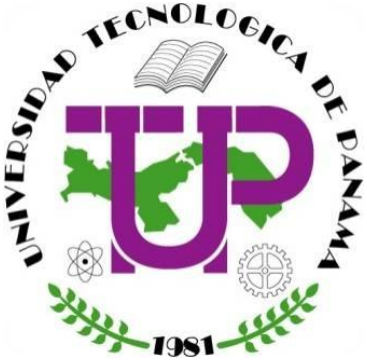


Estudio de Medición de la Actividad de Botnets en la República de Panamá

Mario Góngora Blandón, Gaspar Modelo Howard, Rubén Torres

VII Congreso Iberoamericano de Seguridad Informática CIBSI+TIBETS

Octubre 30, 2013

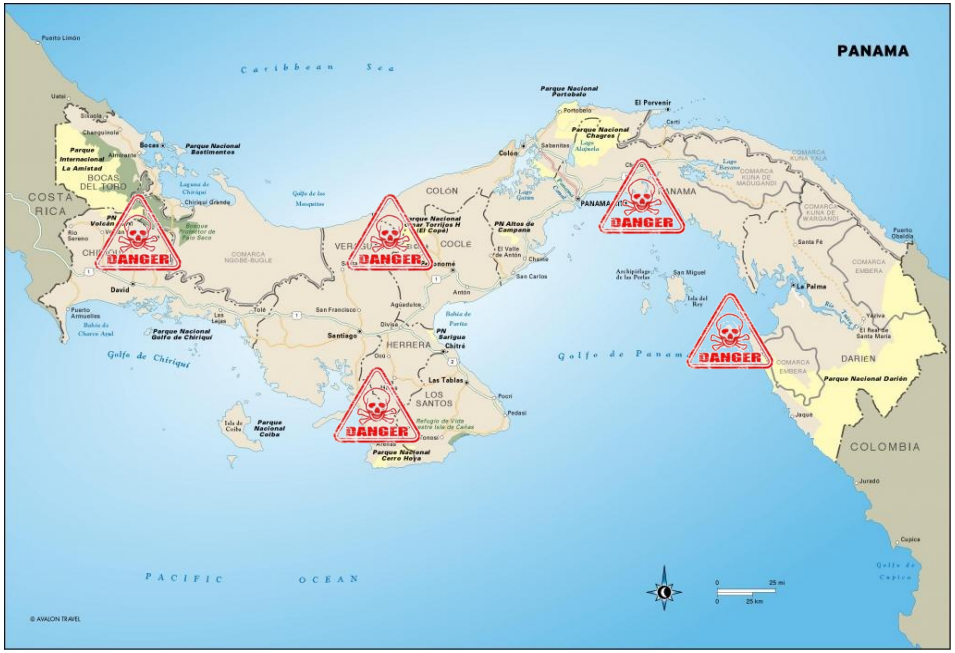
Laboratorio de Redes y Seguridad Informática ARGUS

Agenda

- Introducción
- Plataforma de Captura
- Métricos de Evaluación
- Resultados
- Conclusiones y Trabajo Futuro

Introducción

- Planteamiento del problema
  - Continuo crecimiento de los servicios informáticos motiva actividades ilegales en el ciberespacio.
    - Los botnets son utilizados para cometer delitos.



¿Son los botnets un problema para Panamá?

¿Hay una infección grande de botnets en Panamá?

Si la hay, podemos detectarlos?

