1. Introducción a la Ciberseguridad

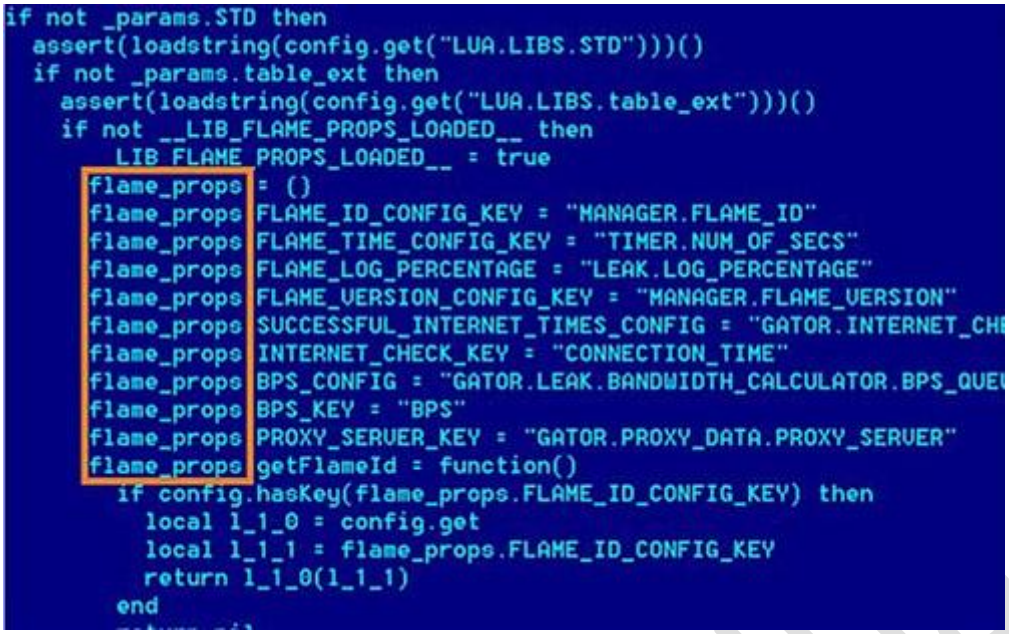
4. Incidentes de Ciberseguridad

4.1 Introducción

En un mundo hiperconectado como el actual donde nuestra dependencia de la tecnología es cada vez mayor, e incluso total en algunos casos, es de esperar que haya quien quiera sacar provecho usando cualquier medio que tenga a su alcance.

Los virus, troyanos y el malware en general existen desde hace años. En sus inicios, los creadores buscaban superarse, demostrar que podían enfrentarse a retos con éxito, conseguir el reconocimiento de otros desarrolladores,… Después entró en juego el dinero. El objetivo de los creadores de malware era y sigue siendo conseguir dinero, en grandes cantidades en algunos casos.

Sin embargo, en los últimos años y, sobre todo, en los últimos meses, estamos asistiendo al auge de un malware que tiene otro objetivo que hasta ahora sólo habíamos visto en películas de ciencia ficción. A lo largo del año 2012 se llevaron a cabo ataques cibernéticos a gran escala contra empresas, gobiernos e infraestructuras de países. Famosos son ya engendros como Duqu, Stuxnet, Flame o Gauss, diseñados para atacar sistemas de control industrial, recopilar información, robar certificados digitales…



```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
      __LIB_FLAME_PROPS_LOADED__ = true
      flame_props = {}
      flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHE
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEU
      flame_props.BPS_KEY = "BPS"
      flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
```

La mayoría de los expertos están de acuerdo en que estas creaciones no son producto de un hacker o un grupo de hackers que trabajan de forma independiente, sino que ha sido necesario el apoyo logístico y financiero de gobiernos con intereses muy concretos.

Según James Lewis, del Centro de Estudios Estratégicos e Internacionales, 12 de las 15 mayores potencias militares ya están desarrollando sus propias estrategias de ataque y defensa electrónica. Podemos hablar de una Ciberguerra Fría, que parece que no va a hacer sino ir a más como ocurrió en 2013 y seguirá en este 2014 que acaba de empezar.

