CyberEspías (Un Futuro Diferente nº 81) (Spanish Edition)

Oswaldo Enrique Faverón Patriau

CyberEspías (Un Futuro Diferente nº 81) (Spanish Edition) Oswaldo Enrique Faverón Patriau

El espionaje, es el proceso de obtener ilegalmente información secreta, es una herramienta utilizada por líderes nacionales, entidades sub-estatales, empresas internacionales y otros actores de la esfera global para tomar decisiones con mejor información.
La ciberseguridad y la ciberdefensa son áreas que se están convirtiendo en prioridades para los gobiernos, debido al incremento del ciberespionaje y otras amenazas basadas en internet. Estados Unidos ha situado a la seguridad del ciberespacio y su defensa en la primera línea de su estrategia de defensa.
Tanto Estados Unidos como China saben bien como el ciberespionaje podría dañar a sus economías. Los ataques de los hackers son la forma más moderna de cometer espionaje.
Según Verizon el 96% del ciberespionaje apoyado por estados se rastrea hasta China. Karspersky apunta a Rusia como el país más atacado del mundo y asegura que el 44% de los ataques web neutralizados por productos de Kaspersky Lab se llevaron a cabo utilizando recursos web maliciosos localizados en EE.UU. y Alemania.
Según Verizone el ciberespionaje es el 22% de las violaciones de seguridad de los datos, el 87% del espionaje electrónico llevado a cabo por los gobiernos, el 11% por el crimen organizado, el 1% por competidores y el restante 1% por un antiguo empleado.
Las direcciones IP de espionaje con software malicioso están situadas en: EE.UU. 54%, Corea 17%, Taiwán 12%, China 9% y Hong Kong 8%. Sin embargo aclaramos que las direcciones IP pueden estar localizadas en un país distinto al del atacante. Uno de los problemas a los que se enfrentan los estados para combatir el ciberespionaje es la dificultad de identificar la fuente de los ciberataques.
Los estudiantes en Rusia y Europa oriental buenos en matemáticas e informática no pueden encontrar trabajos fácilmente porque las economías de sus países son demasiado pequeñas para absorber el talento informático. Los grupos de crimen organizado pagan hasta 10 veces más que en los trabajos de TI legítimos a los mejores graduados.
De acuerdo al informe del Instituto Tecnológico de Massachussets (MIT) «Espías, Tecnología y Negocios» las empresas se están convirtiendo en peones en la Guerra cibernética; hay que resaltar que es muy difícil trazar el límite entre la empresa y la nación.
La seguridad pude convertirse en uno de los principales puntos para decidir entre marcas y servicios. Hay también nuevos negocios emergiendo: las granjas de

servidores seguros en Suiza (Deltalis, por ejemplo) un país que se está convirtiendo en «una plataforma de tecnología avanzada de seguridad» o los criptófonos de ESD America son sólo un par de ejemplos. Los estados están formando grupos rápidos de respuesta a los ciberataques.
Los ciberataques están incrementándose; el gobierno estadounidense está promoviendo cibercarreras, tratando así de satisfacer una demanda a todas luces insatisfecha.
El mundo cibernético es un nuevo campo e implica una nueva forma de relación internacional, está creciendo rápidamente y es cada vez más sofisticado.
Un reciente estudio apunta hacia un cambio en la tendencia de las actividades delictivas a gran escala en el futuro. Diferentes estudios apuntan a que el ciberespionaje se acabe convirtiendo en la actividad criminal más rentable, superando al tráfico de drogas.
El ciberespionaje exige apenas una inversión inicial. Una sola persona bien equipada puede acceder a datos personales de incalculable valor, eliminando todo tipo de intermediación al respecto. La existencia de enormes bolsas de datos en la Red hace que todos los sectores poblacionales puedan ser espiados y aprovechados económicamente. Un negocio amoral y rentable.
Los programas digitales de espionaje constituyen las ciberarmas de la nueva guerra digital; por ello debemos pensar seriamente acerca de nuestra dependencia a la computadora, a fin de contrarrestar sus debilidades con una protección cibernética más eficiente.

