Elementos de ciberguerra en redes WAN

Integrantes

Marcos Betancor - 37.948.600
Jonatan Gimenez - 35.137.586
Gabriel Cascallares - 37.376.896
Diego Salas - 35.793.412

Objetivo

Analizar el creciente escenario conflictivo de la ciberguerra. La ciberguerra como nuevo campo de batalla, los ataques, y las contramedidas.

Índice

1. La Ciberguerra: Introducción

1.1 Introducción

Con el paso de los años el concepto de guerras tal y como lo conocíamos ha cambiado, actualmente en una guerra es más factible derrotar al enemigo atacando su infraestructura informática, que empleando cualquier otro tipo de ataque físico. Esta estrategia ha sido empleada en diversas situaciones, ya sea en ofensivas militares de un país contra otro, de un grupo armado en contra del gobierno, o simplemente ataques individuales de uno o varios hackers.

Podemos considerar que ahora las armas son los virus informáticos y programas especiales para anular la seguridad de los sistemas informáticos y los combatientes son los expertos en informática y telecomunicaciones. Generalmente, los blancos de los ataques son los sistemas financieros, bancarios y militares, aunque se han visto numerosos casos donde se ven afectados los sistemas de comunicación.

Actualmente estos ataques han aumentado considerablemente en número y envergadura. Uno de los ataques más comunes es el envío de gran cantidad de llamadas simultáneas a un servidor, que exceden su capacidad de respuesta y logran paralizarlo, estos son los llamados ataques de denegación de servicio (DDoS).

Otro tipo de ataque, es el "envenenamiento de DNS", que penetra en el servidor de los nombres de dominio para llevar al usuario hacia un servidor planeado por el hacker. Otra forma de realizar estos ataques es incapacitar el antivirus, dejando desprotegido el sistema, luego se envían gusanos mediante el correo electrónico o a través de archivos compartidos en la red.

Pero se considera más peligroso a la propagación de datos confidenciales a través de la red, ya que dicha información puede comprometer a la nación a que pertenece, y en muchas ocasiones ésta se ve comprometida frente a dichos ataques, o también corre peligro de ser eliminada información vital.

1.2 Conceptos básicos

En este apartado definiremos algunos conceptos básicos necesarios para comprender el funcionamiento de la ciberguerra y el ámbito en donde se desarrolla la misma.

Ciberespacio: podríamos definirlo como un espacio virtual creado con medios cibernéticos. Es un entorno esencialmente virtual, es decir, no físico e intangible, que se desarrolla gracias a la unión de los equipos de cómputo en redes informáticas que permiten a los usuarios interactuar con otros individuos con acceso a estas tecnologías.

Ciberseguridad: es el conjunto de herramientas, políticas, conceptos de seguridad, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno.

Ciberataque: es cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones que atacan a sistemas de información como lo son infraestructuras, redes computacionales, bases de datos, con el fin de tomar el control de los mismos, desestabilizarlos o dañarlos.

Ciberdefensa: es el conjunto de recursos, actividades, tácticas y procedimientos para preservar la seguridad de los sistemas y la información que manejan, a su vez incluyen la respuesta a las acciones ocasionadas en un ciberataque, también como la prevención y detección de los mismos.

Ciberdelincuencia: es cualquier tipo de actividad en la que se utilice Internet, una red privada o pública o un sistema informático doméstico con objetivos como destruir o dañar ordenadores, medios electrónicos y redes de Internet.

Los delitos informáticos se pueden dividir en dos grupos:
*Informática como objeto del delito: Esta categoría incluye por ejemplo el sabotaje informático, la piratería informática, el hackeo, el crackeo y el DDNS (Denegación de servicio de nombres de dominio).

*Informática como medio del delito: Dentro de este grupo se encuentra la falsificación de documento electrónico, cajeros automáticos y tarjetas de crédito, robo de identidad, fraudes electrónicos y pornografía infantil.

1.3 Impacto de los ataques.

Considerando el ciberespacio como una colección de recursos, los actores implicados (estados, negocios, organizaciones, grupos o individuos) competirán por controlarlo. Esto nos lleva a conflictos en el ciberespacio. Se puede definir el ciber conflicto como una confrontación entre dos o más partes, donde al menos una parte utiliza los ciberataques contra el otro. Los delincuentes buscarán ingresos ilegales, de modo que secuestran parte del ciberespacio. Los servicios de inteligencia buscan información útil para atacar a partes enemigas, amistosas o neutrales del ciberespacio para obtener acceso a esa información. Los militares buscan interrumpir las operaciones del enemigo, por ello atacan sistemas de sensores, logísticos, de comunicaciones y control en el ciberespacio enemigo. Los conflictos

pueden ser tan simples como disputas civiles sobre la propiedad de un nombre de dominio o más complejos como campañas deliberadas de ciberataques como parte de la guerra convencional entre estados avanzados tecnológicamente.

Dado que los ciber conflictos son inevitables, se pueden establecer varias implicaciones desde la variable tiempo de la que depende el ciberespacio. Esta dependencia del tiempo se puede explicar cómo el cambio en la estructura y contenido del ciberespacio a lo largo del tiempo. El tiempo en el ciberespacio puede ser relativamente corto: minutos, a menudo incluso segundos o fracciones de segundo. Basándose en esto, se pueden deducir implicaciones como el potencial de los rápidos desarrollos de acciones ofensivas y defensivas, la viabilidad de trazar el mapa del ciberespacio y la necesidad de patrullarlo y reconocerlo constantemente. Los cambios rápidos en el ciberespacio implica que se necesita poco tiempo para realizar un ataque o para implementar nuevas defensas, comparado con el espacio físico. Un gusano de red que se auto-replica puede infectar enormes partes del ciberespacio en cuestión de minutos.
En el lado defensivo, en el ciberespacio es posible mejorar las defensas en segundos o minutos implementando nuevas reglas de cortafuegos, por ejemplo. Construir un nuevo búnker en el espacio físico consume mucho más tiempo. Esto no significa que levantar defensas en el ciberespacio se haga siempre en minutos. Simplemente señala que es posible desplegar medidas defensivas preparadas (reglas más restrictivas de cortafuegos, enrutado y alojamiento alternativo, etc.) en menor tiempo. Al preparar un ciber conflicto es necesario conocer el terreno de la zona potencial de conflicto, las capacidades defensivas y ofensivas de los actores y la posibilidad de daños colaterales y escaladas no planificadas. Por la naturaleza del ciberespacio, es difícil hacer esto, ya que el entorno es complejo y está en constante cambio. Los objetivos críticos, los usuarios y la información clave pueden cambiar en segundos.

Hoy día y los próximos años, nos encontramos con la implantación creciente del Internet móvil y la consiguiente proliferación de dispositivos móviles (acceso mediante todo tipo de dispositivos, teléfonos inteligentes, tabletas, libros electrónicos, microordenadores netbooks, ordenadores think (con poca memoria y capacidad de proceso conectados a La Nube) consolas de videojuegos, acceso desde todo tipo de medios de comunicación, automóviles, trenes, aviones, barcos, etc.), de las tecnologías cloud computing, la virtualización, o el avance imparable de las redes sociales y de los restantes medios sociales como blogs o wikis.

Todo esto unido a la difusión cada día mayor de las nuevas tecnologías como la geolocalización, realidad aumentada, la Web en tiempo real o el Internet de las cosas están configurando grandes cambios sociales que afectarán significativamente a la capacidad de los departamentos de TI para mantener la seguridad de la Red.

Los cibercriminales están aprovechándose de las innovaciones tecnológicas para agilizar sus propias operaciones delictivas; por ejemplo, el uso creciente de las redes sociales y cómo los terroristas se están sumando a dichas redes sociales que se han convertido en terreno de juego para los cibercriminales con un creciente número de ataques.

En cuanto al de las amenazas, la ingeniería social y la mezcla de tecnologías por parte de los usuarios son cada vez más peligrosas para la ciberseguridad. Está cada vez más al alza los ataques que combinan diferentes soportes (correo-e, web, voz, vídeo.) para encontrar fisuras. Los cibercriminales y los ciber terroristas siguen atacando sitios web legítimos de forma planificada, a la vez que gestionan ataques de spam controlados (ataques multivectoriales) preparados para actuar en un momento concreto y enfocados en establecer keyloggers (programas capturadores de teclado), bots y puertas traseras. Todo esto hace que la situación actual, con las nuevas tecnologías e internet sean un campo de operaciones magnífico para la ciberguerra.

2. Contexto actual, escenarios y casos.

2.1 Ciberguerra mundial.

En lugar de guerra hablamos de ciberguerra mundial. Ya no se lanzan bombas, sino informes y noticias extraídas de servidores ajenos con técnicas de infiltración. En vez de fábricas y cuarteles, ahora se destruyen reputaciones y carreras políticas. También se bloquean páginas web. En lugar de ocupar territorios, los objetivos son manipular elecciones, sabotear plantas industriales, controlar a opositores o robar secretos, tecnológicos o militares.

Estamos inmersos en una presunta ciberguerra mundial. Según algunos desde 2010, el año en el que se descubrió al gusano Stuxnet. O quizá fue desde 2003, cuando EEUU acusó a China de los ataques informaticos conocidos como Titan Rain. Aunque sí es complicado fijar el supuesto inicio de la ciberguerra, aún más difícil es describir a los bandos en conflicto.

En los ataques han participado estados contra su propia población, grupos activistas. También bandos combatientes en guerras convencionales, redes criminales, crackers individuales, empresas mercenarias, unidades de servicios de inteligencia e incluso ejércitos, entre otros.

