CAPÍTULO 2

DARKNETS Y TELESCOPIOS DE RED

En este capítulo se abarca el concepto, funcionamiento y esquemas de implementación de la tecnología Darknet. Presenta también el análisis a los modelos de detección para poder tener un mejor contexto sobre el diseño y potencial de la Darknet-UNAM implementada en la red académica más grande de México, RedUNAM.

2.1 INTRODUCCIÓN A LAS DARKNETS

Como se mencionó en un apartado anterior, una Darknet es un equipo o conjunto de ellos los cuales utilizan direcciones IP o segmentos de red que no están asignados a ningún servicio o dispositivo específico dentro de un entorno. Esto quiere decir que todas las direcciones IP de la Darknet están explícitamente reservadas para no ser utilizadas en algún equipo de la red de producción lo cual implica que solo los equipos o el equipo, denominado servidor Darknet, hará uso de estas direcciones para su funcionamiento.

2.2 TRÁFICO DE RED "NO ASIGNADO"

El tráfico no asignado corresponde al relacionado con todas las direcciones IP de la Darknet. En un entorno ideal este tráfico no debería existir, sin embargo, es importante mencionar que el hecho de que exista no necesariamente significa que haya actividad maliciosa en la red ya que puede deberse también a alguna anomalía en la configuración de algún equipo o dispositivo de enrutamiento.

Las direcciones IP no asignadas representan una inversión del espacio de direcciones para obtener un mecanismo alterno de detección de tráfico malicioso y anomalías, principalmente cuando se trata de direcciones IP homologadas. El número de direcciones destinadas a la Darknet es proporcional a la cantidad de eventos detectados y dependiendo de las características y capacidades de implementación, es también proporcional a la efectividad de la información obtenida.

En organizaciones grandes pueden existir Darknets internas, es decir, con direcciones IP de segmentos privados. Por la misma razón, este tipo de Darknets serán efectivas solamente dentro del entorno de la red, siendo incapaces de detectar tráfico malicioso externo y limitando su acción a detectar eventos originados desde equipos internos. En este caso, el tamaño de la Darknet juega un papel diferente ya que aunque literalmente se asignen miles o decenas de miles de direcciones IP privadas, el campo de acción continúa limitado a la detección de tráfico generado en la red interna y posiblemente hacia redes externas.

La asignación del tipo de direcciones IP privadas o públicas depende de los objetivos de la implementación de la Darknet, pero para fines de un telescopio de red, se deben utilizar direcciones homologadas con el objetivo de poder detectar eventos desde y hacia redes externas.

La figura 8 muestra un ejemplo de una Darknet en una red en producción.

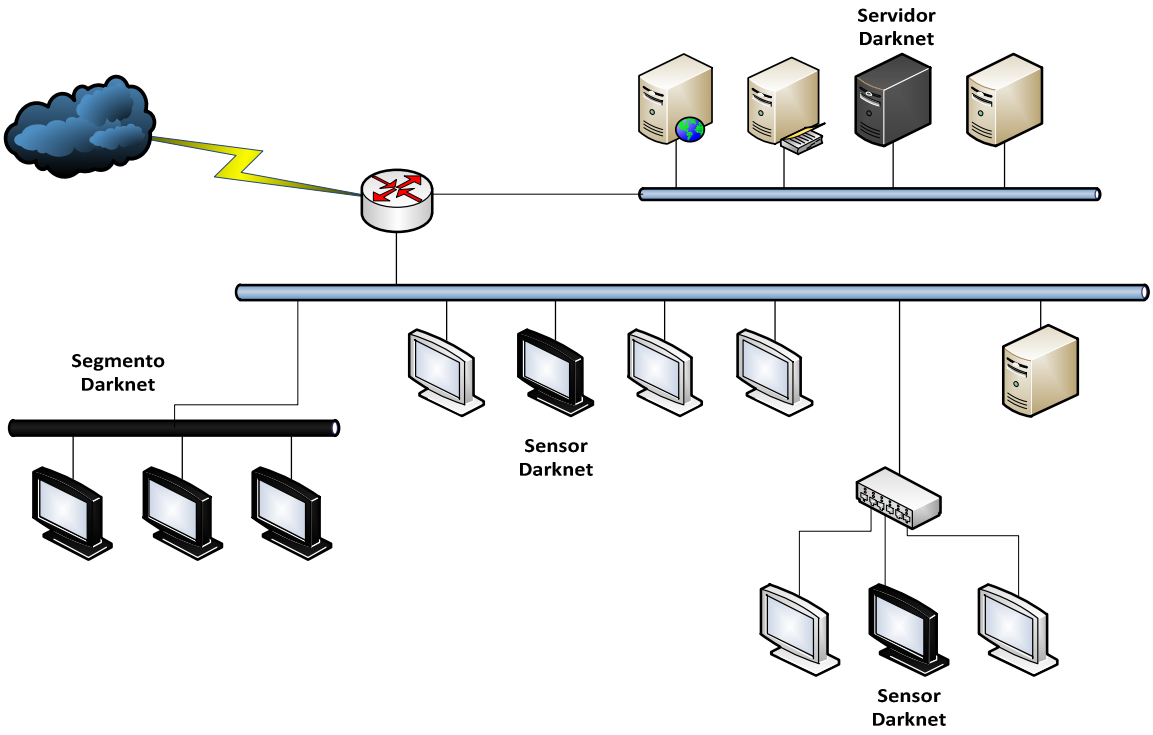

Figura 8. Esquema de una Darknet en una red en producción

2.3 CARACTERÍSTICAS DE UNA DARKNET

Independientemente de sus objetivos e implementación, de manera general una Darknet posee las siguientes características:

- Utiliza direcciones IP no asignadas.
- Todo el tráfico en la Darknet es potencialmente sospechoso.
- La cantidad de falsos positivos en la detección de anomalías es muy bajo.
- Puede detectar tráfico malicioso o anomalías en la configuración de dispositivos.
- Tiene las características para implementar tecnologías honeypot de manera muy conveniente y eficiente para obtener:
    - Muestras de tráfico malicioso
    - Muestras de malware
- Con la información obtenida, tiene la capacidad de generar información estadística importante sobre el tráfico de red.
- Inversión de direcciones IP de la red para su funcionamiento.

