Lunes 13 de Agosto 2018

ELO322
Redes de Computadores 1

Ataques en redes

Integrantes
Alonso Rodriguez Z.
201473018-7
Alexis Santibáñez C.
201473116-7

Resumen

En el presente, el internet es la tecnología probablemente más utilizada por la sociedad, millones de datos se cargan y se descargan de la red cada dia, la información corre a rienda suelta por la internet. Esta sobrecarga de datos es muy valiosa para quienes trabajan con ellos, pero también para quienes desean sacar beneficio irrumpiendo, manipulando o dañando estos datos, los llamados “Hackers” o “Crackers”. La internet tiene multiples tecnicas de seguridad para evitar que los datos de la red sean fáciles de manipular, pero aun asi, con tanta liberación de software nuevo, como pueden ser aplicaciones nuevas o por ejemplo una actualización de sistema operativo, se van creando posibles aperturas que permiten a entes mal intencionadas vulnerar los sistemas de seguridad del sistema. Por lo tanto, se vuelve importante el estar atento a estos posibles ataques, saber cómo prevenirlos y qué hacer si nos encontramos bajo ataque. El presente informe se encargará de mencionar estos puntos, partiendo con los tipos de ataques más comunes que se ven en la red, técnicas básicas de prevención y cómo deshacerse de ellos en caso de encontrarse víctima de uno, para entregar al lector una noción básica de seguridad en la red, mostrando como ejemplo un posible comportamiento de un malware tipo gusano.

