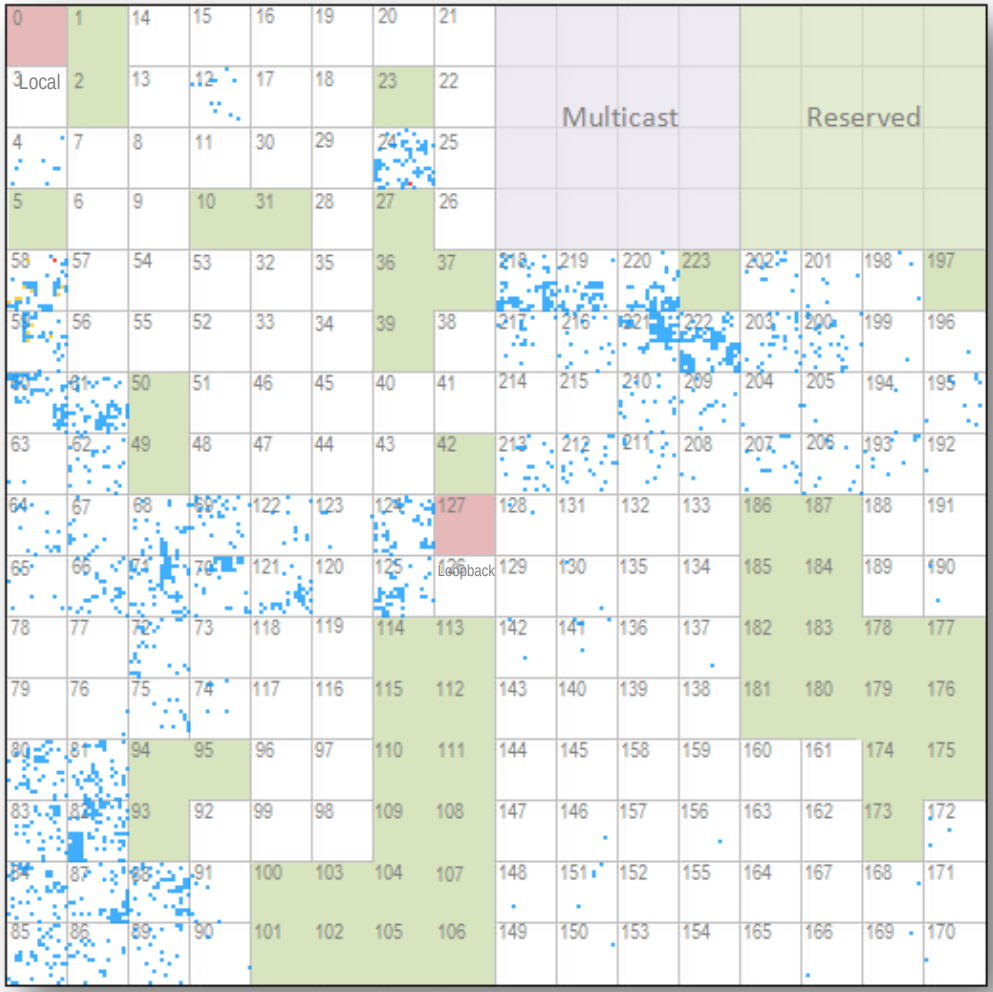
Intensity (rel. to max)

- > 0.66
- 0.33 < x < 0.66
- < 0.33

IPv4 Map

= IANA reserved

Example 1: Botnet wave 3



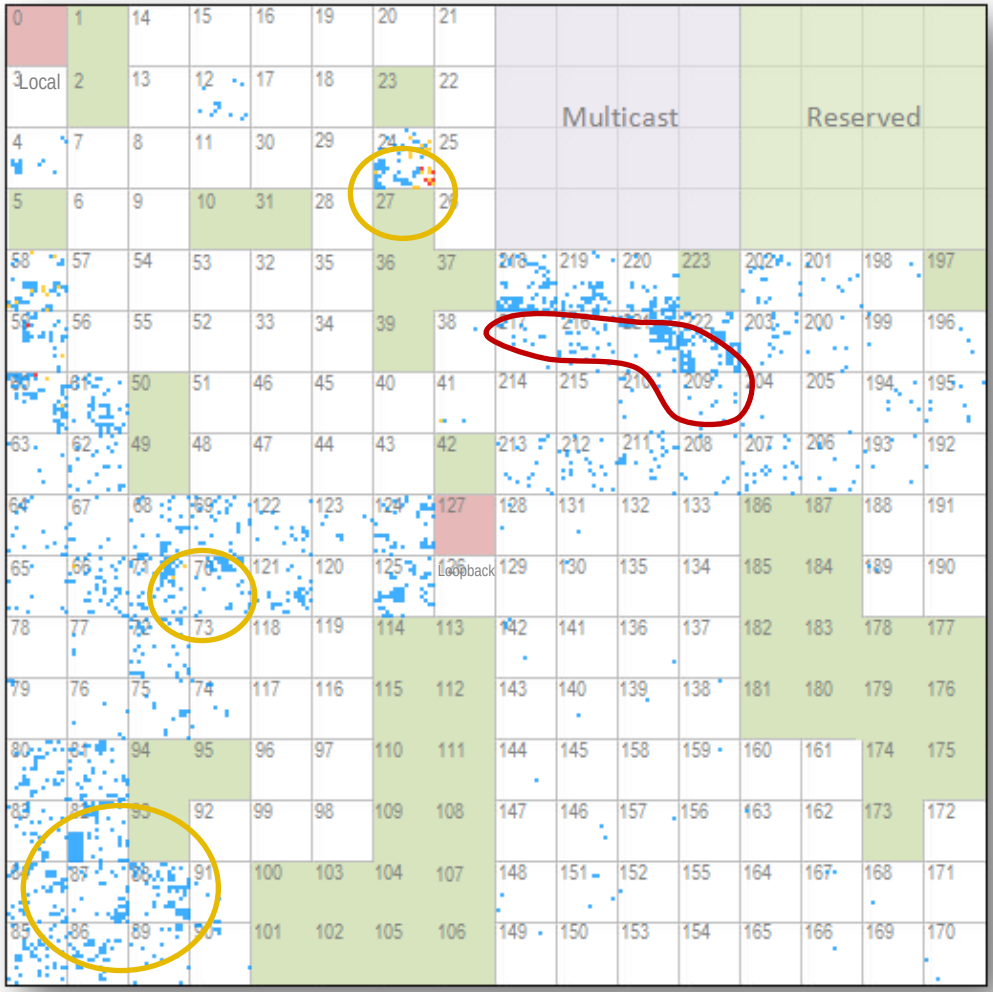
Intensity (rel. to max)

