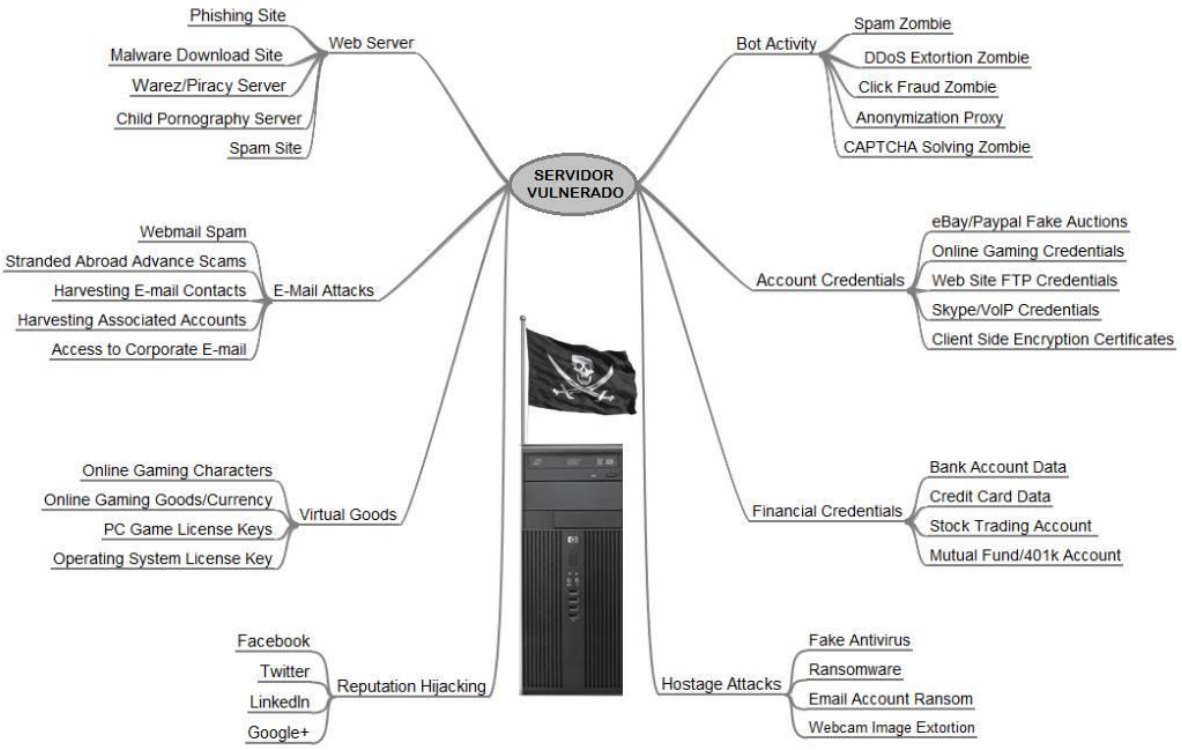
Breve historia de un servidor señuelo: interpretación y análisis de bitácoras.

Introducción:

No cabe la menor duda que Internet es un entorno en donde las amenazas y los ataques informáticos se encuentran permanente activos. Una de las principales virtudes de la gran red de redes, es la de eliminar las barreras geográficas y con ello brindar productos y servicios a cualquier parte del mundo; sin en cambio, esta característica de interconexión es también una de las principales herramientas que los delincuentes informáticos desean aprovechar con el objetivo de lograr beneficios personales y económicos.

Se podrán preguntar **¿Qué beneficios económicos se pueden lograr al vulnerar un servidor?** Déjame decirte que existen múltiples maneras de monetizar un servidor que ha sido comprometido, a continuación te muestro los usos más comunes que se le dan a los servidores afectados.



Es por lo anterior que surge la idea de configurar un servidor y exponerlo de manera controlada. **¿El objetivo?** Obtener evidencias de ataques reales para realizar un análisis de las bitácoras generadas, para con ello, generar un panorama actual del riesgo de exponer servidores sin una adecuada protección.

Características del equipo expuesto:

El servidor ha sido expresamente diseñado para ser expuesto en Internet, la preparación de este laboratorio fue realizado en **3 etapas**: preparación del equipo (totalmente protegido), exposición del equipo y por último el análisis de la información recopilada.