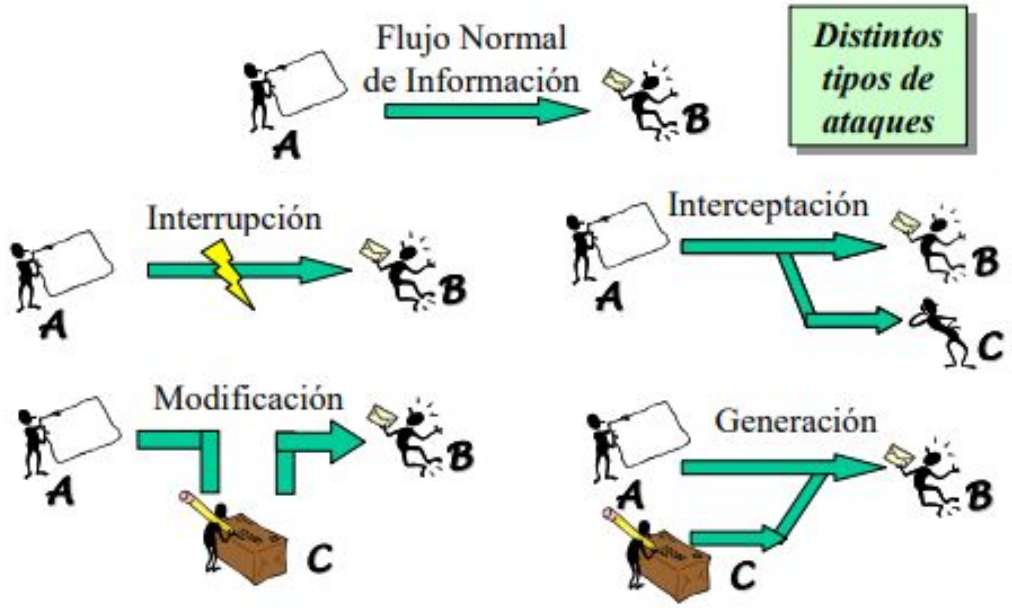
Introducción

Actualmente es fácil reconocer el valor que ha tomado internet a nivel social y tecnológico, nos ha permitido conectar millones de computadores a través del globo, dando a una red de información de un valor incalculable, ha permitido conectar organizaciones distribuidas a lo largo del globo mejorando el rendimiento de estas pero principalmente, ha permitido que la información pueda viajar por todo el planeta en cuestión de segundos, esta es una capacidad muy poderosa de la internet que le permite ser probablemente la tecnología más utilizada en los tiempos modernos.
A lo largo de múltiples años se han ido mejorando cada vez más las tecnologías y protocolos utilizados para crear mejores redes de información, aumentando su rendimiento gracias a nuevas tecnologías de cableado o señales inalámbricas, mejorando los protocolos para fortalecer su privacidad y resguardo de información o en mejores técnicas de ruteo para un mejor direccionamiento de datos, todo esto con el fin de mejorar las capacidades de la red.
Pero a su vez, tanta información termina termina siendo valiosa no solo para gente quien la utiliza para trabajar con ella, si no también para entes malintencionados que buscan obtener provecho de ella o a veces que simplemente desean dañarla para perjudicar, y a pesar de que las conexiones se han vuelto cada vez más seguras y privadas con el pasar de los años, las técnicas de ataques informáticas han ido evolucionando a la par. Por lo tanto, se vuelve necesario conocer de los diferentes tipos de ataques que existen para poder prevenirlos o deshacerse de ellos en caso de que ya se está siendo víctima de un ataque.

Ataques en redes

Un ataque informático es un intento organizado e intencionado para tomar el control, desestabilizar o dañar otro sistema informático o red. Los ataques en grupo suelen ser hechos por bandas llamados "hackers". Una víctima de una ataque puede ser tanto un individuo en particular o una organización, a veces el ataque incluso podría simplemente estar dirigidos a cualquiera, sin blanco en particular.
Un ataque consiste en aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; con el objetivo de causar daño en los archivos de la víctima, espionaje, adquirir información confidencial, obtener control sobre información la víctima, etc. Esto puede ser utilizado no exclusivamente con fines delictuales, ya que a su vez existen distintas instituciones enfocadas a la criminalística que utilizan estas mismas técnicas de pirateo informático para obtener información de bandas delictuales.
Podríamos diferenciar ataques en:

- **Activos**: producen cambios en la información y en la situación de los recursos o servicios del sistema.
- **Pasivos**: se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema.



Tipos de ataques

1. Acceso físico

En caso de poseer acceso a equipos o instalaciones, es posible:

- Apagado manual del equipo.
- Vandalismo.
- Apertura de la carcasa del equipo y robo del disco duro.
- Monitoreo del tráfico de red.
- Trashing

2. Robo de información mediante la interceptación de mensajes (sniffers)

Tratar de interceptar los mensajes de correo o los documentos que se envían a través de redes, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios. Un ejemplo es WireShark, con el que puedes ver todo lo que fluye por la red de nuestro ordenador, incluyendo el tráfico de todos los que hay conectados a la red. Ocurre tanto físico(cable) como lógico (redes inalámbricas).

3. Detección de vulnerabilidades en los sistemas

Tratar de detectar vulnerabilidades para a continuación desarrollar alguna herramienta que permite explotarlas fácilmente (herramientas conocidas popularmente como “exploits”), mandando mensajes construidos específicamente para provocar el fallo de la máquina. Una forma es:

- Ataque de fuerza bruta: trata de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que se busca.
- Monitorización: observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro.
- Inyección de Código SQL: Realizar consultas a la base de datos por vulnerabilidades del sistema.

4. Modificación del contenido

En estos ataques los intrusos tratan de reenviar paquetes, tras haberlos modificado de forma maliciosa (por ejemplo, para generar una nueva transferencia bancaria contra la cuenta de la víctima del ataque). También se conocen como “ataques de repetición” (“replay attacks”). Otros tipos serían:

- Tampering o Data Diddling: Modificación desautorizada de los datos o el software en el sistema víctima (incluyendo borrado de archivos).
- Borrado de Huellas: El borrado de huellas, ya que si se detecta su ingreso, el administrador buscará conseguir "tapar el hueco", evitar ataques futuros e incluso rastrear al atacante.

- También se pueden realizar diferentes tipos de ataques de intrusión utilizando malware, que son software malintencionado también conocidos como malware, estos conocen la misión de ejecutar código que genera efectos negativos en el computador, o que fuerzan a utilizar una computadora infectada para realizar otros tipos de ataques, los más conocidos son los Troyanos y los gusanos (worms).