Estos gobiernos están construyendo a marchas forzadas sus arsenales digitales y algunos están llegando a subcontratar ataques a grupos de hackers. Según ha reconocido la Administración Obama, Estados Unidos está sufriendo ciberataques de forma continua y se ha calificado como especialmente vulnerables el sistema bancario, los mercados de valores, las plantas nucleares y los sistemas de depuración de agua. De hecho, en abril de 2012 se aprobó CISPA (Cyber Intelligence Sharing and Protection Act), que permite al gobierno americano obtener y compartir información crucial de ataques con empresas:

http://money.cnn.com/2012/04/27/technology/cispa-cybersecurity/index.htm

Un temor que ha surgido entre los investigadores de seguridad, es que el crecimiento en número y en intensidad de estos ataques podría tener como consecuencia por primera vez la pérdida de vidas. No parece probable, pero es posible.

Incluso si no llega a ponerse en riesgo la vida de personas, de lo que no hay duda es de que estos ataques son cada vez más destructivos. Baste el ejemplo del ataque que sufrió la petrolera saudí Aramco en agosto de 2012, que dejó inservibles 30000 ordenadores, o el ataque de denegación de servicio (DoS) masivo y considerado el mayor de la historia que sufrieron los sitios web de Bank of America, JP Morgan Chase, Wells Fargo, U.S. Bank y otros en septiembre.

4.2 El ataque a ARAMCO

Fue el 15 de agosto de 2012 cuando un equipo de expertos en seguridad informática que incluía representantes de Oracle, IBM, Crowdstrike, Red Hat, McAfee, Microsoft y otras empresas, llegó a Arabia Saudí para investigar el ataque sufrido por ARAMCO.

El ataque se produjo en la víspera de un día santo musulmán llamado Lailat al Qadr, "la Noche de Poder." Técnicamente, el ataque fue crudo, pero sus implicaciones geopolíticas pronto se convertirían en alarmantes.

Los datos de tres cuartas partes de las máquinas de la red principal de Aramco habían sido destruidos. Los atacantes, que se identificaron como islámicos y se hacían llamar la Cortante Espada de la Justicia ejecutaron un completo barrido de los discos duros de 30000 ordenadores personales de Aramco. En buena medida, a modo de tarjeta de visita, dejaron en la pantalla de cada máquina borrada una imagen de una bandera americana en llamas.

Inmediatamente después del ataque, cuando los analistas forenses comenzaron a trabajar en la investigación, funcionarios de Estados Unidos a medio mundo de distancia se reunieron en la Sala de Situación de la Casa Blanca, donde los jefes de las agencias especularon acerca de quién había atacado a Aramco y por qué, y lo que estos atacantes podrían hacer a continuación. La Cortante Espada afirmó que actuó en venganza por el apoyo del gobierno saudí a "crímenes y atrocidades" en países como Bahrein y Siria. Pero los funcionarios que se reunieron en la Casa Blanca no pudieron evitar preguntarse si el ataque fue promovido por Irán, utilizando al aliado saudita de Estados Unidos como un proxy, contra el programa en curso de guerra cibernética emprendida por EE.UU. e Israel, y probablemente otros gobiernos occidentales, en contra del programa nuclear iraní.

Cuando la historia de la guerra cibernética se empezó a escribir, su primera frase podría ser algo como esto: "Israel dio a Estados Unidos un ultimátum." Desde hacía varios años, los informes de inteligencia indicaban de forma intermitente que Irán se estaba acercando a la construcción de una bomba nuclear, que los dirigentes israelíes veían como una amenaza existencial. En 2004, Israel entregó a Washington una lista de armas y otras capacidades que quería adquirir. La lista, que incluía diversos tipos de hardware y elementos como códigos de transmisión aérea, de forma que los aviones israelíes pudieran sobrevolar Irak sin tener que preocuparse de ser derribados por los aviones de EE.UU., deja pocas dudas de que Israel estaba planeando un ataque militar para impedir el progresó nuclear de Irán. El presidente George W. Bush consideró dicha acción como inaceptable, aunque reconoció que la diplomacia y las sanciones económicas no habían logrado cambiar la opinión de Irán.

