

Configuración adaptativa de honeypots para análisis de malware

Gerardo Fernández y Ana Nieto

gerardo@lcc.uma.es, nieto@lcc.uma.es

NICS Lab, Universidad de Málaga

1. Honeypots, objetivos y limitaciones
2. Malware Intelligence
3. Arquitectura Hogney
4. Caso de estudio: Mirai
5. Conclusiones

■ Utilidad de los honeypots:

- Todo tráfico dirigido contra ellos es sospechoso
- **Entorno productivo:** reproducir servicios entornos productivo para capturar futuros ataques dirigidos contra equipos en producción
- **Investigación:** capturar nuevos ataques, revelar tendencias en los nuevos sistemas objetivos y descubrir nuevos mecanismos de propagación

■ Utilidad de los honeypots:

- Todo tráfico dirigido contra ellos es sospechoso
- **Entorno productivo:** reproducir servicios entornos productivo para capturar futuros ataques dirigidos contra equipos en producción
- **Investigación:** capturar nuevos ataques, revelar tendencias en los nuevos sistemas objetivos y descubrir nuevos mecanismos de propagación

■ Limitaciones:

- De propósito general: difícil desatar fases posteriores del ataque
- Específicos de protocolos/aplicaciones: + visibilidad reducida
- Especializados en cierto tipos de ataques: + visibilidad reducida
- Soluciones adaptativas: suelen combinar algunas técnicas de las anteriores ➡ heredan problemas anteriores aunque en menor medida

■ Utilidad de los honeypots:

- Todo tráfico dirigido contra ellos es sospechoso.
- **Entorno productivo:** reproducir servicios entornos productivo para capturar futuros ataques dirigidos contra equipos en producción.
- **Investigación:** capturar nuevos ataques, revelar tendencias en los nuevos sistemas objetivos y descubrir nuevos mecanismos de propagación.

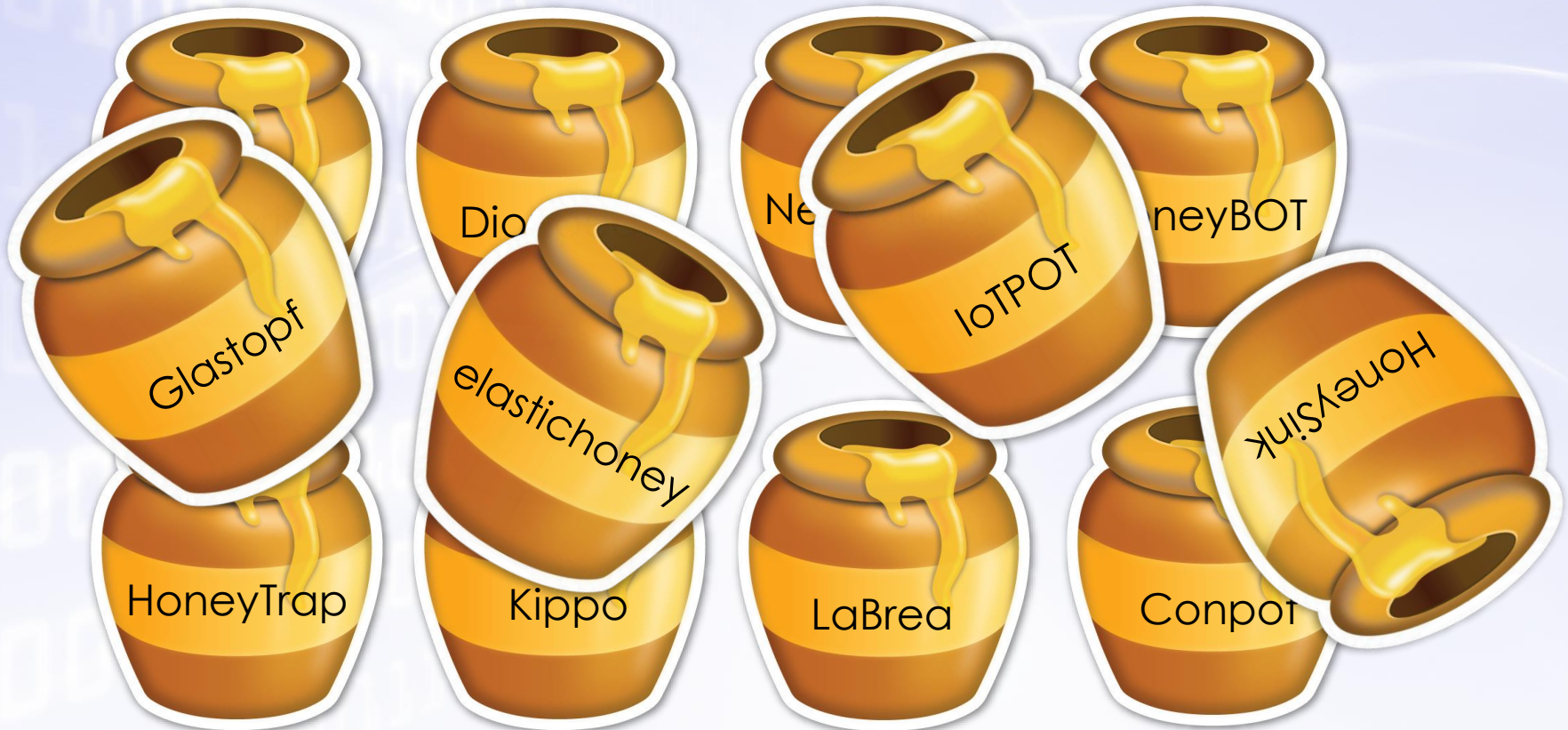
■ Limitaciones:

- De propósito general: difícil desatar fases posteriores del ataque
- Específicos de protocolos/aplicaciones: + visibilidad reducida
- Especializados en cierto tipos de ataques: + visibilidad reducida
- Soluciones adaptativas: suelen combinar algunas técnicas de las anteriores ➡ heredan problemas anteriores aunque en menor medida.

- Multitud de honeypots en la actualidad...



- Multitud de honeypots en la actualidad...



- Multitud de honeypots en la actualidad...



- Con el término *malware intelligence* nos referimos a información de inteligencia sobre el comportamiento y la difusión del malware.
 - ¿A qué **sistemas operativos** afecta?
 - ¿Qué **componentes** del sistema ataca?
 - ¿Con quién se **comunica**?
 - ¿Qué **actividad** realiza?
 - ¿Quién lo ha **creado**?