2.4 ESQUEMA DE FUNCIONAMIENTO Y HERRAMIENTAS RELACIONADAS

El funcionamiento específico de una Darknet depende de sus objetivos, pero el concepto general toma en cuenta aspectos como:

- Tecnologías implementadas
    - Honeypots, IDS, análisis de flujos, etc.
- Capacidad y complejidad de interacción
    - Simulación de servicios, equipos reales, etc.
- Capacidad y complejidad de análisis
- Campo de acción

El objetivo principal es que cada uno de los equipos o el servidor Darknet reciba e interactúe, bajo un ambiente controlado, con todo el tráfico dirigido hacia él. A partir de ese momento se puede identificar el origen, el tipo de tráfico, protocolo, puertos,

etc. y con esto saber si se trata de tráfico malicioso o alguna falla en la configuración de un equipo.

La clasificación de tráfico malicioso dependerá del mecanismo de detección, ya sea un equipo honeypot, un IDS u otro dispositivo, basándose en firmas o en el análisis del contenido del tráfico que dichas herramientas realicen. Mientras tanto, la detección de anomalías se puede identificar cuando se detectan patrones no necesariamente maliciosos y que corresponden a comportamientos como por ejemplo cuando un dispositivo de enrutamiento está mal configurado ocasionando que uno o varios equipos estén realizando conexiones recurrentes e innecesarias a otros equipos.

Ya sea que la Darknet esté compuesta por segmentos dedicados de direcciones IP o en equipos bien identificados de la red en producción, el tráfico no asignado es siempre detectable.

La figura 9 muestra un esquema básico de recopilación de información de cada sensor de la Darknet hacia un servidor dedicado.

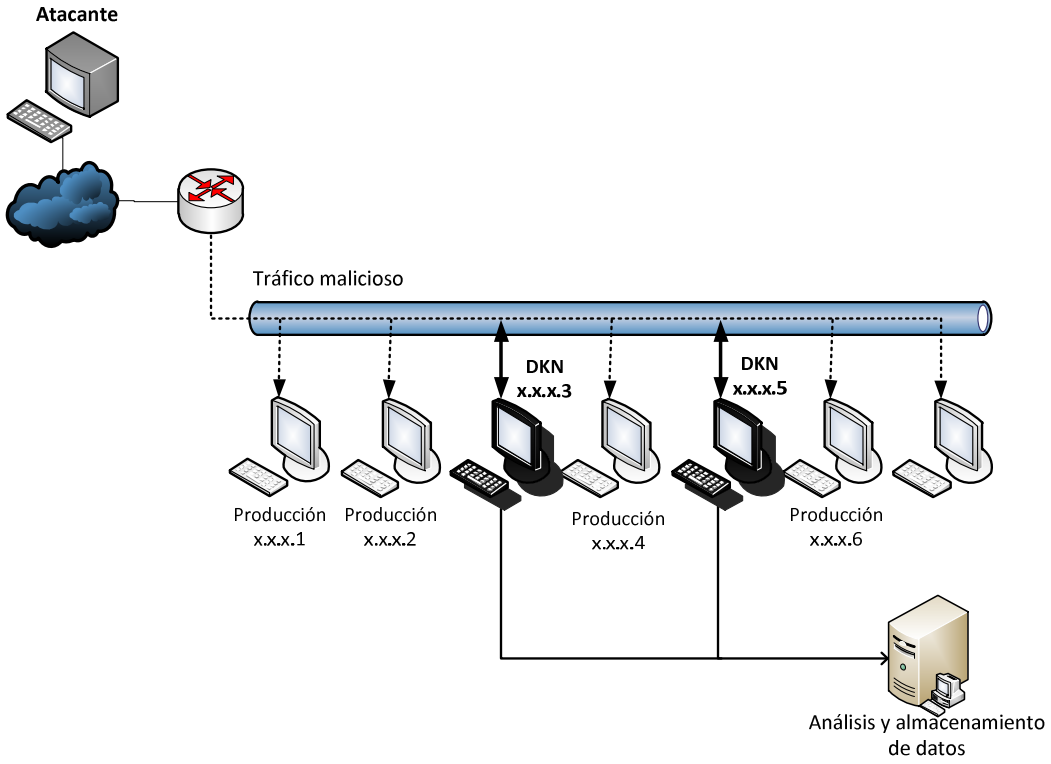

Figura 9. Esquema de funcionamiento de una Darknet.

Para que una Darknet pueda detectar algún ataque o cierto tipo de tráfico malicioso, debe forzosamente involucrar al menos a una de las direcciones IP de la misma. Esto quiere decir que si un ataque es dirigido a una IP fuera de la Darknet, entonces es muy probable que el ataque no pueda ser identificado. Afortunadamente, para los fines de detección, muchas amenazas en la red, principalmente las automatizadas como gusanos, bots, entre otros, presentan patrones en los cuales al intentar propagarse envían peticiones de conexión o algún tipo de escaneo al mayor número de equipos a su alcance. Esto revela las fuentes de los ataques puesto que en teoría el tráfico dirigido a equipos sin asignar no debería existir y en este ejemplo, el tráfico potencialmente sospechoso se convierte en tráfico malicioso identificado.

La gran ventaja de una Darknet es que al presentar bajos porcentajes de falsos positivos, los eventos identificados representan un estimado general de la actividad de tráfico malicioso que se recibe o circula en la red. Para obtener esta información pueden ser utilizadas diversas herramientas dependiendo del tipo de análisis, procesamiento y resultados esperados. La tabla 5 se muestra un ejemplo de tipos de análisis y herramientas utilizadas en la implementación de una Darknet.

Tabla 5. Tipos de análisis y herramientas utilizadas en una Darknet

TECNOLOGÍA	OBJETIVOS	EJEMPLOS
Honeypot	Simulación de servicios, captura de malware y control de tráfico	Dionaea, honeytrap, honeyd, kojoney, kippo, argos, honeybot, glastopf, google hack honeypot, honeywall, Hflow, etc.
IDS	Detección de tráfico malicioso mediante	Snort, Sguil, BASE, Suricata, Ossec HIDS, Prelude Hybrid IDS, Aide
Análisis de flujos	Análisis de flujos y generación de estadísticas de tráfico	Argus, Netflow, Hflow
Análisis de tráfico y protocolos	Análisis del tráfico de red: paquetes, protocolos, aplicaciones, etc.	Tcpdump, Wireshark, Tshark, Snort, Windump, ntop, etc.
Análisis de log	Análisis de logs de aplicaciones y sistema	Scripting perl, python, shell UNIX, Splunk, Logstash, etc.

