Modeling Malware-driven Honeypots

Gerardo Fernández, Ana Nieto and Javier Lopez

{gerardo,nieto,jlm}@lcc.uma.es

Network, Information and Computer Security (NICS) Lab

University of Malaga, Spain

TrustBus 2017, August 30th 2017

Content

1. Honeypots, objectives and limitations
2. Malware Intelligence
3. Hogney Architecture
4. Study Case: Mirai
5. Conclusions

Honeypots

- **Honeypots: what are they used for ?**
  - All traffic received in them are considered suspicious.
  - **Replicate live services of the production environment:** showing a footprint similar to that of the services offered in the production network.
  - **Research environments:** showing a configuration of honeypots that enables attacks to be captured, to later analyse new techniques used.

Honeypots

- **Honeypots: what are they used for ?**
  - All traffic received in them are considered suspicious.
  - **Replicate live services of the production environment:** showing a footprint similar to that of the services offered in the production network.
  - **Research environments:** showing a configuration of honeypots that enables attacks to be captured, to later analyse new techniques used.
- **Limitations**:
  - General purpose: hard to unleashed all stages of malware behaviour
  - Specific to protocols/applications: + reduced visibility
  - Specialized in predetermined attacks: + reduced visibility
  - Adaptive honeypots: usually combine previous techniques

    ⇨ inheriting these problems

Honeypots

- **Honeypots: what are they used for ?**
  - All traffic received in them are considered suspicious.
  - **Replicate live services of the production environment:** showing a footprint similar to that of the services offered in the production network.
  - **Research environments:** showing a configuration of honeypots that enables attacks to be captured, to later analyse new techniques used.
- **Limitations**:
  - General purpose: hard to unleashed all stages of malware behaviour
  - Specific to protocols/applications: + reduced visibility
  - Specialized in predetermined attacks: + reduced visibility
  - Adaptive honeypots: usually combine previous techniques

    ⇨ inheriting these problems

Honeypots

- **Nowadays, there are myriad of honeypots available...**

Cowrie

Dionaea

Nepenthes

HoneyBOT

HoneyTrap

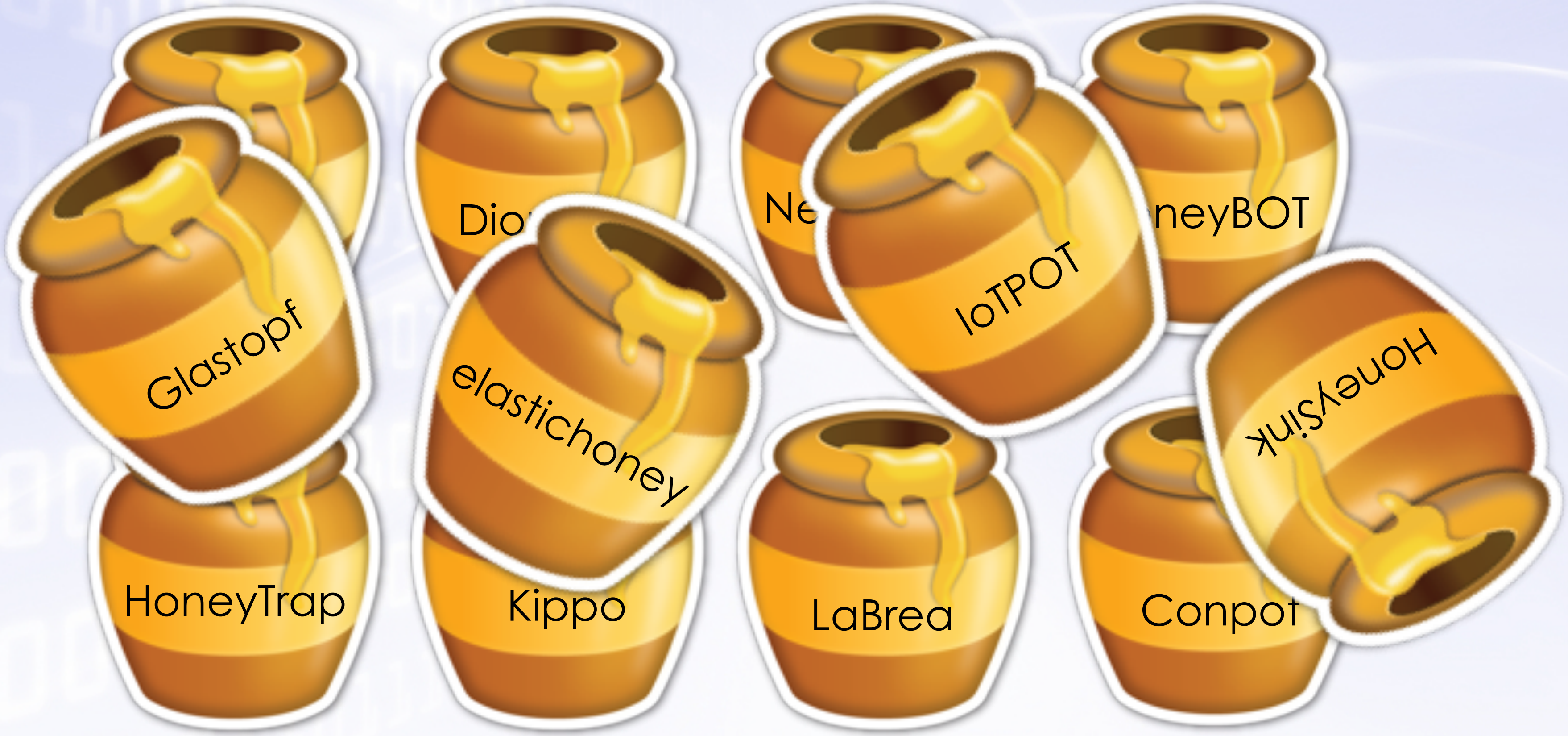
Kippo

LaBrea

Conpot

Honeypots

- **Nowadays, there are myriad of honeypots available...**



Honeypots

- **Nowadays, there are myriad of honeypots available...**

Glastop
BOT
HoneySink
HoneyTrap
Kippo
LaBrea
Conpot

Why not offer them...
“à la carte” ?