5. Ataques de autenticación

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.(su forma más común es recibir un correo electrónico con un enlace de acceso directo falso de paginas que mas visitas)

6. Denial of Service(DoS)

Los protocolos existentes actualmente fueron diseñados para ser hechos en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Denegación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.
Un ejemplo de cómo estos funcionan, es la figura 2 del anexo, en donde se ve que múltiples computadoras “zombie” están intentando acceder a cierto servicio que provee la víctima, de esta forma saturando sus recursos y evitando su correcto funcionamiento. La creación de estos computadores “zombie” se puede lograr esparciendo malware a través de internet, como podría ser un gusano.

7. Ataques de suplantación de la identidad

- **IP Spoofing**: un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado.
- **DNS Spoofing**: pretenden provocar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, facilitando de este modo la redirección de los usuarios de los sistemas afectados hacia páginas Web falsas o bien la interceptación de sus mensajes de correo electrónico.
- **SMTP Spoofing**: El envío de mensajes con remitentes falsos (“masquerading”) para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente es otra técnica frecuente de ataque basado en la suplantación de la identidad de un usuario. De hecho, muchos virus emplean esta técnica para facilitar su propagación, al ofrecer información falsa sobre el posible origen de la infección.

Pasos de un ataque

1. **Intento de ingreso**
En esta etapa, el atacante investiga a la organización blanco. Él puede obtener toda la información pública sobre una organización y sus empleados y realizar exploraciones completas en todas las computadoras y dispositivos que son accesibles desde Internet.

2. **Penetración en la red**
Después de que el atacante haya localizado vulnerabilidades potenciales, intenta aprovecharse de una de ellas. Por ejemplo, el atacante explota las vulnerabilidades en un Servidor Web que carece de la última actualización de seguridad.

3. **Elevación de privilegios**
Luego que el atacante ha penetrado con éxito la red, procura obtener los derechos de Administrador a nivel de sistema. Por ejemplo, mientras que explota el servidor Web, gana control de un proceso funcionando bajo el contexto LocalSystem. Este proceso será utilizado para crear una cuenta de administrador. En general, la pobre seguridad como resultado de usar configuraciones por defecto, permite que un atacante obtenga el acceso a la red sin mucho esfuerzo.

4. **Explotar vulnerabilidades**
Después de que el atacante haya obtenido los derechos necesarios, realiza el intento de romper la seguridad de la red. Por ejemplo, el atacante elige desfigurar el sitio Web público de la organización.

5. **Borrado de huellas**
La etapa final de un ataque es aquella donde un atacante procura ocultar sus acciones para escapar a la detección o el procesamiento. Por ejemplo, un atacante borra entradas relevantes de la intervención en archivos log.

Prevención de Ataques

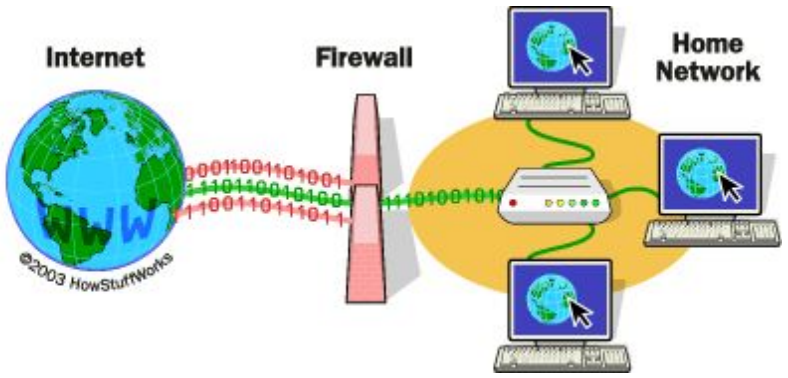
Hoy en día ya podemos decir que las técnicas de seguridad que vienen predeterminadas en un sistema tienen cierta grado de seguridad aceptable, y la verdad es que se necesita realmente de un descuido del mismo usuario para ser afectados, como ejecutar archivos sin certificados válidos, descargar demasiados archivos de páginas desconocidas, instalar programas desconocidos, no utilizar un buen sistema de antivirus, etc.

Por lo tanto en el dia de hoy las principales formas de prevención para una persona individual es la de navegar por sitios fiables en la internet, utilizar un sistema de antivirus o al menos los servicios de seguridad que suelen proveer los sistemas operativos, evitar descargar y ejecutar archivos que provengan de sitios no fiables, para cuando se utilicen aplicaciones que posean un sistema de registro, a la hora de utilizar servicios que se requiera ingresar informacion, conviene crear contraseñas difíciles de forzar, con multiples caracteres y numeros, y jamás entregar la contraseña de estas cuentas privadas.