Implementando alguna de estas tecnologías o combinaciones de ellas, se pueden detectar actividades como:

- Escaneos
- Propagación de gusanos, bots, virus
- Ataques de fuerza bruta
- Ataques específicos que utilicen técnicas de spoofing
- Fallas en la configuración de dispositivos
- Identificación de patrones de botnets o redes P2P
- Patrones anormales de tráfico
- Nuevas tendencias de ataques
- Entre otros

2.5 ANÁLISIS DEL MODELO DE DETECCIÓN EN SEGMENTOS DARKNET

Es muy importante hacer un análisis del modelo de detección para poder estimar de manera general la cantidad de tráfico esperado y los tiempos de captura, verificación, y almacenamiento de datos.

Actualmente, IPv4 (Internet Protocol versión 4) es la tecnología de direccionamiento de red desplegada en la mayoría de los dispositivos en el mundo. Es un protocolo de comunicación que permite un direccionamiento único de 32 bits para cada equipo dentro de la red. Esto quiere decir que el espacio de de asignación equivale a 2^{32}, lo cual resulta en 4.294.967.296 direcciones únicas.

Para poder identificar grupos de direcciones o segmentos, comúnmente se utilizan notaciones como /8, /16, /24, etc. refiriéndose al número de bits fuera de los 32. Por ejemplo, /8 hace referencia a un rango de 2^{24} direcciones que comparten los primeros 8 bits de la dirección. Así, /16 corresponde a un grupo de 2^{16} direcciones con los primero 16 bits comunes y /24 a 2^{8} direcciones compartiendo los primeros 24 bits. El caso de /32 hace referencia a una dirección IP única.

En el contexto de los telescopios de seguridad, estas notaciones son importantes ya que al referirse a bloques de red permiten hacer un cálculo estimado de la probabilidad de que un host dentro del espacio de monitoreo sea seleccionado como destino de alguna conexión por algún equipo en Internet. Si a esto se le agrega lo que la definición de Darknet marca sobre la naturaleza del tráfico en segmentos no utilizados, entonces dicha probabilidad se refiere a la recepción de tráfico de red potencialmente anómalo o malicioso.

La probabilidad *p* está dada por la cantidad de direcciones en el espacio de monitoreo de la Darknet entre la cantidad del espacio total de direcciones. Entonces, para IPv4 la probabilidad de detección en un segmento /x está dada por la ecuación:

$$P_x = \frac{2^{32-x}}{2^{32}} \qquad \text{o bien} \qquad P_x = \frac{1}{2^x}$$

Esto quiere decir que para un segmento /8, la probabilidad equivale a:

$$P_8 = \frac{1}{2^8} = \frac{1}{256} \qquad \text{o bien} \qquad P_8 = \frac{2^{24}}{2^{32}} = \frac{1}{2^8} = \frac{1}{256}$$

Y para /16 y /24 se tiene una probabilidad respectivamente de:

$$P_{16} = \frac{1}{2^{16}} = \frac{1}{65536}$$

$$P_{24} = \frac{1}{2^{24}} = \frac{1}{16777216}$$

De manera general, $P_x = \frac{1}{2^x}$ puede ser aplicada a cualquier otro espacio de direcciones, tal es el caso de IPv6 el cual maneja 128 bits.

2.5.1 TIEMPOS DE DETECCIÓN

Las Darknet son útiles para observar eventos aleatorios y espontáneos entre equipos. La medición del tiempo de detección es útil para poder establecer la duración mínima de espera para observar un evento según el tamaño de la misma. Algunas amenazas,

como los gusanos, intentan propagarse a todos los hosts posibles mientras que otros se propagan a rangos y ritmos específicos. Haciendo cálculos estimados de esta duración tomando como base el rango de objetivos en la Darknet (IP's alcanzadas), se puede hacer también un estimado de su efectividad.

Cuando un host toma como objetivo una dirección IP uniformemente aleatoria en todo un espacio de monitoreo, la probabilidad de detección en una dirección única está basada en una *distribución geométrica*. Una Darknet puede visualizar parte de este espacio, entonces, esta porción denominada *p*, se refiere a la probabilidad de que un paquete de red alcance una dirección dentro de ella. Si el host envía múltiples paquetes, entonces el número de paquetes vistos en el espacio de la Darknet está descrito por una *distribución binomial* con un parámetro *p*.

2.5.2 DETECCIÓN EN EQUIPOS ÚNICOS

Se asume que cada dirección asignada a la Darknet corresponde a un equipo independiente, entonces cuando un host genera múltiples paquetes, cada paquete tiene p posibilidades de alcanzar a la Darknet, y por lo tanto que la actividad sea detectada. Aplicando un análisis matemático, cada host objetivo seleccionado por el host fuente es una prueba de Bernoulli[42].

Considerando el número de paquetes generado por un host como el producto de la frecuencia con que los paquetes son enviados, *r*, y el tiempo T transcurrido., entonces la probabilidad de que al menos un paquete sea visto en la Darknet en un tiempo T está dada por la ecuación $P(t \leq T) = 1 - (1 - p)^{rT}$, la cual corresponde a una distribución geométrica. Su planteamiento se justifica en que corresponde a la distribución de probabilidad del número X del ensayo de Bernoulli necesaria para obtener un éxito contenido en un conjunto de pruebas, interpretando esto, la prueba corresponde al envío del paquete y el éxito a la recepción de la conexión en una IP dentro de la Darknet.

Desarrollando la expresión se tiene que:

$$T = \frac{-1}{rlog_{\frac{1}{1-P(t\leq T)}}(1-p)} = \frac{\log\left[1-P(t\leq T)\right]}{rlog(1-p)} = \frac{\log(Z)}{rlog(1-p)}$$

Así, la ecuación

$$T = \frac{-1}{rlog_{\frac{1}{Z}}(1-p)}$$

representa el tiempo T antes de observar al menos un paquete de un determinado evento con probabilidad Z (para Z=1-P(t≤T)). Entonces, la probabilidad corresponde a observar al menos un paquete con un objetivo determinado a una tasa de *r* pruebas por unidad de tiempo durante un lapso T, con lo cual podemos inferir un claro impacto según el tamaño del espacio de monitoreo dado el posible crecimiento exponencial entre los diferentes tipos de espacio de monitoreo (/8, /16, /24, etc.)