Malware Intelligence

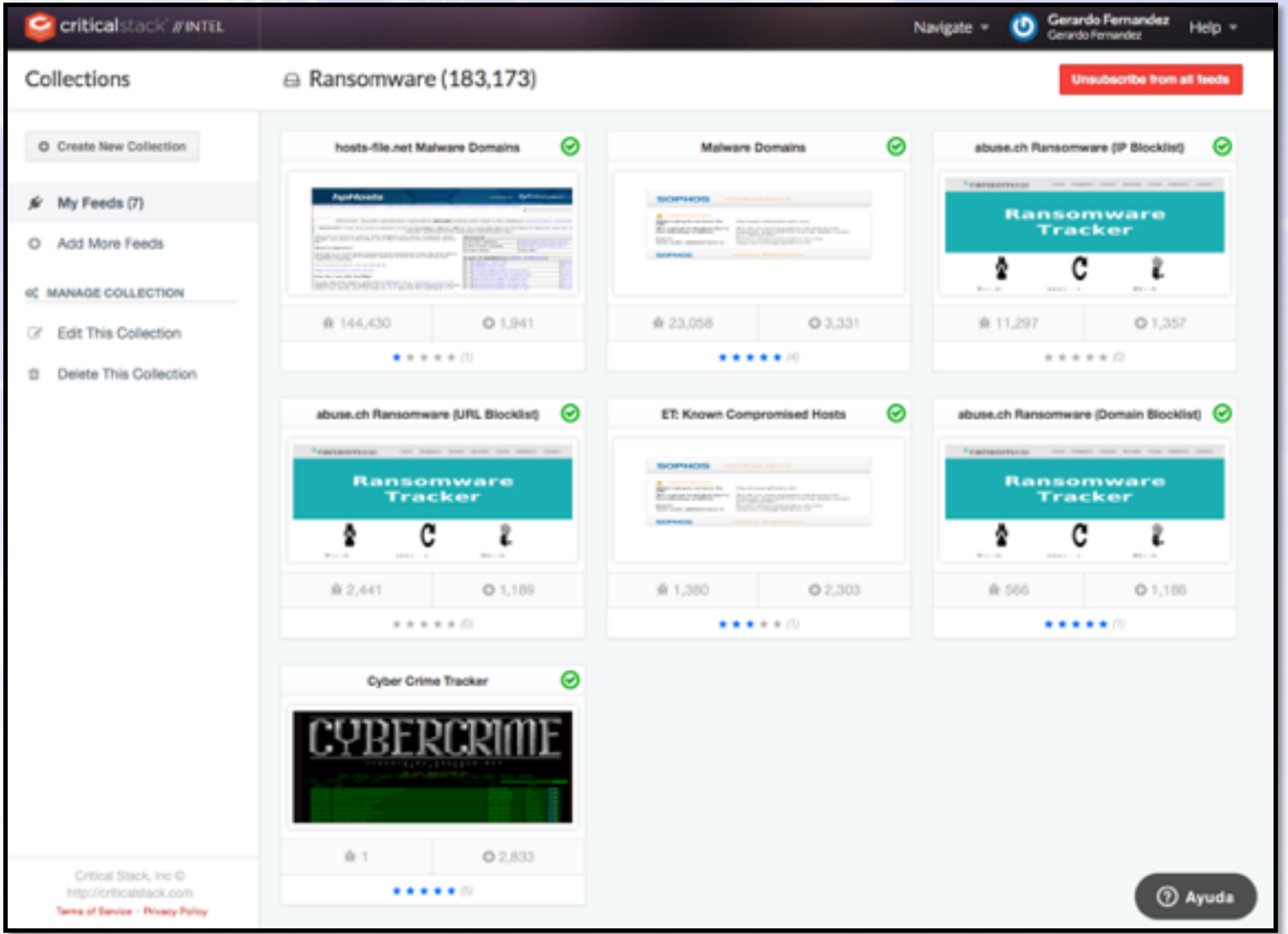
- We use the term *malware intelligence to refer to* information regarding the behaviour and propagation of malware.
  - Which OS is **targeted**?
  - What **components** are attacked?
  - Who **communicates** with?
  - What **activity** is performed?
  - Who **created** and **launched**?

Malware Intelligence

- We use the term *malware intelligence to refer to* information regarding the behaviour and propagation of malware.
  - Which OS is **targeted**?
  - What **components** are attacked?
  - Who **communicates** with?
  - What **activity** is performed?
  - Who **created** and **launched**?
- Depending on the information requested, different types of malware intelligence services can be used. We classify them in **three levels**:
  - **L1**: information about IP and URLs
  - **L2**: information about files: processor, O.S., applications affected, etc.
  - **L3**: intelligence information sharing services (files, URLs, domains, C2 nodes, etc.)

Malware Intelligence

L1



Collections

Ransomware (183,173)

hosts-file.net Malware Domains
144,430 · 1,941 · ★☆☆☆☆ (1)

Malware Domains
23,058 · 3,331 · ★★★★★ (4)

abuse.ch Ransomware (IP Blocklist)
11,297 · 1,357 · ☆☆☆☆☆ (0)

abuse.ch Ransomware (URL Blocklist)
2,441 · 1,189 · ☆☆☆☆☆ (0)

ET: Known Compromised Hosts
1,380 · 2,303 · ★★★☆☆ (1)

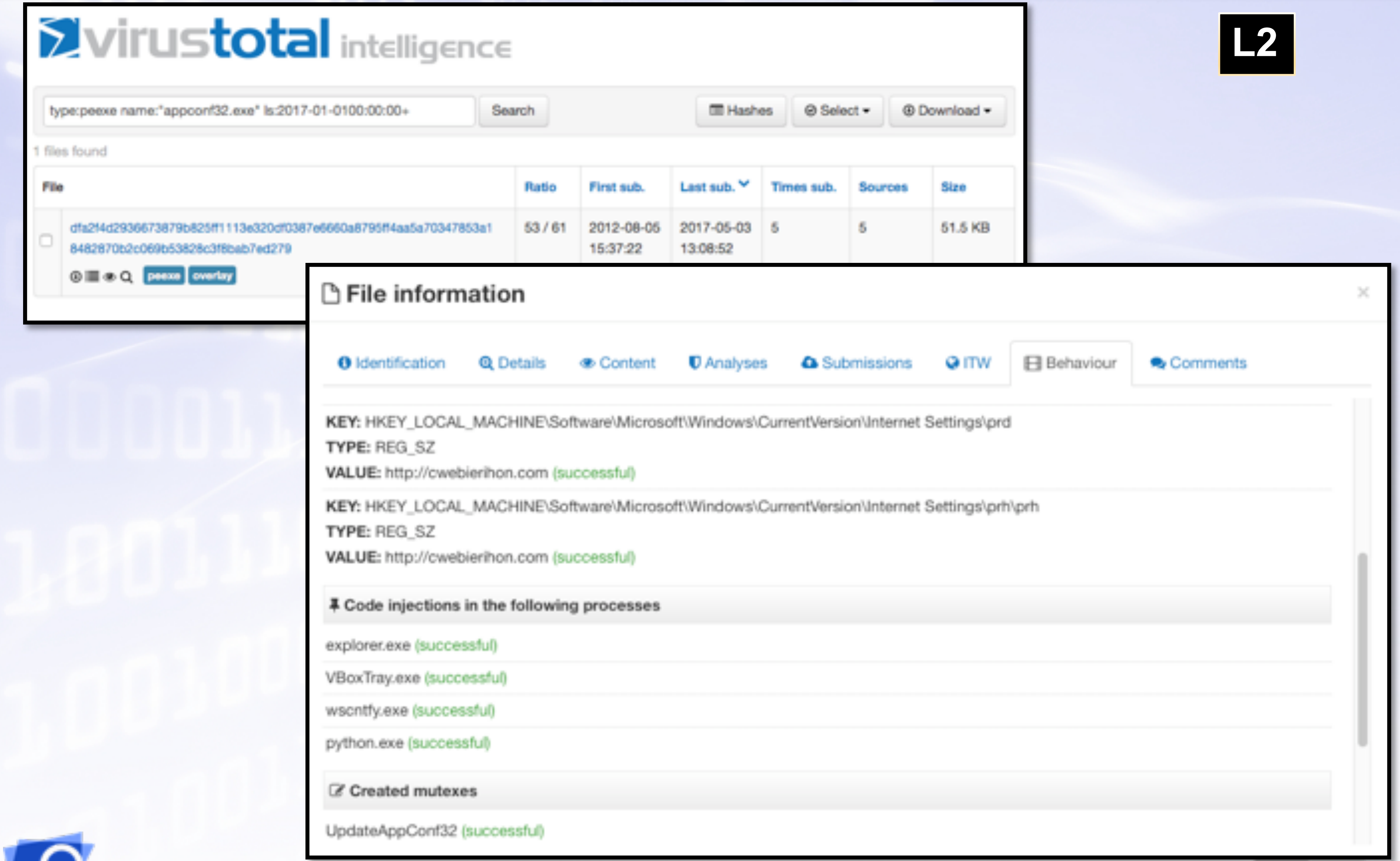
abuse.ch Ransomware (Domain Blocklist)
566 · 1,186 · ★★★★★ (1)