Los funcionarios de inteligencia y de defensa ofrecieron una posible tercera vía, un programa de ciberoperaciones, montado con la ayuda de Israel y tal vez otros aliados, que atacara el programa nuclear de Irán de manera subrepticia y que permitiera ganar algo de tiempo. Al igual que con el programa de aviones no tripulados (drones), el gobierno de Obama heredó este plan, lo aceptó, y se ha seguido promoviendo de una manera importante. Se han lanzado ciberoperaciones significativas contra Irán, y los iraníes sin duda lo han notado. Puede ser que estas operaciones eventualmente cambien las mentes en Teherán, pero ataques como el de Aramco sugieren que, por el momento, el objetivo puede estar más interesado en el contraataque, y con armas de la misma naturaleza.

El ciberespacio es ahora un campo de batalla. Pero es una batalla que no se puede ver, y cuyos conflictos son rara vez descritos públicamente hasta mucho tiempo después de que hayan ocurrido. El conocimiento de la guerra cibernética es intensamente restringido: casi toda la información acerca de estos eventos queda clasificada tan pronto como se descubre. Los comandantes generales de esta guerra tienen poco que decir. Michael Hayden, que fue director de la C.I.A. cuando ocurrieron algunos de los ciberataques de Estados Unidos contra Irán, se negó una solicitud de entrevista con un e-mail de una única línea: "No sé lo que tendría que decir más allá de lo que he leído en los periódicos." Pero con la ayuda hackers de alto rango en el sector privado, así como de funcionarios y exfuncionarios de establecimientos militares y de inteligencia y la Casa Blanca, es posible describir el estallido de la primera ciberguerra mundial conocida y algunas de las batallas clave que se libraron hasta el momento.

4.3 Flame, Duqu, Gauss

Corría el año 2005, y Wes Brown, un hacker sordo y con parálisis cerebral, comenzó un negocio llamado Ephemeral Security con un colega llamado Scott Dunlop. Bancos y otras empresas contrataron a Ephemeral para hackear sus redes y robar información y que luego les dijeran cómo evitar esos ataques. Así que Brown y Dunlop pasaron mucho tiempo ingeniando estos robos. A veces utilizaban estas ideas para aumentar su fama y hacer publicidad de su negocio, haciendo presentaciones en conferencias de la élite de hackers que implican algunas de las mentes más brillantes del mundo.

En un café de Maine, Brown and Dunlop comenzaron una tormenta de ideas, y lo que produjeron fue una herramienta para atacar redes y recopilar información en pruebas de penetración que luego se convirtió en un modelo revolucionario para el espionaje. En julio de ese año, los dos hombres terminaron de escribir un programa llamado Mosquito. Mosquito no sólo ocultó el hecho de que robaba información, sino que sus métodos de espionaje podían ser actualizados, cambiados, y ser reprogramado de forma remota a través de una conexión cifrada con un servidor Command & Control. En 2005 la presentación de Mosquito fue una de las más populares en la prestigiosa conferencia de hackers Def Con, en Las Vegas.

http://www.youtube.com/watch?v=3bPLrIeLb2M

Muchos funcionarios militares y de inteligencia de Estados Unidos asisten a Def Con y lo han estado haciendo durante años.

Como recuerda Wes Brown, ninguno de estos funcionarios del gobierno que acudieron a la conferencia dijo una palabra después de su presentación de Mosquito. "Nadie que yo pudiera identificar como tipos de gobierno, por lo menos", añade, con una sonrisa. Pero dos años más tarde, probablemente en 2007, el malware conocido ahora como Flame apareció en Europa y se extendió a miles de máquinas en Oriente Medio, sobre todo en Irán. Al igual que Mosquito, Flame incluyó módulos que podrían, a través de una conexión cifrada a un servidor Command and Control, actualizarse, cambiarse, y reprogramarse de forma remota. El software Flame escondía una gran variedad de trucos. Un módulo secretamente activaba el micrófono de la víctima y grababa todo lo que podía oír. Otro recogía los planos arquitectónicos y esquemas de diseño, buscando el funcionamiento interno de las instalaciones industriales. Otros módulos de Flame tomaban imágenes de los ordenadores de las víctimas; registraba la actividad del teclado, incluyendo contraseñas, registraba conversaciones de Skype, y los ordenadores infectados se veían obligados a conectarse a través de Bluetooth a cualquier dispositivo con capacidad Bluetooth cercano, como teléfonos móviles, para luego extraer sus datos.