Con lo anterior, el número de paquetes esperados hasta que es visto el primero de ellos es:

$$\mu_N = \frac{1}{p}$$

con una varianza de:

$$\sigma^2{}_N = \frac{1-p}{p^2}$$

Ya que el interés es saber la tasa de transferencia de los paquetes y el intervalo de tiempo, se sustituye el número absoluto de paquetes enviados con rT obteniendo el tiempo transcurrido:

$$\mu_T = \frac{1}{rp}$$

Así, en este caso es más útil saber que el tiempo esperado de observar una amenaza proveniente de un equipo infectado con un gusano del estilo code-red en una red /8 es de 25.6 segundos, a diferencia de calcular que la Darknet tiene un 63.284% de

probabilidad de visualizar un ataque como ese en los mismos 25.6 segundos. Esto quiere decir que se pueden hacer ajustes según la probabilidad, por ejemplo, para observar un paquete del ejemplo anterior con una probabilidad del 99.999% se requieren aproximadamente 4.9 minutos.

La figura 10 muestra la relación tiempo-porcentaje de la probabilidad de observar al menos un paquete de un host que aleatoriamente selecciona un objetivo que esté dentro del espacio de monitoreo de Darknets de diferentes tamaños. En ella se puede observar la relación entre el tamaño del espacio de monitoreo y la efectividad de la Darknet para detectar determinados tipos de eventos. Esto a su vez denota la importancia que tiene la inversión de direcciones IP en este tipo de modelos de detección.

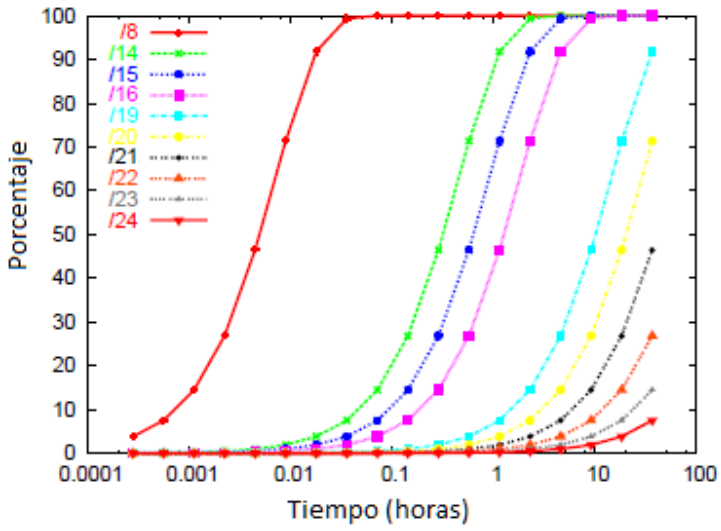

Figura 10. Relación tiempo-porcentaje para detección de un evento según el tamaño de una Darknet

Por su parte, la tabla 6 muestra una estadística de tiempos según el tamaño de una Darknet para un caso de envío de 10 paquetes por segundo provenientes de un equipo cualquiera. La primera columna indica la duración del evento para que la Darknet visualice el 95% de ellos, mientras que la última columna muestra la duración del evento para el cual la Darknet perdería el 95% de los mismos. Las columnas del centro demuestran la media y el promedio, es decir, los casos posiblemente más comunes. En este caso se debe tomar en cuenta que un evento en la práctica tiene una duración

limitada, por lo cual en la mayoría de las ocasiones será suficiente visualizar una mínima cantidad de paquetes para poder clasificarlo.

Tabla 6. Duración de eventos y porcentaje de detección según el tamaño de una Darknet para un caso específico.

Red	95%	Promedio	Media	5%
/8	1.3 min	25.6 seg	17.7 seg	1.31 seg
/14	1.4 hrs	27.3 min	18.9 min	1.4 min
/15	2.7 hrs	54.6 min	37.9 min	2.8 min
/16	5.5 hrs	1.82 hrs	1.26 hrs	5.6 min
/19	1.8 días	14.6 hrs	10.1 hrs	44.8 min
/20	3.6 días	29.1 hrs	20.8 hrs	1.49 hrs
/21	7.3 días	58.3 hrs	40.4 hrs	2.99 hrs
/22	14.5 días	4.85 días	3.36 hrs	5.98 hrs
/23	29.1 días	9.71 días	6.73 hrs	12.0 hrs
/24	58.2 días	19.4 días	13.5 días	23.9 hrs

2.5.3 DETECCIÓN DE MÚLTIPLES PAQUETES

En un esquema similar pero tomando en cuenta la detección de múltiples paquetes provenientes de una misma fuente, se pueden categorizar los tipos de eventos detectados y a su vez, disminuir la posibilidad de que se trate de un falso positivo y aumentando la posibilidad de identificar un potencial evento anómalo pudiendo ser malicioso como un ataque de negación de servicio. Esto es importante tomarlo en cuenta ya que la naturaleza de una Darknet también define la recepción de tráfico debido a fallas en la configuración (por ejemplo fallas en un router), o alguna anomalía que no se trate de una amenaza.

Dependiendo de las características de los eventos a ser monitoreados y propiamente de su diseño, el umbral k de paquetes que pueden ser seleccionados considerando la probabilidad de ver k o más paquetes de N transmitidos es:

$$P(vistos\ \geq k) = 1 - \sum_{y=0}^{k-1} \binom{N}{y} p^y (1-p)^{N-y}$$

La formula anterior se refiere a la definición de una distribución binomial, la cual mide el número de éxitos en una secuencia de n ensayos independientes de Bernoulli con una probabilidad fija p de ocurrencia del éxito entre los ensayos los cuales tienen dos posibles resultados, éxito(p) o fracaso(q=1-p). Interpretando esto, entonces el cálculo de la probabilidad de ver al menos 100 paquetes en un segmento /8 provenientes de un ataque DoS con una tasa de 500 paquetes por segundo y con una duración de 1 minuto está dada por:

N = 500pps * 60 sec = 30000 paquetes

K = 100 paquetes

p = 2^{-8}

$$P = 1 - \sum_{y=0}^{100-1} \binom{30000}{y} (2^{-8})^y (1-2^{-8})^{30000-y} = 95.2\%$$

En cambio, en una red /16:

N = 500pps * 60 sec = 30000 paquetes

K = 100 paquetes

p = 2^{-16}

$$P = 1 - \sum_{y=0}^{100-1} \binom{30000}{y} (2^{-8})^y (1-2^{-8})^{30000-y} = 6.7x10^{-195}$$

Se puede apreciar la variación considerable de la probabilidad según el tamaño del espacio de monitoreo dado el crecimiento exponencial de un segmento a otro de la red. En el Anexo 1 se muestra una comparativa de diferentes probabilidades para redes /8 y /16 haciendo variaciones en el número de paquetes enviados.