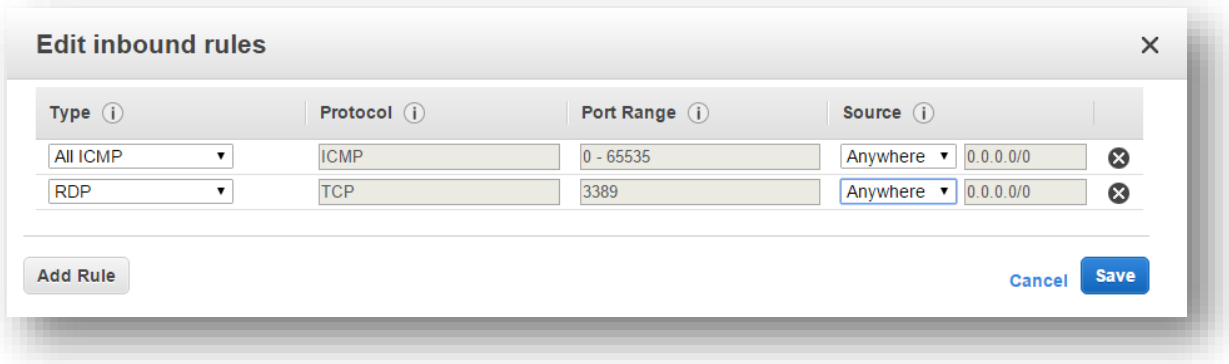
En la primera etapa se ha realizado un fortalecimiento fuera de línea que incluye los siguientes criterios:

- Deshabilitar usuarios no requeridos.
- Establecer contraseña robusta a la única cuenta activa (Administrator).
- Deshabilitado de puertos y servicios no requeridos.
- Instalación de las últimas actualizaciones disponibles para el sistema operativo.
- Habilitado de bitácoras del sistema.
- Protección perimetral por medio de un Firewall.

Las características del servidor son:

- **Sistema operativo**: Windows 2008 R2 (VPS).
- **Dirección IP**: homologada fija.
- **Puertos o servicios habilitados**: únicamente RDP (TCP/3389) y PING (ICMP). El resto han sido bloqueados mediante un firewall a nivel de red.
- **Idioma del servidor**: inglés.
- **País donde se encuentra el servidor**: Estados Unidos (Oregon).
- **Periodo de operación**: 5 días.

En la segunda etapa se configura el sistema firewall para permitir conexiones desde cualquier dirección IP hacia el servicio de **RDP**. La siguiente imagen muestra las reglas configuradas.



Una vez realizada la apertura de puertos, solo fue cuestión de esperar.

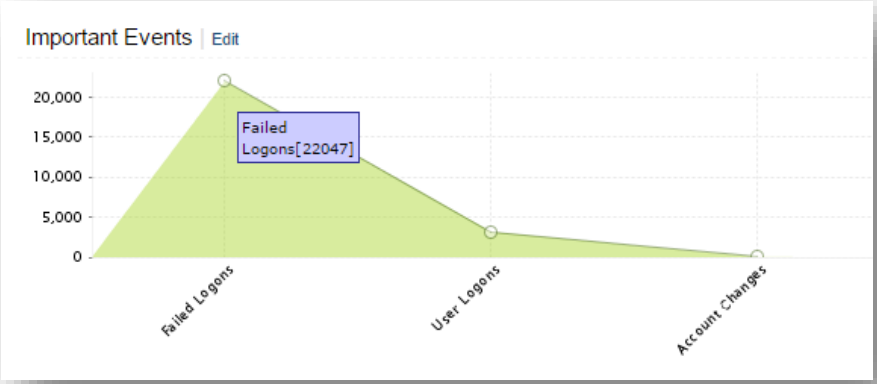
<u>Tercera etapa, los resultados:</u>

Una vez concluido el periodo definido de exposición, se procedió a bloquear el puerto RDP para posteriormente recopilar y extraer las bitácoras que serían objeto de análisis. A continuación se muestran los resultados obtenidos.

