
DISC
2009
MÉXICO
DÍA INTERNACIONAL DE LA SEGURIDAD EN CÓMPUTO

DISC 2009 MÉXICO
Día Internacional de la Seguridad en Cómputo

Telescopio de seguridad UNAM-CERT

Ing. José Roberto Sánchez Soledad
Ing. Javier Ulises Santillán Arenas

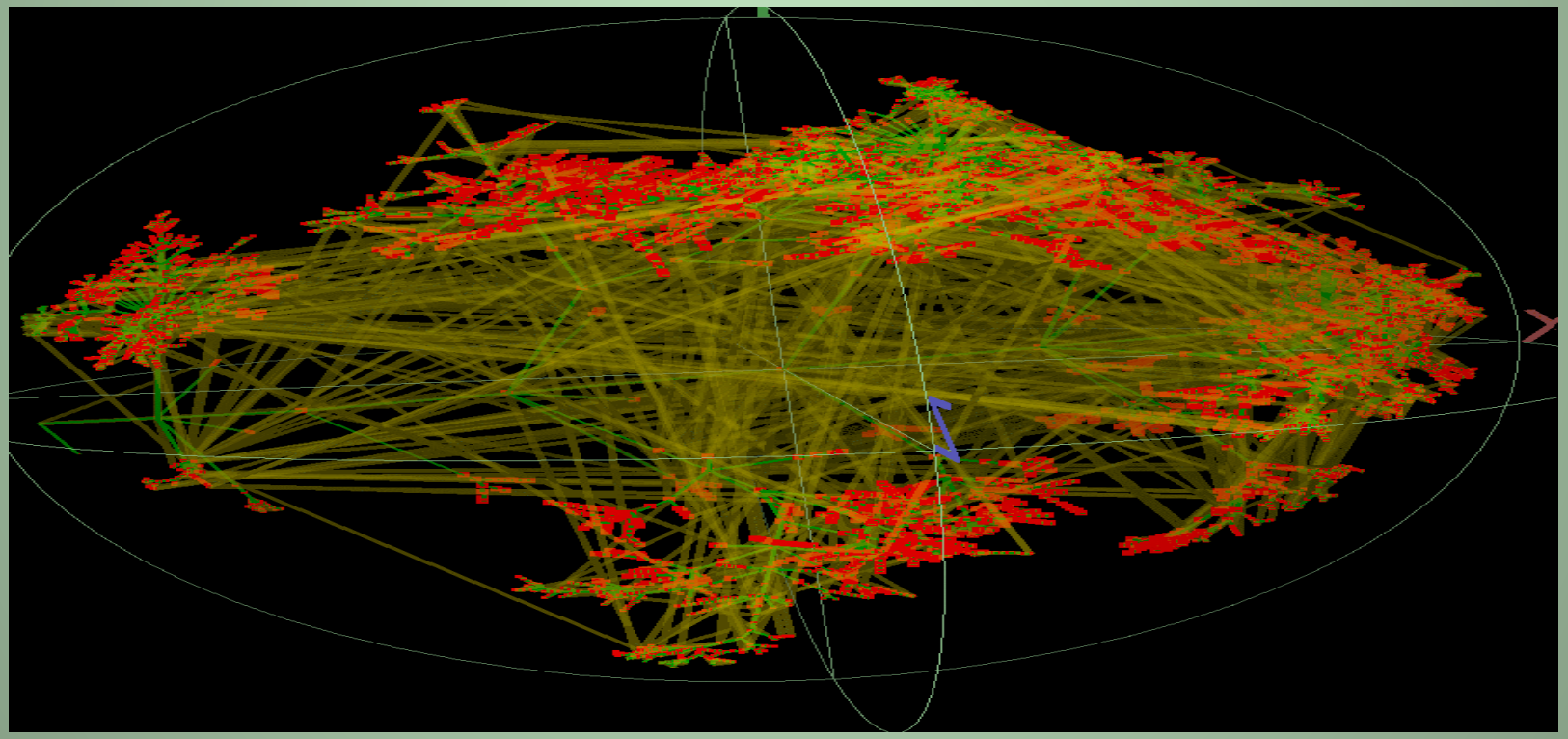
¿Qué es un telescopio?

