Analisis de Malware Con Software Libre

Carlos Ganoza

Malware

- Software malicioso construido intencionalmente para causar daño al PC.

Gusanos

- Troyanos
- bombas logicas
- Guindous?

Vamos hacia atras

- El primer virus fue creado en los Laboratorios Bell con la intención de realizar un juego llamado Core War el cual consistia en llenar la memoria ram del contrincante en el menor tiempo posible.

Robert Morris

En la actualidad

- Es utilizado por ciberdelincuentes para cometer actos ilegales:
- Robar datos, DDOS, SPAM, etc.
- Tambien es aplicado para ataques de sabotaje
- -StuxNet
- -Duqu

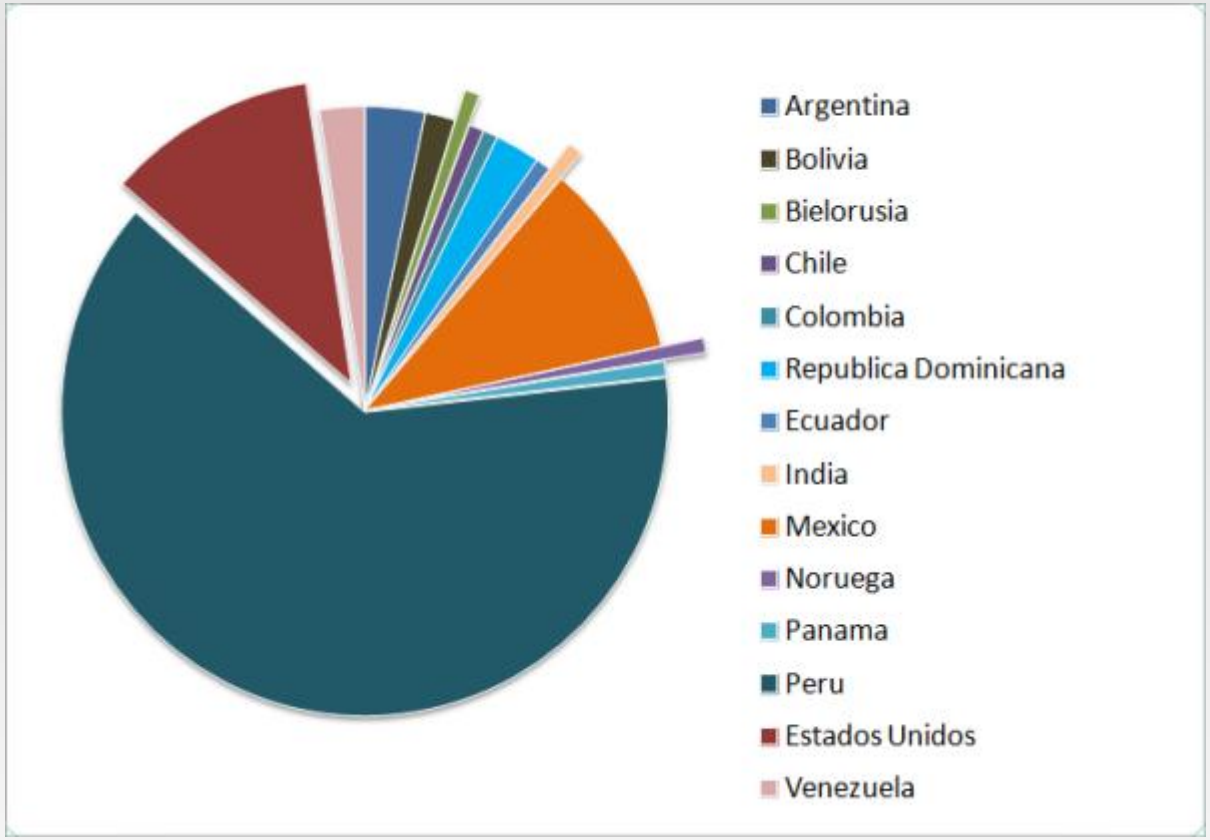
Negocio Rentable

- Un troyano puede costar mas de10.000$
- Computadora zombie 1$

Otros Precios

Datos de tarjetas de crédito	De $2 a $90 USD
Datos de acceso bancario validados	De $80 a $700 USD
Datos de acceso a plataformas de pago y tiendas online	De $80 a $1,500 USD
Renta de servidores para envío de spam	Desde $15 USD
Renta de VPN para esconder identidad	$20 USD por trimestre

El Perú es afectado?



Estadisticas realizadas por eset sobre la botnet volk

Analizando...

Que necesitamos?

Herramientas

- VirtualBox, Quemu (entorno virtualizado)
- Process Hacker (analizar procesos)
- Reg-Shot (comparar cambios de registro)
- Wireshark (analizar trafico)
- Ghex (editor hexadecimal)

Otras herramientas

- **REMnux.- distribución del linux para el análisis de malware.**

GRACIAS!!!

- Mail: cganozap@malwareint.com
- Twitter:@drneox
- Web:Www.todoporelvicio.com