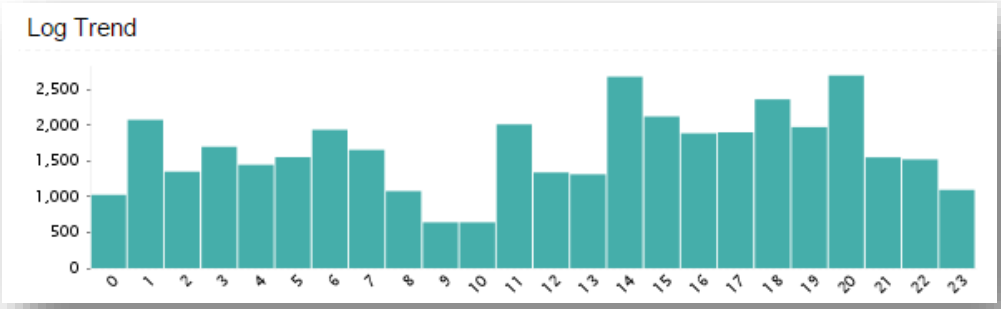
- Tiempo transcurrido desde que se expuso el servidor hasta recibir el primer intento de acceso: **17 minutos**. Esto es menos de lo que tarda una pizza en llegar a casa.

17 Breves minutos para el primer ataque.

- Cantidad de intentos de inicio de sesión fallidos: **22,047** lo que se traduce **en promedio 4400 ataques por día**.



- Horario en el cual los atacantes realizaron el mayor número de intentos de acceso: **20:00 hrs. horario local de México.**



- Usuario más atacado: **Administrator con 10,477 intentos (47.52% de los ataques)**.
- **Top 10** de usuarios atacados:

Top Users by Failed Logins

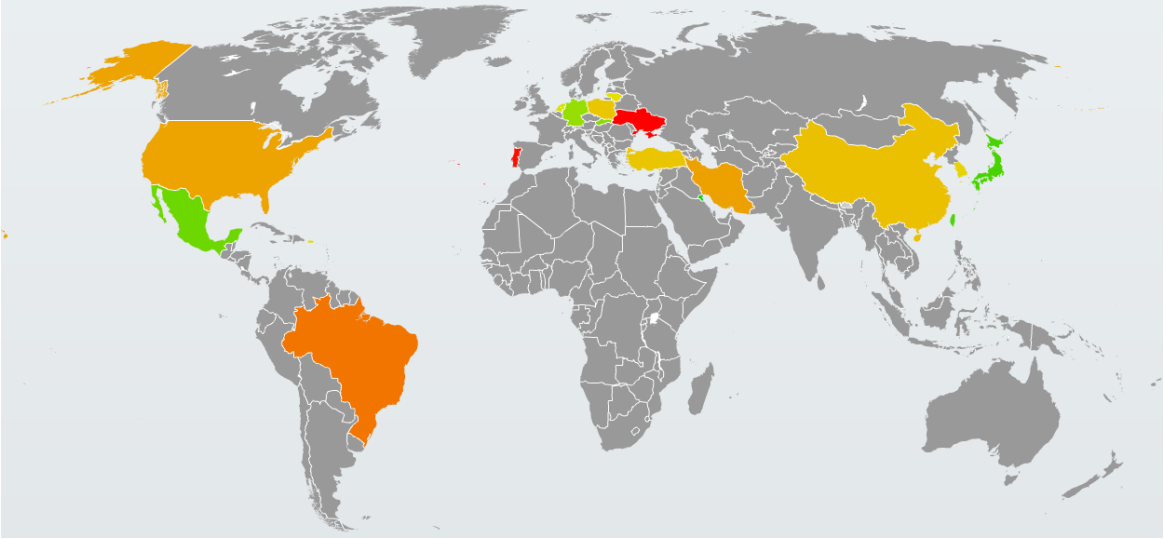
User	Event Count
Administrator	10477
Admin	888
user	505
test	363
user1	360
admin1	231
server	230
user3	225
user2	225
test1	225

