DGTIC UNAM CERT

2do Coloquio de Proyectos de Becarios en Seguridad Informática

Spampot

Desarrollo e implementación para analizar correo electrónico no deseado

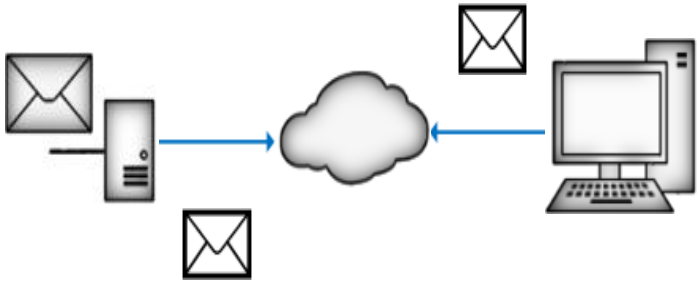
Miguel Raúl Bautista Soria

La necesidad de este proyecto

- La SSI/UNAM-CERT obtiene información acerca de ataques en RedUNAM gracias a los Honeypots instalados por el Proyecto Honeynet UNAM.
- Uno de los ataques más comunes en RedUNAM y en Internet es el envío de correo electrónico no deseado, el SPAM.
- Con esta implementación la SSI/UNAM-CERT pretende capturar y analizar el SPAM en RedUNAM.

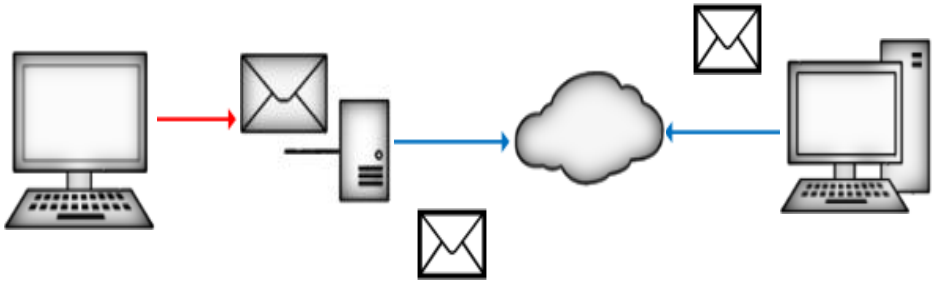
Funcionamiento de un servidor SMTP

- El protocolo más utilizado para enviar correo electrónico por Internet es el SMTP.



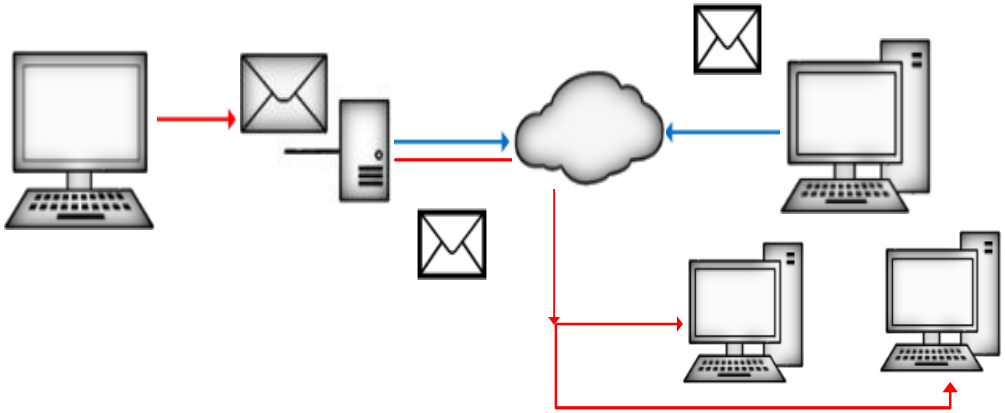
Funcionamiento de un servidor SMTP

- La configuración por defecto de un servidor SMTP permite enviar correos electrónicos desde cualquier equipo en Internet hacia otro sin ninguna restricción. También llamado *Open Relay*.



Funcionamiento de un servidor SMTP

- Los servidores *Open Relay* en Internet son utilizados por atacantes o códigos maliciosos para enviar SPAM a uno o varios usuarios de cualquier servidor de correo electrónico en Internet.