- > 0.66
- 0.33 < x < 0.66
- < 0.33

IPv4 Map

= IANA reserved

Example 1: Botnet wave 4



Intensity (rel. to max)

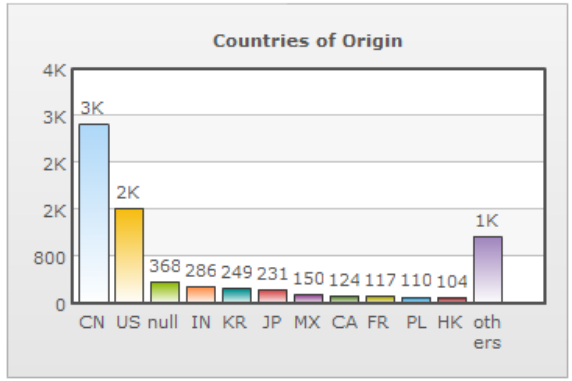
- > 0.66
- 0.33 < x < 0.66
- < 0.33

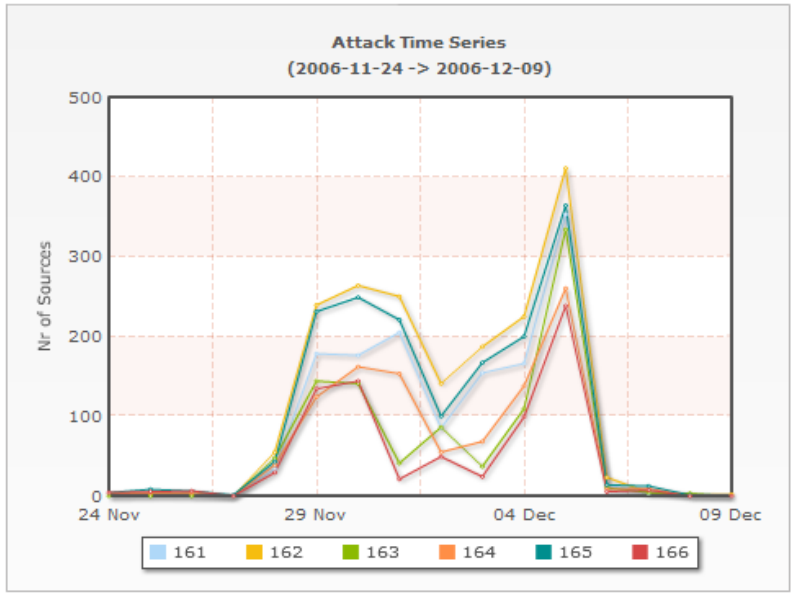
IPv4 Map

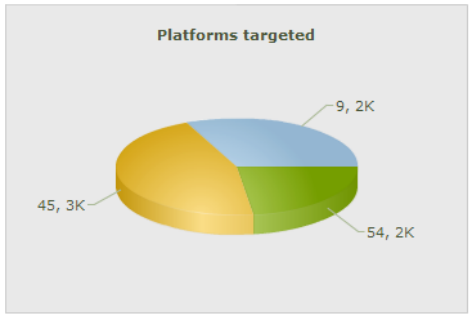
= IANA reserved

Example 2: Dimension-4 viewpoints

- "Multi-headed" attack tool
  - Nov. 2006
  - Port. Seq.: 1433T – 5900T
  - 7.3K sources
  - Dimension-4 concept:
    - Same group of countries
    - Same group of subnets
    - Same time series
    - Same group of 3 sensors hit, all in the same /8!







Ongoing work

- Many features can be used to find relationships between groups of events.
- Not all features are relevant all the time
- There is work in progress on building an automated framework that includes the expert knowledge in order to extract meaningful sets to reason about the modus operandi of the malicious actors.

Overview

- Introduction
  - Data Acquisition
  - Data Enrichment
  - Threats Analysis
- **Conclusions**

Conclusions

- The WOMBAT likes to have new friends.
  - Join the team!
- The WOMBAT has plenty of toys and is eager to share them with his partners.
  - Benefit from the datasets and tools developed so far
- The WOMBAT is always hungry for new datafeeds.
  - Install a sensor at your place.
- CONTACT POINT: marc_dacier@symantec.com

- Thanks!
- Questions?