Cyber Crime Tracker
1 · 2,833 · ★★★★★ (5)

Critical Stack, Inc ©
http://criticalstack.com
Terms of Service · Privacy Policy

Malware Intelligence

L2



type:peexe name:"appconf32.exe" ls:2017-01-0100:00:00+

1 files found

File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
dfa2f4d2936673879b825ff1113e320df0387e6660a8795ff4aa5a70347853a1 8482870b2c069b53828c3f8bab7ed279 peexe overlay	53 / 61	2012-08-05 15:37:22	2017-05-03 13:08:52	5	5	51.5 KB

KEY: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\prd
TYPE: REG_SZ
VALUE: http://cwebierihon.com (successful)

KEY: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\prh\prh
TYPE: REG_SZ
VALUE: http://cwebierihon.com (successful)

Code injections in the following processes

explorer.exe (successful)

VBoxTray.exe (successful)

wscntfy.exe (successful)

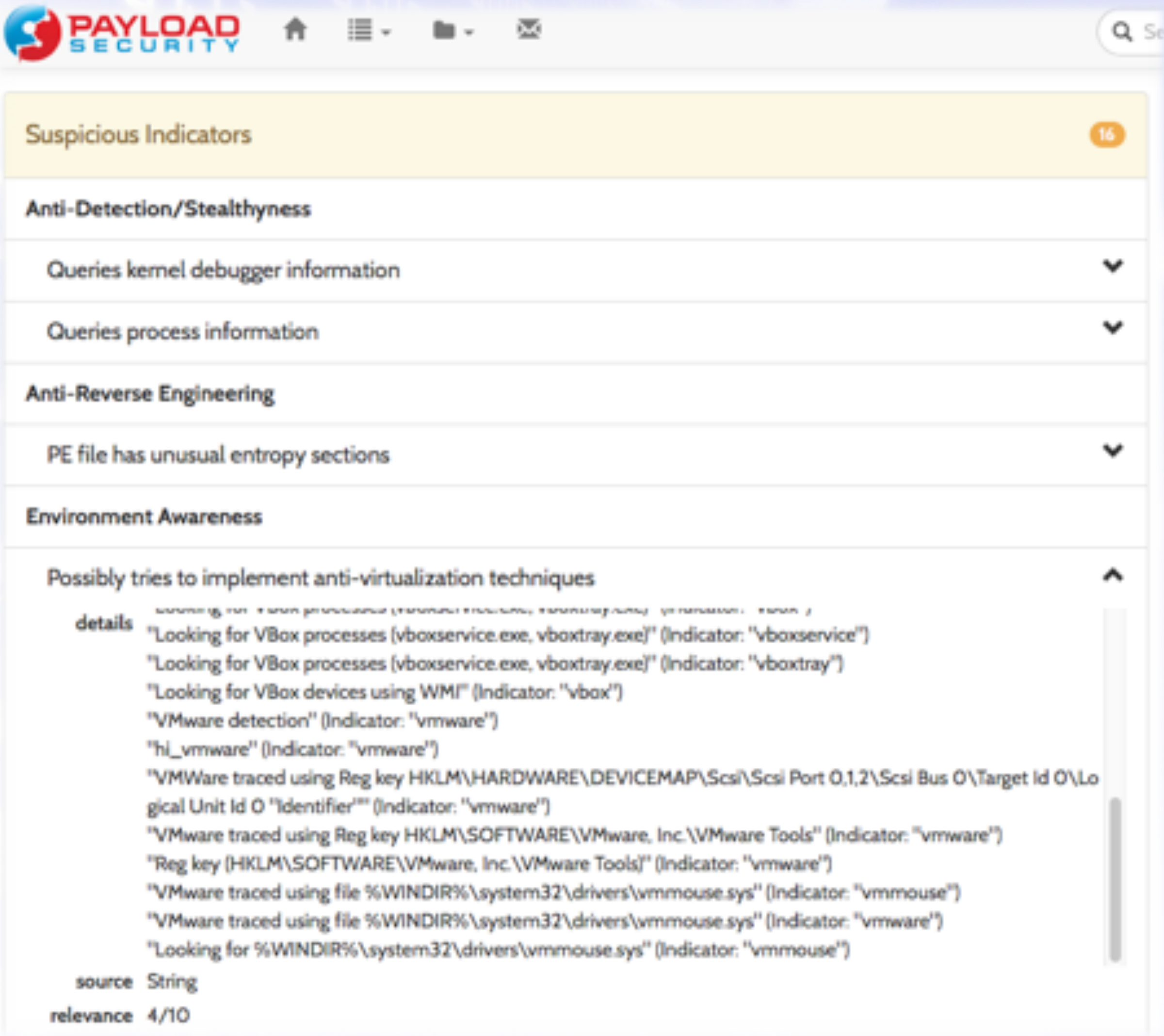
python.exe (successful)

Created mutexes

UpdateAppConf32 (successful)

Malware Intelligence

L2



Suspicious Indicators 16

Anti-Detection/Stealthyness

Queries kernel debugger information

Queries process information

Anti-Reverse Engineering

PE file has unusual entropy sections

Environment Awareness

Possibly tries to implement anti-virtualization techniques

```
details   "Looking for VBox processes (vboxservice.exe, vboxtray.exe)" (Indicator: "vbox")
          "Looking for VBox processes (vboxservice.exe, vboxtray.exe)" (Indicator: "vboxservice")
          "Looking for VBox processes (vboxservice.exe, vboxtray.exe)" (Indicator: "vboxtray")
          "Looking for VBox devices using WMI" (Indicator: "vbox")
          "VMware detection" (Indicator: "vmware")
          "hi_vmware" (Indicator: "vmware")
          "VMWare traced using Reg key HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 0,1,2\Scsi Bus 0\Target Id 0\Lo
          gical Unit Id 0 "Identifier"" (Indicator: "vmware")
          "VMware traced using Reg key HKLM\SOFTWARE\VMware, Inc.\VMware Tools" (Indicator: "vmware")
          "Reg key (HKLM\SOFTWARE\VMware, Inc.\VMware Tools)" (Indicator: "vmware")
          "VMware traced using file %WINDIR%\system32\drivers\vmmouse.sys" (Indicator: "vmmouse")
          "VMware traced using file %WINDIR%\system32\drivers\vmmouse.sys" (Indicator: "vmware")
          "Looking for %WINDIR%\system32\drivers\vmmouse.sys" (Indicator: "vmmouse")
source    String
relevance 4/10
```

Malware Intelligence

L3

```
<response>
<Event>
    <date>2016-12-07</date>
    <info>Locky 2016-12-07 : "Card Receipt" - "CARD123 456789.docm"</info>
    <published>1</published>
    <Attribute>
        <type>ip-dst</type>
        <category>Network activity</category>
        <value>91.142.90.46</value>
        <RelatedAttribute>
            <Attribute>
                <info>"Emailing: MX62EDO 08.12.2016" - "MX62EDO 08.12.2016.docm"</info>
                <value>91.142.90.46</value>
            </Attribute>
        </RelatedAttribute>
    </Attribute>
    <Attribute>
        <type>url</type>
        <category>Payload delivery</category>
        <value>http://wahanaputrayudha.com/hfycn33</value>
    </Attribute>
    <Attribute>
        <type>md5</type>
        <category>Payload delivery</category>
        <value>b923db309a973d7229a1e77352e89486</value>
    </Attribute>
    <Tag><name>misp-galaxy:ransomware=”Locky"</name></Tag>
</Event>
</response>
```