Durante ese mismo período, un virus que sería nombrado Duqu y que tuvo como objetivo menos de 50 máquinas, principalmente en Irán y Sudán, comenzó a recopilar información sobre los sistemas informáticos que controlaban la maquinaria industrial, y para diagramar las relaciones comerciales de diversas organizaciones iraníes. Duqu, al igual que muchas otras piezas significativas de malware, fue nombrado así por una característica del código, en este caso derivada de los nombres que el malware dio a los archivos que creó. Con el tiempo, los investigadores encontraron que Duqu tenía varias semejanzas con un ciberataque aún más virulento.

Ya en 2007, las primeras versiones de un gusano informático, que no estaba diseñado para el espionaje, sino para el sabotaje físico de maquinaria, comenzaron a infectar ordenadores en varios países, principalmente en Irán. Fue una de las piezas más resistentes, sofisticadas y nocivas de malware que se hayan visto. Al año siguiente, después de que el gusano se soltara en Internet, los análisis de expertos privados dieron resultados sobre su origen y objetivos. Nombrado Stuxnet, el gusano parecía haber venido de los EE.UU. o Israel (o ambos), y parecía haber destruido centrifugadoras de enriquecimiento de uranio en la planta nuclear de Irán en Natanz. Si las suposiciones sobre Stuxnet eran correctas, entonces era la primera ciberarna conocida para causar daño físico significativo a su objetivo. Una vez liberado en el medio natural, Stuxnet realizó una compleja misión de buscar y destruir a su objetivo. Jason Healey, ex funcionario de la Casa Blanca, que ahora dirige la Iniciativa Cyber Statecraft para el Consejo Atlántico, sostiene que Stuxnet fue "la primera arma autónoma, con un algoritmo, no una mano humana, capaz de apretar el gatillo."

En septiembre de 2011, otra pieza de malware llevó a la Web: Gauss, que robó información y credenciales de acceso de bancos en el Líbano, un aliado de Irán. (El programa se llama Gauss, como Johann Carl Friedrich Gauss, ya que, como los investigadores descubrieron más tarde, algunos módulos internos habían recibido nombres de matemáticos) Tres meses después, en diciembre, una nueva pieza de malware comenzó a espiar a más de 800 ordenadores, principalmente en Irán, pero también en Israel, Afganistán, los Emiratos árabes Unidos y Sudáfrica. Éste finalmente se llamaría Mahdi, debido a una referencia en el código de software a una figura mesiánica que tiene como misión, según el Corán, limpiar el mundo de la tiranía antes del Día del Juicio. Mahdi se envió por correo electrónico a personas que trabajaban en agencias gubernamentales, embajadas, empresas de ingeniería y compañías de servicios financieros. En algunos casos, los correos electrónicos Mahdi llevaban un archivo adjunto de Microsoft Word que contenía un artículo acerca de un plan secreto del gobierno israelí para paralizar la red y eléctrica y de telecomunicaciones de Irán en el caso de un ataque militar israelí. Otros correos electrónicos de Mahdi se enviaron con archivos de PowerPoint que contenían diapositivas con imágenes religiosas y texto. Cualquier persona que recibía estos mensajes de correo electrónico y hacía clic en el archivo adjunto se hacía vulnerable a la infección, lo que podría dar lugar a que sus e-mails, mensajes instantáneos y otros datos estuvieran siendo monitorizados.

4.4 La respuesta a estos ataques

EE.UU. comenzó a cultivar las cibercapacidades como un complemento a sus operaciones diplomáticas, de inteligencia y militares. El Impulso inicial de Irán era para reprimir la disidencia interna, especialmente a raíz de las protestas de la Revolución Verde en 2009, cuando los ciudadanos salieron a las calles para disputar la reelección del presidente Mahmoud Ahmadinejad. Pero desde el ataque Stuxnet, Irán ha mejorado de su capacidad de guerra cibernética. Unas declaraciones públicas de los líderes del gobierno en marzo de 2011 indicaron que la Guardia Revolucionaria iraní había creado una unidad cibernética para coordinar ataques. En marzo de 2012, el ayatolá Ali Jamenei, creó el Consejo Superior del Ciberespacio; según los informes, Irán gastó mil millones de dólares en la construcción de sus cibercapacidades.