Ahora las agencias estadounidenses de espionaje acusan a Rusia de interferir en las elecciones presidenciales. Algo que para los ganadores no son más que excusas de mal perdedor. En todo caso se trataría tan sólo de la última andanada en un conflicto que dura ya lustros.

En esta ciberguerra mundial desde luego ataques no faltan. Entre las víctimas de robos de información o ataques de denegación de servicio hay redes militares y estatales de países como EEUU, China, Rusia. India, Alemania, Irlanda, Corea del Sur o Estonia. En algunos casos en conjunción con guerras convencionales como en Georgia o Ucrania.

También hay empresas u organizaciones que han sido espiadas y han visto publicada su información interna por razones políticas. Como en el caso Climategate, los datos de la NSA publicados por Edward Snowden, los correos internos de Sony o las empresas de tarjetas de crédito que boicotearon a WikiLeaks, atacadas por Anonymous. En ocasiones se han usado sofisticados gusanos informáticos de origen desconocido como Falme, Stars, Duqu o Careto. Este último de posible origen español.

2.2 Los cinco escenarios de ciberguerra.

1. EEUU y China.

La curiosa relación entre China y los Estados Unidos, los ha llevado a una constante tensión que ni puede ser declarada abiertamente ni se manifiesta más allá de esa guerra oculta que se libra en las redes. Mientras tanto, lugares públicos como el "Foro de la Industria de Internet China y Estados Unidos", acogen calurosas declaraciones de intenciones en las que la colaboración contra el crimen y el espionaje son la clave.

Casos como el de Huawei, acusado en el año 2012 de mantener abiertas puertas traseras en sus routers que permitirían un eventual espionaje y acceso a sus infraestructuras por parte del país de origen de estos dispositivos, desató una polémica comercial que pasaría a primer plano informativo al formalizarse la queja por parte de la embajada China a propósito de la campaña contra una de sus mayores empresas tecnológicas.

En 2009, se produciría el ataque conocido como Aurora, que tendría como principal objetivo un Google que se negaba por aquel entonces a aplicar las cláusulas de censura que el Gobierno chino pretendía imponer al buscador. Las cesiones parciales a la censura no serían suficientes para Pekín. Finalmente, Google decidiría abandonar China, que desde entonces elevaría a Baidu como la gran opción de un internet debidamente fiscalizado por las autoridades.

Otro momento comprometido para las autoridades chinas sería la filtración en un documental de corte propagandístico en el que se mostraba la interfaz de un software de ataque que solicitaba una dirección IP desde la que encubrir el origen real de este. En el fotograma, se empleaba la dirección de la Universidad de Alabama, lo que dejaba en mala posición un reportaje que pretendía mostrar a China como víctima.

La sombra de los ciberataques procedentes de China parece siempre seguir unos parámetros que difícilmente podrían apuntar a hackers individuales. Así los sucesivos ataques a empresas, prensa y organismo gubernamentales como la NASA, no dejan de apuntar, aunque si pruebas concluyentes, hacia miembros apoyados por el propio gobierno.

Ciertamente, las informaciones que se deslizan en los medios apuntan a un espionaje organizado y constante por parte de EEUU. La revelación de todo un arsenal de nuevas armas secretas chinas, directamente recogido en informes públicos del Pentágono, no deja lugar a dudas del espionaje que este mantiene. La exactitud de los datos acerca de armas como misiles balísticos orbitales, cazas y sobre todo nuevas herramientas orientadas al ciberespionaje revelan una actividad importante en este sentido.

2. Guerra cibernética contra "Estados enemigos” como Irán o Corea del Norte

Irán, pasando por Siria en su camino, se ha convertido para EEUU e Israel en el próximo objetivo geoestratégico. La aparición de Stuxnet y la intrusión informática en la planta de enriquecimiento de uranio iraní de Natanz en 2010, ha sido uno de los momentos más señalados de todo este proceso. No se trata solamente de que se haya podido acceder desde el exterior al corazón de los sistemas de control de unas instalaciones críticas, sino que el método planteaba una novedad inquietante. Así Stuxnet abría el camino a toda una

nueva generación de virus espía capaz de actuar de forma casi autónoma y con un potencial aterrador.

No sería hasta bastante después, cuando el propio Gobierno estadounidense confirmara la existencia de un arsenal informático preparado para eventuales ataques preventivos, cuando sabríamos que se confirmaba, de forma tácita, que Stuxnet formaba parte de dicha infraestructura. Posteriormente conoceríamos que sería concretamente parte de una colaboración entre EEUU e Israel.

3. Rusia, la ciberdelincuencia y el espionaje

El caso más famoso de ataque de supuestos hackers a una nación fue el de 2007 a Estonia. Por aquel entonces, el país báltico era una de las naciones de mayor penetración digital de occidente. Diversos sistemas fundamentales, entre los que destacaban el sistema bancario y las infraestructuras públicas, desde saneamiento hasta los mismos semáforos, fueron bloqueados durante cerca de dos semanas a consecuencia de la retirada de un monumento identitario para la población rusa que habita el país. Expertos de la OTAN tendrían que acudir para tratar de hacer cesar dicho ataque cuyo origen se ubicaría finalmente en la Federación Rusa.

En el caso ruso también parece ser más cierto que en ningún otro que existen múltiples operadores independientes que se dedican al delito informático sin relación con el Estado. Informes como es de Russian Underground 101, a cargo de Max Goncharov, detalla todas las actividades ilícitas que se realizan en la red y los precios a los que estos cibercriminales profesionales, prestan sus servicios en el mercado negro del hacking ilícito, en foros como antichat.ru, xeka.ru y cardingcc.com.

Grandes estructuras de ciberespionaje como la recientemente desvelada "Octubre Rojo" apunta a nuevas formas de espionaje netamente delictivo con origen ruso. La sofisticación de este software espía es muy grande. Con un periodo de operación de más de cinco años, este software utiliza distintos módulos independientes, con pautas similares al malware Flame, capaz de replicarse de forma oculta y descifrar códigos como ACID, desarrollado por el Ejército francés y que emplea la OTAN y la Unión Europea.

4. Anonymous y el Hacktivismo

Las sucesivas detenciones de diversos individuos que se atribuyen a redes de Anonymous o miembros de LulzSec apenas han conseguido poner freno a las constantes campañas que estos colectivos agrupados bajo un nombre común realizan.

Desde sus primeras operaciones surgidas de 4Chan contra emisoras racistas o la Cienciología, El colectivo Anonymous ha evolucionado hacia una mayor concienciación de su papel como activista por los derechos en Internet. Su apoyo a Wikileaks, en la llamada Operación PayBack, con las primeras acciones contra su bloqueo financiero, los llevarían a saltar definitivamente al primer plano informativo. También aumentarían su base de simpatizantes agregando un perfil mucho más activista y comprometido.

Desde entonces las operaciones de grupos de Anonymous irían incrementándose, sobre todo contra países con censura, organismos, políticos e incluso empresas. Ni siquiera la pederastia quedaría fuera de los ataques del grupo, que realizaría un masivo bloqueo al servidor de la red oculta que más páginas de este tipo empleaba.

El grupo LulzSec, impulsaría un ataque contra la compañía Sony que culminaría con la caída de PlayStation Network y la revelación de buena parte de nombres y claves de usuarios de sus clientes, como consecuencia de la denuncia de Sony contra George Hotz, creador del Jailbreak para iPhone que luego realizaría igualmente para la PlayStation 3. Los cambios de la política de uso de su consola y las restricciones que trataban de imponer a su este volverían a tener consecuencias para esta con sucesivos ataques que culminarían con la apertura final de esta a ser "pirateada" y la consiguiente puesta a disposición de juegos para su descarga.

La legislación que pretendía limitar la piratería y de paso buena parte de las libertades ciudadanas en la red, denominada SOPA, agruparía a buena parte del sector tecnológico. Acompañando a la línea cívica, que finalmente conseguiría tumbar la ley, las operaciones de Anonymous tomarían el nombre de Operación BlackOut y pasarían por ataques a empresas y organismos gubernamentales que apoyaran dicha legislación.

5. Una difusa guerra contra el terrorismo

Podemos afirmar que el yihadismo internacional ha comenzado a ver cómo la actividad en la red puede ser empleada más allá de fuente de reclutamiento y comunicación entre sus miembros. Así grupos como la ciberguerrilla Izz ad-Din al-Qassam, han comenzado a emplear metodologías muy similares a las que emplean grupos como Anonymous para realizar sus acciones en la red. Una de sus formas más recurrentes de ataque ha sido contra bancos estadounidenses. Parece que grupos vinculados a este país son los que dan soporte a este nuevo "comando" que también suele aparecer como QCF (Izz ad-Din al-Qassam Cyber Fighters).

La "lucha contra el terrorismo" se ha convertido en el nuevo comodín del populismo conservador capaz de justificar cualquier legislación una vez modelada oportunamente la opinión pública. La realidad ha demostrado que la mayor parte de las líneas de actuación que se han anunciado públicamente han terminado por tener un empleo bien distinto. Las diversas unidades surgidas a partir de la Patriot Act, después del 11S, demostraron una escasa eficacia a pesar de la ingente cantidad de recursos destinados a estas. El espionaje del activismo dentro de los propios EEUU ha terminado por ser una de las mayores actividades de dichos grupos. En este sentido la ciber yihad parece ser el placebo necesario para mantener una tensión pública lo bastante asustada como para comulgar con una sustracción de derechos de otro modo intolerable.

