
WOMBAT: Knowing your enemy

Ing. Stefano Zanero, PhD

Politecnico di Milano

Dip. Elettronica e Informazione

Pula, 5/11/2008

Knowledge is the key for victory



- Knowing your enemy is the key to success
 - *“He will win who knows when to fight and when not to fight... He will win who, prepared himself, waits to take the enemy unprepared. Hence the saying: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.” [Sun-Tsu]*
 - Perhaps the most often quoted, and less often practiced, sentence in history
- Understanding is the key to (re)acting sensibly

Disappearance of the worms



- In 2001 we were all worried of worms getting wormier
 - “In July 2001, Code Red spread to \$HUGE_INT systems within \$SMALL_INT hours; the worldwide economic impact was estimated to be \$INSANE_FIGURE billions. SQL Slammer was even faster. We'll see an even greater increase in the speed and destructive capabilities of threats.
 - The trend was so clear:
 - 2001: Li0n, Code Red, Nimda
 - 2002: Slapper, Klez
 - 2003: SQL Slammer, Blaster, SoBig
 - 2004: Sober, MyDoom, Witty, Sasser
 - I have even an iDefense t-shirt with this list on it!

No more opportunities maybe?



- Why didn't the /bin/ladens of the digital world target the infrastructure?
 - FX's and Michael Lynn's works showed the potential to attack routers directly
 - Even with a traditional worm, windows of opportunity:
 - June 2003: MS03-026, RPC-DCOM Vulnerability (Blaster) + Cisco IOS Interface Blocked by IPv4 Packets
 - April 2004: MS04-011, LSASS Vulnerability (Sasser) + TCP Vulnerabilities in Multiple IOS-Based Cisco Products (resets)
- Yet, no worm. Should we just relax?
 - Worms have handed over the scene to botnets

Rise of the robots



- Bots, bots everywhere
 - When I was young (1998), bots were IRC warriors' stuff
 - We used to call remote control trojans “zombies”, and they were usually DDoS tools (2000-2)
- Today's bots are different
 - Intelligent, evolving, with complex C&C infrastructures
 - Larger botnets (10k common, 1M+ seen)
 - Phishing & spamming are more difficult to track than DDoS
- How do we track them? How do we analyze them?
 - Worm explosive propagation vs. bot slow and steady diffusion: there's no network telescope that can see them

Current initiatives



- Efforts by vendors
 - ATLAS (Arbor)
 - DeepSight (Symantec, formerly SecurityFocus)
- Community and no-profit efforts
 - Dshield and the Internet Storm Center (SANS)
 - Network Telescopes
 - The HoneyNet project
 - Leurrecom project
 - MWCollect Alliance

