DECEPTIONPI

ISACA®

Trust in, and value from, information systems

MUNDO HACKER 2016

ANÁLISIS DE LAS TENDENCIAS DE ATAQUES Y MALWARE EN SISTEMAS SEÑUELO PARA INFORMÁTICA FORENSE

¿Quiénes somos?

Diego Jurado Pallarés

IT-ERS Security at CyberSOC Deloitte
Grado en Ingeniería Informática
Universidad Autónoma de Madrid

@djurado9 0d4rujd d_jurado391@hotmail.com

Juan Antonio Velasco Gómez

Doble Grado en Matemáticas e Informática
Universidad de Granada

@juanvelasc0 juanvelascogomez juanvelasco@protonmail.com

Esquema del proyecto

- Introducción
- Definición de honeypot
  - Finalidad
  - Clasificación
- Diseño de la red
  - Implementación
  - Mejora y ocultación
- Resultados obtenidos
- Análisis Forense
- Conclusiones y trabajo futuro

#RetoISACA 2016

Honeypots

Un honeypot es un sistema muy flexible dentro de la seguridad informática, que se encarga de atraer y analizar el comportamiento de los atacantes en internet, y que provee al informático forense de una información extremadamente valiosa.

El objetivo es capturar todo el tráfico de red entrante y conocer todos los detalles acerca de las tendencias y metodologías de ataque de los atacantes así como los fallos de seguridad a los que puede estar expuesto nuestra red con el fin de subsanarlos.

Finalidad de un honeypot

- Expuesto deliberadamente para ser atacado
- Desviar y distraer la atención del atacante
- Detectar y aprender nuevas vulnerabilidades de los sistemas
- Obtener información sobre el atacante (geolocalización, ip, puertos, …)
- Obtener tendencias de ataque y países más atacados
- Detectar nuevas muestras de malware que aún no se conozcan
- Recopilar y estudiar tendencias de ataque
- Aprendizaje en temas de malware
- Uso como complemento a otras soluciones de seguridad

Clasificación de honeypots

Uso

Producción

- Prevenir, detectar y responder.
- Proteger organizaciones en ambientes reales de operación.
- Alertar a los administradores

Investigación

- Aprendizaje. Recursos educativos.
- Recuperar la mayor cantidad de información posible para detectar patrones o analizar nuevas tendencias.
- Retener al intruso el mayor tiempo posible dentro del honeypot.

Interacción

Baja

- Investigación de acciones fraudulentas en la red.
- Detectar nuevas amenazas.
- Fáciles de utilizar y de mantener, riesgo casi nulo.
- Instalación en herramientas de virtualización.