- Con el término *malware intelligence* nos referimos a información de inteligencia sobre el comportamiento y la difusión del malware.
 - ¿A qué **sistemas operativos** afecta?
 - ¿Qué **componentes** del sistema ataca?
 - ¿Con quién se **comunica**?
 - ¿Qué **actividad** realiza?
 - ¿Quién lo ha **creado**?
- Tres niveles de agrupación de servicios:
 - **L1**: información sobre IP y URLs
 - **L2**: información a nivel de ficheros, procesador, S.O., etc.
 - **L3**: servicios de intercambio de información de inteligencia (ficheros, URLs, dominios, nodos C2, etc.)

L1

 criticalstack // INTEL

Navigate  Gerardo Fernandez
Gerardo Fernandez Help

Collections  Ransomware (183,173) Unsubscribe from all feeds

Create New Collection

My Feeds (7)

Add More Feeds

MANAGE COLLECTION

Edit This Collection

Delete This Collection

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)

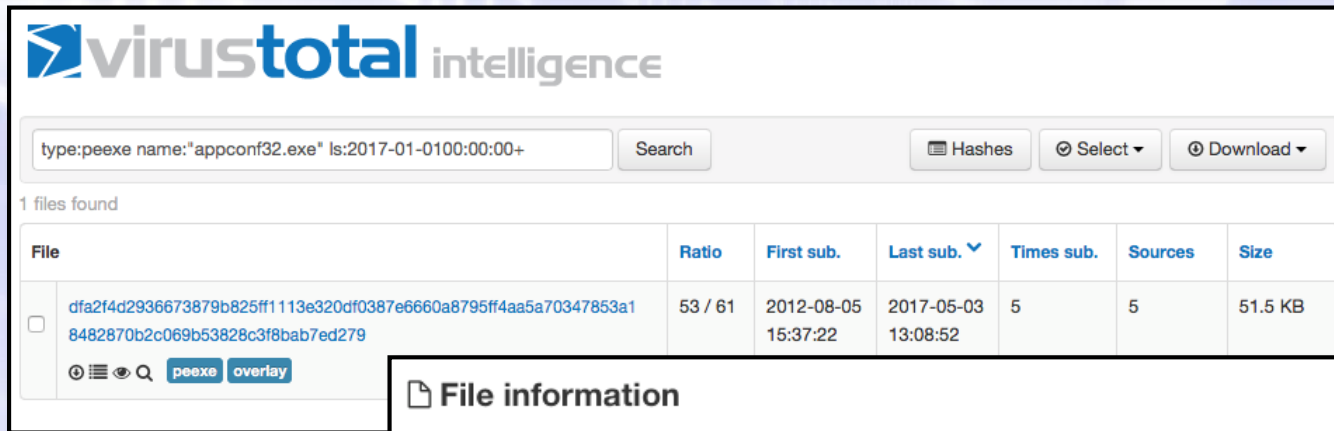
Critical Stack, Inc ©
<http://criticalstack.com>
Terms of Service - Privacy Policy

 Ayuda



Madrid, 1 de Junio 2017





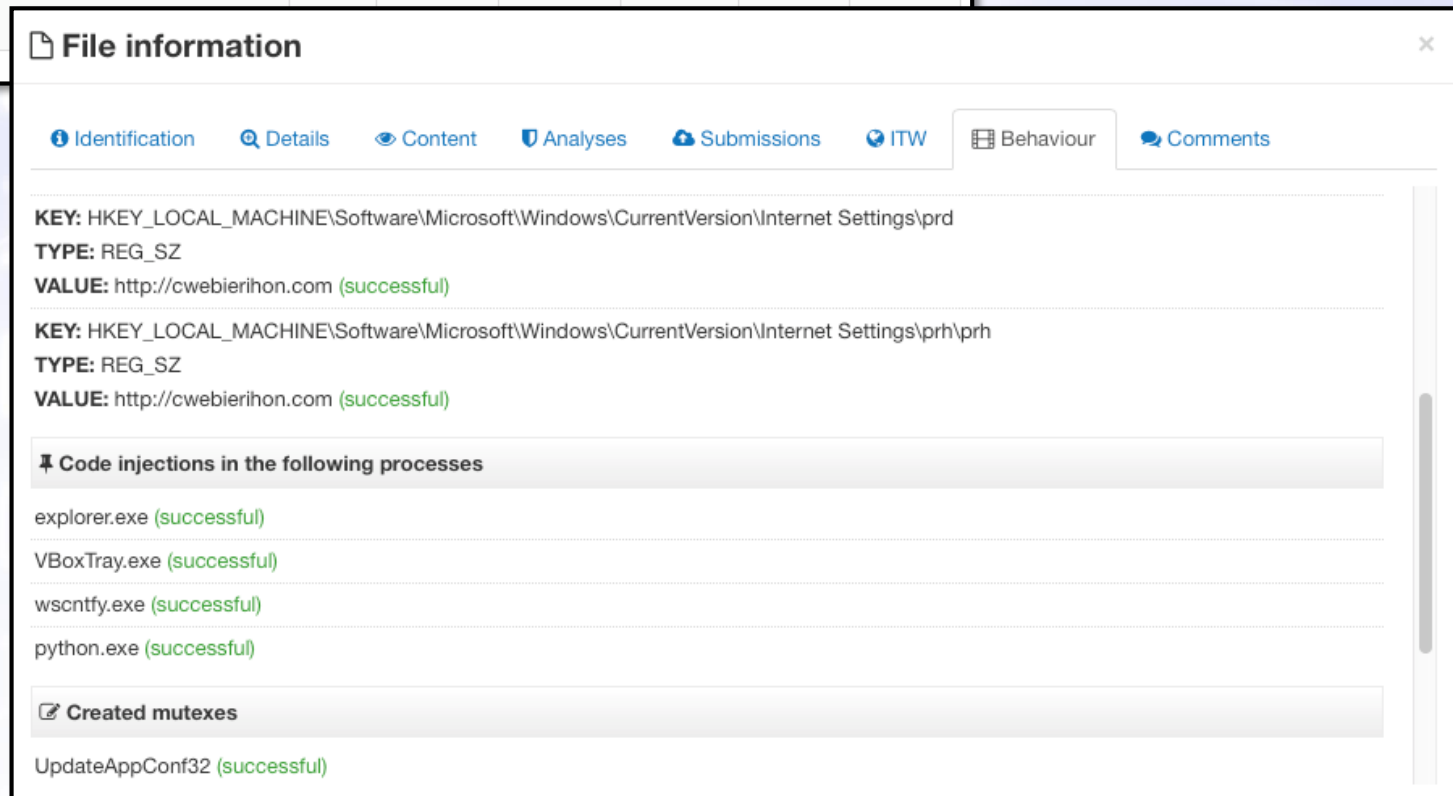
virustotal intelligence

type:peexe name:"appconf32.exe" ls:2017-01-0100:00:00+ Search Hashes Select Download