2.3. Siete de los ciberataques más famosos.

Cada día es más común escuchar sobre ataques cibernéticos a infraestructuras de TI tanto públicas como del sector privado e incluso a cualquier persona que posea un dispositivo. Apenas hace unos días se produjo un ciberataque global de “*ransomware”*, un tipo de código malicioso que cifra los ficheros del ordenador a modo de rehén para solicitar un rescate económico.

Este ataque alcanzó a un centenar de países donde empresas, escuelas e incluso hospitales se vieron afectados. Se habla de un ataque informático sin precedentes. Este ataque se unirá a una ya extensa lista de ciberataques, aquí te presentamos algunos de los más sonados.

Titan Rain (2004)

En 2004, Shawn Carpenter descubrió una serie de "*incursiones cibernéticas*" por parte de lo que, según diera a conocer el FBI, se trataba de células apoyadas por el gobierno chino. Llamado "Titan Rain", durante el ataque los hackers pudieron infiltrarse a varias redes y ordenadores, incluidos los de la NASA.

Considerado uno de los mayores ataques cibernéticos de la historia, en este no sólo se consiguió infiltrar a inteligencia militar y datos clasificados, sino que permitió que otros hackers y entidades de espionaje hallaran la forma de inhabilitar diversas máquinas.

Google China (2009)

En la segunda mitad del 2009, la plataforma Google en China, lanzada apenas tres años antes, sufrió una serie de ciberataques en lo que fuera conocida como Operación Aurora. El ataque robó propiedad intelectual de Google, y no sólo afecto a dicha empresa, sino que otras 30 compañías fueron objeto de este malware. El ataque pretendía tener acceso a cuentas públicas de activistas chinos.

Google, a inicios del 2010, indicó que el ataque no logró su objetivo, y que solamente se había logrado acceder parcialmente a dos cuentas de Gmail. Las infracciones (breaches) provenían de usuarios en Internet Explorer, por lo que los gobiernos de Alemania, Francia y Australia aconsejaron a la población hacer uso de navegadores distintos.

El ataque llevó a Google a revisar sus operaciones en China argumentando que “eso podría tener alcances y consecuencias”. El ataque fue rastreado hasta dos escuelas chinas asociadas a Baidu, el mayor rival de Google en China.

Heartbleed (2012-2014)

Heartbleed no fue un virus, sino un Bug que por error fue escrito en OpenSSL. Esto permitió a los hackers a crear una puerta de entrada hacia diversas bases de datos. Se ha dicho que este es uno de los mayores ciberataques en la historia, pues según algunos reportes sugieren que cerca del 17% de todos los sitios web fueron afectados.

Este ataque permitió que diversos hackers tuvieran acceso a conversaciones privadas sin que los usuarios se percataran, gracias a que implantaron un portal en el sistema para tener acceso en cualquier momento. Pasaron cerca de dos años hasta que el Bug fue finalmente detectado en 2014 por Google Security.

Epsilon (2011)

Uno de los ciberataques que han resultado más costosos en la historia fue el sufrido por Epsilon, el mayor proveedor de servicios de marketing a nivel mundial, entre cuyas empresas a quienes presta servicio se encuentran JP Morgan Chase y Best Buy.

Se estima que el costo por dicho ataque pudo ser de entre $225 millones a $4 mil millones de dólares. Los objetivos de los hackers eran cuentas de correo electrónico para hacer uso de éstas con fines criminales.

PlayStation Network (2011)

A mediados de abril de 2011, Sony dio a conocer que algunas funciones de la PlayStation Network habían sido derribadas. El servicio online de PlayStation se vio afectado por cerca de un mes, en el que 77 millones de cuentas estuvieron sin conexión durante 23 días.

La empresa se vio obligada a comparecer ante la Cámara de Representantes de Estados Unidos y, posteriormente, a pagar una multa de un cuarto de millón de libras al ICO (Information Commissioner's Office) del gobierno británico, por sus malas medidas de seguridad. Sony confirmó que el costó por estos 23 días de interrupción tuvieron un costo alrededor de los 140 millones de libras.

Sony Pictures Entertainment (2014)

Tres años después de las afectaciones a PlayStation Network, los reflectores se pusieron sobre Sony nuevamente, cuando información confidencial de Sony Pictures Entertainment fue filtrada. El autodenominado grupo "*Guardianes de la paz*" se adjudicó el ciberataque, alegando que habían logrado tener acceso a los ordenadores un año antes de que éste se hiciera público.

Los hackers tuvieron acceso a información sobre los empleados de Sony Pictures Entertainment y sus familiares, obteniendo así e-mails, direcciones e información financiera. Otra información obtenida incluía guiones para próximas producciones, así como registros médicos de diversos actores famosos.

Sony empleó 15 millones de dólares para hacer frente a estos ataques, sin embargo, no pudo detener diversas filtraciones. La película "*The Interview"* fue retirada de los cines luego de que los "Guardianes de la Paz" amenazaran con acciones terroristas. El gobierno de Estados Unidos responsabilizó a Corea del Norte por los ataques, aunque el país asiático lo negó.

Yahoo (2012-2014)

A inicios de 2014, Yahoo dio a conocer que cerca de 500 millones de sus usuarios habían sido objeto de ultraje por parte de hackers que se hicieron con información suya.

El ciberataque, el cual fue lanzado un par años antes de que se hiciera público, llevó a que la compañía solicitara a sus usuarios cambiar sus contraseñas si no lo habían hecho antes de aquel año. La información robada incluía contraseñas e información personal, pero no información crediticia.

3. Ataque - Técnicas y metodologías

3.1 Concepto y metodologías principales

Según la RAE, un ataque es la “acción de atacar, acometer o emprender una ofensiva”, por lo tanto, se podría definir un “ciberataque” como la acción de atacar, acometer o emprender una ofensiva en el ciberespacio.
Los ataques cibernéticos o ciberataques aprovechan las vulnerabilidades, ya estén asociadas al software, a los dispositivos informáticos o a las personas que los administran y utilizan. Con el aumento de la complejidad de los sitios web y el rápido desarrollo de aplicaciones, aumenta la posibilidad de sufrir ataques. Mientras tanto, los piratas informáticos y ciber mercenarios crean, distribuyen y utilizan sofisticadas herramientas de exploit y malware para robar o destruir datos empresariales fundamentales, comprometer sitios web e interrumpir estructuras operativas.

Se ha demostrado que actualmente en una guerra es más factible derrotar al enemigo atacando su infraestructura informática, que empleando cualquier otro tipo de ataque físico. Esta estrategia ha sido empleada en diversas situaciones, ya sea en ofensivas militares de un país contra otro, de un grupo armado en contra del gobierno, o simplemente ataques individuales de uno o varios hackers.

Es decir, que ahora las armas son los virus informáticos y programas especiales para anular la seguridad de los sistemas informáticos y los combatientes son los expertos en informática y telecomunicaciones. Generalmente, los blancos de los ataques son los sistemas financieros, bancarios y militares, aunque se han visto numerosos casos donde se ven afectados los sistemas de comunicación.

Durante los últimos años estos ataques han aumentado considerablemente en número y envergadura. Uno de los ataques más comunes es el envío de gran cantidad de llamadas simultáneas a un servidor, que exceden su capacidad de respuesta y logran paralizarlo; son los llamados ataques de denegación de servicio (DDoS).

Otro tipo de ataque, muy semejante al anterior, es el "envenenamiento de DNS", que penetra en el servidor de los nombres de dominio para llevar al usuario hacia un servidor planeado por el hacker y tomar control del dispositivo. Por ejemplo, es el caso de un grupo de hackers que desviaron un satélite militar británico, pidiendo por su restauración una gran suma de dinero.

Otra forma de realizar estos ataques es incapacitar el antivirus, dejando desprotegido el sistema; luego se envían gusanos mediante el correo electrónico o a través de archivos compartidos en la red.

Pero, en nuestra época, lo más peligroso consiste en la propagación de datos confidenciales a través de la red, ya que dicha información puede comprometer a la nación a que pertenece, y en muchas ocasiones ésta se ve comprometida frente a dichos ataques, o también corre peligro de ser eliminada información vital. En este rango caben los ciber arsenales o virus que borran información y se propagan a través del correo electrónico.

También se da el caso de la propagación de información falsa mediante la web, acerca de cualquier tema específico. Esto podría traducirse en falsas especulaciones sobre las posibles causas de algún accidente, o la denuncia basada en falsas fallas a cualquier producto inmerso en la competencia, con el fin de desvirtuar y dañar las ventas de dicho producto.

Estos ataques se pueden dividir en dos partes. **La primera parte es el espionaje convencional**: hackear redes para obtener información. Tanto el espionaje convencional como el espionaje cibernético no se consideran actos de guerra, pero causan tensiones serias. Quizás el caso más famoso es el descubrimiento -gracias a Snowden- de que la NSA espía a una buena cantidad de mandatarios europeos y países.

Por otra parte, tenemos el **sabotaje: ataques directos a la infraestructura** para que dejen de funcionar. Aquí es donde entran los ataques de denegación de servicio o la paralización de infraestructuras críticas.

