NICS

Universidad Rey Juan Carlos

JNIC2017

III Jornadas Nacionales de Investigación en Ciberseguridad

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

JNIC 2017, 1 Junio 2017

Contenido

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

Honeypots

- **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

Honeypots

- **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

Honeypots

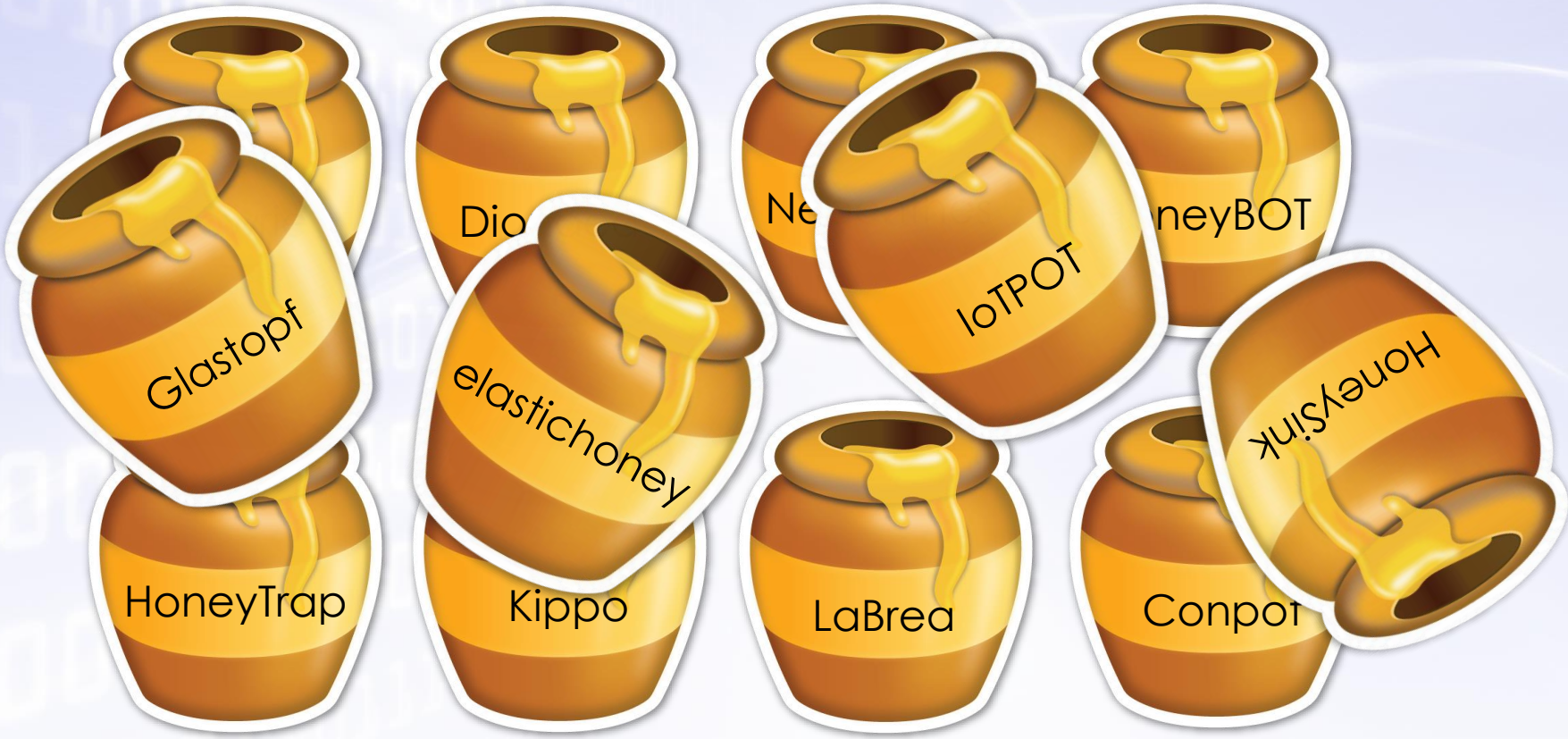
- **Utilidad de los honeypots:**
  - Todo tráfico dirigido contra ellos es sospechoso.
  - **Entorno productivo**: reproducir servicios entornos productivo para capturar futuros ataques dirigidos contra equipos en producción.
  - **Investigación**: capturar nuevos ataques, revelar tendencias en los nuevos 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.