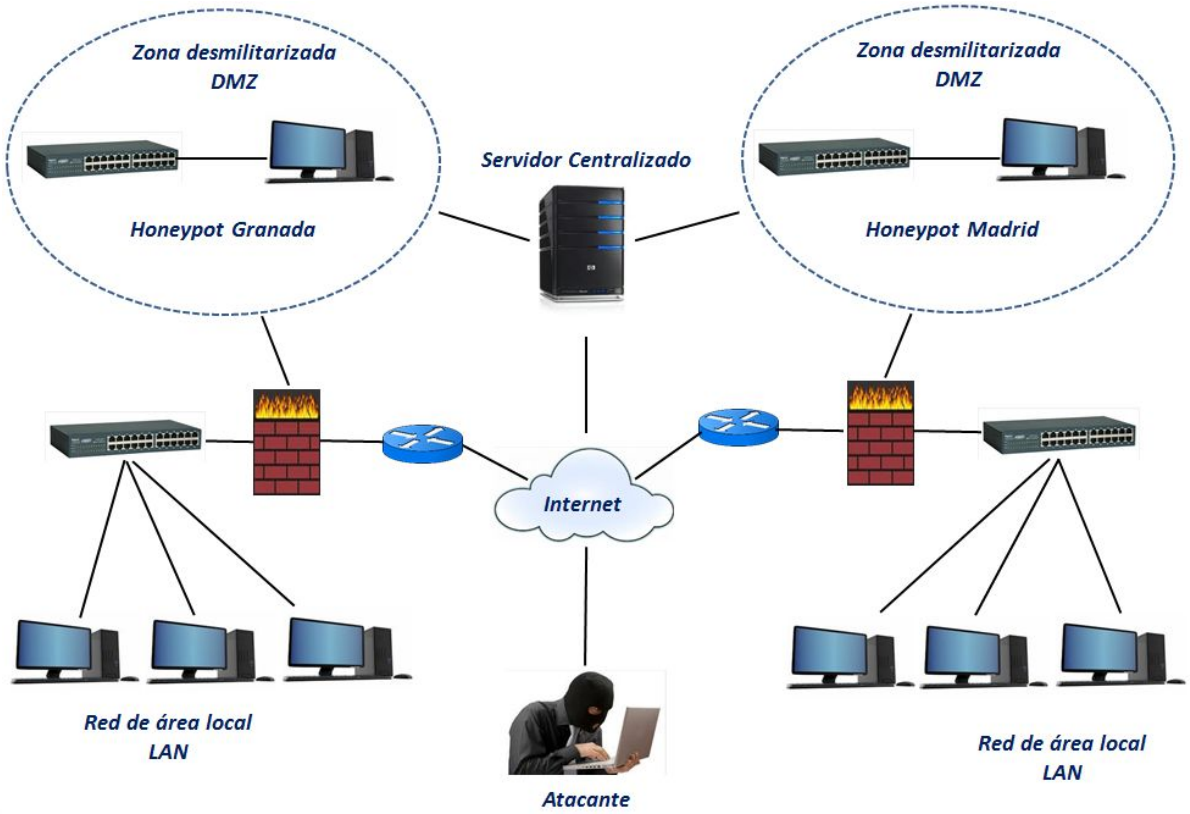
Media

- Mayor nivel de interacción que los de bajo nivel.
- Recolectar información sobre actividades efectuadas por atacantes.
- No emulan únicamente ciertos servicios, también software en particular. Mayor riesgo y más complejos.

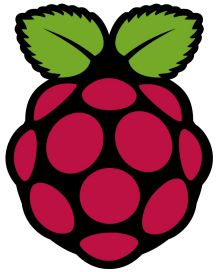
Alta

- Construidos con máquinas reales, como un usuario normal.
- Usados en red interna y único objetivo: ser atacados.
- Cada interacción se considera sospechosa por definición.
- Todo el tráfico es monitorizado y almacenado en una zona segura.