1 files found

File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
dfa2f4d2936673879b825ff1113e320df0387e6660a8795ff4aa5a70347853a18482870b2c069b53828c3f8bab7ed279	53 / 61	2012-08-05 15:37:22	2017-05-03 13:08:52	5	5	51.5 KB

peexe overlay



File information

Identification Details Content Analyses Submissions ITW Behaviour Comments

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)

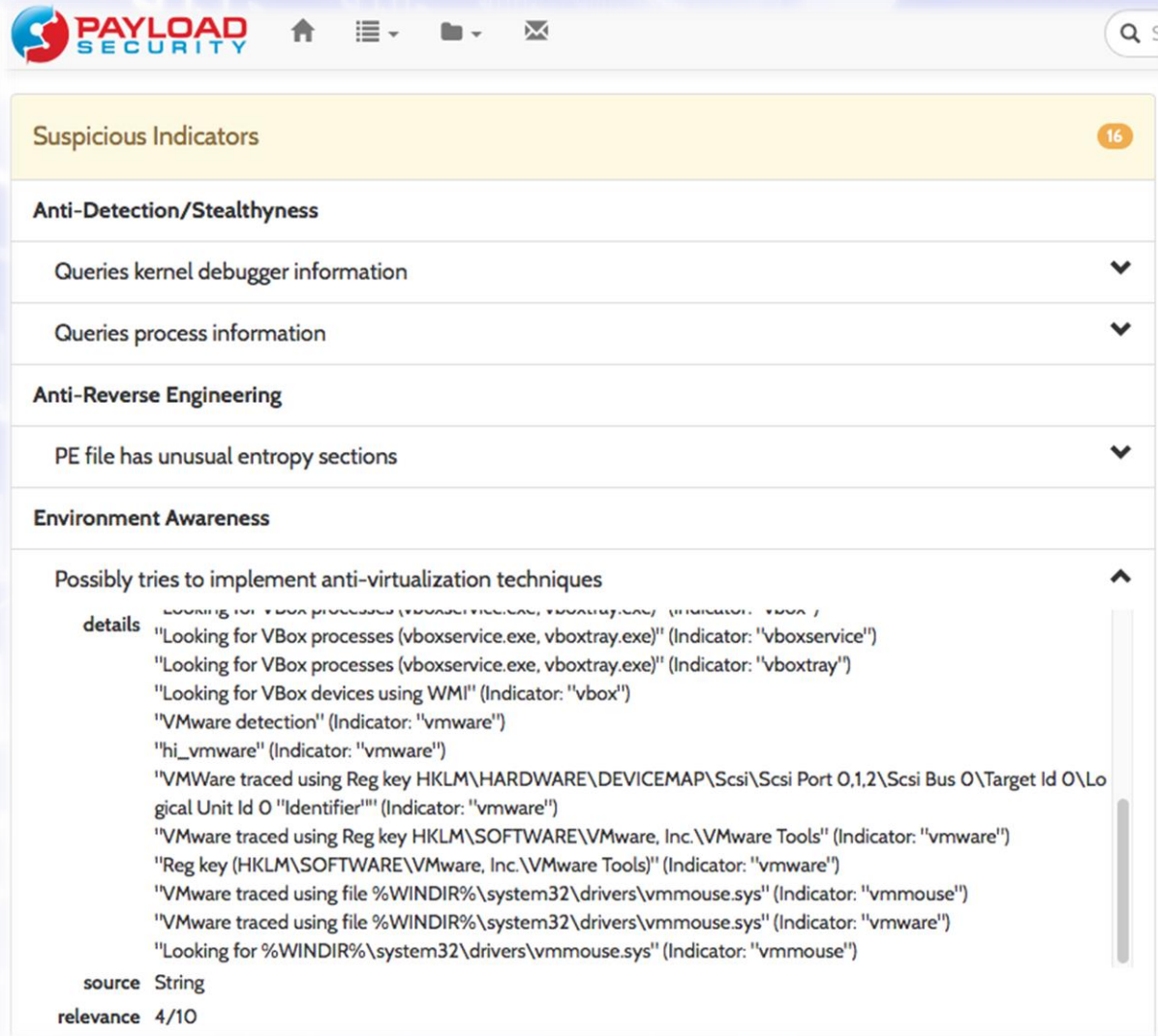
Code injections in the following processes

- explorer.exe (successful)
- VBoxTray.exe (successful)
- wscntfy.exe (successful)
- python.exe (successful)

Created mutexes

- UpdateAppConf32 (successful)

L2



The screenshot displays the PAYLOAD SECURITY web application. The top navigation bar includes the logo, a home icon, a menu icon, a folder icon, and an email icon. A search bar is located on the right. The main content area is titled 'Suspicious Indicators' with a badge showing '16'. It is organized into several expandable sections: 'Anti-Detection/Stealthyness' (containing 'Queries kernel debugger information' and 'Queries process information'), 'Anti-Reverse Engineering' (containing 'PE file has unusual entropy sections'), and 'Environment Awareness' (containing 'Possibly tries to implement anti-virtualization techniques'). The 'Possibly tries to implement anti-virtualization techniques' section is expanded, showing a list of indicators with details, source, and relevance. The indicators include looking for VBox processes, VMware detection, and tracing VMware files.

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: "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\Logical 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

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>
```



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>
```