Durante la segunda semana de septiembre de 2012 comenzó una nueva ola de ataques cibernéticos contra intereses estadounidenses. Esta vez, los blancos estaban en suelo americano: los bancos estadounidenses. Un grupo hasta ahora desconocido que se hace llamar los Luchadores Cibernéticos de Izz ad-Din al-Qassam y presentándose como una organización de los yihadistas suníes hizo una publicación en línea escrita en Inglés, en referencia a un vídeo anti-islámico en YouTube llamado "La inocencia de los musulmanes", que habían provocado disturbios en el mundo musulmán la semana anterior. La publicación afirma que "los musulmanes deben hacer lo que sea necesario para detener la difusión de esta película. Todos los jóvenes musulmanes que están activos en el mundo cibernético atacarán a las bases estadounidenses y sionistas en la web tanto como sea necesario hasta que pidan disculpas por ese insulto".

Si Qassam fuera realmente eran un grupo suní yihadista, Irán, una nación predominantemente chií, difícilmente habría participado. Pero el aspecto yihadista parece ser una falsa bandera. Como un analista de inteligencia de EE.UU. señala, nada en el lenguaje utilizado en la comunicación pública de Qassam tiene ningún parecido con el lenguaje estándar de los grupos yihadistas. No había rastro de la organización Qassam en cualquier foro sunita, yihadista, o de al-Qaeda. Y el propio nombre Qassam se refiere a un clérigo musulmán que tiene importancia para los palestinos y Hamas, pero no para los yihadistas. "Todo está mal", dice este analista. "Parece prefabricado."

Qassam anunció que iba a inundar el Bank of America y la Bolsa de Valores de Nueva York con (DDoS), denegación de servicio distribuida. Estos ataques tratan de bloquear un sitio Web o inducir la caída de una red informática al hacer una abrumadora cantidad de solicitudes de conexiones. Qassam procedió a ampliar sus objetivos para incluir muchos más bancos, incluyendo SunTrust, Regions Financial, Webster Financial Corporation, JPMorgan Chase, Citigroup, Wells Fargo, EE.UU. Bancorp, Capital One, PNC, Fifth Third Bank, HSBC, y BB & T. Qassam golpeó al menos cinco de los sitios Web de estos bancos, aunque la mayoría de los bancos han dicho que se robó dinero o información. En octubre, el CEO de PNC, James Rohr, señaló que "hemos tenido el ataque más largo de todos los bancos " y advirtió que "los ataques cibernéticos son muy reales, y si pensamos que estamos a salvo, sólo estamos tomándonos el pelo a nosotros mismos.". Poco después, los ataques a PNC aumentaron, causando más problemas. Ni Rohr ni ningún otro ejecutivo de alto nivel de cualquier banco víctima ha hecho desde entonces cualquier mención. "La lección de la declaración de Rohr era, no hables", dice un ex funcionario de seguridad nacional.

Las comunicaciones de Qassam han sido relacionadas con un servidor en Rusia que ya había sido una vez utilizado para actividad ilícita. Esto podría indicar que los ataques de Qassam fueron planeados con mayor cuidado y deliberación de lo que es típico en intrusiones hacktivistas o

criminales, que por lo general vienen de servidores donde la actividad ilícita es común. Esta dirección IP dirección, sin embargo, como en casi todos los rastreos de tráfico Web, podría haber sido falseada. Sean quienes sean, Qassam tiene sentido del humor porque algunos de los ordenadores que aprovecharon para su uso en los ataques a bancos estaban ubicadas dentro del Departamento de Seguridad Nacional de EE.UU.

Otro hackeo provocó una amenaza financiera aún más dramática, aunque su origen era difícil de discernir. El 23 de abril de 2013, la cuenta de Twitter de la Associated Press envió este mensaje: "Urgente: Dos explosiones en la Casa Blanca y Barack Obama está herido" Ante esta noticia, el Dow Jones Industrial Average cayó 150 puntos, el equivalente a 136 mil millones de dólares en cuestión de minutos. Al saber que la información era falsa y que la cuenta de la AP simplemente había sido secuestrada, los mercados se recuperaron. Un grupo autodenominado Ejército Electrónico Sirio (SEA Syrian Electronic Army) se atribuyó el ataque.