3.2 Armas de la ciberguerra:

Ataque DoS

En un ataque de denegación de servicio (DoS), un atacante intenta evitar la legitimidad de que los usuarios accedan a información o al servicios.
El tipo más común y obvio de ataque DoS ocurre cuando un atacante "inunda" una red con información. Cuando escribimos una URL de un sitio web en particular
en nuestro navegador, estamos enviando una solicitud al servidor web del sitio para poder ver la página en concreto. El servidor solo puede procesar una cierta cantidad de solicitudes de una vez, por lo que si un atacante sobrecarga el servidor con solicitudes, no puede procesarse dicha solicitud. Esto es una "denegación de servicio" ya que no se puede acceder al sitio y deja inutilizable los servidores.

Síntomas DDoS

- Rendimiento de la red inusualmente lento (abrir archivos o acceder a sitios web)
- Indisponibilidad de un sitio web en particular
- Incapacidad para acceder a cualquier sitio web
- Aumento dramático en la cantidad de spam que recibimos

Tipos de ataques DoS:

Distributed Denial of Service (DDos)

En un ataque distribuido de denegación de servicio (DDoS), un atacante puede usar su computadora para atacar a otra computadora. Al aprovechar las vulnerabilidades o debilidades de seguridad, un atacante podría tomar el control del PC / Servidor. Él o ella podría obligar al PC a enviar grandes cantidades de datos a un sitio web o

enviar correo no deseado a direcciones de correo electrónico particulares. El ataque se "distribuye" porque el atacante está utilizando varios PCs, incluida la suya, para lanzar el ataque de denegación de servicio. Actualmente dichos ataques son lanzados desde las Botnet.

ICMP Flood Attack

Es una técnica DoS que pretende agotar el ancho de banda de la víctima. Consiste en enviar de forma continuada un número elevado de paquetes ICMP Echo request (ping) de tamaño considerable a la víctima, de forma que ésta ha de responder con paquetes ICMP Echo reply (pong) lo que supone una sobrecarga tanto en la red como en el sistema de la víctima.
Dependiendo de la relación entre capacidad de procesamiento de la víctima y el atacante, el grado de sobrecarga varía, es decir, si un atacante tiene una capacidad mucho mayor, la víctima no puede manejar el tráfico generado.

Teardrop Attack

Una serie de paquetes de datos se envían a la computadora destino con superposición de valores de campo y cargas útiles de gran tamaño. Como resultado, el objetivo no puede volver a ensamblar estos paquetes y se fuerza a que se bloquee o incluso a reiniciar.

Smurf Attack

El atacante envía una gran cantidad de solicitudes de eco ICMP a la dirección IP Broadcast. Estas solicitudes ICMP tienen una dirección de origen falsificada de la víctima. Por ello, si el dispositivo de enrutamiento entrega tráfico a esas direcciones de difusión, entrega la transmisión IP a todos los hosts, la mayoría de las direcciones IP envían un Mensaje de respuesta ECHO. Sin embargo, en una red de difusión de acceso múltiple, cientos de computadoras podría responder a cada paquete cuando la red objetivo se vea abrumada por todos los mensajes enviados simultáneamente. La red no podrá funcionar con normalidad.

SYN Flood

La inundación SYN envía una inundación de paquetes TCP / SYN, a menudo con un remitente falsificado en dirección. Cada uno de estos paquetes se maneja como una solicitud de conexión, causando al servidor una conexión semiabierta, mediante el envío de un paquete TCP / SYN-ACK , y esperando un paquete en respuesta de la dirección del remitente. Sin embargo, como la dirección del remitente está falsificada, la respuesta nunca llega. Estos half open en conexiones, saturan la cantidad de conexiones disponibles que el servidor puede hacer, evitando que responda a solicitudes legítimas hasta después de que el ataque termine.

Land Attack

El atacante envía un paquete TCP SYN falsificado en el que la dirección IP de el objetivo se completa en los campos de origen y destino. Al recibir el paquete falsificado, el objetivo se confunde y se bloquea.Estos tipos de ataques son detectados por Antivirus.

Jolt Dos Attack

Un atacante fragmenta el paquete ICMP de tal manera que el objetivo no puede volver a armarlo, como consecuencia, el uso de la CPU aumenta y se crean cuellos de botella y estrechamientos.

Fraggle Dos Attack

El atacante envía una gran cantidad de tráfico de solicitudes de eco UDP a una dirección IP de Difusión. Estos paquetes UDP tienen una dirección fuente falsificada de la víctima prevista. Por ello, si el dispositivo de enrutamiento entrega tráfico a esas direcciones, entrega la transmisión IP a todos los hosts, donde la mayoría de las direcciones IP envían un mensaje de respuesta ECHO. Sin embargo, en una red de difusión de acceso múltiple, cientos de computadoras pueden responder a cada paquete cuando la red objetivo es abrumada por todos los mensajes enviados simultáneamente, y la red será incapaz de trabajar con normalidad

Ping Flood

Ping flood se basa en enviar a la víctima una cantidad abrumadora de paquetes ping, usualmente usando el comando "ping" de UNIX como hosts (el indicador -t en los sistemas Windows tiene una función mucho menos maligna). Es muy simple de lanzar, el requisito principal es tener acceso a un ancho de banda mayor que la víctima.

Escaneo de puertos

El escaneo de puertos es una de las técnicas de reconocimiento más populares que utilizan los atacantes para descubrir los servicios expuestos a posibles ataques. Todas las máquinas conectadas a una red de área local (LAN) o Internet ejecutan muchos servicios que escuchan en puertos conocidos y no tan conocidos. Un escaneo de puertos ayuda al atacante a encontrar qué puertos están disponibles (es decir, qué servicio podría estar enumerando un puerto).
Esencialmente, un escaneo de puertos consiste en enviar un mensaje a cada puerto, uno a uno. El tipo de respuesta recibida indica si el puerto está a la escucha y, por lo tanto, puede probarse más detalladamente para detectar debilidad.

- Puertos conocidos (0 - 1023)
- Puertos registrados (1024 - 49151)
- Puertos dinámicos y / o privados (49152 - 65535)

ARP Spoofing

ARP Poison Routing (APR), es una técnica utilizada para atacar una red cableada o inalámbrica de Ethernet. ARP Spoofing puede permitir que un atacante detecte frameworks de datos en una red de área local (LAN), modifique el tráfico o detenga el tráfico por completo. El ataque solo se puede usar en redes que realmente usan ARP y no en otro método de resolución de direcciones.
La detección la realizamos mediante ARP inverso (RARP) que es un protocolo utilizado para consultar la dirección IP asociada con una dirección MAC dada. Si se devuelve más de una dirección IP, la clonación MAC está presente.

Tipos de ataques ARP Spoofing:

Ataque de inundación MAC:

En un ataque típico de inundación MAC, un switch se inunda con paquetes, cada uno con diferentes direcciones MAC de origen. La intención es consumir la memoria limitada reservada en el switch para almacenar la tabla de traducción de puerto a físico de MAC.
El resultado de este ataque hace que el switch ingrese a un estado llamado modo de apertura fallida, en el cual todos los paquetes entrantes se emiten en todos los puertos (como con un concentrador), en lugar de simplemente hacia abajo del puerto correcto según la operación normal. Un usuario malintencionado podría utilizar un analizador de paquetes (como Wireshark) ejecutándose en modo promiscuo para capturar datos confidenciales de otras computadoras (como contraseñas no encriptadas, correo electrónico y conversaciones de mensajería instantánea), que no serían accesibles si el interruptor funcionará con normalidad.

Envenenamiento de caché DNS

Esta es una situación creada o no intencionalmente creada que proporciona datos a un servidor de nombres de almacenamiento en caché que no se originó en fuentes autorizadas del Sistema de nombres de dominio (DNS). Esto puede suceder a través del diseño incorrecto del software, la mala configuración de los servidores de nombres y los escenarios diseñados maliciosamente que explotan la arquitectura tradicionalmente abierta del sistema DNS. Una vez que un servidor DNS ha recibido datos no auténticos y los almacena en caché para aumentar el rendimiento en el futuro, se considera envenenado, proporcionando los datos no auténticos a los clientes del servidor.

IP Spoofing:

La suplantación de IP se refiere a la creación de paquetes de Protocolo de Internet (IP) con un forjado de dirección IP de origen, llamada suplantación de identidad, con el propósito de ocultar la identidad del remitente o hacerse pasar por otro sistema informático.

ACK flood

Esta es una técnica para enviar un paquete TCP / ACK al objetivo a menudo con una dirección IP falsificada. Es muy similar a los ataques de inundación TCP / SYN

FTP BOUNCE

El atacante puede conectarse a los servidores FTP y tiene la intención de enviar archivos a otros usuarios / máquinas que usan el comando PORT. Para que el servidor FTP intente enviar el archivo a otras máquinas en un puerto específico y verifique que el puerto esté abierto. Es obvio que la transferencia de FTP estaría permitida en los firewalls. En estos días casi todo los servidores FTP se implementan con el comando PORT desactivado.

TCP Session Hijacking

Es el caso cuando el "Hacker" toma la sesión TCP existente, ya establecido entre las dos partes. En la mayoría de las sesión TCP la autenticación ocurre al comienzo de la sesión, los piratas informáticos realizan este ataque en dicho momento.

Man In The Middle

Un ataque MITM ocurre cuando una comunicación entre dos sistemas es interceptada por una entidad externa. Esto puede suceder en cualquier forma de comunicación en línea, como correo electrónico, redes sociales, navegación web, etc. No solo están tratando de escuchar nuestras conversaciones privadas, sino que también pueden dirigir toda la información dentro de los dispositivos.