2.6 DARKNETS EN AMBIENTES ACADÉMICOS

Las redes académicas, principalmente de Universidades, representan un potencial campo de acción para la implementación de Darknets y honeynets. Esto se debe a que este tipo de ambientes posee características como:

- Altos anchos de banda desde y hacia Internet.
- Gran número de equipos utilizados.
- Muchos tipos de servicios, sistemas y arquitecturas utilizadas.
- Equipos con grandes capacidades de almacenamiento y procesamiento.
- Posible administración autónoma en cada área, dependencia, escuela, facultad, edificio, etc.
- Falta de restricciones en varias partes de la red.
- Existencia de tráfico de red inusual debido a proyectos de investigación.

Lo anterior también se complementa con que el principal objetivo de este tipo de implementación está enfocado a la investigación y desarrollo de nuevas tecnologías y herramientas en el campo.

Dependiendo de la infraestructura de la Darknet, siempre se debe tomar en cuenta que es necesario mantener una coordinación estrecha con los administradores de red o encargados de cada área. Esto es porque si se utilizan direcciones IP que ellos administran, es posible que al recibir y capturar tráfico malicioso se viole alguna política de seguridad y levante alertas de sistemas de monitoreo desplegados en la red.

En un documento [28] publicado por The Honeynet Project sobre Honeynets en Universidades, se mencionan algunas lecciones aprendidas, en este caso en The Georgia Institute of Technology (Georgia Tech). Tomando en cuenta que las características de una honeynet y una Darknet son similares, se puede hacer referencia a dichas lecciones:

1) Iniciar poco a poco: Si se desea implementar una honeynet en una organización grande, se debe iniciar con algo pequeño. Esto permitirá evaluar y entender cómo se analizarán los datos y desarrollar sistemas personalizados para ello.
2) Mantener buenas relaciones con los administradores de red: Esto es crítico puesto que son ellos quienes proporcionan la infraestructura lógica de IP's para realizar las tareas, además, en los casos en los que ellos no hayan detectado algún tipo de ataque, exploit o tráfico malicioso específico, quien implementa la honeynet (o Darknet en este caso), podría ser la primera persona que los notifique de ello.
3) Enfocarse en los ataques provenientes de la red de la organización: Este tipo de ataques son de los que más daño causan a las organizaciones. Debe informarse inmediatamente a los administradores sobre los equipos que hayan sido comprometidos dentro de la organización.
4) No publicar el rango de las direcciones IP de la honeynet (o Darknet).
5) No sobreestimar la cantidad de tiempo necesario para analizar los datos recopilados.
6) Para implementar una honeynet no se necesitan equipos con altas prestaciones de procesamiento o almacenamiento (aunque esto depende del esquema de implementación).

Definitivamente, el despliegue tanto de honeynets como Darknets en ambientes académicos traen grandes beneficios y sobre todo permiten obtener y analizar información muy útil sobre detección de tráfico malicioso.

2.7 DARKNETS A GRAN ESCALA

A nivel global existen varios proyectos de diferentes tamaños y características, algunos más complejos que otros, sin embargo persiguen un concepto común: el monitoreo de la actividad de tráfico de red. Estos proyectos ofrecen distintos tipos de información siendo una de sus principales diferencias el tamaño y la forma de recopilación y procesamiento de los datos. Algunos de ellos, debido a su tamaño y capacidad, se han convertido en referencias importantes para consultar la actividad del tráfico de red y las tendencias en Internet.

A continuación se menciona un panorama general sobre algunos de los proyectos de este tipo para poder hacer una comparativa en los modelos de detección y capacidades en general.

2.7.1 INTERNET MOTION SENSOR (IMS)

Es un proyecto desarrollado entre la firma de seguridad Arbor Networks y la Universidad de Michigan. Consiste en un sistema de monitoreo de las amenazas de Internet a nivel global cuyo objetivo es medir, clasificar y dar seguimiento a dichas amenazas. Posee una infraestructura distribuida de sensores ubicados en distintos lugares abarcando segmentos de red desde /25 hasta /8 en redes académicas, comerciales e ISP's y cuenta con una infraestructura de almacenamiento por jerarquías. Su funcionamiento se basa en diversas tecnologías de detección entre las que se encuentran honeypots, análisis de flujos, análisis de payloads, etc. La arquitectura general del proyecto IMS persigue tres objetivos:

- Mantener un nivel de interacción capaz de identificar tráfico del mismo servicio
- Clasificación de las amenazas emergentes
- Visibilidad de Internet más allá de las fronteras geográficas u operativas

Los sensores desplegados están clasificados en “dark IP” (segmentos de la Darknet) y “topology” (segmentos dentro de una topología asignada). La figura 11 muestra la infraestructura del IMS.

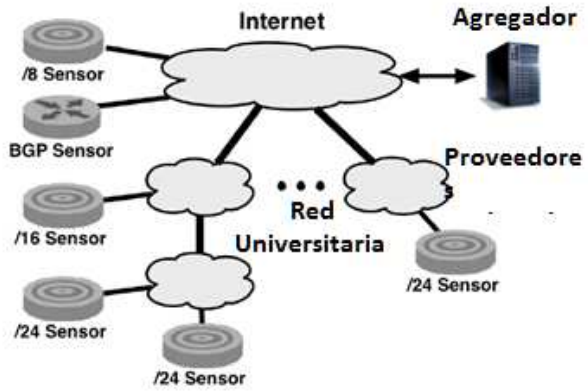

Figura 11. Infraestructura del Internet Motion Sensor

Con esta infraestructura, es capaz de detectar y analizar amenazas como gusanos, escaneos, ataques DoS, entre otros, con la característica de hacerlo en tiempo-real.

La figura 12 muestra el procedimiento de análisis y manejo de información del IMS.