- Instrumento óptico que permite ver objetos lejanos con mucho más detalle que a simple vista.

¿Cómo aplicar este concepto a la seguridad?

- El internet es una red de datos global.
- Imposible monitorear “todo” el tráfico de red.
- Indispensable la creación de un telescopio que nos permita observar comportamientos, tendencias, y nuevos ataques.

Tráfico en Internet



Fuente: CAIDA

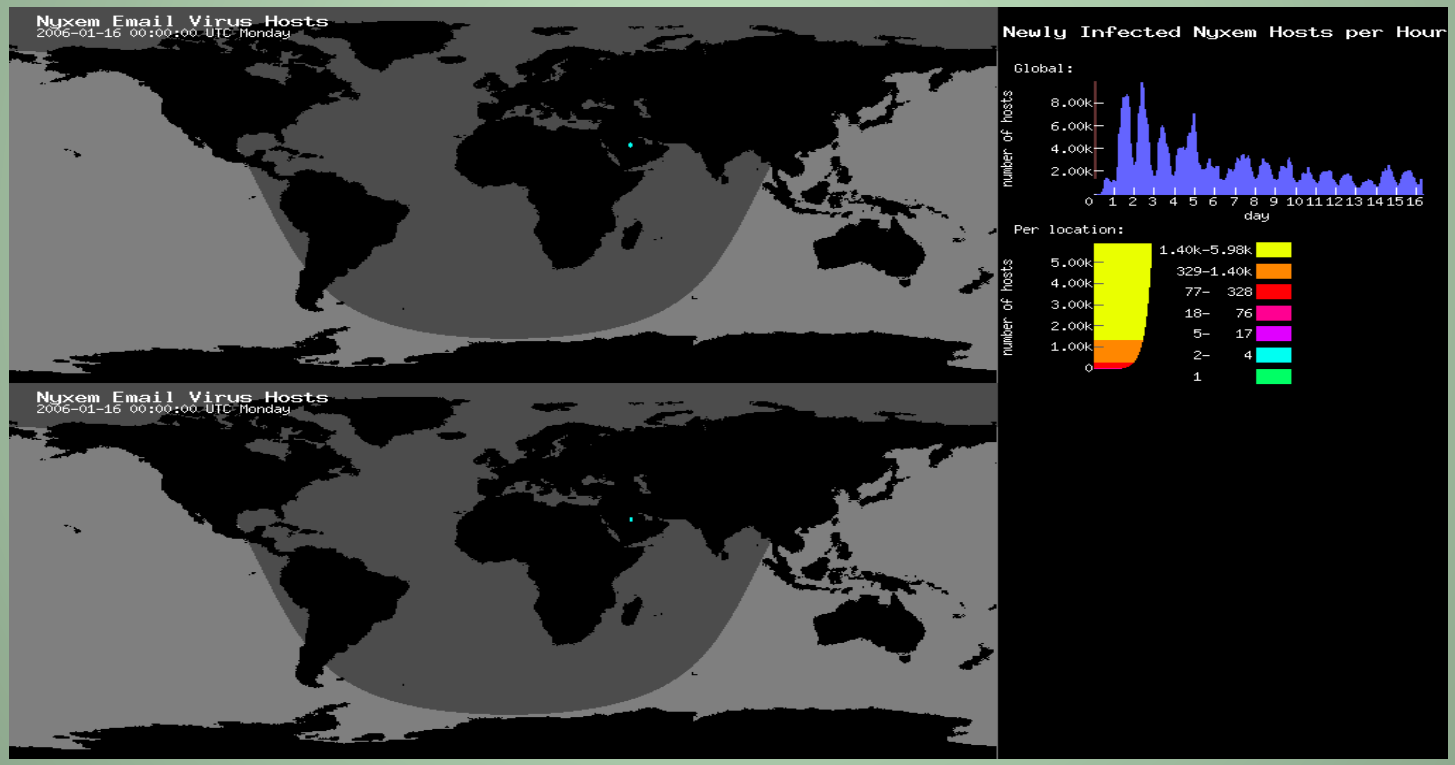
¿Importancia de tener un Telescopio?