Honeypots

- **Multitud de honeypots en la actualidad...**

Honeypots

- **Multitud de honeypots en la actualidad...**



Honeypots

- **Multitud de honeypots en la actualidad...**

Malware Intelligence

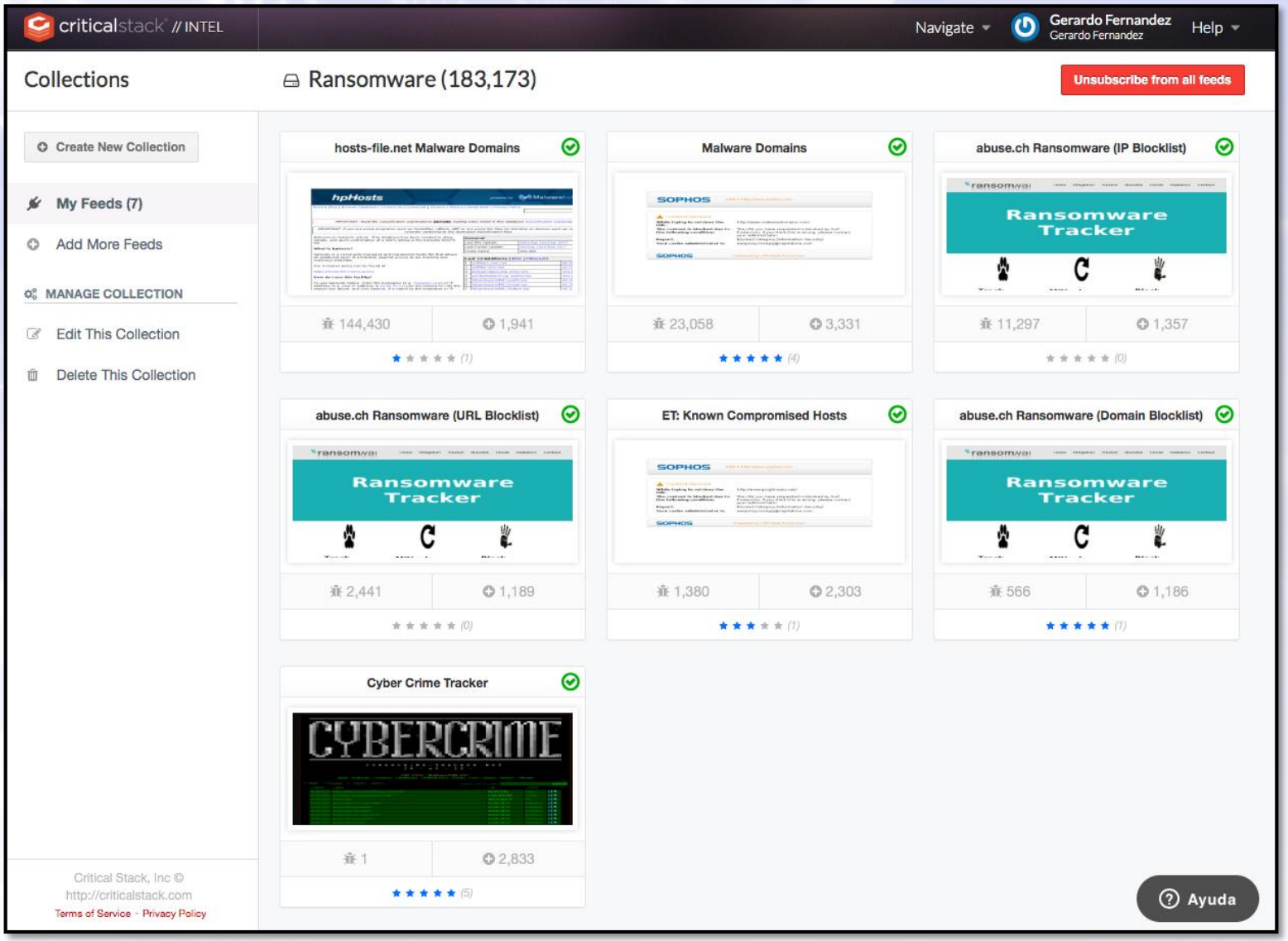
- Con el término *malware intelligence* nos referimos a información de inteligencia sobre el comportamiento y la difusión del malware.
  - ¿A qué **sistemas operativos** afecta?
  - ¿Qué **componentes** del sistema ataca?
  - ¿Con quién se **comunica**?
  - ¿Qué **actividad** realiza?
  - ¿Quién lo ha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

Malware Intelligence

- 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.)