CIRCL MISP Threat Sharing

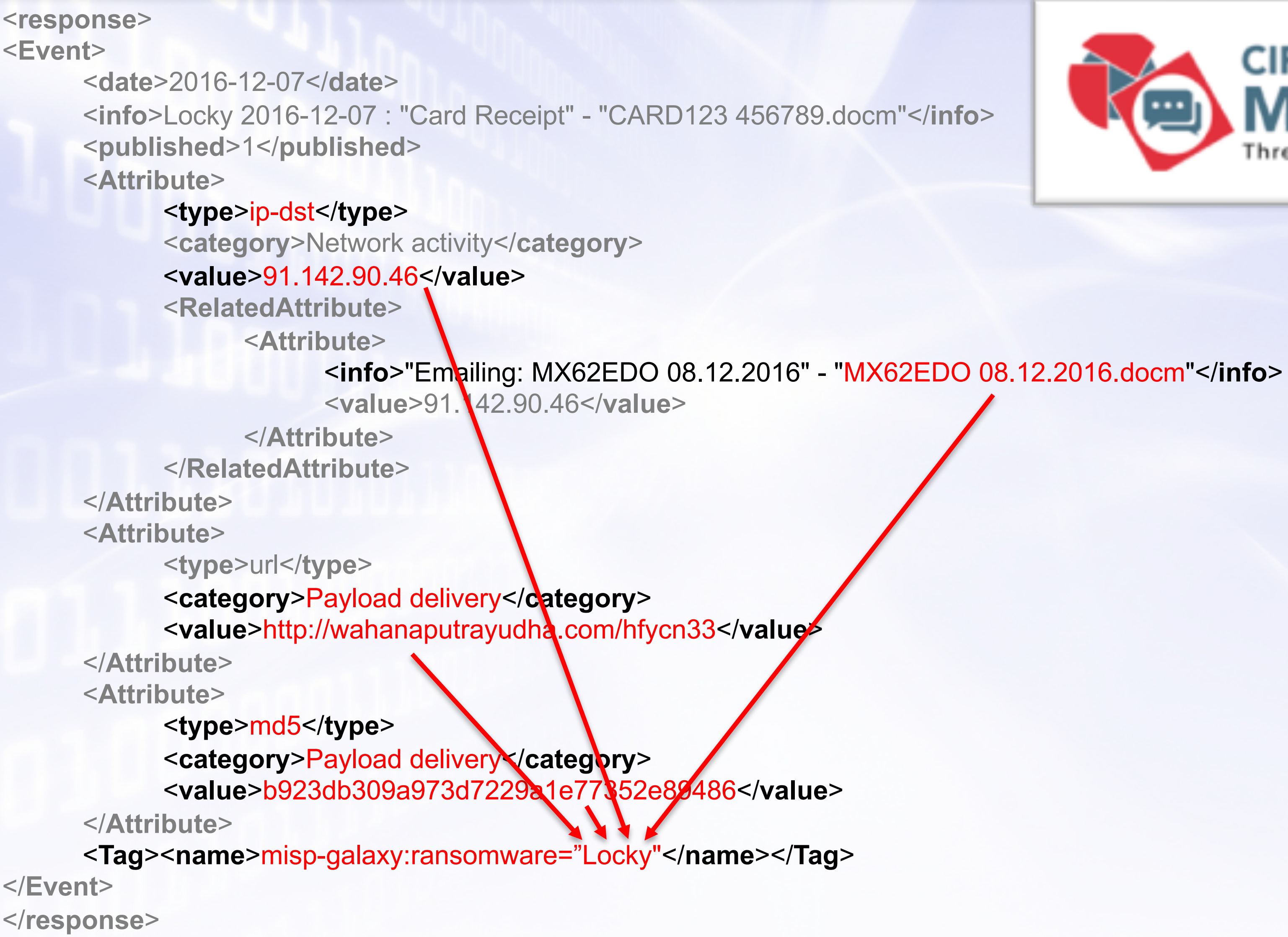
Malware Intelligence

L3

```
<response>
<Event>
        <date>2016-12-07</date>
        <info>Locky 2016-12-07 : "Card Receipt" - "CARD123 456789.docm"</info>
        <published>1</published>
        <Attribute>
                <type>ip-dst</type>
                <category>Network activity</category>
                <value>91.142.90.46</value>
                <RelatedAttribute>
                        <Attribute>
                                <info>"Emailing: MX62EDO 08.12.2016" - "MX62EDO 08.12.2016.docm"</info>
                                <value>91.142.90.46</value>
                        </Attribute>
                </RelatedAttribute>
        </Attribute>
        <Attribute>
                <type>url</type>
                <category>Payload delivery</category>
                <value>http://wahanaputrayudha.com/hfycn33</value>
        </Attribute>
        <Attribute>
                <type>md5</type>
                <category>Payload delivery</category>
                <value>b923db309a973d7229a1e77352e89486</value>
        </Attribute>
        <Tag><name>misp-galaxy:ransomware=”Locky"</name></Tag>
</Event>
</response>
```

Malware Intelligence

L3



```
<response>
<Event>
        <date>2016-12-07</date>
        <info>Locky 2016-12-07 : "Card Receipt" - "CARD123 456789.docm"</info>
        <published>1</published>
        <Attribute>
                <type>ip-dst</type>
                <category>Network activity</category>
                <value>91.142.90.46</value>
                <RelatedAttribute>
                        <Attribute>
                                <info>"Emailing: MX62EDO 08.12.2016" - "MX62EDO 08.12.2016.docm"</info>
                                <value>91.142.90.46</value>
                        </Attribute>
                </RelatedAttribute>
        </Attribute>
        <Attribute>
                <type>url</type>
                <category>Payload delivery</category>
                <value>http://wahanaputrayudha.com/hfycn33</value>
        </Attribute>
        <Attribute>
                <type>md5</type>
                <category>Payload delivery</category>
                <value>b923db309a973d7229a1e77352e89486</value>
        </Attribute>
        <Tag><name>misp-galaxy:ransomware=”Locky"</name></Tag>
</Event>
</response>
```

Hogney Architecture

- **Objective**: to facilitate the analysis of the three stages of malware: exploration, infection and execution of the payload.
  - Focusing on auto-propagated malware
  - Obtaining information before offering a honeypot
  - Integrating tools to capture evidence
  - Adapting services for unleashing all stages of malware

