Ciberdefensa-Ciberseguridad Riesgos y Amenazas

CARI

Noviembre 2013

Diferencias en las definiciones

- Ciberguerra: Conflicto en el Ciberespacio.
- Ciberdefensa: Conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición.
- Ciberseguridad: Conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propia y negarlo a terceros.
- Cibercrimen: Acciòn criminal en el ciberespacio.
- Ciberterrorismo: Acción terrorista en el ciberespacio

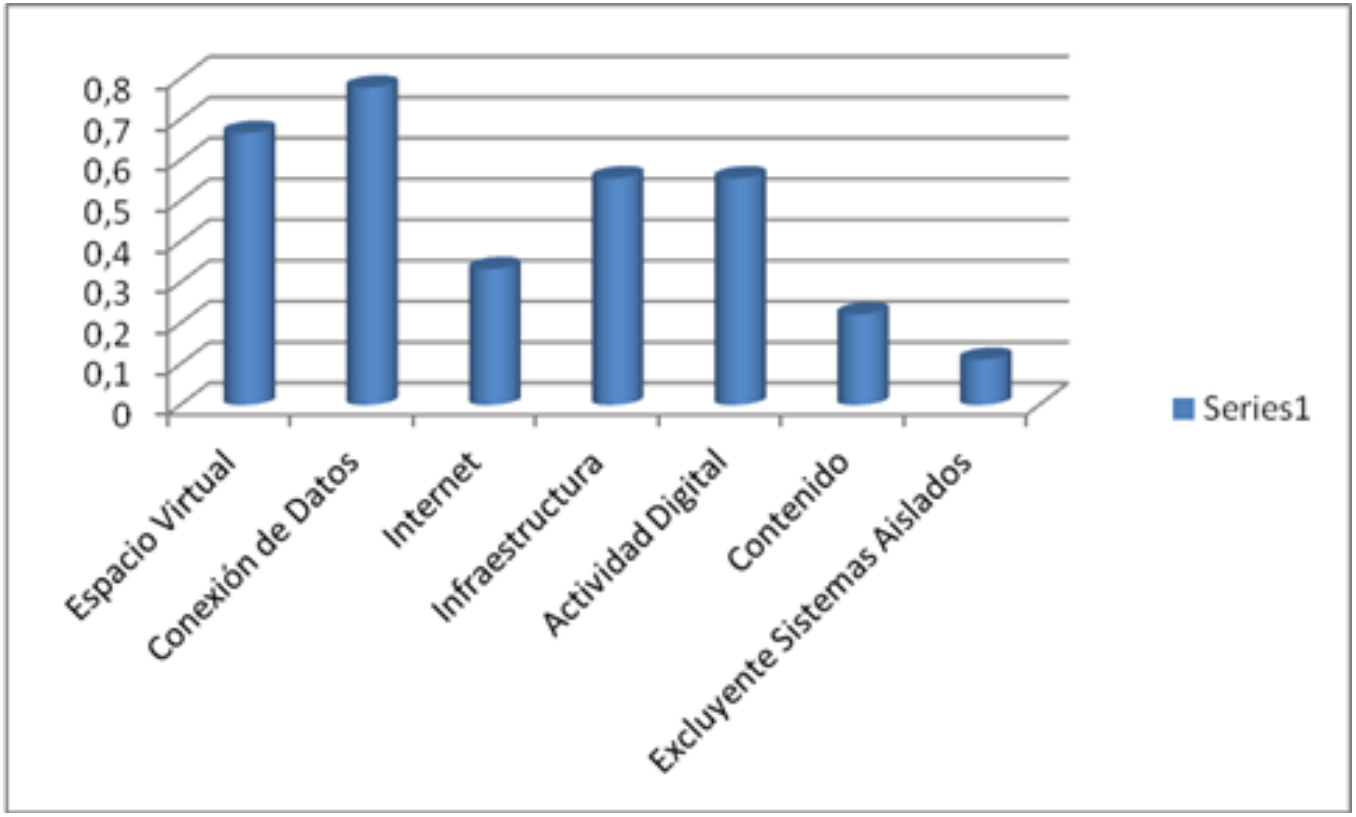
Definición de Ciberdefensa

Ciberdefensa es el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informaticos y teleinformaticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos.