CyberEspías (Un Futuro Diferente nº 81) (Spanish Edition)

Oswaldo Enrique Faverón Patriau

CyberEspías (Un Futuro Diferente nº 81) (Spanish Edition) Oswaldo Enrique Faverón Patriau

El espionaje, es el proceso de obtener ilegalmente información secreta, es una herramienta utilizada por líderes nacionales, entidades sub-estatales, empresas internacionales y otros actores de la esfera global para tomar decisiones con mejor información.
La ciberseguridad y la ciberdefensa son áreas que se están convirtiendo en prioridades para los gobiernos, debido al incremento del ciberespionaje y otras amenazas basadas en internet. Estados Unidos ha situado a la seguridad del ciberespacio y su defensa en la primera línea de su estrategia de defensa.
Tanto Estados Unidos como China saben bien como el ciberespionaje podría dañar a sus economías. Los ataques de los hackers son la forma más moderna de cometer espionaje.
Según Verizon el 96% del ciberespionaje apoyado por estados se rastrea hasta China. Karspersky apunta a Rusia como el país más atacado del mundo y asegura que el 44% de los ataques web neutralizados por productos de Kaspersky Lab se llevaron a cabo utilizando recursos web maliciosos localizados en EE.UU. y Alemania.
Según Verizone el ciberespionaje es el 22% de las violaciones de seguridad de los datos, el 87% del espionaje electrónico llevado a cabo por los gobiernos, el 11% por el crimen organizado, el 1% por competidores y el restante 1% por un antiguo empleado.
Las direcciones IP de espionaje con software malicioso están situadas en: EE.UU. 54%, Corea 17%, Taiwán 12%, China 9% y Hong Kong 8%. Sin embargo aclaramos que las direcciones IP pueden estar localizadas en un país distinto al del atacante. Uno de los problemas a los que se enfrentan los estados para combatir el ciberespionaje es la dificultad de identificar la fuente de los ciberataques.
Los estudiantes en Rusia y Europa oriental buenos en matemáticas e informática no pueden encontrar trabajos fácilmente porque las economías de sus países son demasiado pequeñas para absorber el talento informático. Los grupos de crimen organizado pagan hasta 10 veces más que en los trabajos de TI legítimos a los mejores graduados.
De acuerdo al informe del Instituto Tecnológico de Massachussets (MIT) «Espías, Tecnología y Negocios» las empresas se están convirtiendo en peones en la Guerra cibernética; hay que resaltar que es muy difícil trazar el límite entre la empresa y la nación.
La seguridad pude convertirse en uno de los principales puntos para decidir entre marcas y servicios. Hay también nuevos negocios emergiendo: las granjas de servidores seguros en Suiza (Deltalis, por ejemplo) un país que se está convirtiendo en «una plataforma de tecnología avanzada de seguridad» o los criptófonos de ESD America son sólo un par de ejemplos. Los estados están formando grupos rápidos de respuesta a los ciberataques.
Los ciberataques están incrementándose; el gobierno estadounidense está promoviendo cibercarreras, tratando así de satisfacer una demanda a todas luces insatisfecha.
El mundo cibernético es un nuevo campo e implica una nueva forma de relación internacional, está creciendo rápidamente y es cada vez más sofisticado.
Un reciente estudio apunta hacia un cambio en la tendencia de las actividades delictivas a gran escala en el futuro. Diferentes estudios apuntan a que el ciberespionaje se acabe convirtiendo en la actividad criminal más rentable, superando al tráfico de drogas.
El ciberespionaje exige apenas una inversión inicial. Una sola persona bien equipada puede acceder a datos personales de incalculable valor, eliminando todo tipo de intermediación al respecto. La existencia de enormes bolsas de datos en la Red hace que todos los sectores poblacionales puedan ser espiados y aprovechados económicamente. Un negocio amoral y rentable.

Los programas digitales de espionaje constituyen las ciberarmas de la nueva guerra digital; por ello debemos pensar seriamente acerca de nuestra dependencia a la computadora, a fin de contrarrestar sus debilidades con una protección cibernética más eficiente.

Leer CyberEspías (Un Futuro Diferente nº 81) (Spanish Edition) by Oswaldo Enrique Faverón Patriau para ebook en líneaCyberEspías (Un Futuro Diferente nº 81) (Spanish Edition) by Oswaldo Enrique Faverón Patriau Descarga gratuita de PDF, libros de audio, libros para leer, buenos libros para leer, libros baratos, libros buenos, libros en línea, libros en línea, reseñas de libros epub, leer libros en línea, libros para leer en línea, biblioteca en línea, greatbooks para leer, PDF Mejores libros para leer, libros superiores para leer libros CyberEspías (Un Futuro Diferente nº 81) (Spanish Edition) by Oswaldo Enrique Faverón Patriau para leer en línea.Online CyberEspías (Un Futuro Diferente nº 81) (Spanish Edition) by Oswaldo Enrique Faverón Patriau ebook PDF descargarCyberEspías (Un Futuro Diferente nº 81) (Spanish Edition) by Oswaldo Enrique Faverón Patriau DocCyberEspías (Un Futuro Diferente nº 81) (Spanish Edition) by Oswaldo Enrique Faverón Patriau MobipocketCyberEspías (Un Futuro Diferente nº 81) (Spanish Edition) by Oswaldo Enrique Faverón Patriau EPub

0U32LQOS9VB0U32LQOS9VB0U32LQOS9VB