Diseño de la red



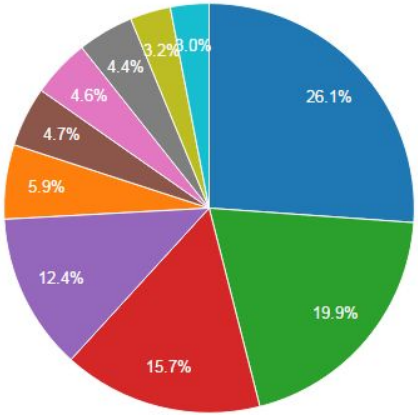
Implementación

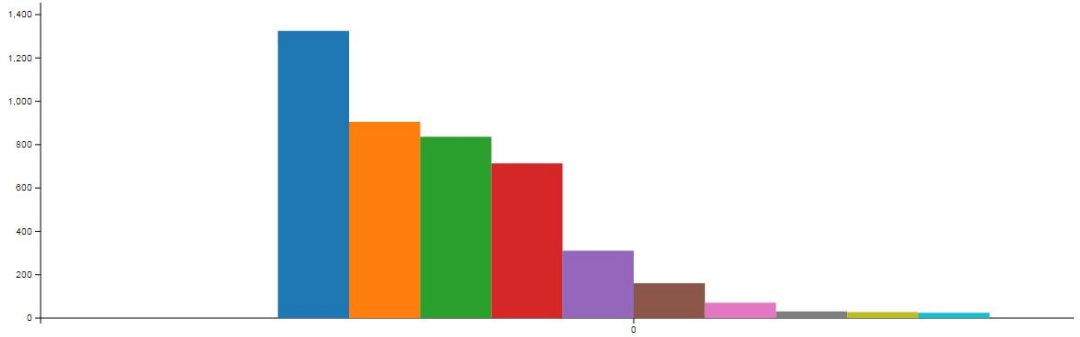


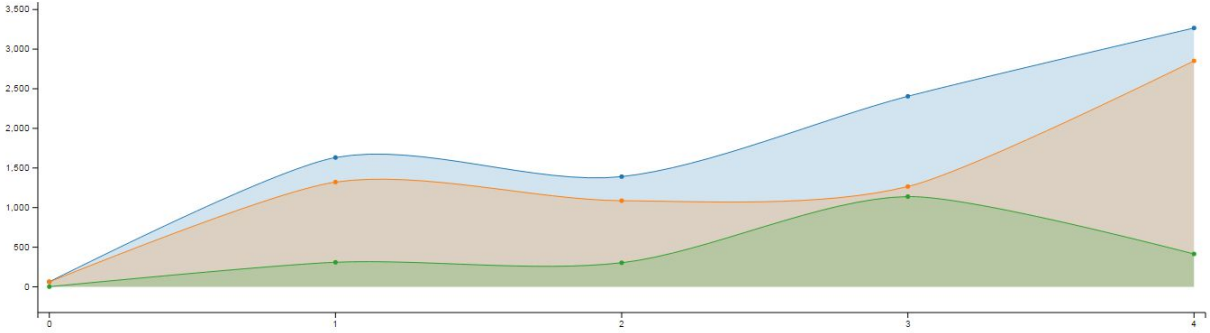
Mejora y ocultación del Honeypot

- Modificación y gestión de usuarios mediante sistema de ficheros
  - Eliminando usuarios por defecto
  - Introduciendo usuarios reales
- Mejorando los directorios del sistema
  - Sistema de archivos básico: createfs.py y fsctl.py
  - Editando directorios importantes: /tmp, var/www, /etc…
  - Directorios para los diferentes usuarios “trampa”
- Archivo de configuración de cowrie
  - Hostname: sr04 → WebServerIsaca
  - Versión de SSH