Funcionamiento de un servidor SMTP

- Para enviar un correo electrónico, de acuerdo al RFC 821, se necesitan una serie de comandos.
- Estos comandos son enviados al servidor SMTP quien debe procesarlos, recabar la información necesaria y finalmente enviar el correo.
- Los comandos básicos para enviar un correo electrónico son:
  - HELO o EHLO
  - MAIL FROM
  - RCPT TO
  - DATA
  - QUIT

¿Para qué simular un Open Relay?

- Para comprender a qué están expuestas nuestras redes o servidores.
- Para identificar posibles equipos o servidores comprometidos o infectados con malware.
- Para identificar si alguna cuenta de correo electrónico ha sido comprometida o es víctima de una campaña masiva de spam.
- Para detectar nuevos ataques o tendencias en spam.

Funcionamiento del Spampot

- Simula un servidor *Open Relay.*
- La programación está orientada a hilos para atender peticiones concurrentes desde varios clientes.
- Después de interactuar con el cliente, leerá el archivo en donde se almacenó la información y extraerá toda la información esencial del correo.
- Cuando un cliente se conecte a la herramienta, éste podrá enviar múltiples correos.
- Se considerará como un evento, a la información enviada a través de una conexión.

Ejecución

nc localhost 25
220 correoelectronico.unam.mx SMTP
HELO correoelectronico.unam.mx
250 correoelectronico.unam.mx SMTP
MAIL FROM: alumno@servidor.unam.mx
250 OK
RCPT TO: rector@mail.unam.mx
250 OK

Ejecución

DATA
354 Enter message, end with "."
Subject: Notificacion de recompensa
Estimado usuario usted ha sido notificado
por recibir recompensa de $1,000,000 dollar
Por favor escribe a da-blob@die.server.de
para notificar su premio
Thank you
.
250 OK: Queued message as ac00bfcedb
QUIT
221 Bye

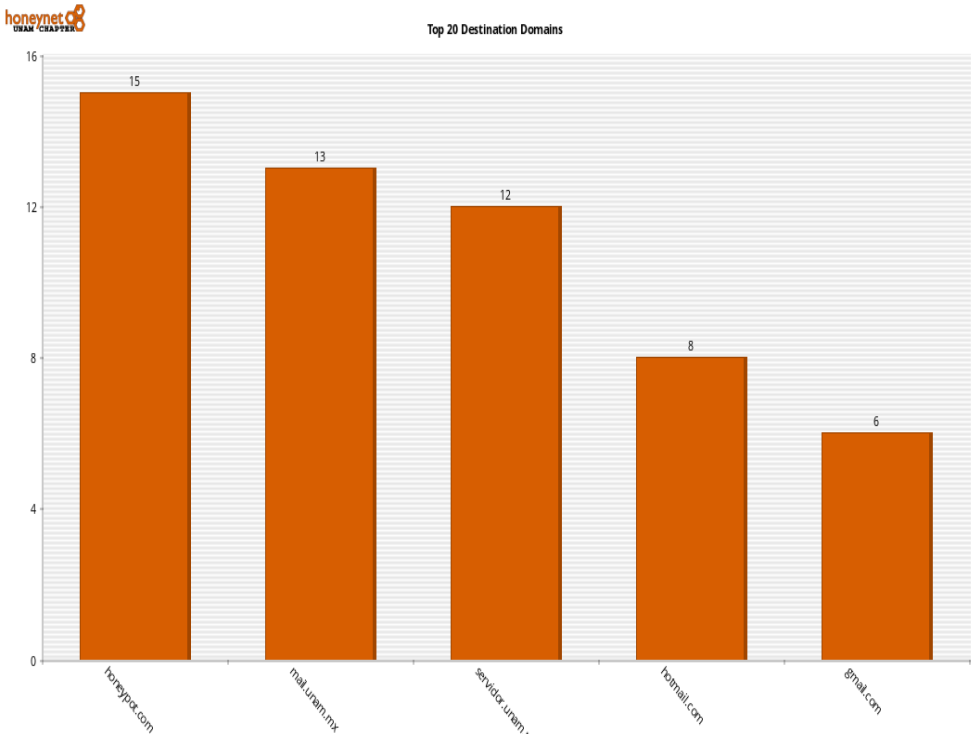
¿Qué se obtiene?