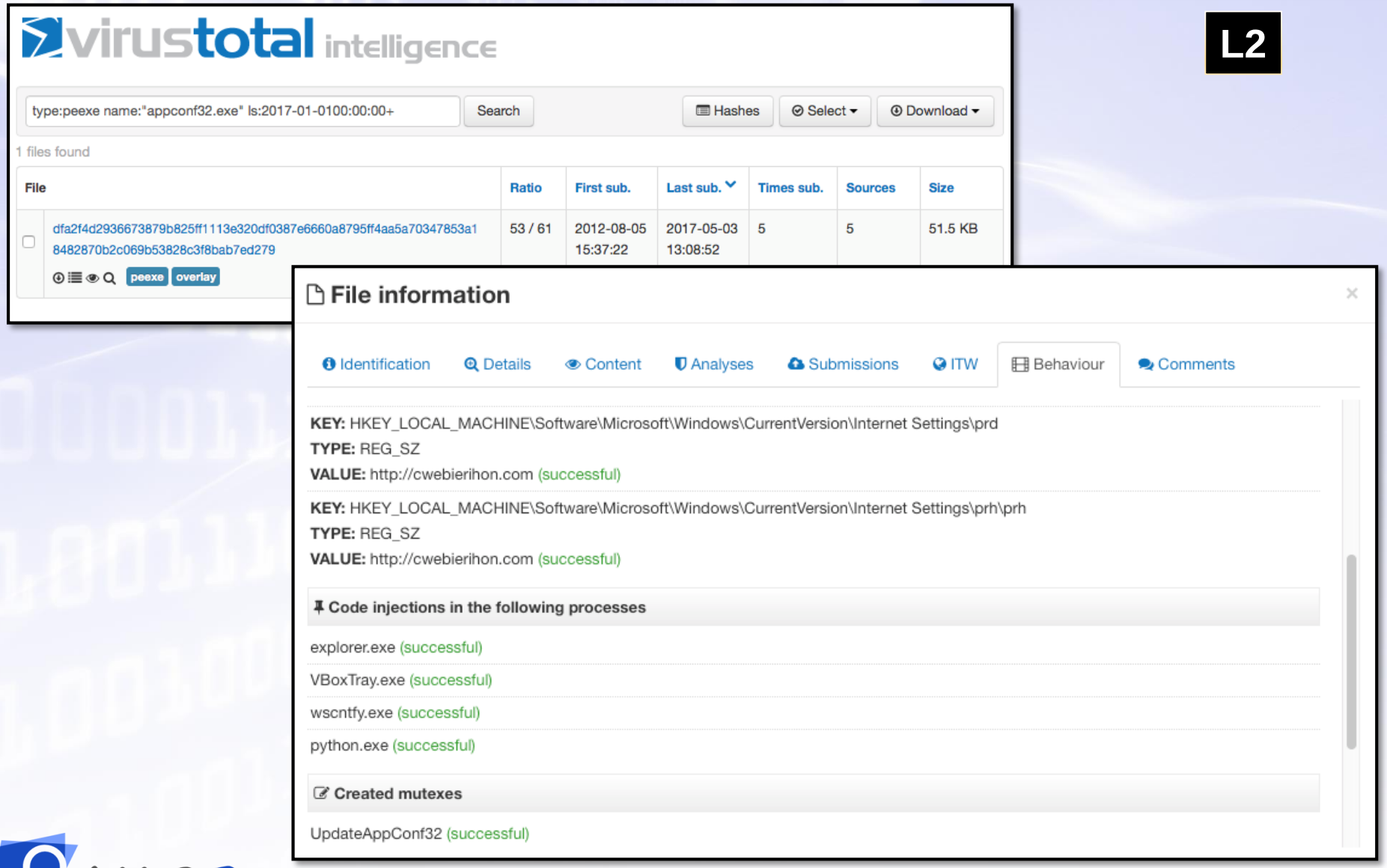
Malware Intelligence

L1



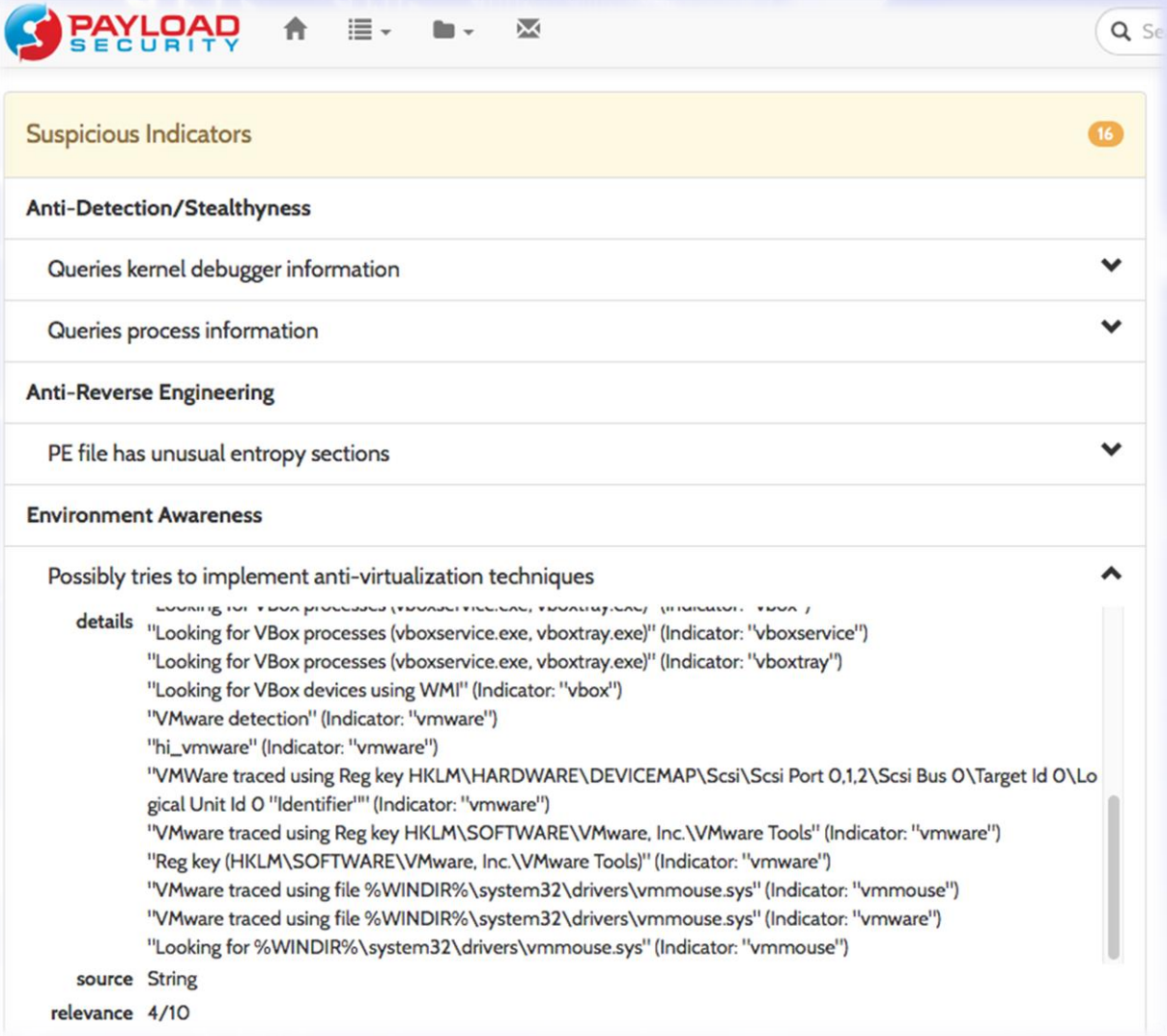
Malware Intelligence

L2



Malware Intelligence

L2



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>
```

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>b923db309a973d7229a1e77352e80486</value>
        </Attribute>
        <Tag><name>misp-galaxy:ransomware=”Locky"</name></Tag>
</Event>
</response>
```