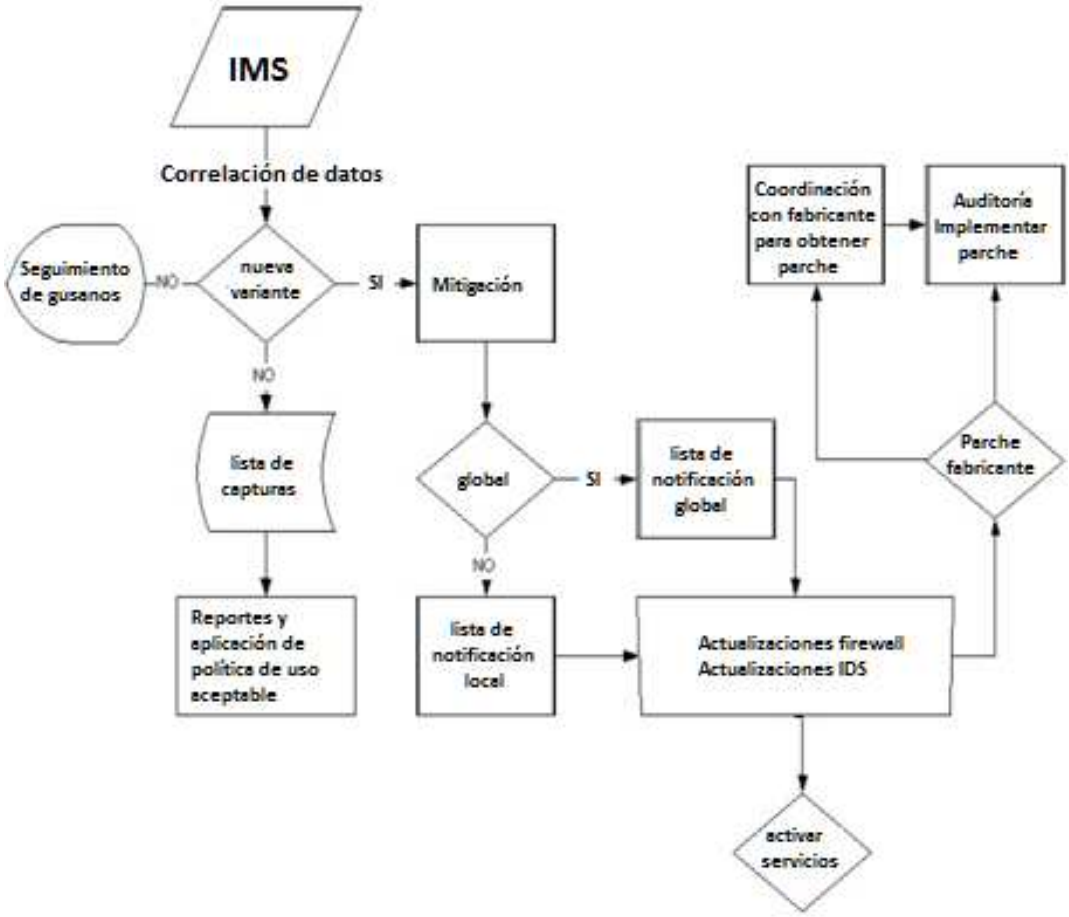

Figura 12. Esquema de funcionamiento del IMS

2.7.2 CAIDA

Cooperative Association for Internet Data Analysis. Es una asociación cuyos objetivos son:

- Medir y entender el tráfico en Internet
- Desarrollar herramientas para la medición y análisis
- Recopilar y proveer datos sobre Internet de diferentes rubros: seguridad, dns, routing, topologías, etc.
- Visualización de red

Posee una de las infraestructuras más grandes a nivel global para la medición y análisis del tráfico en Internet. Consta del llamado "Archipelago" o "Ark" el cual en su última actualización en Febrero de 2010 tenía desplegada 41 monitores en 25 países. La tabla 7 y la figura 13 muestran la distribución por continente y su ubicación geográfica respectivamente.

Tabla 7. Infraestructura de "Archipelago" de CAIDA

Por continente	Por organización
17 Norteamérica	21 Académicas
14 Europa	10 Redes de investigación
5 Asia	5 Infraestructuras de red
2 Oceanía	4 Redes comerciales
2 Sudamérica	1 Red comunitaria
1 Africa	

Figura 13. Monitores del Archipelago de CAIDA

Uno de los proyectos de CAIDA es el UCSD Network Telescope, el cual consiste en una Darknet con un potencial de una red /8, esto quiere decir aproximadamente 16 millones de direcciones IP. Este Telescopio tiene como objetivos la detección de ataques de negación de servicios, propagación de gusanos, y detección general de tráfico malicioso generado por agentes automatizados.

2.7.3 TEAM CYMRU, THE DARKNET PROJECT

Team Cymru es una organización especializada en la investigación sobre seguridad en Internet. Uno de sus proyectos es "The Darknet Project", el cual al igual que sus similares, es capaz de identificar actividad maliciosa en Internet y a su vez generar estadísticas de tráfico para saber qué es lo que pasa en la red. Utiliza tecnologías como el análisis de flujos y el análisis de tráfico de red.

La infraestructura de este proyecto consta de 8 Darknets desplegadas en diferentes zonas geográficas tal como se muestra en la tabla 8.

Tabla 8. Darknets de "The DArknet Project"

Darknet	**Espacio de IP's**
Darknet 1 (ARIN/US)	6 Redes /24 (1,536)
Darknet 2 (ARIN/US)	4 Redes /16 (262,144)
Darknet 3 (ARIN/US)	10 Redes /24 (2,560)
Darknet 4 (ARIN/CA)	1 Red /16 (65,536)
Darknet 5 (ARIN/US)	1 Red /17 (32,768)
Darknet 6 (ARIN/US)	1 Red /24 (256)
Darknet 7 (RIPENCC/NL)	2 Redes /16 (131,072)
Darknet 8 (ARIN/US)	2 Redes /16 (131,072)
	Total = 626,944 DARK IP

A partir de herramientas de monitoreo como RRDTool, es posible monitorear la actividad general de las Darknets, sin embargo, gracias a herramientas de análisis de flujos como Argus, se puede monitorear la actividad específica de algún puerto, IP, protocolo, etc. como el ejemplo de la figura 14, el cual corresponde al monitor de actividad de las darknets de Team Cymru.