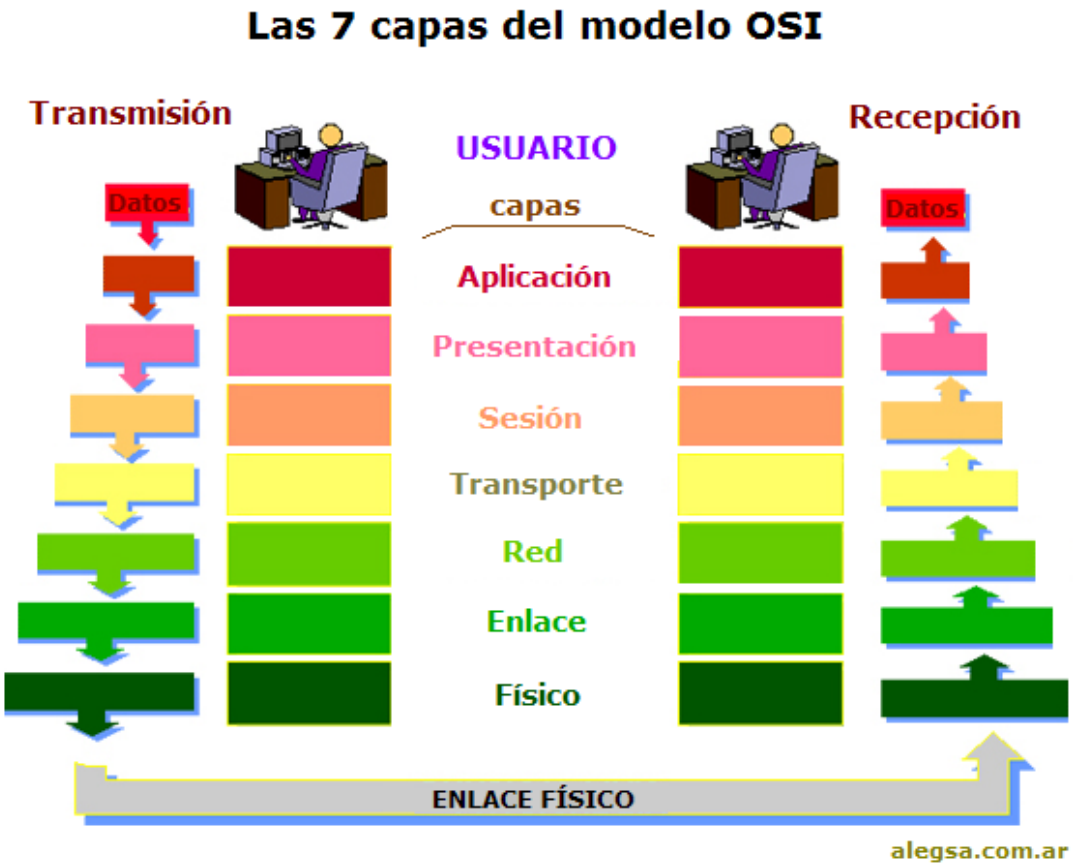
Ciber espacio, definición.

- CIBERESPACIO, es la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos culaesquiera sean estos y las telecomunicaciones que los vinculan.

Incidencia de las definiciones



Integración de Sistemas Abiertos, modelo ISO OSI



Desmitificar la Red.