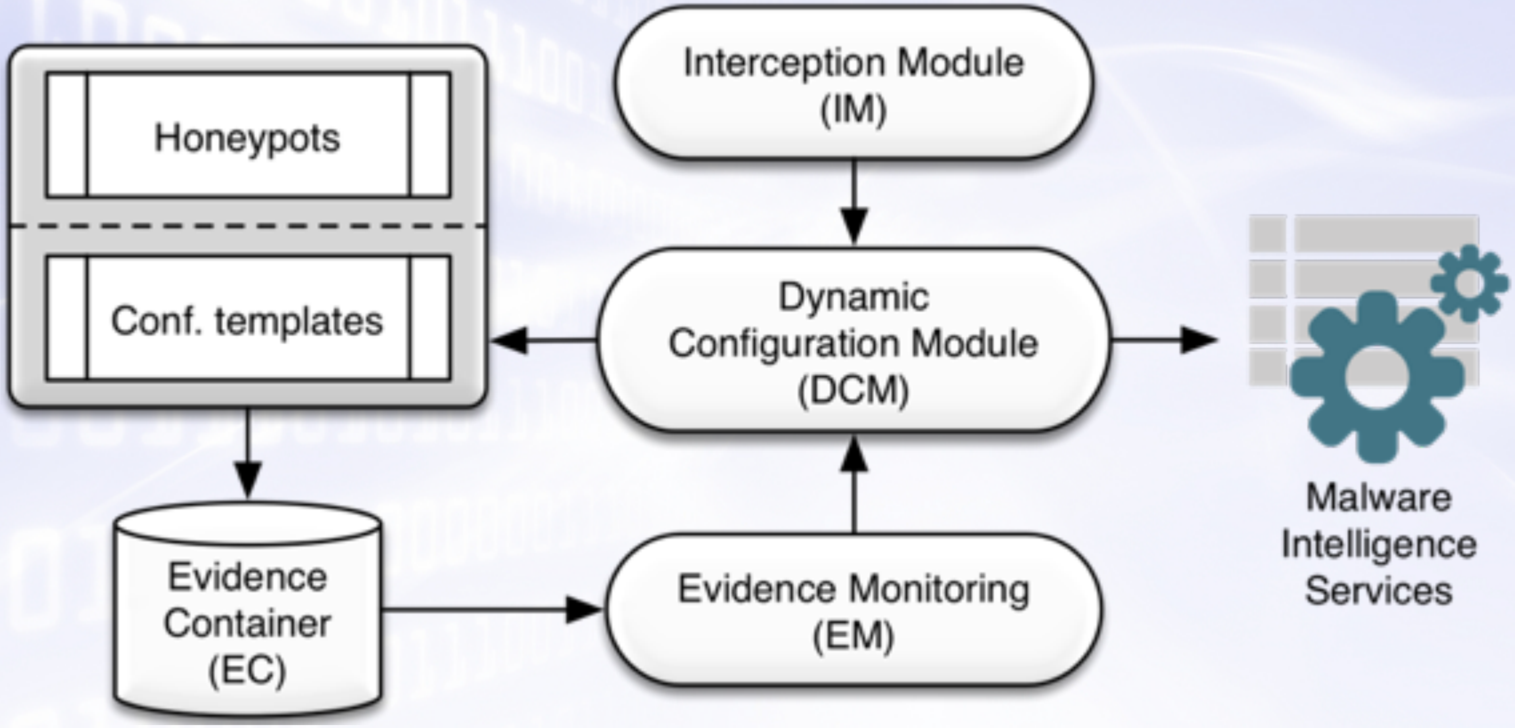
Hogney Architecture

- **Objective**: to facilitate the analysis of the three stages of malware: exploration, infection and execution of the payload.
  - Focusing on auto-propagated malware
  - Obtaining information before offering a honeypot
  - Integrating tools to capture evidence
  - Adapting services for unleashing all stages of malware
- 3 main modules:
  - **Interception** of connections
  - **Configuration** of trap services
  - Evidence **monitoring**

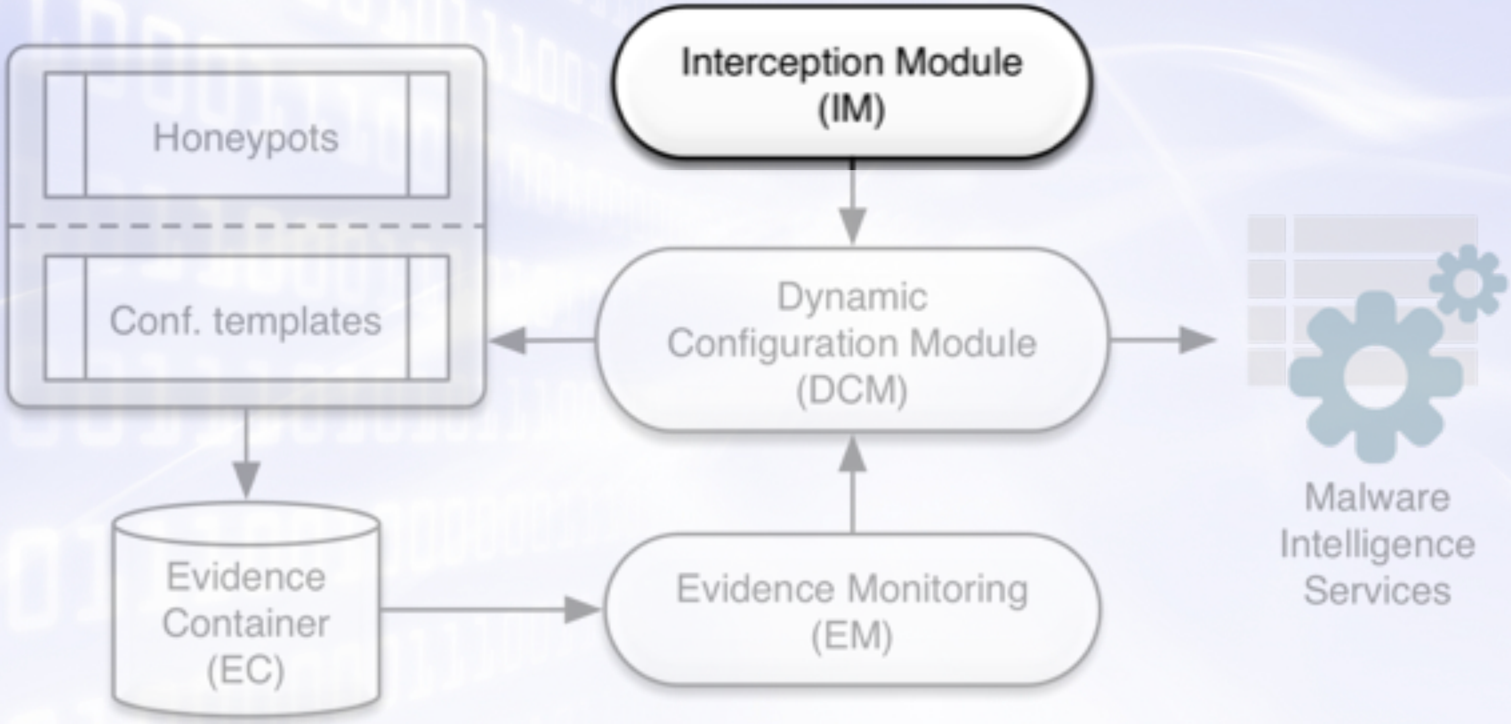
Hogney Architecture

- **Objective**: to facilitate the analysis of the three stages of malware: exploration, infection and execution of the payload.
  - Focusing on auto-propagated malware
  - Obtaining information before offering a honeypot
  - Integrating tools to capture evidence
  - Adapting services for unleashing all stages of malware
- 3 main modules:
  - **Interception** of connections
  - **Configuration** of trap services
  - Evidence **monitoring**
- Using…
  - Low and medium interaction honeypot templates
  - Execution environments (real and virtual) for high interaction honeypots

Hogney Architecture



Hogney Architecture



Hogney: interception

- **Objective**: listen for connections on a set of predetermined ports, accept them and send service requests to the **DCM** component for the configuration of honeypots.