Introducción

- Justificación del Proyecto

2012.07.18

GRUM, WORLD'S THIRD-LARGEST BOTNET, KNOCKED DOWN

Tool to plot ips on a map based on geo location

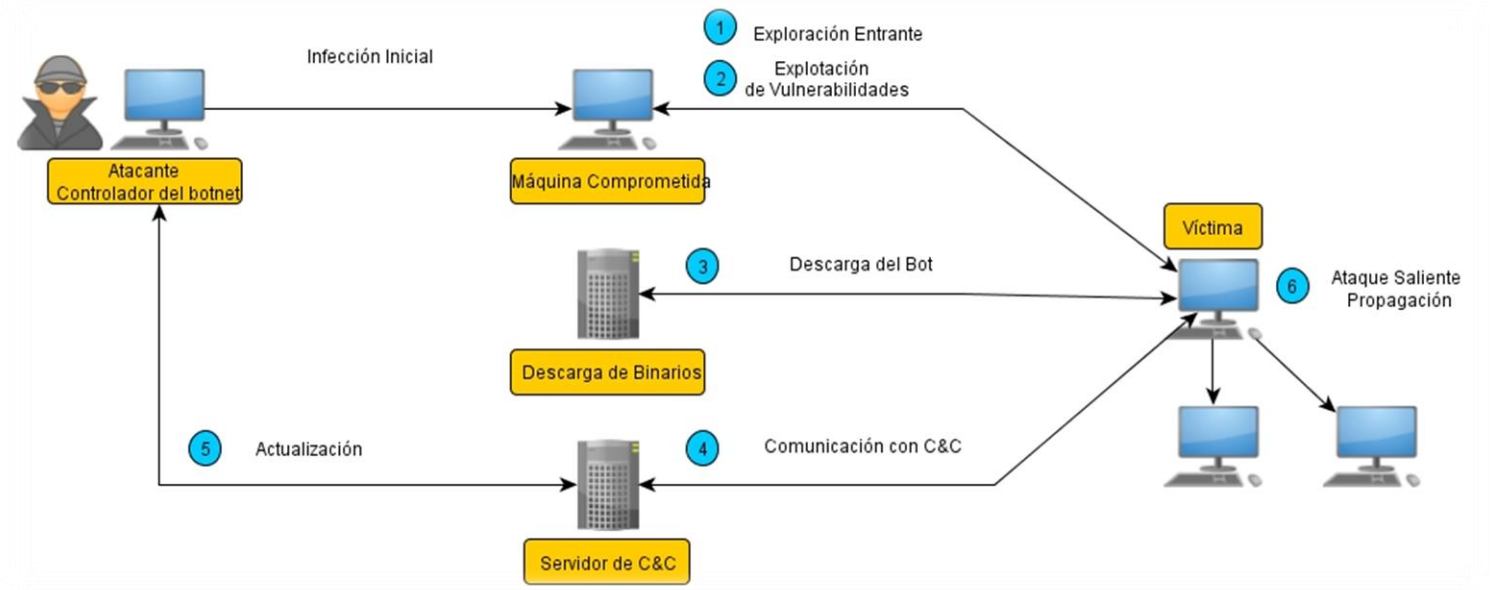
Route Details

IP	City	Country	Longitude	Latitude	Partial Distance(km)	Total Distance(km)
190.123.46.91	-	PANAMA	-79.533	8.967	-	0
190.123.46.92	-	PANAMA	-79.533	8.967	-	0
91.239.24.251	-	UNITED KINGDOM	-4.48211	54.167	8229	8229
94.102.51.226	AMSTERDAM	NETHERLANDS	4.917	52.35	656	8885
94.102.51.227	AMSTERDAM	NETHERLANDS	4.917	52.35	-	8885
94.102.51.228	AMSTERDAM	NETHERLANDS	4.917	52.35	-	8885
94.102.51.229	AMSTERDAM	NETHERLANDS	4.917	52.35	-	8885
94.102.51.230	AMSTERDAM	NETHERLANDS	4.917	52.35	-	8885