- Mediante el telescopio de seguridad, es posible contar con una herramienta que permita identificar tráfico malicioso.
- Tomar acciones que permitan mitigar el tráfico malicioso desde y hacia nuestras redes.

Resultados obtenidos

- Todos los datos son en tiempo real.
- Datos estadísticos de tráfico maliciosos.
- Reportes automatizados de dependencias afectadas

Resultados a obtener



Fuente: CAIDA

¿Cómo se conforma el telescopio?

- Tomando un muestreo del tráfico de una red, nuestra visión es general pero limitada.
- Si la muestra de tráfico a analizar es más amplia, la efectividad de la información obtenida será mayor.

¿Cómo se conforma el telescopio?

- Sensores de tráfico malicioso (PSTM).
- Sensores de Correo Spam
- Sinkhole
- Sensores de Phishing
- Intercambio de información con otras dependencias, cymru, certs, etc.
- Darknet (la más grande de Latinoamérica)

¿Cómo se conforma el telescopio?

- Los sensores del PSTM son equipos que se colocan en el perímetro de redes de cómputo.
- Similares a sistemas de detección de intrusos (IDS), con la funcionalidad de capturar malware que circula por la red
- Esta información es enviada a un servidor de centralizado en el UNAM-CERT.

¿Cómo se conforma el telescopio?

- Contamos con 15 sensores de tráfico malicioso desplegados en 7 instituciones de educación superior a nivel nacional y en diversas dependencias de RedUNAM.

Plan de Sensores de Tráfico Malicioso - PSTM

- La convocatoria del PSTM está abierta a todas las dependencias pertenecientes a RedUNAM, IES del país que deseen colaborar.
- La administración se realiza de forma compartida por el DSC/UNAM-CERT y las entidades participantes.

Beneficios de Pertenecer al PSTM

- Monitoreo perimetral de las redes.
- Información procesada de alertas de seguridad locales.
- Intercambio de la información del telescopio de seguridad con la entidad participante.

¿Cómo se conforma el telescopio?

- Un sensor de Tráfico Spam, en el cual se reciben aproximadamente 23,000 correos spam por Hora.

¿Cómo se conforma el telescopio?

- En colaboración con el NOC de RedUNAM, se implementa un Sinkhole el cual es un equipo especializado para mitigar y analizar el tráfico identificado como malicioso.

Tipos de eventos que son monitoreados

- Gusanos
- Virus
- Escaneos
- Ataques de negación de servicio (DoS)
- Tráfico Spam
- Phishing scam