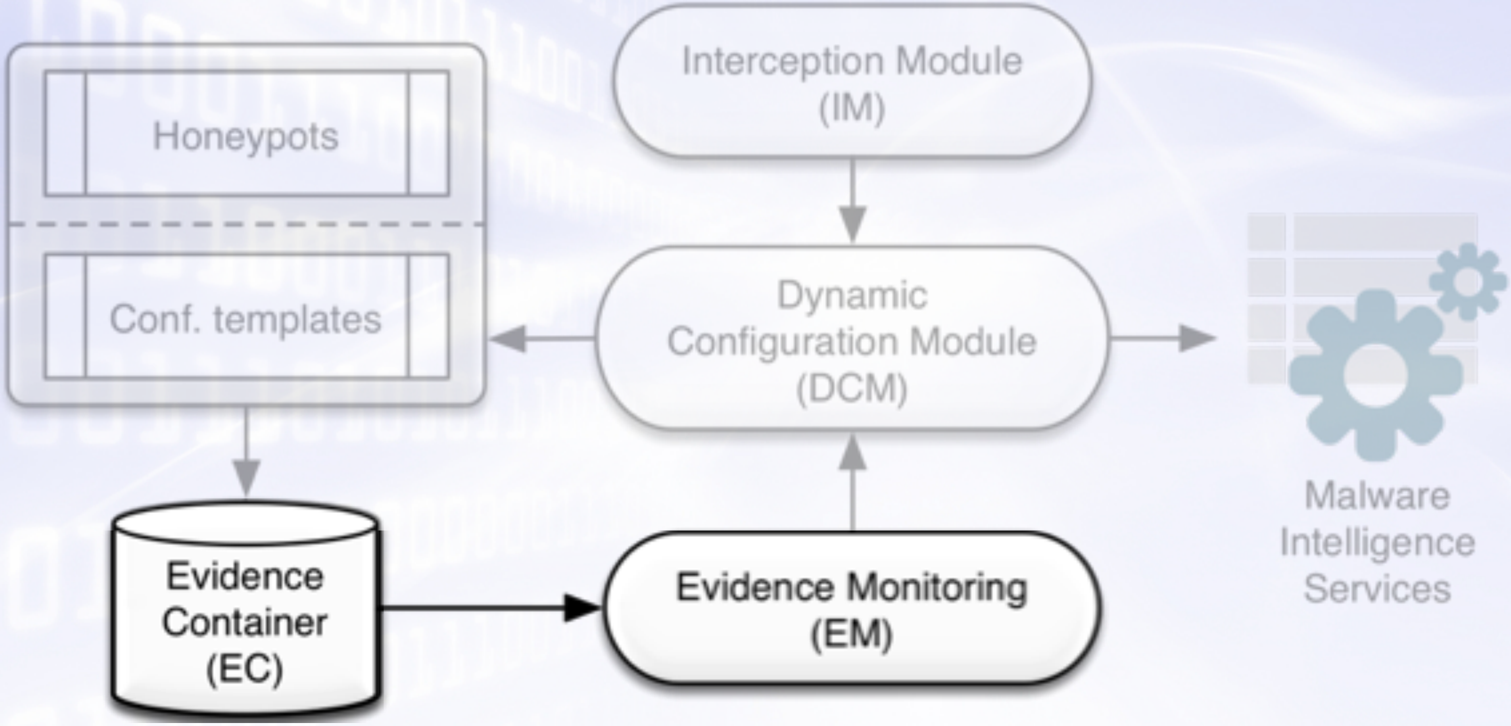
Hogney: interception

- **Objective**: listen for connections on a set of predetermined ports, accept them and send service requests to the **DCM** component for the configuration of honeypots.
- Gathering all the information collected at the time of establishing the connection (**IP**, **destination/source ports**, **protocol headers**, etc.).

Hogney: interception

- **Objective**: listen for connections on a set of predetermined ports, accept them and send service requests to the **DCM** component for the configuration of honeypots.
- Gathering all the information collected at the time of establishing the connection (**IP**, **destination/source ports**, **protocol headers**, etc.).
- This way the **DCM** will deploy a honeypot with the highest probability of success for this connection.

Hogney Architecture



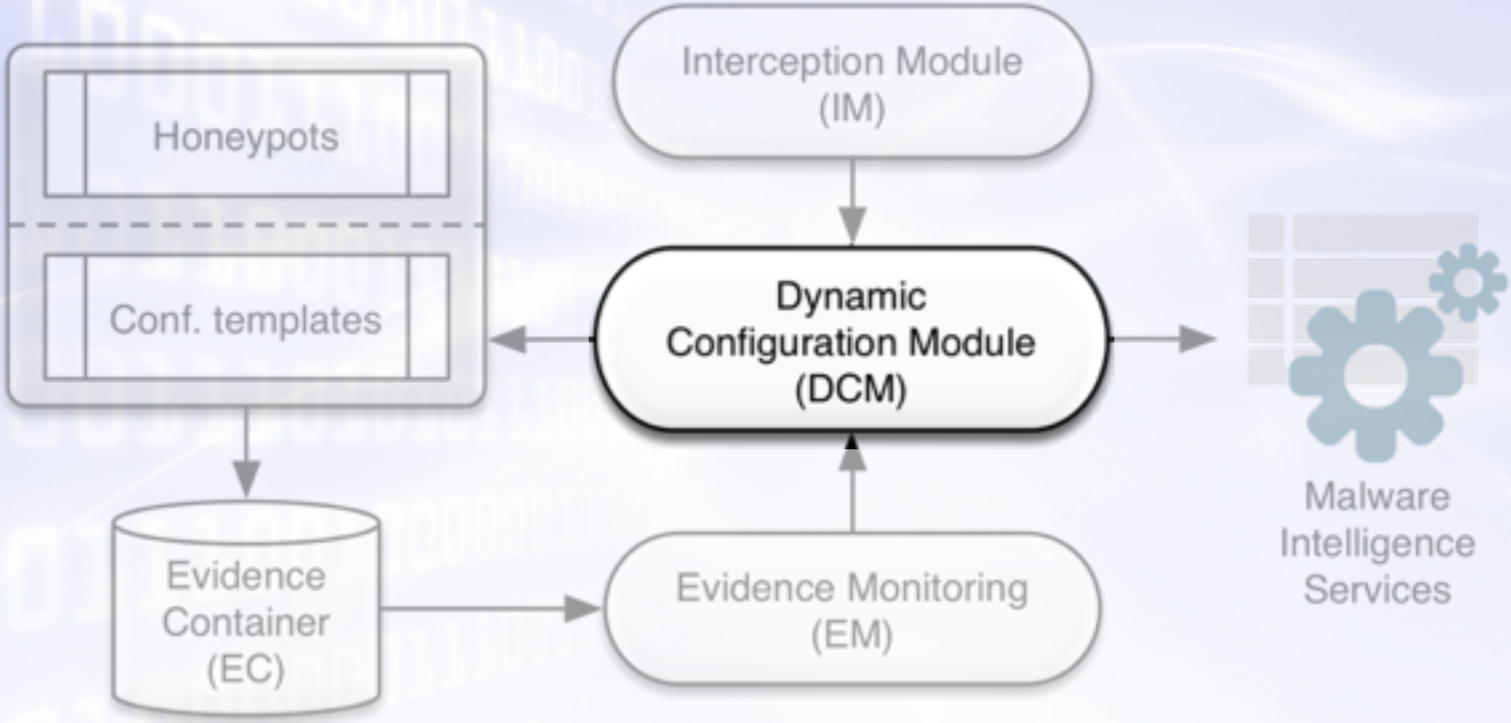
Hogney: evidence

- **Objective**: to gather as much **evidence** as possible about the actions carried out by malware, as well as to facilitate the continuity of the attack process, by activating the different stages implemented in the malware.