Arquitectura Hogney

- **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

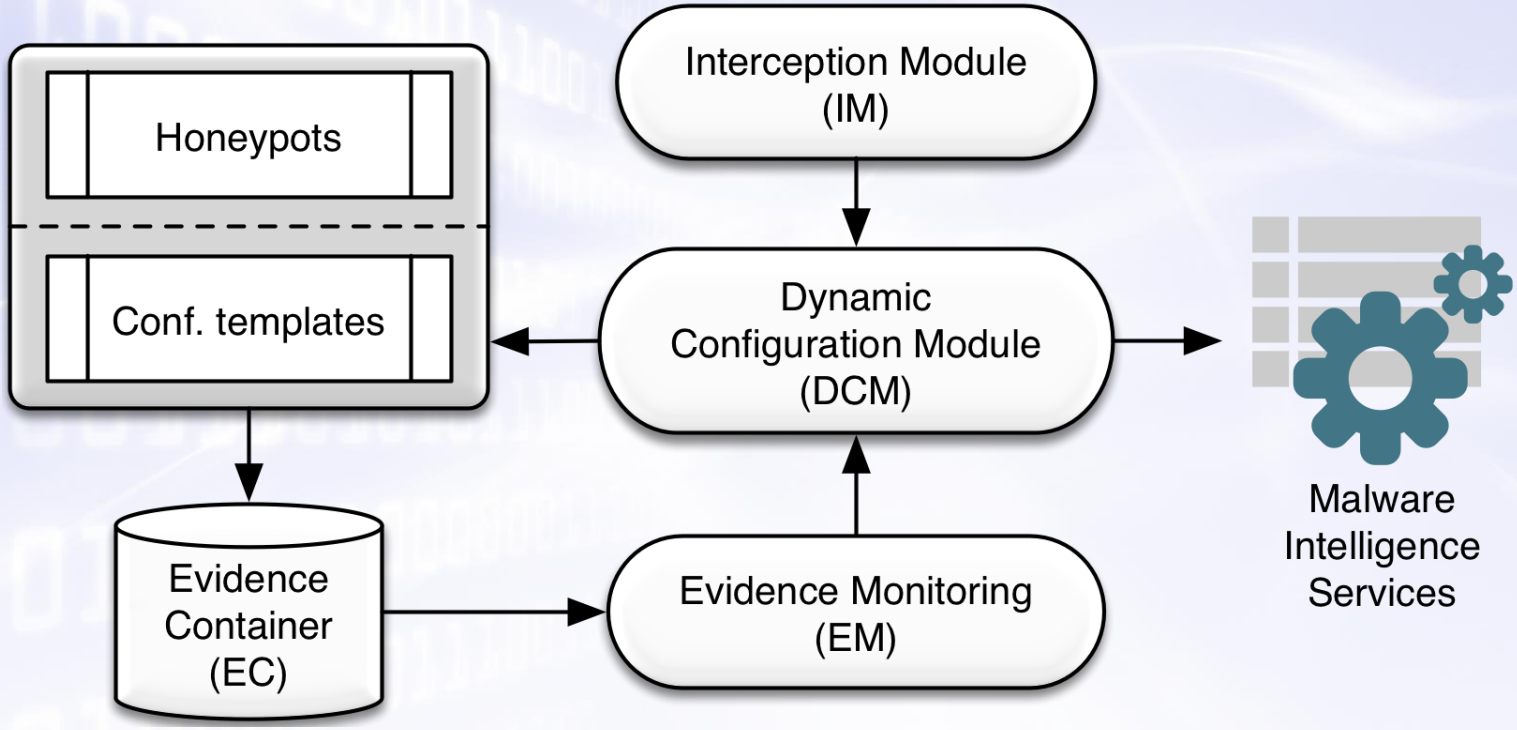
Arquitectura Hogney

- **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

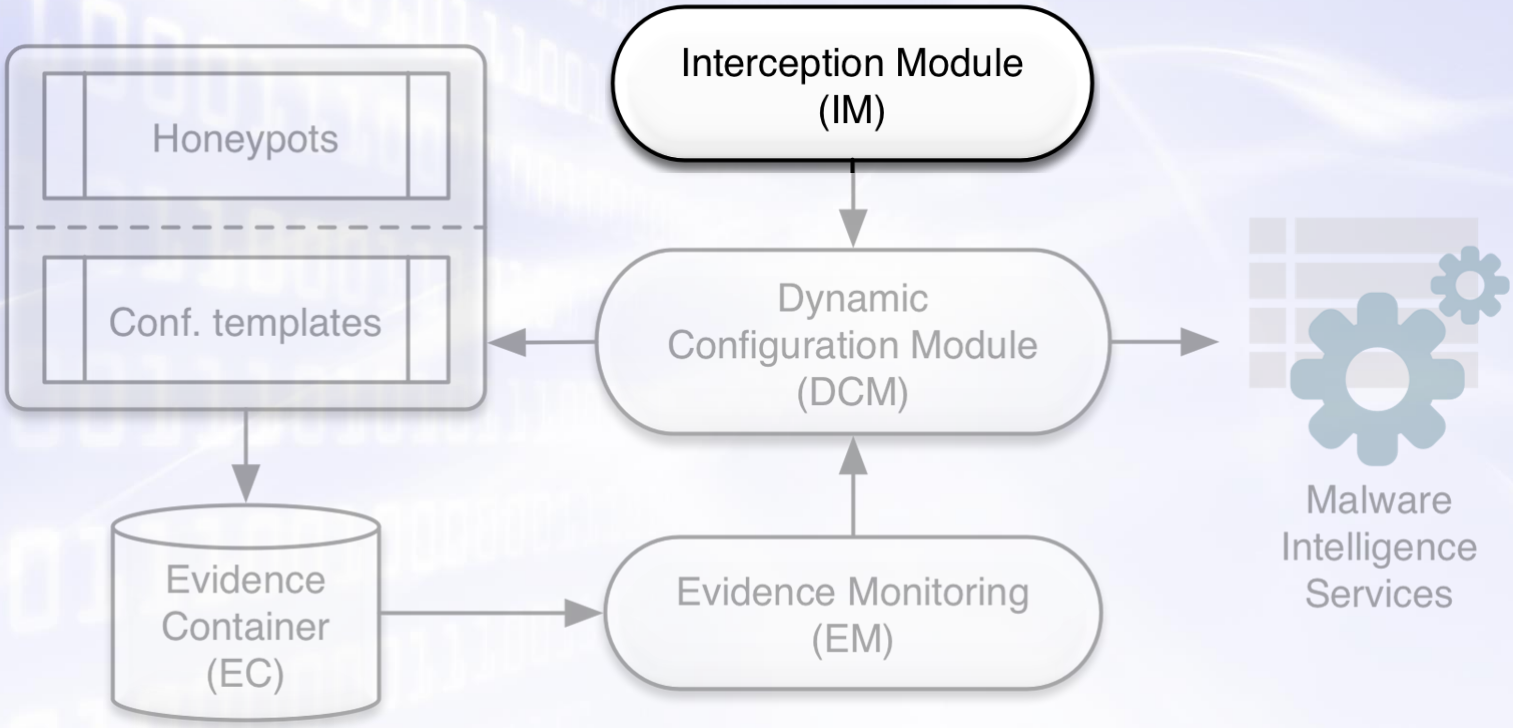
Arquitectura Hogney

- **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

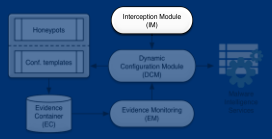
Arquitectura Hogney



Arquitectura Hogney

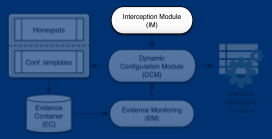


Hogney: intercepción



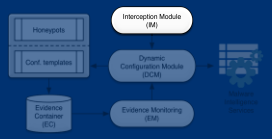
- **Objetivo**: interceptar tráfico de entrada para redirigirlo a un honeypot seleccionado.
  - 3 pasos:
    1. Atender peticiones de inicio de conexión
    2. Pedir el despliegue de un honeypot al DCM
    3. Recibir y aceptar conexiones

Hogney: intercepción



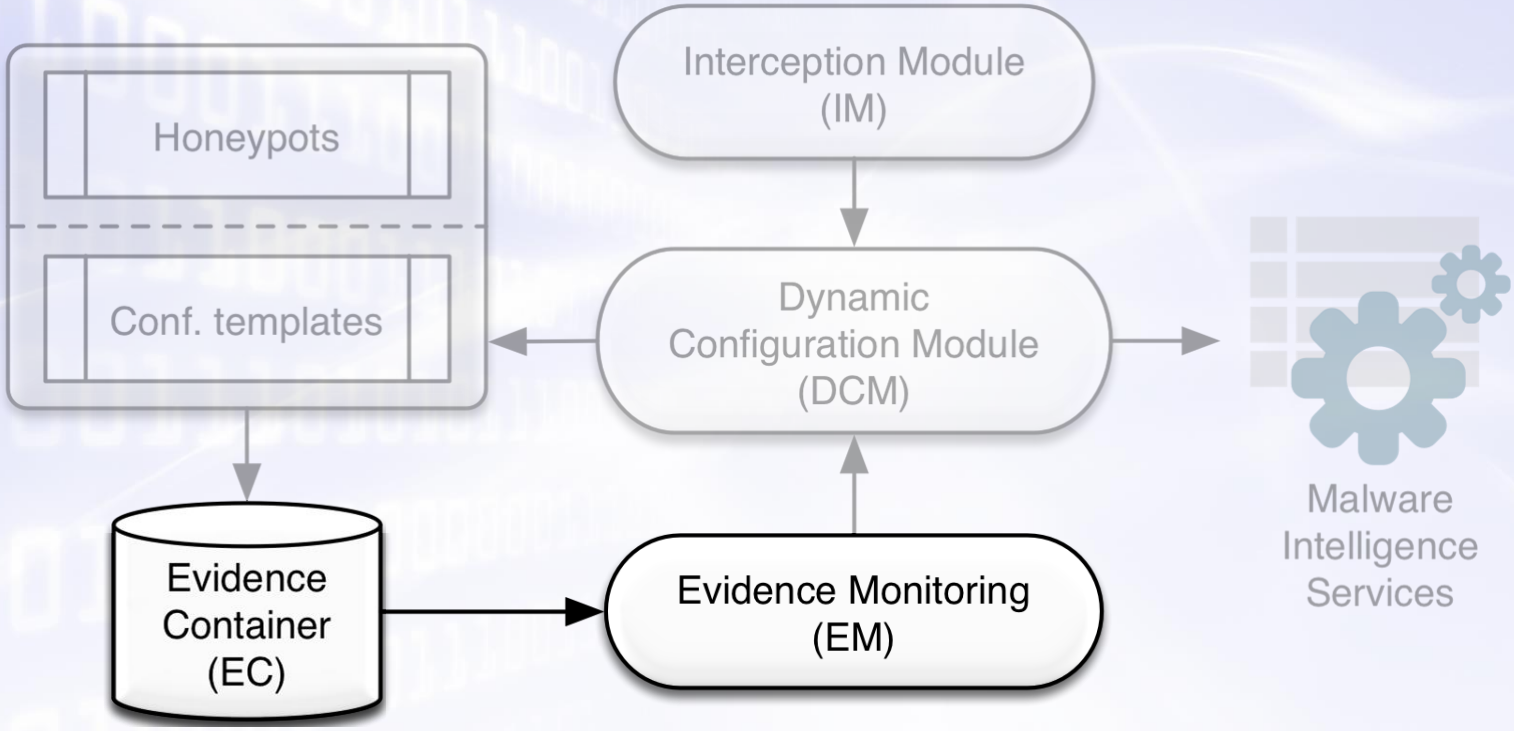
- **Objetivo**: interceptar tráfico de entrada para redirigirlo a un honeypot seleccionado.
  - 3 pasos:
    1. Atender peticiones de inicio de conexión
    2. Pedir el despliegue de un honeypot al DCM
    3. Recibir y aceptar conexiones
- Recopilará:
  - IP y puerto origen
  - Puerto de destino
  -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

Hogney: intercepción

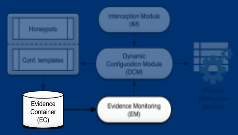


- **Objetivo**: interceptar tráfico de entrada para redirigirlo a un honeypot seleccionado.
  - 3 pasos:
    1. Atender peticiones de inicio de conexión
    2. Pedir el despliegue de un honeypot al DCM
    3. Recibir y aceptar conexiones
- Recopilará:
  - IP y puerto origen
  - Puerto de destino
  -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

Arquitectura Hogney

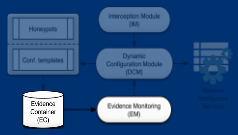


Hogney: monitorización



- **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.