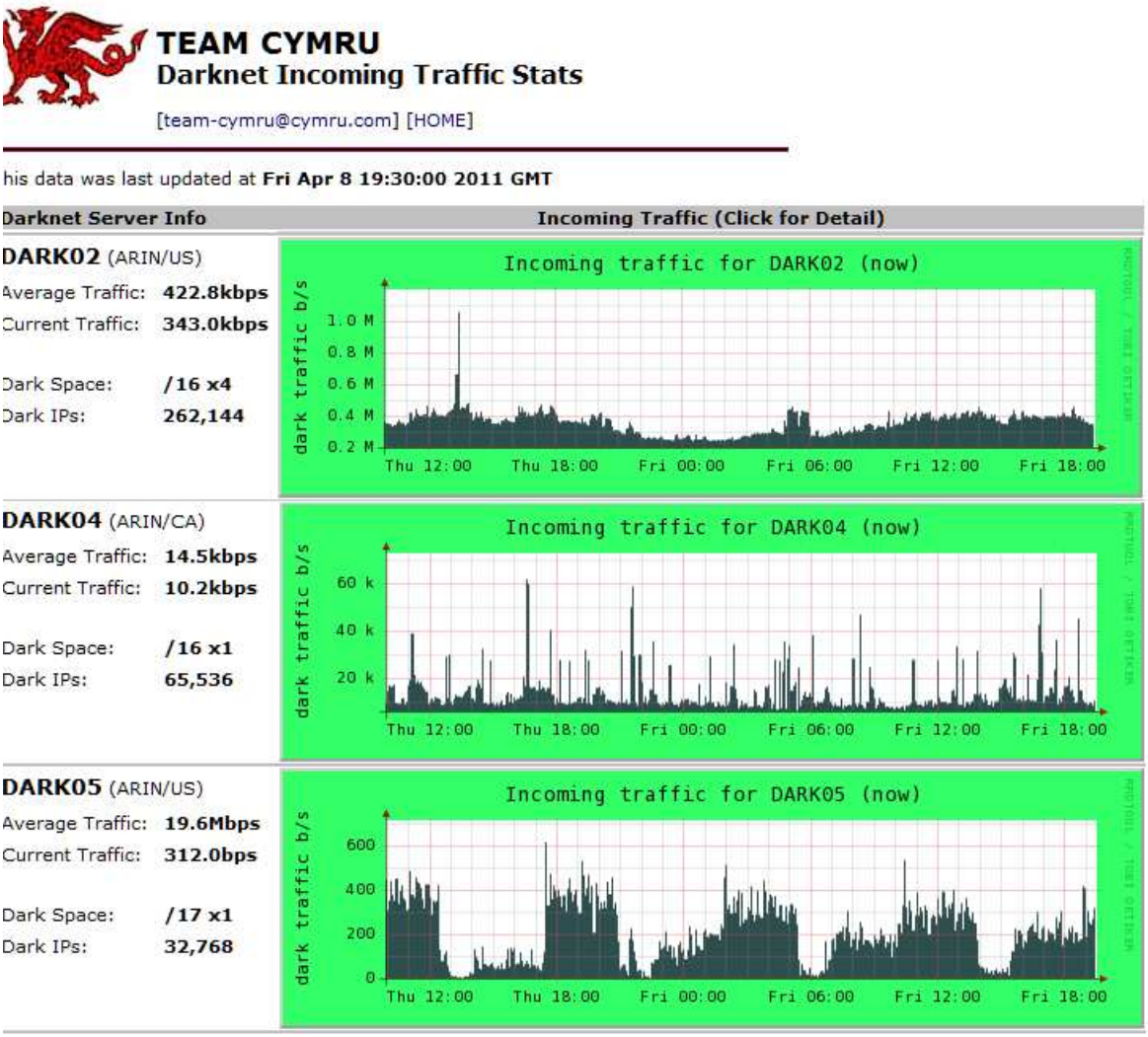

Figura 14. Actividad de las Darknet de The Darknet Project de Team-Cymru

En la página de Team-Cymru [53] sobre su proyecto The Darknet Project, se proporciona un manual práctico[9] de cómo implementar una Darknet.

2.7.4 iSINK (INTERNET SINK)

Es un proyecto desarrollado en la Universidad de Wisconsin el cual consiste en una arquitectura altamente escalable para la medición, monitoreo y análisis automatizado de trafico malicioso. iSink es un sistema basado en tecnologías honeypot

[9] http://www.team-cymru.org/Services/Darknets.html

implementado sobre una arquitectura Darknet, cuya capacidad de emulación de respuestas permite monitorear y clasificar ataques a lo largo de grandes subredes. De acuerdo a su equipo desarrollador en The Wisconsin Advanced Internet Laboratory (WAIL)[10] de la Universidad de Wisconsin-Madison, este sistema implementa un protocolo para la generación de firmas NIDS de manera automatizada las cuales presuponen una baja probabilidad de falsos positivos comparable con algunos sistemas populares NIDS. Los objetivos de iSink son:

- Abordar el problema del diseño e implementación de un sistema de monitoreo para grandes segmentos de red.
- Crear un sistema altamente escalable con un nivel suficiente de interacción para poder detectar gusanos, ataques, fallas en la configuración, etc.

Las características de iSink son:

- Usa componentes activos y pasivos.
- Utilizar técnicas de muestreo en sus componentes para incrementar la escalabilidad.
- Potencial de aproximadamente 100,000 direcciones IP en una Darknet.

La figura 15 muestra la infraestructura de esta darknet.

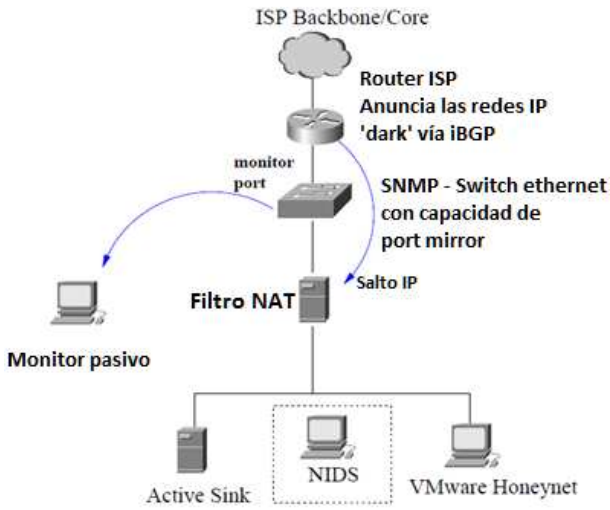

Figura 15. Esquema de conectividad de iSink

[10] http://wail.cs.wisc.edu/

La implementación de iSink consta de los siguientes módulos:

- Passive monitor
- Active Sink
- NAT filter
- Vmware honeynets
- NIDS

2.7.5 THE IUCC/IDC INTERNET TELESCOPE

Es un telescopio de red desarrollado por Israel InterUniversity Computation Center (IUCC). Básicamente permite el monitoreo de trafico sobre una Darknet la cual utiliza la técnica de backscatter[11] para la detección de ataques de IP spoofing. Su espacio de direcciones es un segmento de red /16. Los principales eventos detectados por este telescopio se muestran en la tabla 9.