Un ciberanalista de oriente medio en Londres dijo que "hay fuertes indicios de que los miembros de SEA fueron entrenados por expertos iraníes." Y un analista norteamericano señaló que el hackeo a AP, no sólo se asemeja a la técnica de Qassam, sino que también refleja la propia percepción de Irán de lo que los EE.UU. ha hecho a la República Islámica. (El año anterior, antes de Qassam comenzara sus ataques a los bancos, los medios de comunicación iraníes estatales afirmaron que los EE.UU. habían llevado la moneda de Irán al borde del colapso por decir mentiras sobre Irán.) En este momento, no hay evidencia sólida de que Irán tomara parte para el hackeo de AP.

En noviembre de 2012, una Directiva de Política Presidencial clasificada fue filtrada a The Washington Post, la Directiva permite a los militares tomar medidas más agresivas para defender las redes de computadoras en los EE.UU. En diciembre, Irán llevó a cabo un simulacro de guerra cibernética durante sus ejercicios navales en el Estrecho de Ormuz, para demostrar la capacidad de recuperación de sus submarinos y misiles ante un ataque cibernético. En enero de 2013, funcionarios del Pentágono informan, que aprobaron un aumento de cinco veces en el número de personal del Comando Cibernético EE.UU., de 900 a 4900, en los años siguientes. Un general iraní, como en respuesta, señaló públicamente que la Guardia Revolucionaria controla "el cuarto mayor ejército cibernético en el mundo."

4.5 Mercado de Armas Cibernéticas

En medio de todo esto, el ala secreta de investigación y desarrollo del Pentágono, la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA), invitó a los piratas informáticos a proponer "tecnologías revolucionarias para la comprensión, gestión y planificación de la guerra cibernética " para su uso en un nuevo esfuerzo llamado "Plan X."

Durante al menos una década, los gobiernos occidentales - entre ellos los EE.UU., Francia, e Israel - han comprado "bugs" (defectos en los programas informáticos que hacen posible las vulnerabilidades), así como exploits (programas que realizan trabajos como espionaje o robo) no sólo a contratistas de defensa, sino también a hackers individuales.

Los vendedores en este mercado cuentan historias que sugieren escenas de novelas de espionaje. Un servicio de inteligencia del país crea empresas de fachada ciberseguridad, invitan a hackers a entrevistas de trabajo falsas, y compran sus bugs y exploits para agregarlos a su arsenal. Los defectos de software ahora forman la base de ciberoperaciones de casi todos los gobiernos, gracias en gran parte al mercado negro - el bazar de ciberarmas donde hacktivistas y criminales compran y venden.

4.6 Ciberespionaje

Edward Snowden y PRISM se han convertido en habituales en las noticias diarias y no en la sección de Tecnología, sino en la primera página de noticias sobre Política.

http://es.wikipedia.org/wiki/Edward_Snowden

En los últimos años, los ataques cibernéticos, el ciberterrorismo y el espionaje cibernético se han vuelto más frecuentes en la conciencia pública. Muchos gobiernos han ayudado a que el tema de la seguridad cibernética se introduzca en la agenda corporativa y han llamado la atención sobre un fenómeno que está costando a las economías una cantidad astronómica de dinero cada año. Como si quisiera asegurarse de que los consumidores y las empresas están prestando atención a la seguridad en línea, Edward Snowden filtró detalles de PRISM a principios de junio de 2013.

Como un sueño de un teórico de la conspiración, PRISM fue el proyecto de la Agencia de Seguridad Nacional de EE.UU. que le da acceso a los contenidos de servidores de los gigantes de internet de Estados Unidos - que es casi como decir todos los gigantes de Internet. Todos los datos que fluyen a través de estos servidores son ahora visibles para el Gobierno de los EE.UU. El Gobierno ahora admite que trata de llevar a cabo la vigilancia sobre ciudadanos no estadounidenses. Sin embargo, es irrelevante que las personas que utilizan estos gigantes estén fuera de los EE.UU. - si su flujo de datos pasa a través de estos servidores, PRISM puede espiarlos.

http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

El sentir global de indignación por PRISM ha provocado quejas de gobiernos, sin embargo, pocos pueden decir que sea una sorpresa total. En el Reino Unido, por ejemplo, los ISP están obligados a mantener todos los datos durante un año, en caso de que sean requeridos por las fuerzas policiales o agencias gubernamentales.

El advenimiento de Big Data ha significado que la cantidad colosal de información que pasa a través de estos servidores puede ahora ser analizada.

http://es.wikipedia.org/wiki/PRISM