Un ejemplo sería un hacker entre nosotros (y nuestro navegador) y el sitio web que está visitando para interceptar y capturar cualquier información que enviamos al sitio, como credenciales de inicio de sesión o información financiera.

Ingenieria Social

La ingeniería social es el arte de manipular a las personas para que renuncien a la información confidencial. Los tipos de información que buscan estos delincuentes pueden variar, pero cuando los individuos son blanco, los delincuentes generalmente intentan

engañarlo para que le dé su contraseña o información bancaria, o acceda a su pc para instalar en secreto el software malicioso, que le dará acceso a su contraseñas e información bancaria, así como para darles control sobre el mismo.
Los delincuentes usan tácticas de ingeniería social porque generalmente es más fácil explotar la inclinación natural a confiar que descubrir formas de hackear tu software. Por ejemplo, es mucho más fácil engañar a alguien para que le dé su contraseña que intentar piratear su contraseña (a menos que la contraseña sea realmente débil).
La seguridad se trata de saber en quién y en qué confiar. Saber cuándo y cuándo no hacerlo, para tomar la palabra de una persona; cuándo confiar en que la persona con la que nos estamos comunicando es de hecho la persona con la que piensas que te estás comunicando; cuándo confiar en que un sitio web es o no es legítimo; cuándo confiar en que la persona que está hablando por teléfono es o no es legítima; cuando proporcionar nuestra información es o no es una buena idea.
Pregúntele a cualquier profesional de la seguridad y te dirán que el eslabón más débil en la cadena de seguridad es el ser humano que acepta a una persona o un escenario al pie de la letra. No importa cuántas cerraduras y cerrojos hay en nuestras puertas y ventanas, o si tenemos perros guardianes, sistemas de alarma, reflectores, cercas con alambre de púas y personal de seguridad armado; si confiamos en la persona de la puerta que dice que él es el repartidor de pizzas y lo dejamos entrar sin verificar primero si es legítimo, estamos completamente expuesto a cualquier riesgo que represente dejarle entrar.

OS Fingerprinting

El término "huella digital del sistema operativo" / OS Fingerprinting en Ethical Hacking se refiere a cualquier método utilizado para determinar qué sistema operativo se ejecuta en una computadora remota. Al analizar ciertos indicadores de protocolo, opciones y datos en los paquetes que un dispositivo envía a la red, podemos hacer conjeturas relativamente precisas sobre el sistema operativo que envió esos paquetes. Al identificar el sistema operativo exacto de un host, un atacante puede lanzar un ataque preciso contra una máquina destino. En un mundo de desbordamientos de búfer, conocer el sabor y la arquitectura exactos de un sistema operativo podría ser toda la oportunidad que un atacante necesita.

Keyloggers

Un keylogger puede ser un programa de software o un hardware que utiliza un atacante para registrar las pulsaciones de teclas en el teclado de un usuario. Con un Keylogger, un atacante puede conocer remotamente sus contraseñas, números de tarjetas de crédito / débito, mensajes, correos electrónicos y todo lo que escriba.
Es más probable que los registradores de pulsaciones de teclas estén basados en software que en hardware, ya que estos últimos requerirían acceso físico al dispositivo.
Los registradores de pulsaciones basados en software generalmente infectan el sistema en forma de un malware que un usuario podría haber descargado haciendo clic en un enlace malicioso, ya sea en línea o enviándolo por correo electrónico.

Un software de captura de teclas se ejecuta en segundo plano sin notificar al usuario y tomará nota de cada golpe de teclado y luego lo alimentará a un servidor en línea al que puede acceder el atacante.
Revisar todo el historial de registros de teclas puede brindarle a cualquiera una idea de los sitios web que visitó y la información que ingresó en ellos, lo que le da una forma fácil de acceder a la tarjeta de crédito o credenciales de banca por Internet. Los ataques de teclado son utilizados por los atacantes con intención maliciosa de monitorear las pulsaciones de teclas, siendo importante protegerse contra ellos, para que no seamos vulnerable a perder información de identificación personal, incluidas las credenciales personales o corporativas.

Virus

Un virus informático es un programa informático que puede copiarse e infectar una computadora. El término "virus" también se usa comúnmente pero erróneamente para referirse a otros tipos de malware, incluidos, entre otros, los programas de adware y spyware que no tienen la capacidad reproductiva. Un virus verdadero puede propagarse de una computadora a otra (en algún tipo de código ejecutable) cuando su host se lleva a la computadora de destino; por ejemplo, porque un usuario lo envió a través de una red o Internet, o lo llevó en un medio extraíble, como una unidad USB.

Gusanos

Un gusano informático es un programa informático de malware autoreplicante. Utiliza una red informática para enviar copias de sí mismo a otros nodos (computadoras en la red) y puede hacerlo sin intervención del usuario. Esto se debe a deficiencias de seguridad en la computadora de destino. A diferencia de un virus, no es necesario que se una a un programa existente. Los gusanos casi siempre causan al menos algún daño a la red, al consumir ancho de banda, mientras que los virus casi siempre corrompen o modifican archivos en una computadora específica.

Malware

Malware es una forma corta de software malicioso. El malware no es lo mismo que el software defectuoso, es decir, el software que tiene un propósito legítimo pero contiene errores dañinos. El malware incluye virus informáticos, gusanos, caballos de Troya, spyware, adware deshonesto, software delictivo, la mayoría de los rootkits y otro software malicioso y no deseado.

Spyware

El software espía es un tipo de malware que se instala en las computadoras y recopila pequeñas porciones de información a la vez sobre los usuarios sin su conocimiento. La presencia de spyware generalmente está oculta para el usuario y puede ser difícil de detectar. Normalmente, el spyware se instala secretamente en el PC personal del usuario. A veces, sin embargo, los spywares cómo keyloggers son instalados por el propietario de un PC compartido, corporativa o pública a propósito para monitorizar en secreto a otros usuarios.

Troyanos

Un troyano, a veces denominado caballo de Troya, es un malware no autorreplicante que parece realizar una función deseable para el usuario pero que en cambio facilitar el acceso no autorizado al sistema informático del usuario.

Rootkit

Un Rootkit es un tipo de software que está diseñado para obtener el control de nivel de administrador sobre un sistema informático sin ser detectado. En prácticamente todos los casos, el propósito y el motivo es realizar operaciones maliciosas en un sistema informático host objetivo en una fecha posterior sin el conocimiento de los administradores o usuarios de ese sistema. Los Rootkit se pueden instalar en hardware o software dirigidos en la BIOS, hipervisores, cargadores de arranque, kernel o, con menor frecuencia, bibliotecas o aplicaciones.

Ransomware

Un ransomware (del inglés ransom, ‘rescate’, y ware, por software) es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

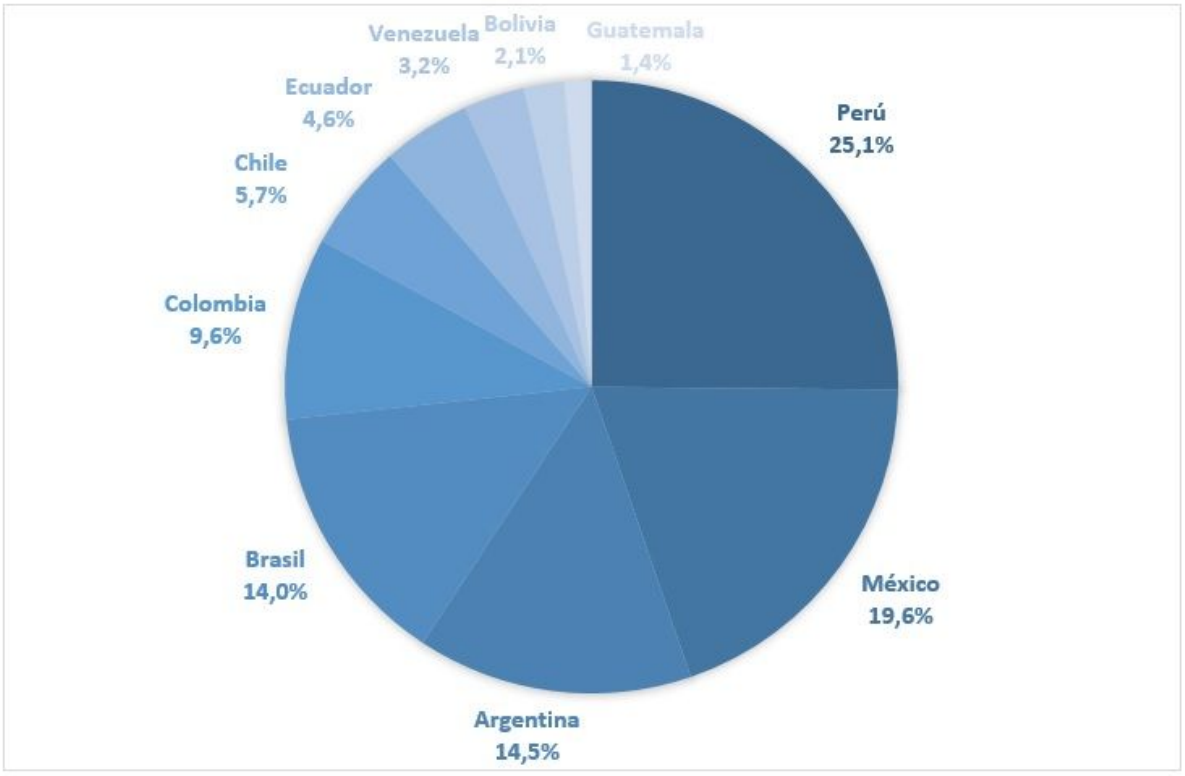
Aunque los ataques se han hecho populares desde mediados de la década del 2010, el primer ataque conocido sucedió a finales de los '80s por parte del Dr. Joseph Popp. Su uso creció internacionalmente en junio del 2013. La empresa McAfee señaló que solamente en el primer trimestre del 2013 había detectado más de 250 000 tipos de ransomware únicos.