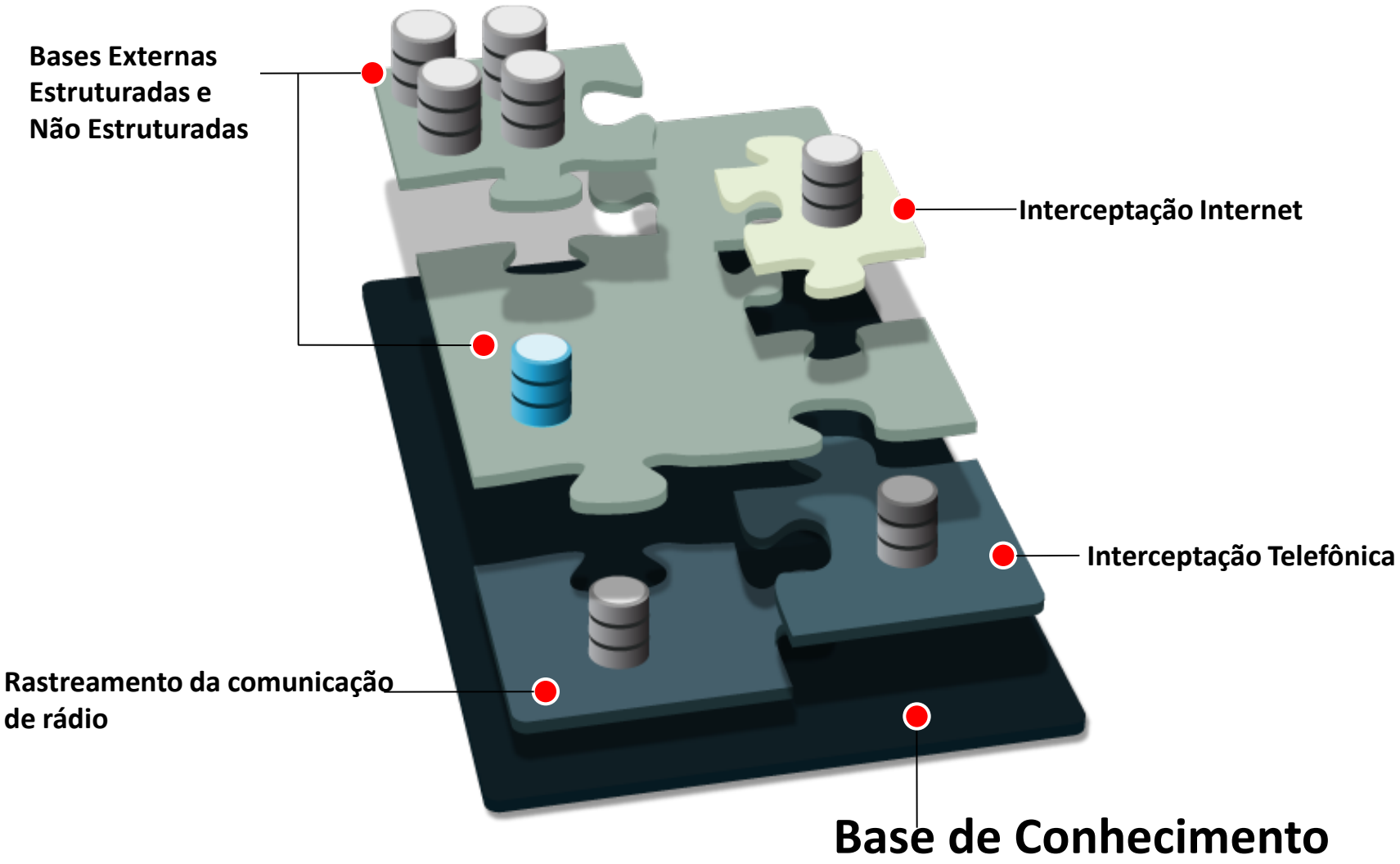
- La red no es gratis, es un negocio
- No es el paradigma de la democracia directa
- La libertad en la red no existe.
- No existe la vigilancia perfecta.
- La privacidad es prácticamente nula (cada vez menor)
- Riesgos de la regulación (Regular que y como)

Web Profunda

La Inteligencia y la Ciberdefensa.

- Se ha planteado iniciar el proceso de la Ciberdefensa por la Inteligencia Informática con el Ciberespacio como ambiente, para poder obtener los elementos descriptores, que conformen la identificación de los escenarios y a la vez parametrizar las amenazas, para poder dimensionar los riesgos y así posibilitar el diseño del los instrumentos de defensa.

Ejemplo de Plataforma de Inteligencia Caso Brasil



¿Vigilancia Global?

- Todos los países hacen inteligencia.
- Brasil conoce perfectamente los riesgos de su conectividad.
- Todos los sorprendidos son complices y conocen de las capacidades que denuncian.
- Costo de los procesos de obtención de información.
- By Pass de redes nacionales
- Planificación de acceso a Big data.
- La Ingeniería Social y las redes sociales.

Caracterización de las Amenazas

Amenazas por el origen

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada un entorno externo, como Internet, no nos garantiza la seguridad de la misma.