L3

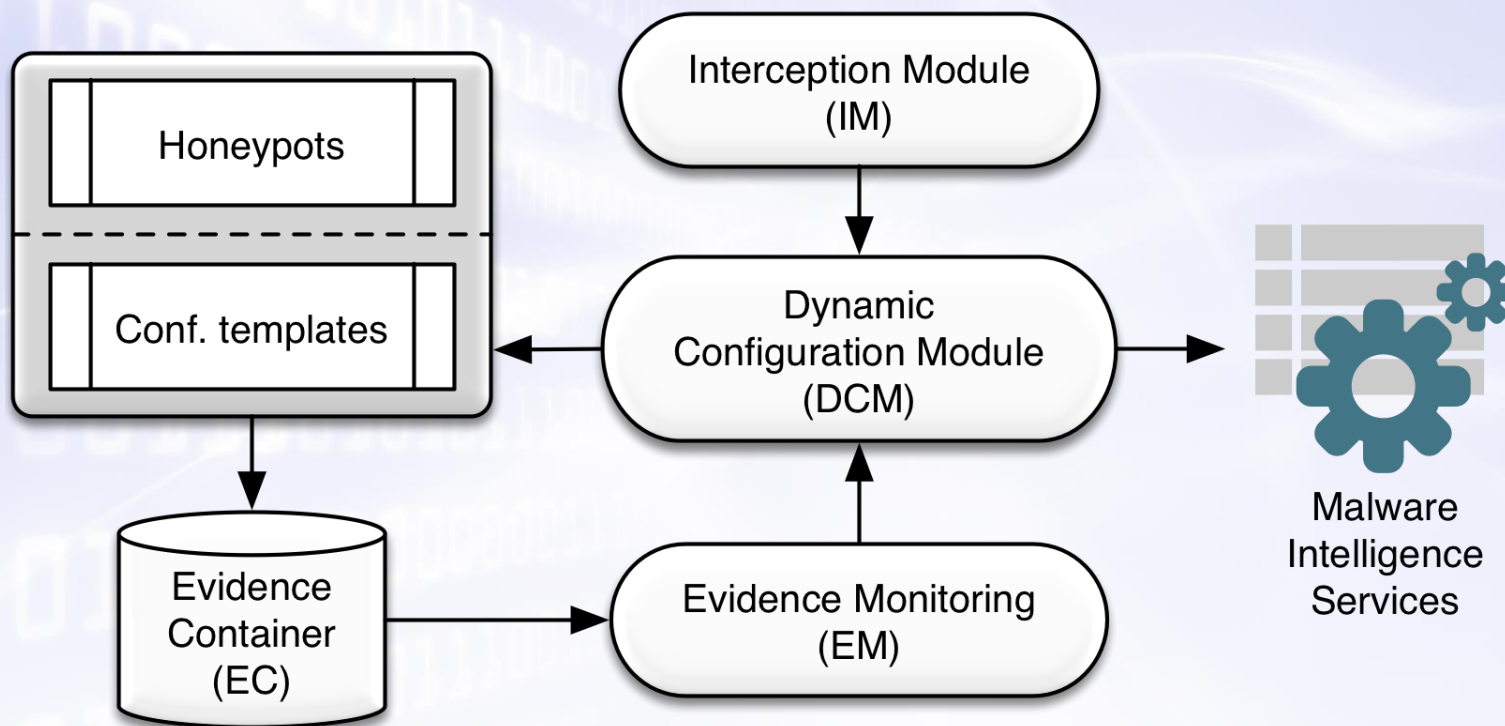
```
<response>
<Event>
  <date>2016-12-07</date>
  <info>Locky 2016-12-07 : "Card Receipt" - "CARD123 456789.docm"</info>
  <published>1</published>
  <Attribute>
    <type>ip-dst</type>
    <category>Network activity</category>
    <value>91.142.90.46</value>
    <RelatedAttribute>
      <Attribute>
        <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>
```

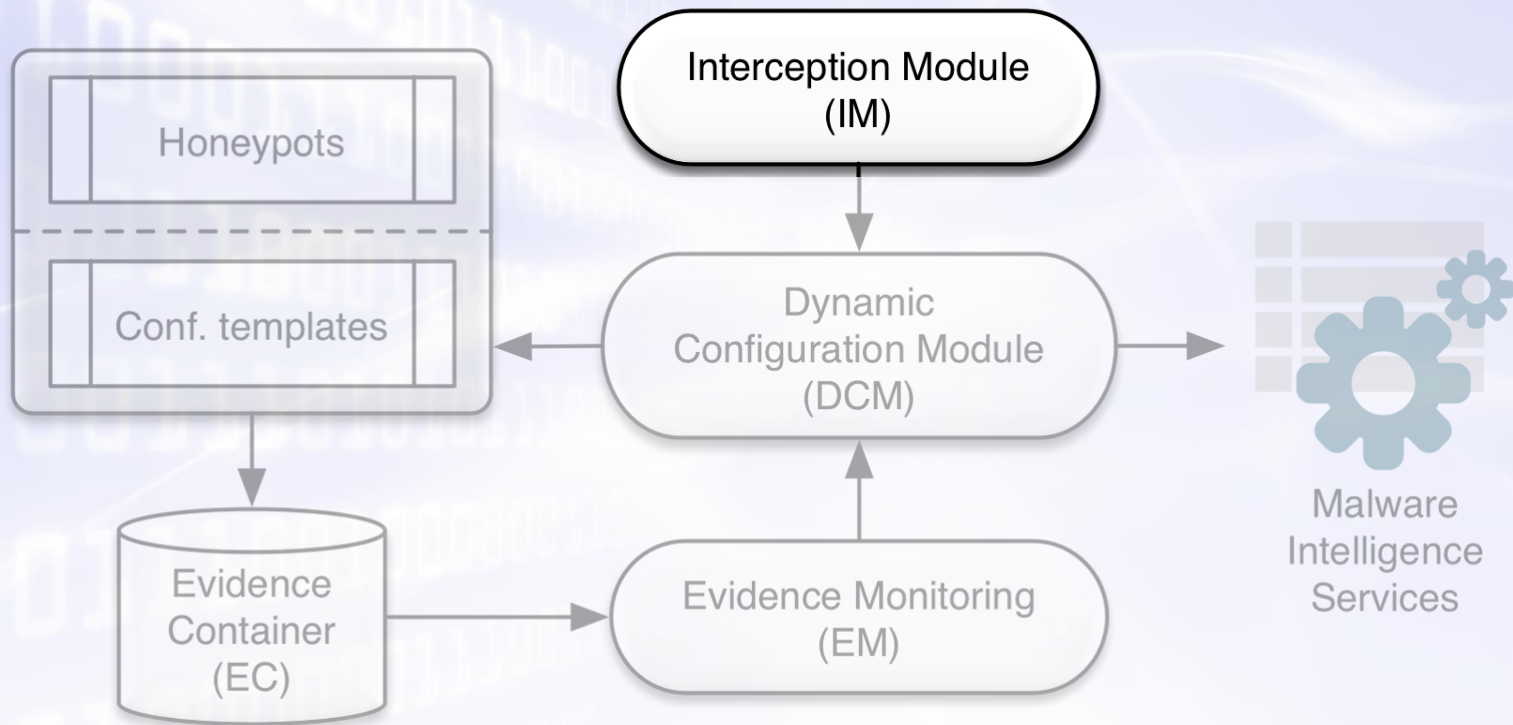


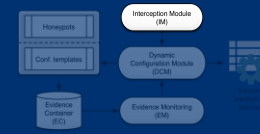
- **Objetivo:** Integrar los servicios de “malware intelligence” en la configuración dinámica de los honeypots.
 - Dirigido principalmente a malware de auto-propagación
 - Obtener información antes de desplegar un honeypot
 - Configurar herramientas de captura de evidencias
 - Adaptar servicios para desplegar fases posteriores del malware