Resultados

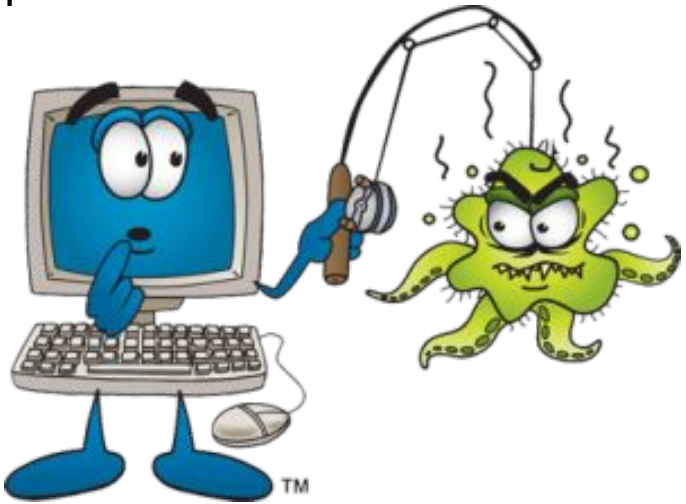

26.1%
19.9%
15.7%
12.4%
5.9%
4.7%
4.6%
4.4%
3.2%
3.0%


1,400
1,200
1,000
800
600
400
200
0
0


3,500
3,000
2,500
2,000
1,500
1,000
500
0
0
1
2
3
4

Análisis Forense

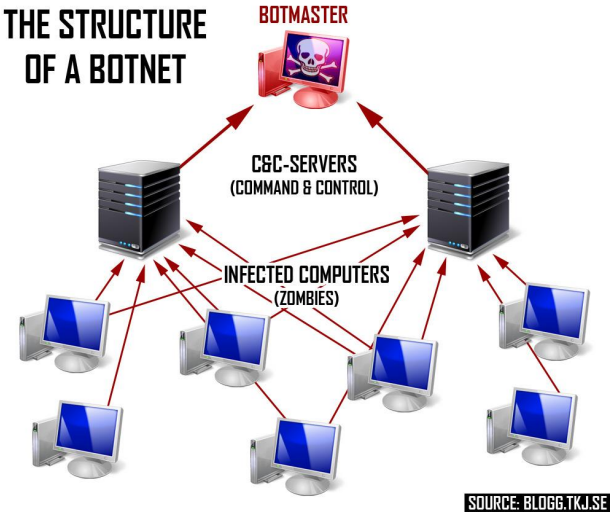
- Detección de Botnets y listas de reputación
- Análisis de Malware
- Ataques por fuerza bruta
- Securización mediante IPTables

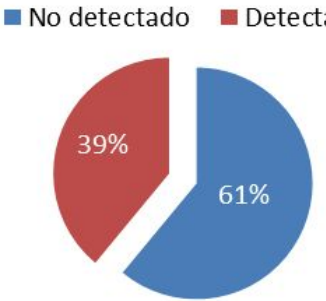


Botnets

- Identificación mediante comportamiento (PlayLog)
- Automatización con listas de reputación
  - Repu-IP by @rbelane

```
root@HoneyPi:/opt/PruebasIsaca# python3 IP-Repu.py suspicious_ips.txt
 [+] 58.218.199.166 Bad IP Reputation -> User Submission - Hacker from this IP on 16 April 2016
 [+] 27.72.64.222 Good IP Reputation
 [+] 74.208.127.6 Good IP Reputation
 [+] 95.128.43.164 Bad IP Reputation -> Unknown Spam Bot masking himself as a normal user on 15 July 2015
 [+] 178.151.69.1 Good IP Reputation
 [+] 58.218.204.248 Bad IP Reputation -> User Submission - Hacker from this IP on 16 April 2016
 [+] 139.162.4.25 Good IP Reputation
```





IP Void

MYIP.MS
Hosting Info, Websites & IP Database

Malware

- Parada de Cortafuegos (service iptables stop)
- Descargas de Malware con SFTP o WGET
  - Independientes de la arquitectura
- Incluir nuestro sistema en parte de una Botnet
- Borrado de huellas.
  - Historial y logs
- Comprobación del sistema en el que se encuentra
  - Ejecución de comandos

- Número de muestras registradas : 830
- API VirusTotal

Fuerza Bruta y Securización con IPTables

- Detección de ataques de fuerza bruta por diccionario
- Registradas 8700 combinaciones usuario/contraseña
  - 33% son únicas
  - 11% consigue su objetivo -> comprometer el sistema
- Solución!! ... configuración de reglas con IPTables
  - Ignorar tráfico que proviene de IPs sospechosas (Blacklist)
  - Mejor aún : bloquear todo el tráfico & permitir conexiones fiables (Whitelist)


```
iptables -A INPUT -s 155.67.33.49 -j DROP
```

Conclusiones y trabajo futuro

Recomendaciones

- Cambiar el puerto SSH por defecto.
- No permitir la autentificación como usuario root.
- Implementar medidas contra ataques por fuerza bruta.
- Uso de contraseñas más fuertes.
- Hacer uso de las opciones host.allow y host.deny para especificar que IP’s se van a permitir y cuáles no.

Trabajo futuro

- Implementar otras honeypots en nuestra red.
- Mejorar la automatización de extracción de datos.
- Fortificar nuestros servicios.
- Emular otros servicios como Telnet.
- Reconfigurar reglas de firewalls e iptables.
- Mejorar la visualización de datos.
- Machine learning.
- Obtener inteligencia.

¿Preguntas?