Normalmente un ransomware se transmite como un troyano o como un gusano, infectando el sistema operativo, por ejemplo, con un archivo descargado o explotando una vulnerabilidad de software. En este punto, el ransomware se iniciará, cifrará los archivos del usuario con una determinada clave, que sólo el creador del ransomware conoce, e instará al usuario a que la reclame a cambio de un pago.

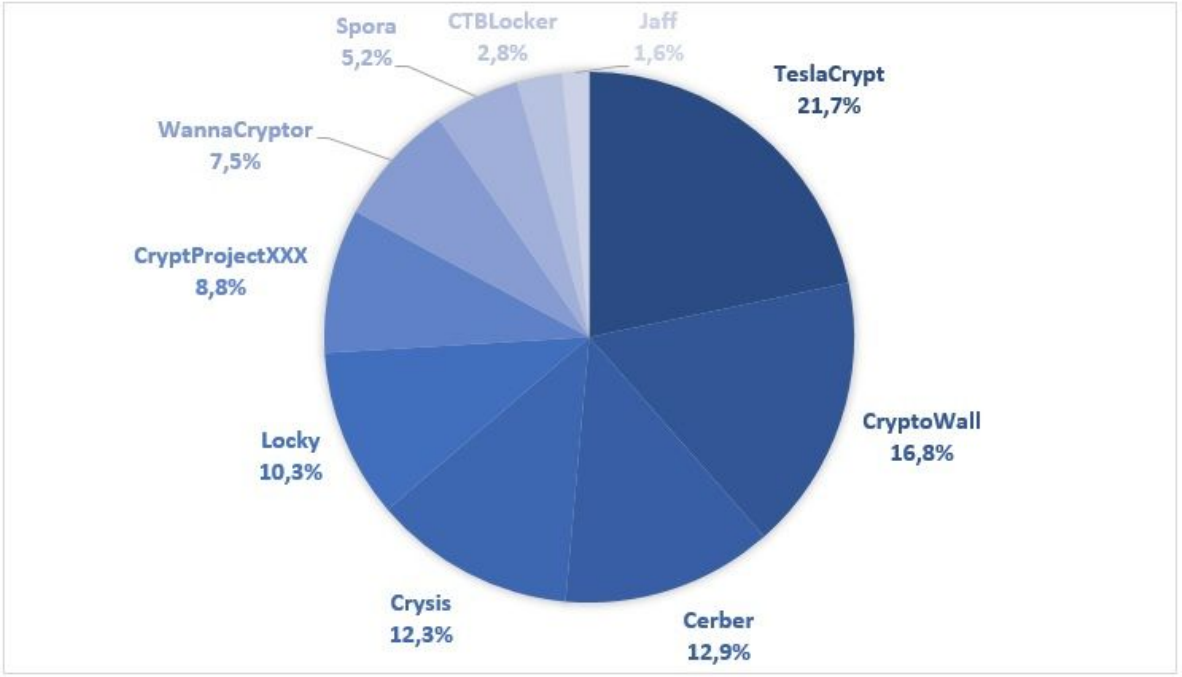
Los ataques más peligrosos los han causado ransomware cómo WannaCry, Petya, Cerber, Cryptolocker y Locky.

En el top 5 encontramos que **TeslaCrypt** es el ransomware más detectado en Latinoamérica, con el 21,7% de los registros; seguido de CryptoWall (16,8%), Cerber (12,9%), Crysis (12,3%) y Locky (10,3%).

El siguiente gráfico muestra el nivel de incidencia de diferentes tipos de Ransomware (File Coders) en diferentes países de Latinoamérica.



Y en el gráfico debajo, qué tipos de Ransomware tuvieron más actividad en la región.



Ataques a Aplicaciones Web

Inyección SQL:

También se denomina Ataque de Inserción SQL que ayuda al hacker a ejecutar un código debido a la presencia de vulnerabilidad en la capa de la base de datos de la Aplicación. En consecuencia, el código obtendrá datos confidenciales o incluso comprometerá la aplicación en sí.

Cross-Site Request:

La falsificación de solicitudes entre sitios, también conocida como ataque con un solo clic o sesión y abreviado como CSRF ("sea-surf") o XSRF, es un tipo de exploit malicioso de un sitio web mediante el cual se transmiten comandos no autorizados de un usuario en el que el sitio web confía. A diferencia de los scripts de sitios cruzados (XSS), que explota la confianza que un usuario tiene para de un sitio en particular, CSRF explota la confianza que un sitio tiene en el navegador de un usuario.

Ataque de envenenamiento de cookies:

Los ataques de envenenamiento de cookies implican la modificación de los contenidos de una cookie (información personal almacenada en la computadora de un usuario web) para eludir los mecanismos de seguridad. Al usar ataques de envenenamiento de cookies, los atacantes pueden obtener información no autorizada sobre otro usuario y robar su identidad.

Robo de cookies:

Este tipo de ataques se realizan mediante scripts del lado del cliente como JavaScript. Cuando el usuario hace clic en un enlace, el script buscará la cookie almacenada en la memoria de la computadora para todas las cookies activas y las enviará (al parecer, los correos electrónicos) al atacante.

Ataques de phishing:

Phishing es el proceso criminalmente fraudulento de intentar adquirir información sensible como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una entidad confiable en una comunicación electrónica.

Web Defacement:

La desfiguración del sitio web es un ataque a un sitio web que cambia la apariencia visual del sitio. Estos son típicamente el trabajo de los crackers del sistema, que entran en un servidor web y reemplazan el sitio web alojado con uno propio. Lo más

probable es que este tipo de ataques se hagan intencionalmente para arruinar la reputación de la compañía que ha alojado este sitio web.

Buffer Overflow:

El desbordamiento de búfer, o el desbordamiento del búfer, es una anomalía en la que un proceso almacena datos en un búfer fuera de la memoria que el programador reservó para ello. Los datos adicionales sobrescriben la memoria adyacente, que puede contener otros datos, incluidas variables de programa y datos de control de flujo del programa. Esto puede provocar errores de acceso a la memoria, resultados incorrectos, finalización del programa o una violación de la seguridad del sistema. Esta vulnerabilidad es completamente un error del Programador.

Navegación forzada:

La exploración forzada es un ataque cuyo objetivo es enumerar y acceder a los recursos a los que la aplicación no hace referencia, pero que aún son accesibles. Por ejemplo, directorios como config, backup, logs a los que se puede acceder pueden revelar mucha información sobre la aplicación en sí, contraseña, actividades, etc.

División de respuesta HTTP:

Un atacante pasa datos maliciosos a una aplicación vulnerable, y la aplicación incluye los datos en un encabezado de respuesta HTTP. Este ataque en sí no causa ningún daño, pero daría lugar a otros ataques sensibles como XSS.

Defectos de inyección:

Las fallas de inyección permiten a los atacantes retransmitir código malicioso a través de una aplicación web a otro sistema. Estos ataques incluyen llamadas al sistema operativo a través de llamadas al sistema, el uso de programas externos a través de comandos del shell, así como llamadas a bases de datos de backend a través de SQL (es decir, inyección de SQL). Los scripts completos escritos en Perl, Python y otros lenguajes pueden ser inyectados en aplicaciones web mal diseñadas y ejecutado. Cada vez que una aplicación web utiliza un intérprete de cualquier tipo, existe el peligro de un ataque de inyección.

4. Defensa. Técnicas y estrategias

4.1 Ciberdefensa. Técnicas

Las técnicas para defenderse ante ataques realizados por grupos organizados consisten en adaptarse a las agresiones conocidas. También se realizan simulacros de diversos tipos de ataques.

Para realizar estos ataques controlados se suelen utilizar “máquinas señuelos”, implementadas con software especial para la tarea y una red configurada de manera que simule ser una red empresarial. De tal forma, los ataques se pueden monitorear y luego analizar para generar técnicas de defensa novedosas y adelantarse a un ataque en tiempo real sin perder bajas significativas.

Los ataques más comunes consisten en generar un colapso en los servidores de las páginas web, a través de solicitudes masivas a las cuales el servidor no es capaz de responder. Es decir, ante tal sobrecarga, el servidor es incapaz de recibir y contestar peticiones. Este tipo de ataque, DoS (*Siglas en inglés de Denegación de Servicio*) se realiza desde un solo ordenador, lo cual facilita el bloqueo de la IP desde donde se origina el ataque. El bloqueo niega el acceso al servidor atacado por parte del atacante.

Un ataque similar, conocido como “Denegación de servicios distribuida” (*DDoS, por sus siglas en inglés*), se diferencia en que el origen del ataque no parte desde una única IP, sino que de varias en forma simultánea. Estas computadoras suelen encontrarse infectadas por troyanos, los cuales aprovecha el atacante original para sincronizar el ataque.

Una de las técnicas para bloquear la petición de servicios es el bloque de las direcciones IP solicitante. Sin embargo, existen dos inconvenientes con este método. El primero es la posibilidad de bloquear el acceso a solicitudes legítimas al servicio web, el segundo corresponde a la capacidad del Firewall para controlar todos los paquetes entrantes (*Capacidad de Hardware*). Se suele recurrir a balanceadores de carga y servidores auxiliares para facilitar esta tarea.