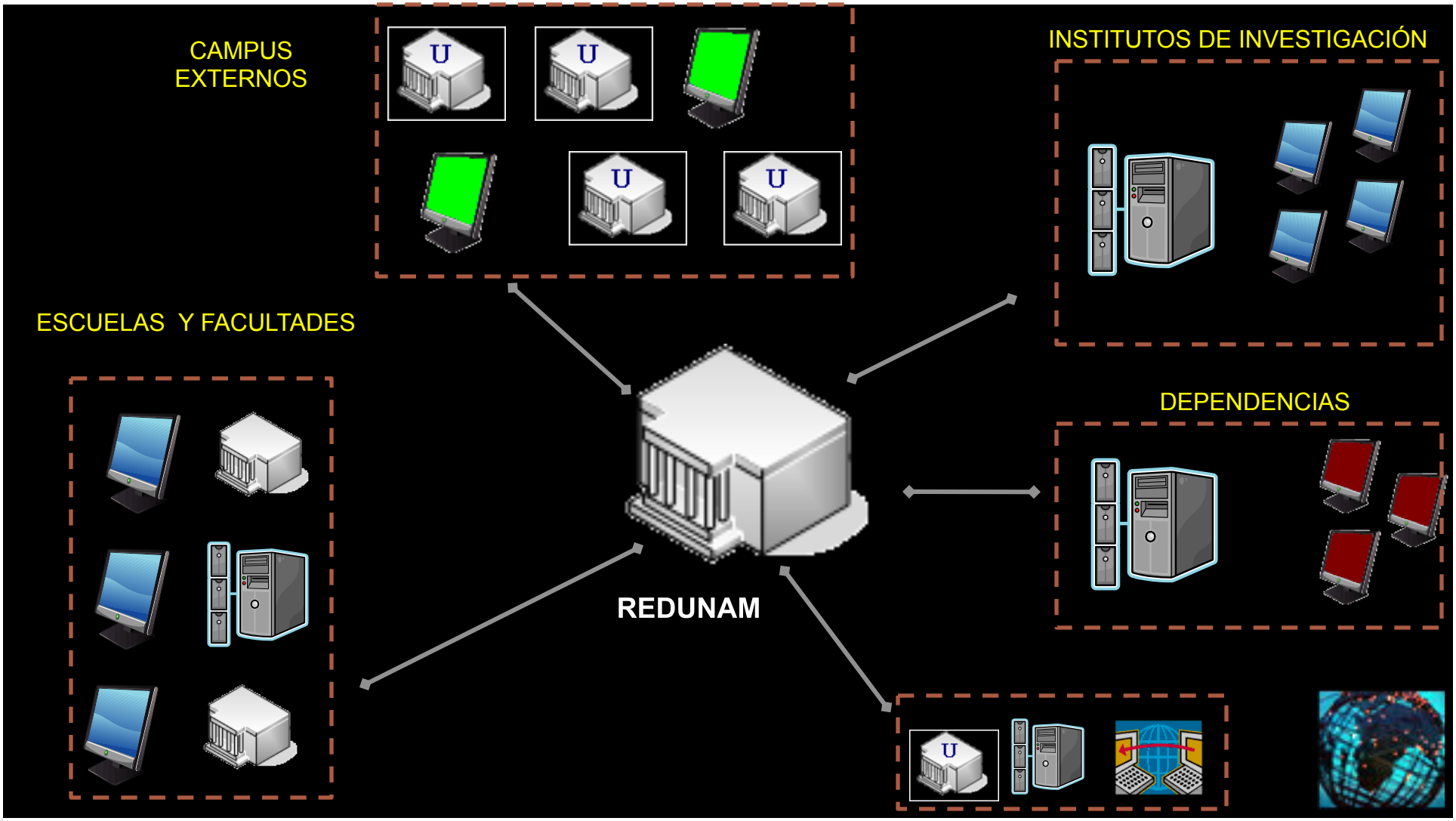
RECOPILANDO INFORMACIÓN

La recopilación de información es esencial para la obtención de resultados.

El correcto análisis e interpretación de la misma permite un mejor aprovechamiento de los resultados y generación de información útil.

Sistema centralizado UNAM-CERT

- Equipo capaz de procesar toda la información, recolectada por los sensores.
- Clasifica el Malware y se envía para su análisis al proyecto Malware del DSC.
- Se procesan los datos de internet y se envían reportes automáticos.



CAMPO DE ACCIÓN → RedUNAM

- Escuelas y Facultades
- Campus Externos
- Institutos de Investigación
- Dependencias Universitarias

DARKNET A GRAN ESCALA

Una Darknet es una red formada por equipos con direcciones IP “no asignadas”. Tiene el objetivo de detectar patrones anormales en la red.

Tratamos como una dirección IP “no asignada” a aquellas direcciones IP reservadas para su no utilización dentro de una red, es decir, no tienen un servicio ni equipo específico.