Fuente: http://blog.fireeye.com/research/2012/07/killing-the-beast-part-5.html

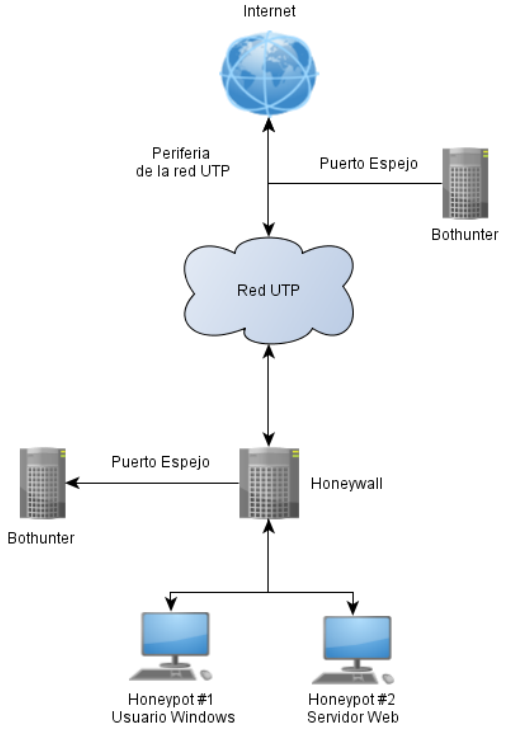
Marco Teórico

- Botnet
  - Red de computadoras controladas remotamente por atacantes para lanzar ataques informáticos, usualmente sin el conocimiento de los dueños de las computadoras.
- Ciclo de Vida



Plataforma de Captura

1. Honeynet Universitario



- Honeywall
  - Consta de dos capas
    - Control de datos
    - Captura de datos
- Bothunter
- 2 honeypots de baja interacción
  - Honeypot #1: Dionaea
  - Honeypot #2: Glastopf

2. Honeypot: Red Residencial

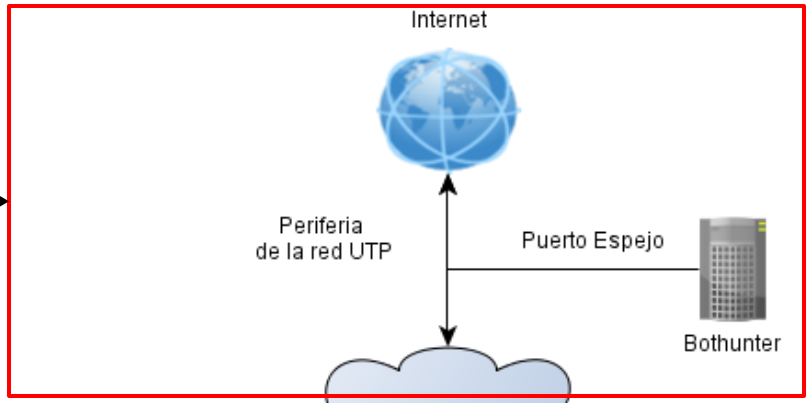
- 1 honeypot
  - Dionaea

Métricos de Evaluación

1. Familias de botnets
   - 1.1 Familias de botnets encontradas.
   - 1.2 Número de casos registrados por familia de botnet en un espacio determinado.
   - 1.3 Tipo de arquitectura del botnet.
2. Centros de distribución de malware
   - 2.1 Distribución geográfica
   - 2.2 Tipo de servicio que brindaban
   - 2.3 Proveedor de servicio al que pertenecen
3. Centros de C&C
   - 3.1 Distribución geográfica.
   - 3.2 Tipo de servicio que brindaban.
   - 3.3 Proveedor de servicio al que pertenecen.

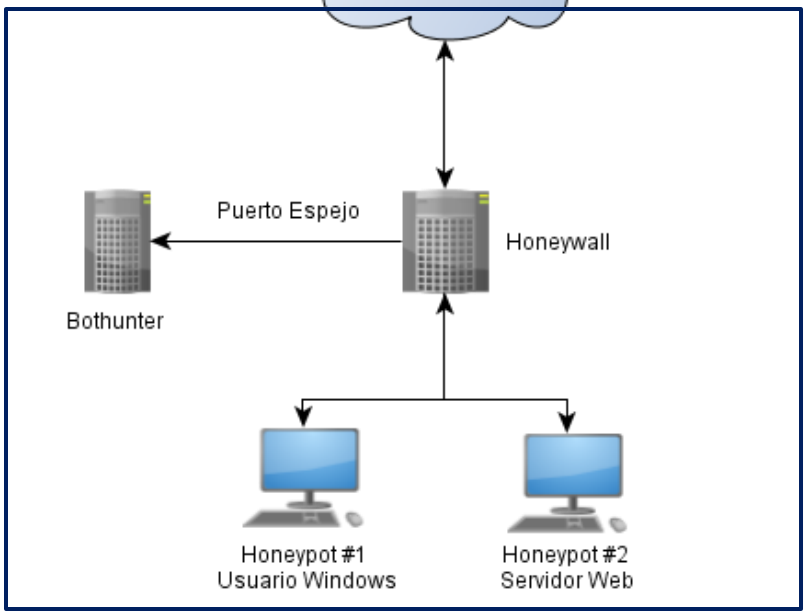
Resultados

Mayo a Julio de 2012 capturamos la actividad maliciosa en el campus universitario utilizando Bothunter.