Hogney: evidence

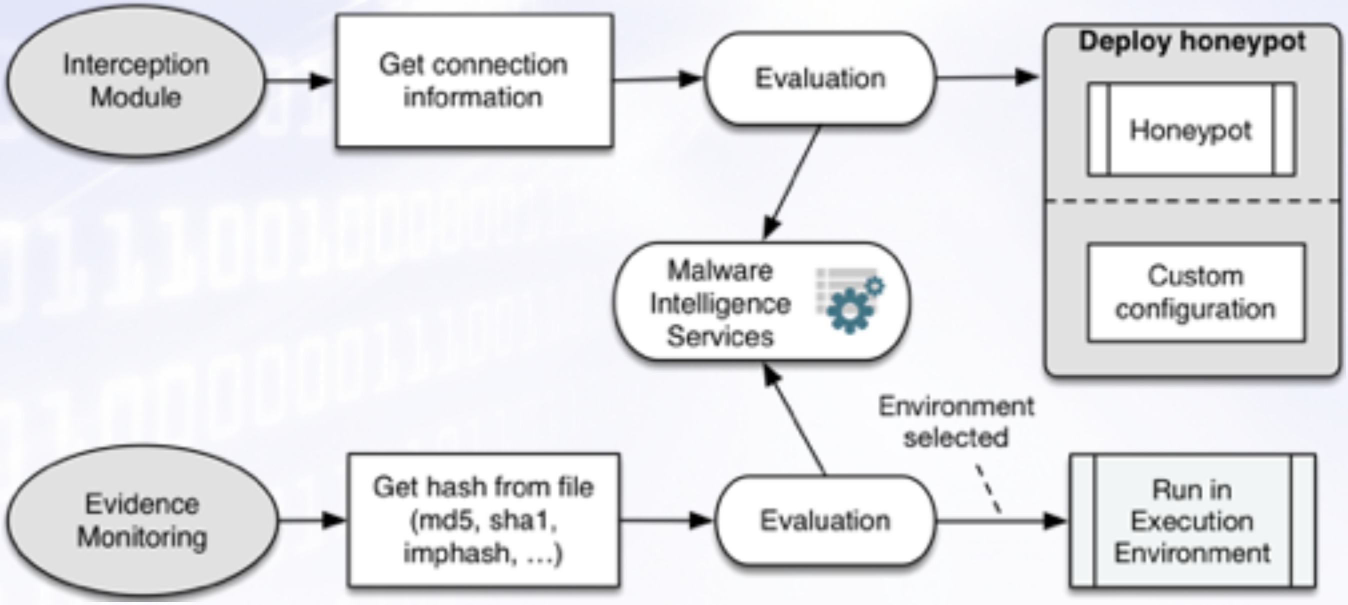
- **Objective**: to gather as much **evidence** as possible about the actions carried out by malware, as well as to facilitate the continuity of the attack process, by activating the different stages implemented in the malware.
- The **EM** component is continuously monitoring the creation of new evidence.
  - When a new piece is detected, a request is sent to the **DCM** containing the characteristics of the evidence (file type, operating system, etc.).
  - Then, a new execution environment is set up to execute and analyse this evidence.

Hogney Architecture

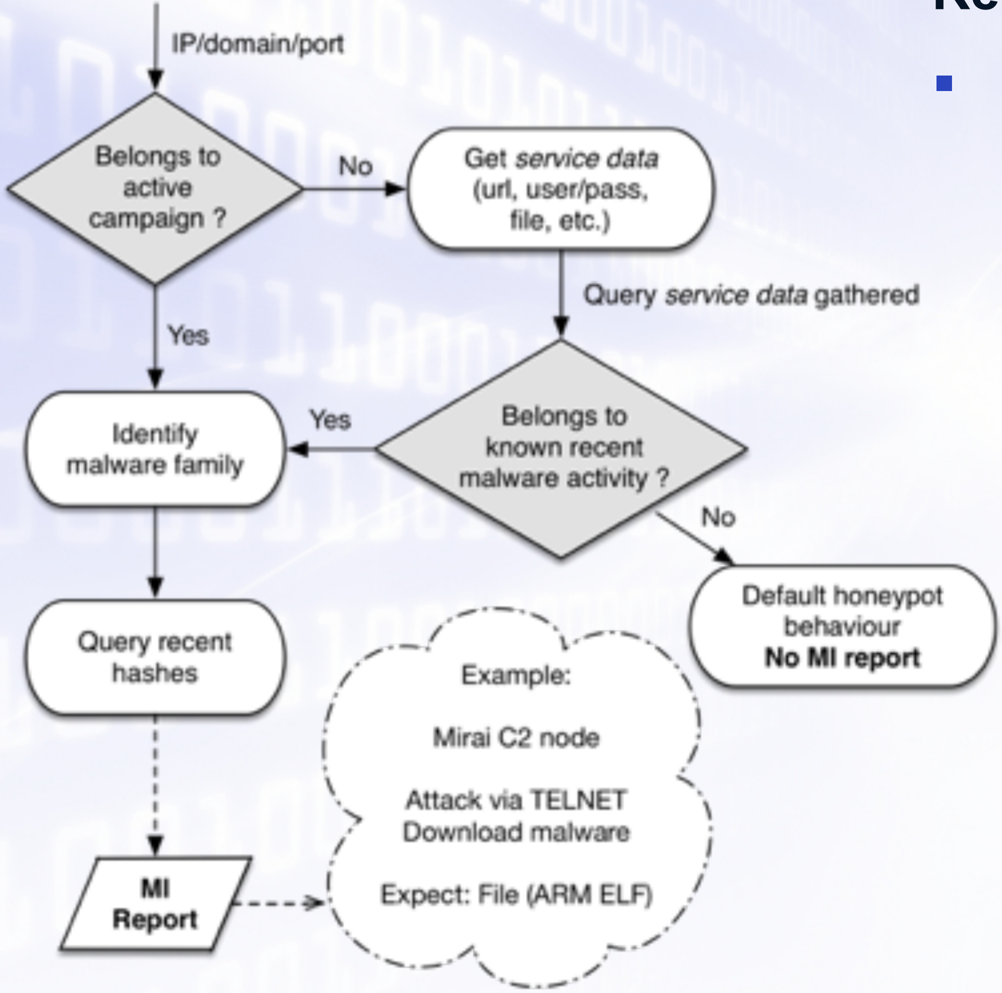


Hogney: adaptation

- **Objective**: to discern which honeypot is the most suitable for the type of malware involved.
  - Receive: src/dst ip, protocol headers, service information, related files
  - Queries to external intelligence services are launched to look for any evidence of malware based on the information collected.
  - Requests can be received from **IM** and **EM**.


Interception Module
Get connection information
Evaluation
Deploy honeypot
Honeypot
Custom configuration
Malware Intelligence Services
Environment selected
Evidence Monitoring
Get hash from file (md5, sha1, imphash, ...)
Evaluation
Run in Execution Environment