De acuerdo con el Computer Security Institute(CSI) de San Francisco aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

Amenazas externas

Amenazas Internas

Amenazas internas:

Generalmente estas amenazas pueden ser más serias que las externas

Los usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos.

Los sistemas de prevención de intrusos o IPS, y *firewalls* son mecanismos no efectivos en amenazas internas por, habitualmente, no estar orientados al tráfico interno.

Amenazas Externas

- Se originan fuera de la red local.
- Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla.
- La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.
- Para clasificarlo como externo debe ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red: rosetas, switches o Hubs accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc.

Amenazas por el efecto

El tipo de amenazas por el efecto que causan a quien recibe los ataques podría clasificarse en:

Robo de información.

Destrucción de información.

Anulación del funcionamiento de los sistemas o efectos que tiendan a ello.

Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc.

Robo de dinero, estafas,...

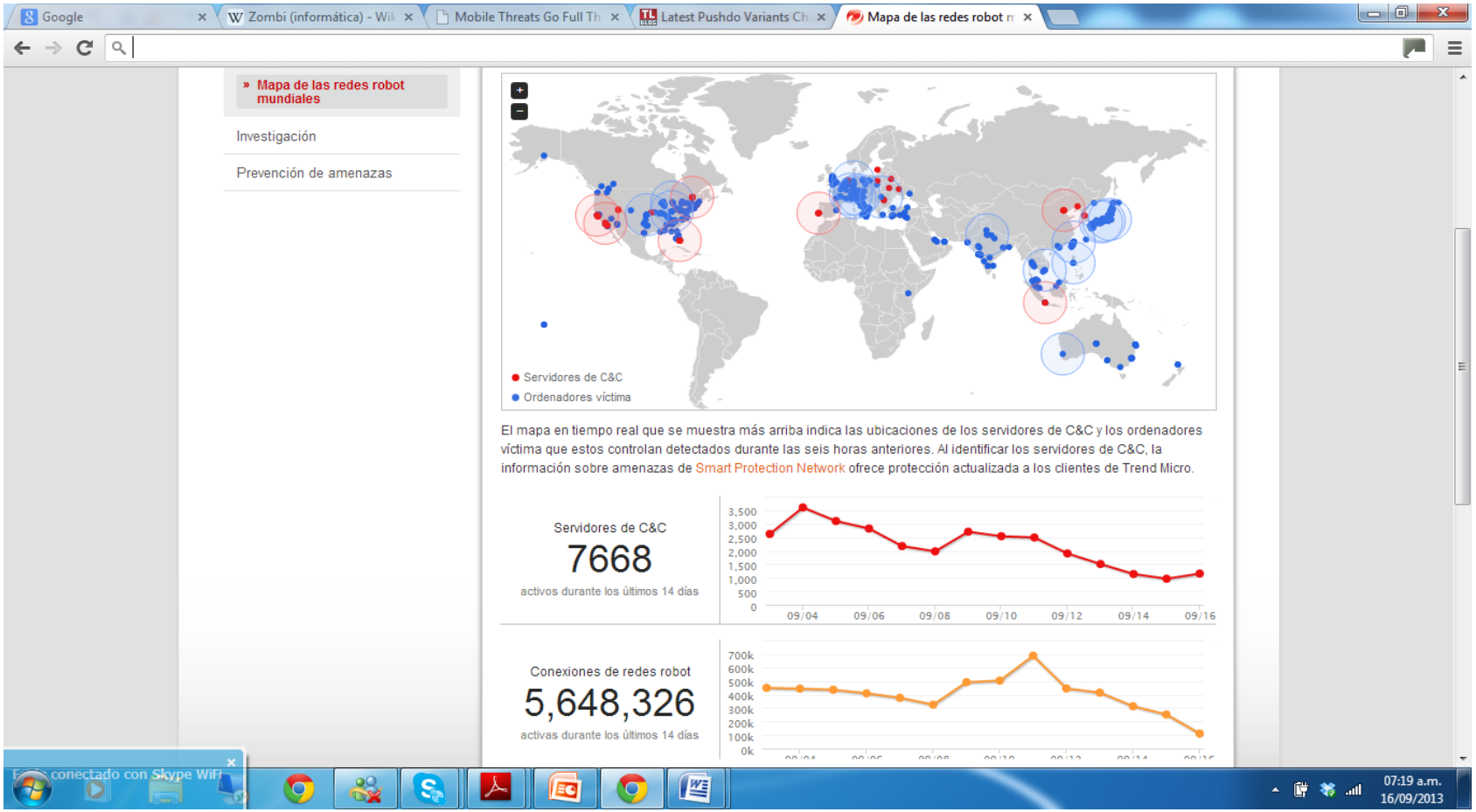
Amenazas por el medio utilizado

Se pueden clasificar por el *modus operandi* del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque

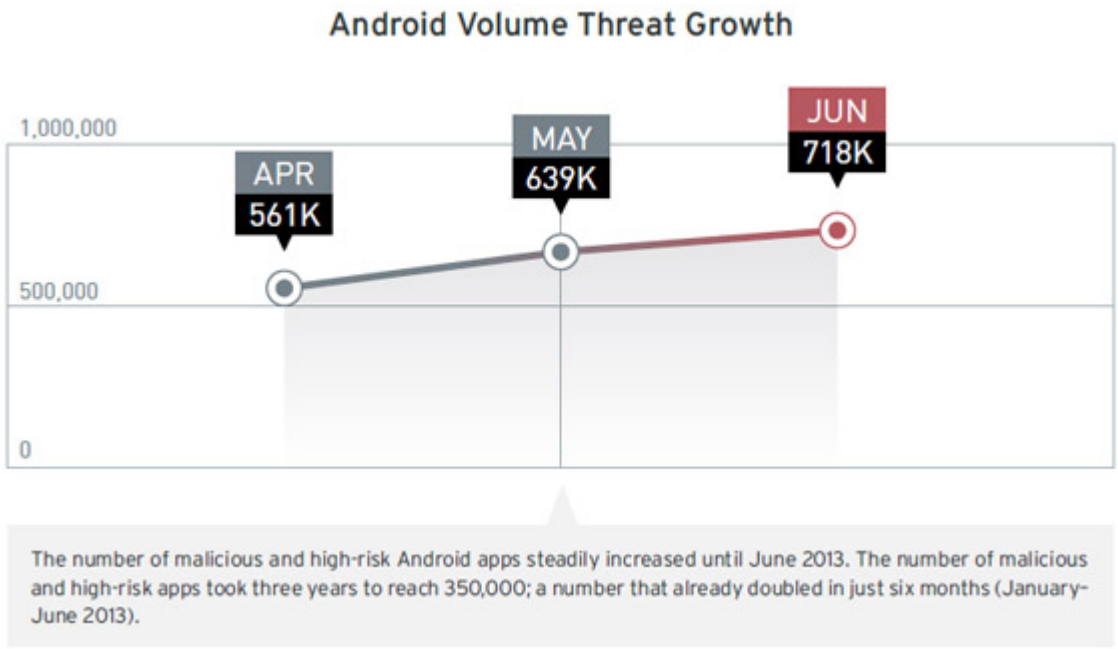
Aquí se clasifican acciones como

- Virus informático: malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.
- Worms
- BOTs
- Adware
- Cookies
- Phishing.
- Ingeniería social.
- Denegación de servicio.
- Spoofing : de DNS, de IP, de DHCP , etc.

Muestra de un monitoreo en tiempo real de redes detectadas y operando el 16 Sep 2013