- **Objetivo:** Integrar los servicios de “malware intelligence” en la configuración dinámica de los honeypots.
 - Dirigido principalmente a malware de auto-propagación
 - Obtener información antes de desplegar un honeypot
 - Configurar herramientas de captura de evidencias
 - Adaptar servicios para desplegar fases posteriores del malware
- 3 módulos principales:
 - **Interceptación** de conexiones
 - **Configuración** dinámica de honeypots
 - **Monitorización** de evidencias

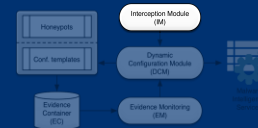
- **Objetivo:** Integrar los servicios de “malware intelligence” en la configuración dinámica de los honeypots.
 - Dirigido principalmente a malware de auto-propagación
 - Obtener información antes de desplegar un honeypot
 - Configurar herramientas de captura de evidencias
 - Adaptar servicios para desplegar fases posteriores del malware
- 3 módulos principales:
 - **Interceptación** de conexiones
 - **Configuración** dinámica de honeypots
 - **Monitorización** de evidencias
- Empleando...
 - Plantillas de honeypots de baja y media interacción
 - Entornos de ejecución físicos y virtuales de alta interacción



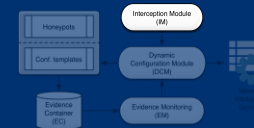




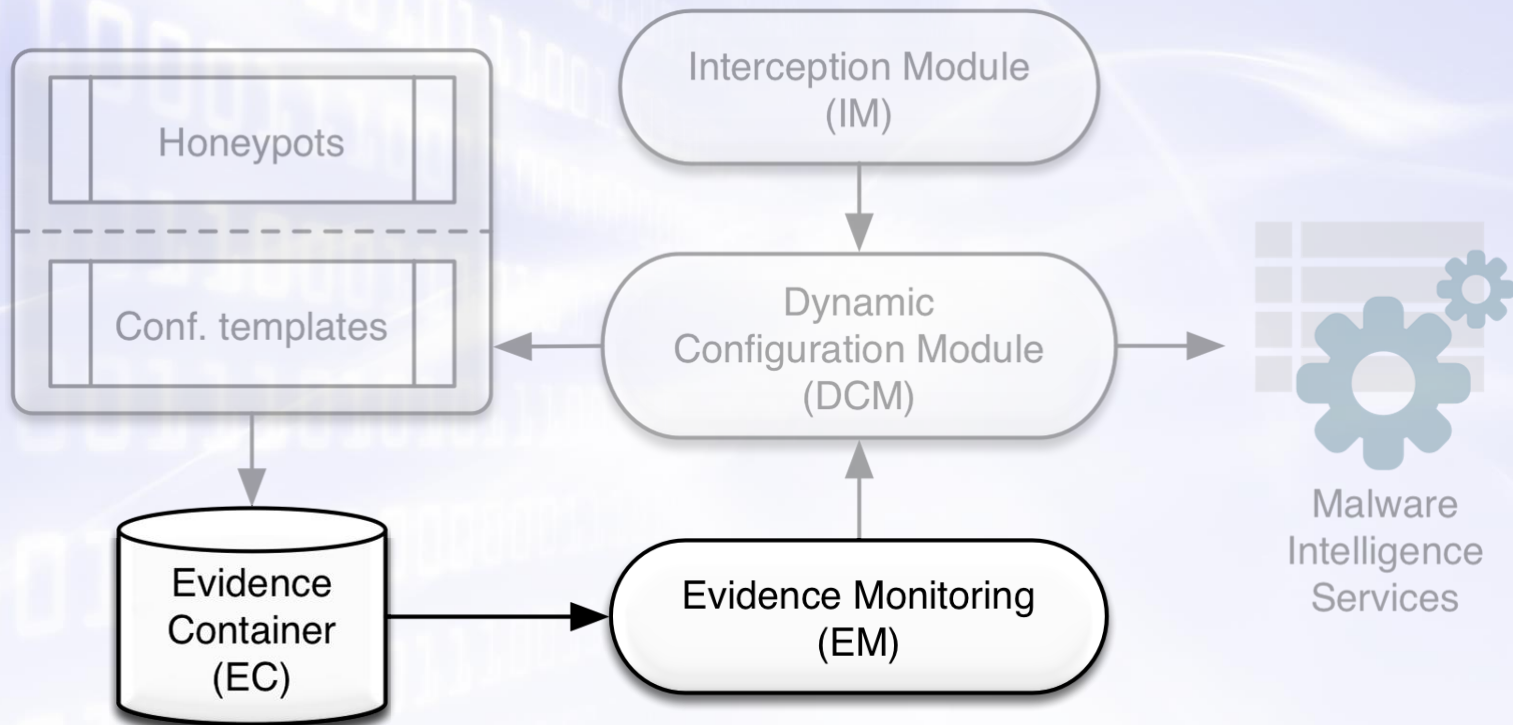
- **Objetivo:** interceptar tráfico de entrada para redirigirlo a un honeypot seleccionado.
 - 3 pasos:
 1. Atender peticiones de inicio de conexión
 2. Pedir el despliegue de un honeypot al DCM
 3. Recibir y aceptar conexiones



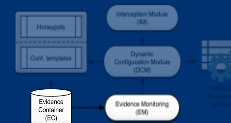
- **Objetivo:** interceptar tráfico de entrada para redirigirlo a un honeypot seleccionado.
 - 3 pasos:
 1. Atender peticiones de inicio de conexión
 2. Pedir el despliegue de un honeypot al DCM
 3. Recibir y aceptar conexiones
- Recopilará:
 - IP y puerto origen
 - Puerto de destino
 - Cabeceras del protocolo recibidas