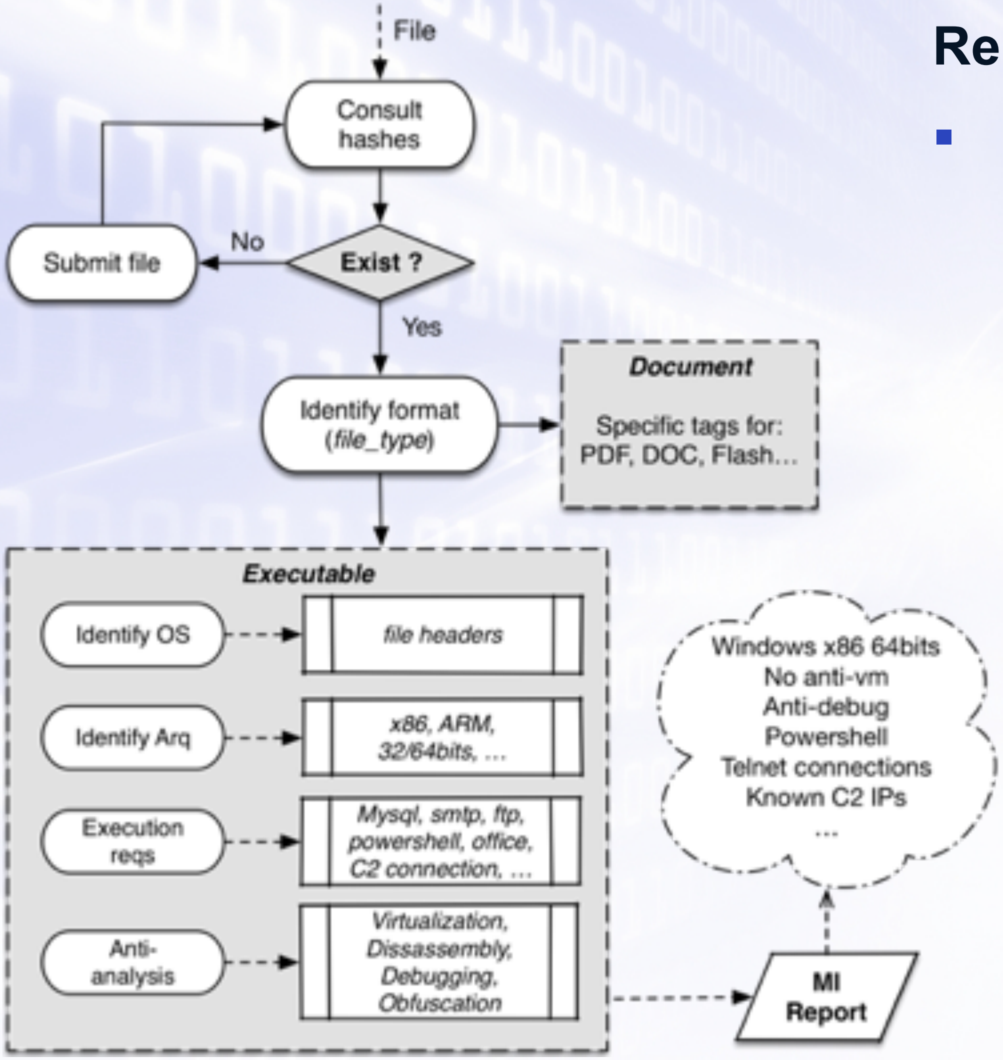
Hogney: adaptation


IP/domain/port
Belongs to active campaign ?
No
Get *service data* (url, user/pass, file, etc.)
Query *service data* gathered
Yes
Identify malware family
Yes
Belongs to known recent malware activity ?
No
Default honeypot behaviour
No MI report
Query recent hashes
MI Report
Example:
Mirai C2 node
Attack via TELNET
Download malware
Expect: File (ARM ELF)

Requests from IM

- Analysis based on IP, protocol, service data, destination files and folders, …
  – Query external **intelligence services** to look for any evidence of malware.
  – Mainly L1 and L3 services
  – Information obtained will allow to deploy a honeypot to the malware needs.

Hogney: adaptation

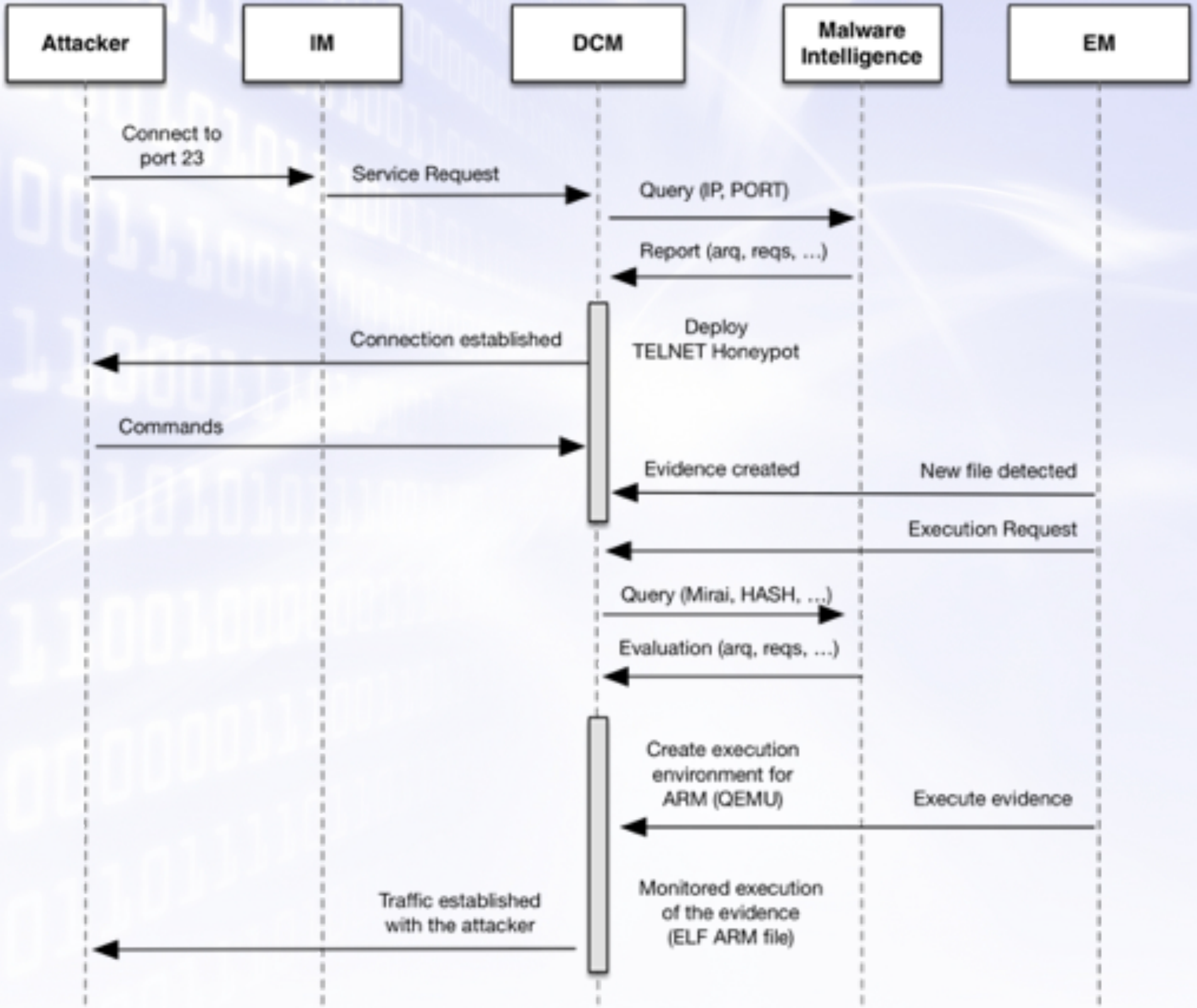


Requests from EM

- A evidence is obtained when the attacker has managed to deploy some type of file in the honeypot.
  - A new file is uploaded into the *Evidence Container*.
  - **EM** will detect this new file and will ask the **DCM** to prepare a execution environment for its analysis.
  - L1, L2 and L3 services

Use Case

Mirai



Attacker

IM

DCM

Malware Intelligence

EM

Connect to port 23

Service Request

Query (IP, PORT)

Report (arq, reqs, ...)

Deploy TELNET Honeypot

Connection established

Commands

Evidence created

New file detected

Execution Request

Query (Mirai, HASH, ...)

Evaluation (arq, reqs, ...)

Create execution environment for ARM (QEMU)

Execute evidence

Monitored execution of the evidence (ELF ARM file)

Traffic established with the attacker

Conclusions

- Malware intelligence services are an unexplored valuable resource for the construction of adaptive honeypots.
- Short-term main challenges:
  - IM: Reduce latency when answering incoming connections
  - DCM: Manage intelligence information in a convenient way (ML)
  - Avoid anti-analysis techniques that can prevent the generation of evidence
- Next step:
  - Integrate the information gathered from malware intelligence services to quickly create an up-to-date [ML] dataset for the DCM component.

Modeling Malware-driven Honeypots

Thank you for your attention !

Gerardo Fernández, Ana Nieto and Javier Lopez

{gerardo,nieto,jlm}@lcc.uma.es

Network, Information and Computer Security (NICS) Lab

University of Malaga, Spain

TrustBus 2017, August 30th 2017