THE WOMBAT API
handling incidents by querying a world-wide network of advanced honeypots

Piotr Kijewski, Adam Kozakiewicz

15th June 2010
22nd Annual FIRST Conference, Miami
WOMBAT Project

- EU 7th FRAMEWORK PROGRAMME (2008-2010)
- Worldwide Observatory of Malicious Behaviour and Attack Threats (http://www.wombat-project.eu)

- 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 approach

Data acquisition (WP3)

Data enrichment (WP4)

Threat analysis (WP5)

Storage analysis

Meta-data analysis

Malware analysis

Context analysis

New collection practices

Honeypots

Crawlers

External feeds

New security technologies

New security practices

Knowledge
Participants

 logos of participating institutions
Existing datasets in WOMBAT

**CLIENT HONEYPOTS**
- Shelia
- HSN
- HARMUR
- Wepawet

**SERVER HONEYPOTS**
- SGNet
- FORTH
- NoAH + extras
- BlueBat

**MALWARE COLLECTIONS**
- VirusTotal
- Anubis

**OTHERS**
- WAPI
WOMBAT API (or WAPI for short)

- What the WAPI is:
  - A SOAP-based API to easily allow a client to traverse a hierarchy of objects, characterized by attributes, methods and references.

- What the WAPI is not:
  - An ontology
  - A detailed specification of how a security related dataset should look like
  - Language-specific. Reference implementation in python, but accessible from any programming language offering a SOAP library (C,C++,Java,PHP,…)
Accessing the datasets

- Mandatory services:
  - `get_objects()`
  - `get_documentation()`
  - `get_methods(object)`
  - `get_references(object)`
  - `get_attributes(object)`
  - `exists(object,identifier)`
  - `call_method(object,identifier,method,atts)`
  - `follow_reference(object,identifier,method,atts)`

- Mandatory objects:
  - Dataset, must have a unique identifier (for example: "hsn")
What else?

- Apart from the previous, hardly any standardization:
  - IP addresses should be specified in dotted decimal format,
  - if one IP address is associated with each object of a given type then the corresponding attribute should be named IPAddress,
  - dates should be specified in the ISO 8601 format, etc.
- SSL-based (certificate) authentication
- Currently only one privilege level (multiple ones will be supported in the future)
The WOMBAT API (version 1.0)

Connecting to the WAPI datasets
- harmur : success
- virustotal : success
- wepawet : success
- anubis : success
- hsn : success
- shelia : success
- sgnet : success
- forth : success

You are connected to 8 WAPI datasets!
Example usage …

```python
> f=virustotal.get_file(md5="3228c641929bb40475c44a26bda8531a")[0]
> print f.first_seen
'2009-05-27 15:38:11'
> an=f.get_first_analysis()
> print an.av_positives_report

{'GData': ['Exploit.PDF-JS.Gen', '19', '2009.05.27'], 'AntiVir': 
['HEUR/HTML.Malware', '7.9.0.168', '2009.05.27'], 'McAfee-GW-Edition': 
['Heuristic.HTML.Malware', '6.7.6', '2009.05.27'], 'Sophos': ['T0j/PDFJs-AX', 
'4.42.0', '2009.05.27'], 'ClamAV': ['Exploit.PDF-63', '0.94.1', '2009.05.27'], 
'Authentium': ['PDF/Obfusc.B!Camelot', '5.1.2.4', '2009.05.27'], 'BitDefender': 
['Exploit.PDF-JS.Gen', '7.2', '2009.05.27'], 'Sunbelt': ['Exploit.PDF-JS.Gen (v)', 
'3.2.1858.2', '2009.05.27'], 'VirusBuster': ['JS.Shellcode.AD', '4.6.5.0', 
'2009.05.26']}
```
In this scenario, the participants take on the role of CERT responders from a bank. The bank needs to conduct a (forensics) investigation of the machine of a client that has reported a fraud case via electronic banking.

The bank up to now has excluded that the fraud was related to phishing or any other physical swindle.

A brief analysis of the infected client does not show any clear evidence of infection, no suspicious BHO is detected and no suspicious registry entries are found in the system…

(First performed by the WOMBAT consortium at the 2nd WOMBAT Workshop in St. Malo, France in September 2009)
The client affected by the fraud is connected to the Internet through an HTTP proxy, and has agreed to give you the list of the HTTP activity of the infected machine in the last week. After a brief look at such activity, you notice a large amount of HTTP requests towards a suspicious domains. Such requests are performed every 20 minutes approximately, during working hours but also during night and weekends.

All the queried URLs are similar to the following one:

http://ijmkkyjves.net/iE=eQBHE8cNe8DRM

So, what happened???
QUESTIONS?

piotr.kijewski@cert.pl