Para el caso de organizaciones que utilicen profundos sistemas de información, que tengan acceso a internet, es necesario tomar medidas más avanzadas, debido a su mayor mayor cantidades de información y a su vez mucho más valiosa. Una falla en un sistema de información que esté implementado en una organización puede generar pérdidas millonarias para la misma, por lo tanto, el mismo sistema ha de tener incorporada medidas extras, como por ejemplo seria incorporar un sistema cortafuega a nivel de aplicacion.
Tambien al caso de Servidor de DNS, o grandes paginas que requieren uptime extensos, o proveen servicios de gran valor, deben implementar sistemas de deteccion de intrusos, para reconocer posibles ataques, y respuestas ante el mismo.

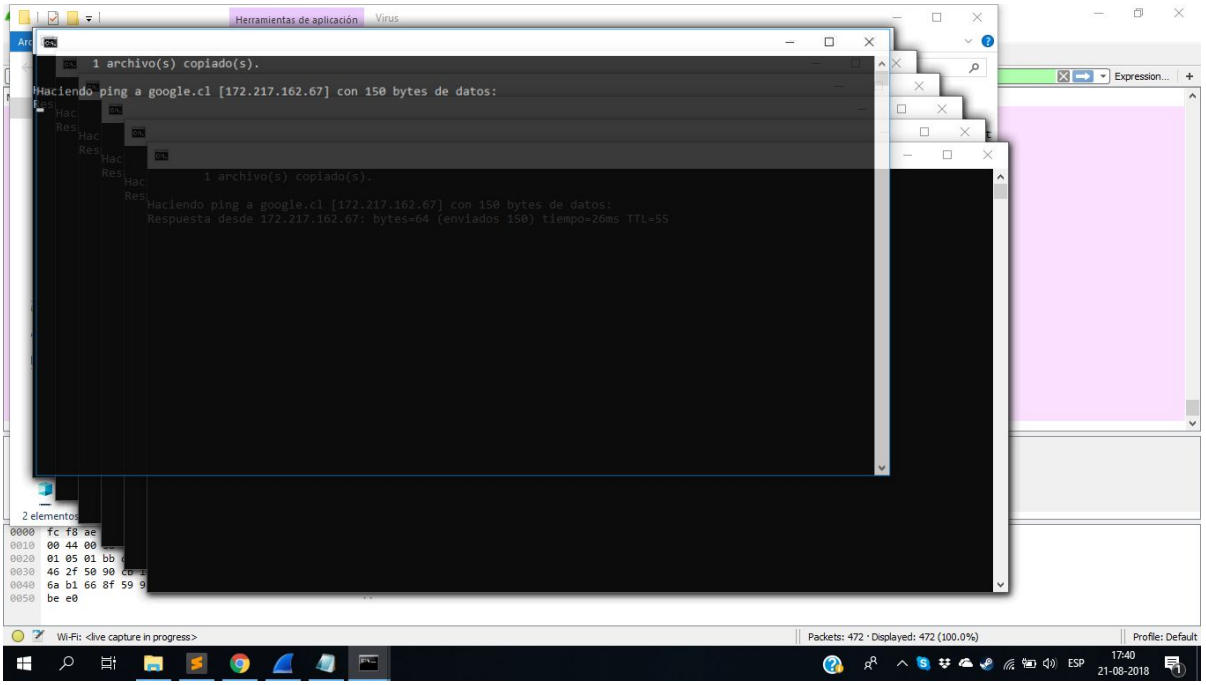
A su vez es importante saber que hacer cuando ya nos dimos cuenta que estamos sufriendo algún tipo de ataque, debido a algún comportamiento extraño del equipo. Generalmente los principales síntomas que se podían encontrar se encuentran en el Anexo, imagen 2. Al detectar, en lo posible, una combinación de estos síntomas, podríamos hablar de un posible malware que está interfiriendo en nuestra computadora.
Estos malwares pueden ser muy escurridizos y muy difíciles de eliminar de forma manual, buscando los archivos corruptos y en si la ubicación del virus, por lo tanto, la forma más eficaz para deshacerse de estos archivos malignos, es utilizando escaneos de **antimalware**. En caso de que sea un ataque que no involucre archivos en el sistema víctima, ya es necesario mejorar los protocolos de seguridad de la red de forma que sea más complicado obtener acceso a nuestro dispositivo, esto se puede lograr, por ejemplo activando “**Firewall**” un sistema de seguridad que viene