En marzo de 2013 capturamos de igual forma la actividad maliciosa, esta vez utilizando un honeynet.

De igual forma durante este tiempo se decidió colocar un honeypot conectada a una red residencial.



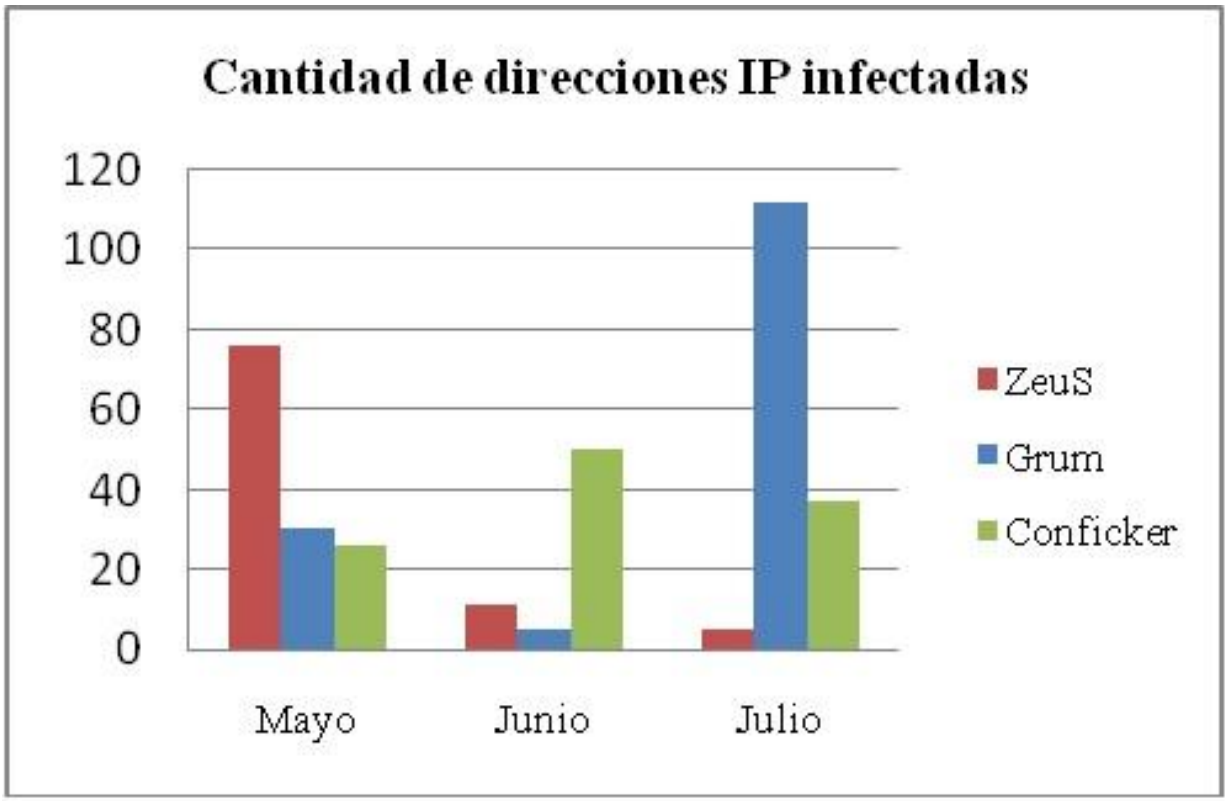
Resultados

- Bothunter
  - Resultados generales obtenidos con Bothunter

	Analizador Pasivo de Tráfico (Bothunter)
Período de Medición	Mayo a Julio de 2012
Fase I: Exploración Entrante	16
Fase 2: Explotación de Vulnerabilidades	0
Fases 3 y 5: Descarga de binario	15609
Fase 4: Comunicación del bot con C&C	5640
Fase 6: Ataque Saliente y Propagación	1357
Familias de bots identificados	Zeus, Conficker, Grum
Arquitectura de los C&C	Centralizada, Descentralizada

Resultados

- Bothunter
  - Cantidad de direcciones IP infectadas por las familias de botnets encontradas por Bothunter.