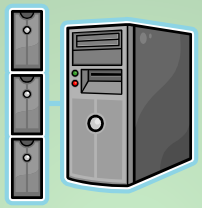
DARKNET A GRAN ESCALA

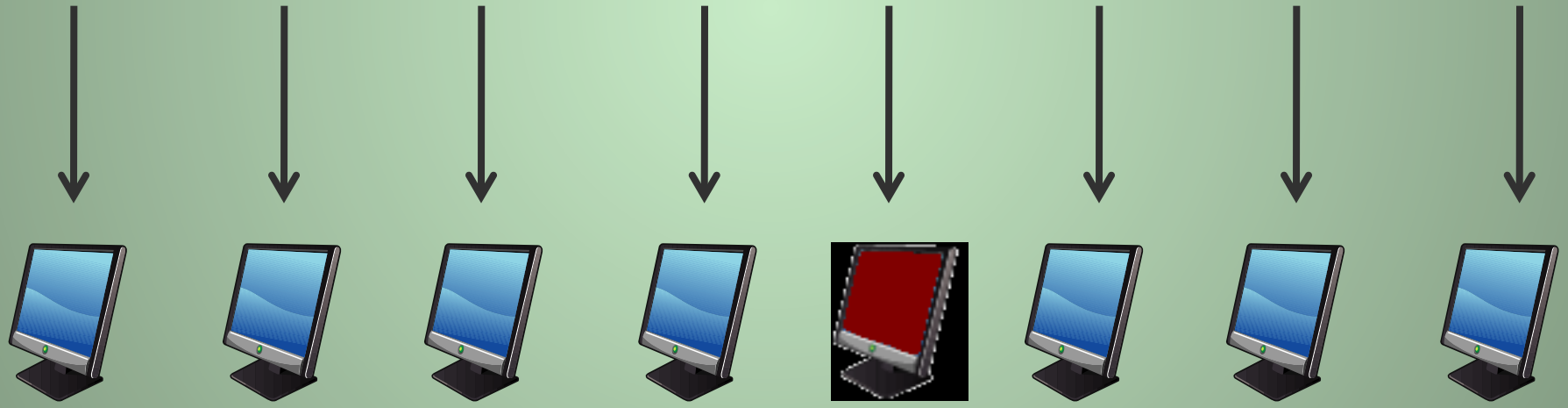
Por su naturaleza, todo el tráfico en una darknet es en concepto tráfico malicioso debido a que son segmentos “no asignados”, por lo tanto, ningún tipo de tráfico debería ser dirigido hacia ellos.

DARKNET A GRAN ESCALA

Generalmente amenazas como gusanos, virus, bots, spam, scaneos, ataques, etc., envían indiscriminadamente tráfico a todos los equipos dentro de una red. Este tipo de patrones son fácilmente detectables por una darknet.

DARKNET A GRAN ESCALA





DARKNET A GRAN ESCALA

Una darknet es un complemento a los sistemas de detección de intrusos (IDS) y monitoreo de la red, sin embargo, requiere una inversión de direcciones IP, por lo cual en redes con pocas direcciones IP disponibles no es conveniente su instalación.

DARKNET A GRAN ESCALA

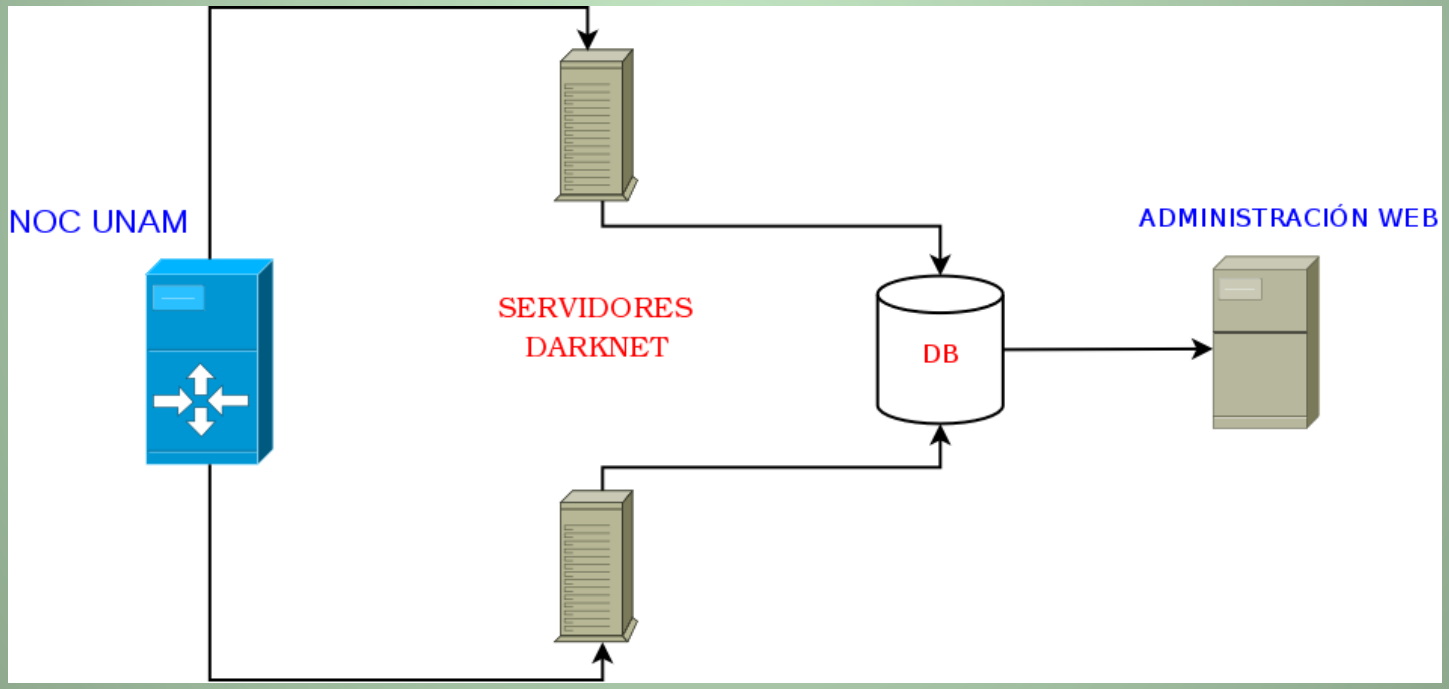
- Los resultados dependen de la ubicación de la darknet.
- Generalmente se obtienen mejores resultados de detección con direcciones IP homologadas que están disponibles desde el exterior.
- Es parecido al concepto de honeynets ya que son señuelos para los atacantes.