Crecimiento de las Amenazas en Android de ABRIL a JUNIO 2013

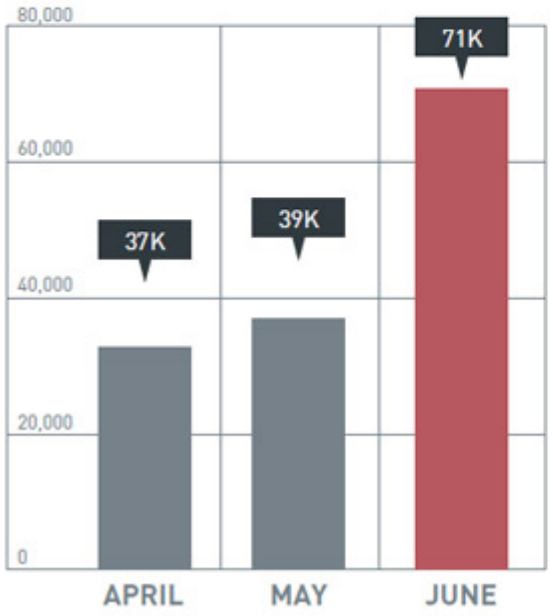


Estadisticas de Malware Bancario 2013

Online Banking Infections

	1Q	2Q
2013	113K	146K

Online Banking Malware Infections



Top Online Banking Victim Countries

COUNTRIES	SHARE
United States	28%
Brazil	22%
Australia	5%
France	5%
Japan	4%
Taiwan	4%
Vietnam	3%
India	2%
Germany	2%
Canada	2%
Others	23%

The online banking malware volume significantly increased this quarter due in part to the rise in the ZeuS/ZBOT malware volume in the wild. Online banking threats are spreading across the globe and are no longer concentrated in certain regions like Europe and the Americas. The United States was most affected by online banking malware, accounting for 28% of the total number of infections worldwide.

Ranking de Vulnerabilidades detectadas

Puesto	Proveedor	Vulnerabilidades comunicadas el T3 de 2012	Proveedor	Vulnerabilidades comunicadas el T2 de 2012
1	Apple	163	Oracle	97
2	Moodle	93	Linux	76
3	Google	72	Google	74
4	Oracle	71	Microsoft	55
5	Mozilla	57	Mozilla	48
6	Cisco	55	Cisco	45
7	IBM	53	IBM	37
8	Ffmpeg	53	Adobe	27
9	Adobe	42	Apple	26
10	Microsoft	35	HP	24

Ranking de Ip de origen malicioso

Puesto	País
1	Arabia Saudí
2	India
3	Turquía
4	Estados Unidos
5	Perú
6	Brasil
7	Corea del Sur
8	Vietnam
9	Colombia
10	China

Ranking de URLs Bloqueadas

Puesto	URL maliciosa bloqueada	Descripción
1	trafficconverter.biz:80/4vir/antispyware/loadadv.exe	Distribuye malware, especialmente variantes de DOWNAD.
2	trafficconverter.biz:80/	Distribuye malware, especialmente variantes de DOWNAD.
3	www.funad.co.kr:80/dynamic/adv/sb/searchnqpopu.html	Introduce riesgos de seguridad en sistemas y/o redes comprometidos.
4	deepspacer.com:80/y2x8ms42fge0otk4y jhmzwu4ztu5y2e4mtfjngewztqxnjmyodczfdmxm a==	Aloja URL maliciosas registradas a nombre de un creador de spam conocido.
5	tags.expo9.exponential.com:80/tags/burstmediacom/audienceselectuk/tags.js	Participa en la distribución de software malicioso.
6	www.trafficholder.com:80/in/in.php	Sitio con tráfico conocido por distribuir malware.
7	mattfoll.eu.interia.pl:80/logos.gif	Distribuye troyanos.
8	www.funad.co.kr:80/dynamic/adv/sb/searchnq_popu.html	Introduce riesgos de seguridad en sistemas y/o redes comprometidos.
9	96.43.128.194:80/click.php	Distribuye troyanos.
10	am10.ru:80/code.php	Aloja adware y mensajes emergentes que redireccionan a sitios de phishing.

Frontera Digital

- Como se Define la Frontera Digital
- Ciudadanía digital
- Titularidad de redes y dominios

¿El ataque de interceptación de celulares es Ciber guerra?

- No, es un caso avanzado de Guerra Electrónica.
- Los casos de validación de terminales en una red de servicio falsa es guerra electrónica aunque se use los medios compartidos con la Cyber Guerra.
- En el caso del smartphone la frontera se diluye.

Batallón de Hackers ¿Para hacer qué?

- Aquí hay un tema básico de contra infiltración, el hacker es un agente encubierto por definición y debe tener un Handler acorde a las capacidades.
- Las motivaciones e incentivos del Hacker deben ser manejados con un alto sentido de lo ético y del deber.
- ES IMPORTANTE EL PLAN DE CAPACITACION DE ESTE PERSONAL Y DE SUS LIDERES.