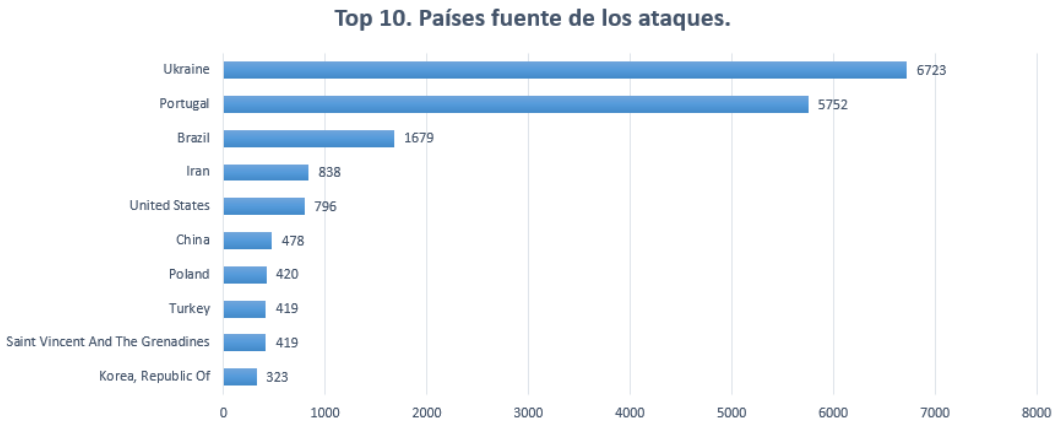
- Total de direcciones IP origen de los ataques: **52 localizables geográficamente**.

EVENTOS	IP ORIGEN	BANDERA	PAÍS
6603	37.57.174.121		Ukraine
5752	188.251.249.157		Portugal
1257	187.23.176.162		Brazil
419	177.0.211.231		Brazil
419	188.252.14.148		Poland
419	208.234.33.213		United States
419	69.73.201.226		Saint Vincent And The Grenadines
419	78.185.23.31		Turkey
419	81.29.247.181		Iran, Islamic Republic Of
419	84.241.5.25		Iran, Islamic Republic Of
282	113.240.62.94		China
270	192.158.62.18		Puerto Rico
236	5.199.172.36		Lithuania
137	175.0.185.237		China
120	77.122.115.49		Ukraine
65	80.82.64.38		Netherlands
63	104.155.224.220		United States
63	104.155.235.254		United States
63	130.211.253.202		United States
52	106.248.241.170		Korea, Republic Of
48	64.94.239.236		United States
46	121.184.216.66		Korea, Republic Of
45	1.246.219.116		Korea, Republic Of
45	121.176.83.209		Korea, Republic Of
45	210.103.23.76		Korea, Republic Of
45	210.108.200.13		Korea, Republic Of
45	211.253.9.242		Korea, Republic Of
45	64.94.239.237		United States
41	108.161.133.86		United States
41	96.44.187.163		United States
40	92.68.29.222		Netherlands
32	62.141.38.192		Germany
30	27.17.47.18		China
29	115.182.49.89		China
24	93.174.95.77		Netherlands
19	94.228.87.254		Slovakia
12	68.71.134.244		United States
8	189.212.9.36		Mexico
4	212.7.209.9		Netherlands

4	89.248.162.130		Netherlands
4	94.102.56.130		Netherlands
3	177.202.105.9		Brazil
2	122.116.92.44		Taiwan, Province Of China
2	212.7.209.6		Netherlands
2	80.82.64.81		Netherlands
2	93.174.93.164		Netherlands
1	106.165.183.217		Japan
1	113.33.225.157		Japan
1	168.187.232.195		Kuwait
1	45.35.20.215		United States
1	91.238.134.90		Poland
1	94.102.63.56 Resto de direcciones IP	 N/A	Netherlands No reconocido.

- Principal país atacante: **Ucrania** seguido de **Portugal** y **Brasil** ¿Quién lo diría?
- Cantidad de países de donde provienen los ataques: **19 países**. A continuación la distribución geográfica.





Hallazgos y conclusiones:

Entre los diversos hallazgos se pueden enlistar los siguientes:

- Los delincuentes informáticos no descansan, no importa el día ni la hora, en todo momento existe la intención de vulnerar servidores, ya sea esto con herramientas automatizadas o por medio de ataques ejecutados manualmente.
- Tan solo transcurrieron 17 minutos para recibir el primer intento de acceso, a partir de ese momento el servidor se encontró activamente atacado.
- Un punto realmente relevante es que este servidor no contenía un servidor Web, FTP, de correo electrónico o cualquiera que pretendiera dar un servicio a usuario finales, el equipo fue objeto de los ataques aun cuando no fue promocionado o publicado en algún sitio en Internet. Este es un hallazgo vital ya que aún existen administradores de red y de sistemas que piensan en el obsoleto método de control "seguridad por oscuridad" y creen fielmente en que al exponer un servidor en Internet del cual solo ellos conocen la dirección IP no correrán riesgo alguno. Que equivocados están.
- Antes de exponer un servidor a Internet, es vital implementar y aplicar **al menos** las medidas preventivas indicadas en la **etapa 1** de este laboratorio. Si los ataques sufridos han sido el resultado de un solo puerto expuesto, imaginar la cantidad de ataques que sufren los equipos que tienen diversos servicios publicados.
- Dentro de las mejores prácticas asociadas a protocolos de gestión remota se encuentran las siguientes:
    - El protocolo deberá usar un mecanismo de cifrado.
    - Se recomienda que la manera de accederlo sea por medio de una conexión VPN.
    - Que se cuenten con umbrales de bloque en caso de múltiples intentos fallidos de acceso, es decir, que después de N número de intentos fallidos realice un bloqueo de la cuenta y un "baneo" de la IP ofensora, ya sea temporal o permanente.
    - En caso que el protocolo deba estar expuesto a Internet, se sugiere la implementación de un segundo factor de autenticación (2FA).
- Implementar mecanismos de monitoreo de bitácoras en automático (SIEM), en caso de no ser posible esto, se deberá contar por lo menos con una rutina manual de revisión de bitácoras en búsqueda de comportamientos sospechosos.

Como se puede observar, las condiciones no están balanceadas, ya que la defensa y protección de sistemas es demandante y para los atacantes bastará una sola debilidad para lograr su cometido.

A manera personal puedo resumir que este laboratorio generó los resultados que esperaba y me ha generado una visión real y actual. Por si te lo preguntas, el servidor no fue vulnerado.

El laboratorio y reporte han sido realizados por GF0S Incorporado como un ejercicio personal. Si deseas estar en contacto conmigo, puedes realizarlo por medio de
www.facebook.com/gf0s.seguridad

Anexo 1: Lista total de usuarios empleados en los intentos de inicio de sesión.

En total se observaron **209** cuentas usadas para los ataques, el detalle se muestra a continuación:

Administrator
admin
user
test
user1
admin1
test1
user2
user3
server
support
adm
backup
root
sys
guest
administrador
par
manager
user01
user02
info
remote
testuser
access
account
accountant
administrateur
administrators
agent
art
asus
auto
backup1
besadmin
besadmin1
boss
canon
computer
connect
control
demo
director
host
local
login
manager1
marketing
microsoft
network
office
office1
operator
qwerty
reception
reception1
scan
scaner
server1
service
sysadmin
system
temp
temp1
terminal
tester
training
training1
username
windows
work
xerox
sql
owner
david
aspnet
1
123
a
actuser
admin2
console
john
support_388945a0
test2
test3
user4
user5
AMHS-Services
srv-backup
OneStepRetail
OneStepRetail1
RetailTasks
RetailTasks01
RetailTasks1
Alex
alex66
alex99
alex996
bobkok
Masger
miass
MSQLertans
UBM
yangyang
justin
rbms
okqokvokb
action
adm01
adm555
admin11
admin888
Alex5
ASP
ASP.NET
billr
CSSI
db2admin
EDGAR
Gh4fMJostUser
hei
INASysWatcher
itsupport
IUSR_RCTION
IUSR_SSQL
jackie
James
jane
jcbatte
ji
kelly
LogMeInRemoteUser
management
Manger
Max112
Max12
mgarrett
mkrout
obobomom
okkmkokb
okqmkomko
op
oprrss
postgres
psaadm
ray
rec
rico
soss
spectra
SQLD
updater
vok
voookk
vvb
William
xukongwen
Administartor
HCRS01
MetricAlertServer
qbooks_ywish
USSSUPPORT
VNIAdmin_DoNotDel
ete
Adam
aspadmin
chirotouch
ETB User
fax
gadmin
HBS_Admin
her
malu
MetasysSysAgent
mroot
N2P_SERVICE
ntsec_admin
oigadm1n
OMESQR
Roma
sftsh_mng
srvadmin
system_backupDB
tech
tskusr
User88
aloha
ftpadmin
microssvc
midas
niabi
paul
POS1
scanner
admin01
ampm
cash
cbsuser
ConquerorServer
Engineer
FPLOGSVCUSR
FPUPDENGUSR
Inventory
jcarmona
market
midwest
pos
pos2
XIOS

¿Alguna te suena familiar?