ESQUEMA DE MONITOREO

NOC UNAM
Redireccionamiento de tráfico cuyo destino son IP's "no asignadas"

SERVIDORES DARKNET

ESQUEMA DE FUNCIONAMIENTO



¿QUÉ SE PUEDE DETECTAR?

- Actividad sospechosa por puertos (diferentes protocolos; TCP, UDP, ICMP, etc)
- Tráfico relacionado con servicios específicos (SSH, WEB, DB, etc)
- Direcciones IP y dominios en listas negras
- Ataques comunes a equipos de la red universitaria (fuerza bruta, escaneos, etc)

¿QUÉ SE PUEDE DETECTAR?

- Patrones generados por malware (escaneos, trafico excesivo, baja de servicios)
- Flujo de tráfico (gusanos, virus, exploits automatizados, etc)
- Botnets dentro y fuera de la red universitaria
- Posible tráfico malicioso hacia redes externas (spam, phishing, etc)

PROCESANDO LA INFORMACIÓN

La información que se obtiene en los servidores de la Darknet, es parseada y procesada mediante scripts los cuales están escritos en perl y shell script.

Debido a la gran cantidad de información que se obtiene diariamente, ésta es procesada en tiempo real.

PROCESANDO LA INFORMACIÓN

Los objetivos del procesamiento son:

- ✓ Clasificación de la información
- ✓ Formato de la información
- ✓ Detección de falsos positivos

HERRAMIENTAS UTILIZADAS

- Sistemas Operativos
  - GNU/Linux Debian 5.0
- Herramientas para obtención de información
  - Honeytrap
  - Argus & ra tools
  - SNORT
  - Tcpdstat
  - Tcpflow
  - Nepenthes

HERRAMIENTAS UTILIZADAS

- Herramientas para procesamiento
  - PERL
  - Shell script y utilerias UNIX (awk, sed, grep, sort, etc)
- Herramientas para el almacenamiento de información
  - SMDB PostgreSQL

GENERANDO ESTADÍSTICAS

Durante la fase de pruebas:

- Se reciben, manejan, procesan y registran aproximadamente 2.5 millones de conexiones diariamente.

- Alrededor de 5Gb de bitácoras diariamente

GENERANDO ESTADÍSTICAS

- Miles de incidencias de malware (principalmente bots y gusanos) y ocasionalmente decenas de muestras diferentes en un día.

- Miles de direcciones IP's externas e internas con posible actividad maliciosa.

Gracias por su atención

jsantillan@seguridad.unam.mx
rsanchez@seguridad.unam.mx

Visita:

http://www.disc.unam.mx/2009
http://www.seguridad.unam.mx
http://www.honeynet.unam.mx
http://www.malware.unam.mx
http://tv.seguridad.unam.mx
http://revista.seguridad.unam.mx