ICT-216026-WOMBAT
Worldwide Observatory of Malicious Behaviors and Attack Threats

Sotiris Ioannidis
FORTH
Project Motivation

- Cyber-crime becomes harder to battle
  - Malware specifically designed to defeat today's best practices
  - Organization is consolidating malicious activity into a profitable professional endeavour

- Data collection and sharing is limited
  - Collection initiatives are heterogeneous
  - Privacy or confidentiality limits sharing
  - Data structure and analysis remains private

- No investigation framework exists for consistent and systematic malware analysis
The WOMBAT Consortium
Main objectives and principles

Data enrichment (WP4)

- Malware analysis
- Context analysis

Storage Analysis

- Data acquisition (WP3)
  - Honeypots
  - Crawlers
  - External feeds

- New collection practices

Meta-data Analysis

- Threat analysis (WP5)
  - New security technologies
  - New security practices
  - Knowledge
Services/Tools

- Argos
- Shelia
- Paranoid Android
- Anubis
- SGNET
- VirusTotal
- Harmur
- Bluebat

- HoneySpider
- Network
- Honeybuddy
- FIRE
- Exposure
- Banomad
Ongoing data feeds

- Several of the new services will remain available for the greater good of the community

- Symantec has launched the WINE initiative, as a follow up to its experience within WOMBAT

- WINE will keep supporting some of these data feeds and provide a place to host and use these data.
WAPI

- The WAPI is the common interface to most of the new data feeds

- WAPI has been offered to the community and is being used by other data collectors

- WAPI is now an open source project hosted on sourceforge.
Technical transfer

Several partners have initiated technical transfers:

- Hispasec with Banomad
- NASK with HoneySpider Network
- Symantec with WINE (SGNET and HARMUR) and TRIAGE
Impact

- Improve our knowledge about malicious code
  - through data exchange
    - Malware
    - Analysis results for context consolidation
  - to understand malware activities and trends
- Supported by technologies and tools
  - New sensors for data acquisition (wireless, …)
  - New analysis techniques (code, context, …)
- To improve our posture w.r.t. threats
  - Proposals for new technologies for enterprise and home-use
  - Proposals for new practices (CERTs, ISPs) and regulations
Other stuff
Visibility

- More than 60 peer reviewed publications (conferences, journal, books)
- 55 other dissemination activities
- Several dozens of articles in mass media
- The WOMBAT/BADGERS workshop was very well attended and received
- “WOMBAT” is a known and well regarded project within the security community.
Outcome: the big picture

- A very strong team
- An extraordinary visibility
- A role model in operational security
- A number of new services on the web
- Ongoing data feeds collaboration
- The WAPI
- Several industrial technical transfers.
- A number of lessons learned on the threats landscape
Lessons learned

- The TRIAGE framework enables multi dimensional analysis of security events.

- It has been applied to several data sources and led to interesting findings. It has been used and is being transferred within Symantec.

- Publications of these lessons contributed significantly to the visibility of WOMBAT.