Una estrategia diferente se basa en realizar un ajuste en la configuración TCP del sistema operativo del servidor que soporta el servicio WEB para aumentar los tiempos de respuesta. Se busca minimizar los efectos sobre el servicio que se ofrece a los usuarios mientras el ataque se encuentra en curso.

Las técnicas más efectivas poseen una estrategia combinada en referencia a las medidas de protección. Es decir, poseen un sistema de protección automático para bloqueo de direcciones IP, activación de recursos latentes, ajustes de configuración TCP o de parámetros de hardware para alivianar el uso de recursos. Algunos lenguajes de programación ofrecen módulos de protección que también pueden ser usados, por ejemplo PHP.

4.2 Aspectos legales en relación a la ciberguerra

4.2.a Ciberguerra

En el pasado, las guerras se llevaban a cabo en los espacios terrestres, marítimos, aéreos, e incluso el electromagnético. A partir de la década de los 90, debido al crecimiento de la infraestructura tecnológica y el uso de redes, el ciberespacio se tornó en un nuevo campo de batalla. Las consecuencias de la ciberguerra no solo se limitan a equipos informáticos, incluso pueden ser reflejadas en el mundo físico.

Ante estas amenazas, algunos países comenzaron a organizarse. Por ejemplo, Estados Unidos. Los desafíos tecnológicos inducen la creación de “ejércitos” dedicados al campo de la ciberguerra. Algunos de los miembros de estos grupos son hackers reconocidos, los cuales son tentados para participar de los mismos.

Con respecto a la regulación de los conflictos, los gobiernos que piensen en recurrir a la ciberguerra, deben tener en cuenta los derechos relacionados a las razones legítimas para entrar en guerra (*ius ad bellum*) y aquellos que refieren a las prácticas aceptables durante el conflicto (*ius in bello*) como si se tratase de un escenario común, ya que no hay regulaciones acordes a estos tipos de ataques que usan equipos informáticos.

4.2.b Normativas nacionales e internacionales

Una vez planteada la cuestión respecto al vacío legal en el ciberespacio y las posibles formas de regularlo, se expuso una normativa principal, la cual existe tanto en el plano nacional como internacional. Esta normativa es muy escasa y los estados no muestran voluntad en cumplirla actualmente.

La OTAN puso en marcha un programa global de coordinación para la ciberdefensa, con el objetivo de reforzar las capacidades de alianza y luchar contra los ataques informáticos. En este programa, se contemplan los ciberataques como acciones que pueden poner en riesgo la prosperidad, seguridad y estabilidad de los estados miembros, por lo que se dan recomendaciones sobre cómo actuar.

4.2.c Manual de Tallin

La falta de una legislación aplicable a los conflictos bélicos a través del ciberespacio, incentivo iniciativas como la convocatoria de un Grupo Internacional de Expertos (*GIE*) en defensa, ciberseguridad y derecho internacional, para crear un equivalente a la Convención

de Ginebra sobre DIH, aplicado al ciberespacio. El resultado fue el manual de Tallín, dirigido por Michael Schmitt de la US Naval War College, presentado en Londres en 2013.

La premisa fundamental para redactar el manual, fue que la guerra no deja de ser tal por llevarse a cabo en el ciberespacio. Actualmente no se tienen datos empíricos reales sobre los efectos de las ciberarmas, pero hechos como los de Estonia (2007) y Stuxnet (2010) hacen ver que los efectos pueden ser mucho más peligrosos que una simple denegación de servicio. Acciones como intrusiones en los ordenadores centrales de una represa con el fin de descargar el agua son equivalentes a si las compuertas se volaran con explosivos.

El manual, tiene como objetivos principales: unir el mundo cibernético con el jurídico en sus análisis y comprensiones mutuas. Valorar la capacidad de los estados de buscar consenso sobre límites éticos y jurídicos en el ciberespacio, especialmente respecto a la agresión armada y el empleo de la fuerza.

El manual de Tallín tiene los siguientes aspectos claves…

Ciberataque y conflictos del DIH: Partiendo de la definición de ciberataque como aquella operación cibernética ofensiva o defensiva de la que se espera que pueda causar pérdidas de vidas humanas, lesiones a las personas y daños o destrucciones de bienes; se puede ver que este tipo de acción entra dentro de la definición contemplada en el artículo 49 del Protocolo Adicional I a los Convenios de Ginebra. El primer aspecto controvertido es determinar si cualquier operación de ciberguerra puede ser considerada como un “conflicto armado” y regularse a través del DIH. Existen dos puntos de vista, uno afirma que cualquier ciberataque entra en tal categoría, mientras que en el otro creen que debe existir una relación directa entre la operación y los objetivos militares. La segunda opción tiende a ser la más lógica, ya que en un conflicto en proceso, pueden surgir ataques de actores no gubernamentales.
Soberanía y responsabilidad: La soberanía de un Estado también puede ser violada por ataques desde el ciberespacio. Los Estados deberán controlar las infraestructuras cibernéticas que se encuentren en su territorio o que actúan bajo su bandera, sin estar en sus límites geográficos. La controversia se refleja en la responsabilidad del estado ante acciones llevadas a cabo en su territorio, sin que se pueda comprobar conocimiento o capacidad para detectarlas a tiempo. Otro aspecto problemático es el control de un estado ante acciones que puedan llevar su nombre. En los ciberataques a Estonia en 2007, si bien se acusó a Rusia, jamás se pudo probar su implicancia.
Uso de la fuerza: Respecto a la ambigüedad existente, para determinar cuándo un acto en el ciberespacio se considera “uso de la fuerza” se tendrán en cuenta los efectos, los cuales deben ser comparables a los de un ataque convencional. Algunos indicios útiles para evaluar una acción cibernética son…

- Gravedad: Se trata del factor más importante y la cuestión fundamental será determinar cuáles son los límites que, una vez sobrepasados, determinan que se ha hecho "uso de la fuerza". El alcance, la duración y las consecuencias tendrán gran importancia en la valoración de su gravedad de la acción. En resumen, se tratará de responder a cuestiones como: ¿cuántas personas han muerto?, ¿qué daños se han causado?, etc.

- Inmediatez: Refiere a la separación temporal entre acciones y efectos. Muchas acciones en el ciberespacio no producen efectos inmediatos, sino que éstos aparecen con el paso del tiempo. Cuanto mayor sea la separación acción-efecto, más complicado será la posibilidad de afirmar que se ha hecho "uso de la fuerza".

- Intrusión: Se refiere al grado de penetración o alcance de las operaciones. Así, por ejemplo, una intrusión a un dominio gubernamental tiene mucho más peso que un ataque sobre dominio de uso común por la población civil.
  El ciberespionaje, que podría ser otra forma intrusión, no está considerado como un "uso de la fuerza". Un ejemplo serían las acciones para deshabilitar los mecanismos de seguridad y acceder a la información de una red. Sin embargo, un avión que penetra en un espacio aéreo, sin autorización y con intención de llevar a cabo acciones de ciberespionaje, si podría ser acusado de "uso de la fuerza".

- Carácter militar e implicación de estado: Cuanto mayor sea la relación entre las ciberoperaciones y las operaciones militares, mayor será la probabilidad de ser considerado un ciberataque como de "uso de la fuerza".

- La presunción de legalidad: El DIH es por naturaleza prohibitivo. Si algo no está prohibido estaría autorizado. El ciberespionaje, no parece que suponga una violación del DIH, en cuanto a ser considerado como "uso de la fuerza". A priori, no supone ni una violación del principio de no intervención ni siquiera un elemento coercitivo, aunque para ello tenga que superar elementos de seguridad (*cortafuegos,..*). Acciones de denegación de servicio, como los llevados a cabo en el caso de Estonia y que paralizaron su administración, no se consideraron tampoco como una violación del "uso de la fuerza".

Ataque armado: Definición íntimamente ligada al "Uso de la fuerza", cabría en los ataques informáticos que hieren, matan o destruyen propiedad, y no aquellos relacionados con inteligencia (*robo*) o los cuales no interrumpan servicios esenciales (*Un ataque que logre envenenar una distribuidora de agua sería considerado un ataque armado*).

A día de hoy, ningún ciberataque fue considerado un "ataque armado". Stuxnet, al atacar infraestructura nuclear de otra nación es el único que merecería tal clasificación. Este incidente resulta significativo porque, hasta la fecha, inhabilitar una instalación de este tipo sólo habría sido posible mediante alguna acción física, por ejemplo, un bombardeo.

Legítima defensa. Inminencia e inmediatez: Es necesario comentar que también en el ciberespacio, como ocurriría en el caso de armas nucleares, se puede aprobar la "legítima defensa anticipada" (*inminencia*). Aunque este tema ha planteado muchos debates, parece que ésta sólo se pudiera aprobar en el caso de que, de no llevarse a cabo y el estado esperara a sufrir un ciberataque, éste hubiera perdido cualquier oportunidad de responder ante los efectos del mismo (*la relación causa-efecto debe estar muy*

justificada).

Relacionado con la "legítima defensa" también estaría el principio de inmediatez. El requisito de "inmediatez" (*a diferencia de la exigencia de la inminencia*) distingue un acto de legítima defensa de la mera represalia. Si la "inminencia" plantea discusiones, la "inmediatez" lo es más ante el tiempo que puede transcurrir hasta que se descubran los efectos y la identificación de los culpables. Esto se debe a que los efectos de los ciberataques no siempre serán conocidos de inmediato y por lo tanto no será fácil verificar si se ha recurrido al "uso de la fuerza" que determine una respuesta del tipo "legítima defensa".