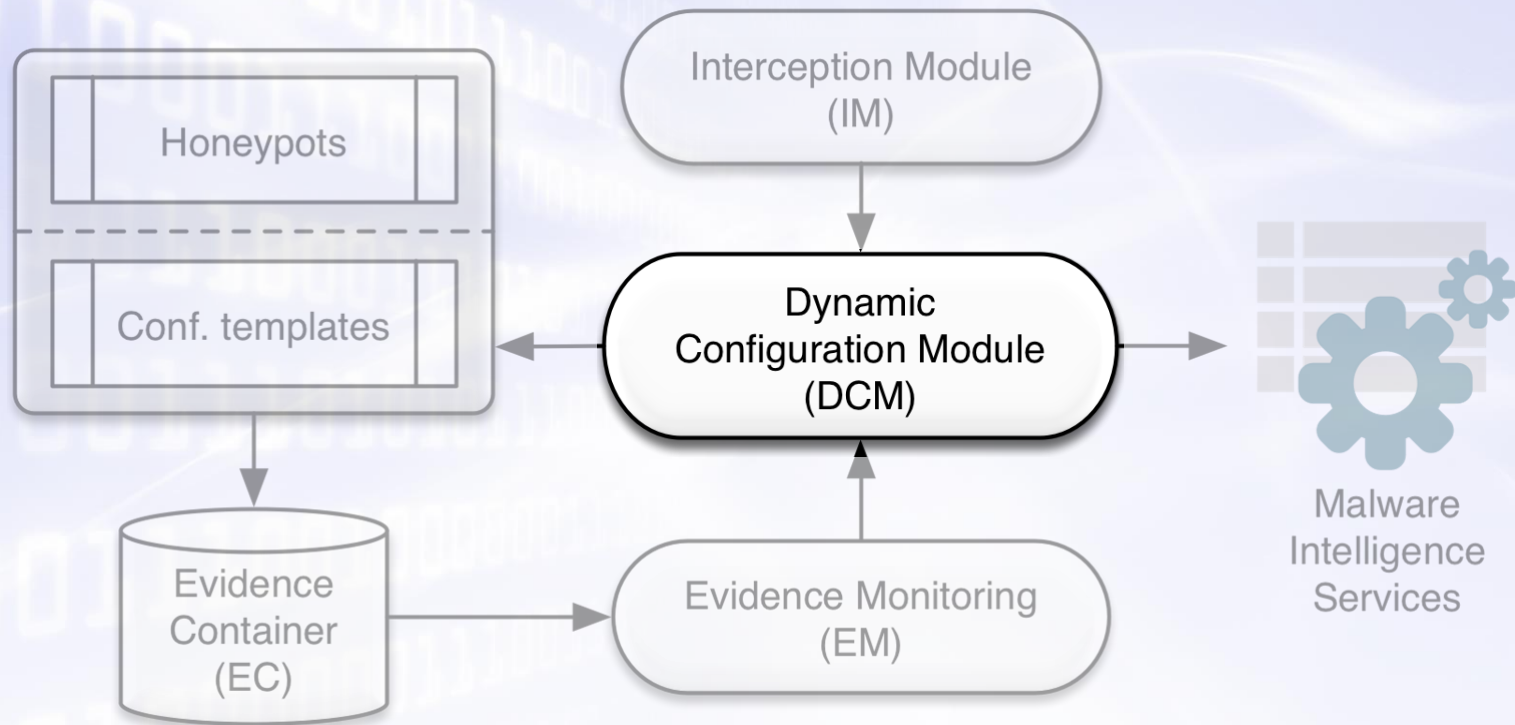
- **Objetivo:** interceptar tráfico de entrada para redirigirlo a un honeypot seleccionado.
 - 3 pasos:
 1. Atender peticiones de inicio de conexión
 2. Pedir el despliegue de un honeypot al DCM
 3. Recibir y aceptar conexiones
- Recopilará:
 - IP y puerto origen
 - Puerto de destino
 - Cabeceras del protocolo recibidas
- Esta información será procesada por DCM para el despliegue del honeypot



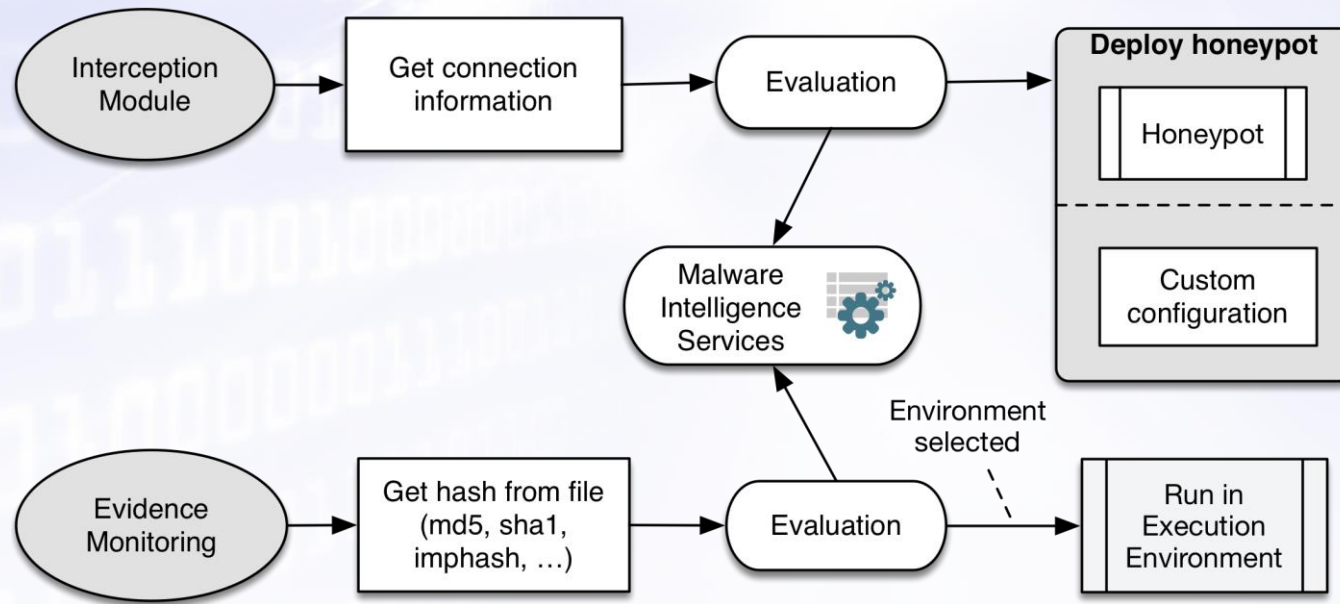
- **Objetivo:** controlar la aparición de nuevas evidencias creadas en el contenedor de evidencias (EC).
 1. Cuando se detecta un nuevo elemento se analiza su contenido (tipo de fichero, sistema operativo necesario, etc.)
 2. Se envía una petición de honeypot al componente DCM
 3. La evidencia es llevada a ejecución en un honeypot a medida.