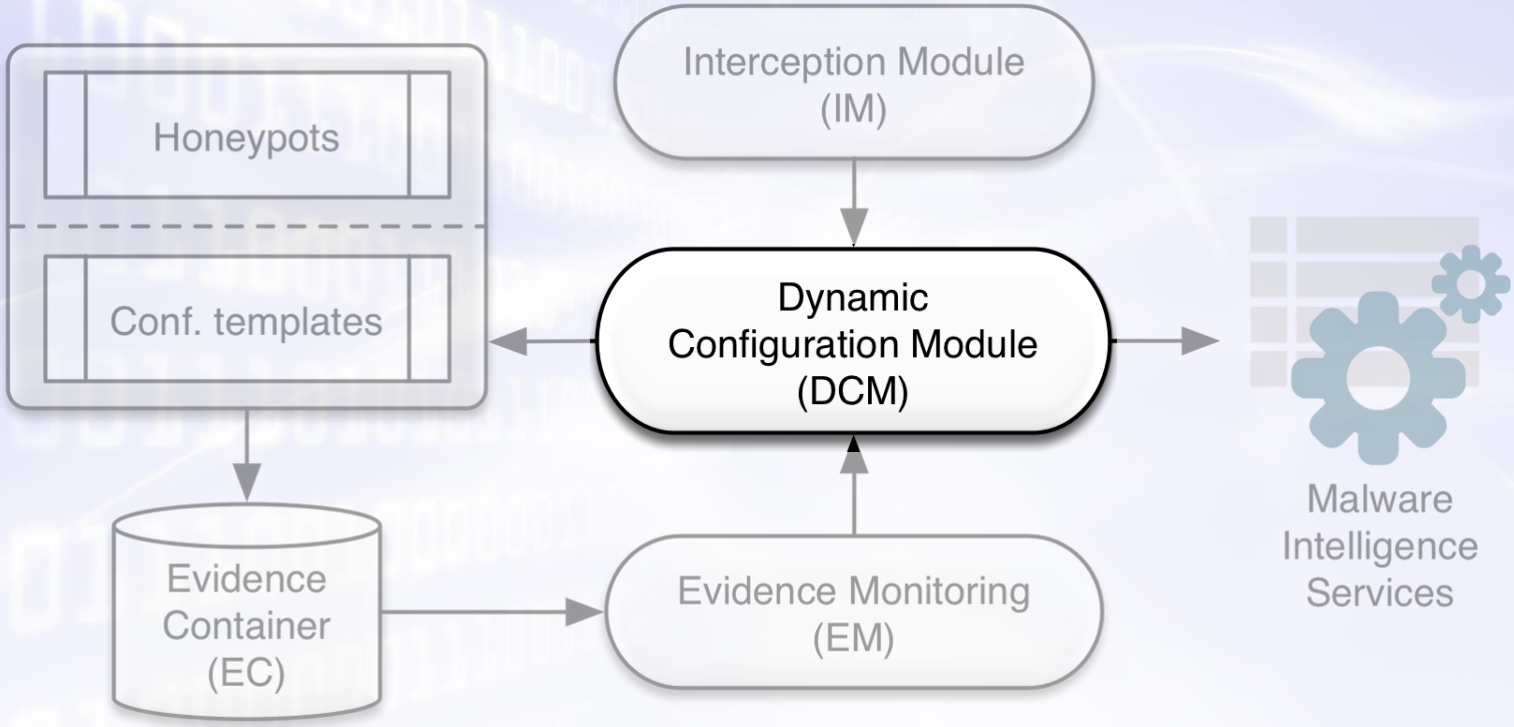
Hogney: monitorización



- **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.

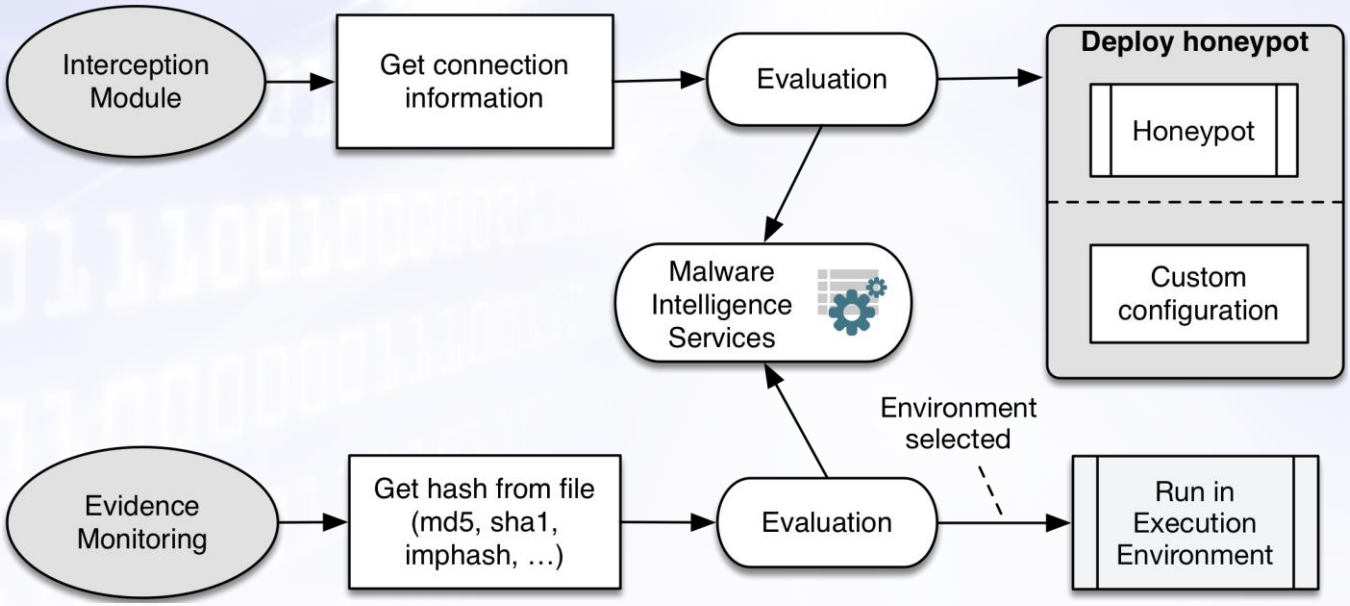
- El objetivo del contenedor de evidencias es doble:
  - recopilar información sobre las acciones realizadas por el malware,
  - dar continuidad al mismo mediante la ejecución de las distintas fases que implementa.