Resultados

- Honeynet Universitario
  - Principales Fuentes (Pais) de Ataques

País	Porcentaje
España	46.32%
Reservada	19.78%
China	12.14%
Estados Unidos	6.58%
Egipto	4.69%

  - Puertos más atacados incluyen aquellos de servicios Windows (139/TCP, 445/TCP, 3389/TCP) y bases de datos (1433/TCP, 3306/TCP)

Resultados

- Honeynet Universitario
  - Malware capturado
    - De las cinco muestras de binarios capturados, dos fueron reconocidas como binarios de bots.
      - Virut
      - Brambul
    - El método más popular para la descarga del bot fue la explotación de vulnerabilidades en servicio SMB.

URL de Descarga	Nombre
smb://190.254.16.50	Troj/Brambul-A
smb://175.45.63.226	PsExec
smb://80.171.153.215	Mal/Spy-Y
smb://175.45.63.224	Mal/HckPk-A
smb://82.224.120.125	Win32/Virut-Gen

Resultados

- Prueba Residencial
  - En total se recibieron 42351 ataques (1400 intentos diarios)
  - 95.75% de los ataques eran procedentes de máquinas en misma subred
  - Puertos más populares: 445/TCP y 139/TCP
  - 95% de binarios descargados eran Conficker.A
    - Resto eran distintas versiones de Zeus (Zbot)

País	Porcentaje
Panamá	95.75%
China	2.50%
Estados Unidos	0.96%
Chile	0.23%
Colombia	0.21%

Resultados

- Comparación

	Honeynet Universitario	Honeypot Residencial
Período de Medición	Marzo 2013	
Fases 1 y 2: Exploración Entrante y Explotación de Vulnerabilidades	2178	42351
Fases 3 y 5: Descarga del binario	5	7337
Puertos más utilizados	445/tcp, 139/tcp, 1433/tcp	445/tcp, 139/tcp
Cantidad de binarios únicos capturados	5	10
Familias de bots encontrados	Brambul, Virut	Conficker, Zeus
Arquitectura de los C&C	Centralizada	Centralizada, Descentralizada

Conclusiones

- A lo largo de un año de monitorización podemos concluir que la actividad de botnets en Panamá es real y dinámica
- Ocurre la ***regionalización*** de los botnets en Panamá
  - 95% de eventos clasificados como exploración entrante en la red residencial fueron originados de la misma red
  - Botnets como Zeus y Conficker utilizaban servidores de descarga ubicados en Panamá
  - Grum tenía servidores de C&C ubicados en Panamá

Conclusiones

- La capacidad de evolucionar del malware utilizada por los atacantes se ve reflejada en nuestro estudio
  - Al encontrar distintas versiones de Conficker operando en redes de distintos proveedores en diferentes períodos de tiempo ayudó a mostrar la resistencia que presentan ciertos botnets al mutar y utilizar nuevos vectores de infección
  - La actividad persistente de Conficker sugieren el escenario sobre el alto número de máquinas que reciben poco o ningún mantenimiento

Conclusiones

- Luego que Grum fuera desmantelado en julio de 2012 los ataques salientes registrados disminuyeron en un 97%
  - Método utilizado (sinkhole) para un caso como el de Panamá fue altamente efectivo

- El método de utilizar sinkholes para eliminar Conficker ha dejado bots sin C&C y todavía siguen apareciendo máquinas infectadas por este botnet

¡Muchas Gracias!

¿Preguntas?

Para mayor información:
http://argus.utp.ac.pa
Laboratorio de Redes y Seguridad Informática ARGUS