Tabla 9. Estadísticas del telescopio de IUCC/IDC

Tipo de paquete	Porcentaje
Escaneo de puertos/equipos	92%
DDOS Backscatter	5%
Fallas de configuración	2%
Otros	1%

Es capaz de generar información estadística tomando como criterios el origen y el destino de los paquetes. Sin embargo, existen algunos ataques que no pueden ser vistos por este telescopio como los de bogon[12], ataques sin suplantación de IP y ataques de Botnets.

[11] Se refiere a las respuestas que un equipo devolvería a un equipo víctima de suplantación de IP. Si un atacante hace una suplantación de manera aleatoria, el ataque es visible debido a que el telescopio mandaría respuestas del tipo (SYN-ACK) a equipos aleatorios.

[12] Es un ataque que proviene de una dirección IP que no está en las tablas de ruteo de ningún dispositivo en Internet. Existe una lista definida por IANA de estas direcciones

2.7.6 *INTERNET BACKGROUND NOISE (IBN)*

Es un proyecto desarrollado por la organización SWITCH[13] que consiste en un sistema de monitoreo de tráfico de red basado en tecnologías Darknet. Todo el tráfico de las direcciones IP no utilizadas es redirigido a un servidor IBN el cual recopila y procesa la información. Tiene un potencial de aproximadamente tres segmentos /17 para monitoreo. Su principal objetivo es generar estadísticas según el tipo de protocolo, puertos destino, tipos de mensajes ICMP, etc. así como se aprecia en la figura 16.

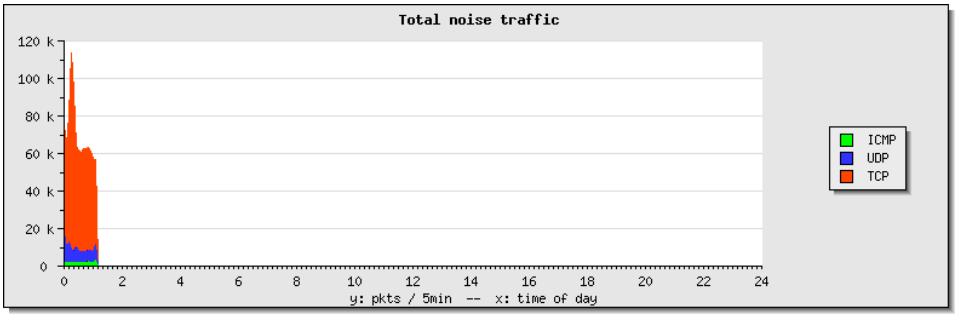

Figura 16. Estadísticas generadas por IBN

2.7.7 *SHADOWSERVER*

Shadowserver Foundation es un grupo de especialistas en seguridad que se encargan de recopilar, dar seguimiento y reportar malware, actividad de botnets y fraudes electrónicos. Su misión principal es mejorar la seguridad en Internet mediante la concientización de la presencia de servidores comprometidos, atacantes maliciosos y la propagación de malware. Sus tareas fundamentales se basan en:

- Captura y recepción de software malicioso o información relacionada de dispositivos comprometidos.
- Análisis de malware mediante sandbox, desensamblado y otras técnicas.
- Monitorear y reportar atacantes maliciosos.
- Seguimiento y reporte de actividad de botnets.
- Diseminación de información de *cyber-amenazas.*
- Coordinación en respuesta a incidentes.

---

http://www.team-cymru.org/Services/Bogons/

[13] http://www.switch.ch/about/

Su estructura de funcionamiento se representa en la figura 17.

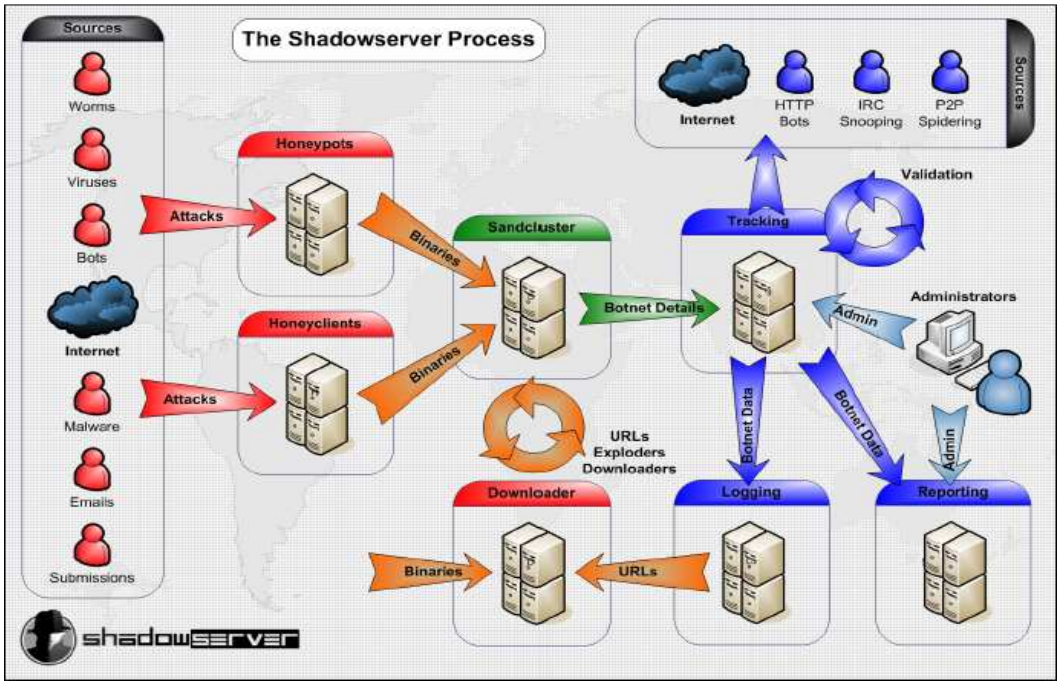

Figura 17. Proceso de manejo de información de Shadowserver Foundation

El UNAM-CERT tiene un convenio con Shadowserver para intercambio de información sobre actividad maliciosa detectada la cual se utiliza específicamente para complementar el proceso de atención a incidentes de equipos de RedUNAM.