Arquitectura Hogney

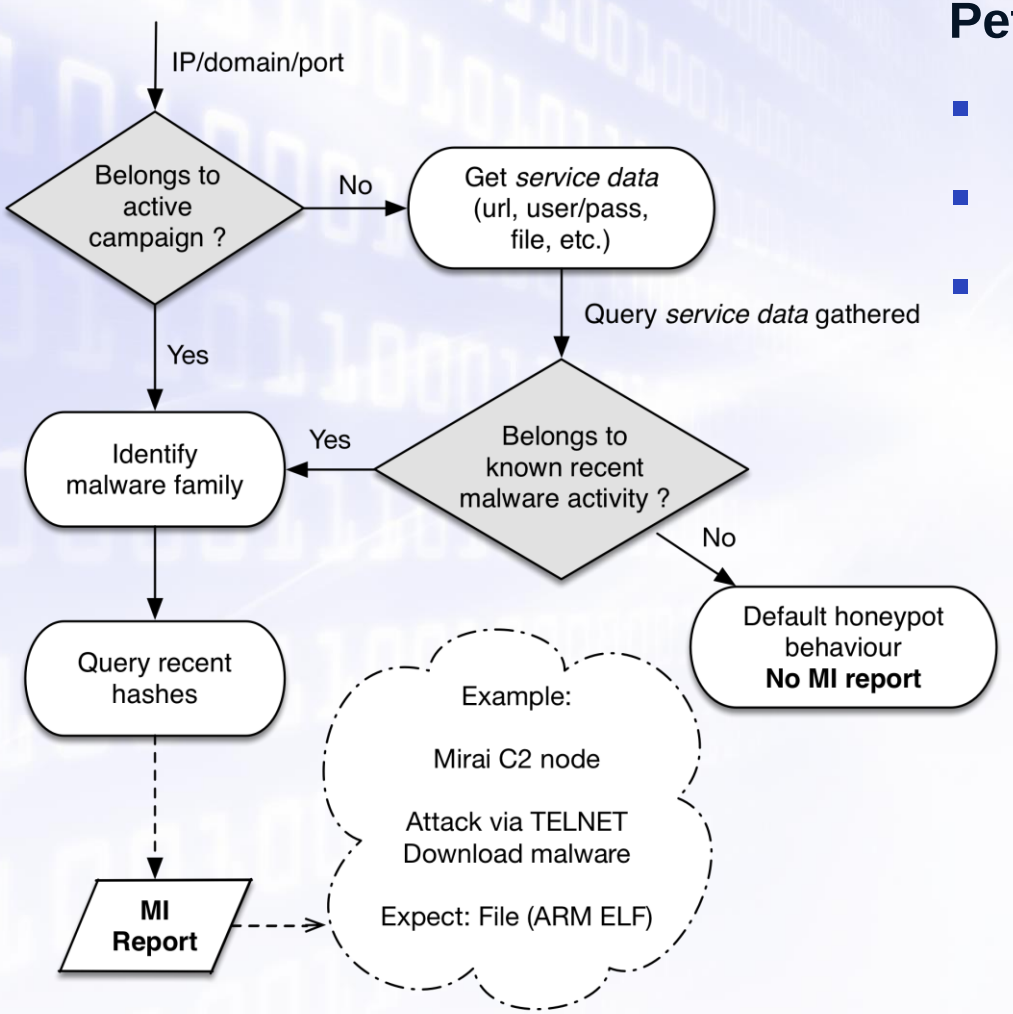


Hogney: adaptación

- **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



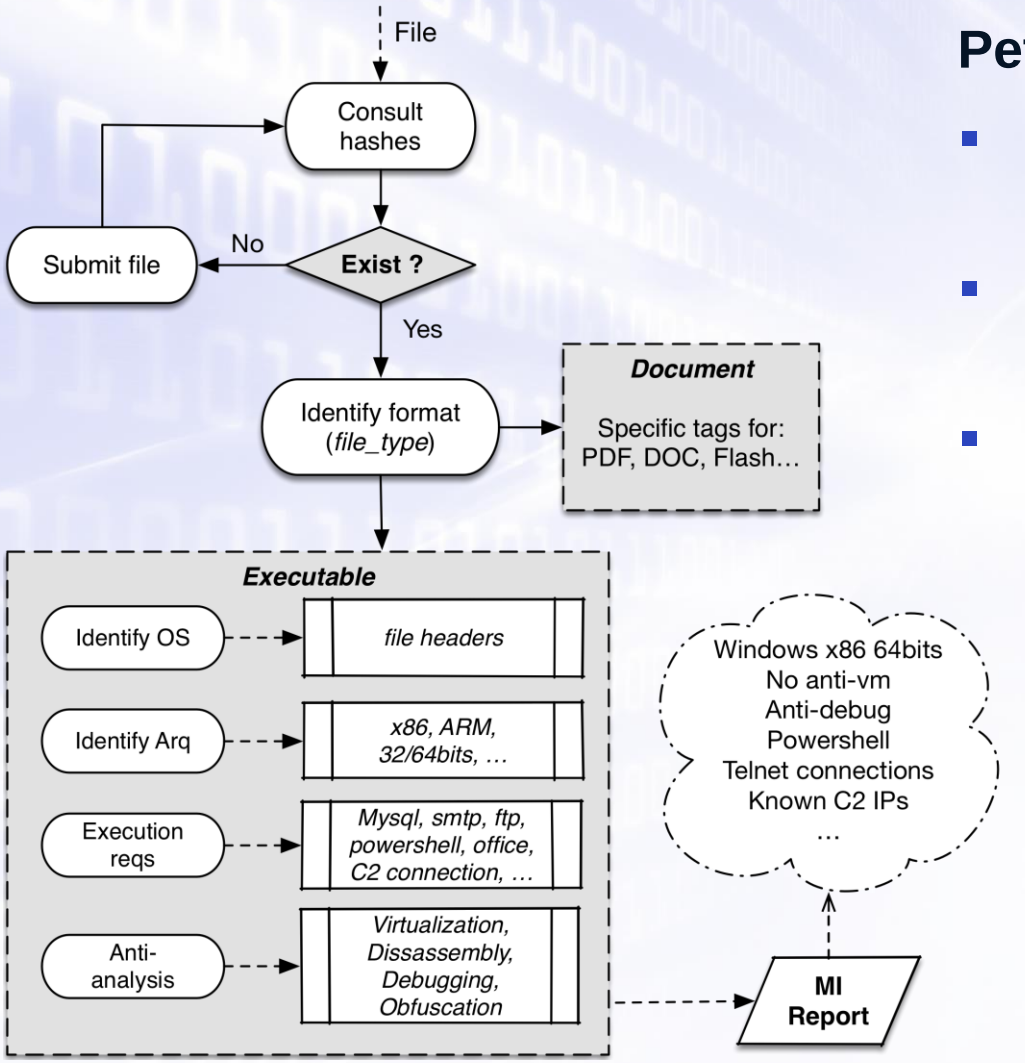
Hogney: adaptación



Peticiones sobre servicio

- Procedentes del componente IM
- Obtener datos de la conexión
- Consultar son 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.

Hogney: adaptación