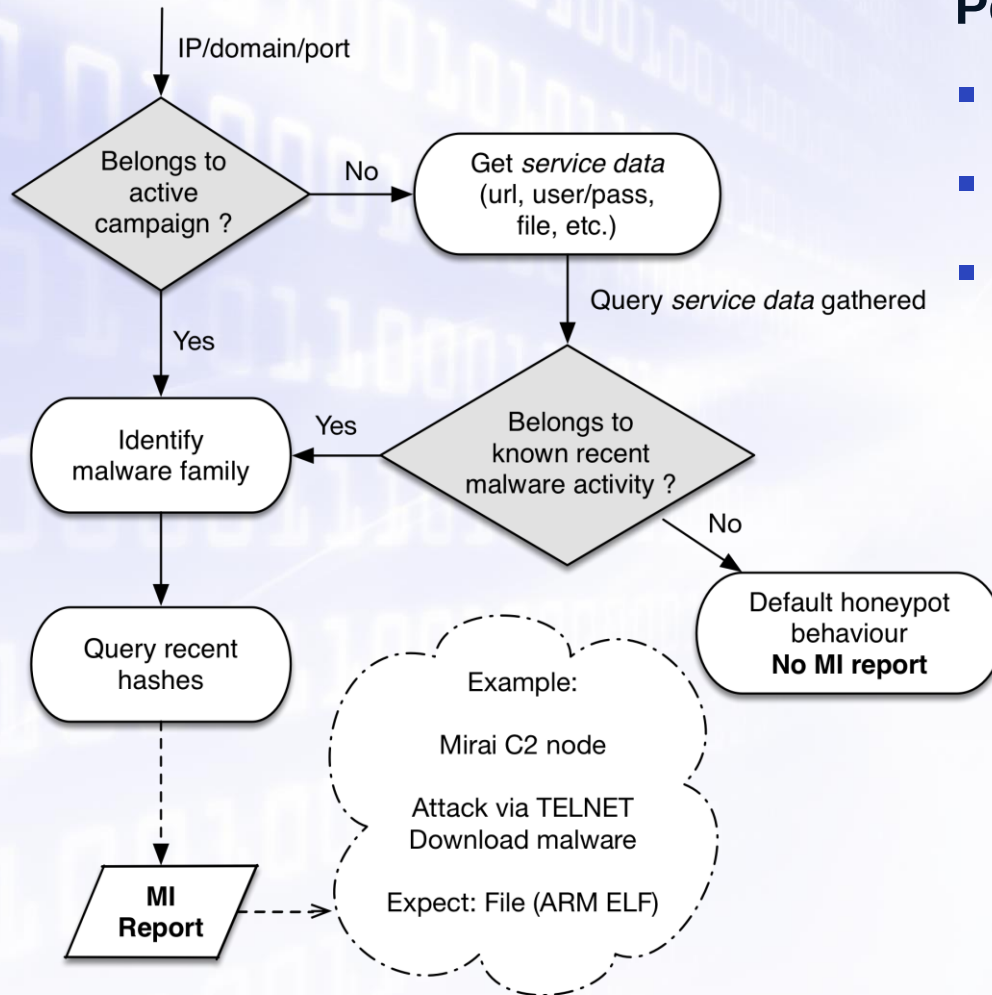
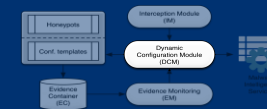


- **Objetivo:** controlar la aparición de nuevas evidencias creadas en el contenedor de evidencias (EC).
 1. Cuando se detecta un nuevo elemento se analiza su contenido (tipo de fichero, sistema operativo necesario, etc.)
 2. Se envía una petición de honeypot al componente DCM
 3. La evidencia es llevada a ejecución en un honeypot a medida.
- El objetivo del contenedor de evidencias es doble:
 - recopilar información sobre las acciones realizadas por el malware,
 - dar continuidad al mismo mediante la ejecución de las distintas fases que implementa.



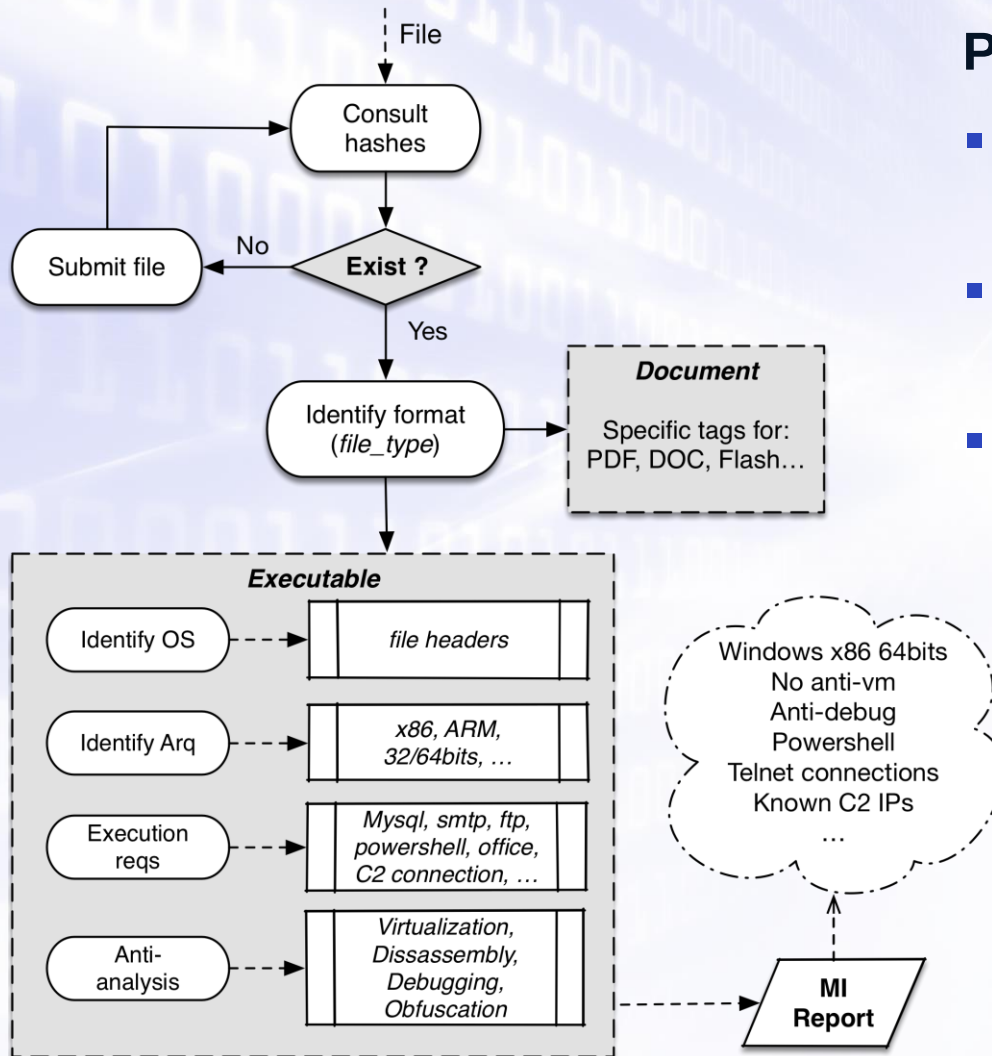
- **Objetivo:** decidir entorno más apropiado para servir al atacante.
 - Recibe: ip src, ip dst, cabeceras protocolo, información del servicio, ficheros relacionados
 - Para ello hará uso de servicios de malware intelligence
 - Este componente puede ser invocado por IM y por EM