de forma base en sistemas operativos como Windows, que sirve como punto de control entre los datos que llegan de internet hacia el computador.

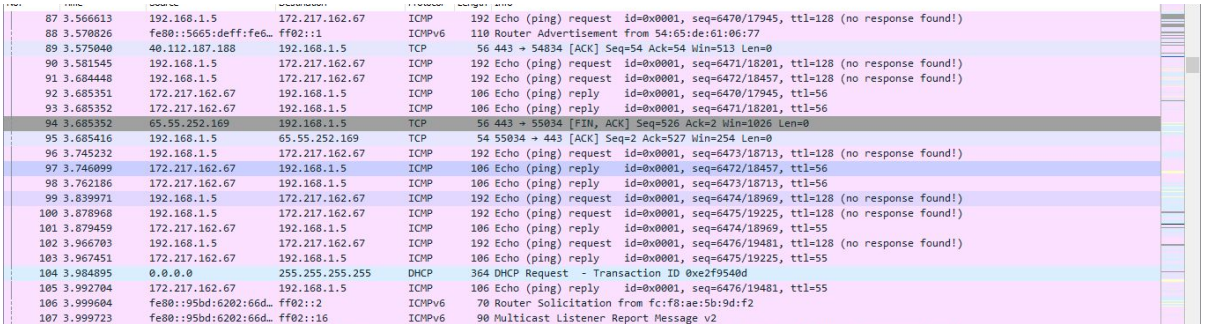


Resultado de parte práctica (capturas de pantalla con texto explicativo)

Para ver como reacciona un servidor ante un posible DDoS, realizamos un pequeño virus autoreplicante, que en si, solo se duplica y se ejecuta nuevamente, para intentar multiples señales de Ping, a google.cl, o a cualquier pagina que se especifique.
El virus en si es bastante basico, y para los estandares de seguridad que poseen los sistemas hoy en dia, es muy probable que solo sea molestoso, debido a su constante ejecucion, pero no muy servero.
Abajo se ve una ejecucion del mismo.



Despues de realizar un ataque buscamos ver que sucede con todos los paquetes que van y vuelven desde google.cl. Para eso utilizando wireshark:



87	3.566613	192.168.1.5	172.217.162.67	ICMP	192	Echo (ping) request id=0x0001, seq=6470/17945, ttl=128 (no response found!)
88	3.570826	fe80::5665:deff:fe6…	ff02::1	ICMPv6	110	Router Advertisement from 54:65:de:61:06:77
89	3.575040	40.112.187.188	192.168.1.5	TCP	56	443 → 54834 [ACK] Seq=54 Ack=54 Win=513 Len=0
90	3.581545	192.168.1.5	172.217.162.67	ICMP	192	Echo (ping) request id=0x0001, seq=6471/18201, ttl=128 (no response found!)
91	3.684448	192.168.1.5	172.217.162.67	ICMP	192	Echo (ping) request id=0x0001, seq=6472/18457, ttl=128 (no response found!)
92	3.685351	172.217.162.67	192.168.1.5	ICMP	106	Echo (ping) reply id=0x0001, seq=6470/17945, ttl=56
93	3.685352	172.217.162.67	192.168.1.5	ICMP	106	Echo (ping) reply id=0x0001, seq=6471/18201, ttl=56
94	3.685352	65.55.252.169	192.168.1.5	TCP	56	443 → 55034 [FIN, ACK] Seq=526 Ack=2 Win=1026 Len=0
95	3.685416	192.168.1.5	65.55.252.169	TCP	54	55034 → 443 [ACK] Seq=2 Ack=527 Win=254 Len=0
96	3.745232	192.168.1.5	172.217.162.67	ICMP	192	Echo (ping) request id=0x0001, seq=6473/18713, ttl=128 (no response found!)
97	3.746099	172.217.162.67	192.168.1.5	ICMP	106	Echo (ping) reply id=0x0001, seq=6472/18457, ttl=56
98	3.762186	172.217.162.67	192.168.1.5	ICMP	106	Echo (ping) reply id=0x0001, seq=6473/18713, ttl=56
99	3.839971	192.168.1.5	172.217.162.67	ICMP	192	Echo (ping) request id=0x0001, seq=6474/18969, ttl=128 (no response found!)
100	3.878968	192.168.1.5	172.217.162.67	ICMP	192	Echo (ping) request id=0x0001, seq=6475/19225, ttl=128 (no response found!)
101	3.879459	172.217.162.67	192.168.1.5	ICMP	106	Echo (ping) reply id=0x0001, seq=6474/18969, ttl=55
102	3.966703	192.168.1.5	172.217.162.67	ICMP	192	Echo (ping) request id=0x0001, seq=6476/19481, ttl=128 (no response found!)
103	3.967451	172.217.162.67	192.168.1.5	ICMP	106	Echo (ping) reply id=0x0001, seq=6475/19225, ttl=55
104	3.984895	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xe2f9540d
105	3.992704	172.217.162.67	192.168.1.5	ICMP	106	Echo (ping) reply id=0x0001, seq=6476/19481, ttl=55
106	3.999604	fe80::95bd:6202:66d…	ff02::2	ICMPv6	70	Router Solicitation from fc:f8:ae:5b:9d:f2
107	3.999723	fe80::95bd:6202:66d…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

En donde podemos ver que muchos de nuestros ping, terminan siendo no respondidos, esto sucede a que Google esta preparado para este tipo de situaciones, y cuando detecta algo que podria considerarse un ataque DDoS, realiza diferentes tecnicas de seguridad para no verse afectados. Un ejemplo puede ser ignorar todo lo que llegue de cierta IP o reenviar el exceso de solicitudes a un servidor de seguridad que se encargara de diseccionar los paquetes, y corroborar su legitimidad y estados.

Conclusión

Es evidente la importancia de las redes hoy en día, tanto para usuarios como para organizaciones que utilizan servidores para proveer servicios o productos, y es en estas organizaciones donde existe un gran riesgo de ataque, ya que gran cantidad de datos personales dependen de ellos, como por ejemplo información personal, cuentas bancarias, etc; Por lo que existe una lucha día a día por conseguir una mayor seguridad en los sistemas y evitar daños inducidos por terceros.

Al identificar o describir los posibles ataques en redes, entregamos un amplio conocimiento para reflexionar y examinar aspectos relevantes en las redes y sistemas informáticos, en los que se debe prestar más atención para poder descubrir, identificar y bloquear ataques externos. De esta manera, se da a entender que es posible la alteración de datos o la infiltración a sistemas, debido a que las redes fueron creadas en base a la relación de confianza mutua, así al coexistir diferentes sistemas, es posible vulnerar de diversas maneras mediante las redes, es por esto que hay que ser prudentes y cuidadosos a la hora de entregar nuestra información y establecer una correcta seguridad de los datos en caso de ser parte de una organización.

Referencias

Leyes sobre “Delitos Informáticos. Chile y legislación extranjera”:
https://www.camara.cl/pdf.aspx?prmTIPO=DOCUMENTOCOMUNICACIONCUENTA&prmID=11020

Ataques informáticos:
https://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico

Respuestas ante amenazas:
https://www.akamai.com/es/es/resources/network-attacks.jsp

Legislación informática jurídica:
http://www.informatica-juridica.com/legislacion/chile/

Tipos de ataques e intrusos en las redes informáticas:
https://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

Anexo

Figura 1.