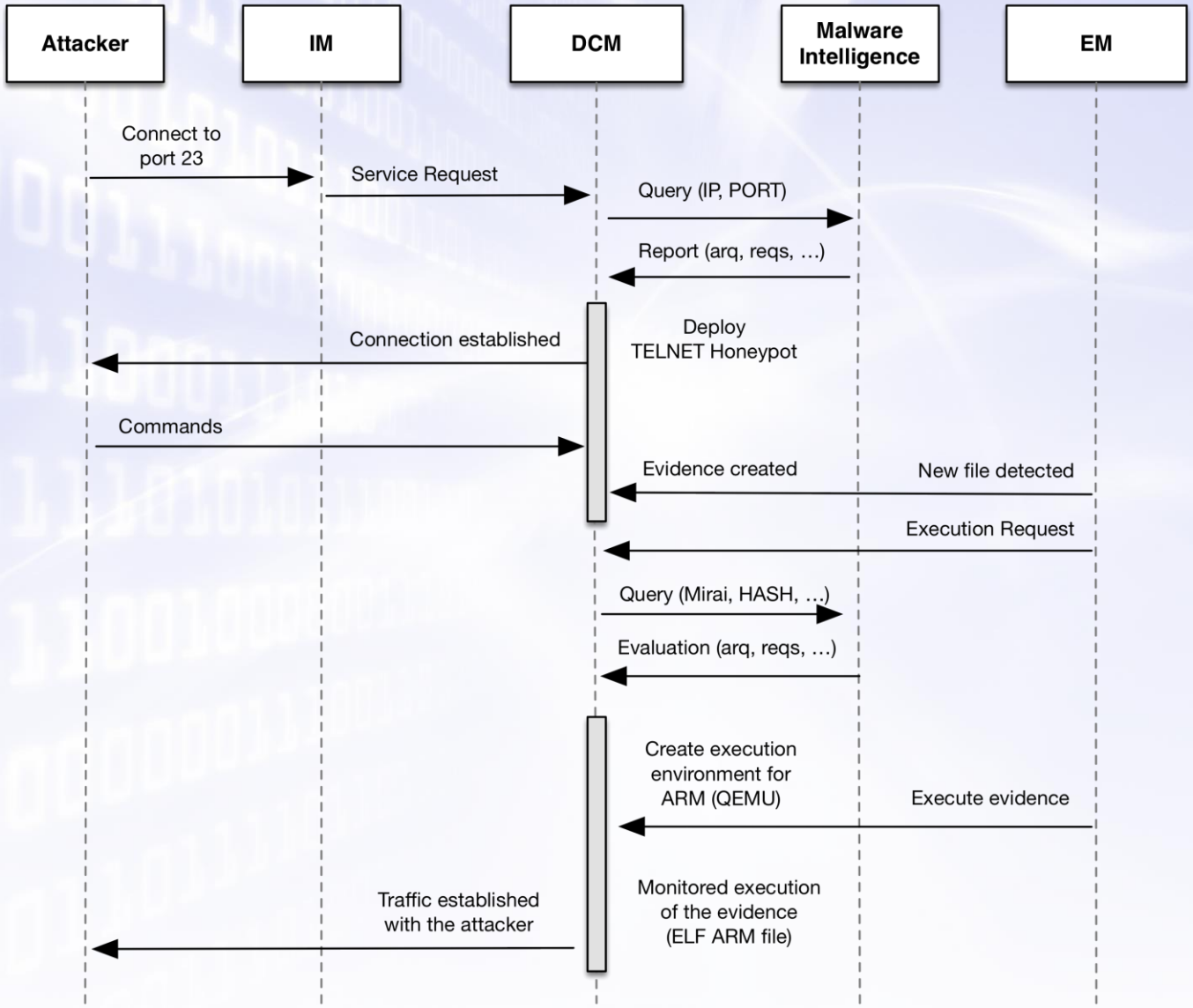


Peticiones sobre ficheros

- 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

Caso de uso

Mirai



Conclusiones

- 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

Universidad Rey Juan Carlos

JNIC2017

III Jornadas Nacionales de Investigación en Ciberseguridad

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

JNIC 2017, 1 Junio 2017