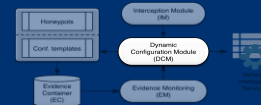
Peticiones sobre servicio

- Procedentes del componente IM
- Obtener datos de la conexión
- Consultar con servicios MI:
 - Comprobar si IP/dominio está relacionado con actividades de malware (L1 y L3)
 - Identificar la familia del malware
 - Obtener información sobre el entorno esperado.

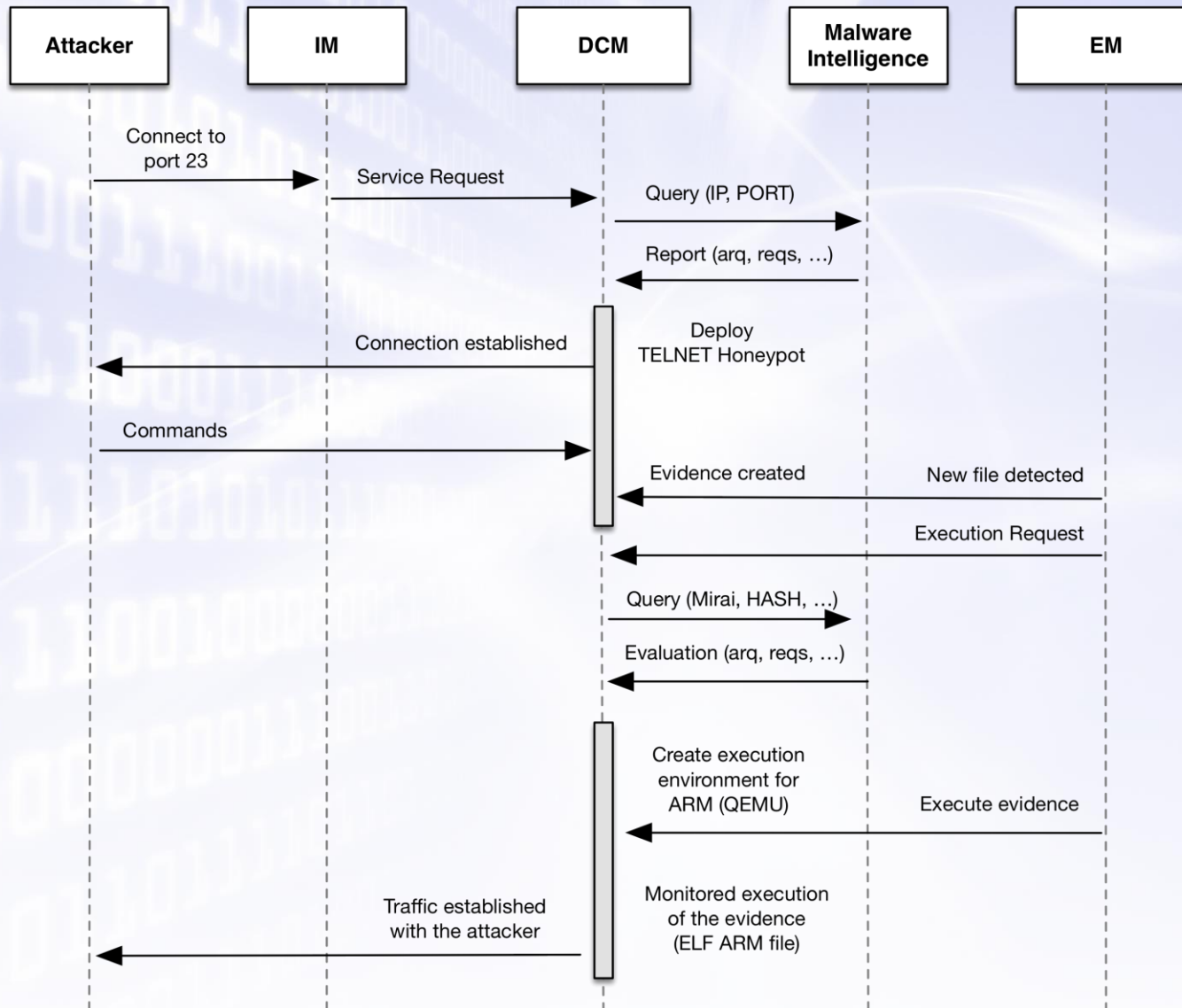


Peticiones sobre ficheros

- Procedentes del componente EM
- Ficheros almacenados en el contenedor de evidencias (EC)
- Empleando servicios L2 (y L3) obtendremos:
 - Sistema operativo necesario
 - Arquitectura del procesador
 - Servicios o aplicaciones afectadas (ya instaladas)
 - Técnicas anti-análisis empleadas



Mirai



- Los servicios de malware intelligence constituyen un valioso recurso no explorado hasta la fecha para la construcción de honeypots adaptativos.
- Principales retos:
 - Responder a las peticiones de conexión en el menor tiempo posible
 - Gestionar la información de inteligencia de manera adecuada
 - Evitar técnicas anti-análisis para evitar ofrecer un honeypot inadecuado
 - Clasificar repositorio de honeypots por objetivos (servicios, arquitectura, sistema operativo, aplicaciones, ...)
 - Tráfico malware no procede únicamente del interfaz de red externo
- Próximos pasos:
 - Gestión automatizada de acceso a información de inteligencia
 - Construir DCM

Configuración adaptativa de honeypots para análisis de malware

¡ Gracias por su atención !

Gerardo Fernández y Ana Nieto

gerardo@lcc.uma.es, nieto@lcc.uma.es

NICS Lab, Universidad de Málaga