Cual es la diferencia entre esta Guerra Informática y la Convencional

- Ninguna, solo el conocimiento del escenario.
- No usar protección es como dejar la puerta de calle abierta.
- Securizar una red es como cerrar con llave.
- El hacker busca vulnerabilidades igual que los ladrones.
- Hacer un ataque de distracción es como tirar agua por debajo de la puerta y alguien abre para ver es el momento de mayor vulnerabilidad.
- Un ataque masivo tiene por objeto tirar abajo un servicio o un servidor por saturación de su capacidad de proceso (Es un ataque de demolición).
- Estos son solo algunos ejemplos.

¿Qué implicancias tiene esto?

La necesidad de formar cuadros preparados en las nuevas tecnologías.

Se debe ordenar el relevamiento de este nuevo ambiente y para defenderlo se debe interactuar con distintos organismos del gobierno (Cooperación entre Agencias).

No se debe actuar a las apuradas, ni salir a contratar a un chico amigo que sabe, si no darle un enfoque sistémico y planificado.

Las redes de comunicaciones son objetivos estratégicos de la Nación y por ende debe ponderarse sus capacidades y vulnerabilidades.

¿Por donde empezar?

- Definir los planes de Obtención
- Inventario de los escenarios
- Identificación de actores.
- Cuadros de ligazones
- Metodologías de acceso a red.
- Características de los protocolos de comunicaciones.
- Capacitar, adiestrar y educar al personal en este ambiente de la guerra.
- Establecer Doctrina, técnicas y Procedimientos,

El problema del diseño de las capacidades en la Ciberguerra.

CAPACIDAD

- Es la aptitud o suficiencia de una organización para lograr un efecto deseado en un ambiente dado, dentro de un determinado tiempo, y de sostenerlo por un plazo establecido.
- Esta definición de capacidad proveniente de la publicación conjunta PC20-09
- Para lograr el diseño de las capacidades en cada uno de sus componentes a saber:
  - Recursos humanos
  - Material
  - Infraestructura
  - Logística
  - Información
  - Adiestramiento
  - Doctrina
  - Organización

¿Que hacer primero en Ciberdefensa?

- Es mandatorio primero entender las distintas naturalezas de las amenazas en el ciberespacio en cada uno de los niveles de interconexión y por ende como previo y especial pronunciamiento se entiende que la inteligencia estratégica debe nutrir a la Estrategia Nacional de los elementos que puedan constituir una amenaza a la Nación en el marco específico de este nuevo ambiente de la guerra, a fin de conformar luego las SGP o situaciones Generales de Planeamiento a fin de aportar los nuevos descriptores estratégicos necesarios para la conceptualización de la DEN (Directiva Estratégica Nacional) la DEMIL (Directiva Estratégica Militar) y el PEM (Planeamiento Estratégico Militar)
- La dificultad en este nuevo escenario es la propia característica virtual del ciberespacio y asociado a la duración en el tiempo de conexión de sus características físicas ya no solo ligadas a la geografía e infraestructura física y eléctrica (que solo constituye la primera capa del modelo de interconexión de sistemas) si no a las estructuras lógica, de red, de transporte, de sesión y de aplicación y presentación que definen su existencia para cada una de las parametrizaciónes particulares y cambiantes de cada uno de esos niveles, lo que hace necesario la definición sistemática de la categorización de la amenaza en los términos que acompañan a cada uno de los niveles referidos.

- Es así entonces que sin esta tarea previa de la Inteligencia estratégica no es posible dotar a la DEMIL del material básico para formular las orientaciones que permitan.
- a)Identificar las efectos a lograr para neutralizar las amenazas en cada nivel del ciberespacio
- b)Definir las aptitudes para lograr dichos efectos.

Conclusiones

- Esta guía básica indica como empezar y que información se debe comenzar a relevar.
- Es importante comenzar a elaborar los planes de capacitación y adiestramiento en técnicas y tácticas con un enfoque sistémico de la Ciberdefensa
- Iniciada la colección de información, se seguirá con el registro, clasificación y análisis de la misma, de manera tal que resulte útil al sistema de la Defensa, puesto que el Ciber Ataque, puede vulnerar objetivos de valor estratégico nacional y dejar al país sin capacidad de Comando y control en cualquiera de sus áreas ejecutivas.
- En el Ciber Espacio no hay un limite geográfico claro y el teatro de operaciones son las redes globales interconectadas.