- Toda la información del correo se almacena en un archivo de texto.
- El archivo se procesa y se analiza el contenido en busca de los siguientes patrones:
  - Direcciones IP, origen y destino
  - Direcciones de correo electrónico
  - Direcciones IP en el contenido del correo
  - Asuntos de correo
  - Nombres de dominio
  - URLs de Internet
  - Cadenas o patrones específicos
  - Archivos adjuntos

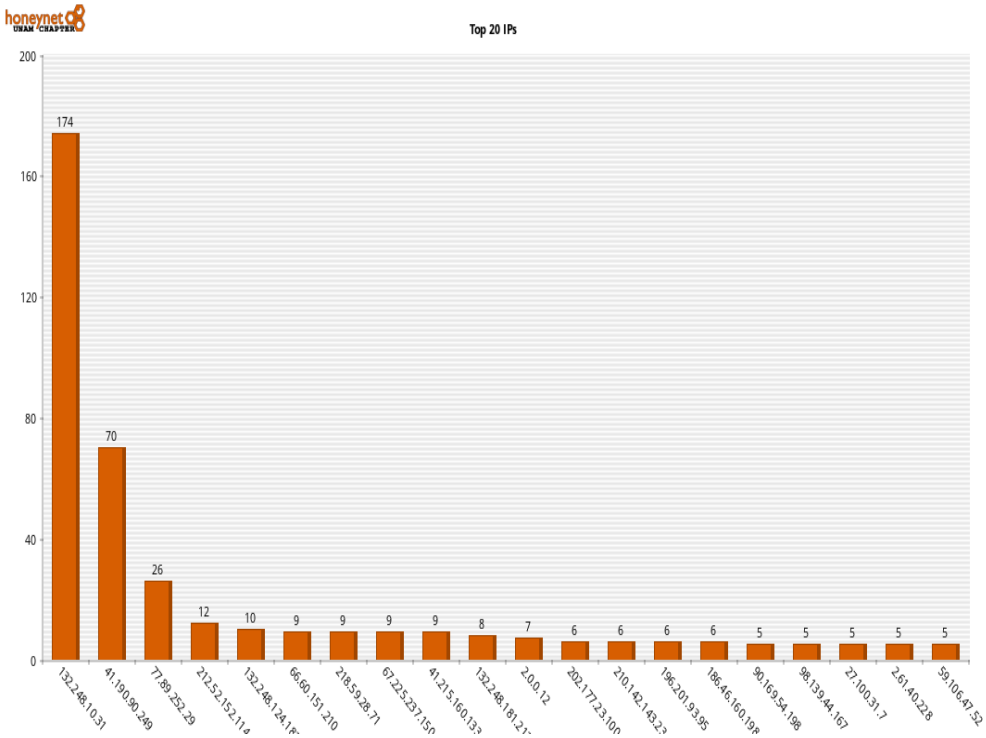
¿Qué se hace con la información obtenida?

- Se identifican las direcciones IP origen para obtener una lista de las IP que más SPAM generan.
- Se obtiene una lista de direcciones de correo electrónico y dominios de Internet más utilizados.
- Se descargan las URL detectadas.
- Se decodifican los archivos adjuntos.
- Se generan gráficas para una mejor visualización de la información.

Gráfica de dominios



Direcciones IP



Extras

- La herramienta funciona con algunos servicios de detección de *Open Relay* como Mail Radar, MX Toolbox, SpamHelp, entre otras.
- Un cliente Thunderbird puede ser configurado para enviar correo a través de esta herramienta y funcionará sin problemas.


THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
JUSPAXAR
DANKSCHEEN
TASHAKKUR ATU
YAQHANYELAY
SUKSAMA
EKHMET
MEHRBANI
GRAZIE
PALDIES
KOMAPSUMNIDA
MAAKE
GOZAIMASHITA
EFCHARISTO
BOLZÏN
MERCI
BÏYAN
SHUKRIA
TINGKI
SPASSIBO
SNACHALHUYA
NUHUN
CHALTU
WABEEJA
MAITEKA
YUSPAGARÄTAM
HUI
GUI
HATUR
SPASIBO
DENKUJA
NENACHALHYA
UNALCHEESH
EKOJU
SIKOMO
MERSI
DHANYAVAAD
ANIHA
ATTO
MERASTAHHY
GAEJYHO
TAVTAPUCH
MEDAWAGSE
GAHCO
LAH
AGUYJE
FAKAAUE
BAJKA
MAKETAU
MINMONCHAR