Principio de necesidad y proporcionalidad: La ciberguerra puede ser un medio recurrente para los actores que se enfrentan a oponentes con los que existe un gran desequilibrio en recursos militares *(personal, material, tecnología, etc.*). Esta asimetría de medios, también puede completarse con una asimetría de valores provocando que la ciberguerra sea parte de una "guerra sin restricciones".

Estas acciones deben responder al principio de necesidad de tal forma que se consiga un equilibrio entre las necesidades de la guerra y los condicionamientos humanitarios. En definitiva, se aplicarán ciberataques de tal grado que sus efectos sean los mínimos necesarios para conseguir el objetivo deseado, que es hacer que el enemigo cese en sus acciones.

La proporcionalidad hace referencia a la prohibición de armas y métodos que causen en las personas civiles y a sus bienes, o a ambos a la vez, daños excesivos con respecto a la ventaja militar concreta y directa prevista. Tras esta afirmación se plantea dos cuestiones: si hay alguna limitación o prohibición en cuanto a las ciberarmas. Todo parece apuntar que los efectos serán el factor que las delimite. Así pues, el alcance, duración e intensidad será el mínimo que haga al agresor desistir de sus acciones.

Participación directa en las hostilidades: Los civiles (*a veces de forma individual tipo "lobo solitario"*) podrían llevar a cabo ciberataques que tengan relación directa con las hostilidades, con los efectos ocasionados y a favor de una de las partes, por simpatizar con ellas.

El problema de estas acciones es la variable "tiempo". Los expertos, mayoritariamente, consideran que la participación comprende desde el momento de la preparación de la misión hasta el final de la participación activa.

Un atacante puede preparar un virus para ser introducido en el sistema informático que controla los procesos de una planta de depuración de aguas y que, al cabo de unos días, provoque muertos por envenenamiento entre la población. El inicio de la participación directa lo definiría el momento en que empieza a diseñar el virus informático, sin embargo, el final no queda claro. Se podría decir que acaba cuando lanza el virus, aunque los efectos se manifiesten después. Cabe también preguntarse si se le podría atacar, en el momento de conocer los efectos, aunque haya pasado ya un tiempo.

La mayoría del GIE acordó que los civiles retienen su estado civil, incluso si participan directamente en las hostilidades cibernéticos.

4.3 Situación en Argentina

En Argentina existe el “Comando conjunto de ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas”, el cual tiene funciones como…

- Ejercer la conducción de las operaciones de ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del instrumento militar de la defensa nacional.

- Coordinar acciones con los Centros de Ciberdefensa de las Fuerzas Armadas.

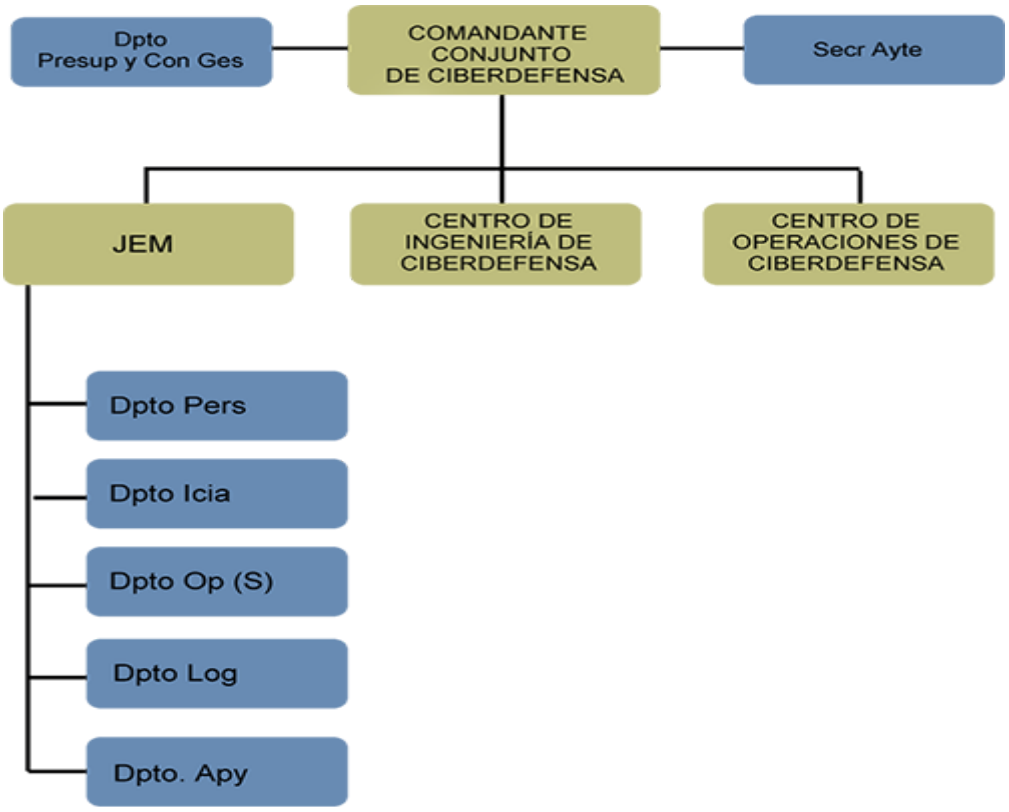
- Establecer los criterios rectores, para la determinación de infraestructuras críticas a ser protegidas.

- Capacitarse en estándares y procedimientos de ciberdefensa, criptografía, informática forense, en el proceso de capacitación de personal propio (*organización y desarrollo de actividades académicas como seminarios o simposios*).

- Intervenir en la elaboración, revisión y experimentación de doctrinas de ciberdefensa.

- Participar a requerimiento del Ministerio de Defensa, en apoyo a otros Organismos, en la concientización de las FF.AA. en materia de Ciberdefensa y en la determinación y supervisión de los estándares de seguridad y certificación de protocolos afines en las FF.AA.

<u>Estructura jerárquica:</u>



4.4 Responsabilidad de los distintos actores en relación a la ciberdefensa

Estado: Debe establecer o favorecer canales de colaboración eficientes entre proveedores tecnológicos, proveedores de ciberseguridad, organizaciones industriales y CERTs para alertas tempranas, así como generar regulaciones para controlar que las empresas tomen las medidas requeridas. Tiene la responsabilidad de fomentar planes de recuperación y continuidad, así como procesos que garanticen la recuperación de las configuraciones. También es obligación hacer partícipes a los miembros de las fuerzas de seguridad especializados para analizar los incidentes y confirmar si se trata de un ataque aislado o una amenaza para el país.
Proveedores tecnológicos: Deben definir buenas prácticas para el resguardo y la protección de configuraciones y archivos críticos de los sistemas, así como mantener canales de comunicación bidireccionales con las CERT nacionales y las fuerzas de ciberseguridad nacional.

Trabajar de forma conjunta entre proveedores permite generar, de manera más eficiente, herramientas y configuraciones para garantizar la integridad de los archivos y proteger los mismos de accesos no autorizados. Al momento de una intrusión, deberán analizar de forma conjunta el ataque con especialistas para definir y adecuar las medidas de prevención y defensa para nuevas instalaciones.
Organizaciones industriales: Deberán encargarse de establecer planes de recuperación y continuidad garantizando la recuperación de las configuraciones, dar alertas tempranas ante un incidente siguiendo los procedimientos establecidos, tanto dentro de la organización, como a nivel de los CERT nacionales y los proveedores tecnológicos. Estos planes se ejecutarán ante un incidente, además de realizarse un análisis forense.

5. Conclusión

Con el crecimiento tecnológico, el cual conlleva muchas ventajas tales como la comunicación instantánea, la posibilidad de compartir información en tiempo real desde cualquier punto del planeta solo con un dispositivo conectado a internet o poder acceder a una gran cantidad de informaciòn. Pero hay que tener en cuenta que dichos beneficios también traen consigo sus desventajas.

Ciertamente, siempre podemos estar expuestos a algún ciberataque, ya que los métodos ofensivos siempre están un paso adelante de las medidas de seguridad. No obstante, debemos adoptar ciertos hábitos para ayudar a prevenir el riesgo, como pueden ser, en un ámbito individual, instalar algunos software como un anti-virus y mantenerlo actualizado, otros como un anti-Spyware que tiene como objetivo la remoción y prevención de ejecución del software espía, no abrir ficheros de remitentes desconocidos, evitar la descarga de ficheros sospechosos o de URL no originales.
En un ámbito organizacional, poseer grandes sistemas de seguridad, personal capacitado para hacer frente a una amenaza, tener planes de contingencia y respuestas rápidas a un ataque.

La seguridad en la red, es una tarea que necesita de la colaboraciòn de todos, lo ideal es tomar conciencia del alcance que puede tener un ciberataque y sus consecuencias, el rango de éstas va desde la actividad criminal tradicional del hurto y fraude, hasta el espionaje avanzado y daño a la información y el equipamiento.

Es por ello que tanto el estado como las empresas deben establecer estructuras legales, programas educacionales y capacidad institucional para responder a los acontecimientos que se presenten a lo largo del espectro de amenazas. Dicha tarea no es imposible, solo requiere del tiempo y los recursos necesarios para ser llevada a cabo.