Enter the WOMBAT



Project Motivation

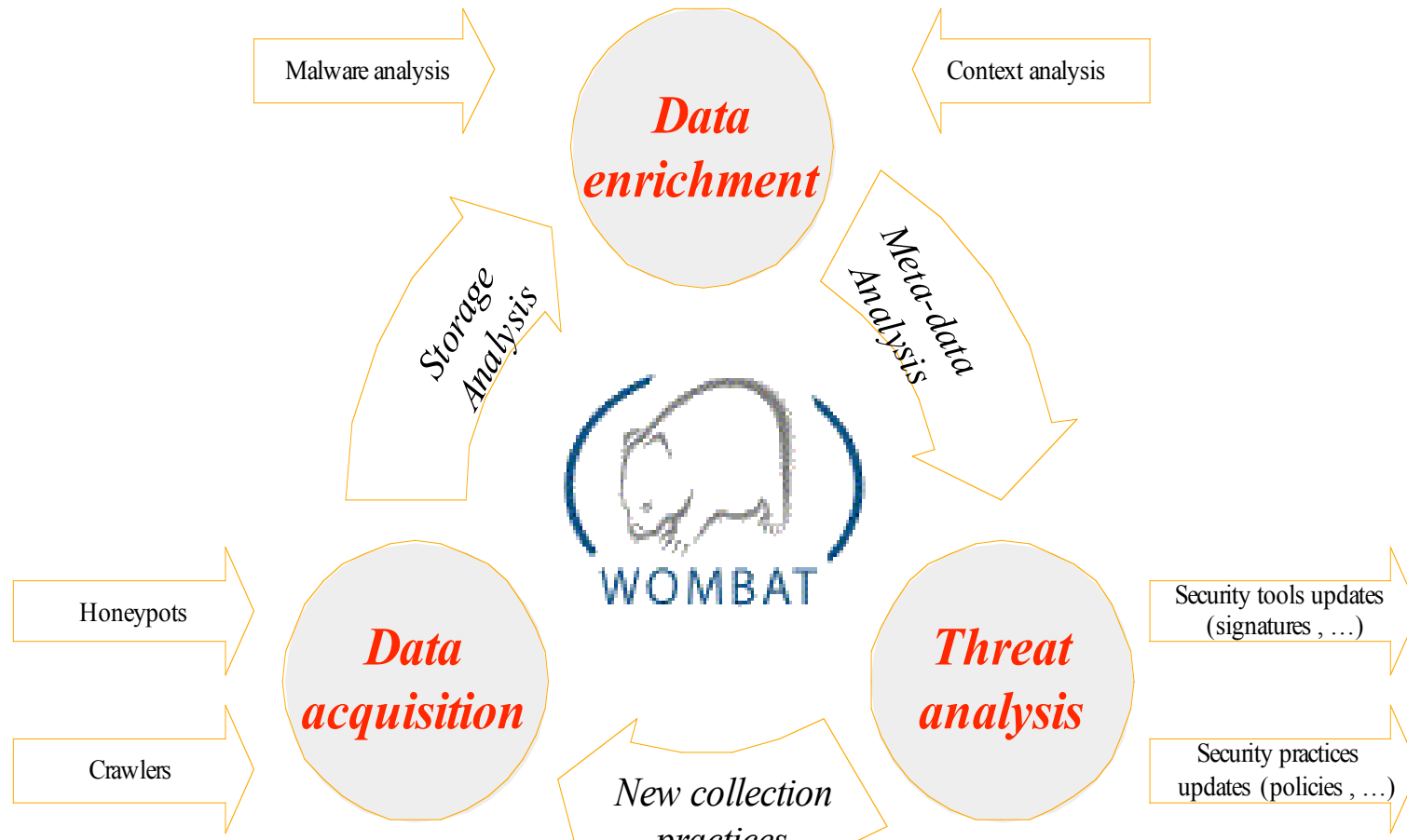


- Cyber-crime becomes harder to battle
 - Malware specifically designed to defeat today's best practices
 - Organization is consolidating malicious activity into a profitable professional endeavour
- Data collection and sharing is limited
 - Collection initiatives are heterogeneous
 - Privacy or confidentiality limits sharing
 - Data structure and analysis remains private
- No investigation framework exists for consistent and systematic malware analysis
 - How to link the binary, the motivation and the perpetrators?

The WOMBAT Consortium



Main objectives and principles



Project aims and innovation



- New data gathering tools
 - Advanced features (high interaction, real-time analysis)
 - New targets (wireless, bluetooth, RFID, ...)
- Tools and techniques for characterization of malware
 - Malware-based analysis
 - Behavioral techniques
 - Code analysis
 - Contextual analysis
- Framework and tools for qualitative threat analysis
 - Creation of an early warning system

Key results and milestones



- **Infrastructural**
 - Invitation-based Workshop on Internet Security Threats Data Collection and Sharing (WISTDCS), held in Amsterdam, 21-22/04
 - Proceedings by the IEEE CS, available soon on IEEEXplore
 - State of the art review and requirements analysis deliverables complete
 - Infrastructure design to be delivered soon
 - 2009: development and deployment of new sensors (incl. BlueBat, a Bluetooth sensor developed by POLIMI)
- **Characterization**
 - End of 2008: code behavior analysis specifications
 - 2009: automated behavior and structure analysis tools
 - Early 2010: gathering and analysis of contextual informations
- **Early warning and root cause analysis: exp. 2010**

Questions ?



Thanks for your attention!

www.wombat-project.eu

Stefano Zanero

stefano.zanero@polimi.it