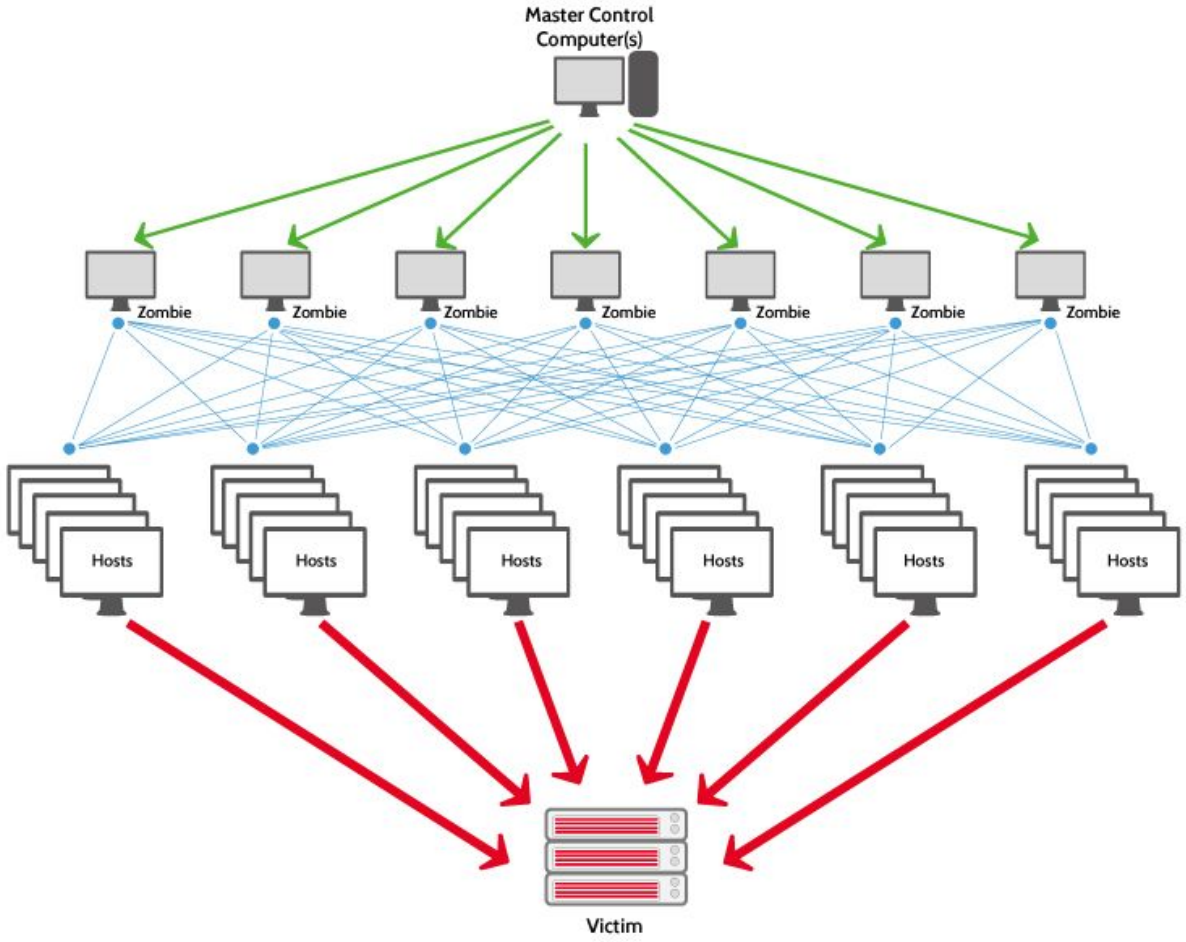


Figura 2.


Call US : 1-800-251-4919 (Toll-Free)
10 SIGNS
YOUR COMPUTER HAS
A VIRUS
1
The computer is really slow.
2
Nothing responds when you click on an icon and/or your software applications do not work correctly anymore.
3
The system reboots, freezes up, or crashes for no reason.
4
Your antivirus security program and/or firewall is suddenly disabled.
5
You can't access your disk drives or hard drive.
6
You are suddenly unable to print.
7
YOUR COMPUTER MAY BE AT RISK
You start seeing strange pop-up windows stating you have a virus or that your computer is infected (the name of the virus program/scanner is something you have not heard of and you can't seem to close the window).
8
WIN BIG!
You start seeing pop-up advertisement windows at unexpected (random) times.
9
DOWNLOADING...
You have major problems trying to install or download an antivirus software or any other software.
10
You seem to have suddenly lost the icons on the desktop and/or all other program files in your folders.